The trade-off between usability and security in the context of eGovernment

by

Abdulla Juma Abdulla Ali ALSHAMSI

Submitted in partial fulfilment of the requirements for the award of the degree of **Doctor of Philosophy** of the University of Keele

December 2019

Acknowledgements

I would like to express my gratitude to many people for their constant support, contribution encouragement, without which this thesis would not have been possible.

I am greatly indebted to my supervisor Professor, Peter Andras, for his great advice, support, encouragement and perceptive ideas throughout the duration of research and writing-up process for my PhD. Thank you for making my stay at Keele University memorable and my PhD experience wonderful.

I would like also to thank my beloved country United Arab of Emirates (U.A.E) and my scholarship provider, the Ministry of Defence, for offering me the opportunity to undertake this thesis.

I would also like to acknowledge my friends, the academic staffs and all the PhD students at the School of Computing and Mathematics, Keele University. Thank you all for your friendship and support.

Last but not least, my endless and deepest appreciations go to Parents, Brothers, my Wife, and Children (Nahyan, Manayer, and Nayel) for their continuing love and support.

Author's Declaration

During this Ph.D. a significant portion of work has already been published or been sent for publication. Details of papers along with Journal, conference are presented in this section:

Journal Papers

- Abdulla Alshamsi and Peter Andras (2019) ***User perception of Bitcoin usability and security across novice users***. International Journal of Human-Computer Studies 126, 94-110.

- Abdulla Alshamsi and Peter Andras (2019) ***Users' perception of Smartwatch usability and security***. Sent for publication, International Journal of Human-Computer Studies.

Refereed Conference Papers

- Abdulla Alshamsi, Nikki Williams, Peter Andras (2016) ***The trade-off between usability and security in the context of eGovernment: a mapping study***. In Proceedings of the 30th International BCS Human Computer Interaction Conference: Fusion!, p. 36.

Table of Contents

List of Tables

List of Figures

Abstract

Electronic government (e-government) implements a wide range of online services that are supported by the latest information communication technology (ICT) and accessible by devices that have great mobility in delivering services to citizens. The ongoing rapid advancements of these portable devices make user centred service design more challenging and complex as citizens' demands, needs and preferences are varied and become more complicated over time. Also, existing research reveals that e-government still experiencing the challenge of creating better users' interaction in terms of accessing online information and using electronic services. Among a variety of reasons for this challenge, usability and security have been recognised in previous research to be the main reasons in users' decisions to use e-government services and need to be investigated. In addition, to the limited attention given to users' preferences and human-centred design guidelines, creates more unusable and unsecure services.

This research attempts to investigate the trade-off between usability and security from a user perspective, in order to understand how users, perceive the usability and security of e-government services by focusing on three elements of e-government. The research investigates three aspects related to e-government services, when new service being introduced, new devices being integrated, and new technology adopted. Each research study examines one of these aspects to explore how users or citizens perceive them in term of usability and security. By conducting these three studies, the researcher seeks a clear and comprehensive picture of users' attitudes, opinions and preferences, and a rich insight into users' needs. This research tries to explain user requirements for new services, devices and technology implemented in e-government settings, in terms of usability and security features. A mixed methods strategy, using quantitative and qualitative methods, is used capture users' experiences and attitudes to the use of e-government services in terms of usability and security. These methods help us understand the three, related, aspects of e-government through the eyes of the participants rather than in categories predetermined by the researcher. Therefore, a questionnaire survey is used, with open-ended questions, and focus group research. A broader landscape view on the present state of users' perception and attitudes about the trade-off between usability and security was studied and reported according to the findings from the three studies. The three studies findings and the literature review help the researcher to propose a set of usability and security guidelines to

improve e-government services, which in turn would improve e-services usability and security aspects. The proposed set of guidelines complement the general usability guidelines or heuristics by considering user concerns and insights. The author presented some recommendation based on the findings of each study. These guidelines can be useful to guide designers to develop a usable and more secure e-services that match with users' requirements.

Chapter 1 Introduction

This chapter introduces the focus of this thesis and places the motivation of the research, related to the trade-off between usability and security. The research aims and research questions are explained. Finally, the thesis layout is presented.

1.1 Introduction and Motivation

The advancement of the Internet and ubiquitous use of computing in everyday life (iPads, Tablets, smart phones, etc.) has noticeably boosted the growth of the private sectors, such as e-commerce. The growth that is occurring in the private sectors has galvanised governments worldwide to catch on to this revolution and changed the traditional way of delivering services to their citizens. This revolution in the ubiquitous use of computing allows citizens to interact with government digital services (GDS) at any time and in any place (Choi et al., 2013). The fact that these devices have great mobility in delivering services to citizens has become a main point of focus for government organisations. Local and national governments across developed and developing countries aim to leverage the power of ubiquitous computing to provide fast, easy, secure and reliable GDS (Huang & Benyoucef, 2014). Therefore, governments aim to provide services based on users' needs, that are usable and secure, which are critical for the successful adoption and use of GDS (Bertot & Jaeger, 2006; Taylor et al., 2009). Nowadays, citizens use their smart devices to access GDS at any time and in any place for paying tax, applying for new or renew license, and new or replace birth and marriage certificates, school registration, as well as utilizing many other services (Kotamraju & van der Geest, 2012). However, some researchers claim that the real benefits of GDS cannot be obtained unless there is continued monitoring of these services in order to satisfy a wider range of users (Papadomichelaki & Mentzas, 2012; Aichholzer et al., 2009). In fact, there are some reasons hindering the citizens' adoption and acceptance of GDS. Some authors (Kotamraju & van der Geest, 2012; Baker, 2009) have claimed that the design of GDS must meet citizens' expectations, and also provide a clear view of the citizens' requirements to be considered satisfactory before they go on to adopt these services. Citizens will only accept and use GDS when they feel that the interface, they interact with is easy to use, trustworthy and can create a sense of trust and control within the citizens. Regardless, the aim of governments is to have a citizen-centric design for their GDS, but the challenge still presents itself to e-government service designers and providers (Verdegem & Verleye, 2009; Kotamraju & van der Geest, 2012). Verdegem & Verleye (2009) also state that there is a lack of citizen-centric designs in many government online services, which has resulted in the underutilisation of e-government initiatives. However, users still find these services are inherently difficult to use in most cases, and in others, not secure to use.

Although, there has been some work in understanding users' acceptance of services, less work has been done to understanding users' preferences, especially associated to trade-offs between different service aspects such as usability and security (Venkatesh, Chan and Thong, 2012; Venkatesh, Hoehle and Aljafari, 2014). Understanding the trade-offs of service design is significant, in order to have a good usable secure design (Venkatesh and Agarwal, 2006). This service design trade-off may influence citizens or users to perceive some services more secure and less usable due to design complexity.

The current users' belief about how security works and its functions in any system is to make things complex and difficult for them. In fact, human nature always tends to try to avoid complexity, feel the control over systems and feel the sense of this control (Sasse, 2015). This belief makes users ignore or bypass some of the security functions or alerts due to the complex nature of these systems and the absence of control over that system. Therefore, it is obvious that the human being is a critical aspect in system design, but on the other hand it is considered the weakest element (Sasse, Flechais and Famed Hacker Kevin, 2005). Most attackers have recognised that the human is the most exposed element and have succeeded in paying more attention to it than the system developers have and they took advantage of it for their own benefits, to make their attacks easier and more successful (Mitnick, Kevin D and Simon, 2011). Security, from the user's perception is difficult to understand, and it may distract their attention from focusing on their tasks (Whitten and Tygar, 2005). This undesirable trend leads to the implementation of unusable systems that are more secure having negative effects on user interaction, and in some cases, leads users to abandon the system. By applying these functions, usability of interfaces seriously decreases and affects the user interaction.

System developers and designers need to consider user-centric designs during the development phase in order to understand the system users and their abilities to achieve an effective balance between security and usability. This will help end users to interact with system more easily and efficiently, and will assist them in understanding how to use the system functions correctly without bypassing or ignoring any of the security alerts (Sasse & Flechais, 2005).

Usability and security are considered two related elements that have a significant influence on users' communication and engagement with e-government, and therefore, need to be studied and understood together as one concept (Bertot and Jaeger, 2006; Kotamraju and Van Der Geest, 2012). Consequently, it is very significant to understand usability and security in the e-government setting in order to improve e-services and provide positive feedback for designers to develop usable secure GDS that can be used by a wide range of citizens. The main aim of this project research is to understand the users' perception of the trade-off between usability and security, which will assist the government service designers to better understand the users' perception of trade-off between usability and security.

Moreover, this research project is focusing more to understand users' perception of the usability of security and how the security features in the studied systems are usable. The emphasis of the conducted studies is concentrating more on the usability feature and the usability of security features than technical aspect of security. The research scope is users' perceptions of usability, usable security and trade-off. The technical part of security is outside this research scope as it is requiring a series of testing to identify and detect loopholes and risks of failure in the studied system.

E-government online services are a good example of spaces where there is a vital need for usable security. The likely contributions of usable security to e-government services provide positive prospects; however, the usability and security of online services remains a legitimate concern. The need for a usable security in e-government context has been highlighted, as it is seen as a possible solution to improve security and privacy issues (Just, 2004; Plotnick, Hiltz and Burns, 2013; Choi, Ae Chun and Cho, 2014). Taking this into account, the purpose of the research is to understand what users' need from usability and security of e-government services by evaluating usable security from users' perspective to address the usability and user experience issues that users face with regard to the security and privacy features available to them in the e-government context.

In addition, this research project will help e-government service designers to understand users' preferences and attitudes when interacting with e-government services. Therefore, the usability and security need to be understood based on users' perspective, which will help e-government services designers to identify the users' requirements of usability and security and design services based on their needs.

The selection of the research topic is based on the results obtained by conducting a mapping study, as there is a considerable amount of research which has been published on different subjects within the field of usability and security in the context of e-government. A systematic mapping study was conducted as a structured method to identify research clusters and any possible gaps in this area of research (Kitchenham & Charters, 2007).

1.2 Problem Description and Rationale

The implementation of information technology in many aspects of today's life brings with it many types of threat that hinder the user data assets which need to be protected. Therefore, organisations understand the importance of protecting user's assets and have developed security methods that can be used to help users from the negative side of this technology. These methods, from the developers' perspective are very effective, where used in wide range of systems. However, these methods also have influential negative effects on some systems features (e.g., usability) and users (e.g., understanding how to use security functions correctly) (Sasse, Flechais and Famed Hacker Kevin, 2005; Sasse, 2015).

Researchers found that users need to understand and adopt secure behaviours and have usable interaction with the system at the same time (Gutmann and Grigg, 2005; Yeratziotis, Pottas and van Greunen, 2012; Sasse, 2015; Acar, Fahl and Mazurek, 2017). The lack of some users' skills and knowledge make it difficult for them to deal with the increasing unknown threats and protect themselves. In view of that, the system designers and researchers in the field of human computer interaction (HCI) have a great responsibility towards users and should help them to protect themselves and provide them guidance and education where required. Therefore, system developers and designers need to consider user-centred design in the development phase in order to understand the users and their abilities (Braz, Seffah and M'Raihi, 2007; Plotnick, Hiltz and Burns, 2013; Shay et al., 2014). This will help end users to interact with system easier and efficiently and will assist them to understand how to use the system functions correctly without bypassing or ignoring any of these significant functions or alerts (Sasse, Flechais and Famed Hacker Kevin, 2005).

When systems have a usable design of security and usability features, the user's behaviour and interactions will improve and they will have the ability to learn and use system or website efficiently (Ben-Asher et al., 2009). Governments around the world have many active users and businesses using e-government services intensively, and the user-base is rapidly increasing. Therefore, it is essential for e-government service designers to understand the importance of usability and security in order to make users interaction secure and easy when accessing e-services. In order to avoid having unusable and insecure designs, developers and researchers need to collaborate to understand the user's perception about usable secure design, and how users experience this design in an e-government setting (Braz, Seffah and M'Raihi, 2007; Herley, 2014).

Government environment is a good example which includes many users interacting frequently with the government where there is a critical need for usable security. There is a need to address usability and security matters in more detail to enlighten e-government service developers and designers to create a balanced design that will improve the quality of e-government services and increase users' use and engagement (Kotamraju and Van Der Geest, 2012; Choi et al., 2013b).

On the other hand, e-government services are frequently utilised by users with different backgrounds and requirements. This kind of a complex environment with differences in background and diverse users' needs proves a challenge for service developers to identify the right balance for providing usable and secure services. In order to avoid such complexity in service design, users need to be involved in the early design process, which is very important and would be helpful to identify their needs of usability and security features (Bertot & Jaeger, 2006). In addition, users' involvement will also help e-government service developers to identify the features which may influence users about usability and security. Therefore, it is essential to focus more towards users' needs and assess usability and security from users' perception to develop a citizen-centric e-government service design that can help users to acquire the desired results and increase their engagements in e-government (Huang & Benyoucef, 2014; Johnson & Willey, 2011).

Based on the conducted mapping study (Alshamsi, Williams and Andras, 2016), there is a lack in guidelines, principles and theories about how users perceive usability and security in an e-government setting and the available one still in their early stages. Moreover, usability and security from users' perspective in an e-government setting needs to be further explored through focused research as e-government service developers still struggle to understand how to create the balance between usability and security, based on users' requirements (Huang & Benyoucef, 2014).

Therefore, this research project is trying to investigate and understands users' preferences and attitudes towards the use of e-government services in term of usability feature and usability of security feature. Furthermore, our goal is to capture users' perception and understand what users perceive and; how they perceive it in this way; and how they will behave afterwards. Capturing users' perception and preferences will help service designers to understand what users want in term of the trade-off between security and usability.

The aim of this project research is to consider these issues by attempting to study usability and usability of security of current e-governments from users' perspective, and this will be achieved through three studies. These studies will be the groundwork to obtain the related data to assist the researcher and the e-government service developers to understand usability and security features from the users' perspective.

According to the aforementioned, it's clear there is a lack of existing research and knowledge in the literature concerning usability and security in the e-government context. Therefore, the aim of this research project is to address this gap by studying the fields of human-computer interaction (HCI), to understand users' perceptions towards usability and security.

This research study will benefit the service designers to address the e-government service design considerations from users' perspective in order to ensure a unified process of security and usability in e-government service interface design, and to achieve a higher level of usable security.

1.3 Research Aims and Questions

The main aim of this research thesis is to understand the trade-off between usability and security in an e-government domain from the users' perspective. This study aims to obtain insight on the user experience, investigating and explaining user behaviour and attitudes in order to have a comprehensive view about the different influences and their significance to perceived security and usability in e-government context. This research relies on three studies to address the research questions, focusing on users' impressions, preferences, and opinions about the trade-off between usability and security in an e-government setting. The research intends to investigate how users perceive usability and security and trade-off. This research study's main focus is not intended to evaluate or measure usability and security using traditional assessment methods, but to discover what it is users' requirements when using and interacting with e-government services when new service being introduced, new device being integrated, and new platform adopted in term of usability and security. Also, to understand users' behaviours and attitudes in relation to a studied system.

The reviewed literatures, motivation and objectives, lead the study to address the following primary research question:

1. How do users perceive the trade-off between usability and security in e-government context?

   (a) How does a secure and anonymous system such as "Bitcoin" influence user experience of usability and security?

   (b) How does wearable device influence user experience of usability and security?

   (c) How does Blockchain technology influence user experience of usability and security?

To obtain more understanding about the research aim, the following objectives were pursued:

1) Examining wearable devices influence on users' perception of usability and security.
2) Examining anonymous payment system on users' perception of usability and security.

3) Examining the influence of Blockchain technology on the use of e-government services in term of usability and security.
4) Propose recommendations based on the research findings.

1.4 Studies Selection and Relation to E-government

There have recently been government efforts to implement latest revolutionary technologies that offer fast, secure, and efficient services with positive social change. These revolutionary technologies have a great chance to improve the e-government online services provided to citizens. Some of these technologies' present opportunities for all kinds of public services by providing away to cut errors, reduce costs, increase security, avoid fraud and enhance productivity (Boucher, Nascimento and Kritikos, 2017). These promising technologies could revolutionise the way citizens interact and transact with e-government over the Internet. However, such technologies may also have negative influential effects on e-government services if not implemented based on users' requirements. In addition to that, some of these technologies are still in their early stages of development and need more investigation in order to be accepted and utilised. These emerging technologies would be a new addition to e-government system once implemented, and before that they have to be evaluated and examined in term of its usability and security features, which is the focus of this research. Therefore, to evaluate and assess these emerging technologies, we have chosen three trending technologies to study and investigate that can be implemented in e-government and replace the current used technology. The chosen technology to be investigated are feasible and would help to improve public sector services in term of usability and security. These emerging technologies represent the payment system (Bitcoin), medium to connect (Apple watch device) and platform (Blockchain technology). Therefore, we believe these chosen emerging technology would be the best to be studied and investigated in order to provide a comprehensive view of users' needs and would allow us to assess e-government services from different angles with emphasis on usability and security. The researcher and advisory team agreed on the selection of the three studies which are the most related emerging technology that match the characteristics of the current used technology in e-government and can be used by public sector in the near future. Also, studying these three emerging technologies would give us a complete picture of users' viewpoints and requirements of e-government online services (González Martínez et al., 2011; Papadomichelaki & Mentzas, 2012; Aichholzer et al., 2009). This research focus on crucial elements that are significant to both e-government and citizens and contributes to a better understanding of what users need from the integration of a new payment service (Bitcoin study), new device (smartwatch study) and new platform (Blockchain study) in e-government.

Our main aim in conducting these three studies is to explore users' perceptions of usability and security in e-government from three different angles to obtain rich insights into users' requirements.

1.5 Layout of the thesis

The thesis is divided into eight chapters. The following presents a brief summary of the eight chapters that make up the thesis.

Chapter 1 is the introduction and research motivation with an overview of the research. Also, it describes the problem, outlines the research questions, research aims and the methodology.

Chapter 2 reviews existing literature to explain the importance of usability and security to e-government services. This chapter is a general background about e-government followed by relevant studies to indicate the importance of usability and security. After that, usability and security effects on users and e-government services. Usability and security assessment and evaluations tools have been introduced. Also, the relationship between usability and security has been described and explained.

Chapter 3 This chapter starts with the Mapping study conducted by researcher to identify aspects of usability and security in e-government domain that have been researched or where research is lacking.

Chapter 4 Focuses on the research methodology and presents the research philosophies, research approach, techniques and procedures used. Also, the rationale behind the selected methods is explained. This chapter also discusses and describes the mixed-methods approach and the rationale behind selecting the mixed-methods methodology.

Chapter 5 This chapter presents study one (Bitcoin). The study was conducted on Bitcoin crypto-currency payment system. Related literature, methodology, data analysis are discussed and described. This followed by results and discussion of the results with recommendations.

Chapter 6 This chapter presents study two (Smartwatch). This qualitative study was conducted on Apple smartwatch. The study used four focus groups to collect data to examine novice users' perception and used the Reddit discussion website to understand how expert users perceive smartwatch usability and security. The chapter contains the literature review and methodology with data analysis techniques used. Also, results are discussed based on the findings with recommendations for future improvements.

Chapter 7 This chapter presents a critical analysis of Blockchain technology. This study conducted based on literature review analysis. The study followed the systematic review techniques recommended by (Brereton et al., 2007).

Chapter 8 The contribution of the thesis is presented in this chapter, and summary of three studies with findings. Also, this chapter highlights the limitation of the research and the possible avenues for future research.

Chapter 2 Theoretical Background

2.1 E-Government

E-government has been defined in the reviewed literatures as the use of the web internet technology, to deliver government services (e.g., informational, transactional), to citizens (Huang & Benyoucef, 2014). Thus, most of the governments around the world are adopting and implementing the latest information computer technology (ICT) to provide a wide range of services to their citizens (Kotamraju & van der Geest, 2012; Olalere & Lazar, 2011). Recently, many governments have changed from using a traditional service delivery platform to one where the electronic service allows users to take on new roles in the delivery of services. Therefore, the transactional journey of the government-citizen relationship needs to be focused on easy-to-use interface design, which is critical to the successful adoption and use of applications (de Jong & Lentz, 2006; Taylor et al., 2009). These services aim at enhancing the accessibility of the services, with a reduction in the cost of delivery and delay. However, as researchers (Papadomichelaki & Mentzas, 2012; Aichholzer et al., 2009) contend, these benefits cannot be obtained unless there is continued monitoring of the e-government services to identify the real benefit to the end user.

Challenges to research that exist within the implementation of effective e-government have been discussed in the literature. Ruba et al. (2014), contend that there is lack of citizen-centric designs in many government services, which has resulted in the under-utilisation of e-government initiatives. Additionally, since there is a great deal of sensitivity and need for confidentiality with respect to the sharing of such information within the e-government framework, it becomes imperative to ensure security and protection. As Choi et al. (2014)

argue, security and trusted information should be key issues that are adopted in order to prevent unauthorised disclosure and leakage of secret information.

Also, Lesemann et al. (2007) and Markova et al. (2007), have addressed that usability issues need to be examined while designing new functions and services in any platform, as this can ensure an enjoyable user experience. Alberto (2010), presents an excellent conclusion to the need for usability and security. The author claims that IT-enabled service interactions must meet the users' expectations from his needs from the service. Therefore, e-government services must be designed based on the users' backgrounds, knowledge, skills and context of use in order to have a satisfactory services (Raptis et al., 2013).

Additionally, there are many studies that have addressed the problem of the eService design and the need to have a citizen-centred eService design in order to meet the expectations of users (van Dijk et al., 2008; Bertot & Jaeger, 2006). The aim of this study is to have a more thorough understanding of citizens' needs and expectations towards e-Government in terms of users' preferences about usability and security among their preferences.

The domain of usability and security has grown rapidly in recent years, with the rapid use of smart devices such as iPads, smart phones, and so forth. These smart devices bring with them several security and usability problems that have an undesirable effect on the users and the domain they are accessing (Sauro & Kindlund, 2005; Sasamoto et al., 2008). Nowadays, users frequently utilise smart phones to access e-government services (e-services) to pay taxes, penalties and other related services. However, governments tend to have more securely designed services which makes it more difficult to manipulate or jeopardise through unauthorised access, but this also helps face the threats that prevail in the environment of today's internet (Muslukhov et al., 2013). The focus on the security of these e-services and their functionality creates an imbalance between maintaining security and usability. This unintentional behaviour leads to the implementation of unusable e-services that are ineffective and not easy to use (Kotamraju & van der Geest, 2012). The decline in the usability of these e-services has a major effect on security, because citizens and users of the government services may ignore or bypass some of the security functions or alerts due to the complexity of these services

Therefore, this review of literature argues that e-government promotion at different levels of the government has been well researched in developed and developing countries. Though the multiple benefits of an e-government are evident, the associated challenges require more research. The literature review highlights some of these challenges that hinder the adoption of a government service that needs to be examined and studied from users' perspectives.

2.2 E-government Portal

The e-government portals have served as a gateway which provide a main entry into government websites to ensure that citizens and government stakeholders have a central gateway to experience the speed of accessing the government services (González Martínez et al., 2011). Researchers such as Gouscos et al. (2007) and Choi et al. (2014) support this assertion by arguing that government portals are a single access point for government-linked information and services. In addition, Papadomichelaki & Mentzas (2012) stated that the assessment of e-government services (e.g., quality) is applicable to government portals as these portals provide the 'window' for e-government access. The authors further argue that a vital element in the evolution of government services is to understand how citizens perceive government portals and ensure that there is delivery of superior service quality.

As argued in the introduction, the objective of this research project is to study the user perception of usability and security in e-government services when adopted through smart devices. Therefore, as Choi et al. (2014) contend, a key step towards establishing smart government within the public sector is to enhance the sharing of government data and improving services provided to their citizens and their stakeholders. The authors further argue that smart governments should also look to adopt citizen perspectives and reflect citizen feedback in their policies and public service provisions. This requires the use of mobile devices where citizens can have better access to e-government services in order to develop agile and fully context-aware government services. The authors contend that the establishment of an e-government portal should, therefore, be suitable for smart devices like mobile technologies to improve C2G (Citizen-to-government) sharing. Therefore, the authors suggest that mobile e-government portals are the future of smart technology and a one-stop government services in many countries.

Hung et al. (2013), contradict this perspective by arguing that though there has been significant research into multiple features of e-government services provided by many countries, most of them have revolved around e-government websites rather than mobile platforms. Also, Duh et al. (2006) supports the previous argument where they argued that the complex problems which is faced by service providers is the difficulty in communicating with their intended stakeholders. Since, mGovernment (i.e. e-government through smart devices) is a possible solution to address this issue, there should be more research conducted on the challenges linked to its provision. As Hung et al. (2013) and Choi et al. (2014) conclude, an assessment of government service acceptance requires an understanding of mobile communication requirements from citizens along with a focus on human-computer interaction.

The e-government portals have served as a gateway which provides a main entry into government websites to ensure that citizens and government stakeholders have a central gateway to experience the speed of accessing the government services (González Martínez et al., 2011).

2.3 Usability

2.3.1 Usability concept

Usability has been broadly addressed in system design and it has a significant role in human computer interaction (HCI) field (Huang & Benyoucef, 2014). Usability was defined by the International Standard Organisation (ISO), as the “effectiveness, efficiency, and satisfaction, with which the intended users achieve specific goals in the defined context of use” (ISO, 1998). However, usability known in the field of software engineering as the quality of a system, in terms of users-friendliness, ease of learning, and satisfaction (Frandsen-Thorlacius et al., 2009; Kokini et al., 2012). In the field of web-based systems, usability is perceived in the ease of use, the simplicity of system functions, the speed of navigating, and the users' perception of having control on the system (Hornbæk & Frokjær, 2005).

There are many guidelines that have been used for evaluating website usability. Nielsen (2005) used 10 criteria to assess usability and developed a set of standard usability guidelines to explain the usability concept. These guidelines were developed and used a long time ago and were employed to evaluate website usability in general.

Many researchers have stated that usability should commonly address the broad notions linked to quality of use of interactive systems (Hornb et al., 2007; Hertzum, 2010). This is of particular importance to government organisations which are emerging as key domains, where usability becomes vital to e-government. Interestingly, as González Martínez et al. (2011) report, governments are looking to provide a single access point to government information and transactional services. Furthermore, as Huang & Benyoucef (2014), indicate, accomplishment of this objective requires web developers to continuously examine and assess user needs, and ensure that usability features form part of the developmental process. Also, researchers such as Baker (2009), Welle Donker-Kuijer et al. (2010), and González Martínez et al. (2011), stated that usability should also involve the use of tools and methods to help developers understand and incrementally improve web-portals based on user requirements, in order to have citizen-centric- services.

An examination of usability metrics and evaluation studies shows interesting perspectives on the definition of usability. For example, Lewis (2014), argues that the definition of usability revolves around the measurement of effectiveness, efficiency, and satisfaction, or the absence of any usability problems. On the other hand, Hertzum (2010), reports that a single definition of usability is not the most effective methodology to identify usability-linked needs. The authors argue that six images of usability need to be developed to address the true definition of usability, including "universal usability, situational usability, perceived usability, hedonic usability, organisational usability, and cultural usability" (Hertzum, 2010). The author concludes that having different concentrations on usability images can help understand the multiple aspects related to usability within the designed system.

Interestingly, as Frandsen-Thorlacius et al. (2009) and Følstad et al. (2012), report that various concepts, methodologies and components of usability have been tested. Additionally, some researchers identify the needs of well-accepted methods of usability engineering in order to understand users' needs. Similarly, Chilana et al. (2010), indicates that even when there are well-established methodologies prevalent, the system interfaces will continue to possess usability issues. Therefore, understanding existing usability issues and making an assessment of usability components are important issues in human computer interaction research.

Another important attribute which needs to be identified is the development in defining usability in light of increasing use of smart-devices like mobile phones, in accessing e-government services. Most authors agree with the view of Lewis (2014) with respect to the usability definition. However, some additional metrics have been identified. For instance, Lesemann et al. (2007) reports that increasing use of mobile devices with complex functionalities has resulted in limited use of functions and features. Therefore, the author concludes that usability requirements are significant in the area of mobile HCI to ensure an enjoyable user experience with a focus on portability as a key usability parameter. Raptis et al. (2013), on the other hand, report that usability metrics in mobile phones require assessment of attractiveness, effectiveness, and efficiency. The author states that simultaneous testing of these aspects is important. The literature review shows that very few researches have focused on addressing the usability of smart devices and very few of them have considered the smart phone usability effects on users (Raptis et al., 2013; Bhattacharya et al., 2014).

2.3.2 The usability effects on e-government

The requirements of usability of e-government web-based services, Baker (2009) emphasised on the importance of concentrating on e-government services usability, where e-government is still need to put more efforts to improve the design of service provided in order to increase the users engagement and interactions. The author identified six quality elements that are affecting the e-government website usability, which are "online services, user-help, navigation, legitimacy, information architecture, and accessibility"(Baker, 2009).

Moreover, the significance of usability in an e-government website design is also indicated in the study done by Welle Donker-Kuijer et al. (2010). He highlighted the significance of usability in e-government websites and considering it as a quality indicator. He also emphasised to regularly assess and inspect the usability of e-government websites in order to improve the quality of the services provided to citizens.

The assessment of usability effects on e-government provides some interesting perspectives. It is interesting to see that most of the authors highlight similarities and interlinks between different usability metrics. For example, Gouscos et al. (2007), and Baker (2009), show in their researches that learnability and memorability are key factors which govern user requirements and user interaction with e-government services. Furthermore, Ruba et al. (2014), in their assessment of a government linked healthcare of Obama website contended that convenience and familiarity were important parameters in web-based services. Familiarity can help improve the understanding of the content. Similarly, Hung et al. (2013) argued that it was essential to examine if the proposed platforms enhance learnability through the assessment of recognition rather than recall and visibility of system status.

Also, researchers such as Huang & Benyoucef (2014) and Hung et al. (2013), in their assessment of e-government platform, highlight the importance of usability in e-government. They declare that the satisfaction of the user is related to the assessment of support users' skills and respectful interaction. Also, Verdegem & Verleye (2009), used formative evaluations to examine the importance of satisfaction as a metric in e-government. They conclude in their assessment that both satisfaction and error rate are related, where that reduced user error rate improves satisfaction, and increase in reuse.

From the above evidences, it is clear that multiple aspects linked to usability metrics have been highlighted in literature. The reviewed literatures highlighted the importance of usability in e-government, and usability need to be examined and assessed regularly.

2.3.3 The effects of usability on users

Usability and its effects on users are measured with respect to different metrics. One of these metrics used widely is, Nielsen (2005) metrics, which include Efficiency, Satisfaction, Learnability, Memorability, Errors, and others (Kyung et al., 2006). Nielsen (2005) metric is used in this part to explain how usability affects users in terms of these metrics. Extant literature reviewed as part of this literature review has agreed with the perspective that there are multiple metrics, scales, and methods, which have been adopted in the past to identify the effect of usability from the perspective of user needs (Sauro & Kindlund, 2005; Sasamoto et al., 2008). It should be noted that most of the studies contend that there is more need to assess the aspects linked to usability features and associated effects on the users (e.g. Følstad et al., 2012; Frandsen-Thorlacius et al., 2009).

Usability issues have been highlighted in the different research articles. It is evident that accessibility is the most commonly highlighted attribute with respect to usability issues. For example, Chilana et al. (2011), in their assessment of post-deployment problems in complex domains, identify the need to improve overall accessibility within the platform to meet the challenges linked to user needs. Similarly, Lindgaard (2007) identify from an assessment of factors linked to usability metrics that accessibility should be the primary focus of any user requirement. Interestingly, Petrie & Power (2012), in their assessment of expert and user needs, argue that both groups look for reduction in error, learnability and improved accessibility as key parameters.

Learnability is another usability dimension in the e-government setting which has been highlighted by many researchers. According to researchers (e.g., Zezschwitz et al. 2013; Hung et al. 2013), learnability in the context of mobile devices requires enhancement in terms of interactivity to improve user understanding and reuse of the device and its platform. The importance of learnability in the context of usable security has been highlighted in research. For example, Whalen (2011) argued that placement of consistent information and control is a key to the enhancement of learning. On the other hand, Ahmad et al. (2015) stated that while it is important to ensure that learnability links to user learning and context, the presence of guidelines is the absolute key to improvement in usability issues. For example, the authors argue that difficulty in understanding some terms and instructions is prevalent if there is lack of clarity in guidance.

Memorability as a key usability indicator has been highlighted in many papers. In Chowdhury et al. (2014) study, he contends that assessment of memorability and secure authentication systems requires improvement in user memorability. Andreasen et al. (2007) and Egelman et al. (2008) further argue that comprehension of the uses derived from a given platform is important. Zezschwitz et al. (2013) contend from a mobile HCI perspective that memorability helps assess the importance of user efficiency and performance.

Satisfaction is another important metric which has been highlighted in literature. Researchers identify satisfaction as the precursor to future use (Sauro and Kindlund, 2005). This is of particular importance to this research for understanding how satisfaction element influences the users' perception about the use of e-government services through using smart devices to access these services. Zezschwitz et al. (2013), in their assessment of usability metrics of mobile devices, contend that satisfaction ensures re-use of the system and helps develop better indicators of performance. Hornbæk & Frøkjær (2008) and Hornb et al. (2007) also indicate that if examined from a practical evaluation perspective, there is a significant impact of user satisfaction on performance. Akers et al. (2009) and Egelman et al. (2008) contend that the effectiveness assessment of existing systems can be promoted only through the assessment of user satisfaction.

2.4 Security

2.5 Security concept

Security, in general, is all about the protection of information systems (IS) from disruption or misuse of the service they provide. The concept and notion of security is defined using clearly established metrics rather than a blanket definition. For example, some studies examine confidentiality and integrity as key determinants of security, where the computer system or the network discloses information only to authorised parties (Ben-Asher et al., 2009; Inglesant & Sasse, 2010; Shay et al., 2014). On the other hand, other studies define security from the perspective of integrity, wherein improper alterations to the secure computer cannot be carried out and the alteration to the asset is only made through authorised assets (e.g. Yeratziotis et al., 2012). These are the two different overarching themes of security, discussed in most of the studies identified as part of this literature review.

Security as a factor in mobile platforms has also been well discussed in literature. For example Muslukhov et al. (2013), reported that the increasing use of mobile and smartphone devices had led to the need for improvements in security linked research. The authors have argued that malware in smartphones have attracted significant attention and conclude that assessing and reducing the impact of malware linked attacks is a key concern of security threats. Sieger & Möller (2012), reflect on security perceptions and the needs of users in terms of gender perspective. The authors conclude that features and applications that can be monetised, including “online shopping”, “online banking” require effective safety promotion protocols. These protocols should support privacy and confidentiality. Also, Ben-Asher et al. (2009), in his study, contended on the importance of security for understanding usability and trade-offs between them.

The importance of security has been highlighted in the e-government context. For example, Aichholzer et al. (2009), contend that provision of security is most important to ensure seamless sharing and interoperability of citizen-service related information. Alberto (2010), support this argument with the view that provision of security and management of security needs can be carried out when there is enhancement of data security and integrity. Kotamraju & van der Geest (2012), in their assessment of e-government websites (municipal platforms), contend that security is predominantly linked to the ability to provide privacy and enhance the overall security policy and ensure confidentiality.

2.5.1 Security effects and outcomes

The concept of protection is linked to confidentiality and integrity. For example, Chowdhury et al. (2014), contend that people often find it difficult to remember alphanumeric passwords which are complex and difficult to implement. The authors argue that while these passwords are important to improve authentication and ensure protection of confidentiality of the user, alternatives in the form of password hint authentication systems are important. Muslukhov et al. (2013), in their assessment of security in smart phones, identify a similar perspective where authentication and validation were highlighted. The author argues that protection can be enhanced when authentication and validation through centralised exchange of context information as well as confidentiality through the use of anonymisation methods are promoted.

Similar parameters are also studied by Bhattacharya et al. (2014), as he highlighted security issues in mobile phones. The authors conducted a detailed seven module analysis, where mobile device security and privacy was done to identify phishing threats (integrity), and secure development (authentication). They support the views of Muslukhov et al. (2013), who identify that integrated security platforms need to enhance different dimensions of security.

The importance of authentication is another key aspect which is acknowledged in literature. The study evidences of Shay et al. (2014), indicate that inflexible password composition was a key factor which impacted password management. They argue that authentication needs to be secure and usable in order to fulfil the users' needs.

Shay et al. (2014) also view that inflexible password compositions are considered a key deterrent to authentication. The authors conclude that security should be examined with usability measures in order to have usable and secure authentication. Sasamoto et al. (2008), report that the primary element of security examined, is the authentication tests. The authors indicate that security development should focus predominantly on an undercover authentication system. Petrie & Power (2012), further argue that authentication systems as part of websites, contribute to usability needs. The authors argue that there are problems with choosing and validating passwords. As reported by Sasamoto et al. (2008), information leaks, including pointing at the map, hand movement, and speech, can be linked to lack of privacy. Petrie & Power (2012), feel that information leaks can be threats to privacy. They believe that users look for confirmation regarding privacy of their data, especially with respect to treatment of personal data and information. Alberto (2010), supports this argument by indicating that there is a direct link between security and usability. The author indicates that the enhancement of usability is evident when simple efforts are taken to ensure privacy. The author also argues that authentication should be simple, to improve usability and repeat usage. The author contends that user-centric services should therefore arrive at a balance between the two elements.

2.5.2 Security effects on e-government

Choi et al. (2013), present a detailed analysis of security framework in e-government services. The purpose of their research was to assess a government information sharing system. The "SecureGov" components were tested for authentication, confidentiality, and integrity. Interestingly, another research by the same authors (Choi, Ae Chun and Cho, 2014), with respect to the Smart "SecureGov" framework, also shows that similar parameters are highlighted with respect to mobile government security. Baker (2009), highlighted that legitimacy dimensions including security policy, authentication, privacy policy, and webmaster contact, govern usability and implementation of e-government websites. The study, therefore highlight the view that security dimensions of authentication, confidentiality, and integrity are crucial to users in order to use e-government services. The study also argues that to improve citizen-centric design is important in applying security policies. Furthermore, the study also argues that understanding the security features will lead to the adoption of usable services and increase the users' engagement.

2.6 Assessment Methods

2.6.1 Usability

As illustrated in the previous sections, usability and security are two important elements in e-government service design need to be addressed frequently. It is necessary to evaluate usability and security of web-based e-government services to identify any usability and security issues that need to be enhanced and improved. However, e-government users are coming from different backgrounds, and varied in their knowledge, skills and experience, which require the government service designer to consider the background differences and the needs of usability and security. Such heterogeneous backgrounds make things difficult for service designers to conduct usable and secure design in such systems (Schedler & Summermatter, 2007). The selection of the evaluation methods is generally based on defining if it will be conducted with users or experts.

Researchers such as Grossman et al. (2009) and Andreasen et al. (2007) indicated that assessment of usability can fall under two categories, including summative and formative methods, and can share multiple properties. Hornbæk & Frokjær (2005) contend that the development of these methods of assessment and evaluation strongly depends on the participants, the type of tasks and environment, and the debriefing protocols involved during the testing process. Researchers (Sauro & Kindlund, 2005; Inglesant & Sasse, 2010), state that summative evaluations are commonly used to assess usability problems. Duh et al. (2006), agrees with this view and provides the argument that the aim of summative evaluation is to simply evaluate the system with making any changes to the performance or the task or no change in the product design. Interestingly, most of the studies have identified a summative evaluation where specific usability design has been tested, based on pre-existing parameters and guidelines (Wang et al., 2009). On the other hand, Sauro & Kindlund (2005), contend that formative studies provide variation in techniques wherein different methods are adopted where perspectives on existing usability parameters and pre-tests are conducted to identify usability frameworks and assessment tests.

Many studies have adopted summative evaluation approach to test usability (e.g., Sauro & Kindlund, 2005; Grossman et al., 2009; Følstad et al., 2012). An assessment of summative evaluation tests shows different methodologies, for instance, general summative tests have been used by many authors (e.g., Sauro & Kindlund, 2005). Other forms of summative evaluation include mixed factorial and between study designs (e.g., Grossman et al., 2009; Tohidi et al., 2006), survey methods (e.g., Shay et al., 2014; Chowdhury et al., 2014), focus Group Expert Walkthrough (GEW), and Group Domain Expert Walkthrough (DEW) (Petrie et al.. 2006), and think aloud user testing (Hornbæk & Frokjær, 2005; Hornbæk & Frøkjær, 2008). Inspection methods have been used, including Security Usability Symmetry (SUS) inspection method, and Quality in Use Integrated Measurement (QUIM) (Braz et al., 2007), collaborative critique and critical incidence assessment (e.g. Babaian et al., 2012; Akers et al., 2009), and remote evaluation (Inglesant & Sasse, 2010; Andreasen et al., 2007). Additionally, some of the assessments of the existing frameworks and systems have been carried out in the e-government context (e.g., Choi et al., 2013; González Martínez et al., 2011).

Formative evaluation, on the other hand, has been relatively less examined in literature. Zhang and Taylor et al. (2009), adopted an exploratory research to identify problems in usability of mobile applications, where both laboratory and field based formative testing were carried out. Yeratziotis et al. (2012), report that a tailored approach helps in evaluating online networks, where social networking (SN) based formative assessment was carried out.

This research contends that across different forms of platforms, including new software or web browsers (e.g., Egelman et al., (2008), e-government (e.g., Welle Donker-Kuijer et al., (2010), and mobile HCI testing (e.g., Duh et al. 2006), both formative and summative evaluations have been used with many overlapping methods. Also, the use and selection of the methods are based on different factors such as time, cost, context, and objective of the study.

Reviewing the literature also highlighted that most of the studies focused entirely on usability features. Most of the studies do not consider the factors that may have effects on security. Therefore, it is important to evaluate both usability and security to have a better understanding of how users perceive usability and security features.

In regard to security, there is a lack of studies discussing the security assessments, specifically in an e-government setting. It is crucial that security factors need to be measurable. For example, Kainda et al. (2010) indicated that security elements such as attention, conditioning, motivation, vigilance, memorability, knowledge or skill, and social context are important and must be addressed when assessing security in any system. Also, some authors have assessed security, based on threat models and (negative) scenarios. The reviewed studies of security fall into six categories, namely, Authentication, Encryption, PKI, Device pairing, security tools, and secure systems (Kainda et al., 2010).

Also, Kainda et al. (2010) state, that in order to understand the social context effects of security features of a system, it requires a qualitative approach to understand users' behaviours and how they interact in relation to a studied system.

2.7 Usability and Security

According to researchers (e.g., Dhamija, R.; Dusseault 2008) security issues are increasing in most interactive systems due to changes in user interface design strategies. The authors contend that identity management (authentication) systems have a wide range and complexity, combined with the privacy and security requirements. These result in multiple challenges and decreases usability in the intended system. The security and usability parameters can, at times, be fundamentally at odds with each other. Every system that is more secure requires more control (Gutmann & Grigg, 2005). However, as the authors argue, when there is more control, there is a likelihood of less security. The different examples discussed with respect to security management and password authentication highlight this perspective.

According to Braz et al. (2007), who examine the concept of secure usability, trade-off between usability and security can be achieved when the authentication mechanisms do not hinder the use of the platform. For example, the authors support this argument with the evidence that less hindrance can be enhanced when there are more warning messages, wizards, and interacting tools. Gutmann & Grigg (2005), on the other hand, argue that effectiveness of layered security can be addressed only when associated usability issues are addressed and developed. Interestingly, while high complex authentication measures are assured, the use of five-step sequences can act as a hindrance to usability. Therefore, usability-security trade off often revolves around convenience, memorability, and learnability, versus authentication.

Shay et al., (2014), further argue that when security is adopted from the early stages of development, there can be advancements in usability. The article contends that for conducting psychology and human–computer interaction research to inform, secure system design is needed. Through this article, the assessment of existing usability issues in security promotion and identifying methods which have attempted to address this challenge is evident.

According to researchers (e.g., Shay et al. 2014 and Braz et al., 2007), security and usability often do not work together. In most cases, security comes first, followed by usability or vice versa. The authors contend about layered approaches where usability and security are addressed during the developmental stages. Shay et al. (2014), also argue that adherence to human activity centred design is important to improve system security. The authors draw examples where reduction of burden is required on users, who consider additional integrity or confidentiality measures as unwanted distractions. The authors highlight the presence of a usability-security paradox in the area of access control, password security, and the use of antivirus software.

Renaud (2012), presents an excellent perspective on this. The author argues that human elements are key to noncompliance. The author also indicates that the assessment of human elements should address confidentiality, privacy, and authentication, only after ensuring that the user is aware of the system. Similarly, Yeratziotis et al. (2012), support such a perspective and argue, that most applications have security features that end-users have to interact with. However, the manner in which the security aspects are presented, in terms of design and usability, makes it a complicated process, which users prefer to avoid, and in most cases, even ignore. Therefore, understanding noncompliance requires addressing the usability elements.

2.8 Research Gap

According to the Mapping Study conducted between July and November 2105, the reviewed literatures indicate the importance of usability element (Welle Donker-Kuijer, de Jong and Lentz, 2010), (González Martínez et al., 2011), and security features (Choi et al., 2013b), (Choi, Ae Chun and Cho, 2014), to e-government. On the other hand, the literature also indicates that there is a lack in the studies addressing the usability in the e-government service design (Venkatesh, Hoehle and Aljafari, 2014), (Verdegem and Verleye, 2009). In regard to security also, the reviewed study showed that there are a few papers focused on security evaluation in an e-government setting (Kainda, Flechais and Roscoe, 2010), (Choi et al., 2013a). Ben-Asher et al. (Ben-Asher et al., 2009) and Egelman et al. (Egelman et al., no date), also indicated that users' interaction and their ability to understand the required security functions, need to be acknowledged in the system design. The literature review also highlights that the current e-government services are designed without considering users' needs in term of usability and security (Verdegem and Verleye, 2009). Additionally, researchers in human computer interaction conclude that users assume that systems are inherently more difficult to use and in others are more usable. This conflicting design of getting usability and security to work together in harmony needs to be understood from the users' perspective to avoid them from being the weakest link in security chain (Sasse, Flechais and Famed Hacker Kevin, 2005).

Mike Bracken, a government expert (Turnbull 2014), in his discussion at the Code for America Summit in San Francisco in 2014, highlighted the importance of e-government services design and the need to have the right balance between usability and security in the e-government context. He argued that when the system or the service is more secure, the intended users will abandon the services or the system that is being protected. The speaker focused on the need to know "how much security is too much and how do you find the right balance" (Turnbull, 2014).

2.9 Conclusion

According to the examination of the literatures, there is a need to understand the security and usability requirements for an e-government service from a user perspective and to identify the factors that influence people's perception of usability and security. Moreover, the literature concludes the need to understand usability and security features that may hinder the users' interactions in an e-government setting. Furthermore, the literature highlights the designer's lack of understanding to the users' needs and requirements of usability and security in an e-government setting. Also, based on the literature and the mapping study protocol, there is no specific literature that clearly shows how users perceive usability and security and the trade-off between them in e-government setting.

This thesis conducted based on three studies related to understand the trade-off between usability and security in e-government context. The related literatures of each study were presented in each dedicated chapter of related study.

Chapter 3 Literature Review

3.1 Introduction

Most governments implement the latest information communication technology (ICT) to improve online experience for their citizens and businesses. Governments put great effort into providing user-focused services that are usable, secure, and accessible by portable and wireless devices (e.g. tablets, smart phones, etc.). However, such devices bring with them their specific problems with usability and security that affect how users interact with government digital services (GDS). This chapter presents a systematic mapping study to investigate the existing problems of usability and security for GDS when accessed through smart devices, to find out what evaluation methods have been used by researchers and to investigate how the trade-off between usability and security is assessed in the context of GDS when being accessed through smart devices and to summarise the current knowledge that is available with regards to this trade-off between usability and security over the last 10 years. The result of the mapping study helped us to identify several research gaps, leading us to outline areas for new research in the domain of usability and security in the context of GDS. The study reported in this chapter has been published in the International BCS Human Computer Interaction Conference 2016.

This mapping study is aiming to identify aspects of usability and security in government digital services that have been researched or where research is lacking. The process of the mapping study review is presented and described in detail. The findings of the review and the answer to the research questions are discussed in this study. The references from this study have been appeared in numerical referencing style, in order to accommodate the nature of the presentation of the results and categories. The references list of this study is listed at the end of the thesis references section.

3.2 Research Method

A considerable amount of research has been published on different subjects within the field of usability and security for GDS. A systematic mapping study is recommended as a structured method to identify research clusters and any possible gaps in this area of research [7]. The mapping study supports the collection and categorisation of all the available studies and literature in this area, with the aim of making it simple to identify the various subtopics, as well as showing where current research is being focused. This method was selected because it provides a credible and rational evaluation of studies on the usability and security of GDS and helps to identify any gaps in current research. To achieve these goals a review protocol was developed to reduce the possibility of researcher bias and to identify areas where more primary studies needed to be carried out. The developed protocol was assessed and reviewed by two external experts in the field to ensure validity of the protocol and that it met the requirements stated by Kitchenham [7]. The first step of the review protocol was creating research questions, identifying the search strategy and the search scope. A search process based on the research questions was then conducted. Then, inclusion and exclusion criteria for studies were developed; these were designed in the search phase to assess the thoroughness of the literature search. A strategy was designed for assessing the quality of the papers, collected in the search process. Next, the elements of data to be extracted from the selected literature were determined, in order to help address the review questions and synthesis of the data. Finally, the strategy to evaluate and analyse the data extracted from the literature was devised. In the following subsections the detail of the procedure is explained and the strategy that was followed in conducting the systematic review is described.

3.2.1 Research Questions

Four research questions were formulated to guide the mapping study. Thus, based on the research objectives stated previously, the review protocol is driven by the following questions:

- RQ1. What are the existing usability and security problems concerning government digital services when accessed by smart devices?
- RQ2. What methods of evaluation have been used to assess the usability and security of government digital services when accessed by smart devices?
- RQ3. How is the trade-off between usability and security measured and assessed in the context of government digital services?
- RQ4. What training and policies are available to the public to ensure effective usability and security of government digital services when accessed by smart devices?

The findings of the proposed review questions are critically important for evidence-based engineering of eGovernment services and will contribute to the knowledge of usability and security within the domain of eGovernment.

3.2.2 Search Strategy

The review includes a search strategy that was developed to utilise publication databases in an efficient way. This search strategy is considered essential when performing the search process to avoid including many irrelevant search results. The search strategy was designed based on selecting major terms from each of the research questions and using alternate words and synonyms in each search string. This helped to reduce the effect of variance in the terminologies. Boolean "OR" was used to link alternate words, and synonyms as well as Boolean "AND" to join major terms if the databases allowed that. The search string consisted of four parts: "usability" AND "security" AND "services" AND "smart phone" attributes. The alternate terms were connected through Boolean OR to produce a reference search string for automatic search of databases. Following the search strategy, and using the outcome from the pilot search activity, the final search strings were derived and used to retrieve the relevant papers. The created search strings were adjusted based on the search criteria of each electronic database used. Different search strings were formed for different database sources, for each database an equivalent search string was produced to suit the database's search requirements. The process shown in Figure 3.1 for the retrieval of papers shows the nominated databases and the respective number of papers that were retrieved in each phase of the search process.

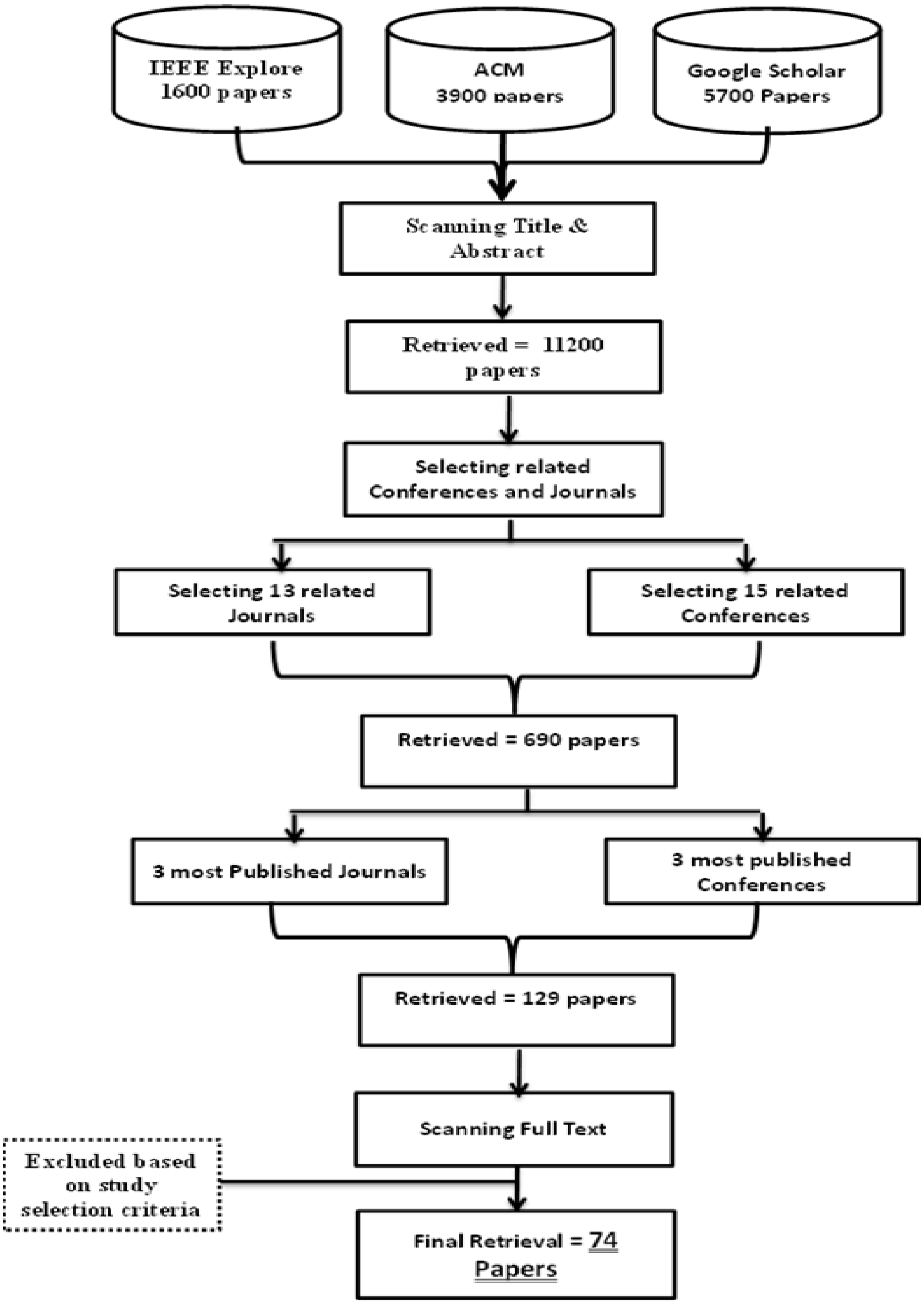

Figure 3.1: The Search process

3.2.3 Search Process

The scope of the search was focused on the publication period and source. The search for publications was limited to the period from January 2005 to July 2015. In terms of search engines, three electronic data sources were selected (ACM Digital Library, IEEEXplore Digital Library and Google Scholar). For each data source, the return results per search were documented and retrieved papers were manually imported into Mendeley software. In this stage, some irrelevant papers were excluded based on scanning their titles and abstracts before saving them into the reference manager software. The first total number of retrieved papers was 11,200 papers from all sources. The number of papers retrieved was considered very high for this review, so the most relevant conferences and journals were selected which had the most published papers in them and were linked to the field of usability and security in the context of GDS. The two other authors reviewed the validity of the selection of the conferences and journals. There were 15 conferences and 13 journals selected that were considered most relevant for the review study. The selection was based on the Institute for Scientific Information's (ISI) impact factor ratings, the number of articles published and whether the authors were cited in other reputable journals and conferences (See Table 3.1). After the consideration of these selected journals and conferences, the number of papers retrieved was narrowed to 690 papers. Then, the conferences and journals that had fewer papers were excluded from the review. This resulted in three conferences and three journals that had the highest volume of papers being included in the final selection. The total number of papers in the 3 journals and the 3 conferences was 129 (See Table 3.2).

The 129 full text papers were read in accordance with the inclusion and exclusion criteria. The inclusion and exclusion decisions are shown in the next section. After the process of inclusion and exclusion decision-making was completed and the final set of primary studies was reviewed. The total number of primary papers selected was 74. These papers were considered the most relevant for this review.

Table 3.1: Initial Conferences and Journals Selection

No	***Conferences***
1	*Computer Human Interaction CHI (ACM)*
2	*International conference on Digital Government Research (ACM)*
3	*European conference on Information systems ECIS*
4	*Australian Conference on Information systems*
5	*International Conference on Availability Reliability and security ARES (IEEE)*
6	*Symposium on Usable Privacy and security SOUPS (ACM)*
7	*American Conference on Information systems*
8	*International Conference on eDemocracy & eGovernment (IEEE)*
9	*Symposium on Security and Privacy (IEEE)*
10	*International Conference on Information Assurance and Security (IAS)*
11	*Symposium on Computer and Communications Security (CCS) (ACM)*
12	*International Conference on Security of Information and Networks*
13	*ACM Conference on Data and Application Security and Privacy (CODASPY)*
14	*ACM International Joint Conference on Pervasive and Ubiquitous Computing*
15	*Mobile HCI conference (MobileHCI)*
No	***Journals***
1	*European Journal of Information systems*
2	*International Journal of Electronic Governance*
3	*Journal of information and software technology*
4	*Journal of systems and software*
5	*International Journal of Human-Computer Interaction*
6	*Personal and Ubiquitous Computing international Journal*
7	*Security & Privacy Journal*
8	*Journal of Transactions on Information Forensics and Security*
9	*Transactions on Consumer Electronics*
10	*International Journal of Engineering and Technology*
11	*International Journal of Mobile Human Computer Interaction (IJMHCI)*
12	*Journal of Usability Study (ACM)*
13	*Journal of government information quarterly*

Table 3.2: Final selection of conferences and journals

Selected Conferences	No of Papers
Computer Human Interaction CHI (ACM)	*27*
International conference on Digital Government Research (ACM)	*5*
Mobile HCI conference (MobileHCI) (ACM)	*10*
Selected Journals	
International Journal of Human-Computer Interaction	*9*
Security & Privacy Journal (IEEE)	*13*
Journal of government information quarterly	*10*

3.2.4 Inclusion and Exclusion Criteria

It is imperative that any mapping study contains comprehensive inclusion and exclusion criteria to highlight only those primary studies that provide evidence related to the research questions. The inclusion and exclusion criteria of this review study were developed based on the research questions and they were conducted to ensure that the obtained results were reliable, and they could categorise studies correctly according to the guidelines set by Kitchenham [7]. The following inclusion criteria were applied to all the 129 papers obtained from the search process. The reviewed papers had to meet one of the following inclusion criteria to be included in the review:

- I1: Papers discuss and describe any usability and security problems in the context of GDS.
- I2: Papers report any usability and security problems of smart devices (smart phones).
- I3: Papers report usability and security evaluation methods and guidelines in the context of GDS.
- I4: Papers describe the methods used to evaluate usability and security of smart devices.
- I5: Papers discuss the trade-off between usability and security and how it is measured.
- I6: Papers discuss training guidelines, policies and security awareness in the context of GDS.

On the other hand, papers that met any one of the exclusion criteria shown below were discounted from the review:

- E1: Papers that do not have a specific problem to investigate, search process, or data analysis process.
- E2: Papers focusing on the technical side (cryptography, coding, etc.).
- E3: Non peer-reviewed literature.
- E4: Tutorial summary, panel discussion, technical report, or a book chapter or literature in PowerPoint slides.
- E5: Papers not written in English.

After the process of inclusion and exclusion were employed, the validity of the inclusion and exclusion process was checked. Each author randomly selected 10 papers to apply the inclusion and exclusion process to verify if the included or excluded papers were properly reviewed and classified. Following this, a meeting was held between the authors to reach a consensus about any disagreements on the included or excluded papers.

3.2.5 Quality Assessment

To evaluate the quality of the papers obtained from the inclusion and exclusion phase, 11 quality assessment criteria were applied based on the recommendation of Dyba [8]. The 11 quality criteria questions are not listed in this paper and can be found in [8]. These criteria were used to rate the quality of reviewed papers and to ensure the selected papers contributed effectively to the review study. The criteria were "Agree", ‘‘Partially Agree" and "Not Agree" scale, criterion in ‘‘Q1’’ was used as a basis for considering or rejecting a study. In the case that question ‘‘Q1’’, or both of questions ‘‘Q2’’and ‘‘Q3’’, scored a "Not Agree" answer, there was no further quality assessment done by the reviewer. The scoring procedures were calculated based on giving different values to the quality criteria: Agree = 1, Partially Agree = 0.5 and Not Agree = 0. The validity of the quality assessment process was checked based on the suggestions of Kitchenham [9]. Accordingly, one researcher should extract the data and another researcher should check the extracted data. In this case, the reviewer conducted the assessment on all of the retrieved papers based on the recommended 11 criteria. Then, the second and the third author independently performed the quality assessment on the selected papers and compared both quality assessments. This validity check helped to resolve any scoring differences in the assessment.

Of the 74 papers assessed for quality, the number of papers were included based on the screening criterion was 71 papers. All disagreements of the remaining three papers were resolved by setting a discussion between the three researchers. Finally, the researchers were agreed to include the three remaining papers in the review.

3.2.6 Data Extraction

The 74 primary studies have been read in detail to extract the data required in order to answer the review questions. A data extraction form was developed to extract the data so as to have reliable and accurate extraction of the relevant data from each paper. Table 3.3 shows that some of the data that were extracted were specifically focused on the research questions and other data were required for later analysis, irrespective of the research question.

Table 3.3: Data extraction form

Code	Field /Data	Related Research question
D1	Extraction date	Documentation
D2	Author name	Documentation
D3	Title of publication	Documentation
D4	Publication source	Documentation
D5	Year of publication	Documentation
D6	Type of publication	Documentation
D7	Aims and objectives	Documentation
D8	Research question	Documentation
D9	Security and usability problems	RQ1
D10	Security elements	RQ1,RQ3
D11	Usability attributes.	RQ1,RQ3
D12	GDS usability and security problems	RQ1
D13	Smart devices usability and security problems	RQ1
D14	Evaluation method used (name and short description)	RQ2,RQ3, RQ4
D15	Guidelines, Policy, Training	RQ4
D16	Statistical data used for analysis	Documentation
D17	Domain or Context	RQ1,RQ2, RQ3

The two other authors reviewed and checked the consistency of the data extraction process, each one selected 10% of the primary studies and extracted the data for the second time and then compared their data sheet with the primary reviewer’s data sheet. Any differences found in the data extraction between the primary reviewer and the other two authors were reconciled and resolved collaboratively [9]. The extracted data was documented and kept in a Mendeley file and Excel spread sheets for future analysis.

The papers found were categorised based on 3 different categories and each category was further divided into sub-categories in order to minimise possible misrepresentations of the data extracted. This classification of the primary studies was based on defining a set of possible answers for each of the research questions.

3.2.7 Usability and Security Issues

Papers in regard to research question one (RQ1) were categorised based on four main categories (C1-A, C1-B, C1-C, and C1-D) and each category was further classified into sub-categories. The following classifications were used to describe any paper that discussed or reported any of the usability and security issues in eGovernment settings:

- **C1-A**: GDS usability problems (efficiency, satisfaction, learnability, memorability, errors, other).
- **C1-B**: Smart device usability problems (device context, connectivity, screen size, display resolution, processing, capability and power, data entry method, other)
- **C1-C**: Smart devices security issues (authentication, access control, availability, data and message security, non-repudiation, secure storage).
- **C1-D**: GDS security issues (authentication, availability, confidentiality, integrity, non-repudiation, other).

3.2.8 Assessment of Usability and Security

Regarding research questions two and three (RQ2 & RQ3) the retrieved papers were grouped based on four main categories (C2-A, C2-B, C2-C, and C2-D) and each category has a sub-category. What follow next are the main categories and their sub categories:

(i) **C2-A:** *The focus of the assessment:*

(a) Usability assessment.

(b) Security assessment.

(c) Trade-off between security and usability.

(ii) **C2-B:** *Usability and the method of security evaluation:*

(a) Testing (if it involves an evaluator observing participants interacting to determine problems).

(b) Inspection (if it involves an expert evaluator using a set of criteria to identify potential usability problems e.g., heuristic evaluation).

(c) Inquiry (if it presents a method that collects participants' preferences or feelings from interviews and questionnaires).

(d) Analytical Modelling (if it presents an engineering method that employing different kinds of models).

(iii) **C2-C:** *The type of study used to evaluate security and usability:*

(a) Controlled experiment.

(b) Interview.

(c) Focus group.

(d) Survey.

(e) Case Study.

(iv) **C2-D:** *Domain or context:*

(a) E-government.

(b) Academic.

(c) Industrial.

(d) Medical.

(e) E-Commerce.

(f) Others.

3.2.9 Training and Policies

Any retrieved papers that fell under research question four (RQ4), were classified based on the following categories:

(i) C3-A: Types of training:

(a) Social engineering training.

(b) Security Awareness.

(c) Population awareness.

(ii) C3-B: Types of existing policies:

(a) Security policy.

(b) Acceptable use policy.

(c) Legalisation and regulation policy.

(d) Others.

3.2.10 Data Synthesis

The data extraction and data classification processes were completed according to the designed protocol and all the processes were assessed. Extracted data that was redundant was removed and the quality of the data was rechecked. This meant that all of the checked data was considered suitably qualitative and valid and therefore applicable to explain and answer the research question. The aim of the mapping study was to answer the research question with effective and reliable data. The data synthesis activities were used to summarise the results of the primary studies, the extracted data was manually studied, and descriptive synthesis was conducted to show the results in a different tabular form. Descriptive statistics were applied for analysing and summarising the data.

3.3 Results and Analysis

The extracted data was analysed and summarised in a structured way that assisted in finding some possible answers for the stated research questions. In the next section we provide an overview of the selected primary studies and the extracted information in regard of research questions.

3.3.1 Results Overview

After carrying out the filtering phases described previously, 74 primary studies were obtained from 3 journals and 3 conferences (across multiple years) and were used for data analysis and answering the research question. The highest volume of conference papers had been published in 2009 and most of the journal papers had been published in 2014, this is due to the release of various multi-touch interface smart devices in 2007 such as the Apple smart phone.

Out of the 74 papers found, 57% of them were conference papers and 43% were journal papers. This indicates that the majority of papers collected were from conference sources rather than journal publications and this could be due to the longer time required by authors to publish work in journals rather than conferences.

3.3.2 Research Questions' Results

Research question one (RQ1) asked: "What are the existing usability and security problems concerning government digital services (GDS) when accessed by smart devices?" To find the data to answer this question the data from D9, D10, D11, D12, and D13 were analysed from the data extraction form (see Table 3.3). The analysis of selected papers shows that 40 papers contained relevant content and discussed usability and security problems concerning an eGovernment platform.

The answer to this question (RQ1) is divided into four sections to give a clear view of the reviewed papers.

GDS usability problems: Usability is considered an important feature that can affect the user's interaction with government digital services. This review identifies five attributes that can affect the overall usability of GDS. These attributes are based on the Jacob Nielsen usability model [10] and they are: efficiency, learnability, satisfaction, memorability and errors attributes. Based on the review question and categorisation of the selected papers, most of the studies explain and address the usability issues in an eGovernment setting based upon these five attributes as shown in Table 3.4. Learnability and efficiency are the most addressed attributes of the selected papers and each of them are present in 11% of the reviewed papers. Conversely, error is the least addressed usability attribute, only present in 3 papers. The other two attributes are each present in 8% of the reviewed papers. Amongst the analysed studies, 3 studies do not clearly specify which usability attributes are addressed. These studies [5], [11], and [12] concentrated more on content analysis without stating any of the usability attributes. From Table 3.4 it is obvious that usability attributes have been considered by most of the studies selected in regard to RQ1.

Smart devices usability problems: In this section papers related to smart devices' usability problems are analysed and examined based upon six elements identified in [4]; device context, connectivity, screen size, display resolution, processing capability, and data entry method. The retrieved papers in regard to RQ1 were categorised by at least one of these elements. In total there were 12 papers found discussing the usability of smart devices. Some of the reviewed papers investigated more than one element of usability for smart devices and so these would be counted twice or more. The greatest volume of work was focused on device context (i.e. this includes the location, identities of nearby people, time, temperature, colour, weight). Eight selected papers discuss this element. The elements of connectivity and data entry methods are equally second ranked, with 3 papers each. In terms of display resolution, screen size and processing capability, there were two papers found for each element. Generally, the selected publications considered in this section have not focused on the field of GDS so far.

The analysis of the papers indicates that a general usability evaluation for smartphones has been done but it has not focused on the problems generated by these devices in an eGovernment setting. This could be due to the unique features of such smartphones and that current smartphone platforms differ considerably in terms of the functionality provided and the security features.

GDS security problems: The security problems were broken down into subcategories to provide a broad view about the problems of security in a GDS setting and to make it easier for later evaluation. This review study classifies the papers for this section based on six well-known security elements. The elements are: authentication, availability, confidentiality, integrity, non-repudiation, and security storage. As shown in Table 3.4, there are only a few papers that discuss security in a GDS setting. Similarly, to the previous section, the total number of papers shown in Table 3.4 is more than the number of papers included in the review of this section and this is due to some of the studies falling into more than one element of security; so, they were counted twice or more for each of the elements for which they were considered. The most researched elements found concerning the security of GDS in this section were authentication and integrity, with 6 and 3 papers respectively. The other remaining elements were addressed among the reviewed papers by 2 papers each. There were few papers that were found in this review addressing the security of GDS, due to the complex nature of the government system and the availability of information for researchers about it.

To conclude, the reviewed papers were indicated the importance of usability and security in an eGovernment setting, and their effects on users' attitudes, perceptions and interactions. The results of the selected papers related to this question indicate that the set of reviewed studies do not address the usability and security problems that may occur when services are accessed through smart devices. In addition to this, there was no evidence found from the reviewed papers that they considered the assessment of the problems of usability and security in an eGovernment setting when using smart devices. It has also been found from the analysis that most of these attributes have been assessed independently without considering the smart devices' needs concerning GDS.

The main concerns of the currently reviewed studies relating to usability issues in an eGovernment context are the efficiency, learnability, satisfaction, and memorability. These attributes have been measured and assessed in a GDS setting and addressed by most of the papers found. The results determine that the element of authentication in the security of GDS and smart devices is the most studied element by the papers reviewed. Finally, the analysis of the reviewed papers related to research question one shows that comprehensive assessment of security and usability is missing in the context of GDS when accessed by smart devices.

Table 3.4: Papers addressing research question one

Problem	No of Papers	Papers Reference
GDS usability problems	**13**	
1) Efficiency	*8*	(González Martínez et al., 2011), (Baker, 2009), (Welle Donker-Kuijer, de Jong and Lentz, 2010), (Gouscos et al., 2007), (Huang and Benyoucef, 2014), (Hung, Chang and Kuo, 2013), (Papadomichelaki and Mentzas, 2012),(Venkatesh, Hoehle and Aljafari, 2014).
2) Satisfaction	*6*	(González Martínez et al., 2011), (Gouscos et al., 2007), (Huang and Benyoucef, 2014) , (Hung, Chang and Kuo, 2013), (Papadomichelaki and Mentzas, 2012),(Ahmad, Shoaib and Prinetto, 2015).
3) Learnability	*8*	(González Martínez et al., 2011), (Baker, 2009), (Welle Donker-Kuijer, de Jong and Lentz, 2010), (Gouscos et al., 2007), (Huang and Benyoucef, 2014), (de Jong and Lentz, 2006), (Venkatesh, Hoehle and Aljafari, 2014), (Ahmad, Shoaib and Prinetto, 2015)
4) Memorability	*6*	(Baker, 2009), (Gouscos et al., 2007), (Huang and Benyoucef, 2014), (de Jong and Lentz, 2006), (Venkatesh, Hoehle and Aljafari, 2014),(Ahmad, Shoaib and Prinetto, 2015).
5) Errors	*3*	(Gouscos et al., 2007), (Huang and Benyoucef, 2014), (de Jong and Lentz, 2006)
6) Others	*3*	(Olalere and Lazar, 2011),(Kokini et al., 2012), (Kotamraju and Van Der Geest, 2012).
Smart devices usability problems	**12**	
1) Device Context	*8*	(Adami et al., 2011),(Markova et al., 2007), (Heller et al., 2010), (Keijzers, den Ouden and Lu, 2008), (Wang et al., 2009),(Yeratziotis, Pottas and van Greunen, 2012), (Rohnke and Yahner, 2008).
2) Connectivity	*3*	(Nylander, Lundquist and Brännström, 2009),(Lesemann, Woletz and Koerber, 2007), (Sieger and Möller, 2012), (Rohnke and Yahner, 2008).
3) Screen size	*2*	(Reynaga, Chiasson and van Oorschot, 2015), (Sousa, Smeets and Brenner, 2012)
4) Display resolution	*2*	(Reynaga, Chiasson and van Oorschot, 2015), (Sousa, Smeets and Brenner, 2012)
5) Processing capability	*2*	(Lesemann, Woletz and Koerber,

		2007),(Keijzers, den Ouden and Lu, 2008)
6) Data entry method	*3*	(Reynaga, Chiasson and van Oorschot, 2015), (Sousa, Smeets and Brenner, 2012), (Rohnke and Yahner, 2008).
GDS security problems	***7***	
1) Authentication	*6*	(Aichholzer and Strauß, 2009), (Sieger and Möller, 2012), (Papadomichelaki and Mentzas, 2012), (Inglesant and Sasse, 2010), (Just, 2004), (Sasse, 2015).
2) Availability	*2*	(Aichholzer and Strauß, 2009), (Papadomichelaki and Mentzas, 2012).
3) Confidentiality	*2*	(Choi et al., 2013a), (Papadomichelaki and Mentzas, 2012).
4) Integrity	*3*	(Choi et al., 2013a), (Sieger and Möller, 2012), (Papadomichelaki and Mentzas, 2012).
5) Non-repudiation	*2*	(Choi et al., 2013a), (Papadomichelaki and Mentzas, 2012).
6) Secure storage	*2*	(Choi et al., 2013a), (Papadomichelaki and Mentzas, 2012).
Smart devices security problems	***11***	
1) Authentication	*10*	(Reynaga, Chiasson and van Oorschot, 2015), (Jakobsson et al., 2008),(Chowdhury, Poet and Mackenzie, 2014), (Chilana et al., 2011), (Spinnewijn, 2009),(Sieger and Möller, 2012), (Robertson, 2001), (von Zezschwitz, Dunphy and De Luca, 2013),(Herley, 2014), (Dhamija and Dusseault, 2008).
2) Access control.	*1*	(Dhamija and Dusseault, 2008).
3) Availability	*2*	(Herley, 2014), (Dhamija and Dusseault, 2008).
4) Data and message security	*3*	(Choi et al., 2013a), (Sieger and Möller, 2012), (Robertson, 2001).
5) Non-repudiation	*1*	(Dhamija and Dusseault, 2008).

RQ2 asks "What methods of evaluation have been used to assess the usability and security of government digital services when accessed by smart devices?" D14 and D17 have been analysed from the data extraction sheet summarised in Table 3.3. About 33 papers were found that related to this question from all of the papers reviewed (see Table 3.5, 3.6 and 3.7). This question contains two parts that are required to be answered in terms of the evaluation methods used. The first part is the usability evaluation methods used to assess the usability of GDS when accessed by smart devices. The second part is the evaluation methods that measure the security of GDS when accessed by smart devices. The results from the two parts of this question help to identify the most widely used methods that have been used in the context of GDS.

Table 3.5: Usability testing methods used

Usability Testing	No of Papers	Papers Reference
Coaching Method	*1*	(González Martínez et al., 2011)
Thinking-Aloud Protocol	*10*	(Rohnke and Yahner, 2008),(Hornbæk and Frøkjær, 2005),(Mankoff, Fait and Tran, 2005; Bruun et al., 2009), (Jakobsson et al., 2008), *[56],[57],[58], [65],[78]*
Question-Asking Protocol	*1*	(Grossman, Fitzmaurice and Attar, 2009)
Teaching Method	*2*	(Keijzers, den Ouden and Lu, 2008; Akers et al., 2009)
Performance Measurement	*1*	(Kokini et al., 2012)
Log File Analysis	*1*	(Ben-Asher et al., 2009)
Retrospective Testing	*4*	(Mankoff, Fait and Tran, 2005; Tohidi et al., 2006; Wang et al., 2009; González Martínez et al., 2011)
Remote Testing	*3*	(Petrie et al., 2006; Andreasen et al., 2007; Bruun et al., 2009)
System Usability Scale (SUS)	*2*	(Sauro and Kindlund, 2005; Sousa, Smeets and Brenner, 2012)
Metaphor of human	*1*	(Hornbæk and Frøkjær, 2005)
Collaboration critique method	*1*	(Babaian, Lucas and Oja, 2012)

Usability evaluation methods: The analysis of the reviewed papers found that a wide range of usability evaluation methods (UEMs) have been used to improve the usability of GDS by measuring the users' attitudes, perceptions and interactions with the eGovernment system. Most of these methods have been used to assess the problems of GDS, the findings of these methods vary widely from one evaluator to another and this can be due to different reasons such as the evaluator’s skill and the method not having been appropriately applied. The analysis of the reviewed papers revealed that there are different classes of UEMs that were recognised and have been used in the context of eGovernment. These methods are grouped into different classes such as usability inspection methods, testing, usability inquiry, and analytical modelling. Testing, usability inspection and usability inquiry are utilised for formative and summative purposes in software engineering [46]. There are several methods tested and used which come under one of the above categories based on their attributes. The methods found in the reviewed papers that are related to this section are shown in (Table 3.5, 3.6 and 3.7). The analysis of the selected papers found that the method most used to evaluate the usability of GDS was the “Thinking-Aloud Protocol”, which was found in 10 papers (see Table 3.5). This method was used at different levels of the software development life cycle; this technique is cost-effective. An evaluator uses it in order to ask the participant to express his or her thoughts, feelings, and opinions whilst interacting with the system. The second UEM that has been used and is well recognised by experts in the field is “Heuristic Evaluation” this method is classified as a usability inspection method, where an expert identifies violations of the heuristic. This method is considered very popular in comparison to other types of usability inspection and it expends fewer resources [46]. There were 8 papers found considering this method and that evaluated the eGovernment portals (see Table 3.7). The other remaining methods were not intensively used to examine the eGovernment setting because these techniques require special resources and the data type collected (quantitative or qualitative) [46]. The third class of usability evaluation method used and identified in the reviewed papers is the inquiry method or the type of usability study used. Usability inquiry method is about obtaining information after the evaluator observes the interaction of the user with the system in real-time.

The most popular usability inquiry methods that have been recognised by the reviewed papers are: case studies, surveys, questionnaires, interviews, and field studies, alongside many other techniques shown in Table 3.6. The aim of these methods is to collect subjective user impressions, preferences and opinions about the characteristics of the user interface. These methods can also be used by testers to gather additional data after the implementation of the system has occurred. The analysis of the related papers in this section also shows that some papers have described the author’s own experiments whilst some of them have evaluated other studies. The analysis of the reviewed papers indicates no evidence that these evaluation methods have been used to assess the usability of GDS in parallel with smart devices needs. There is no paper that has discussed whether eGovernment services are usable when browsed and accessed by smart devices (e.g. smart phones, iPads, etc.).

Table 3.6: Usability inquiry methods used

Usability Inquiry	No of Papers	Papers Reference
Questionnaires	*6*	(Lesemann, Woletz and Koerber, 2007; Keijzers, den Ouden and Lu, 2008; Frandsen-Thorlacius et al., 2009; Følstad, Law and Hornbæk, 2012; Hung, Chang and Kuo, 2013; Ahmad, Shoaib and Prinetto, 2015)
Interviews	*6*	(Robertson, 2001; Markova et al., 2007; Rohnke and Yahner, 2008; Chilana, Wobbrock and Ko, 2010; Inglesant and Sasse, 2010; Kotamraju and Van Der Geest, 2012)
Field study	*3*	(Rohnke and Yahner, 2008; Wang et al., 2009; von Zezschwitz, Dunphy and De Luca, 2013)
User Feedback	*5*	(Petrie et al., 2006; Andreasen et al., 2007; Jakobsson et al., 2008; Akers et al., 2009; Chilana, Wobbrock and Ko, 2010).
Surveys	*7*	(Robertson, 2001; Gouscos et al., 2007; Chilana et al., 2011; González Martínez et al., 2011; Papadomichelaki and Mentzas, 2012; Renaud, 2012; Venkatesh, Hoehle and Aljafari, 2014)
Focus Groups	*4*	(Just, 2004; Mankoff, Fait and Tran, 2005; Markova et al., 2007; Chan and Wei, 2009)
Self-Reporting Logs	*5*	(Mankoff, Fait and Tran, 2005; Lindgaard and Chattratichart, 2007; Leon et al., 2012; Petrie and Power, 2012),(Baker, 2009)
Case Study	*7*	(Petrie et al., 2006; Lesemann, Woletz and Koerber, 2007; Markova et al., 2007; Aichholzer and Strauß, 2009; Choi et al., 2013a; Choi, Ae Chun and Cho, 2014),(Ji et al., 2010)
Analytical modeling	*3*	(Tohidi et al., 2006; Bruun et al., 2009; Chowdhury, Poet and Mackenzie, 2014)
Simulation	*5*	(Mankoff, Fait and Tran, 2005; Petrie et al., 2006; Jakobsson et al., 2008; Heller et al., 2010; Chowdhury, Poet and Mackenzie, 2014)

Controlled experiment	*12*	(Hornbæk and Frøkjær, 2008b; Keijzers, den Ouden and Lu, 2008; Rohnke and Yahner, 2008; Ben-Asher et al., 2009; Frandsen-Thorlacius et al., 2009; Spinnewijn, 2009; Wang et al., 2009; Kokini et al., 2012; Leon et al., 2012; Sieger and Möller, 2012; Sousa, Smeets and Brenner, 2012; Plotnick, Hiltz and Burns, 2013)
Screen Snapshot	*1*	(Leon et al., 2012)

Table 3.7*: Usability inspection methods used*

Usability inspection	No of Papers	Papers Reference
Heuristic Evaluation	*8*	(Ji et al., 2010; Welle Donker-Kuijer, de Jong and Lentz, 2010; Olalere and Lazar, 2011; Yeratziotis, Pottas and van Greunen, 2012; Alonso-Ríos, Mosqueira-Rey and Moret-Bonillo, 2014; Huang and Benyoucef, 2014; Venkatesh, Hoehle and Aljafari, 2014; Reynaga, Chiasson and van Oorschot, 2015)

Security evaluation methods: The analysis of the reviewed papers found that papers that relate to security could be divided into two categories. The first set of the reviewed papers reports on some of the technical security threats and the second set reports on the non-technical viewpoint. The reviewed papers focus more on threat analysis of eGovernment services and risk assessment. These assessments are followed by some guidelines and recommendations proposed by the author to mitigate the security risks that have been identified in the analysed system. The total number of papers reviewed describing evaluation methods of security is 11. There is no clearly favoured method that can be identified from the reviewed papers, some of them propose security evaluation methods by following HCI guidelines, and that use security standards such as ISO/IEC 27002 and ISO/IEC 27001 for evaluating the security of the system. To conclude, it was difficult to identify any framework or security model that considered the eGovernment security requirements needed when being accessed by smart phones.

About research question three (RQ3): *"How is the trade-off between usability and security measured and assessed in the context of government digital services?"* The data analysis of D10, D11, D14 and D17 from the data extraction form revealed that 32 papers were found focusing on usability assessment and 17 other papers discussed security assessment from the total selected papers (See Table 3.8). Furthermore, trade-offs in the domain of usability and security in a government setting were not addressed in the reviewed papers; only 7 papers were found that focused on different settings such as (eHealth, eBanking and email). The papers found were too limited in scope to specifically address how the balance between usability and security is deployed in an eGovernment context. The main focus of the selected papers was on the trade-off between usability and security of passwords and logins, because passwords and login are considered the most vulnerable aspect of a secure system.

However, in order to achieve a balance between usability and security in an eGovernment setting, it is obvious that a new framework or approach is necessary to address the specific needs of the eGovernment domain. Therefore, a newly focused assessment of trade-offs should be developed to meet the requirements of usability and security in the context of GDS. To summarise, the retrieved papers acknowledge the presence of the trade-off as evident in the literature, but actual measurement and metrics could not be found in the reviewed papers. Suggestions on how the trade-off between usability and security can be managed have been provided; however, there is distinct lack of direct assessment of usability and security trade-offs in the context of eGovernment.

RQ 4 asks *"What training and policies are available to the public to ensure effective usability and security of government digital services when accessed by smart devices?"* the data of D15 and D14 were analysed to identify any policies or training that have been provided to ensure the effectiveness of usability and security in the context of GDS. There are seven reviewed papers related to this question.

Table 3.8*: Matter of assessment*

Papers Focus	No of paper	Papers Reference
Usability	*32*	(Sauro and Kindlund, 2005),*[48]*,(Følstad, Law and Hornbæk, 2012),(Hornbæk and Frøkjær, 2005),(Babaian, Lucas and Oja, 2012),(Tohidi et al., 2006),(Mankoff, Fait and Tran, 2005),(Petrie et al., 2006),(Chilana, Wobbrock and Ko, 2010),(Lindgaard and Chattratichart, 2007),(Petrie and Power, 2012),(Andreasen et al., 2007),(González Martínez et al., 2011),(Sousa, Smeets and Brenner, 2012),(von Zezschwitz, Dunphy and De Luca, 2013),(Keijzers, den Ouden and Lu, 2008),(Wang et al., 2009),(Baker, 2009),(Welle Donker-Kuijer, de Jong and Lentz, 2010),(Gouscos et al., 2007),(de Jong and Lentz, 2006),(Olalere and Lazar, 2011),(Papadomichelaki and Mentzas,

		2012),(Venkatesh, Hoehle and Aljafari, 2014),(Verdegem and Verleye, 2009),(Johnson and Willey, 2011),(Alonso-Ríos, Mosqueira-Rey and Moret-Bonillo, 2014),(Ji et al., 2010), (Rohnke and Yahner, 2008), (Hertzum, 2010), (Lewis, 2014), (Ahmad, Shoaib and Prinetto, 2015).
Security	*17*	(Jakobsson et al., 2008),(Petrie et al., 2006),(Spinnewijn, 2009),(Plotnick, Hiltz and Burns, 2013),(Choi et al., 2013a),(Choi, Ae Chun and Cho, 2014),(Aichholzer and Strauß, 2009),(Sieger and Möller, 2012),(von Zezschwitz, Dunphy and De Luca, 2013),(Just, 2004),(Bhattacharya et al., 2014),(Herley, 2014),(Chan and Wei, 2009),(Johnson and Willey, 2011),(Renaud, 2012),(Burch, 2010),(Yeratziotis, Pottas and van Greunen, 2012).
Trade-off between usability & security	*7*	(SHAY ET AL., 2014),(BRAZ, SEFFAH AND M'RAIHI, 2007),(BEN-ASHER ET AL., 2009),(SASSE, 2015),(WHALEN, 2011),(GUTMANN AND GRIGG, 2005),(CRANOR AND BUCHLER, 2014)

The retrieved papers were classified based on the category shown in Section 3.2.9 recommended previously in order to answer this question. The retrieved papers' main focus was about general legalisation and regulation policy of security and usability. Others were classified on security policy elements, such as making suggestions to the users about the design of passwords and the design of security questions. Some of the other papers provided recommendations about user security education and how to enhance the users' understanding about security. However, the papers related to this question were insufficient to provide any evidence about policies and training in the domain of GDS. To conclude, it was apparent from the reviewed papers that such policies and training in the context of eGovernment have not been well studied and addressed.

3.4 Review Limitations and Threats to Validity

The main threat to the validity of the review is the limitation of the conferences and journals selection. The 74 papers were retrieved from three conferences and three journals (editions / volumes over multiple years, 2005 – 2015), which could have contributed to missing a considerable number of relevant papers to the review study. This was due to time concern and the high number of papers retrieved in the automatic search. In addition to this, inaccuracy and bias in the retrieved papers for review during the automatic search is one of the study limitations. Conducting manual searches and then comparing those with the automatic searches mitigated this bias and ensured that the search string for the automatic search resulted in all the relevant papers. Another bias was reduced with the inclusion and exclusion process, which influences the process of paper selection. Having two additional authors checking the included and excluded papers mitigated this bias. Another important threat to validity was identified in the review as inaccuracy in data extraction. The data extraction process was somewhat complicated to extract relevant information from the selected papers, as some papers do not clearly report the methods used and what type of setting was used. Finally, the reviewer's lack of experience in designing protocol for a mapping study is another threat to the validity of the study that should be considered. The guidelines provided by [7] and advice from experienced practitioners of systematic reviews and mapping studies helped in reducing and avoiding some of these threats.

3.5 Conclusion

This chapter aims to answer four research questions with respect to usability and security in an eGovernment setting. A systematic map of 74 publications has been conducted in order to answer the study questions.

The results highlight that very few of the papers reviewed being published included any kind of usability and security assessment in the GDS setting. The Mapping Study also highlights that the majority of papers looking into the trade-off between usability and security are restricted to the examination of the login methods in different contexts. Therefore, the need to have empirical research focusing on an eGovernment setting in terms of evaluation methods and the trade-off between usability and security is clearly identified. The reviewed papers confirmed that usability and security in GDS, when accessed with smart devices, is not being addressed and there is scope for more work in this area. Future work should focus on the aspects of usability and security in an eGovernment setting and aim for an integrated framework for the assessment of these in order to achieve an optimal trade-off between usability and security. Furthermore, this needs to be complemented by more research on awareness and education policies related to the usability and security trade-off in the context of eGovernment services accessed through smart devices.

Chapter 4 Methodology

This chapter presents the methods used to accomplish the research, how the qualitative and quantitative data is collected an overview of the study participants and how the analysis is performed. The ethical issues are discussed were applicable for each part of the research.

4.1 Introduction

This chapter presents the methods used to accomplish the research. The research strategy is conducted based on three sub-studies related to the e-government context. The main purpose of conducting the three sub-studies is to obtain insight into the user experience and investigate and explain user behaviour and attitudes in order to get a comprehensive view of the influences and their significance to perceived security and usability. The three sub-studies explore the negative and positive aspects users experience with e-services in terms of usability and security features. This study aims to generate guidelines to help government service providers understand the trade-off between usability and security from the users' perspective. Both quantitative and qualitative data are collected through a questionnaire survey and focus group in order to achieve the research goals and answer the research questions. Therefore, the study is mixed method research, using a triangulation approach. Triangulation is a research strategy researchers use to overcome the weaknesses of a single research method by examining the same phenomenon using different methods (Heale, Forbes and Heale, 2013). Combining various methods such as surveys and focus groups in the same research is a triangulation approach (Olsen, 2004). Figure 4.1 illustrates the thesis research design.

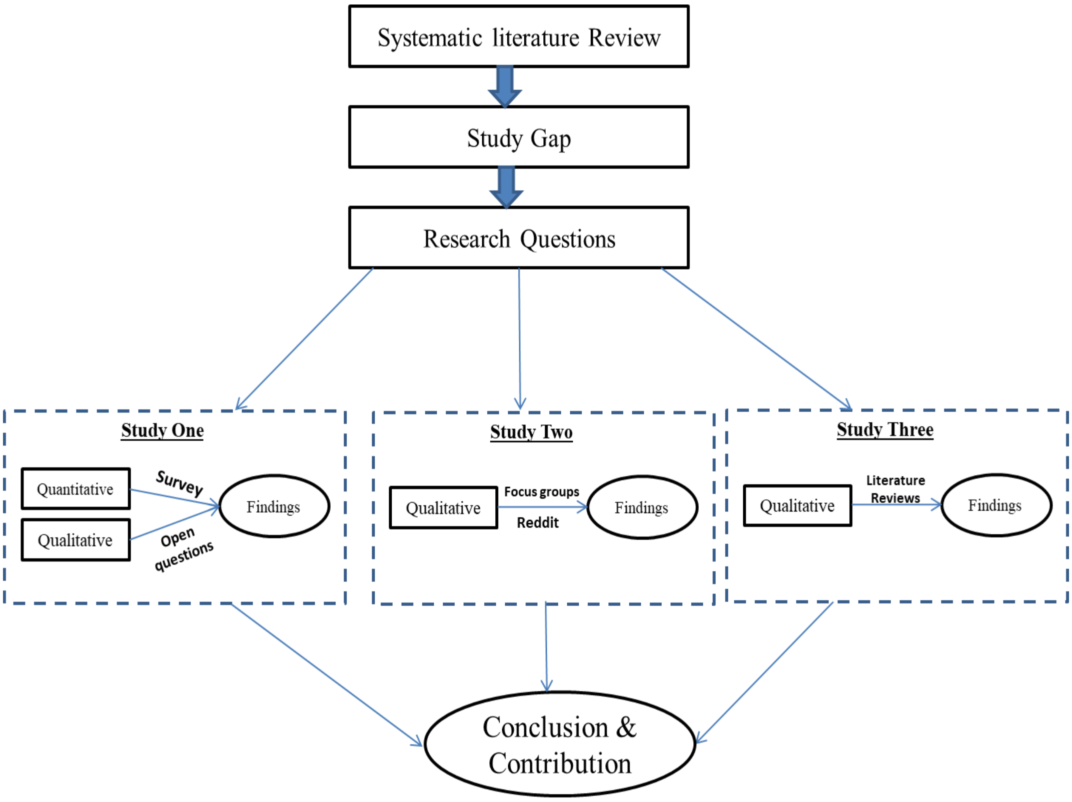

Figure 4.1: Research Study Design

4.2 Research Strategy

This research as a whole is situated between two schools of belief, positivist and interpretive. The researcher finds both approaches are applicable to achieve the aims and objectives of the study. Positivism and interpretivism are two approaches to research in the natural sciences (Bryman, 2016). A positivist approach is usually taken with quantitative methods, as it deals with numbers that generate evidence, collecting data as quantifiable variables to give good reliability and representativeness (Lichtman, 2012). This approach has a scientific paradigm, mainly carried out in the field of information systems, to test the validity of hypotheses (Saunders, Lewis and Thornhill, 2017) and to investigate certain phenomena regardless of the researcher's perspective or beliefs. Positivist researchers attempt to stay detached from the research participants by maintaining a distance, which can help them stay emotionally neutral and make clear distinctions between reason and feeling (Hudson, Research and 1988, 1998)(Hudson, 2018; Carson et al., 2001). Positivist researchers remain neutral, and use a formal reporting style, an impersonal passive voice and technical terminology (Tashakkori and Teddlie, 1998). However, this research paradigm has been criticised by many researchers for ignoring related findings (Trochim, 2006), despite providing a clear theoretical focus and increasing the ability to control the research process (Saunders, Lewis and Thornhill, 2017; Collis & Hussey 2013). Orlikowski and Baroudi (1991) assert that a positivist approach is used in information systems and information technology (IS/IT) research and is carried out based on deductive reasoning.

On the other hand, an interpretive approach is also used widely in IS to create a better understanding of the context of the information system, and the process by which the information system influences, and is affected by, the context (Walsham, 1995). This approach is mainly used in order to get a better understanding of a phenomenon through qualitative research, by focusing on the meanings people give to phenomena rather than measurement. An interpretive approach observes reality from both subjective and objective points of view and complements the weaknesses of positivism (Bryman, 2016). This approach is centred on qualitative research, and provides comprehensive detailed information about the phenomena being explored (Howitt, 2016). The approach can be used to answer research questions that could not be answered by quantitative research. Interpretive research is more suitable to mixed methods where both qualitative and quantitative research are used to enhance the researcher's understanding of reality. The approach is based on an inductive process of building theories, qualifying the research findings, determining the gap, analysing the collected data and understanding the human experience in a specific setting (Howitt, 2016). However, with an interpretative approach, the data collection and analysis are time consuming and the outcomes may be misinterpreted by the researcher, leading to unclear patterns in the analysed data at the end of the research process (Wahyuni, 2012).

4.3 Mixed Research Methods

Quantitative and qualitative approaches are obviously different. Quantitative research is 'hard' research that mainly deals with numbers and statistical methods to interpret data

(Bryman, 2016). Quantitative research uses a deductive approach to test the association between theory and reality. In contrast qualitative research is mainly concerned with words rather than numbers in its data collection and analysis processes. It investigates the nature of people's experiences of a given phenomenon that are not easy to capture as part of quantitative research (Strauss and Corbin, 1990). Qualitative research is about interpreting social realities based on inductive processes (Patton, 2005).

Many researchers have questioned the difference between qualitative and quantitative research and which approach is better (Tashakkori and Teddlie, 1998). Others, such as Trochim (2006) and Patton (2005), claim that qualitative and quantitative data are related and both are acknowledged as legitimate approaches. The authors acknowledge that there are no reasons why qualitative and quantitative methods cannot be used together. Even though qualitative methods are good in some situations and quantitative methods are applicable to others, in many cases there is great benefit to using mixed methods in the same research. Researchers combine qualitative and quantitative research methods in a single research study, when quantitative methods are right for answering certain research questions and qualitative methods are right for others (Hayati et al. 2006; Avison et al. 2001).

This approach is called 'methodological triangulation', meaning the application of more than one method in the same study (Amaratunga et al., 2002). Triangulation is used by researchers to ensure the validity of their research findings through the use of various methods of collecting data (Johnson and Onwuegbuzie, 2004). Using triangulation increases confidence in the research findings through the use of mixed methods and gives a more comprehensive picture of the results than one approach could alone (Johnson and Onwuegbuzie, 2004). Creswell (cited in Marvasti 2018) and Brannen (2005), argue that mixed method study serves other purposes beyond triangulation. There are a number of advantages that can be identified when methods are combined. The first is data validation, when both qualitative and quantitative methods give the same results. The second is elaboration, as in some cases the analysis of qualitative data explains and clarifies the quantitative findings. The third benefit of mixed methods is complementarity, where results are generated from the two methods, but new understandings or perceptions are captured when they are taken together. However, contradiction is another possible outcome, if the qualitative and quantitative results are in conflict with one another (Johnson and Onwuegbuzie, 2004).

Mixed methods help the researcher be more confident in the study results than a single method. The use of mixed methods in research can reduce measurement error and help overcome any bias issues (Clarke, 1999). However, mixed methods may lead to contradictions or confusion for researchers if their objective is only to obtain a broader picture of the phenomenon tested. In our research, three studies are conducted, and the methods selected for each study are based on the study objectives and research questions, as explained in the dedicated chapters.

4.4 Research Design

The research design can be categorised into four types, exploratory, descriptive, explanatory and predictive (Collis and Hussey, 2013). Exploratory research is carried out when a phenomenon has not been studied clearly and not much information is known. Such research is undertaken in order to better understand the nature of the problem, and obtain new insights into phenomena (Sekaran & Bougie 2016; Saunders, Lewis and Thornhill, 2017). This type of research uses research methods such as interview, observation and case study, to collect both qualitative and quantitative data. However, exploratory research can hardly give conclusive answers to the research problem (Collis and Hussey, 2013).

Descriptive research uses quantitative and statistical techniques to describe and explore problems, as well provide the researcher with the relevant characteristics of the studied phenomenon. Descriptive studies, can go beyond exploratory research, as quantitative data is considered more important in producing descriptive information about the problem (Sekaran and Bougie, 2016).

Explanatory research is an extension of descriptive research, as it explains how and why things happen. It determines the causal relationships between the variables in the study (Saunders, Lewis and Thornhill, 2017).

Predictive research is more widespread than it used to be, and is used to predict the future and provide answers to “what could happen?” questions on the basis of hypothesised and general relationships (Collis and Hussey, 2013).

4.5 Choice of Study and Rationale

The selection of an appropriate data collection strategy is essential in order to have a reliable investigation and solid evidence. Some factors to consider when selecting among the methods include the ease of data collection, the data's credibility and the resources available to the researcher. Other factors that help the researcher decide which research methods to use include cultural perspectives, the participants' backgrounds and the validity of the finding that are obtained through the methods selected. The literature review in Chapter Two identifies some issues concerning e-government services usability and security that need to be examined using the most appropriate research methods. The researcher's background and familiarity with the research context plays a role in deciding the best methodology for the area of research that can achieve the study objectives. The researcher considers the best methods and approaches that are applicable to the study being conducted.

This thesis reports on three studies conducted to understand the trade-off between usability and security in an e-government context using a mixed methods approach. The research investigates three aspects of this trade-off, the new service being introduced, the new devices being integrated, and the new technology adopted. Each research study examines one of these aspects to explore how users or citizens perceive them in term of usability and security. By conducting these three studies, the researcher seeks a clear and comprehensive picture of users' attitudes, opinions and preferences, and a rich insight into users' needs. This research tries to explain user requirements for new services, devices and technology implemented in e-government settings, in terms of usability and security features.

The research combines elements of three types of research design. It is mainly exploratory, since it purposes to explore user attitudes and opinions about the trade-off between usability and security in an e-government context. It contributes to a better understanding of what users need from the integration of a new service (Bitcoin study), new device (smartwatch study) and new platform (Blockchain technology study) in e-government. To the best of the researcher's knowledge, no studies have been conducted covering these three areas in an e-government context. Our main aim in conducting these three studies is to explore users' perceptions of usability and security in e-government from three different angles to obtain rich insights into users' requirements. In this research, both qualitative and quantitative methods are used to give good coverage of the research topics, as guidelines can be developed, and hypotheses formulated.

This research is also descriptive, as statistics are generated to explain the characteristics of the sample used in the three studies, to describe the categorical variables and to give detail about how many respondents gave each response. Additionally, this research can be considered explanatory as the quantitative data results are explained along with the qualitative data, and vice versa.

A mixed methods strategy, using quantitative and qualitative methods, is believed to be most suitable as it can capture users' experiences and attitudes to the use of e-government services in terms of usability and security. These methods help us understand the three, related, aspects of e-government through the eyes of the participants rather than in categories predetermined by the researcher. Therefore, a questionnaire survey is used, with open-ended questions, and focus group research.

The methods used for each study are selected by mutual agreement between the researcher and the supervisory team. However, the researcher puts a lot of effort into following research standards and consideration of the research objectives and research questions, in order to make them logical and convincing through well-constructed reasoning that makes clear the key ideas and expressions.

4.6 Research Techniques

The research project follows a mixed approach of interpretivism and positivism as the research philosophy. The three studies employed as the research strategy support the research approach. The mixed method research approach is usually used to explore the nature of, understand and describe phenomena (Ormrod and Leedy, 2005). A mixed method approach is usually used when scientists want to explore the subjective and experiential aspects of human beings (Hite, Fontana and Williams, 2015). The results obtained from a mixed research approach help discover or develop a theory (Ormrod and Leedy, 2005). Based on the nature of the research questions, the three studies guide the research project towards a better understanding of usability and security, from the users' perspective, in an e-government setting.

The methods used to obtain results follow the inquiry approach, and such methods require feedback from users as the main focus of the study. It is not about studying specific users' tasks or measuring users' performance. However, the nature of the research is to gather subjective impressions and preferences about the various aspects of usability and security in an e-government setting. Each sub-study of the research uses a different collection method. This research project employs two data collection methods that approach the research questions from different perspectives. The two techniques are the questionnaire and the focus group. Both the methods are explained in detail in the following subsections.

4.6.1 Literature Review

Literature review plays a fundamental role in any study. The researcher has to study the existing information related to the research area. A literature review offers researchers a method to understand and gain insight into the previous research on the topic (Saunders, Lewis and Thornhill, 2017). The literature can be categorised into three types (Saunders, Lewis and Thornhill, 2017):

Primary literature (also called grey literature): The grey literature includes published sources such as reports and government white papers. Unpublished grey literature sources include letters, memos and committee minutes. Grey literature is more difficult to find than other literature.

Secondary literature: Secondary literature resources include publications of primary literature, journals, books and newspapers. Secondary literature is easier to find than primary literature.

Tertiary literature: These are search tools that help researchers locate primary and secondary literature or introduce subjects. Well know tools include encyclopaedias, dictionaries, indexes, abstracts, catalogues, citation indexes and bibliographies.

4.6.2 Questionnaire

A questionnaire is a useful method for assessing subjective satisfaction with an interface. It contains a well-designed set of questions that are circulated to a certain number of users, who return their responses and opinions. Responses to a questionnaire are usually quantitative (e.g., ratings on a 5-point scale), otherwise the results of the activity can be unclear and open to interpretation.

The questionnaire technique used in this study assesses usability and security from users' perspectives and how the participants perceive usability and security as it relates to e-government. A questionnaire is a set of questions that are easy to use and easy for participants to understand. It is a suitable and reliable method used by most researchers to collect scientific data (Zaharias and Poylymenakou, 2009). It is commonly used to identify respondents' opinions, preferences and judgments. It is a cost-effective method, which takes less time to manage than other techniques (Chin, Diehl and Norman, 1988). Therefore, the questionnaire is a useful method for this kind of research to collect data about usability and security perceptions from users' perspectives. The data collected using this method can be quantitative or qualitative, from closed- and open-ended questions.

User perceptions and opinion ratings are usually gathered using questionnaires. Generic questionnaires have been developed for this purpose, such as the system usability scale (SUS), software usability measurement inventory (SUMI), questionnaire for user interface satisfaction (QUIS), after-scenario questionnaire (ASQ) (Chin, Diehl and Norman, 1988), post-study system usability questionnaire (PSSUQ), and computer system usability questionnaire (CSUQ) (Lewis, 2014). These measurement questionnaires are not only intended to focus on user satisfaction, but also evaluate how users perceive the attributes of usability. There are other specific questionnaires designed for assessing intention to use, trust and ease of use, such as the mobile phone usability questionnaire (MPUQ), which serves as a tool to collect data to enhance usability and interface features (Markova et al., 2007).

Questionnaires are used to assess user perceptions and satisfaction about usability and security. The design of the usability and security questionnaire is based on the questionnaires above, modified and extended to better measure users' perceptions and the factors influencing users' engagement in an e-government setting.

The questionnaire is pre-tested by a group of 10 post-graduate respondents from the Computer Science Department at Keele University. Their feedback leads to further elaboration and enhancement of the final version of the questionnaire.

All the responses to the questionnaire are measured on a 5-point Likert scale: 1 (strongly agree), 2 (agree), 3 (neutral), 4 (disagree), 5 (strongly disagree). Once the measurement scale is determined, the researcher uses descriptive statistics to describe the scale in tabular and chart formats in order to draw conclusion about the users' perceptions and the issues that concern them about usability and security.

4.6.3 Focus Group

A focus group interview is a meeting of about six to eight participants, wherein they can reveal their ideas and feelings about matters relating to the topic. A focus group is considered to be a comfortable method, from the participants' point of view, as it is a kind of discussion that assesses users' requirements and feelings before interface design or after deployment. Nielsen (1993) recommends that it is most effective for a focus group session to last about two hours, and to be recorded in an organised way that helps the researcher retrieve all the data with little effort. The data gathered through group interactions in a short period of time are deeper and richer than one-to-one interviews (Krueger and Casey, 2014). The evaluator, or moderator, plays an important role in inquiring and gathering information on predetermined issues from the discussion. Another important feature of a focus group is the influence of the participants on each other through their ideas, discussions, answers and contributions during the meeting (Krueger and Casey, 2014). This technique is used by many researchers and experts to assess how users perceive usability and security features (Verdegem & Verleye 2009; Sieger & Möller 2012; Chan & Wei 2009). Van Velsen et al. (2009) say that researchers use many different methods to assess citizen-centric requirements such as literature review, interviews with experts, surveys and focus groups.

Sieger & Möller (2012), for example, employ the focus group method in their research to observe the perceptions of the genders about the security of authentication and payment functions on smartphones. The data collected presents significant variances in the perceived security and future use of security functions. The method is very helpful and the discussion during the focus group interviews influences the participants' ability to present their ideas, contributing in many different ways during the focus group interview.

Markova et al. (2007) use a focus group method to conduct a study of nine taxi drivers, to evaluate the factors that influence drivers using a mobile taxi booking system. The researcher uses a digital voice recorder to record the sessions, then converts the recording to text for analysis. The text is qualitatively analysed to find the important themes of the system context.

Verdegem & Verleye (2009) investigate the perceptions of citizens towards e-government services and their actual satisfaction by using a focus group method. They conclude that focus group interviews allow for completing the list of indicators of satisfaction in the study, and help them reformulate some of the indicators, which are important for measurement. The use of focus group interviews makes it possible for researchers to establish the priorities of the respondents.

However, the disadvantages of this method that have been identified include the number of non-attendees, which may be a challenge for the evaluator. Recruiters can over-recruit by 10-25% to avoid this problem. Also, in order to maximise the engagement of participants, the recruiter can inform them in advance about the scheduled date of the interviews and remind them a few days before the meeting to insure their commitment. As an ethical consideration, it is important to notify the participants about their time commitment. In a focus group meeting, the moderator should have a good knowledge of the topic discussed and be well trained in managing and organising interviews (Krueger and Casey, 2014).

4.6.4 Data analysis

Data analysis techniques are used to transform data into information in a meaningful form. There are many techniques and approaches which are used for data analysis in qualitative research. This qualitative study attempts to interpret and understand the trade-off between usability and security from users' perspectives in an e-government setting. There are two techniques identified and applied in HCI research that are applicable to this study, theme analysis and descriptive statistics. This research project uses both data analysis techniques to obtain reliable results that answer the research questions and achieve the research objectives. The focus of this research study is inductive analysis, which is mainly descriptive and exploratory in nature. In the following paragraphs, the data analysis techniques used for the purpose of this study are highlighted and explained.

4.6.5 Theme Analysis

Thematic or theme analysis is one method used by researchers to analyse the complexities of meaning within textual data. This method is used to analyse qualitative studies that seek to understand people's opinions and their meanings (Marvasti, 2018). Theme analysis includes identifying, analysing and reporting themes within the textual data drawn from focus group interviews (Braun and Clarke, 2006). Theme analysis involves coding the collected data in order to extract meaning, then removing redundancy and breaking down the codes into broad themes (Marvasti, 2018). The codes are labelled to help the researcher describe each segment of the text (e.g., participant or context). Braun & Clarke (2006), propose several steps to conducting thematic analysis for qualitative data, as shown in Table 4.1: Phases of theme analysis (Guest, MacQueen and Namey, 2011). These steps are followed in order to identify the main themes that represent the requirements for trade-offs between usability and security in an e-government setting.

Table 4.1: Phases of theme analysis (Guest, MacQueen and Namey, 2011)

Phase	Description of the process
1. Familiarising yourself with your data:	Transcribing data (if necessary), reading and re-reading the data, noting down initial ideas.
2. Generating initial codes:	Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code.
3. Searching for themes:	Collating codes into potential themes, gathering all data relevant to each potential theme.

4. Reviewing themes:	Checking in the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic 'map' of the analysis.
5. Defining and naming themes:	Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells; generating clear definitions and names for each theme.
6. Producing the report:	The final opportunity for analysis. Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis.

This method also has drawbacks, especially if the analysis is poorly conducted. One drawback of this method identified is the inherent flexibility which can lead to a wide range of interpretation resulting from the themes, as well as applying the themes to large amounts of textual data (Guest, MacQueen and Namey, 2012). Additionally, this method is sometimes difficult as it requires concentrating on what features of the data need to be focussed on (Braun and Clarke, 2006).

The data collected from focus group is sorted in a format that is easy to analyse, and MS Excel and Nvivo software are used to record the data. All the themes (patterns) are examined in order to understand the trade-off between usability and security in the e-government context from users' perspectives.

4.6.6 Descriptive Statistics

Descriptive statistics are used in this research project to summarise the data in a meaningful way and describe the data through graphs and tables. Tables are one of the simplest methods of representing data in categories. This method is an exploratory way to understand how the categories of values are distributed inside the sample data. Frequency tables are used to summarise the responses of the participants, including their responses to the questionnaire. Additionally, graphs are used to compare the results of the questionnaire and the focus groups, in the form of column charts. Inferential statistics are also used to observe any differences between groups (McHugh, 2003). Both these techniques are quantitative methods of analysing data (Trochim, 2006). Data analysis techniques used for each sub-study of this research are also explained based on the data analysis requirements of each sub-research, which identifies that a non-parametric analysis test (Mann Whitney test) and Chi-square test are the most applicable analysis method for analysing data in sub-research one, and sub-research two respectively. Statistical analysis of the data was conducted using the Statistical Package for Social Science (SPSS) for Windows (Version 13). The significant value (P) was pre-defined as less than 0.05. Also, data analysis techniques used for each sub-study are explained in detail in each dedicated chapter of each study.

4.7 Participants

The ideal number of participants recommended for a study varies according to author. Nielsen et al. (1990), for example, find that half of major problems can be detected by 3 participants, whereas Virzi (1992) states that 80% of issues can be identified by 4 or 5 participants and 90% of issues can be identified by 10 participants. Dumas et al. (1999) recommends 6 to 12 participants, claiming that additional participants are unlikely to find new issues. The researcher needs to consider their resources such as the research time and budget, and the statistical significance of the results. The total number of participants selected to join the two main studies of this research is 78. Of the 78 total participants, 55 are recruited for the Bitcoin study and 23 for the smartwatch study. The participants are recruited on the university campus via mailing lists and flyers. Most participants are given some incentive described in more detail in each study along with the recruitment process and participant demographics.

4.8 Ethics

It is very important for researchers to adhere to ethical norms of research, in order to minimise any risk of harm. The researcher has ethical clearance and approval from the Keele University Ethical Review Panel to conduct the research as appropriate. The researcher acknowledges the privacy and protection of all participants throughout the research process. There are five recommended key elements to providing ethical protection for the participants in a research study, voluntary participation, informed consent, risk of harm, confidentiality and anonymity (Trochim, 2001). Participants should not be forced to take part in research. The participants in this study are under-graduate students who participate voluntarily. All participants are fully informed of the procedures and whether any risks exist in the research. All participants provide their consent before they participate. The participants are guaranteed to stay anonymous during the course of the study. The researcher assures the anonymity of the study participants by identifying each participant with a P combined with a numeric value, for example P1. The researcher considers these elements throughout the research journey, and the rights of all participants are fulfilled as per the Keele University research ethics standards and regulations.

4.9 Summary and Conclusion

This chapter describes the research methodology used in this study. It identifies and explains the appropriate research strategy employed for each sub-research in this study. To conduct the research study one, a mixed approach with an emphasis on the quantitative aspects is implemented. Study two also implemented a mixed approach focused on qualitative elements. Third study is a critical analysis based on reviewed literatures. Also, quantitative data and qualitative data are collected through, questionnaire and focus group research. In addition, research design for each sub-research study is also identified. Data analysis techniques applied for each sub-study of this research are also explained based on the data analysis requirements of each sub-research and the suggestions from relevant studies, which identifies that a non-parametric analysis (Mann Whitney test) and Chi-square test are the most applicable analysis method for analysing data in sub-research one, and sub-research two respectively.

Chapter 5 Bitcoin Study

This paper investigates users' perceptions and experiences of an anonymous digital payment system (Bitcoin) and its influence on users in terms of usability and security in comparison to other non-anonymous payment systems such as credit/debit cards. This paper identifies users' perceptual differences in terms of usability and security. Two versions of user survey are used to collect data, which reveal significant differences in users' perceptions of credit/debit cards and Bitcoin. The usability attributes of both systems examined show that respondents perceive the usability of credit/debit cards to be higher than Bitcoin. This has a great negative influence on users' security perceptions of Bitcoin. We conclude that Bitcoin, as a crypto-currency, is still in its infancy and requires user education and a new way of thinking. The study recommends developing users' mental models to deepen developers' understanding of anonymous digital payment technology and improve user-centred design. We also make recommendations with respect to e-government services that may be developed relying on crypto-currencies. This study was given a title "User perception of Bitcoin usability and security across novice users" and was published in Elsevier International Journal of Human-Computer Studies on 2019.

5.1 Introduction

Bitcoin is the world's first new decentralised digital currency that depends on a decentralised peer-to-peer network to allow Internet users around the world to transact freely and anonymously without relying on governmental or third-party institutions. Bitcoin experts and researchers report that active Bitcoin users will number almost 5 million and the number of transactions will increase by 50% by the end of 2019 (Bitcoin Stats, 2017). In the last two years, the popularity of Bitcoin has exploded. Its price jumped from nearly 572 U.S. dollars in August 2016 to about 4,700 U.S. dollars in August 2017, resulting in a huge surge in demand worldwide (Bitcoin.org, 2018). Regardless of the mixed opinions about the future of Bitcoin and the extreme volatility of Bitcoin's value over its short history, it has gained many supporters (BusinessInsider, 2018).

Bitcoin has novel features including decentralisation, user anonymity and control, not seen in any previous digital payment systems. These unique features may have a great influence on how users and designers think about all cryptocurrency transactions in the near future (Churchill, 2015). Churchill (2015), in her article in Interaction magazine, emphasises the importance of the underlying structure of Bitcoin (Blockchain) and how such innovative technology could be used widely in sectors other than finance. We found few studies that investigate user perceptions of Bitcoin usability and security. One of these studies investigates the sociological implications related to the emergence of Bitcoin and provides an anthropological opinion on Bitcoin users. The paper discusses user privacy, the role of miners, and the volatility of Bitcoin value (Maurer, Nelms and Swartz, 2013). The characteristics of Bitcoin users and user motivations are studied by analysing Google Trends data (Yelowitz and Wilson, 2015). The study finds that users' interest in using Bitcoin is driven by computer programming and illegal activity but finds no support for political or investment motives. An interesting exploratory study interviewed three groups, end consumers, e-commerce merchants, and Bitcoin exchange employees, with differing levels of skill, to investigate usability, usefulness and subjective norm. The results reveal that most Bitcoin stakeholders perceive ease of use to be low and perceive its usefulness to vary according to group. The study claims that most interviewees agreed that Bitcoin had a promising future as a payment method (Baur et al., 2015). Eskandari, Clark, Barrera, & Stobert (2015) present a first look at the key management of Bitcoin by evaluating the most used Bitcoin wallets. The study concludes that poor usability of key management and malicious exchange causes Bitcoin users to lose money. The study highlights that poor usability and users' lack of knowledge of Bitcoin usage are the main influencers of security breaches. Gao, Clark, & Lindqvist (2015), in their peer-reviewed study, examine adopters and non-adopters' perceptions of the cryptocurrency. The results reveal that both adopters and non-adopters misunderstand how Bitcoin actually works. The study states that people with no experience with Bitcoin find it too hard, or too scary, to use. A comprehensive survey and assessment of existing academic research into Bitcoin indicates that Bitcoin is an exceptional case where practice appears to be ahead of theory. Analysis of the academic research available shows a tremendous opportunity and need for future research into user attitudes and perception of Bitcoin (Bonneau et al., 2015).

Recently, the HCI community has started to explore areas of digital currency and discuss the value of cryptocurrency from users' points of view (Kaye et al., 2014). However, there is limited academic work on user-centred approaches to the exploration of Bitcoin's social aspects, system adoption, user attitudes or behaviours [68], [71],[73]. Some researchers agree that usability is key to increasing Bitcoin usage as a payment system, but there are many other concerns to overcome before that point. Balancing security and usability is one of the biggest challenges for the HCI community [74], [76].

Examination of the available literature shows no studies jointly addressing users' perceptions of Bitcoin usability and security. We found only a few good quality papers in journal level publication venues, with most papers published in symposiums, conferences and workshops. Accordingly, there is a need for good quality journal papers with in-depth analysis with a focus on users' perceptions of Bitcoin usability and security and the trade-off between them.

The objective of this study is to carry out a user study, which not only provides deep insight into how users perceive the usability and security of Bitcoin, but also indicates the level of user interaction with the newly emerged decentralised anonymous digital currency system. This study provides concrete prescriptions for developing user-centred decentralised payment services that can be implemented by government entities. Governments around the world strive to promote their e-services, using the latest technology. Bitcoin, as a promising payment system, offers new approaches for governments by introducing Blockchain technology. Blockchain technology offers fast and cheap transactions, improves transparency, prevents fraud and increases trust among users. This study provides a clear picture of users' attitudes and opinions about Bitcoin to help e-service developers understand end-user perceptions in terms of usability and security.

This study investigates users' perceptions and experiences relating to secure and anonymous systems such as Bitcoin, compared with other current systems such as credit/debit cards. The main goal of this study is to investigate the trade-off between usability and security from a user perspective, in order to understand how users perceive the usability and security of an anonymous payment system. This study seeks a comprehensive understanding of how users interact with the anonymous payment system, what they perceive, and their experience in respect of usability and security. The study focuses on understanding users' requirements from an anonymous payment system and capturing their experiences of the usability and security, compared to credit/debit card users. The analysis of the results increases the knowledge in this field and deepens our understanding of user requirements with respects to usability and security. Additionally, the findings help e-government service designers to design more usable and secure payment systems based on user requirements of anonymous payment system. This research provides developers with a clear view of user opinion that may help in the development of new concepts or standards for e-government services, in terms of usability and security. The study presents a good chance to learn about aspects of Bitcoin which require further focus in order to enhance user satisfaction with applications to novel e-government services based on the use of crypto-currencies. The study also provides a theoretical foundation for academics and practical guidelines for service providers in dealing with the usability and security aspects of decentralised systems.

The paper addresses the following research question: ''*How does a secure and anonymous system such as Bitcoin influence user experience of usability and security compared to a non-anonymous payment system such as credit/debit cards''*?

This paper presents a comprehensive user study of the human computer interaction (HCI) aspects of the anonymous payment system. The goal is to understand users' interactions and capture their experiences in terms of usability and security, in comparison to their experience of the currently most-used non-anonymous payment systems. The research scope is users' perceptions of usability and security trade-off. Perceived novelty is outside this research scope as it is another dimension of the potential predictors of IT innovation adoption that explain how and why individuals adopt an IT innovation (Wells et al., 2010).

5.2 Related Literature

Bitcoin is a new type of currency that does not require any specific governmental authentication. There is a platform for this currency to thrive in the cyber world. Bitcoin is used for 130,000 transactions daily, and $3.5 billion US exists in the current market (Krombholz et al., 2016). According to Bitcoin Stats (2017), daily trading in Bitcoin is around $151 million US. The increase in the volume of Bitcoin trading indicates its growing popularity (Bonneau et al., 2015).

However, Bitcoin has had adverse effects on users. For example, a person lost a hard disk containing Bitcoins worth £4 million in landfill in Newport, UK (Hern, 2013). This leads to the question of whether a digital wallet is more secure than a credit/debit card, where a third party can protect users when money gets lost. Digital currency is legally unregulated, therefore, if the user dies, the currency dies too, as there is no ability to inherit Bitcoin (Yin, Zhang and Wang, 2004). This is a practical downside of using Bitcoin compared to credit/debit cards.

Indeed, both the weaknesses and strengths in the areas of usability and security are derived from the very nature of the encryption of Bitcoin. Thus, it is necessary to explore the concept of Bitcoin as a currency before examining its usability and security aspects (Eskandari, 2015).

The traditional system of transaction via the Internet involves three parties, the payer, the payee and the bank. Hence the perceived security and perceived ease of use come at the cost of the need for service users to trust a third party (Sas and Khairuddin, 2015b). This dependency on a third party has led to an undermining of both security and usability. In terms of security, the third party holds sensitive financial information about both sides, which can be used illegally. In terms of usability, the third party is obliged to follow complicated bureaucratic processes for each international transaction which slows the speed of transactions (Singh et al., 2013). In order to overcome these two issues, e-commerce relies on crypto currency such as Bitcoin (Böhme et al., 2015).

Bitcoin is a unique payment system using crypto currency (Sas and Khairuddin, 2015a). It makes use of encryption techniques in order to regulate the generation of digital currency units and verify funds transferred (Reid and Harrigan, 2013). This process is carried out independently, without the intervention of any bank. The main advantage of Bitcoin crypto currency is that it provides a vent for personal wealth which is beyond confiscation or restriction. It is considered a useful medium of exchange in digital form, secured by cryptography, which not only secures transactions but also controls the generation of currency units.

Bitcoin was established in 2008 by Satoshi Nakamoto. It uses open source software which can be downloaded directly from the Internet. Users require a cell phone, laptop or other electronic medium to download the software and make transactions as Bitcoins are connected to particular IP addresses (Mainelli and Smith, 2015). It is a peer-to-peer transaction medium (Bamert et al., 2013). Each transaction made with Bitcoin is verified at the network nodes and documented in Blockchain, which is a publicly distributed ledger (Moser, Bohme and Breuker, 2013). As there is no bank or other third party needed to carry out the transaction it is a decentralised system, unlike other payment or monetary systems which are centralised under the authority of banks (Kornmesser, 2008).

5.2.1 Rethinking government e-services

Governments around the world are adopting and implementing the latest information computer technology (ICT) in order to provide a wide range of services to citizens (Kotamraju and Van Der Geest, 2012). Recently, many governments have changed from traditional service delivery platforms to electronic platforms which allow users to take on new roles in the delivery of services. The transactional journey of the government-citizen relationship needs to focus on easy-to-use interface design, which is critical to the successful adoption and use of applications (de Jong and Lentz, 2006; Rohnke and Yahner, 2008). Such services aim to enhance the accessibility of services, while reducing the cost of delivery and the delay. However, these benefits cannot be obtained without continued monitoring of the e-government services to identify the benefit to the end user (Papadomichelaki & Mentzas, 2012; Aichholzer, 2009).

The effectiveness of e-government implementation is challenged in the literature. Ruba, Hartmut, & Viswanath, 2014 contend that there is lack of citizen-centric design in many e-government services, resulting in the under-utilisation of e-government initiatives. Additionally, since there is a great deal of sensitivity and a need for confidentiality of information in the e-government framework, it is imperative to ensure security and protection. As Choi, Ae Chun, & Cho, 2014 argue, security and trusted information should be key issues that are adopted in order to prevent unauthorised disclosure or leakage of secret information.

Lesemann, Woletz, & Koerber, 2007 say that usability issues need to be examined in the design of new functions and services on any platform, to ensure an enjoyable user experience. Alberto, 2010 presents an excellent conclusion to the need for usability and security, claiming that IT-enabled service interactions must meet users' expectations. Therefore, e-government services must be designed based on users' backgrounds, levels of knowledge, skills and contexts of use in order for there to be satisfactory services (Sousa, Smeets and Brenner, 2012).

There have recently been government efforts to adopt a new revolutionary emerging technology that offers fast, secure, efficient and transparent services. This emerging technology is Blockchain, a collaborative technology with a great ability to improve online government services. Blockchain and its underlying technology presents opportunities for all kinds of public services to provide tools that cut errors, reduce costs, increase security, avoid fraud and enhance productivity. This promising technology could revolutionise the way citizens interact and transact with e-government over the Internet. Blockchain technology opens doors for many potential applications including tax collection, identity management, local (or national) digital currencies, property and land registry, and other government records (Boucher, Nascimento and Kritikos, 2017).

Government experts have found that Blockchain technology brings many benefits and contributes to the development of many aspects of public service. Countries including Estonia, Georgia, India, France and Dubai are competing to introduce Blockchain technology to their governmental applications. Estonia for example, has been testing the technology since 2008, and in 2012 started to use Blockchain technology in a number of government activities such as national health registries and judicial services (Mainelli and Smith, 2015). Dubai Land Department has announced on October 2017, that it is the world's first government entity to adopt the Blockchain technology to its operations (Law, 2017).

However, the development of Blockchain technology has both opportunities and risks. It can change the way e-services for citizens are delivered and managed, but the lack of mature Blockchain applications in other fields is a problem. Therefore, we need a more thorough understanding of citizens' needs and expectations about such technologies, in terms of usability and security (Boucher, Nascimento and Kritikos, 2017).

5.2.2 Current payment systems and Bitcoin

The use of debit and credit cards has increased significantly, but it involves a third party, a bank, to authenticate each transaction. The method of transaction using debit/credit cards involves a series of authentication steps (Goldfeder, Felten and Kroll, 2015). Authentication processes occur between the service user, or payer, and the bank, between the merchant, or receiver, and the bank, and between the payer and the receiver.

According to Plassaras, 2013, online transactions are mainly completed using debit/credit cards. This involves the service user sending details of their card over the Internet to be accessed by the bank. The majority of customers who perform transactions online are worried about hacking or their personal details being used by unauthorised personnel. The involvement of a third party for a successful transaction undermines the security of the transaction process and makes it more cumbersome (Herrera-joancomart, 2015).

Bitcoin, on the other hand, is less cumbersome as the transaction is carried out directly between users with no involvement of a third party or external agency (Garcia-Alfaro et al., 2015). According to its founder, (Kornmesser, 2008), Bitcoin gained immense popularity due to its high level of perceived security.

5.2.3 User perception of Bitcoin usability

The Bitcoin payment system has various advantages over other payment systems such as payment by credit/debit cards, as reported by Sas & Khairuddin (2015), who undertook an exploratory study collecting data from nine interviewees about their motivation for using Bitcoin. They indicated that the most important characteristic is its decentralisation as a method of payment, and the entire process not being controlled by a single authority. Each of the machines that process transactions and mine coins work together to form a network. Hence, no monetary policy can be decided on. According to Wankmueller (2005), conventional payment systems involve opening bank accounts, and there is a need for a merchant account which makes the system expensive. In the Bitcoin system, users can set up a Bitcoin address in seconds and no money is charged (Barber et al., 2012).

Bitcoin users can set up more than one Bitcoin address. The most advantageous usability element of Bitcoin is that the payment system is transparent. It stores each detail of a transaction within a network across the Internet. The details are stored in a form of general ledger known as the Blockchain. Anyone can detect the number of Bitcoins available at a particular Bitcoin address, however they are not able to detect who the Bitcoins belong to (Fine, 1998). Users can take appropriate measures to ensure the activities they perform are opaque. According to Miers, Garman, Green, and Rubin (Miers et al., 2013), users should use various Bitcoin addresses rather than using the same address consistently, and not transfer large numbers of Bitcoin to a single address.

Androulaki (Yelowitz et al., 2015), observe that merchants are charged an amount for each debit/credit card transaction, which is a significant cost to a company. Customers who make payment via these cards are also bound to pay certain charges for using the services of a bank. This sometimes dissatisfies customers despite the ease of making a transaction not in cash. Transactions carried out internationally via the card system have significantly increased transaction charges, which makes merchants dissatisfied. In contrast, Bitcoin has no such transaction charges. Any transaction between users, whether overseas or within the same country, is not subject to any charges, and the number of transactions that can be made per day is not limited. The major disadvantage of debit/credit card payment is that the money transferred might take as long as two days. However, the biggest difficulty faced by users of Bitcoin is that Bitcoins are non-refundable. According to Luther and Olson (Luther and Olson, 2013) , once Bitcoins are sent to the recipient they are gone from the transferee forever and are not refundable. On the other hand, payments made via card do not have this limitation. The money transferred is refundable and reaches the payer within a couple of days. The payer can also terminate a credit/debit card transaction (Moser, Bohme and Breuker, 2013)

Among the various clients of Bitcoin (i.e. full clients, headers-only clients, signing-only clients, thin clients, and mining clients) questions of usability do exist. Absolute trust is demanded of the provider of the eWallet for two reasons; they know the history of the user and monitor the users' Bitcoin. There is no overt process to assure the user that the eWallet provider has the sum that appears as their balance supported by reserved Bitcoin (Ben-Sasson et al., 2014). The eWallet provider can also become a victim due to theft, loss or malicious takeover of Bitcoin, leading to a loss of funds for the customers (Donalek et al., 2008). Nonetheless, usability is buttressed through QR codes, Bitcoin URIs, deterministic wallets and brain wallets. By applying theses digital services, the experience and attitude of Bitcoin users about the usability of Bitcoin could become similar to traditional credit/debit cards (Meiklejohn et al., 2016).

Recent studies show that the Bitcoin system is complex to use and there are misconceptions about how it works (Sas and Khairuddin, 2015a; Gao, Clark and Lindqvist, 2016). This may affect users' perceptions of the Bitcoin payment system in comparison to other payment systems (Baur et al., 2015; Yelowitz and Wilson, 2015; Khairuddin et al., 2016). Learnability is the most important usability attribute (Cameron, 2007). Any system should be easy to learn so that the user can rapidly accomplish basic tasks, first time, using the system. Learnability is considered an important usability aspect for novice users who may be put off using the system if it is not easy to learn (Dzida, Herda and Itzfeldt, 1978). Evidence from recent studies shows that ease of learning perception has a significant effect on user attitudes to e-payment systems and the likelihood of errors. The system is considered more efficient and effective if the user is able to accomplish tasks or transactions with speed and simplicity.

Some researchers compare Bitcoin wallet interfaces and find serious issues in terms of complexity and lack of help (Skudnov, 2012; Simpson, 2014). Other studies state that there are concerns about Bitcoin transaction speeds, with the average time needed to confirm transactions being about 25 minutes (Bonneau et al., 2015; Athey et al., 2016). The time taken to confirm transactions delays the operation of selling and buying, while credit/debit card transactions are confirmed in less time (Barber et al., 2012; Skudnov, 2012; Singh et al., 2013; Garcia-Alfaro et al., 2015). Nielsen, 2012 states that if the delay time is longer than ten seconds, users switch to other faster alternatives or applications. The literature review shows some evidence of memorability concerns for users related to Bitcoin addresses and login IDs for Bitcoin clients, which are worse than computer-generated IDs. Users find it hard to remember these login IDs and addresses (Barber et al., 2012; Skudnov, 2012; Luther and Olson, 2013). Accordingly, users might find less memorability attributes in Bitcoin payment systems than credit cards. Obviously, Bitcoin transactions cannot be reversed, and access can't be restored. Therefore, a mistaken Bitcoin transaction or a lost credential results in a loss of user funds (Singh et al., 2013; Böhme et al., 2015). Thus, the user might perceive more unrecoverable errors with Bitcoin than credit/debit cards. Bitcoin, as an emerging complex technology, is not yet systematically explored and the information available is insufficient to give users a full picture of how it works. A few studies indicate an absence of complete or reliable information about most Bitcoin exchanges and Bitcoin clients (Böhme et al., 2015; Goldfeder, Felten and Kroll, 2015; Khairuddin et al., 2016; Eskandari et al., 2018). Users need access to a help system in any application in order to learn the system functions and features.

User satisfaction is another important dimension of usability. Research shows that the overall impression and experience of users is influenced by other usability attributes such as learnability, efficiency, help and errors. These usability attributes affect the overall user satisfaction of the system studied.

The usability attributes mentioned in the literature should be assessed as a whole subset, unless domain specific studies suggest otherwise. Studying all these attributes gives a sufficient indicator of the overall usability of the studied system rather than assessing one or two aspects that may lead to unreliable conclusions about overall usability.

5.2.4 User perception of Bitcoin security

Bitcoins are considered pseudonymous (Reid and Harrigan, 2013), which means that the funds are not associated with real-world identities but Bitcoin IP addresses (Koshy, Koshy and McDaniel, 2014). The Bitcoin users who are supposedly the owners of the Bitcoin addresses cannot be identified explicitly, but the transactions they make are recorded in the Blockchain which is public (Campbell-Verduyn, 2017). Other users can see the number of Bitcoins that are transferred or received by a single Bitcoin address but are unable to identify who the owner is (Mainelli and Smith, 2015). Transactions can be linked by observing the times and types of transaction. If it can be observed that a transaction includes coins from various inputs, there is a common owner to those inputs (Sas and Khairuddin, 2015a). According to Reid and Harrigan (2013), when Bitcoins are traded for traditional currencies, it is important that the personal information of the owner is collected, and that this is compulsory under the law of the relevant country. In order to increase financial privacy, owners can generate new addresses for each Bitcoin transaction (Yin, Zhang and Wang, 2004). Each transaction requires a single passphrase, which could help in tracking all transactions made by a single owner (Garcia-Alfaro et al., 2015). This helps in securing the user's identity as the public is unable to identify which transactions are made. As the identity or any personal information is not accessed by any third-party agent, such as a bank, and information is not stored on servers, there is no possibility of hackers accessing the personal information of Bitcoin users or making fraudulent transactions. According to Androulaki et al. (2013), the use of debit/credit cards over the Internet poses a significant threat for users. Hackers can hack security passwords or access PIN numbers, and make illegal transactions (Krombholz et al., 2016). Users often experience or perceive a lack of privacy and confidentiality in transaction information, and are therefore afraid of making online transactions (currency and 2015, 2013).

Security is considered a significant barrier for online users and can have a great influence on the use of online applications. Generally, user confidence in technology is greatly weakened if that technology is not supported by an accredited organisation or legal authority. Therefore, security could be a determinant of users' decisions to use e-payment systems. With Bitcoin currency being a novel decentralised digital currency, and having some legality concerns, users might be less able to use protection effectively (Coutu, 2014; Gao, Clark and Lindqvist, 2016). Also, poor usability of security functions and features may put the security of the system at risk. This can lead to a misconception among users that security is not important for them and they can ignore or try to bypass it (Braz, Seffah and M'Raihi, 2007). Some researchers, and standards organisations, identify other viewpoints on usability, and include security as a characteristic of usability (Rinaudo, 2018). Lack of usability and system complexity may cause security exposure directly and make users avoid the issue by bypassing the security mechanisms, even when the intention is to comply with the security mechanism.

The literature indicates that Bitcoin has earned immense popularity from 2008 over credit and debit cards due to the higher privacy offered by Bitcoin wallets. Due to the very nature of Bitcoin as an encrypted currency, it eliminates third party involvement. There is no need for the authentication steps imposed by governments or mathematical processes which can be manipulated illegally.

5.2.5 Summary

As this field is brand new (since 2008), this study is unique. It aims to explore the attitudes and opinions of users related to security and usability aspects and pave the way for better ways of increasing end user perception of the usability and security of Bitcoin.

To the best of our knowledge, there has not been any empirical research comparing anonymous and non-anonymous payment systems. With this paper, we contribute to the HCI field by means of an exploratory, mixed qualitative and quantitative approach using survey questionnaires. This study helps narrow the gap in research by investigating Bitcoin users' perceptions of usability and security and recommending appropriate guidelines to help developers understand Bitcoin users' need.

The findings help significant aspects of usability and security to be identified so that appropriate guidelines can be formulated to support and promote the use of Bitcoin payment systems. Furthermore, the results contribute to e-governments, banking institutions, online transaction providers, and developers by uncovering Bitcoin users' concerns and views about using Bitcoin payment systems, thereby enabling them improve systems based on user requirements.

5.3 Methodology

This paper aims to present a comprehensive user study covering the human computer interaction (HCI) aspects of the Bitcoin payment system. It examines novice smartphone users' perceptions and experiences of an anonymous, secure, digital payment system (Bitcoin) in comparison to the most used payment system (credit/debit cards), bringing insight into user experience of Bitcoin in terms of usability and security. The findings of the survey are important and contribute to HCI community understanding of how users experience, and feel about, the usability and security aspects of crypto-currency digital payment systems. Before we describe the methodology, we must outline the research hypotheses. The hypotheses, shown in Table 5.1: Research Hypotheses below, are based on the research questions and the usability guidelines of Nielsen (Nielsen, 1992). They explore users' perceptions of the Bitcoin payment system environment. To ascertain high level opinions, we designed two online survey questionnaires to compare users' perceptions of anonymous and non-anonymous payment systems. We explored the usability and security features which could influence users' perceptions. This allowed us to compare users' opinions of anonymous and non-anonymous systems in terms of the usability and security aspects. Evidence from previous studies specifies that usability is a key element in determining system or service quality (Hornbæk and Law, 2007b; Johnson and Willey, 2011; Leon et al., 2012), and ensuring user engagement. Usability can directly impact users' perceptions, opinions and attitudes (Lee and Koubek, 2010). To understand how users perceive usability in an anonymous payment system, five usability attributes are included in the hypotheses which assess and capture user experience and opinion. These usability attributes are learnability, memorability, efficiency, error and help. In order to keep the hypotheses simple, we assume there is no difference between user attitudes towards Bitcoin use and the use of credit/debit cards. Then we explore the extent to which these default hypotheses are valid. The hypotheses are as follows.

Table 5.1: Research Hypotheses

#	Research Hypothesis
H1	*Bitcoin and credit/debit card users perceive no difference in term of learnability.*
H2	*Bitcoin and credit/debit card users perceive no difference in term of efficiency (speed, accuracy, micropayments).*
H3	*Bitcoin and credit/debit card users perceive no difference in term of memorability (used occasionally).*
H4	*Bitcoin and credit/debit card users perceive no difference in term of error and recoverability.*
H5	*Bitcoin and credit/debit card users perceive no difference in term of help and documentation.*
H6	*Bitcoin and credit/debit card users perceive no difference in term of security.*
H7	*Bitcoin and credit/debit card users perceive no difference in term of satisfaction.*

To accomplish the study objectives, two versions of a survey were designed to capture smartphone users' insights and experiences of each payment system. Both surveys were conducted online, separately, between January and March 2017. This technique is in line with previous studies of usability and security practices (Abrazhevich, 2004; Braz, Seffah and M'Raihi, 2007; Ben-Asher et al., 2009; Kainda, Flechais and Roscoe, 2010). There are several methods for testing usability, the most common being thinking aloud, field observation and questionnaire. These methods offer direct information about how people use systems and determine the exact problems with a specific interface. The first commonly used method is thinking aloud (THA) which is a most valuable usability engineering method. It involves the end user continuously verbally expressing his thoughts while using the system (Virzi, Sorce and Herbert, 1993; van den Haak, De Jong and Jan Schellens, 2003). This method enables system designers to understand how users see the system, which helps them recognise the end users' misconceptions. The method has some disadvantages; sometimes participants perceive it as unnatural, distracting and strenuous. Some participants have issues expressing or explaining their actions. It is also time-consuming, as meeting and briefing the participant is an essential part of the preparation (Riihiaho, 2017). Another important and widely used method is field observation. This is much simpler than the other methods. It requires the researcher to visit one or more users in their places of work and take notes without interfering. In some circumstances, researchers use video recording for field observation to avoid user disturbance and make observation less obtrusive (Holzinger, 2005). Figure 3 shows a comparison of usability testing methods based on criteria such as time required, number of users needed, and resources required to run the evaluation.

	Inspection Methods			Test Methods		
	Heuristic Evaluation	Cognitive Walkthrough	Action Analysis	Thinking Aloud	Field Observation	Questionnaires
Applicably in Phase	all	all	design	design	final testing	all
Required Time	low	medium	high	high	medium	low
Needed Users	none	none	none	3+	20+	30+
Required Evaluators	3+	3+	1-2	1	1+	1
Required Equipment	low	low	low	high	medium	low
Required Expertise	medium	high	high	medium	high	low
Intrusive	no	no	no	yes	yes	no

Comparison of Usability Evaluation Techniques

Figure 2: Comparison of usability evaluation techniques (Holzinger, 2005)

Questionnaire is also a widely used and a very useful method of collecting data for scientific research (Zaharias and Poylymenakou, 2009). It is a very flexible method, extensively used to identify respondents' opinions, judgments and preferences. Questionnaires bring the participants' attention directly to the research topic and enable them to clearly focus. Using a questionnaire can get participants' responses very quickly and deliver the same questions to each participant. It encourages respondents to offer truthful replies, especially when talking about controversial issues, as questionnaires offer more anonymity than other evaluation methods (Tashakkori and Teddlie, 1998). A questionnaire is also an efficient and manageable method, which is cheap and takes less time than other methods (Root and Draper, 1983). Thus, the questionnaire is an appropriate method to gather data related to users' perceptions of usability and security of the e-government payment system for this study. Also, with the THA and field observation techniques, the data collection and analysis are time consuming and the outcomes can be misinterpreted by the researcher, leading to unclear patterns in the analysed data at the end of the research process (Wahyuni, 2012). The researcher needs to consider the availability of resources such as time and budget.

5.3.1 Survey design

The survey questionnaire is designed based on the usability and security criteria derived from the literature (Nielsen, 1993; Wich and Kramer, 2015; Coursaris and Kim, 2006), and usability and security related questionnaires from previous surveys (Lewis, 1995; Venkatesh, Hoehle and Aljafari, 2014). The findings from the literature review are used to identify which usability and security features capture users' perceptions when they interact with payment systems. Both surveys explore user experience with an emphasis on the usability and security features of each payment system. Nielsen's usability guidelines (Nielsen, 1995; Cameron, 2007), and ISO security standards (Candiwan, Beninda and Priyadi, 2016), are used widely, and their practicality has been proved by a number of studies. Since a number of scholars have proved the validity of these guidelines for capturing users' perceptions of usability and security, we extend and redesign the guidelines to fit the specifics of the systems reviewed, with a detailed emphasis on the aspects of usability and security. The questions in both surveys are designed based on these guidelines. There are slight differences in the survey design of each questionnaire to tailor them to each payment system. The questions used in the Bitcoin survey form the basis of the usability and security questionnaire in the credit and debit card survey. The usability feature questions are designed based on Nielsen's usability guidelines (Nielsen, 1995). Usability is divided into five sub-categories, learnability, memorability, efficiency, error and help, to give a broad view of the usability of the systems reviewed and make later evaluation easier. Security survey questions are designed to capture users' experiences of the security features based on the available functions of the systems reviewed with an emphasis on authentication, confidentiality, integrity, backup and storage. The security survey questions are not divided into sections like the usability survey. Our intention is not to underestimate the security aspect, as it is an important feature of usability. The design of the security questionnaire covers and measures three main elements, authentication, confidentiality and integrity. There are other elements of any e-payment system, therefore we try to make it simple for average users to evaluate the security aspect. Also, the procedures in e-payment (e-wallet) are totally different from those in the traditional payment system (debit/credit card) because the transaction processes are different. Therefore, we design a security questionnaire to fit with both systems. The guidelines are too broad to develop usability and security questions in the questionnaire, so we extend them in consideration of the tested systems and users in order to have in depth evaluation of the tested systems. Satisfaction is the third and final section of each survey, designed to measure the general satisfaction of the participants. Both surveys are designed with both closed and open-ended questions.

In both surveys participants are asked to respond on a five-point Likert scale, indicating their level of agreement with statements (strongly agree = 5; strongly disagree = 1). An odd number of responses allows for a neutral answer (neither agree nor disagree) in the middle, so the respondents don't have to select a positive (agree) or negative (disagree) option. The quantitative results obtained from the five-point Likert scale can be easily collected and statistically analyzed. Both surveys were piloted and non-author respondents went through the usability and security questionnaires.

This study went through a standard ethical review process at Keele University (Research Ethics Committee's approval number ERP1289). Two different sets of recruiting material and screening questionnaire were created for the two versions of the survey. The procedures and recruitment processes for each survey are described in detail in the next sections.

5.3.2 Bitcoin survey

Survey participants were limited to undergraduate students studying at Keele University, over the age of 18, with a smartphone, with basic knowledge of using Bitcoin digital currency, willing to participate in the study. In the first part of the study, participants were recruited on the university campus via mailing lists and flyers in January 2017. An invitation email was sent to candidates along with a pre-survey questionnaire and consent form. In the pre-survey questionnaire, we asked the participants to rate themselves on their knowledge of cryptocurrencies. This was done in order to select participants who had basic or no knowledge of Bitcoin currency, as the study objective is to capture novice users' perceptions. The invitation email explicitly stated that we were conducting a study on digital currency and payment systems and were interested in candidates willing to experience crypto-currency payment systems and undertake tasks using their smartphones. Candidates were made aware that an allocated amount of Bitcoin currency would be transferred to them (0.040 Bitcoin ≈ £35 at that time) to use after successfully completing the assigned tasks. Interested candidates were asked to fill in a pre-survey questionnaire to help us select appropriate candidates based on predetermined criteria. The pre-survey questionnaire was designed to collect demographic information such as age, gender, education level, and familiarity with Bitcoin clients (wallets) and smartphones. The screening survey was successfully completed by 27 students, and 25 candidates were selected to proceed with the study based on the study criteria. Three of the participants were later withdrawn from the study because of legality concerns about Bitcoin in the UK.

In stage two of the Bitcoin survey, 22 participants were asked to perform a set of practical tasks on the Bitcoin eWallet, typical of those users need to carry out to transact with Bitcoin. The goal was to allow respondents to perform tasks in a real-life context to give them the freedom of an uncontrolled environment and increase their understanding of Bitcoin. This would indicate the user's level of interaction with the system and give insight into the participant's perception of usability and security. The tasks were appropriate for the participants to perform in the study. Time and task length were considered, and a clear description given by the researchers in order to avoid any misunderstanding or misinterpretation. All the tasks were thoroughly checked and pre-tested in a pilot study.

To complete the tasks, the candidates were advised to use Blockchain.info as the hosted wallet provider and to watch the tutorial video before starting the tasks. The choice of this hosted wallet was due to the popularity of Blockchain.info and it is accessibility from various smart mobile devices. Blockchain.info is one of the most used mobile Bitcoin applications that do not require much storage, network bandwidth or computing power. It is one of the leading Bitcoin eWallets, providing end-to-end encryption for users, allowing them to experience secure transactions with greater privacy and less third party surveillance, protecting their keys and Bitcoins from sniffers (Eskandari et al., 2018).

All the participants received task sheets by email and were instructed to do the tasks and send them back to the researcher in order to fulfil the survey objectives. All the tasks were carefully checked and pre-tested in the pilot study. The tasks assigned to participants were:

T1: Configure a new Bitcoin account: participants had to navigate to the Blockchain.info site and set up a new wallet by providing an email address.

T2: After successfully configuring the wallet and obtaining a wallet ID, the participants had to create a new Bitcoin receiving address and write it down carefully on the task sheet. A Bitcoin receiving address can be shared with others to receive Bitcoin directly to a wallet. The Bitcoin receiving address changes with every payment.

T3: The third task was locating and setting up auto logout options, to automatically log out of their wallet after five minutes of inactivity and write the steps on the tasks sheet. This task was given to participants to allow them to experience one of the security features.

T4: Participants were asked in the fourth task to change their login passwords and write the steps on the task sheet.

T5: Participants were asked to get their backup recovery phrase, check the online help available with this task, and write the steps on the task sheet. The recovery phrase can be used to restore all unused Bitcoins in the case of a lost password or a loss of service at Blockchain. The recovery phrase never changes and recovers all existing Bitcoins and newly received funds in the wallet. Participants were asked to comment on the number of words (phrases) generated automatically when conducting this step without mentioning or writing the phrases on the task sheet.

T6: Participants were advised to navigate Blockchain.info, experience the features and functions available to users and comment on their overall experience and what they most liked and disliked about using Bitcoin, clarifying their responses.

Participants were asked to return the filled in task sheets to the researcher, after double checking their receiving Bitcoin address. Participants were also advised to contact the researcher if they needed any help with the tasks.

All participants were given one week to do the tasks and return the sheets to the researcher. After they had successfully completed the tasks, the researcher sent 0.040 Bitcoin (≈ £35) to each participant who provided a valid Bitcoin address. When all the participants confirmed that they had received the Bitcoins in their wallets, they were advised to use this amount to buy any online items they wanted. The participants were given the freedom to use this amount of Bitcoins in any online store accepting Bitcoin digital money, transfer it to friend or withdraw cash from any available Bitcoin cash machine. A map of all Bitcoin cash machines was sent to the participants. This was important to ensure that the participants felt in control of their experience when transacting with Bitcoin digital money in a real environment and kept researcher interference to a minimum. Nielsen (1992) recommends observing how users interact with systems in their natural environments and giving them the freedom to experience the system without any interference.

In Stage three of the Bitcoin survey, the 22 participants who successfully completed Bitcoin tasks were invited to fill out a web-based survey questionnaire hosted by Survey Monkey (www.surveymonkey.com). This consisted of closed and open-ended questions in three sections, usability, security and satisfaction. Usability was further divided into five aspects based on Nielsen's usability guidelines (Cameron, 2007), learnability, memorability, efficiency, error and help. Each section of the survey was designed to capture the participants' views of Bitcoin use in terms of usability and security. Each section of the survey consisted of sets of questions that captured the end users' views of the Bitcoin client. The Blockchain.info client wallet was revised based on its capability and used as inspiration for the design of the survey questionnaire, with an emphasis on usability and security features as shown in Appendix A.

5.3.3 Credit and Debit Card Survey

The credit/debit card questionnaire was distributed online using Survey Monkey (www.surveymonkey.com). Keele University undergraduate students were contacted using internal e-mail and flyers. The invitation email explicitly stated that the participants needed to be over the age of 18, have a debit or credit card and had used a smart mobile phone to purchase items online with the credit/debit card in the last six months. Participants were offered entry into a draw for a £30 gift voucher in return for filling in and submitting the survey.

The study included 33 undergraduate students, who are over the age of 18 and had used debit/credit card in the last six months. The questions were revised and reviewed by the authors to improve the construct validity. The participants were asked the extent to which they agreed with various statements, each one scored on a five-point Likert scale (1 = strongly disagree; 2 = disagree; 3 = neutral; 4 = agree; and 5 = strongly agree). The five-point Likert scale has become the norm in much research work because it offers sufficient choice and is easy to respond to. However, research has confirmed that more than five points in a Likert scale confuses respondents.

The questionnaire contained a few nominally scaled background questions. These questions sought information on demographics, smartphone use, and online purchases. The survey investigated the respondents' previous experiences and perceptions of using credit/debit cards in terms of usability and security. The survey was divided into three main sections, usability, security and satisfaction. The usability section was further divided into five sub-categories, learnability, memorability, efficiency, error, and help, as with the Bitcoin survey. Each section was designed to capture the participants' opinions about credit/debit card features and capabilities. Each section of the survey questionnaire assessed, in depth, with the emphasis on the features that may influence users' perceptions of usability and security as shown in Appendix B. These questions were carefully designed based on the credit/debit card features available that can help us to capture the participants' experiences and opinions and how they perceived the usability-security trade-off.

5.4 Data Analysis

The reliability of the questionnaire design was verified by Cronbach's alpha (overall=.876; learnability=.857; efficiency=.847; error=.875; memorability=.844;

help=.852; security=.868; satisfaction=.860). The reliability test confirmed that the questionnaire design had satisfactory reliability with a Cronbach's alpha above 0.7.

The data from the questionnaires was processed and analysed statistically, using a non-parametric analysis (Mann Whitney test) as suggested by Siegel (1956) to compare the views and opinions of the two groups (credit/debit card users versus Bitcoin users). This test is useful for a small sample size where the data are not normally distributed. The Mann-Whitney U-test does not make any assumptions related to the distribution. The logic behind the Mann-Whitney U-test is to rank the data for each situation, and examine the differences of the two rank totals (Gibbon, 1985).

Effect size was used to identify precisely how large the effects in the data really were. Effect size is a way of quantifying the size of the difference between two groups. Cohen's effect size estimates were used to interpret the meaning of the ''r'' score in the data. Cohen classifies of effect size as 0.1 (small effect), 0.3 (moderate effect) and 0.5 or above (large effect) (Coín-Mejías et al., 2007).

To indicate whether the two systems had a difference in overall perception of usability and security, the Mann Whitney U-test was conducted with the two payment systems as independent variables and usability and security perception as dependent variables.

Statistical analysis of the data was conducted using the Statistical Package for Social Science (SPSS) for Windows (Version 13). The significant value (P) was pre-defined as less than 0.05.

5.5 Results

5.5.1 Demographics

The total sample size participating in the Bitcoin study, after filtering, was 22 participants. Of these, 78% claimed to be male, 22% claimed to be female. Their ages ranged from 19 to 35. About 76% of the participants reported being in their 1st or 2nd year of university; 24% stated they were in their last year.

The participants were asked to report on their use of Bitcoin after watching the introductory video: 66% of respondents reported that they would use Bitcoin to buy goods and services; 14% of participants would use it for investing in crypto-currency; 6% reported they would use it to mine Bitcoin; and 20% of participants would use Bitcoin for all the reasons mentioned above.

The participants were also asked to state what things would encourage them to use Bitcoin: anonymity and no transaction fees were chosen by 66.5% of respondents; ease of use was chosen by 23% of respondents; 10.5% of respondents chose all three reasons mentioned above.

The participants described themselves as experienced and regular smartphone users: 67.7% had used smartphones for more than two years; 32.3% for more than three years; 81.41% spent at least two hours per day on smartphones; and 18.59% spent four hours or more per day.

The credit/debit card survey was completed by 33 undergraduate students, all of whom had no specific technical background in credit/debit cards but had used them before. Of these, 9 participants reported to be female (27%), and 73% (24) to be male. Ages ranged from 19 to 35. Of the participants, 58% claimed to be in their last year in university and 42% in their 1st and 2nd year. 92% of the participants described themselves as regular smartphone users; 79% had used smartphones for more than two years and the rest for more than three years; 83% spent at least two hours per day; and 53% spent more than four hours a day. The respondents were asked how many times they had used credit/debit cards online in the previous six months. About 63% of the respondents claimed to have used them two times a week; 18% reported that they had used them once every two weeks; and 9% reported that they used them once every month.

5.5.2 Task results

T1: In this task, all 22 participants were able to navigate the Blockchain.info site and successfully complete the task of creating a new Bitcoin wallet by providing an email address and a 10-character password. On the task sheets, all respondents successfully provided the correct steps. Most of the participants commented that the steps for configuring a new Bitcoin wallet were simple and straightforward.

T2: This task was about obtaining a Bitcoin receiving address and writing it down on the task sheet. The sheets showed that 72.7% (16) of the participants successfully managed to create a new Bitcoin address; 9 participants rated this task as difficult, and surprisingly 6 of the respondents failed to find the Bitcoin receiving address. The task sheet shows that those participants confused between the wallet ID and Bitcoin address. Later those (6) participants received some assistance from researcher and were successfully able to obtain the Bitcoin address required to proceed with the study.

T3: This task was about experiencing one of the security functions (auto logout) offered by the Bitcoin wallet. Almost half the participants (45.5%) were unable to locate this important function; 10 participants were confused and had problems finding the auto logout function. Only 12 (54.5%) of the 22 participants successfully got the right steps.

T4: The fourth task was changing the login password: 95% (21) of the participants successfully did the task and set a new login password for their Bitcoin wallet; only 1 participant was unable to change his login password and was confused by the second password offered by the wallet for extra security when sending Bitcoin or transacting.

T5: This task was about backing up the recovery phrase in the Bitcoin wallet in case of a lost password: 81.8% (18) of the participants were able to perform this task and set up the recovery phrase for their Bitcoin wallet; only 4 participants failed to set up a new back-up recovery phrase. The task sheets showed that 4 participants were not sure how to do the task and some confused backing up their wallet with authentication of passwords.

Table 5.2: Tasks Completion Rate

Task	*Completed (%)*	*Completed with assistance (%)*	*Failed (%)*	*Rated task as difficult (%)*
T1	*100%*	*0%*	*0%*	*8%*
T2	*73.9%*	*26.1%*	*26.1%*	*41%*
T3	*53%*	*0%*	*47%*	*50%*
T4	*95%*	*0%*	*5%*	*5%*
T5	*82%*	*0%*	*19%*	*28%*

T6: This was not a core task that participants had to perform, it was optional. They were advised to go through the Bitcoin wallet and experience the security features offered along with the other useful functions, and comment on what things they most liked and disliked about the Bitcoin wallet. Some of the positive comments from 18 of the participants were:

A. Offers advanced authentication features, such as 2-step verification.
B. Balance can be shown in user local currency.
C. Can automatically be set to auto-generate a new wallet address after each transaction.
D. QR code can help pair the web wallet with a mobile device scanning and using it to share addresses to avoid having to type them.

On the other hand, there were some negative comments that were considered very significant from the participants' perspectives:

E. 9 of the participants stated that the wallet ID, used to log in to the wallet, was a very long and unmemorable phrase. A wallet ID contains numbers, letters and dashes, is used only to log into the wallet, and should be kept private. The wallet ID can only be found in the welcome email.
F. 4 of the participants claimed that they faced some technical error messages when trying to send Bitcoin that were not understandable; for example, 'no free outputs to spend' was displayed when transactions were created without sufficient Bitcoins. Also, the participants mentioned that there was no available option to recover coins sent to the wrong address.
G. Participants reported that they couldn't buy Bitcoins by credit/debit card if the purchase amount was more than £200. They had to verify their identity before buying any Bitcoin valued over £200.
H. Participants also claimed that authentication processes were too long and complicated.

To gain a preliminary thought on users' perceptions of Bitcoin usability and security, the data from task ''6'' is coded thematically, using standard qualitative analysis techniques and analyzed using a form of content analysis to extract the main themes from participants" comments. Based on these comments, we found that Security Authentication and usability efficiency perception are most frequently acknowledged by participants about the Bitcoin payment system. Participants expressed their appreciation of the 2-step verification method provided by the Bitcoin wallet. Implementing more than one step verifications increase users trust and reduce users' perception of risk. One of the participants said "2 step verification adds extra security when sign-in and you feel more protected - honestly, it's only an extra click" another participant stated, "It will be harder for anyone else trying to access my wallet". On the other hand, some participants claimed that authentication methods and long login IDs and special password characters require more work on the user's part, and it's another pain point. The following quotes represent participant views about this feature: "Not sure how someone can remember the login ID, every time needs to copy it from my email to get access". These complications of passwords and lengthy IDs may lead to frustration and reduce users' productivity. Bitcoin clients should consider using different login approaches to give the users freedom to choose the best approach that fits with his device and make him feel protected and productive.

The second theme found is efficiency attribute of usability, where efficiency is concerned about users' ability to accomplish tasks with less effort and less time. Users indicated that wallet allows users to see coins balance in their local currency. This helps the user to transact faster without the need to convert coins to their local currency using other application. Also, using QR code can minimise the time needed to type Bitcoin address or pair between web and mobile device. One of the participants stated, "QR code makes it easy for me to share my Bitcoin address, and quick to link my web wallet with my mobile device wallet". Such features may help to increase users' performance efficiency and reduce efforts needed to accomplish tasks. This is a brief analysis of the participants' comments that help us to recognise some preliminary indications about users' perception of Bitcoin payment system.

5.5.3 Survey results

The descriptive statistics derived from the survey results are shown in Table 5.3. The Mann-Whitney U-test is a powerful test to compare outcomes between two independent groups and compare the number of times a score of one of the samples ranks higher than a score of the other sample regardless of the data normality. To find any difference between credit/debit card and Bitcoin perception and whether the scores between the two groups are statistically significant we applied two tailed probability to compare the scores of the two groups on the seven aspects examined.

Table 5.3: Descriptive Statistics

	N	*Mean*	*Std. Deviation*	*Minimum*	*Maximum*	*Percentiles*		
						25th	*50th (Median)*	*75th*
Learnability	*55*	*3.7909*	*.95108*	*2.000*	*5.000*	*3.000*	*4.000*	*4.000*
Efficiency	*55*	*3.7091*	*.95593*	*2.000*	*5.000*	*3.000*	*4.000*	*4.000*
Memorability	*55*	*3.6727*	*1.00101*	*2.000*	*5.000*	*3.000*	*4.000*	*4.000*
Error	*55*	*3.6818*	*.53023*	*2.000*	*5.000*	*3.500*	*4.000*	*4.000*
Help	*55*	*3.3818*	*.78742*	*2.000*	*5.000*	*3.000*	*3.000*	*4.000*
Security	*55*	*3.2364*	*.92223*	*1.000*	*5.000*	*3.000*	*3.000*	*4.000*
Satisfaction	*55*	*3.6182*	*.90760*	*2.000*	*5.000*	*3.000*	*4.000*	*4.000*

Table 5.4: Mann Whitney Test

	Learnability	*Efficiency*	*Memorability*	*Error*	*Help*	*Security*	*Satisfaction*
Mann-Whitney U	*172.500*	*153.000*	*259.500*	*358.500*	*241.000*	*230.000*	*117.500*
Wilcoxon W	*425.500*	*406.000*	*512.500*	*611.500*	*494.000*	*483.000*	*370.500*
Z	*-3.447*	*-4.009*	*-1.873*	*-.083*	*-2.186*	*-2.410*	*-4.358*
Asymp. Sig. (2-tailed)	*.001*	*.000*	*.061*	*.934*	*.029*	*.016*	*.000*
Effect size (r)	*0.46*	*0.54*	*0.25*	*0.11*	*-0.30*	*0.32*	*0.58*

Table 5.4 shows the results of the Mann-Whitney U-test. The results indicate that, of the 7 areas examined, 5 show significant differences between credit/debit card and Bitcoin

perceptions. The following sub-sections statistically explain the results for each area examined. The results of each sub-section are discussed based on the aspects of the systems examined.

5.5.3.1 Learnability

Based on the descriptive statistical results shown in Table 5.5, credit/debit card users' perceptions (median = 4.00; mean rank = 33.77) scored higher on learnability than Bitcoin (median = 3.00; mean rank = 19.34). U = Mann-Whitney test statistic = 172.500; W = Wilcoxon W statistic = 425.500; z = U transformed into a normally distributed z = -3.447; p < 0.001 as shown in Table 5.5. The test results show a significant difference between credit/debit card and Bitcoin in terms of learnability. The difference between the groups is medium (r = -0.46). Therefore, hypothesis H1 is rejected.

Table 5.5: Analysis of learnability

	Learnability
Mann-Whitney U	*172.500*
Wilcoxon W	*425.500*
Z	*-3.447*
Asymp. Sig. (2-tailed)	*.001*

5.5.3.2 Efficiency

Descriptive statistics show that credit/debit card (median = 4.00; mean rank = 34.36) scored higher on efficiency than Bitcoin (median = 3.00; mean rank = 18.45) as shown in Table 5.6, U = Mann-Whitney test statistic = 153; W = Wilcoxon W statistic = 406; z = U transformed into a normally distributed z = -4.009; p = 0.000 < 0.001 as shown in Table 5.6. The test results show a significant difference between credit/debit card and Bitcoin in terms of efficiency. The difference between the groups is quite large (r = -0.54). Therefore, hypothesis H2 is rejected.

Table 5.6: Analysis of efficiency

	Efficiency
Mann-Whitney U	*153.000*
Wilcoxon W	*406.000*
Z	*-4.009*
Asymp. Sig. (2-tailed)	*.000*

5.5.3.3 Memorability

Based on the Mann-Whitney U test results the mean rank for memorability is not statistically significantly different between credit/debit card and Bitcoin. U = Mann-Whitney test statistic = 259.500; W = Wilcoxon W statistic = 512.500; z = U transformed into a normally distributed z = -1.873; p = 0.061. Even though there are no significant differences in the memorability aspect, credit/debit card (median = 4.00; mean rank = 31.14) scored higher than Bitcoin (median = 3; mean rank = 23.30) as shown in table 5.7 The difference between the groups is small (r = -.025). Therefore, hypothesis H3 is accepted.

Table 5.7: Analysis of memorability

	Memorability
Mann-Whitney U	*259.500*
Wilcoxon W	*512.500*
Z	*-1.873*
Asymp. Sig. (2-tailed)	*.061*

5.5.3.4 Error & Recoverability

Based on the Mann-Whitney U test results, the mean rank of error and recoverability is not statistically significantly different between the examined systems, U = 358.500, z = -0.083, p = .934 as shown in Table 5.8. However, both systems achieved high median scores for error & recoverability (median = 4.0 & 3.50). The difference between the groups is very small (r = -.011). This reveals that the participants found both systems equally easy regarding errors & recoverability. Therefore, hypothesis H4 is accepted.

Table 5.8: Analysis of Errors

	Errors & Recoverability
Mann-Whitney U	*358.500*
Wilcoxon W	*611.500*
Z	*-.083*
Asymp. Sig. (2-tailed)	*.934*

5.5.3.5 Help

Based on the descriptive statistics results in Table 5.9, credit/debit card users' perceptions (median = 4.00; mean rank = 31.70) scored higher on help than Bitcoin (median = 3.00; mean rank = 22.45). U = Mann-Whitney test statistic = 241.000; W = Wilcoxon W statistic = 494.000; z = U transformed into a normally distributed z = -2.186; p < 0.029 as shown in Table 5.9. The test results reveal a significant difference between credit/debit card and Bitcoin in terms of help support. The difference between the groups is medium (r = -0.3). Therefore, hypothesis H5 is rejected.

Table 5.9: Analysis of Help

	Help
Mann-Whitney U	*241.000*
Wilcoxon W	*494.000*
Z	*-2.186*
Asymp. Sig. (2-tailed)	*.029*

5.5.3.6 Security

The Mann-Whitney U-test shows a significant difference between credit/debit card participants and the Bitcoin group in terms of security perception. Mann-Whitney test statistic = 230.000; W = Wilcoxon W statistic = 483.000; z = U transformed into a normally distributed z = -2.410; p < 0.016 as shown in Table 5.10. Credit/debit card users' perceptions (median = 4.00; mean rank = 32.03) scored higher on security than Bitcoin (median = 3.00; mean rank = 21.95). The difference between the groups is moderate (r = -.32). Therefore, hypothesis H6 is rejected.

Table 5.10: Analysis of Security

	Security
Mann-Whitney U	*230.000*
Wilcoxon W	*483.000*
Z	*-2.410*
Asymp. Sig. (2-tailed)	*.016*

5.5.3.7 Satisfaction

Based on the Mann-Whitney U-test results, the mean rank of satisfaction is statistically significantly different between credit/debit card and Bitcoin. U = Mann-Whitney test statistic = 117.500; W = Wilcoxon W statistic = 370.500; z = U transformed into a normally distributed z = -4.358; p = 0.000 < 0.001. The median reveals that credit/debit card (median = 4.00; mean rank = 35.44) scored higher than Bitcoin (median = 3; mean rank = 16.84) as shown in Table 5.11. This indicates that the participants were more satisfied with credit/debit card than Bitcoin. The difference between the groups is large (r = -.58). Therefore, hypothesis H7 is rejected.

Table 5.11: Analysis of Satisfaction

	Satisfaction
Mann-Whitney U	*117.500*
Wilcoxon W	*370.500*
Z	*-4.358*
Asymp. Sig. (2-tailed)	*.000*

5.6 Discussion

This study investigates the perceptual differences between Bitcoin's anonymous system and credit/debit cards as a non-anonymous payment system among undergraduate students in terms of usability and security. The goal of this paper is to answer the research question given in Section 5.1 in order to understand how users interact with anonymous Bitcoin compared with the currently most used payment system (credit/debit cards), with an emphasis on usability and security. This is a first user study, which focuses on user perception of Bitcoin usability and security trade-off in comparison with other payment systems. As we noted earlier, this study was performed at the time when the Bitcoin was still primarily used as a digital crypto-currency and not as an investment tool.

The main aims of setting the tasks was to encourage the participants to explore the capabilities of an anonymous payment system, improve the participants' familiarity with Bitcoin, and increase our understanding of their perceptions of the usability and security aspects. Giving the respondents tasks helps to reduce the potential ambiguity of answers to survey questions.

The survey results indicate that 5 of the tested hypotheses, H1, H2, H5, H6 and H7, are rejected. The analyzed data reveal significant differences in users' perceptions of credit/debit cards and Bitcoin for learnability, efficiency, help, security and satisfaction, as explained in Section 5.3. However, no significant difference is shown relating to the usability aspects of memorability and error. Comparing the usability attributes of both systems shows that the respondents perceived the usability of credit/debit cards higher than Bitcoin. The participants had negative perceptions of Bitcoin's security that been affected by the low rate of usability.

The following subsections discuss the result of each aspect individually and recommend a guideline for each. We also explore the relevant lessons for the application of secure crypto-currencies in the context of e-government services.

5.6.1 Learnability

Learnability is how easy the system is to learn and use. This attribute is essential for novice users. A key finding revealed by the analysis of participants' experiences, is that the ease of learnability criterion was an issue for Bitcoin. The T2 results show that 26.1% of participants (see Table 5.2) were unable to find the Bitcoin receiving address, which is an essential piece of information needed when conducting any transaction. This task was rated by 41% of the participants as difficult. By evaluating the Bitcoin client, we found that the receiving address can be located under the "Request" tab, which could easily be confused by users for the other tab "Received Coins". The "Received Coins" tab only shows the history of the Bitcoin received. There was a popular misconception among novice users that a Bitcoin address looks like an email address, which makes it hard for users to find the receiving address first try. T3 was rated as difficult by 50% of participants who were unsuccessful in locating and setting up one of the available functions; 47% of participants failed to accomplish this task. We assume that the failure to locate the “Auto Logout” function was due to the function location. The “Auto Logout” function should be located in the “Security Settings” tab but is located under the “User Preferences” tab. It is obvious that novice users were not able to accomplish basic tasks the first time they used Bitcoin. Learnability is a major usability aspect with a great influence on how users rate other usability attributes.

The survey results reveal that credit/debit cards have higher learnability than Bitcoin based on user experience. This indicates that users took more time to learn to use the Bitcoin wallet and were not able to use it effectively. However, using credit/debit cards for online purchases requires users to fill in lengthy forms with personal data and card details, and therefore cannot be considered as an easy option. The results reveal that users perceive it differently in term of being easy to learn, even though it is not an appropriate method. It could be that users have become familiar with filling in these types of payment details over the years, or usability experts overestimate the complexity of credit/debit card payments.

The survey results on usability emphasise the importance of learnability to Bitcoin users.

In order to develop crypto-currency based e-government systems that are likely to become popular, designers must give high priority to learnability. Learnability is an essential usability attribute that has a great influence on novice users’ perceptions. Improving system learnability is likely to improve users’ perceptions of other usability aspects.

In light of the above, we recommend that Bitcoin developers focus on the essential functions that are used most by users, such as “Bitcoin Address”, “Receive” and “Send”. Developers should make the most important functions accessible from every section of the Bitcoin client, make them specific and avoid being ambiguous. Everyday familiar short words should be used to identify these functions. This would help simplify user interaction with the Bitcoin client and help users adjust to it quickly. The system should be consistent and logical to help Bitcoin users recognise repeating patterns and use the Bitcoin client intuitively. Developers should focus on reducing prioritisation and organisation functions to simplify user interaction with the Bitcoin client. We propose that developers reduce the number of actions or clicks needed to accomplish essential tasks, in order to decrease the cognitive load on users. Designers should also present a balanced set of options to the user.

Fewer relevant choices would help users make the right decision and improve the overall learnability. Prioritisation of these important functions, based on their significance to the user, would help users pay attention to them. Also, appropriate categorisation and grouping related functions in tabs would reduce the chance of users being confused by the vast number of options. Adding standard interactive graphical elements to Bitcoin clients would help users learn quickly from previous experience and make them feel more comfortable. Designers could also use icons that are more comfortable for users and allow them to modify these icons by choosing from sets of alternatives. Using a graphical icon is meaningful to users from different backgrounds and can be perceived faster than text.

5.6.2 Efficiency

Efficiency is another issue for the Bitcoin system, based on the participants' comments on the tasks. Participants commented negatively on the accuracy and speed of performing tasks as stated in comments E and H in Section 5.2. Rating tasks as difficult is an indication that the participants expended effort accomplishing them, as shown in Table 5.2.

The survey results show that credit/debit cards have a higher degree of efficiency than Bitcoin. Bitcoin as a payment system was rated by respondents as not efficient compared to credit/debit cards. Based on Cohen's classification, the difference between the two groups is large enough to be significant. Users perceive Bitcoin as less efficient than credit/debit cards despite the ability of Bitcoin systems to accept micropayments, without transaction fees. It is possible that users consider micropayments as unimportant features for them. Small payments of less than £1 are rare nowadays. Transaction speed is another potential issue for Bitcoin Blockchain; for example, if you purchase a cup of coffee using Bitcoin, you may wait for minutes or hours for your transaction to be approved in the Blockchain by miners. Users' lack of background knowledge of Bitcoin may also influence their perception. Clearly there is a potential usability issue in respect to efficiency. While it may sound obvious, it is important to underline that providing the experience of efficiency is key for the development of successful crypto-currency based e-government services. Our results show that lack of efficiency can undermine very much the perception of usability and consequently may limit considerably the take-up of the service.

Based on the results above, we recommend that designers consider applying two different designs to the Bitcoin client. They should consider implementing two different modes designed to fit novice and expert users and give them the freedom to choose and switch between them as required. As we know that the two sets of users have different experiences and strategies for using the same application, this design would increase efficiency for both novice and expert users. It would provide users with alternative methods of accomplishing the same activity efficiently and help them switch between the designs based on technology experience and preference. Giving the users the option to choose between two designs would allow them to accomplish tasks faster, as each design would be directed to suit each set of users. On the other hand, the volatility in transaction time makes it challenging for Bitcoin to be applied as a payment system, despite the lower fees. What we currently see, is that Bitcoin has always been slow in comparison to a credit card transaction, and senders and receivers are uncomfortable if they have to wait more than 10 minutes, on average, for the Bitcoin network to propagate the payment. Bitcoin's developer community has to find a solution to this problem in order to enable users to transact quickly, with lower fees. Right now, there are some promising projects trying to solve the transaction speed issue for Bitcoin and increase the number of transactions per second to ensure the highest efficiency.

5.6.3 Memorability

The statistical results show no significant difference between users' perceptions in terms of memorability. Users perceived both systems equally. However, on further investigation and comparing the difference between the two groups using Cohen's classification, credit/debit cards scored 25% higher than Bitcoin, which is a small difference. This means that credit/debit cards are perceived to have greater memorability, even though the difference is small. It is possible that when a system is easy to learn, users are more willing to relearn how to use it, and therefore memorability may not be as important as it is for credit/debit cards. Bitcoin has a steeper learning curve, and is considered by users as difficult to learn, therefore learning such a system requires a significant amount of time. For this reason, designers must consider memorability as an important usability aspect when designing crypto-currency based e-government systems and services.

Generally, Bitcoin addresses are too long and extremely difficult to remember for most users. Some Bitcoin clients implement QR codes to allow users sharing addresses to avoid having to type them. However, QR codes are not an efficient solution due to the vulnerabilities inherent in the standard, and the ease of social manipulation attacks. In our opinion, Bitcoin developers should introduce an appropriate system to translate the Bitcoin hash address into a visual representation, similar to the name system of DNS, and vice versa. This would help make Bitcoin addresses more human and easier to remember. Bitcoin developers should also address the issue of long login IDs, which are not easy to remember. Developers should make these login IDs slightly personalised and therefore easier to recall. Bitcoin clients should have more graphic interfaces, for better memorability, because humans are better at recognition than recall.

5.6.4 Error & Recoverability

With regard to the error and recoverability information aspect of usability, the participants found some of the error messages too technical to understand, as stated in comment F in Section 5.2. Also, the participants showed some concern about sending Bitcoin to the wrong address, in which case the transaction can't be recovered.

However, the survey results reveal no significant difference between Bitcoin and credit/debit card users' perceptions of error and recoverability. Comparing the difference in effect of the two groups shows a small difference, with credit/debit cards having a lower error rate (by 11%) and higher recoverability than Bitcoin. A possible explanation is that Bitcoin users can't reverse or cancel transactions, whereas credit/debit card users can call their banks and reverse any transactions. Moreover, inadequate user knowledge of Bitcoin and Blockchain, which are not mature technologies, may influence users' perceptions.

Novel e-government services relying on crypto-currencies must make sure that the error and recoverability information provision to users is adequate and technical terms used in such information are sufficiently easy to understand and operate with.

In order to reduce the possibility of errors due to the lack of an undo feature in the Bitcoin client for the transfer of coins to other party, Bitcoin developers should implement a system to allow users to roll transactions back, for a fixed fee. Also, it is possible for developers to put an optional feature in Bitcoin clients to allow users to lock any transfer of a large amount for one day and send a notification to the receiver to confirm the Bitcoin address. We recommend that any Bitcoin client should have smart error prevention features, such as user reminders about the amount of coin sent (e.g., too small or too big) before processing the transaction. This could help effectively minimise the occurrence and consequences of errors. Regarding the technical error messages that users encounters, developers should avoid using technical terms and codes. These error messages should be clear, easy to understand and concise. The developer should implement a way of taking the user to a screen that explains why they received the error message and tell them what to do next. In general, users need a description of what has happened to work out how to fix the error. Error messages should be expressed in plain language that suggests what further action users need to take to overcome the error and suggest a solution.

5.6.5 Help

Help is a significant usability attribute, and the help available should be relevant, understandable, searchable and useful in a specified context of use. The results show that users perceived credit/debit cards better than Bitcoin in terms of help. A potential explanation is that Bitcoin clients use highly technical language when providing help, and there is a lack of resources which users can turn to for help. Some users said that help messages were not understandable. In general, when a system is easy to learn and easy to use, users put minimal reliance on help and documentation. Bitcoin interface designers should keep the instructions easy to identify, and they should appear in a consistent location whenever they are needed. Bitcoin clients should include a help section with all the relevant answers expected by users when they encounter problems. The help section should have the capability to increase the problem-solving ability of users and contain guidance and advice on most expected issues. Developers should make information that easy to search, focused on the user's task, list concrete steps to be carried out, and not be too large.

As with the cases of error and recoverability information, it is important that any new e-government service that may use crypto-currencies provides adequate and technically easy to understand help information to the users in order to achieve high take up.

5.6.6 Satisfaction

Some of the assigned tasks were challenging for many users, and many failed to do them, for example finding the receiving address and setting the auto logout and backup. Some participants expressed discomfort in using the Bitcoin wallet due to its complexity and the lack of knowledge of novice users.

In term of user satisfaction, in line with the task experience reports, the survey results show that the credit/debit card respondents had high levels of comfort compared to the Bitcoin users, who were unsatisfied with their Bitcoin experience. This could be explained by Bitcoin users being influenced in negative ways by the usability limitations of the system.

The findings imply that users' satisfaction with Bitcoin is significantly influenced by their perceptions of usability. Missing important functions and features in Bitcoin clients, such as the lack of an undo option, along with long transaction processing times cause lower user satisfaction. In general, the complexity of Bitcoin, the absence of legal authority, and having no control over transactions have a great influence on users' overall levels of satisfaction. To increase user satisfaction, we recommend that developers put more effort into user requirements and apply features that make users feel in control when using the system. User satisfaction would be perceived as better if developers make the operational tasks that users have to perform easier, speed up transaction processing time, and simplify the features of the Bitcoin system.

The satisfaction results highlight the importance of delivering good usability in order to achieve good customer satisfaction with any new e-government service relying on crypto-currencies. While this is generally true, in the context of introduction of new services relying on novel and sophisticated computational technology, this is particularly important.

5.6.7 Security

With regard to the security aspect, the participants had a negative experience with the Bitcoin, which is reflected in some of their comments about the authentication methods. The participants reported that logging in to the wallet was difficult because of the long ID used. Also, the time and effort needed to set up all the security authentication features for the wallet were problematic. On the other hand, the participants gave some positive comments about features they found useful such as advanced authentication features, 2-step verification, balance shown in user local currency, the ability to auto-generate a new wallet transaction address after each transaction, and the option to pair a web wallet with a mobile device by scanning a QR code.

The survey results reveal that the respondents perceived Bitcoin security differently from the way it is actually realised. Despite the fact that credit/debit card payments are less secure and have less anonymity, users perceived them as more secure than Bitcoin. A possible explanation is that users do not find anonymity important or are unaware of the actual situation.

Another possible reason is that the usability limitations of Bitcoin have a negative influence on how users perceive security. Also, the knowledge or skill level of the respondents plays a major role in user security perceptions. This means that many users don't have enough knowledge about Bitcoin's benefits or are just following the trend of using Bitcoin. According to the results, many users were concerned about Bitcoin's legal status and customer protection, both of which may indirectly influence their security perceptions. Some of the security features highlighted by the tasks may have had negative impacts on the users' perceptions, such as the length of the authentication process and login ID.

We suggest that Bitcoin developers focus on providing various security levels in Bitcoin clients, for example transfers between the user's own Bitcoin wallets should not be treated the same as transfer to a trader. Security alerts and notifications should be clearer and more concise, and users should be notified when confidential settings are accessed or when there is any change. Important security settings should be categorised and grouped under one tab and guidance provided for users on how to use them. Also, we propose that developers help users switch between two privacy preferences, anonymous and non-anonymous, to give them freedom and feeling of control over transactions. Designers should make sure that security settings are easy to set up and clearly visible to the end user. Bitcoin payment systems, as with any systems, have some security and privacy vulnerabilities. Developers should acknowledge these vulnerabilities to end users, so they can protect themselves by applying the security and privacy features of the application correctly and effectively.

These results highlight the importance of usability and legal clarity in relation with any crypto-currency that might be used to support novel e-government services. The lack of appropriate delivery of these features can undermine the appreciation of security or other advanced technical features of the service by its users. This in turn may considerably reduce the willingness to take-up and use the service.

5.7 Similarities & Differences in Findings

The findings of the study reveal that credit/debit cards are perceived higher by participants in terms of usability and security, and the statistical interpretation described in the previous sections shows significant differences in five aspects: learnability, efficiency, help, security and satisfaction.

The results of the hypothesis testing, and statistical interpretation, show that credit/debit cards have the best overall usability perception which has a positive influence on security perception. On the other hand, Bitcoin has poorer usability perception which has a negative influence on how users perceive its security.

The study also reveals that credit/debit card and Bitcoin users perceive memorability and errors of usability attributes in almost the same way. The users' low satisfaction with Bitcoin is significantly influenced by their negative experience of eWallet usability. Missing important functions and features in the Bitcoin clients, such as the lack of an undo option, along with long transaction processing times cause lower user satisfaction.

5.8 Study Limitations & Future Research

Similar to other studies, this study has several limitations that should be mentioned. These limitations can be considered opportunities for further research.

The small sample size is one limitation, due to the nature of the study and the methodology used. This small sample size limits the generalisability of the study. Larger samples may increase the chance of finding significant differences, since they more reliably reflect the population, making the findings more generalisable.

Another limitation is that the researchers do not focus on the social influences or social interactions that may influence user perceptions of usability and security. Some respondents may have a socio-culturally biased interpretation of some of the questions in the questionnaire. However, all the questions were thoroughly pre-tested and improved in a pilot study before being given to the participants.

The third limitation is that demographic variables, such as age, gender, education level and prior experience, were not included in the study. Some previous studies have indicated these demographic variables and their influence on users' perceptions of usability and security (Fogg et al., 2003; Peng, 2013; Baglin, 2015). Dwivedi and Williams (2008) reveal that demographic characteristics, such as age, gender and educational backgrounds influence users' perceptions of usability. This is consistent with Choudrie and Ghinea (2005), who found that users' perceptions of usability are influenced by their age and education level, showing the significance of individual differences. However, demographic characteristics are not sufficiently covered in this study, although we did tried to minimise such effects by recruiting participants with similar demographic characteristics, such as education level (first year university students) and age (18 to 24 years).

Further studies need to investigate the effects of demographic variables and individual differences on users' attitudes and perception of the usability and security of anonymous payment systems. The findings would be valuable for developing and designing e-government anonymous payment systems that could be accepted and used by a variety of individuals.

The fourth limitation concerns the use of the specific Bitcoin e-Wallet used to get users' insights into usability and security. The study selected Blockchain.info as the wallet provider, based on certain criteria such as popularity, accessibility, network bandwidth, computing power and storage, as explained in Section 5.3, compared to other wallets. The hosted wallet was decided on by mutual agreement between the researcher and the supervisory team. The hosted wallet chosen was the perfect e-wallet for the study objectives and tasks, but further work could be carried out with other e-wallets, comparing the results with the current study's results.

The last limitation concerns the usability and security survey questionnaire and the process of selecting and designing the questionnaire groupings, which were based on the relevant studies reviewed. Based on the insights gained from other studies which used usability and security questionnaires, the survey questionnaires were developed and redesigned to be tailored to the systems tested within an e-government context. The final version of the survey was tested by the supervisory team and approved by the ethics committee.

5.9 Summary & Recommendations

This comparison between credit/debit cards and Bitcoin users' perceptions in terms of usability and security shows significant differences in five aspects: *learnability, efficiency, help, security and satisfaction*. The study shows that credit/debit cards and Bitcoin users perceive memorability and errors of usability attributes in almost the same way. The results of the hypothesis testing, and statistical interpretation described in the previous sections, show that credit/debit cards have the best overall usability perception, which has a positive influence on their security perception. On the other hand, Bitcoin has the poorer usability perception which has a negative influence on how users perceive its security.

Therefore, our results show that usability and security have a close relationship. In other words, users' perceptions of usability and security positively influence each other. The findings suggest that perceived security, as measured by the questionnaires, is affected by the users' overall usability perception.

The results revealed that Bitcoin, as a crypto-currency, is still a major challenge for many users. We conclude that Bitcoin cryptocurrency payment system is still in its infancy and requires user education and a new way of thinking. It is recommended that users' mental models are developed in order to deepen developer understanding of anonymous cryptocurrencies technology and improve user-centred design. The results indicated that users perceive some usability characteristics of crypt-currency payment system higher than others and some characteristics much less. From our point of view, it is significant to understand what usability aspects of anonymous payment systems have most direct influence on user perception and what characteristics are more essential for user acceptance.

Also, it is important to narrow the gap between Bitcoin Blockchain technology and user expectations, in order to have better user usability and build trust. Insufficient government regulation and Bitcoin application standards are among many reasons that affect users' acceptance of Bitcoin as an anonymous payment system. Bitcoin Blockchain technology still not mature enough, not systematically studied and risks surrounding it still unknown. A common Blockchain platform, application standards, and application programming interfacing are required to improve user perception and interaction.

Our analysis of the results provides useful guidelines for the development of future e-government services that rely on the use of anonymous crypto-currencies and related technologies. In particular, our key recommendation is to invest in the improvement of the usability of the service and delivery of usability features at a high level. Without these potential users will not appreciate sufficiently the security benefits of such new e-government services and the likely take-up and user satisfaction will be limited.

Our study points to the need for further investigation to get a better understanding of users and address user usability and security issues and the trade-off between these. A comparison between expert and novice users is recommended in order to investigate how expert users perceive usability and security in comparison to novice users.

Chapter 6 Apple Watch Study

6.1 Introduction

Smartwatches are widely used, multipurpose, wrist devices, yet little is known about how users experience and perceive the usability and security of their features. In order to understand users' perceptions of the usability and security of smartwatches, we conducted a qualitative study using four focus groups and the Reddit discussion website to collect data. The data collected from the focus groups was used to assess novice users' perceptions, and the Reddit data was used to understand how expert users experience smartwatch usability and security. The results reveal perceptual differences between the two user groups toward some smartwatch features. On the basis of our qualitative analysis, we present key findings about users' perceptions of the usability and security of smartwatches as experienced by the two categories of user. Based on our findings, we make recommendations with respect to the usability and security of smartwatches to improve user-centred design.

6.2 Background

Over the last four years, smartwatches or smart wrist watches have invaded markets and started to become widely used worldwide by various segments of users. According to International Data Corporation (IDC) analysts, the number of smartwatch shipped in 2018 was 46.2 million, about 39 percent more than in 2017 (Llamas and Ubrani 2018). Recent polls of smartwatch sales forecasts predict that global smartwatch sales will double by 2022 to 94.3 million units (Llamas and Ubrani 2018). These figures indicate that smartwatches are globally accepted, and users feel comfortable wearing them (Kim, He, Lyons & Starner 2007). Most smartwatches come with various impressive technical and computational capabilities that help fulfil certain users' needs such as heart rate sensors, built-in GPS (global positioning system), and AI (artificial intelligence) software that helps users get instant analyses of their health and fitness (Rawassizadeh et al., 2015). Some smartwatches are designed to be complementary, multipurpose devices to serve users who are not pleased by handheld mobiles, but most are dependent, subservient devices. In the coming years, we may see subtle advances in smartwatches that make them the hub of our daily lives and give them a distinct advantage over smartphones. Such technology proliferates in our everyday lives, and researchers and practitioners consider it a promising technology that can bring the power of smartphones to our wrists. The spread of smartwatches has helped users become more connected, more social and more productive. Also, their wearable nature and the various advancements in smartwatch functionality enable users to have a convenient way of keeping track of notifications, fitness and instant messages, even when their smartphone is not available at hand.

All these features, along with the modern sensing capabilities provided by smartwatch devices, make them intelligent and flexible devices that can improve users interactions with surrounding technologies (Link et al., 2019). The spread of smartwatches and their social impact on users has encouraged governments and public servants to evaluate the use of this technology, to improve citizens' interactions with e-services made accessible on smartwatch devices. The adoption of smartwatches by e-government should improve the life quality of citizens and increase the use of e-services. A smartwatch, as an emerging technology with sensing capability, can collect anonymous data from its smart sensors and share them with concerned governmental entities. For example, in the smart health sector, governments can use smartwatch body analysis sensors (biosensors) to collect certain data about citizens and use cloud computing and the internet-of-things to improve health services. Smartwatches have the potential to be useful in a variety of healthcare applications. They have smart health monitoring apps capable of sending information and updating the user's health record daily. Similarly, they can be used in emergency cases to ask for help from police or ambulance services. However, governments at this early stage are proceeding with caution in creating citizen-facing apps for smartwatches, as the technology is still very early in its cycle(Jr, 2019). Governments can provide new levels of convenience to citizen using the smartwatch technology.

The smart apps of smartwatches could improve government efficiency and performance by providing services to a wide range of users in various settings. The sensing capability of smartwatches is a promising technology that can help users become more connected with public servants and provide valuable data about citizens' needs.

Recently, research into smartwatches has concentrated on how to enhance their hardware capabilities (Cohen 2013) and on theories of technology acceptance from an organisational perspective (Kim and Shin 2015; Wu & Chang 2016). There are few studies that investigate users' perceptions and attitudes or the aspects of smartwatches that have an impact on the intention to use. Choi & Kim (2016) investigate the factors that affect the intention to use smartwatches using the technology acceptance model (TAM) extended to include the concepts of perceived enjoyment and perceived self-expressiveness. The study finds that the characteristics of the smartwatch as a fashion product have significant impacts on the intention to use but no significant effect on the perceived ease of use. However, Kim and Shin (2015) and Wu, & Chang (2016) find that users perceive ease of use to be a non-significant factor in their attitudes to using smartwatches. Chun, Lee and Kim (2018) asses the usability of smartwatch devices and suggest guidelines to enhance the user input interaction and performance. Also, some studies investigate the daily experience of using smartwatches and their applications (Lundell and Bates 2016; Vega et al. 2015) or smartwatch map navigation (Kerber, Krüger and Löchtefeld, 2014). In fact, few studies have intensively considered the usability and user experience of smartwatches in particular and most of the academic research tends to be more technology driven than audience driven (Chun et al. 2018; Oakley and Human 2014; Choi & Kim 2016).

We found some contradictory results from studies regarding users' perceptions of smartwatches (Kim, Lee & Kim 2017). Two of the studies reviewed report that the users' perceived ease of use is non-significant for choosing between devices (Kim and Shin 2015; Wu & Chang 2016). Meanwhile Choi & Kim (2016) state that the users' perceived ease of use is a significant factor in user choice. These contradictory empirical research results are often seen by designers as difficult to understand and generalise to the design of smartwatches (Shirazi and Henze, 2015; Ha et al., 2017). In our view, the reason behind such inconsistent findings for smartwatches users' perceptions is that smartwatches are still in their nascent stages of adoption as a new technology, and still do not have a well-established user base. Smartwatches come with different input methods, styles and sizes, with robust built-in applications or third-party apps available to download. Some researchers argue that smartwatch designers and developers have applied their past smartphone design experience to a device historically not meant for user interaction, without considering the user experience of the smartwatch, which is different to today's generation of smartphone devices (Davie and Hilber, 2016; Pizza et al., 2016; Liu et al., 2017). Some recent papers acknowledge that smartwatch devices suffer from complex user interface usability issues that affect users' perceptions (Han and Luximon, 2016; McMillan et al., 2017; Nguyen and Memon, 2017; Wong et al., 2017; Chun et al., 2018). In our view, empirical investigations into how users perceive smartwatches have not been sufficiently covered, and most relevant research results are still preliminary.

Security is a significant barrier for users and can have a great influence on the use of smartwatches. Generally, user confidence in technology is greatly weakened if users perceive it to be insecure, and this can be a determinant of users' decisions to use them (Alshamsi & Andras 2019).

Therefore, there is a need to understand users' perceptions of smartwatches and to conduct in-depth analysis with a focus on users' interaction with smartwatches and their concerns about usability and security features. The first goal of our study is to investigate the differences and similarities in perceptions between expert and novice users and capture their insights about usability and security aspects. Understanding the differences and similarities in the perceptions between these two user types could have a number of positive outcomes to help improve the design of smartwatches and close the gap between novice and expert users. Including novice and expert users is done in order to get insights into the perceptions of those who have and haven't used smartwatches. The understandings of both types of user can add additional layers to the quality of our findings.

The differences between novice and expert users in human computer interaction (HCI) are defined by Nielsen (1993). Experts are individuals who are skilful and have rich interaction knowledge of the system, while novices are individuals who are unskilful and have poor interaction knowledge of the system.

The second goal of this research is to examine the most important smartwatch features that are significant to both types of user, and assessment of the extent to which the two user types perceive these features differently. We aim to identify the features that most strongly influence the perceived usefulness of smartwatches and which influence user expectations about smartwatches, both for novice and expert users.

In this study, we intend to explore the trade-off between usability and security from a user perspective, in order to understand how users perceive the usability and security of smartwatches. The study seeks a comprehensive understanding of how users interact with the smartwatch, what they perceive as useful or useless, and their experience in respect of usability and security. The study focuses on understanding novice users' requirements from a smartwatch and capturing their experiences of the usability and security, and a comparison with expert users' experiences and priorities. The analysis of the results increases the knowledge in this field and deepens our understanding of user requirements with respects to the usability and security aspects of smartwatches.

We aim to use our results to identify aspects that influence the use of smartwatches and their application in e-government, and to provide guidelines and indicate future research directions in terms of analysis of user interaction in this context. Our findings benefit e-government service designers by explaining the user requirements of smartwatches and help them design services that are usable and match these requirements.

Our study provides a conceptual foundation for academics and smartwatch designers, with a set of guidelines and clear view of user opinions that are likely to contribute to a better overall user interaction experience. To the best of our knowledge, there has not been any empirical research comparing novice and expert users' perceptions of smartwatches before this. With this study, we contribute to the HCI community by means of an exploratory, mixed method, qualitative study using data from focus groups and Reddit semi-anonymous comments to capture a broad picture of an emerging technology that is not yet well researched.

To conduct our study and accomplish the study goal, we select the Apple smartwatch, called the Apple Watch, to investigate the differences and similarities in users' perceptions and attitudes. The choice of the Apple Watch is due to its popularity among users and the fact it combines the health functionality and communications aspects into one device. There is no information or market research available related to user perceptions or attitudes to the Apple Watch provided by the Apple company at the time this research began.

The paper addresses the following research questions:

RQ1. How does a smartwatch influence novice user perceptions compared to expert user perceptions?

RQ2. How can the design of smartwatches be improved to generate better user interactions and experiences?

6.3 Related Literature

Smartwatches are regarded as cutting-edge technologies which have transformed the lifestyles of regular people all over the world (Chuah et al., 2016). They are wearable devices used by individuals for various purposes. Silva et al. (2016) state that smartwatches have made the lives of people simple and convenient. As such, the gadget can be dubbed a wearable computer since it provides the same utility and services as a computer system. According to Cecchinato et al. (2017), the first smartwatch was built by Steve Mann in 1998, and was used to run the Linux operating system. He was given the title ‘the father of wearable computing’. According to Hankerson et al. (2016), this invention was made with the motive of satisfying the needs of customers within a much shorter time period.

The device looks like a wristwatch and thus individuals can wear it at any time and execute their tasks. Schrack et al. (2017) say that smartwatches were invented to help and support users in accessing any kind of information as required, anywhere, anytime. According to Schrack et al. (2017) they are a radical innovation in the information and communication technology (ICT) domain. Communication and interaction is widely facilitated by smartwatches. According to Xu et al. (2015), they have specific sensors which are different from those used in other mobile electronic devices. Jhajharia et al. (2014) say the sensors of the smartwatch store personal data and information needed by people in the near future.

These devices can be connected to several other electronic devices within a short-range by wireless connectivity. According to Ioannidis (2017), smartwatches are useful in providing alert notifications to users. The smartwatch gained maximum public attention after the Pebble Smartwatch Kickstarter campaign of 2012, and 2013 is regarded as the ‘year of the smartwatch’ when people increasingly purchased such wearable computers and connected them to their smartphones. According to Do et al. (2017), in 2014, Google’s Android Wear Smartwatch was announced followed by Apple’s smartwatch, the Apple

Watch, in 2015. Since then, according to Kim et al. (2015), the leading smartwatch manufacturing company has been Apple Inc.

6.3.1 User Perceptions of Apple Watches

Usability is defined as a quality which identifies the degree of user satisfaction with using a certain product (Chuah et al., 2016). In other words, usability can be explained as the degree to which a particular device or software can be used by users to achieve their goals in an effective manner (Schrack, Gresham and Wanigatunga, 2017). The usability of smartwatches denotes the extent of ease and comfort that users receive when using the gadget. According to Chuah et al. (2016), the initial models of smartwatch were used by people to perform basic tasks such as telling the time digitally, game-playing, translation and calculations. However, according to Kim et al. (2015), with progress, smartwatches have been redesigned as wearable computers. Houben et al. (2015) states that Apple smartwatches are designed with an interface which provides ease of use to the users. According to Tim Cook (2015) Apple CEO, smartwatches are intended to provide users with an enhanced and upgraded technological experience. Indeed, users' lifestyles and attitudes are widely changed by the use of these devices (Schrack, 2017).

According to Ioannidis (2017), in order to ensure positive perceptions and increasing usability, it is an antecedent step to know exactly how the device is being used. Technology is constantly changing and upgraded facilities and user interfaces are applied to help users with all their possible needs. As recommended by researchers, users should have the skills and knowledge to use smartwatches, so that they can be familiar with the device. Astrup et al. (2016) say that the usability of smartwatches is dependent on two factors, perceived ease of use and perceived usefulness. The former defines the extent to which users feel at ease using the technology, and the latter denotes the extent to which the users feel the technology is useful. According to Sultan (2015), users can get knowledge about Apple smartwatches through the user manual provided when purchasing the device. They can surf the internet and get access to the ways in which they can operate their smartwatches. Custard et al. (2015) say that adequate knowledge about the device helps them feel ease at using it and experience its useful services. It was observed in 2016 by Ali et al. (2016) that the sale of Apple Watches had increased considerably in the previous few years. Hence, users feel a high level of effortlessness and a low level of complexity using the device and acquire an adequate understanding of its usage. Their keenness to know about the technology and its functionalities influences the usability of the Apple Watch.

Nordman et al. (2017) say that when users find it less convenient and efficient to use a particular technology, their attention gets driven away and their technology acceptance reduces. Smartwatches are designed to enhance users' positive perceptions of them. Hence, Karlsson (2016) states that measuring the effectiveness of the Apple smartwatch device is an essential step ensuring an increase in usability for users. According to Kirschner (2018), users can accomplish various tasks with the Apple smartwatch and become productive. They can adjust their notifications to get up-to-date about various vital matters. For example, using the technology, users can easily get services such as mail alerts, fitness alerts, healthcare alerts, weather information, and traffic updates which make their lives easier. They can also turn off these notifications at their convenience. The Apple Watch screen is one of the best displays and attracts users. Moreover, as pointed out by Schrack et al. (2017), users all around the world feel comfortable wearing the smartwatch like a normal wristwatch and can access any kind of information whenever they want. By calculating task time, the efficiency of the smartwatch could be measured.

According to Kirschner (2018), wearable devices are worn by people and are used anytime and anywhere. Thus, as using the user manual all the time is a daunting process, users, through wearable devices, can remember the steps to access the device and accomplish any kind of activity they wish. In the case of Apple smartwatches, the guide manual explains all the steps to access the device in plain simple language which helps the user easily memorise the steps (Kirschner, 2018). It has been observed by Karlsson (2016), that users of the Apple smartwatch are well acquainted with the accessibility of the device and thus feel at ease using it.

Sometimes, due to an error in connectivity, smartwatches cannot be connected to Bluetooth, which discourages users from using the device. Schrack et al. (2017) indicate that, without effective internet connectivity, users might not receive accurate data and notifications regarding their health and fitness tracking, weather reports or map directions. It has been observed by Nordman et al. (2017) that the heart rate sensors and calculator do not show accurate results. Moreover, errors in information can also occur due to the limited battery life. The battery life of smartwatches is barely 1 to 2 days depending upon the extent of its use. Hence, to ensure uninterrupted services, users have to charge the battery every day. Furthermore, researchers identify that, in the case where users forget their passwords or any other code to access data, Apple smartwatches provide easy recovery options for them through which they can conveniently recover their data. Thus, the usability of the wearable devices increases.

Users get essential information about various matters in seconds. Instant access to data is possible with the help of smartwatches. Therefore, smartwatches provide facilities to people which makes them highly dependent on the gadgets (Schrack, 2017). Generally, users feel happy and are convinced to use a particular technology or gadget when they find it suitable and worthy of satisfying their needs. In today’s technologically advanced era, people have grown highly tech-savvy and use various types of technology to manage their tasks. According to Custard et al. (2015), smartwatches provide enough knowledge to users to make them feel highly motivated and influenced to use the device. In other words, it can be concluded that users regard it as their personal assistant that does their tasks effectively.

Apple Watches provide users with high grade security settings to ensure proper protection of data and the information stored within the device (Cecchinato, Cox and Bird, 2017).

If an Apple smartwatch is lost, the user can open the Apple Watch app from their iPhone and choose the ‘my watch’ menu to select the ‘mark as missing’ option (Do et al. 2017). This disables the users Apple Pay card and related features. The ‘activation lock’ mode always remains on, even if the data in the watch is erased. According to Xu et al. (2015), unless the third party knows the Apple password and ID, they cannot access the smartwatch.

The security of the watch can be strengthened by using a passcode. According to Rawassizadeh et al. (2014), users can keep a strong and secret passcode to unlock their Apple smartwatches which no other person can think of. People might leave it somewhere where there is a possibility of third-party access, but the passcode helps prevent any intrusion into the smartwatch.

Jhajharia et al. (2014) say that the notifications of data that users receive from their Apple smartwatch can be kept private and confidential through the excellent notification privacy feature of the watch. Whenever there is a notification, the details are shown on the watch screen which anybody can peep at. Accordingly, to conceal the details, Sultan (2015) suggests that users can turn on privacy of notifications received. Then users get notifications, but the details are hidden unless they click the watch.

To ensure safety and security of data, Cecchinato et al. (2017) state that users should activate the 'erase data' option which erases all the data if the wrong passcode is entered more than 10 times. This is an attractive feature as it prevents intruders accessing the system.

Every category of data and information can be kept safe and private in the Apple smartwatch. According to Sultan (2015), people can easily manage and secure their health and fitness tracking data, location data and Apple Pay card details by choosing the categories individually and locking them.

Hence according to Jhajharia et al. (2014), Apple smartwatches ensure the privacy and security of the data and information stored within the device, thereby allowing the user to access the system without any tension. Users tend to depend on the gadget to a large extent and thus data security is quintessential to ensuring their protection.

Nowadays, as identified by Tabane et al. (2015), people use wearable devices to run their mobile applications through a mobile operating system. Several e-government services and facilities are provided through smartwatches. According to Kim (2015) Apple smartwatches are meant to deliver facilities and services to users that support them in their daily tasks. As indicated by Nordman et al. (2017), smartwatches tend to make users deeply self-obsessed. Apple smartwatch could be the main guide to the health and fitness of the user. It does not just state the time but also helps users acquire other information such as diet updates, exercise alerts, weather notifications, banking details and railway or airplane schedules. According to Johnston & Hansen (2011), the use of a smartwatch is very convenient and helpful for people.

The government provides a wide range of ICT services to customers or citizens efficiently and easily online. According to Wu et al. (2016), smartwatches are used widely in business affairs. These wearable devices are considered one of the best information and communication technologies and are universally accepted in business organisations. According to Wiig & Wyly (2016), employees are able to access their emails and be notified about workplace matters. The dates of meetings can be notified to employees through smartwatches. The judge can keep a track of his mail and client details in the midst of the courtroom, where his presence is mandatory.

According to Cicoria et al. (2014), smartwatches are used in healthcare domains as clinicians can send notification messages and check-up dates to their patients. Before discharging their patients, doctors give clinical smartwatches to them for adjusting medication timings and dietary plans, so they can take care of themselves at home. Wiig & Wyly (2016) state that many individuals set notification alerts for their medicines and exercise timings so that they can self-manage their health. According to Tabane et al. (2015), smartwatches are useful for monitoring and sharing heart rate, glucose level and fitness.

These wearable gadgets have also changed the way in which people make monetary transactions. For instance, Apple smartwatches provide users with the facility to pay through Apple Pay. According to Johnston & Hansen (2011), architects and fashion designers can use the gadget to share their drawings and sketches. People can get notifications about railway bookings, maps and GPS directions, banking activities and other e-governance services through smartwatches. Schrack et al. (2017) say that users feel great, as they do not need to take their phones out of their pockets to access notifications amidst a hassle. They can just check them through their watches, which saves a lot of time. All e-governance services are offered to the users of the Apple smartwatch. Hence, according to Silva et al. (2016), users are satisfied and pleased to use Apple smartwatches to help them accomplish and govern all their activities effectively.

6.3.2 Conclusion

The overall study indicates that the smartwatch has been invented to make the lives of the people easier and simpler. This wearable device is the most effective and latest technological innovation to transform the lifestyles of people to a great extent. They no longer have to depend on their phones, computers or laptops, but rather they can just wear the smartwatch and get all sorts of functionality, according to their needs (Astrup, Jansen and Aksic, 2016). Various types of information can be accessed through the smartwatch, anytime and anywhere, such as health and fitness data, road maps, workplace emails and meeting dates. The users’ perceptions of the usability and security of Apple smartwatch are examined in this study.

6.4 Methodology

This paper aims to identify novice and expert users' perceptual differences and similarities regarding the Apple smartwatch. We design the study as descriptive research as this aligns with the aforementioned study goals of gathering subjective impressions and preferences about Apple smartwatch features. The study is qualitative in nature and two methods are used to collect data, focus groups and anonymous Reddit comments. The findings are important and contribute to the HCI community understanding of differences and similarities in the perceptions between two user types, allowing us to compare views of Apple smartwatch use. Using mixed methods is very important in understanding user perceptions and can improve the qualitative and quantitative aspects of future studies. Our work makes a significant academic contribution to the HCI community.

Before we define the research methodology, we outline the research hypothesis. In order to keep the research hypothesis simple, we hypothesise that there are no differences between the two user types in how they perceive the Apple smartwatch features that can be discovered from the collected data. The perceptions of Apple smartwatch features we get from the collected data are tested to find any perceptual differences between expert and novice users. Then we investigate the extent to which the default hypothesis is valid for each feature. The research hypothesis is based on the research questions and aligned with its goals:

***H0**: There is no perceptual difference between novice and expert users towards the features of the Apple smartwatch.*

In the following sub-sections, the research design, procedures and recruitment processes for each method are described in detail.

6.4.1 Focus Group

Focus groups are applied in research to generate information on collective views, wherein participants reveal their ideas and feelings about certain matters relating to the studied topic. A focus group is considered a comfortable method, from the participants point of view, as it is a kind of discussion that can generate a rich understanding of the participants' experiences and beliefs. Nielsen (1993) recommends that a focus group session lasts for about two hours and the session is recorded in an organised way that can help the researcher retrieve the data with little effort. The data gathered through group interactions over a short period are deeper and richer than one-to-one interviews (Krueger & Casey, 2014). Another important feature of a focus group is the influence of participants on each other, through their ideas, discussions, answers and contributions during the session (Krueger and Casey, 2014). Focus groups are widely used throughout the HCI research community, on a diverse range of topics, to gain a rich understanding and clear view of users' perceptions (Verdegem & Verleye 2009; Just 2005; Sieger & Möller 2012; Chan & Wei 2009). On the other hand, focus groups can be tricky to analyze and need critical thinking about the ideas in order to identify the main themes from the transcribed text.

Novice users' opinions and views on the Apple smartwatch were collected from four focus group sessions conducted between mid-September 2018 and mid November 2018. Keele University students were recruited for the study through flyers distributed on campus and by word of mouth. Focus group participants were limited to undergraduate students studying at Keele University, over the age of 18, with an Apple smartphone, who had not used an Apple smartwatch before, and who were willing to participate in the study. Participants were compensated £10 cash for their time and provided with snacks and coffee during the session.

For the purpose of this study, Keele University funded the purchase of two Apple Watches (Series 1, 38mm with black sport band). All participants were given the chance to use and experience the smartwatch for three days. The goal was to allow participants to experience and familiarise themselves with the smartwatch in a real-life context and give them the freedom of an uncontrolled environment. The participants were advised to go through the smartwatch functions, experience the features available, and take notes about what they most liked and disliked about the smartwatch.

This study is based on responses gathered from 23 students over four focus group sessions. We planned to have a minimum of six participants in each focus group session but invited eight in case any participants were unable to attend. Unfortunately, for objective reasons, we conducted the first session with five participants and the other three with six each. The total number of participants in the four focus group sessions was 23. Of the 23 participants, 7 were female. They ranged in age from 18 to 23, with a median age of 20.

Most participants described themselves as regular Apple smartphone users and had used the Apple smartphone for more than two years.

Each focus group session took place at Keele University, School of Computing and Mathematics in a conference room and ran for about 60 to 90 minutes. The participants were informed by email of the exact room one week prior to each focus group session. The focus group sessions were conducted by the first author assisted by another postgraduate student. The authors did not have any kind of prior relationship with the participants. The participants were given an information sheet that gave a clear description of the study and the participants rights and asked to fill in the consent prior to each session. All focus groups were audio-recorded, transcribed verbatim by the first author and reviewed by the second author. The research study was conducted in accordance with the ethical guidelines of Keele University and data protection to guarantee the confidentiality of personal data, thus codenames are used to identify the participants in the research.

The first author (moderator) followed a discussion guide developed jointly by the authors to direct the interactive discussion. The participants were first welcomed by the author, provided an introduction to the study and given the chance to ask any question before starting the discussion. The participants were asked questions about their first impressions of the Apple smartwatch, familiarity with the Apple smartwatch features, their usage, and what they liked or disliked. The participants were given the time and freedom to discuss their experiences and were asked to explain in detail what particular feature or app they liked or disliked about the Apple Watch. The discussion questions were designed to capture the participants' views of Apple smartwatch use. The discussion questions are described below.

- What is your first impression of the Apple Watch?
- Did you find Apple watch easy to use?
- How useful do you find Apple watch applications?
- Was there anything you particularly like or dislike about the Apple Watch?
- Is there any feature or app that would put you off using an Apple watch?
- Did you find Apple watch work as you expected?
- Do you think Apple Watch would be useful to you personally and if so in what way?

- When using smart phone with your smart watch – have you ever chosen not to install or update an application? If so why? Has privacy ever been part of your decision?
- Did you feel that is secure and safe to use contactless Apple Pay with your Apple watch?
- If you get the chance to use your Apple Watch to access government electronic services, would you think it is convenient? And what other apps or features that you think they would be useful?

The difference in demographic characteristics of focus groups participants were not included in this study, though we tried to minimize such effects on users' perceptions and judgments by inviting participants with similar demographic characteristics such as experience level (Not used Apple watch before), education level and age (18 to 24 years). However, if we recruited for example specific group of people with same demographics other than students and compare the results, it is difficult to tell whether this difference can be attributed to the demographic differences of the participants. To understand the demographic differences between focus groups participants, we believe that another in depth study is required. This limitation is discussed in section (6.10) for further details.

6.4.2 Anonymous Reddit Users' Comments

Expert users' opinions and views on the Apple smartwatch were collected from Reddit by examining a randomly selected set of posts and the related top-level comments in the smartwatch subcategory. Reddit is a user-generated social networking site where users share opinions and views on various topics. Reddit contains hundreds of sub-communities, recognised as sub-reddits and each sub-reddit covers a specific topic, such as technology, news, fitness or music. Registered users can address a topic with a post and discuss the topic by commenting on other users' posts. Reddit gives users the option to express their agreement with a post by voting on the comment. The post and comment data for six Apple Watch (Series 1) sub-reddits were collected through a web scraping software program called ParseHub. This tool saved a lot of time extracting data from the selected sub-reddits and provided it in a spreadsheet. All comments and posts posted between October 2015 and March 2016 were extracted. The reason for selecting this timeframe was due to the high volume of comments. The Apple Watch (Series 1) was released in April 2015. All the posts and comments extracted were manually investigated and checked by the authors. Through this qualitative review, the authors categorised the contents of the posts and comments and drew meaningful insights from them.

6.5 Data Analysis

To get a better understanding of the data, we employed a thematic analysis which offers a flexible approach to textual data assessment. It allows for the identification of major themes which are further described in the sub-sections. We also employed a content analysis approach to quantify the qualitative textual data and convert it into quantitative measures in order to interpret the data statistically and understand the perceptual differences between the two user types. The use of the mixed methods approach in this study draws from the strengths and minimises the weaknesses of the quantitative and qualitative research approaches. The themes drawn from the textual data are compared to each other to give common themes that represent both groups, in order to capture the differences and similarities of the perception of Apple Watch use. The sub-themes extracted from the textual data are compared to the textual data and we count the number of times participants address them positively or negatively.

To determine whether there is a significant difference in user's perceptions of Apple Watch features between novices and experts, the Chi-square test is used. This test determines whether frequency counts are distributed identically across populations (Tullis and Albert, 2013). The Chi-square test determines the difference in two population proportions, when the response variable has only two categorical outcomes and we compare two populations. We use the Chi-square test if the response variable has two categories and we wish to compare two independent populations. From the definition, we find that the Chi-square test is the most appropriate statistical method to find out whether there is a significant difference in views of Apple Watch features, since the variables are categorical and measured using a nominal scale. Statistical analysis of the data is conducted using the Statistical Package for Social Science (SPSS) for Windows (Version 13). The significant value (P) is pre-defined as less than (0.05). In conclusion, the analysis of the textual data collected from the novice and expert groups involves a combination of quantitative and qualitative methods.

6.5.1 Focus Group

NVivo software was used to code the verbatim transcripts and the data were analyzed using inductive thematic analysis. The four focus group transcriptions were input and analyzed in NVivo as a whole. Each focus group transcription was read carefully in order to become familiar with the data and identify the initial codes that capture significant user perspectives. In the first round of analysing the data, the authors identified 46 initial codes, and then these codes were developed and modified based on the raw data. The initial codes were predetermined and guided by the interview questions and Apple Watch features, to direct the textual analysis (Shannon, 2005). The authors went through the generated codes and examined them in an iterative way in order to collate them into preliminary themes that captured the essence of the focus group discussions. After modifying and developing the codes we were left with 27 sub-themes that represent important Apple smartwatch aspects. The sub-themes were classified and grouped into eight categories for further analysis, as shown in Table 6.1. The classifications and categorisation of the sub-themes were discussed by the authors, and compared to the raw data in order to reach a consensus (Guest, MacQueen and Namey, 2012). The authors read the textual data carefully and counted how many times each sub-theme was mentioned, positively or negatively, by the participants. All comments were assigned as either positive, when praise was given or good qualities described, or negative, when comments included criticism. This deductive enumeration of comments became the basis for theme comparison across the two user types, and the outcomes can be presented as quantitative results (Goetz and LeCompte, 1981) in order to statistically analyse and capture any perceptual differences between the two user types.

6.5.2 Anonymous Reddit Users' Comments

All textual data collected through the web scraping software program (ParseHub) were saved in an Excel spreadsheet. The authors thoroughly read the textual data and removed all jargon words and typographical errors from the users' comments and posts. We put effort into standardising the feature names found in the textual data. To deal with textual data extracted from Reddit, we used the same procedure as the focus group data. The sub-features found in the four groups were used to guide our analysis of the textual data gathered from the sub-reddits. The sub-features identified from the focus group data were compared to the textual data gathered from the sub-reddits. In-depth analysis of the textual data detected another three sub-features not identified in the focus groups and these were classified into one more theme. After categorising them further, we were left with 9 main themes (features) as shown in Table 6.1.

Table 6.1 Apple Watch features and sub-features emerging from the data

No	Main themes	Sub-themes				
1	Design	Watch size	Menu icons	Icon colours & graphics	Watch faces	
2	Applications and usefulness	Built-in apps	Third party apps	Apps usefulness		
3	Notification centre	Text messages	Weather	Calendar	E-mails	Social media
4	Screen	Screen Size	Resolution	Readability		
5	Health & fitness	HeartRate	Fitness tracking			
6	Battery & performance	Battery life	Performance	Storage		
7	Connectivity	Wireless	Bluetooth			
8	Interaction	Keypad	Siri	Force touch	Digital crown	
9	Dependency	iPhone dependency	Store dependency	Universal compatibility		

In conclusion, eight Apple Watch features were identified relating to the two populations, as shown in Table 6.1, (1 to 8), and one extra feature emerged from the analysis of the Reddit textual data. In the following section we present a short summary of the findings of the quantitative and qualitative analyses. These findings are divided into sub-sections reflecting the categories presented in Appendix C.

6.6 Results

The research questions come from analysing the qualitative data from four focus groups and sub-reddits comments. The analysis is split into two main areas, statistical analysis and qualitative analysis, which draws data from the focus groups and Reddit. This section presents the descriptive statistics and general findings from the data collected. The participants' demographics are presented in Section 6.4.1.

6.6.1 General Findings

The total number of negative and positive impressions collected from the focus groups and Reddit data were 1,489. Of these, the negative comments from both groups outnumbered the positive comments (60% to 40%). The expert group gave more negative comments (63%) than the novice group (37%). The total number of negative comments was 896. The number of positive comments given by the novice group (53%) was slightly higher than the expert group (47%), as shown in Table 6.2. Table 6.2 shows the total number of positive and negative comments by both groups for each Apple Watch feature. Clearly, applications & usefulness, notifications, and design were the features that received the highest number of comments from both groups. Obviously, of the total number of comments, notifications and applications & usefulness received the highest scores, 22% and 17%, respectively. The analysis of the Reddit data for the expert group generated more comments (56%) than the focus groups (44%), as shown in Figure 6.1.

Table 6.2: Total number of comments by both groups

`	Feature	Positive	%	Negative	%	Total	%
1	Applications & usefulness	118	37%	203	63%	321	22%
2	Notification	122	47%	137	53%	259	17%
3	Design	81	47%	92	53%	173	12%
4	Interaction	58	35%	107	65%	165	11%
5	Battery and performance	50	32%	108	68%	158	11%
6	Screen	58	41%	83	59%	141	9%
7	Health and fitness	53	50%	52	50%	105	7%
8	Connectivity	43	41%	61	59%	104	7%
9	Dependency	10	16%	53	84%	63	4%
	Total	**593**	40%	**896**	60%	1489	100%

The Chi-square test was used to test whether the novices and experts had the same distribution of preferences or if there was any significant difference between novices and experts for positive and negative comments on the Apple Watch. The statistical results indicate that, of the 26 Apple Watch sub-features examined, 15 show significant differences between novices and experts, as shown in Table: . In the following sub-sections, the Chi-square test results are presented and discussed in detail for each main feature and sub-feature.

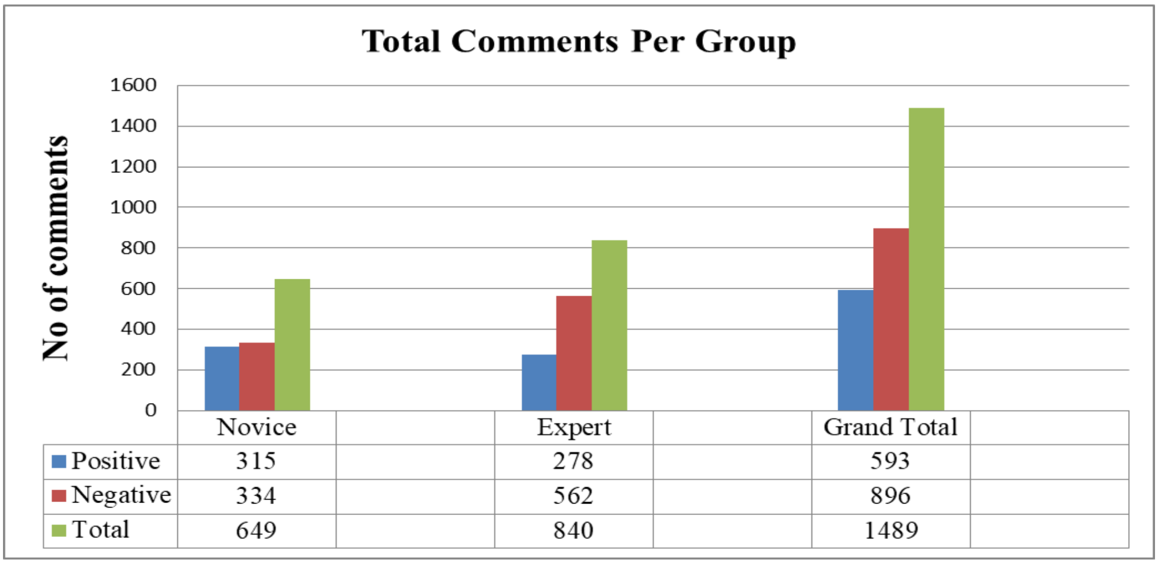

Figure 6.1: Comments per group

6.6.2 General Focus Group Findings

A total of 649 positive and negative novice group comments were coded from the four focus groups for the 27 relevant Apple Watch features, which were grouped into eight main Apple Watch features (1 to 8) as presented in Table 6.1. Of the 649 novice comments, 315 (49%) were positive and 334 (51%) were negative, as shown in Table 6.3. The highest total of positive and negative novice group comments referred to applications & usefulness and notification features, with 27% and 17% of the total respectively, as shown in Table 6.3. The less rated features were connectivity and health & fitness, with 7% each. The features that scored higher for positive comments than negative were notification, interaction, design, connectivity and health & fitness, as shown in Table 6.3. Battery and screen features were rated as negative almost twice as often as positive. Overall, the grand total for positive comments was slightly lower than the grand total of negative comments (49% to 51%).

Table 6.3: Focus group inputs for each Apple Watch feature

No	Feature	Novice Inputs				Total novice	%
		Positive	%	Negative	%		
1	Applications & usefulness	68	40%	104	60%	172	27%
2	Notification	72	66%	37	34%	109	17%
3	Interaction	40	50%	40	50%	80	12%
4	Battery and performance	20	29%	49	71%	69	11%
5	Screen	20	30%	46	70%	66	10%
6	Design	37	63%	22	37%	59	9%
7	Health and fitness	29	60%	19	40%	48	7%
8	Connectivity	29	63%	17	37%	46	7%
	Total	315	49%	334	51%	649	100%

6.6.3 General Reddit Data Findings

The analysis of the textual data collected from the sub-reddits produced a total of 840 positive and negative expert comments that matched the relevant 27 sub-features from the focus groups, with another 3 sub-features found from the analysis of the sub-reddits, making 30 sub-features. The data shows that of the 840 expert comments, 278 (33%) were positive and 562 (67%) were negative, as shown in Table 6.4. The highest number of positive and negative comments referred to notifications, applications & usefulness and design features, with 18%, 18% and 14% of comments respectively, as shown in Table 6.4. Eight of the nine features were rated negatively by the expert group, all except the screen feature. Overall, the Apple Watch features were rated more negatively with 67% negative ratings and 33% positive.

Table 6.4: Reddit inputs for each Apple Watch feature

No	Feature	Expert Inputs				Total expert	%
		Positive	%	Negative	%		
1	Notification	50	33%	100	67%	150	18%
2	Applications & usefulness	50	34%	99	66%	149	18%
3	Design	44	39%	70	61%	114	14%
4	Battery and performance	30	34%	59	66%	89	11%
5	Interaction	18	21%	67	79%	85	10%
6	Screen	38	51%	37	49%	75	9%
7	Dependency	10	16%	53	84%	63	8%
8	Connectivity	14	24%	44	76%	58	7%
9	Health and fitness	24	42%	33	58%	57	7%
10	Total	278	33%	562	67%	840	100%

6.6.4 Analysis and Results

The following sub-sections present basic statistics and highlight the important patterns emerging from the results. These findings are divided into 9 sub-sections based on the categories of Apple Watch features presented in Appendix C.

6.6.5 Design

The design of the Apple Watch contained four sub-features in the analysed textual data, as shown in Table 6.5. The sub-features that emerged from the analysis are, watch size, menu icons, colours and watch faces. There were a total of 173 comments related to the design sub-features (watch size, menu icons, colours and watch faces) which were either positive or negative. As per the Chi-squared test, a significant difference exists between the novice and expert groups with respect to total inputs of the four sub-features; χ^2 (1, N = 173) = 9.081 P = 0.003. The Chi-square test for each sub-feature reveals that only watch size shows a significant difference in positive and negative views between the two groups; χ^2 (1, N=70) = 11.173 P = 0.001. Testing each feature separately does not reveal a significant differences between the two groups with respect to menu icons, colours or watch faces, as shown in Table 6.5Table: Table 6.1. The total number of negative comments by both groups was higher than the positive comments, almost double (114 to 59). However, the percentage of novice user positive comments about the watch design feature was almost double that of the experts (46% to 24%). This indicates that the novice group praised this feature more than the expert group, despite the total number of negative comments. However, the percentage of expert user negative comments associated with the design feature was more than triple their positive comments. Most of the watch design sub-features were more appreciated by novice users, except colour, and this feature was perceived positively by the expert group, as seen in Table 6.5. It can be concluded that novice users see the design more positively than expert users, except the watch colours.

Table 6.5 Design feature statistical analysis

Main feature	Sub-feature	**User views**	**Groups**		**Chi**	**df**	**P-value**
			Novice	**Expert**			
Design	Watch size	Positive	22 (71%)	12 (31%)	11.173	1	0.001
		Negative	9 (29%)	27 (69%)			
	Menu icons	Positive	6 (67%)	9 (41%)	1.697	1	0.193
		Negative	3 (33%)	13 (59%)			
	Icon colours	Positive	3 (33%)	12 (57%)	1.429	1	0.232
		Negative	6 (67%)	9 (43%)			
	Watch faces	Positive	6 (60%)	11 (34%)	2.077	1	0.15
		Negative	4 (40%)	21 (66%)			
	Total design	Positive	37 (46%)	22 (24%)	9.081	1	0.003
		Negative	44 (54%)	70 (76%)			

6.6.6 Applications & Usefulness Feature

The applications & usefulness feature of the Apple Watch had three sub-features found in the analysed textual data. The sub-features coded from the analysis are built-in apps, third-party apps and apps usefulness. The two groups made a total of 321 comments associated with the application & usefulness sub-features (built-in apps, third-party apps and apps usefulness) which were divided into positive and negative. The Chi-squared test reveals no significant difference between the novice and expert groups with respect to the grand total of the four sub-features; χ2 (1, N = 321) = 1.227 P = 0.268. Testing for a significant difference between the two groups for each sub-feature reveals that only apps usefulness shows a significant difference in positive and negative views between the two groups; χ2 (1, N=102) = 4.292 P = 0.038. The other two features (built-in apps, third-party apps) do not show any significant difference between the two groups, as shown below in Table 6.6Table: Table 6.1.

Table 6.6: Application & usefulness feature statistical analysis

Main feature	Sub-feature	User views	Groups		Chi	df	P-value
			Novice	Expert			
Application usefulness	Built-in apps	Positive	57 (51%)	29(37%)	3.49	1	0.062
		Negative	55 (49%)	49 (63%)			
	Third party apps	Positive	3 (33%)	4 (20%)	0.603	1	0.438
		Negative	6 (67%)	16(80%)			
	Apps usefulness	Positive	8 (16%)	17(33%)	4.292	1	0.038
		Negative	43 (84%)	34 (67%)			
	Total	Positive	68 (40%)	50(34%)	1.227	1	0.268
		Negative	104 (60%)	99(66%)			

The total number of negative comments for both groups was higher than the positive comments by almost double (203 to 118). The percentage of novice user positive comments associated with the Apple Watch application usefulness feature is slightly higher than the expert group, at 40% and 34% respectively. The novice group comments were negative about almost all the sub-features of application usefulness except built-in apps. On the expert group side, the negative comments were close to double the positive. Both groups had a similar negative perceptions of the application usefulness of the Apple Watch.

6.6.7 Notifications

The analysis of the focus groups data identified five sub-features sharing characteristics and grouped them into one feature, notifications. The five sub-features coded from the analyzed texts are text messages, weather, calendar, email, and social media. A total of 259 comments were extracted from both groups relevant to the notification sub-features, positive and negative. The data reveals significant differences between the novice and expert group with respect to all sub-features, as shown in Table 6.7. The Chi-squared test reveals a highly significant difference between the novice and expert groups with respect to the grand total of the four sub-features; $\chi 2$ (1, N = 259) = 27.127 P = 0.001.

Table 6.7: Statistical analysis of notifications feature

Main feature	Sub-feature	User views	Groups		Chi	df	P-value
			Novice	Expert			
Notifications	Text messages	Positive	18 (78%)	14(40%)	8.215	1	0.004
		Negative	5 (22%)	21(60%)			
	Weather	Positive	17(74%)	8(38%)	5.74	1	0.017
		Negative	6(26%)	13(62%)			
	Calendar	Positive	11(61%)	13(31%)	4.775	1	0.029
		Negative	7(39%)	29(69%)			
	E-mails	Positive	13(59%)	7(29%)	4.182	1	0.041
		Negative	9 (41%)	17(71%)			
	Social media	Positive	13(57%)	8(29%)	4.073	1	0.044
		Negative	10(43%)	20(71%)			
	Total	Positive	72(66%)	50(33%)	27.127	1	0.001
		Negative	37(34%)	100(67%)			

The total number of negative comments is close to the number of positive comments for both groups (122 to 137). The percentage of novice group positive comments is roughly double that of the expert group (66% to 33%). However, the percentage of negative expert group comments is about double the novice group (67% to 34%). The novice group appraised the Apple Watch notification sub-features with a clear positive rating, as shown in Table 6.7, whereas the expert group rated all the sub-features negatively. The data analysis reveals that the two user types did not share a view of the notifications feature of the Apple Watch.

6.6.8 Screen

The screen feature emerged from the analysis of the focus group data, and contains three sub-features related to the Apple Watch screen properties, screen size, screen resolution and screen readability, as shown in Table 6.8. Both groups contributed a total of 141 negative and positive comments relevant to the screen sub-features. The Chi-square test reveals significant differences between the novice and expert groups with respect to all sub-features except readability, as shown in Table 6.8. The test indicates a significant difference in the total number of comments between novices and experts; $\chi 2$ (1, N = 141) = 6.012 P = 0.014.

Table 6.8: Statistical analysis of screen feature

Main feature	Sub-feature	User views	Groups		Chi	df	P-value
			Novice	Expert			
Screen	Size	Positive	8 (33%)	17 (63%)	4.464	1	0.035
		Negative	16 (67%)	10 (37%)			
	Resolution	Positive	7 (30%)	13(68%)	6.019	1	0.014
		Negative	16(70%)	6 (32%)			
	Readability	Positive	5 (26%)	8 (28%)	0.009	1	0.923
		Negative	14 (74%)	21(72%)			
	Total	Positive	20(30%)	38(51%)	6.012	1	0.014
		Negative	46(70%)	37(49%)			

The number of novice group positive comments was less than half the number of negative comments (30% to 70%). On the expert side, the positive comments were slightly higher than the negative (51% to 49%). The novice group assessed all the screen sub-features negatively, almost double their positive ratings, whereas the expert group rated them all positively except the readability sub-feature. Clearly, there is a perceptual difference between the groups towards the Apple Watch screen, with the expert group perceiving this feature more positively than the novice group.

6.6.9 Health & Fitness

The health and fitness category contain two relevant sub-features identified from the analysis of focus group data, heart rate and fitness tracking. The number of negative and positive comments extracted relevant to the health and fitness sub-features was 105. The Chi-square test reveals no significant differences between the novice and expert groups with respect to the total number of comments about the sub-features; $\chi 2$ (1, N = 105) = 3.495 P = 0.062, as shown in Table 6.9Table 6.8. However, the Chi-square test indicates a significant difference in the fitness tracking sub-feature between novices and experts; $\chi 2$ (1, N = 56) = 3.908 P = 0.048, but not heart rate, as shown in Table 6.9.

Table 6.9: Statistical analysis of health and fitness feature

Main feature	Sub-feature	User views	Groups		Chi	df	P-value
			Novice	Expert			
Health & fitness	Heart rate	Positive	9(39%)	7(27%)	0.827	1	0.363
		Negative	14(61%)	19(73%)			
	Fitness tracking	Positive	20(80%)	17(55%)	3.908	1	0.048
		Negative	5 (20%)	14 (45%)			
	Total	Positive	29(60%)	24(42%)	3.495	1	0.062
		Negative	19(40%)	33(58%)			

Interestingly, both groups share similar positive views towards the fitness tracking sub-features, and also similar negative opinions towards the heart rate sub-feature. Overall, the novice group found this feature more pleasant than the expert group (60% to 42%), as shown in Table 6.9. The total number of negative expert group views was higher than their positive views (58% to 42%), and this can be attributed to the higher negative rate given to heart rate sub-feature.

6.6.10 Battery & Performance

The battery and performance category contain three relevant sub-features extracted from the focus group data, battery life, performance and storage. A total of 159 negative and positive comments were coded into the three sub-features, battery life (37%), performance (38%) and storage (25%). The Chi-square test reveals no significant differences between the novice and expert groups with respect to the total number of comments of the sub-features; $\chi 2$ (1, N = 159) = 0.401 P = 0.527, as shown in Table 6.10Table 6.9Table 6.8. Testing the sub-features independently, the Chi-square test reveals no significant difference between the groups, as shown in Table 6.10.

Table 6.10: Statistical analysis of battery & performance feature

Main feature	Sub-feature	User views	Groups		Chi	df	P-value
			Novice	Expert			
Battery & performance	Battery life	Positive	8 (35%)	11(31%)	0.115	1	0.735
		Negative	15(65%)	25(69%)			
	Performance	Positive	5 (22%)	14(38%)	1.699	1	0.192
		Negative	18(78%)	23(62%)			
	Storage	Positive	7 (30%)	5 (31%)	0.003	1	0.957
		Negative	16 (70%)	11 (69%)			
	Total	Positive	20(29%)	30 (34%)	0.401	1	0.527
		Negative	49 (71%)	59(66%)			

The grand total shows that the novice group perceived most of the sub-features slightly less positively than the expert group (29% to 34%), but overall both groups share similar negative perceptions of the battery and performance features of the Apple Watch.

6.6.11 Connectivity

The connectivity feature of the Apple Watch had two related sub-features identified in the textual data, Wi-Fi and Bluetooth. A total of 104 negative and positive comments were coded into the two sub-features, Wi-Fi (46%) and Bluetooth (54%). The Chi-square test reveals significant differences between the novice and expert groups with respect to the total number of comments; $\chi 2$ (1, N = 104) = 16.012 P = 0.001, as shown in Table 6.11Table 6.9Table 6.8. The two sub-features of connectivity show also a significant difference between the groups, as shown in Table 6.11.

Table 6.11: Statistical analysis of connectivity feature

Main feature	Sub-feature	**User views**	**Groups**		**Chi**	**df**	**P-value**
			Novice	**Expert**			
Connectivity	Wi-Fi	Positive	16(70%)	5 (20%)	11.959	1	0.001
		Negative	7 (30%)	20 (80%)			
	Bluetooth	Positive	13(57%)	9 (27%)	4.861	1	0.027
		Negative	10(43%)	24(73%)			
	Total	Positive	29 (63%)	14 (24%)	16.012	1	0.001
		Negative	17 (37%)	44(76%)			

The two sub-features were rated more positively by the novice group almost double the expert group, but the expert group perceived both sub-features negatively, as shown in Table 6.11. Generally, the novice group showed a higher positive perception of the connectivity features than the expert group.

6.6.12 Interaction

The interaction feature of the Apple Watch contains four sub-features found in the analysed textual data, as shown in Table 6.12. The sub-features that emerged from the analysis are keypad, Siri, force touch and digital crown. The groups gave a total of 165 comments related to the interaction sub-features, both positive and negative. The Chi-squared test shows a significant difference between the novice and expert groups with respect to the total number of comments on the four sub-features; χ^2 (1, N = 165) = 14.089 P = 0.001. The Chi-square test with respect to each sub-feature reveals that all show a significant difference in positive and negative views between the two groups, except the keypad sub-feature for which no positive comments were found, as shown in Table 6.12. Table: Table 6.1The total number of negative comments for both groups was higher than the total number of positive comments (107 to 58).

Table 6.12: Statistical analysis of interaction feature

Main Feature	Sub-feature	User views	Groups		Chi	df	P-value
			Novice	Expert			
Interaction	Keypad	Positive	0	0	NA	1	NA
		Negative	11	7			
	Siri	Positive	13 (57%)	4 (16%)	7.302	1	0.007
		Negative	10 (43%)	21 (84%)			
	Force touch	Positive	14 (61%)	6(26%)	5.662	1	0.017
		Negative	9 (39%)	17 (74%)			
	Digital crown	Positive	13 (57%)	8 (27%)	4.851	1	0.028
		Negative	10 (43%)	22 (63%)			
	Total	Positive	40 (50%)	18 (21%)	14.089	1	0.001
		Negative	40 (50%)	67 (79%)			

However, the percentage of novice users' positive comments associated with the interaction feature was more than double that of the experts (50% to 21%). This indicates that the novice group praised the interaction feature more than the expert group, regardless the total number of negative comments. Almost all the watch interaction sub-features were appreciated by novice users, except the keypad sub-feature, where no evidence of positive ratings was found in the data. The expert group posts had more negative comments, almost three times the positive comments, and all three sub-features were rated negatively.

6.6.13 Dependency

Dependency is about the watch's reliance on other Apple devices for tasks where the Apple Watch cannot be configured or used on a standalone basis or using any device other than Apple. This feature consists of four sub-features found by analysing the Reddit textual data, as shown in Table 6.13Table 6.12. The sub-features that emerged from the analysis are iPhone dependency (tethering), Apple Store (no specific store for watch apps), and universal compatibility (Apple Watch cannot be used with any other devices than Apple iPhone). The expert group made a total of 63 comments related to the dependency sub-features, both positive and negative. No evidence about this feature came from the focus group data except the pairing issues encountered by respondents. Therefore, the Chi-squared test is not applicable in this case. Table: Table 6.1The total number of negative comments made by the expert group was higher than the total number of positive comments (10 to 53). Overall, this feature was perceived negatively by the expert group.

Table 6.13: Dependency feature frequency rates

Main feature	Sub-feature	User views	Groups	
			Novice	Expert
Dependency	iPhone dependency	Positive	0	7
		Negative	0	23
	Apple Store dependency	Positive	0	3
		Negative	0	17
	Universal compatibility	Positive	0	0
		Negative	0	13
	Total	Positive	0	10
		Negative	0	53

6.6.14 Summary of the Results

This section presents a summary of the qualitative results for the novice and experts' users of the Apple Watch. The statistical results reveal a significant difference for some of the Apple Watch features examined, as described above.Table: In conclusion, of the 26 Apple Watch sub-features examined statistically, 15 show significant differences between novice and expert users, as shown in the Chi-Square results (Table: Appendix C). Moreover, comparison between positive and negative comments reveals that the novices were more satisfied with notifications (66%), connectivity (63%), design (63%) and health & fitness (60%), while the experts only praised the screen (51%). However, the novice group perceived battery & performance (71%), screen (70%) and apps & usefulness (60%) less favourably, while the expert group were not satisfied either, and view all Apple Watch features negatively, except the screen feature. The grand total of the positive novice comments was higher than the expert group. Overall, we can conclude that the analysis reveals a clear difference between the groups' perceptions of Apple Watch use.

Interestingly, the novice group had a more positive experience than the expert group in terms of the total number of positive comments.

6.7 Discussion and Findings

This section discusses the findings of the quantitative and qualitative analysis including the differences and similarities between the novice and expert users. To add an additional layer of quality to our findings and to get insight into the perceptions of the novice and expert group, the authors present some quotes to support the significant findings of the qualitative review.

6.7.1 Design

The design of any device includes its shape, colour and layout (Chin, Diehl & Norman 1988). The design can influence users' perceptions and experiences of using smartwatches. The analysis of the transcribed focus group data reveals that the Apple Watch design enhanced the positive experiences of the novice group and influenced their positive ratings, as mentioned here by P2-1: "*Watch buttons and concept are impressive*"; "*menu icons and watch faces are very attractive*". The novice group was very positive about the Apple Watch design except for the icon colours. The novice group reported that the icon colours were meaningless and didn't add anything to the watch, as outlined by P5-2: "*Icon colours are very similar to my iPhone icons which don't add anything to watch*"; and P4-4: "*I didn't get the meaning of the icon with multi-coloured circles a lot of colours without any meaning for me*". For this reason, some participants looked for icons where the colour conveyed information and allowed them to get a meaningful message from that colour at first glance without a need to read, as mentioned by P5-3: "*icons colour and graphics should give meaningful information especially on small device like watch as you can barely read texts*". Apple smartwatch designers should consider the importance of colour in design for drawing users' attention to things that are significant in order to enrich the user experience.

On the other hand, the expert group found the Apple Watch design not to be pleasing, and this reflects on their overall perception of the design aspect. The expert group made more negative comments about the watch size and watch faces sub-features, contributing to their overall dissatisfaction with the Apple Watch design, as outlined here by C1: "*I have to say that I am a bit disappointed with watch size, it looks so small on my wrist*"; and C5: "*Number of watch faces are very limited and my biggest gripe is how hard to get back to the watch face*". Also, a few comments pointed out that the watch size and shape were not suitable for some settings such as work, as observed by C23: "*Watch looks very sporty, its size and shape not fit with my professional work, it doesn't have a mix design between the classic watches and digital ones*". Several participants indicated in their comments that the smartwatch should be a mixed design between classic and digital with various designs to be worn in different circumstances. Smartwatches are considered by most adopters to be a mix between fashion and technology, rather than just a piece of technology, therefore designers need to not limit their design to functional components without taking the fashion aspect into account.

Clearly, the novice group were more enamoured of the Apple Watch design features than the expert group, with more positive comments reported. This can be attributed to the novice group having less interaction with the Apple smartwatch, so they experienced fewer issues, as outlined by P5-4: "*I also haven't gotten enough time to really know where it adds a whole lot of value*". The power of first impressions of any brand or media has an influence on users' opinions (Schivinski and Dabrowski, 2012) and can affect their judgment, as pointed out by P1-3: "*I just remember when I heard about Apple Watch my impression was 'wow' and was wishing to have one*"; and P5-4: "*My first impressions was very good, as Apple always introduce great devices*". Also, users' background knowledge and experience varies, and this might be another reason for the differences between the groups. The novice users seemed to be more attracted to the design of the Apple Watch, whereas the experts had a remarkably low interest. Therefore, smartwatch designers need to rethink the design, with consideration of users' background knowledge and experience, in order to match their individual needs. Good design can support the interaction between the user and the product, therefore designers should ensure that the smartwatch is well designed based on user needs, in order to support this interaction.

6.7.2 Applications and Usefulness

There are number of built-in applications that come with the Apple Watch to help users do certain tasks and connect with iPhone core functions such as phone calls, camera, Siri, music and photos. Also, the Apple Watch allows users to run third party apps that are compatible with WatchOS Version 5 such as Citymapper, Workflow, and many others. These apps can be used in various settings based on user needs. Some users find them convenient, while others find they do not fit with the screen size. The statistical analysis reveals no significant difference between the novice and expert groups except for the apps usefulness sub-feature. The results indicate that, to some extent, the novice group valued the built-in apps but not the third-party apps which they didn't perceive as useful. Meanwhile, the expert group were very frustrated with the Apple Watch applications and its usefulness. The overall opinion of both groups was similar, as they perceive the smartwatch applications as not fitting their expectations and most as not useful. Through textual data analysis we identified a number of reasons for novice users' negative perceptions of the Apple Watch apps. One reason is that built in apps do not deliver any extra value to users, who argue that smartwatch apps are actually duplicates of those on the smartphone, as pointed out by P2-3: "*It is pretty the same like iPhone so why I have to carry two devices that do mostly the same tasks*". Others found the apps did not improve their productivity or meet their productivity goals, as outlined by P4-6: "*I went through some of apps given by Apple Watch but arguably how many of these apps are realistically improve my productive in my daily life*". We also came across usability issues. Some participants pointed out an ease of use issue, with some apps being confusing and difficult to use from their point of view, such as the music app encountered by P4-1: "*I am not sure but the music app looks have an issue as there is no button to see more from this artist, and that confused me. The app is not very straightforward, really strange*". Some participants were satisfied with some apps, such as answering and making calls, for example P4-3 said: "*Receiving and answering calls are my favourite, you feel too cool using them, but you need to be in private place like home*".

On the other hand, the expert group encountered some other issues when interacting with the Apple Watch apps. Some of the posts pointed out a privacy issue, as most third-party apps ask for permission to access resources on the watch during the installation process, such as asking for location or Apple Pay. The expert group showed a negative attitude toward the use of third party apps as they had no control and the apps may have harmed their privacy, with no guidance available, as one poster, C23, mentioned: "*One of news app that I downloaded it asks me for my permission to access my location and address book, I am not sure if that information could be used in non-helpful way*". Another comment, from C39, said: "*If I granted access to my contacts for one time and then later, I cancelled it, is the app still able to keep my data I have shared before. Really these things need to be explained*". Other posts reveal that the expert group shared the same feelings as the novice groups about applications and usefulness, for example their experience of the music app, drawn from a post by C56: "*The music app is messy in some spots*". Some expert users saw the map app as a distracting feature of the Apple Watch, that may distract their attention from focusing on the road, especially when walking in cities, and maybe put their lives in danger, as pointed out by C21: "*I believe that map app is too dangerous, I found it distracts my attention mainly when I used it in cities*". Designers and developers must ensure that apps are free from any kind of risk to users and must alert them about dangerous situations they may encounter while using the app. Moreover, application developers should ensure that smartwatch applications are practical, effective and easy to use, with minimal action required and error free. The features given in any applications must be consistent to prevent users from getting confused or losing interest. We suggest that smartwatch app designers pay attention to reducing users' perceptions of privacy and security risk. For apps that over-request privacy-sensitive permission to work, developers should clarify in simple, clear language why the app requests such permissions in order to reduce users' perceptions of privacy risk.

6.7.3 Notification

The results reveal that the groups had different perceptions of the notifications feature of the Apple Watch. The novice group rated all the sub-features positively, whereas the expert group showed negative reactions to the notification sub-features. From the textual data analysis, we came across some interesting comments by novice participants showing their preferences regarding these features. The novice users found that notifications from text messages, the weather app and calendar were more convenient than other apps, as can be concluded from the higher positive ratings and participants comments, for example P2-1 said: "*If you are at your class, it would be helpful to have a glance on your calendar to check your next class and check your text messages notifications that maybe important*". Also, the novice participants found that receiving notifications on the wrist can inform them about a wide range of information, including new messages, upcoming meetings or the weather, and can save the time of picking up their iPhones, as outlined by P3-2: "*Receiving notifications on my wrist save me a lot of time especially when I follow up my meetings and checking weather*"; and P3-4: "*getting notifications from different apps are quite useful and time saver, as you don't have to pick up your phone from your pocket every time you receive a message or email*". However, some participants pointed out that they wanted to limit the amount of notifications they received in some circumstances, as they found some unimportant and too annoying, as mentioned by P1-2: "*Notifications are useful feature to have even though some of notifications are not important and annoying*"; and P5-2: "*Some notifications are disturbing, I need to receive only important notifications from some applications*".

Far more negative comments related to notifications were generated by the experts, and this can be attributed to some usability and design issues. One post shows user frustration at having to keep both devices' notifications active at the same time, as outlined by C95: "*I would like have the option of notifications coming through on my watch, but not my iPhone. But that could get annoying having to activate/deactivate it in two places*". C114 commented regarding missing notifications from the email app: "*I can't seem to get an email notification though*". Also, some posts mentioned difficulties using notifications, such as this from C266: "*I've had a few emails throughout the day, and they don't seem to pop up in notifications. Swipe down to acknowledge a notification, it took me a while to figure out how to say, ok I see the text message, you can take it away now*". Another general reason that may have led the experts to rate notifications poorly is over-familiarisation, as over time the device seems more normal. Our suggestion to designers is to reduce the notification frequency and give the user more options to easily configure the times and types of notifications received. Also, we recommend that developers apply features that make users feel in control when interacting with notifications and give users the final say in how and when they are notified. Developers should focus on providing users with a good notification experience that relies on quick information gathering and lets them interact easily and quickly rather than distracting them from their day-to-day lives.

6.7.4 Screen

The results clearly show that the groups had different perceptions of the Apple Watch screen and its sub-features. The novice users had an unpleasant experience during their interaction with the Apple Watch screen, as indicated by the higher negative ratings. Generally, this can be attributed to the novice group finding the screen the easiest way to interact with the Apple Watch, despite other interaction options such as digital crown and Siri. They therefore experienced some usability issues. Through analysis of the novice comments we conclude that the screen size is something that may limit their interaction experience. Some novice participants reported that the screen size had a significant effect on their efficiency of completing some tasks, as reported by P1-1: "*I found it hard to input the passcode number in small screen. It took longer time to type the right pin to unlock the watch, always clicking wrong number buttons*"; and P3-2: "*I feel that tiny screen is not worth use it, the time you spend to navigate and the hassle to reply on messages make me not think even to use it anymore*". The Apple Watch screen size makes it difficult for some users to navigate between apps, as pointed out by P2-4: "*I felt it's difficult to scroll between the apps with small screen*". The participants' comments above show that the screen efficiency issue can very much undermine the perception of the Apple Watch usability, and consequently considerably limit the interaction experience. The Apple Watch resolution was quite disappointing for the novice group, as they found the overall quality for viewing images and pictures very poor, as pointed out by P6-3: "*Viewing photos is useless and I don't know if there is a proper way to do it, but when I try them was shocked of the low photo quality*"; and P5-4: "*Browsing photos is not a good option to use on watch as you can't see photos clearly*". Readability is about how easily users can read text and other content on the smartwatch. The novice participants experienced difficulty checking and reading messages or emails on the smartwatch, which is worn on the wrist. The participants chose not to read full messages because of the inconvenient reading pose, instead they chose to glance at the watch and then read the full text on their iPhones, as mentioned by P2-4: "*To be honest, replying and reading messages annoyed me because I have to left my wrist closer to my face to be able to read messages or emails, I prefer reading messages with iPhone but the watch wasn't that easy for me*". Another issue reported by the participants was that when they read text messages on the smartwatch, scrolling up and down by finger blocked them from reading the text, meaning either they could not read the message or they clicked on unwanted selections, as pointed out by P2-1: "*It wasn't easy for me to scroll up or down and read messages especially if you have too pudgy finger, I can't see what I am reading and sometimes I click on wrong button*".

The expert comments for the screen feature were slightly more positive, led by the positive comments about screen size and resolution sub-features, whereas the readability sub-feature comments were more negative. The differences between the groups' perceptions of the screen size and resolution can be attributed to experts being able to overcome their initial frustrations through work-around solutions using other functions such as the digital crown or Siri to navigate quickly without the need to interact with the touchscreen, as stated by C42: "*After a short period of use it did seem to be a suitable size for what it is, watch crown looks to be more useful than force touch*". Many of the negative comments about the screen referred to the readability issue, where users wanted to make sure they could read what was required with a single glance, as pointed out by C57: "*definitely not something I'd do too much reading or even photo viewing on, only quick glance for some messages, as it too small and strains the eyes*". Some participants faced a readability issue when they tried to make normal fonts so large the text wouldn't fit on the screen, as pointed out by C77: "*Increasing the font size doesn't fit with screen size, I have to scroll left and right to read the text*".

Based on the above comments, it is clear that screen size, resolution and readability sub-features have a great influence on users' perceptions of the Apple Watch and the information communicated through it.

Accordingly, we understand that users failed to accomplish some tasks in a reasonable time or accurately, interacting with the smartwatch screen, as they found the touchscreen not to be efficient in some circumstances. The Apple Watch touchscreen was found to be a significant feature affecting users' interaction experience and efficiency in accomplishing tasks. Similarly, it can make a difference for designers, as it can influence their design decisions. The screen size makes designers compress information to fit the tiny screen, making text illegible. Moreover, smartwatch users may accidently touch the wrong buttons due to the size of the touchscreen, and these accidental touches require designers to make a simple way of correcting them such as a back control or undo button, which is not provided on the Apple Watch.

Devices with small displays, such as the Apple Watch, might be better supporting swipe gestures (moving the fingers across the screen in a horizontal or vertical direction) to enhance the user interaction experience, rather than forcing users to touch small buttons. Designers should focus on understanding the capability of their touchscreen, what it was designed to do, and its limitations. The touchscreen is designed to allow users to complete tasks as quickly and easily as possible in order to improve their interaction experience, avoiding too many options that may confuse or frustrate them. All operations done through the touchscreen should be visible and understandable, not confuse users or force them to try touching everything on the screen just to find out what are touchable and non-touchable objects. Developers should avoid making users perceive the Apple Watch as an extra screen for the iPhone device.

6.7.5 Health & Fitness

The results show that both groups shared a similar positive view of the fitness tracking sub-features, and a similar negative judgment about the heart rate sub-feature. However, the novice group were more attracted by the fitness tracking feature than the expert group. Apple Watch has two main fitness apps, activity and workout, which both collect fitness data and synchronise it to the iPhone to give a holistic view of the user's health on the iPhone device. Novice users mentioned some motives for their interest in using the Apple Watch for fitness tracking. Some were interested in checking their daily activity (e.g., calories consumed and step counts) or moving their body more. Others stated that they were satisfied with having information about themselves, as pointed out by P3-1: "*For me, it's changed my life because it's given me motivation to get in shape, I keep track on calories I burned and remind me to move when I sit for long time*"; and P6-3: "*Activity tracking has been a surprise for me, I wasn't imagine to like it, one thing I really like is that it tracks exactly calories you burn throughout the entire day*". On the other hand, some participants questioned its accuracy at measuring running distances, as mentioned by P6-3: "*overall I found fitness tracker is amazing, but I found some readings not accurate*".

The novice participants reported the same accuracy issue with the heart sensor, as variations in heart beat were observed and sometime no readings were detected when the sensor was either not in direct contact or too tight against the skin. Some participants wondered about the heart sensor readings, and how they could deal with low or high readings, as no help was provided, as P2-2commented: "*I went to check my heart rate and that made me worried and confused as wasn't sure what should I do, it kept showing different readings every time and I wasn't sure if it's accurate or not*".

The results reveal that the expert group was satisfied about the fitness tracker but not the novice group. This can be attributed to the expert group interacting more with this feature than the novice group, so they experienced more issues. Some participants reported that using the Apple Watch was a convenient and fun way to track their fitness activities, as pointed out by C255: "*Fitness tracking is really nice to use while running… the watch makes keeping track of health and fitness stats more fun*". Other users said that occasional notifications about their physical movement status helped them refresh themselves during long work hours, as C311 explained: "*I like the fitness reminder of this feature when reminds me to stand up if I sit for long time, it helps me to refresh myself*".

Some users were disappointed by the limited fitness app's ability to support various sports activities, such as cycling, as mentioned by C254: "*Hopefully there is an app for cycling that can show your speed, etc*". Some posts indicate that users were disappointed as their health data could not be shared with other devices. C368 said: "*I will say that at this point Apple doesn't share health data between devices, so you may be disappointed if you want to use your other iPhone and iPad to look at your health data*". The heart rate app caused more frustration for the expert group, as heart rate readings varied which made them worried about how to handle the unreliable readings, as discussed by C114: "*By looking at my heart beat readings, I felt not confident to trust these different readings, if I have a heart problem history, I would be more panic and may sought medical attention*".

Apple Watch health and fitness feature makes it easy for most users to learn about their health and track their physical activities. It was perceived as a convenient way to keep tracking of fitness and activity. Some issues were reported by the participants that hindered their interaction experience and caused frustration. The device used to count steps is unreliable, as it may make assumptions that a step has been taken when it is just quivering a leg. This may lead users to lose confidence in the fitness tracker if there are differences noticed between the trackers' measurements and the users' perceptions. Therefore, fitness trackers need alternative measures that are perceived as easy to understand and accurate for the user. Designers should consider that users' preferences vary from one to another, and their needs change over time and even throughout the day. Therefore, it is necessary for the fitness tracker app to have a feedback system that can support trainers with exercises or allow them to share information with a personal trainer or anyone from whom the user seeks guidance. This would give users more control over their fitness and health data and promote competition, as they could share workout experience with friends or family members.

6.7.6 Battery & Performance

The statistical analysis reveals that both groups shared similar negative perceptions of the battery and performance feature of the Apple Watch. Both groups found that the watch had long loading times of applications and a short battery life below their expectations. Limited battery power was a commonly reported issue by most of the participants. The battery last less than a day of average use. Some participants said that the short in battery life was caused by some apps that drain the battery such as music apps, according to P1-4: "*I am very disappointed with the battery life, listening to music and making calls consume the battery very fast*". The watch size limits the internal storage, as is the case for most smartwatches. A lot of users where not happy about the limited storage of the watch and this is seen in many comments, such as P5-1: "*It's very limited and useless when there is not enough storage*". Some novice participants perceived the smartwatch's performance as very low in loading apps, as pointed out by [P1-3]: "*It is too slow. It just takes forever to open apps on it, not work as expected*". It also crashes a lot, which might be due to the technical limitations of the Apple Watch, as commented by P2-3: "*Sometimes it becomes unresponsive and freezes a lot*"; and P4-4: "*The performance is so bad that makes you frustrated trying to use it*".

The expert group expressed their disappointment with the Apple Watch battery performance, as stated by C271: "*Battery life is really starting to be a problem, I couldn't track more than two hours of workouts, without the battery dying completely*". Also, the watch's performance in loading apps was poor and made users feel it was unusable, as commented by C323: "*Apps loading time is more than I expected, take longer time than iPhone, it's beginning to be unusable*". Poor performance may influence user effectiveness in accomplishing some tasks and may lead them to give up using certain apps. Also, user efficiency may decrease during the interaction as the time needed to accomplish tasks using the Apple Watch is affected by poor performance.

Designers should not trade-off smartwatch performance for animations and fancy graphics. They should strike a balance between meeting the needs of the user and the limitations of the technology they are designing for. However, designers can still influence how users perceive the low performance and battery life. Smartwatch designers should show status bars or icons when an app is loading, so users know there is an activity running and do not think the application is unresponsive. Also, a recent approach has been introduced to smartwatches, bot technology, which only requires basic storage and processing power to process images and texts. This technology is much better than apps for many reasons, for example, bots need less processing power, no videos needed to load, there is no interface to learn, The user only needs to send a text based message or basic voice command to the company server hosting the bot service (Looper, 2016).

6.7.7 Connectivity

The Apple Watch comes with Bluetooth and Wi-Fi and connects to a paired iPhone to complement its cellular communication capabilities. The smart watch switches between Bluetooth and Wi-Fi to select the most efficient connection in order to save battery power.

The novice group's comments indicate that most participants had a good connectivity experience of the Apple Watch. There were some participants who showed concern about some of usability issues they encountered such as slow connection when retrieving data from the paired device, or a lack of appropriate synchronisation and coordination. This was perceived by P3-1: "*I found it sometimes very slow in synchronizing photos or browsing them and it keeps disconnecting*". Some users perceived using Bluetooth and Wi-Fi to communicate with the paired iPhone as unsafe when using Apple Pay, as stated by P5-1: "*Wouldn't necessarily use Apple Pay on my watch if it's paired with my iPhone through Bluetooth, I don't feel it safe enough*".

On the other hand, the expert group were less satisfied with the Apple Watch connectivity, as most experienced poor or slow connection. Many users faced connectivity issues on their Apple Watch and were not able to interact or do some tasks efficiently, as mentioned by C386: "*My Apple Watch says network connection lost when I get on email or* *notifications. It works after restarting it*". Others experienced the same when updating the smartwatch as said by C396 "*I lost connection many times and interrupted the watch update, it kept restarting, doesn't make sense*". Losing connectivity can be due to problems with the device itself or the users moving the smartwatch away from the paired iPhone or out of Wi-Fi range. Whether losing connectivity is due to the users or the device itself, Apple developers should provide some support and suggestions to resolve such issue without making users speculate about the problem or think it is more complicated. Users should get very quick and sufficient help to guide them through avoiding or solving issues. Developers should focus on increasing the ability of users to solve most expected issues very quickly and efficiently.

6.7.8 Interaction

The first release of the Apple Watch introduced two new input methods, force touch and digital crown, alongside the keypad and voice recognition (Siri). These input methods are a kind of control tool to help users interact with and control the smartwatch.

Based on the analysis of the statistical results, we found a significant difference between novice and expert users' opinions about the three sub-features, except the keypad where a statistical test was not applicable. The novice users rated three of the four input methods slightly positively, except the keypad which was rated negatively only with no evidence found of positive comments.

The analysis of the novice group data revealed some qualitative insights about the participants' thoughts and concerns about the sub-features. There were a few common issues stated by the participants. There was common confusion about how to use the digital crown and touch force. These two input controls require some knowledge and in order to use them you need to find hidden shortcuts that are not announced by Apple. The force touch and digital crown confused many users who were not sure when to use them, as stated by P3-3: "*Somewhat I was confused and lost to use force touch, do I tap it or force touch the screen… for how long I should press on the screen*"; and P4-3: "*The digital crown movement and feel is just beautiful and it feels like a quality piece of watch, but I was lost when I use it, not sure is it single-press, double-press or press-and-hold and when should I use it*". Even though users seemed to like the digital crown, they were uncertain how to use it and navigate the watch. Many users also found that typing on the watch was not very helpful or efficient. Using the scribble app to reply to a message took longer with the tiny screen, as stated by P4-1: "*In some iMessage messages, reply by scribble took longer time from me than on my iPhone, seemed too slow to write full sentence and no space to write*". Users reported frustration with the watch being slow to respond, and the scribble app failed to recognise some scribbles.

Some users indicated that using the voice control, Siri, instead of fingers allowed hands-free interaction, despite the small delay in voice recognition encountered by some and the inconvenience of using it in a crowd, as stated by P1-2: "*Using Siri is cute way to reply on messages and good way to make calls but I feel it will be embarrassing to use it in crowd*". On the other hand, the expert users found interaction with the input methods of the watch was not practical, and this impacted their overall experience. The digital crown was considered by most users a good addition to the smartwatch design with a classical look, but it didn't give the users a smooth or accurate rotating experience, and there was not much support provided, as mentioned by C189: "*I'm not sure if this happen to other but I found crown was light stickiness every time I rotate it and not hit exactly what you want*".

Lack of accuracy and misinterpretation by the voice recognition (Siri) were reported by most expert users, as well some languages not being supported, as mentioned by C243: "*Siri wasn't that helpful, I find it cumbersome, not able to distinguish between some words*". This could be attributed to the varying accents of users or background noise interference.

Overall, both groups shared similar negative views of the input methods of the Apple Watch. The voice input, scribble and force touch were all limited and caused inconvenience to most users, reducing their interaction experience.

Smartwatch designers should consider how interaction with a small display might be better if they introduce hands-free interaction or body-based gesture inputs that do not require the fingers or hands to be used on the display (Heo, 2017). Smartwatch designers are recommended to provide users with interaction methods that fit with various settings to enrich users' experiences and allow them to feel in control. The more they feel in control the more they will like the experience and decreasing user uncertainty lessens the risk of frustration.

6.7.9 Dependency

Apple Watch Series 1 requires wireless connection to an iPhone to do most tasks such as stream music, send messages or perform other functions. Apple Watch Series 1 is a non-cellular model that only allows users to get data when the watch is connected to Wi-Fi or an iPhone device. Many users' posts on Reddit were negative about the smartwatch's reliance on the iPhone. Some users perceived the smartwatch as a diminutive iPhone on the wrist that runs almost identical functions to the iPhone, as mentioned by C432: "*How the watch is work makes me not interested in it because there is no specific task Apple Watch can do that can't be done by an iPhone*"; and C354: "*Not personally, I wouldn't use it like a mini iPhone on my wrist*".

Some users reported that the reason for the lack of useful third-party apps was the absence of a watch app store. Some users felt that an Apple Watch app store was essential and could stand alone, as mentioned by C518: "*I thought that watch comes with its own store app but I have to download apps via iPhone, and still not many useful apps available there*"; and C548: "*If the watch has its own store app we can see many useful apps available*". A lack of compatibility with other devices was also seen as a barrier and limited their ability to use accessories such as power bank, headphones and other apps that only work with certain models of iPhone, iPad, or iPod Touch.

Actually, the Apple Watch was designed to operate in tandem with an Apple smartphone, not as a standalone device. Apple, with its current design, put some effort into differentiating the smartwatch from an iPhone, but it still does not totally reflect or represent users' perceptions or opinions about using the smartwatch. This can be attributed to smartwatch designers imitating their iPhone interaction methods, and directly porting to the smartwatch without considering the size of the smartwatch or its functionality. Designers should focus on allowing users to access the smartwatch without interrupting their daily tasks such as when jogging, running or holding something in their hand. However, the current interaction methods of the Apple smartwatch interrupt users and make them pay full attention to the smartwatch. Therefore, Apple smartwatch designers should consider redesigning the smartwatch interaction methods to not interrupt users' daily activities. The designers should take advantage of the smartwatch's fixed position on the wrist of the user to get information about the hand orientation and wrist movement.

This information could be analysed to improve the smart interactions and adapt to the user's hand orientation and activity level, in order to give users more control over the interaction in several activity contexts. Designers could implement body gesture interaction methods such as head, eye and face movement. For example, head movement could be used to make the watch to do some tasks and enhance users' hands-free input.

6.8 Qualitative Review of Users Perceptions of Apple Watch Security and Privacy

Intentionally, we allocate a separate section the in-depth analysis of users' perceptions of the Apple Watch security and privacy, in order to highlight its importance from a user perspective.

As we have seen, the Apple smartwatch has the ability to collect data, and process and communicate them to an iPhone device through Wi-Fi and Bluetooth. As they become more prevalent, Apple can store sensitive information such as locations or credit card details (Apple Pay) or unlock cars with the remote features of the smartwatch. These functions could allow attackers to breach user security and obtain private data in order to gain access to sensitive user data such as position, text messages and personal financial information. Smartwatches are becoming more attractive for attackers, as there is insufficient authentication, a lack of encryption, and privacy concerns (Karakaya, Bostan and Gökçay, 2016). To gain in-depth insights into user perceptions of Apple Watch security and privacy, we analysed the data for both user type's security and privacy concerns. The analysis of the qualitative data reveals some privacy and security concerns.

The Apple Watch collects a lot of information about its users, including personal details, locations visited, health data and financial information. Depending on the apps installed, there is a lot of personal information saved on a smartwatch. The novice participants were generally reticent to do some tasks on the smartwatch, mainly money-related tasks, or provide personal information, as mentioned by P4-2: "*There is a lot of important personal information being passed through my watch, and I don't feel safe to use Apple Pay for shopping*". This is related to users' mistrust of certain apps and the weaknesses in the current connectivity features of the Apple Watch such as Wi-Fi and Bluetooth, when connected to an iPhone. The users seemed to have a misconception about these connectivity functions, feeling they were easily hacked, especially Bluetooth, as mentioned by P5-1: "*Wouldn't necessarily use Apple Pay on my watch if it's paired with my iPhone through Bluetooth, I don't feel it safe enough*". This misconception might be related to a misunderstanding of how Bluetooth communication works and a lack of information provided by Apple to educate users about the protocols of such technology. Also, some participants mentioned that the Apple Watch has no anti-virus or other protection software, as stated by P4-4: "*What I see that Apple didn't release any anti-virus software for its products even smartwatch, other brands has its own, still don't understand why*". Users, especially those with less experience and knowledge, perceived more protection and trustworthiness in a device if there was software or other features to prevent any potential breach. Users felt that the authentication methods used on the watch were not sufficient in case the watch got lost or stolen, as explained by P6-1: "*I am worried about if the watch is lost or stolen. I feel the passcode is not secure enough*". The participants knew that the Apple Watch Series 1 doesn't have GPS to track the watch if it gets lost or stolen, as is the case for an iPhone.

The novice participants were asked the reason for not installing or updating applications and are their decisions were related to privacy. Most participants mentioned the lack of storage and the time required, as was the case with P3-1: "*It all depends on my storage and time needed to install updates*"; or they were forced to do updates, as was the case with P3-2: "*If you didn't do the updates some features won't work and your device keep freezing or stop working*". A few participants felt sincerely confused about what data apps can and can't access and most available descriptions were misleading, as was the case with P4-2: "*Some apps are confusing when installing them, really I don't know when to give access and when should not*". There is an increase in the number of control functions used to manage app permissions, which add together and force users to make impossible decisions. The lack of usability of apps such as Apple Pay, and other sensitive functions of the smartwatch make users less comfortable and not secure. The novice users' privacy and security perceptions of the Apple Watch were influenced by factors such as their education, absence of security indicators, and a review system to help them through the decision process.

On the other hand, we found a few posts that explain how expert users perceive the privacy and security of the Apple Watch. Some relating to app permissions are discussed in Section 6.7.2. Others are discussed in detail here.

Some posts mentioned that it's not smart to walk around with a device that contains personal information without enough authentication as it may be an easy target for any attacker, as stated by C542: "*I really think it's not smart to have only 4 digits passcode, as it's always connected to my iPhone through Bluetooth and Wi-Fi… they should add more authentication like two-factor authentication*".

There were a few comments about the usability of the 4-digit passcode and how inconvenient it would be to enter 4 numerical passwords on a small screen. The user may even disable or bypass this function to feel more comfortable, as expressed by C611: "*Sometimes accidently I clicked on wrong buttons when I input the passcode to unlock my watch but I turned it off and used my iPhone to unlock it*".

The smartwatch also has the ability to remotely unlock and control certain brands of cars, TVs, and smart-homes. For instance, the Apple Watch can be used to unlock cars and control some Apple appliances (Hite, Fontana & Williams 2015). Some posts identified expert users' worries about devices being lost or stolen leaving the user in a vulnerable physical and informational position, as explained by C619: "*The watch gives a lot of useful functions, but how someone can feel safe if he lost it, especially when its connected to his home or car, basically we putting our life in risk of those mentally-ill and obsessed with technology*".

Some of the Apple Watch functions and apps, created physical fear for users. There is a possibility that an attacker could breach the device security, and unlock home doors remotely, or find the user's location or daily patterns. This could enable an intruder to plan an attack on the user's home, based on the user's daily patterns retrieved from the compromised smartwatch.

Despite the wide acceptance of the Apple Watch, there are some reasons to believe that privacy and security concerns might be preventing users from understanding the full potential of their device. Even though the smartwatch functions are useful to most users, we still see some being hesitant to perform some tasks on the smartwatch due to privacy and security concerns. Therefore, we need to understand the security and privacy effects on users' perceptions before we plan to improve the security of the smartwatch. This can help us design solutions that may strengthen users' privacy and security. The participants were concerned about privacy and security of some tasks and applications on their smartwatches as a consequence of factors such as fear of theft and data loss, misconceptions about security, smartwatch app permissions and a lack of authorisation and authentication methods. Therefore, smartwatch designers and developers must understand users' concerns about performing certain tasks on their smartwatches and identify opportunities to improve security and user privacy. Even though major progress is being made to develop smartwatch security, it is still in its infancy. Smartwatch designers should put more effort into making the smartwatch functions learnable, in order to incorporate proper security, and to avoid users bypassing the security functions.

Smartwatch designers should make a case for better user education and user interfaces that address common misunderstandings and the hesitation to perform certain tasks or use certain apps. Developers should add new security indicators to smartwatches to address users' mistrust of applications. To further address users' apprehensions about the loss and theft of smartwatches, developers are recommended to enhance the features that allow users to remotely lock or wipe their watch. Also, to give users a better security and privacy experience, developers could design better authentication services, especially for devices with tiny screens, such as facial, finger print or iris recognition authentication. In the case of app permissions, many app store platforms force app developers to come up with explanations for why their app wants permissions before they can request them. Also, smartwatch developers should make permission controls consistent to allow users to manage permissions and make the right decisions, as well as implement a privacy policy to stop app developers from taking advantage of ongoing consents and auto revoke them once users stop using the app. Developers should acknowledge that the smartwatch has vulnerabilities for end users, and design the most effective security and privacy features that fit the users' settings, experiences and preferences. Without improving the security and privacy features, Apple Watch users may not perceive the smartwatch as sufficiently safe, and this could undermine its usage and hinder user interaction.

6.9 Applications in eGovernment

The smartwatch is a wearable communication device. Unobtrusive and easy to wear, it comes with capabilities and sensors that could be useful in a variety of government applications (Frissen et al., 2007). Novice users were asked to give their opinions about the use and convenience of the Apple Watch for government e-services, and the apps or features they think would be useful. The analysis of the focus group data indicates that users consider three areas where the Apple Watch might be useful.

6.9.1 e-Health

The availability of biosensors in the Apple Watch and their closeness to the skin, mean the smartwatch can be a useful source of physiological data about the users' body (Lu et al., 2016). The biosensors have the ability to provide important healthcare information and could update users' health records if they were connected to health records in hospitals, as expressed by P1-2: "*It would be more convenient for updating patient record if it's linked with Apple Watch. It can send your blood pressure and heart rate readings daily and update your health record*". It should be equipped with accurate sensors and an emergency call option according to P1-3: "*Apple Watch should focus more on giving more accurate readings and a built-in emergency button with GPS*".

The Information derived from a smartwatch could be helpful for doctors or health providers to monitor patients with special needs and improve health services and practices. Therefore, before integrating smartwatch devices into health and clinical practice, researchers and practitioners should focus on conducting rigorous research on the smartwatch's accuracy, and investigate easy to use functionality for patients (Reeder and David, 2016).

6.9.2 e-Learning

Smartwatches are very useful devices that have the functionality to support students and teachers in education. Teachers may find new teaching practices and students may find new sources of information presented in a convenient way to enhance their learning and make material more accessible. The results of the focus groups reveal that some student participants were frustrated that there were no apps or specific feature of the Apple Watch to be used by students, as stated by P2-5: "*No apps found I can use it as student, and can use them to connect with university and libraries, these apps can help*".

The smartwatch can provide a wide range of benefits in education in the long term as it can enhance the quality of students' learning processes. Also, students with disabilities could take advantage of the smartwatch to make their learning experience easier. University ID cards could be integrated into the Apple Watch and used to open classrooms doors and labs by scanning the watch, as suggested by P3-6: "*I always forget my university card, and if there is a way to connect it with the smartwatch, it will be great help for us*". The smartwatch has the ability to present information quickly, and this can benefit students by providing educational content related to their study, customised to fit with their learning systems and the watch's capability. Therefore, smartwatches like the Apple Watch could be introduced and used to improve existing education systems and the learning processes of students.

6.9.3 Emergency Services

Some users indicated the benefit of using the Apple Watch in emergency situations, and rescue missions. They realised that the nature of the smartwatch and its smart sensing ability could help in emergency situations such as with a smoke detecting sensor connected to the fire department, as expressed by P1-5: "*It can be used as smoke detector alarm if it has smoke sensor and linked with emergency service*". Some participants stated that emergency buttons were missing, and such buttons would be significant for elderly and disabled users to ask for help from police or ambulance services, as mentioned by P3-4 "*I think Apple Watch is missing emergency call option, which is an important feature that can be provided for elder people and disabled*".

The smartwatch was perceived by the users as a helpful device in an emergency, when it could save lives and increase the efficiency of first response teams. Smartwatch designers should consider such situations when designing smartwatches and consider implementing sensors to increase the effectiveness of the smartwatch. Also, smartwatch designers could add emergency alert buttons that fit with users' settings, experiences and preferences.

In conclusion, smartwatch devices with their multi-purpose sensor technology have a promising future in delivering e-government services to citizens. However, smartwatches may become an issue for the government sector without proper integration, policy or security controls in place. Smartwatches, as a new technology, need to be studied and assessed for their applications and benefits for e-government. Also, e-service designers should have a policy of keeping up with such technology and its features to get the most benefit.

6.10 Limitations

There are some limitations to this study, some of which were beyond the researcher's control, mostly arising in the focus groups (e.g., some of the participants appeared to bond more than others). The two methods of data collection could introduce biases. The focus group method might lead participants' thoughts and views to influence other participants' views, while some participants might be reluctant to share their opinions in a focus group setting, if they feel others disagree with them. Following the discussion guide prepared by the authors for the focus groups, the researchers were able to direct the interactive discussion and create a permissive and nurturing atmosphere that encouraged the participants to share their perceptions and points of view about the research topic. The participants in the focus groups were all university students, but in order to be confident in our comparisons, greater similarity in group size and age could have been confirmed. However, recruiting participants is challenging, particularly if, for example, specific demographic characteristics are required.

The participants in a focus group are expressing their own personal views and experiences of a specific situation, within a specific culture, but it may be not easy for the researcher to clearly understand the participants' views. This is considered a potential limitation of all focus groups. The researcher and moderator put great effort in the focus group sessions into understanding and clarifying participants' views by probing for details when there was any uncertainty on any point.

The method used to collect posts and comments from sub-reddits focused on the Apple smartwatch might have failed to include important comments from other sub-reddits. Due to the time and resource limitations, the authors focused only on gathering highly ranked posts and comments. Another limitation was that the study focused on the Apple Watch Series 1 and some of the results may not be applicable to new releases of the Apple Watch. Some of the user concerns found in this study are avoided in the new releases. Future research could investigate other well-known web forums or run a comparative study with another smartwatch brand, which may provide richer insight into users' perceptions and attitudes.

The data collected from sub-reddits were beyond the researchers' control, with regard to the posters' demographics such age, gender, nationality and education level. The Reddit forum would not allow the researchers to have access to such data. Therefore, future research could investigate the effects of demographic differences on users' attitudes and perceptions of the Apple smartwatch by creating a new sub-reddit forum and inviting participants to join, providing their demographic details, even though this would be time consuming.

Despite its limitations, the research study adds important qualitative evidence to the current research on smartwatches and provides important benefits for researchers and smartwatch designers who wish to improve marketing practices.

6.11 Summary & Recommendations

In general, the results indicate that novice users perceive some Apple smartwatch features more favourably than expert users. The mixed qualitative and quantitative approach used in this study reveals answers related to the research question that give us a clearer picture of the differences between the two user types in how they perceive the Apple Watch features. Of the 26 watch features tested statistically, 15 show significant differences between novice and expert users. The number of positive and negative comments reported show that novice users find most features useful, whereas expert users experience almost all features less favourably. The results show that novice users report usability and privacy issues differently from expert users. The inclusion of both expert and novice groups provides an extra layer of information about the usability and security issues of the Apple Watch, because different users may experience different problems due to their unmatched experiences and backgrounds. Clearly, the usability and security issues recognised by the novice group have a trivial effect on their overall perception of Apple Watch use. This can be attributed to the limited interaction time given to the novice users, the power of first impressions, and brand and media influence. On the other hand, the expert group encountered many usability and security issues that, over time, impacted negatively on their perception of Apple Watch use. This negative perception could be attributed to familiarisation or the novelty effect, as, over time, the device becomes more ordinary for users. Interestingly, we note that the more time users spent using the Apple Watch, the more the level of frustration increased, and the more usability and security issues were detected. This could explain why expert users feel more frustrated and comment negatively about most Apple Watch features. The outcome of the study points out that most features are perceived as less usable and rated more negatively by the novice group, including the battery & performance, screen size, applications & usefulness, and interaction. However, the results reveal that the Apple Watch features did not meet expert users' expectations and were rated highly negatively, including dependency, interaction, connectivity, and notifications. The most striking result is that the expert users were more frustrated and perceived most Apple Watch features as not efficient, and that a remarkable number of usability and security problems still remain after extensive use. Despite the fact that time can mend some issues and reduce others by allowing users to learn tactics to overcome them, expert users were not able to control these issues. Another interesting result is that the novice users perceived the smartwatch as a supplementary device or extra screen for the iPhone, not something to replace a smartphone. However, expert users perceived it as a dependent device that needs to be redesigned to work independently without relying on the iPhone.

The findings of the study form the basis of recommendations for how the design of smartwatches can be improved to generate better user interaction and experience as well as security and privacy. The main purpose of the proposed recommendations, discussed previously for each smartwatch feature, is to help design practitioners understand users' perceptual differences of smartwatches use.

The qualitative analysis of the results provides useful recommendations for the development of future e-government applications that rely on the use of smartwatches and their sensing capabilities. In particular, our main suggestion is to invest in the enhancement of the usefulness and ease of use of smartwatches and the delivery of smartwatch features with a high level of security. Without this, potential users may not sufficiently appreciate the benefits of smartwatches for e-government services, and user acceptance and satisfaction may be very limited.

Chapter 7 Blockchain Study

This c the focus of this thesis and places the motivation of the research, related to the trade-off between usability and security. The research aims and research questions are explained. Finally, the thesis layout is presented.

7.1 Introduction

The world has recently witnessed a digital currency revolution and become a major concern for many industries, investors, academics and government institutions. The revolution of Bitcoin digital crypto-currency has caused a stir worldwide by introducing Blockchain technology as a potential solution for most of real digital world problems. Blockchain is a digitised, decentralised, distributed ledger technology composed of immutable, indelible blocks of data, where each block holds a list of transactions and linked with each other by a unique reference in proper linear, chronological order. Bitcoin crypto-currency is the most prominent existing application of Blockchain technology. Some experts and practitioners argue that Blockchain will establish new foundations for many domains, and a gateway to multiple significant wider applications. However, the research and development of other vital practical applications remains limited. Some explanations that can be drawn is Blockchain technology is still not mature enough, not systematically explored and risks surrounding it are still unknown.

On the other hand, recent studies show that Blockchain considered by developers and service designers as complex to use and there are misconceptions about how it works (Wüst & Gervais 2016.; Seebacher & Sch 2017). One of these challenges that might limit a wider use of Blockchain applications is deciding between the different types of Blockchain that are available today, for example public, private, Federated Blockchains or Consortium. Blockchain integration with business processes and fit with the users need is another concern. Understanding the design of each type of Blockchain is another challenge that requires developers and service designers' attention. Regardless the wide use of public decentralised Blockchain with cryptocurrencies; private Blockchain technologies are being introduced within governmental and industrial sectors. Such Blockchains are based on different trust models not similar to the public Blockchain and only certain users can join the peer-to-peer network.

The utilisation of Blockchain technology to enhance the public services delivery has become acute from a government standpoint. Currently, Blockchain has the potential to increase trust in public sectors and improve delivery of public services by making the government operations more efficient (Mainelli and Smith, 2015). In addition, Blockchain applications can change the ways transactions are conducted and recorded because of its transformative nature.

7.2 Literature Review

7.2.1 Current State

According to Atzori & Ph (2015), the Blockchain technology has emerged as a technological breakthrough for individuals and collective groups to influence their interaction in business, politics and society. The aforementioned aspect is possible by disintermediation of unprecedented process. Globally, various governments have started to document the potential advantages and drawbacks of the integrating applications based on Blockchain into both the public and private sector (Peck, 2017). However, Ølnes and Jansen (2018) have established that governments gain from benefits such as privacy, security, enhancing trust, reducing corruption, manipulation, transparency, data quality, data integrity, and avoidance of fraud. In support of this, Hyvärinen, Risius and Friis (2017) stated that numerous governments have already been attracted by the benefits of

Blockchain technology to eliminate corruption and improve transparency. In fact, White, M., Killmeyer, J., and Chew (2019) mentions that countries such as the United Kingdom, United States, United Arab Emirates, Netherlands, Sweden, Estonia, and China have announced initiatives pertaining to Blockchain to vigorously discover its implications in the public sector. Besides this, Yli-huumo et al. (2016) have highlighted the significance of interdisciplinary research in the possible utilisation of Blockchain technology for government. They have argued that Blockchain can enhance public services and solve some problems pertaining to governance, for instance, corruption, fraud, and inefficiency.

Atzori and Ph (2015) referred to Blockchain-based government as final stage of decentralisation which supports the bottom-up approach to politics that increases the participation of public in governmental process. Furthermore, it ignores the values contributed by the centralised system of government, privatisation of government services to shift the power from centralised system to the individuals or markets and supports the use of strong encryption to promote publics freedom and privacy.

Moreover, Atzori and Ph (2015) stated that another potential benefit of Blockchain technology is the decreased dependency of people on government. Various stakeholders consider Blockchain as a consensus driven repository, which allows the development of applications which reduces the dependency of general public on the government and supports the increasing focus of government towards e-government services. Thus, it can be stated that the world is at the stage where individuals can overcome the centralised political institutions (government) with the help of distributed consensus. This could result in the development of a society with attributes such as equality and flatter structures for effective performances. However, Ølnes and Jansen (2018) has pointed out that Blockchain technology in e-Government is still in its preliminary stages despite having a tremendous potential for disrupting this sector.

7.2.2 Usability and Security of Blockchain Technology in e-Government

Blockchain technology has a great influence on the way these electronic services are used in the e-government context. Ølnes and Jansen (2018) agree that services that are provided to the citizens must be dependent on the following factors that include accessibility, web security assurance, and usability. However, Swan (2015) notes that that there are some websites where the factor of usability is not given as much preference as the other two attributes are given, comparatively. Therefore, in order to make these websites accessible, progress has to be made to make these websites friendly for their users. Yet, an agency called the e-government agency must establish a certain code of conduct which would ultimately help the organisations for their guidance. Moreover, Wright and De Filippi, (2015) have highlighted that there are some websites that efficiently makes use of validation through HTTP and they are able to make the password system applicable. As a result, both medium and high severity vulnerabilities are monitored. On the flip side, as far as the privacy and security are concerned these vulnerabilities work as an ultimatum for the hackers. However, Crosby et al., (2016) concluded that this platform helps to bring ease by removing complexities for use and simultaneously putting barriers for the hackers. Thus, it is important to protect the websites from cross-site scripting and SQL injection because in HTTP the passwords are concealed.

As a result, it is applicable that in order to protect the citizens these e-government websites should be further upgraded. Yet, there are some problems that can be tackled without facing any disposition such as loading speed time of the homepage and broken links, etc.; others might be costly if not handled and corrected in the development and design stage. While the Sortsite tool can be efficiently used to manage the problems related to the accessibility errors, through which the errors could be transformed to Web Content Accessibility Guideline. However, Catalini et al. (2016) argued that other errors should be easily eliminated in the development stage, for instance, reading texts on the move, linking or moving content etc. Therefore, web developers must be trained in order to guide them on the issue of usability and accessibility that must not be given oversight during the development stage. By following this step, the creation of the website becomes easier and proficient.

The three main security characteristics of confidentiality, integrity, and availability must be ensured by an e-government system. When the knowledge is not intercepted by a third party then confidentiality is achieved. Finck, (2017) reported that when the information is safeguarded by all means then integrity is achieved.

This Blockchain technology can have a big impact on the e-government context since it provides methods of implementation that ultimately provides its user the grounds that makes an individual capable to proficiently interact and bridge the gap between the public and citizens themselves. Other advantages include cost and bureaucracy reduction, staying safe from corruption etc. Consequently, it will increase its reliability among citizens.

However, there are issues associated with the scalability of Blockchain technology. Conoscenti et al., (2016) indicates that there is a trade-off between security and scalability of Blockchain. Batubara and Janssen (2018) also mentioned the limited scalability problems of Blockchain based systems that are a major hurdle in the implementation of Blockchain technology for e-government. The issues associated with the scalability of the Blockchain systems can further be understood by considering POW and BFT Blockchain algorithms. The Proof of Work (POW) algorithm has a better scalability but less power efficiency. Whereas, the Byzantine Fault Tolerance (BFT) algorithm has poor scalability but better efficiency (Bucolic, 2015). The Blockchain technology needed to support the e-government services needs to have significant scalability potential and efficiency to deliver the service to the public.

Theoretically, scalability aspect of the Blockchain is vital to achieve the complete decentralised concept of government. Currently, the limited scalability of the Blockchain technology resulted in the development of semi-decentralised systems such as Bitcoins (Beck et al., 2016). According to Koteska, Karafiloski and Mishev, (2017), the scalability of the Blockchain is limited due to the size of data that can be managed in a transaction. The data added to the blocks, which are of finite size, limit the upscale of Blockchain based services from smaller number of users to the entire population of a nation. The scalability issues of Blockchain also affect the latency between submission and confirmation of transaction, particularly in linear Blockchain models. Hence, it is argued that for e-government service applications and systems, linear Blockchain technology must be avoided to reduce the latency issues in Blockchain systems. Koteska, Karafiloski and

Mishev, (2017) referred to scalability issues as a product of factors: block size, block interval, network latency and transactional cost. All of these factors contribute to the limited scalability of Blockchain technology that limits its use in providing governmental services to the public. Currently, the block size is of 1MB, which restricts the amount of data that can be stored in a particular block per transaction. Moreover, the block interval varies widely and should be within 12 seconds for high efficiency. The average network latency for the Bitcoins platform of Blockchain is 10 minutes that needs to be reduced for improved scalability. Moreover, transaction cost is another important factor that also needs to be reduced in order to upscale the Blockchain for e-government purposes (Goswami, 2017). He further investigated the scalability of the Blockchain systems through Blockchain stimulation system and evaluated that the increased amount of transactions lead to increased network latency, network delay and confirmation time that reduces the scalability potential of the technology.

Another drawback of Blockchain technology that affects the usability of Blockchain technology on a large scale is its security (Koteska, Karafiloski and Mishev, 2017). Despite numerous researchers claiming high security of Blockchain technology, Lim et al. (2014) identified the public distributed ledgers involved in Blockchain transaction as the biggest security issue. The public Blockchain provides access to all the nodes in the network that affects the security and privacy desired by the public. Various security breaches in Blockchain based systems have been reported where viruses and Trojans has been used to gain unauthorised access (Vasek and Moore, 2015). These issues lead to poor User Experience (UX) of the Blockchain systems, which affects the usability of the Blockchain. The UX significantly affects the usability of Blockchain based platforms among public and needs to be addressed in order to successfully implement them in offering governmental services electronically (Koteska, Karafiloski and Mishev, 2017).

7.2.3 Blockchain Applications for e-Government

The importance of Blockchain applications in public healthcare cannot be overemphasised. It has the potential to improve the integrity of the medical records of the patients. Hyvärinen, Risius and Friis (2017) have emphasised that the lack of data integrity and integration can also be overcome in sector of public education. Moreover, Biswas and Muthukkumarasamy (2016) documented that smart cities is another application that the platform of Blockchain may utilise in the context of e-government. However, Ølnes, Ubacht and Janssen (2017) argued that the ideas of tax system, e-voting, and digital identity can also be implemented in this regard. Similarly, the applications that involve recording of licenses, certificates, vehicle and land registry can also be stored in an effective manner.

Blockchain technology could be beneficial in a wide array of e-government use cases. Blockchains can be deployed to share and secure important records and data, for instance, identity records can be stored on chain, which would then be used to provide a verifiable, unique, and secure identity to every actor in the digital economy (Abeyratne and Monfared, 2016). Similarly, Ølnes, Ubacht, Janssen (2017) elucidated that Blockchain has great implications for asset registries, for example, with respect to land title or to enhance the sharing and securing of confidential data, for instance, educational certifications and patient health records. However, Martinovic, Kello, and Sluganovic (2017) documented that if Blockchain is shaped to consist the verified data, the possibility of attaining a trustworthy design for e-voting systems is quite possible.

Apart from this, other applications of Blockchains circulate around regulating and monitoring of different kinds of market, keeping markets safe and viable while supporting governments in their task of safeguarding consumers (Wright and De Filippi, 2015). Similarly, Lamarque (2016) described that governments may benefit by shared ledgers, which can aid the governments to mitigate friction in aggregating and gathering data from market participants they oversee, while also paving way for market supervision and real-time data collection. These shared ledgers could be used to tackle fraud and streamline how governments manage their own expenditures, whether in administration, entitlements, or procurement, and how taxes are collected and calculated. Blockchains can also aid in reducing costs and increase efficiency in government operations.

7.2.4 Blockchain Platforms for e-Government

Currently, three types of Blockchain platforms exist, namely, public, private, and permissioned. Generally, the purpose of maintaining these platforms is to control access rights, for instance, write, read, or read/write. Government can make use of private Blockchains to attain control and authority for the purpose of maintaining a high performance and secured database. This is because if immediate finality, transaction throughput, and high confidentiality are required, private permissioned Blockchain is the platform that e-Government needs to adopt. This is because native token is not mandatory since identities of participants are known and are approved by notaries. The figure below signifies why private permissioned Blockchain would act as a fitting platform for e-government:

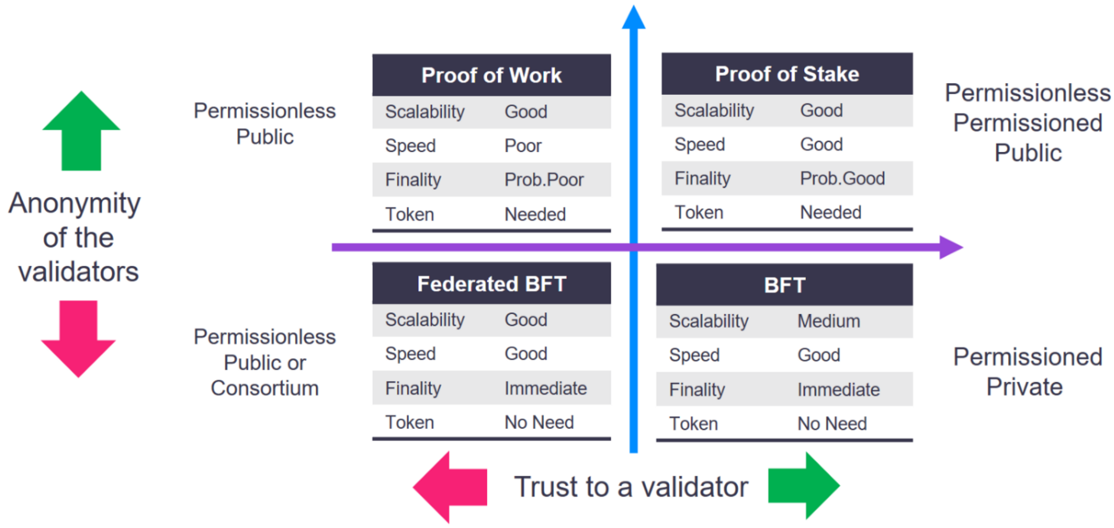

Figure 7.1: Private, Public, and Permissioned Blockchain (Kolisko, 2018)

Theme 1: Current State of Block Chain technology in E-government

The key characteristics of block chain technology in recording transactions on distributed ledges offer immense potential to be used in e-government services. Atzori, (2015) suggested that the importance of block chain technology for improving the E-government security in terms of usability and security is immensely high as it offers more potential in making government function more efficiently, while addressing the issues of delivery and trust. Its potential of changing the way in which transactions are recorded has the potential of bringing transformation because even the most insignificant of information is permanently recorded in the block chain. Ølnes, (2016) suggested that potential of integration of block chain technology in public sector is big; it can benefit government sectors with its key characteristics such as data integrity, data quality, prevention of fraud and mishandling, enhancing transparency in government transactions and reducing corruption. It also has the potentials for enhancing trust, security, and privacy. Hou, (2017) pointed that, such great potentials of this technology has already attracted the attention of many countries, and their e-governments such as the United Kingdom, the Netherlands, USA, the United Arab Emirates, Sweden, Estonia, and China and these countries have already announced the integration of this technology into their public sector. Ølnes et al., (2017) outlined that the key characteristic of decentralisation has the potential of fault tolerance, ensuring data consistency, imparting higher user control, ensuring attack resistance and imparting transparency. Thus, it can help in removing third-party control over transactions. Moreover, Ølnes and Jansen, (2017) suggested that technology is persistent with a consensus mechanism and uses time stamp and cryptographic seals which ensure that invalid transactions are not permitted. Hence, it ensures data consistency, ownership assurance, and fraud protection. Atzori, (2015) argued that the suitability of block chain technology is far better than the other techs because the transactions are stored in a chronological order which increases their traceability. Hou, (2017) illustrated the case study of UAE where the government of UAE has already taken some measures for establishing global block chain council for promoting using block chain-based services in the government as well as private sector. They have already strategised block chain-based projects on e-democracy, e-residency, and land registration.

Theme 2: Block chain technology influence usability and security in e Government context

Despite the huge potentials of Blockchain technology to be used in e-government services, there exists some issues or problems that restricts its wide-scale implementation in the public sector. Wright and De Filippi, (2015) highlighted the issues of complexity with the technology. The technology is sophisticated with many complexities like public keys, private keys, and cryptography. The e-government sectors tend to opt for simpler technologies with much less complexity hampering the wide-scale acceptability of this technology. Yli-Huumo et al., (2016) pointed out the scalability issues of this technology. The size of the blocks is limited offering limited storage capacities thus more the number of transactions easier these faster the block fills up. Moreover, linear block chain lacks mining speed as only one clock can be mined. For block chain to be implemented in public sector transaction, the mining speeds must be increased because in such cases the numbers of users at a time is much higher. Yeah, (2017) suggested that while the decentralisation nature offers its own sets of benefits, it also imposes the issue of having no centralised authority of recording transaction. While trust in the network is established, the removal of a central authority to oversee the network imposes a problem for the government. Michael et al., (2018) outlined one major issue that is imperative here is the environmental impact of this technology. The technology is far from being sustainable due to its high-power requirements and consumption. As the e-government sector is moving towards environmentally sustainable technologies, block chain imposes a challenge as more electricity is consumed for mining each block chain and with improvements the hardware blocks are getting harder to mine increasing the electricity consumption rate. These issues must be analysed before considering the wide-scale implementation of block chain in the e-government sector.

7.3 Method

This section presents the details of the process followed to conduct this study. A mapping study was conducted based on the articles reviewed in Batubara, Ubacht and Janssen (2018) that were the most relevant on the subject when this study was conducted. The systematic review guidelines in (Kitchenham and Charters, 2006) were used for this study to identify current research around the area of usability and security of Blockchain technologies in e-government. The research question focuses on information regarding: *What is the current state of the art research in how the usability and security of Blockchain technologies are influencing their use in e-government*.

The literature search Batubara, Ubacht and Janssen (2018) performed reviewed articles up to 30 December 2017 and their search terms were:

(blockchain OR "block chain" OR "distributed ledger") AND (government OR "public service" OR "public sector")

They executed the search on three electronic database resources to find research articles, namely Scopus, ScienceDirect, and SpringerLink. Title, abstract and keywords were used to search published journals papers, conference proceedings, workshops, and symposiums. They obtained a total of 354 articles, which were reduced to 21 articles after applying a number of additional criteria.

7.3.1 Selection Criteria

The criteria for this study included their original criteria and a set of secondary criteria were applied to reflect the research question. Selected articles should:

- be published in a peer-reviewed journal or conference proceedings
- present research about the use of Blockchain technologies in e-government
- topic should be around usability and security of Blockchain technologies in e-government
- be presented in English
- be accessible in full-text
- Not duplicate with articles from other databases.

Out of the 21 selected articles in the study of Batubara, Ubacht and Janssen (2018), a total of 11 articles were directly linked to the usability and security of using block chain technologies in e-government. They separated the terms usability and scalability, whereas in this study scalability is included as part of the usability of Blockchain technologies for e-government. The search from the previous study stopped at the end of 2017, therefore in this current study the search was performed from the period of January 2018 to March 2019. An updated search was performed based on their search terms, with the following keywords:

(blockchain OR "block chain" OR "distributed ledger") AND (government OR "public service" OR "public sector") AND (security OR usability OR scalability)

The keywords security, usability and scalability were added to the search terms in order to filter the results to focus on the current research question in this study. The 'scalability' keyword was added as a constraint, because some researchers separate the scalability from the usability of Blockchain technologies.

All the eligible papers were reviewed in detail to assess the suitability of the topics covered in relation to the research question of the study. Each paper had to cover the technological aspect of Blockchain technologies in e-government either conceptually or as an actual implemented system. Furthermore, the papers had to address the challenges posed by security, usability and scalability. The Scopus database returned 62 documents, the SpringerLink database returned 211 results and the ScienceDirect database returned 311 results. The SpringerLink and ScienceDirect databases returned a substantial number of results that did not contain the words security, usability or scalability in the title or abstract of the articles, which made filtering the results more cumbersome. The filtering process included applying the list of criteria and the total number of articles was reduced to 20 articles and these papers were manually reviewed in detail to ascertain the relevance of the topic discussed to the research question. The number of papers was further reduced to 13 after rejection of the 7 papers.

The year of publication of the papers were recorded to provide an indication how the emergent field of study of Blockchain technologies is evolving as more researchers are working in this area.

7.4 Results

In this section, the results of the literature review are presented. An overview of the selected papers will be presented followed by a discussion of how the papers addressed use or challenge of security and usability of Blockchain technologies for e-government.

There were 24 research papers that were published that contained the topic of security, usability of Blockchain in e-government, some of the papers covered conceptual ideas and proposed frameworks while other articles proposed prototypes of applications using Blockchain technologies. Two papers were published in 2016, 9 were published in 2017, and a further 9 were released in 2018, while 4 papers have already been published in the first three months of 2019. The number of publications per year will increase and shows the mounting interest that researchers have in the security and usability of Blockchain technologies in e-government. Olnes (2016) observed that the use of Blockchain technologies has not been broadly adopted in government sectors.

Most of the articles cover the evaluation of the potential use of Blockchain for government services and how they might benefit from the increased security, privacy and usability. Quite a few articles provide a detailed description of the functionality of Blockchain followed by how it can be implemented in existing public services. Some articles have looked at a design and implementation of an application that uses the Blockchain technology.

Some papers discuss current trends and benefits of adopting Blockchain for preserving the privacy, security of the data of citizens when they interact with government services such as e-voting and citizen records management (Shukla et al, 2018; Liu et al,2018; Chalaemwongwan et al, 2018; Moura et al (2017)). Shukla et al (2018) designed and developed a peer to peer network to act as a private Blockchain, where the underlying architecture is hidden to online voters who are uniquely identified. The system is secure by using encryption to reduce vote tampering and one person voting more than once. Votes cannot be tracked back to the voter and it is expected that the system will increase voter turnouts because the voting is done online. Liu et al (2018) discusses the issue of privacy for citizens interacting with governmental services and a statistical data sharing framework among governmental departments based on local differential privacy and Blockchain is established. The security of information sharing between government departments is improved and the local differential privacy provides better usability and security for sharing statistics.

Chalaemwongwan et al (2018) demonstrated the Thailand national Digital ID Framework based on Blockchain to improve digital identity government service to simple single sign-on. Their system helps preserve the privacy of users by providing personal information to service only when users grant permission for each service. The security is increased due to the data being distributed. Wang et al (2018), designed and implemented a system that consists of a blockchain structure, a network sharing model and consensus algorithms. Their system is decentralised to make the data sharing more efficient. The results of the experiments show that their system is more secure and more reliable than conventional sharing systems. Alketbi et al (2018) investigated the use cases, security benefits and challenges of using Blockchain for government services. They found that there can be huge potential for implementing Blockchain technologies for enabling smart government services.

Blockchain in healthcare is covered in three papers, where they look at to improve privacy and security of patients records with one amalgamating big data for enhanced healthcare coverage (Dhagarra et al, 2019; Ahram et al, 2017; Angraal et al, 2017). Dhagarra et al (2019) proposed a healthcare framework using big data and Blockchain, where they focus on providing timely and appropriate healthcare services to all citizens. The framework provides access to secure, immutable and comprehensive medical records of patients across all treatment centres. The security and privacy of the medical records are enhanced. Ahram et al. (2017), Angraal et al. (2017) propose the integration of Blockchain into the system of medical records and how to preserve the integrity of the patients' records.

Foisie et al (2019) and Kaijun et al (2018) investigated the use of Blockchain technology in supply chain management. Foisie et al (2018) mentioned that Blockchain is a potentially disruptive technology that faces many potential barriers for application in supply chain management. Kaijun et al (2018) targeted the Chinese public service platform in relation to agricultural supply chain system. They proposed a public Blockchain of agricultural supply chain system based on double chain architecture, mainly studying the dual chain structure and its storage mode, resource rent-seeking and matching mechanism and consensus algorithm. The results show that the chain of agricultural supply chain can take into account the openness and security of transaction information and the privacy of enterprise information.

Some papers looked at Blockchain to improve public service delivery and incorporate Blockchain as a lynchpin for the development of smart cities (Lander et al, 2017; Margheri, 2017; Olnes, 2016; Olnes et al, 2017; Mottur et al, 2018). Furthermore, Hardwick et al (2018) looked at the concept of smart contracts to government tendering activities. They implemented their scheme on the Ethereum platform to evaluate the performance and financial cost implications, along with an evaluation of the potential security and auditability challenges. Mottur et al (2018) investigated citizen engagement in smart cities using Blockchain. They developed a platform to mobilise the crowd and encourage them to submit information to the platform. The crowd is being seen as another sensor in the smart city. Blockchain technology is used to store the reports on decentralised ledgers and smart contracts are used to allocate SPOT tokens to people that upload incident reports. One of the rewards of the platform has been awareness towards security threats.

Blockchain adoption in higher education has been investigated in Harthy et al (2019), by securing the data transactions such as student records and certifications across campuses in different cities and countries. By securing the transactions, potential employers and other higher institutions have more trust in the records and certifications of the students. Lopez et al (2018) presented a Blockchain framework for addressing the privacy and security challenges associated with the Big Data in smart mobility. Each participant shares their encrypted data to the Blockchain network and can make information transactions with other participants as long as both parties agrees to the transaction rules (smart contract) issued by the owner of the data. The transaction and data are secured by providing access control, auditability, transparency and data ownership. Kuzmanovic (2019) investigated the fact that Blockchain do not scale due to the decentralisation nature of the technology. Cloud-delivery networks could dramatically improve the scalability of Blockchain.

7.5 Conclusion

Analysis of the literatures revealed that, on using this technology in the e-government sector, the technology offers higher potentials of usability and security by being decentralised, persistent, anonymous, and highly auditable. The block chain is a highly secured technology as it has high data integrity, improved data quality, the ability of prevention of fraud and mishandling. It has enhanced transparency in government transactions and opportunities for reducing corruption in government transactions making it a far more secure technology that other traditional techs. Other than cryptocurrency, block chain has high potentials for being used in many user-centric paradigms such as in the development of social media platforms for government to public transactions, government mobile-based applications and many other service sectors. The case study of UAE revealed the potential of using this technology in projects like e-democracy, e-residency, or land registration. The research analysis has focused on the various characteristics of block chain technology such as anonymity, transparency, security, and decentralisation, which proves the potential of using this technology in the e-government sector. The characteristic of decentralisation has the potential of fault tolerance, ensuring data consistency, imparting higher user control, ensuring attack resistance and imparting transparency. The block chain is also very transparent as well as persistent with a consensus mechanism and uses time stamp and cryptographic seals, which ensures that invalid transactions are not permitted. Therefore, it enhances transparency by ensuring data consistency, ownership assurance, and fraud protection. However, the technology has some challenges and social impacts in terms of its utility in e-government sectors.

There are scalability issues along with issues like high complexity, low-quality user interface, limited storage capacity in each block and low environment sustainability. Among these issues, the most prominent issue is the environmental impact of this technology. The e-government sector is moving towards environmentally sustainable technologies, and in this area, block chain imposes a challenge because more electricity is consumed for mining each block chain and with improving, the hardware blocks are getting harder to mine increasing the electric consumption rate. The block chain technology has great promise for its usage in the e-government sector, however; the challenges that are imposing the biggest issues must be carefully addressed before building the frameworks for its largescale application. Issues like its problem of high electricity consumption and lack of central control for overseeing the network must be addressed first.

Chapter 8 Conclusion & Recommendations

This chapter presents a summary of the research and its major findings. The research contribution of each study is presented and discussed in relation to the whole thesis, followed by general recommendations to improve design based on the findings. The general research limitations are discussed, along with suggestions for future research.

8.1 Summary of Research Studies

8.1.1 Study One –Bitcoin

Sub-study one (Bitcoin) investigates users' perceptions and experiences of an anonymous digital payment system (Bitcoin) and its influence on users in terms of usability and security in comparison to other non-anonymous payment systems such as credit/debit cards. This paper identifies users' perceptual differences in terms of usability and security. Two versions of a user survey are used to collect data, which reveal significant differences in users' perceptions of credit/debit cards and Bitcoin. The usability attributes of both systems examined show that respondents perceive the usability of credit/debit cards to be higher than Bitcoin, showing a great negative influence on users' security perceptions of Bitcoin. We conclude that Bitcoin, as a crypto-currency, is still in its infancy and requires user education and a new way of thinking. The study provides developers a comprehensive view of user requirements in regard to the usability and security trade-off of an anonymous digital payment service (Bitcoin) to help improve user-centred design. The analysis of the results reveals that perceived security, as measured by the questionnaires, is affected by the users' overall usability perception. The low user perception of system usability has a great influence on their low security perceptions of the anonymous payment service. The study indicates that usability and security are two related aspects that both have a significant influence on users' perceptions towards the use of the Bitcoin system. Usability and security are two important system features for users that go hand-in-hand with one another and actually improve together.

8.1.2 Study Two - Smartwatch

To capture novice and expert users' usability and security perceptions towards the use of smartwatches and how they perceive the features, a qualitative approach was used. The reviewed literature shows that little had been done to assess user experience or perception of the trade-off between usability and security of smartwatches. A qualitative study was conducted using four focus groups and the Reddit discussion website to collect data. The data collected from the four focus groups was used to assess novice users' perceptions and the Reddit data to capture expert users experiences of smartwatch usability and security. The results reveal perceptual differences between novice and expert users towards some smartwatch features. Novice users were more pleased to use the Apple smartwatch than expert users, and found most features more usable. Notably, the number of usability and security issues identified by the novice group had only a slight influence on their overall perception of Apple smartwatch use. This could be related to the limited time given to the novice users to use the smartwatch, the power of first impressions, brand reputation (Apple), and media influence. However, the expert group encountered some major usability and security problems that, over time, negatively affected their perceptions of the use of the Apple smartwatch features. The negative ratings of expert users could be attributed to familiarisation or the novelty effect, as over time of using the device it becomes more ordinary and users become less motivated. Interestingly, we note that the more time spent using the Apple smartwatch, the more the level of frustration increased and more usability and security issues were detected. This shows us why the expert users felt more frustrated and negatively reported more Apple smartwatch features. Moreover, the outcome of the study points out that the features perceived least usable and rated most negatively by the novice group were battery & performance, screen size, application & usefulness and interaction, while the features which least met expert users' expectations and were rated most negatively were dependency, interaction, connectivity and notifications. The most striking result is that the expert users were more frustrated and perceived more of the Apple smartwatch features as not efficient, and the remarkable number of usability and security problems that remained after extensive use. Despite the fact that time can mend some issues and reduce others by allowing users to learn tactics to overcome problems, expert users were not able to develop any such tactics or take better control over these issues. Another interesting result is that the novice users perceived the smartwatch as a supplementary device or extra screen for the iPhone, not as something that one day may replace the smartphone. The expert users felt that the Apple smartwatch would be more useful and effective if it were more independent and worked without relying on another device. Clearly, the analysis indicates that the Apple Watch has a stylish colourful design but is an overly complicated piece of wearable technology that, so far, doesn't really know what it wants to be. Meanwhile, the Apple smartwatch proved that it can be a useful device in many ways but is still not able to work either in harmony with a smartphone or independently.

8.1.3 Study Three - Blockchain Technology

To understand Blockchain technology the researcher employed a pragmatic methodology, providing a comprehensive literature review of the usability and security of Blockchain in an e-government setting, based on academic journals and conference proceedings. A mapping study was conducted based on the articles in Batubara and Janssen (2018) that were most relevant to the subject when the study was conducted. The mapping study guidelines in (Brereton et al., 2007) were used for this study exploring the current research around the area of usability and security of Blockchain technologies in e-government settings.

Analysis of the literature selected reveals that, using Blockchain technology in the e-government sector provides higher potential for usability and security by being decentralised and anonymous. The Blockchain is a highly secure technology as it has high data integrity, improved data quality, and the ability to prevent fraud and mishandling.

Blockchain technology has high potential for being used in many user-centric paradigms such as the development of social media platforms for government to public transactions, government mobile-based applications and many other service sectors.

The analysis of the literature confirms that Blockchain technology faces some challenging issues such as security, scalability, interoperability and flexibility (Koteska, Karafiloski and Mishev, 2017). However, Blockchain technology is still not mature, has not been systematically explored, and the risks surrounding it are still unknown. The analysis of the literature also indicates that there is no still clear standards or guidance available to measure the appropriateness of this technology to e-government application.

Blockchain technology has great promise for the e-government sector, but the challenges that pose the biggest issues must be addressed carefully before building frameworks for its large-scale application. Issues such as its high electricity consumption and lack of central control for overseeing the network must be addressed first.

8.2 Guidelines and Recommendations

In this section, the author proposes appropriate guidelines in line with the thesis aims and the findings from the three studies. The proposed guidelines and recommendations do not replace the general usability guidelines or heuristics but complement them to take into account user concerns and insights. The author searched the literature for general guidelines to improve the usability and security of the studied systems in an e-government context. The author gathered the most appropriate guidelines recommended by the literature in order to compare them with the findings of the three studies conducted. General guidelines are presented below, drawn from the literatures and based on the findings of the three studies

(i). Design for all types of users.

Developers should pay attention to user interface usability and security features and make the designed interface and its functionality more flexible to accommodate novice and expert users. Novice users, in most cases, need help and time to accomplish tasks while expert users should be given the option to quickly access any feature or functionality of the system via shortcuts or hotkeys. This guideline highlights the need for different methods of system interaction (Dontamsetti and Narayanan, 2008; Kuo and Perrig, 2009). This guideline is based on the findings from study one (Chapter 5, Sections 5.5.3.1 and 5.5.3.2) and study two (Chapter 6, Sections 6.6.5 6.11)

(ii). *Give informative feedback.*

Most important for both novice and expert users is a useful and clear feedback system. Feedback should be clear and specific. It is the key ingredient to several other guidelines on usable cyber-security given below (e.g., help, error handling and visibility of the security system state). Feedback should be understandable, not too technical, sufficient, and give suggestions for accomplishing the task (Kuo and Perrig, 2009; Chiasson, Oorschot and Biddle, 2007). Developers should provide help and documentation when its required and users should be able to find and use help options easily. Users are likely to avoid using the system when they fail or are unable to determine how to use the system features. This guideline is based on the findings from study one (Chapter 5, Section 5.6.5) and study two (Chapter 6, Sections 6.7.2 and Section 6.7.4).

(iii). Error prevention, recovery and undo

This guideline recommends that usable security interface designs should prevent users from making errors and help users handle errors Systems should be designed such that they anticipate user errors and prevent them. Also, when users face errors in the system, they should be able to handle them efficiently and the system should outline steps for recovery (Johnston et al., 2003; Whitten and Tygar, 2005). A clear message should warn users about the error and give them obvious options to stop going forward or provide a small link to ignore the warning and continue. In addition, interface designs should support undo and quit functions when users make mistakes or go to an unwanted screen. System designers should make systems reliable so that users can rely on them to do the intended tasks and not feel lost or confused by the interaction (Chiasson, Oorschot and Biddle, 2007; Dontamsetti and Narayanan, 2008; Kuo and Perrig, 2009). This guideline is based on the findings from study one (Chapter 5, Sections 5.5.3.15.6.4 and 5.6.5) and study two (Chapter 6, Sections 6.7.1, 6.7.3 and 6.7.5).

(iv). Make security functionality visible and accessible

Security functionality should be easily located and accessed by users. System designers should make the functionality reachable by users and not hidden among the advanced options of the interface, as this can make tasks more confusing and may affect system usability (Kuo and Perrig, 2009; Chiasson, Oorschot and Biddle, 2007). This guideline is based on the findings from study one (Chapter 5, Section 5.6.7) and study two (Chapter 6, Sections 6.7.3 6.116.7.4).

(v). Design for learnability

User interfaces should be easy to learn. Learnability is an important attribute of usability, and has great influence on novice users' perceptions. Therefore, improving system learnability is likely to improve users' perceptions of other usability aspects. Using metaphors relating system functions to the real-world, with consistent terms, could increase users' familiarity with the system (Johnston et al., 2003). This guideline is related to the findings from study one (Chapter 5, Section 5.6.1) and study two (Chapter 6, Sections 6.7.1 6.116.7.7).

(vi). Emphasise a positive system experience and high rate of user satisfaction

Designers and system developers should aim to provide users with a positive and satisfactory experience when interacting with system interfaces. This might involve some changes to interfaces such as allowing users to customise or modify them to suit their preferences (Johnston et al., 2003; Kuo and Perrig, 2009; Chiasson, Oorschot and Biddle, 2007). This guideline is related to the findings from study one (Chapter 5, Section 5.6.6) and study two (Chapter 6, Section 6.8).

(vii). Aesthetic and minimalistic design

Designers should aim to simplify interfaces, reduce the overload of information and avoid difficult interface setups. Designers should leave only the essential features, with rarely used or redundant features being removed from the system. This would help users focus on main the system functions and make the right decision when facing difficulties with the system (Johnston et al., 2003). This guideline is related to the findings from study one (Chapter 5, Section 5.6.2) and study two (Chapter 6, Section 6.8).

(viii). Maintain the balance between security and usability

Developers and designers should use efficient and careful design to ensure system performance. They should develop security features and make sure that users can use them efficiently. Developers should help users select the right options by providing information about what they can and cannot do (Braz, Seffah and M'Raihi, 2007; Ben-Asher et al., 2009; Welle Donker-Kuijer, de Jong and Lentz, 2010). This guideline is related to the findings from study one (Chapter 5, Section 5.6.7) and study two (Chapter 6, Sections 6.7.2 and 6.8).

8.3 Contributions of the Thesis

Usability and security issues have been studied and researched over the years in the areas of human computer interaction (HCI), and user-centred design. E-government discipline brings its own challenges for usability and security, an issue which has gained less research attention.

This thesis contributes to the discipline of e-government services with empirical knowledge about user perception and experience. This subject has not been studied previously in the discipline of e-government with a focus on emerging technology, devices or services. This research makes a broad contribution to human computer interaction (HCI) and user-centred design in e-government.

This thesis reports on three studies conducted into the trade-off between usability and security in an e-government context using a mixed methods approach. The research explores three elements of e-government services usability and security. The thesis focuses on new services being introduced, new devices being integrated, and new technologies being adopted. Each research study examines one of these aspects, exploring how users or citizens perceive their usability and security. By conducting three studies, the researcher seeks a clear and comprehensive picture of users' attitudes, opinions and preferences, and a rich insight into users' needs. This research explains user requirements for new services, devices and technologies implemented in e-government settings, in terms of usability and security. The research considers three important elements of e-government that are significant for providing e-government services and supporting citizen interaction. Any e-government, in order to work properly, needs elements that work together to provide efficient and successful services, such as well-established online payment systems, and platforms to connect with their users. Therefore, the researcher selects three elements that are significant to both citizens and government authorities to conduct research. Based on the findings, the research proposes recommendations to improve usability and security. These recommendations could help increase the overall usability and security of the three elements, based on users' preferences in the e-government context, which can result in better user interaction and use of e-government services. The research makes the following contributions to e-government context and practice.

1) The first contribution of this thesis is the first published mapping study of the trade-off between usability and security in an e-government context. The mapping study was conducted at the end of 2015 and published in British HCI 2016 Fusion, Bournemouth, UK. The mapping study identified the aspects of usability and security in e-government services that have been researched or where research is lacking. The mapping study found that most papers looking into the trade-off between usability and security focus on other contexts and restrict the examination to login methods. The mapping study highlights the need to have empirical research focusing on e-government in terms of assessing the trade-off between usability and security. The mapping study confirms that the trade-off between usability and security in an e-government context is not being addressed and there is scope for more work in this area.

2) This research focuses on users' perceptions, opinions and preferences for the trade-off between usability and security in an e-government context. The research not only provides deep insight into how users perceive the usability and security of e-government, but also gives feedback about user insights and attitudes when new services are introduced, new devices are integrated, or new technology is adopted. Therefore, this research contributes to the field of e-government research, by covering three important elements which serve as a

reference for e-government service designers and developers, for the purpose of understanding users' needs and future service implementation.

3) The second study (Bitcoin), contributes to the HCI field by means of an exploratory, mixed qualitative and quantitative approach, using survey questionnaires. This is the first user study to focus on user perceptions of Bitcoin usability and security in comparison to other payment systems. The findings of the study apply to e-governments, banking institutions, online transaction providers, and developers by uncovering Bitcoin users' concerns and views about using Bitcoin payment systems, thereby enabling them to enhance and develop services based on user requirements. The study findings identify significant aspects of usability and security and appropriate guidelines are proposed to support and promote the use of Bitcoin payment systems in e-government. Moreover, the study contributes to the e-government field with a set of guidelines based on an exploratory study. The guidelines proposed by the author complement the general usability and security guidelines in the e-government field. This paper was accepted and published in ELSEVIER International Journal of Human-Computer Studies in 2019.

4) The Smartwatch study provides a conceptual foundation for academics and smartwatch designers, with a set of guidelines and clear user opinions that are likely to contribute to a better overall usability and security interaction experience. Research into smartwatches and wearable devices is scarce, so this study contributes to the limited body of research. In addition, to the best of our knowledge, there is no qualitative research comparing novice and expert users' perceptions of smartwatches before this. The study contributes to the field of user experience (UX) and HCI by employing a mixed research method to explore users' preferences regarding smartwatch usability and security.

5) The Blockchain study is a critical review of papers addressing Blockchain technology usability and security in an e-government context. This critical analysis is a reference for researchers, enabling them to get better acquainted with the main areas of Blockchain technology in an e-government context. The paper identifies areas for future research and provides practitioners a useful starting point in the area of Blockchain technology in an e-government setting.

8.4 Future Research

The findings and the reflection on the research limitations suggest some areas for future research.

There are a number of pieces of research which show that individual differences, such as education level, age, gender and experience level, influence users' perceptions in an e-government context (Dwivedi and Williams, 2008). Thus, future research could investigate the effects of individual differences on users' attitudes and perceptions of usability and security in e-government. This may help service designers in e-government develop and improve services based on individual differences.

It would be useful to conduct a study investigating expert and novice users' perceptual differences of usability and security and the trade-off between them. Understanding how experienced users perceive usability and security in comparison to novice users would help improve future design and close the gap between novices and experts.

A longitudinal study could be conducted to investigate users' perceptions of the trade-off between usability and security in an e-government context in order to monitor the changing attitudes of users, which would help service designers and developers provide more responsive services based on users' needs.

The first two sub-researches were limited to one group of student users at Keele University. The subjects selected might limit the generalisability of the research findings. Therefore, future research could survey other groups of potential users in society in order to understand how other groups perceive the trade-off between usability and security in an e-government context.

8.5 Summary

This chapter summarises the three sub-studies' findings and makes recommendations based on each sub-study. The main contribution of this research is presented. The study limitations and suggestions for future work are discussed. This research aims to deepen our understanding of users' perceptions of usability and security in an e-government setting in order to improve service design based on users' needs. This in-depth study is the first of its kind that explores the trade-off between usability and security from a user's perspective in an e-government context by investigating three related elements of e-government, using a mixed-method approach. From this point of view, this research study represents an empirical contribution to the literature on the trade-off between usability and security in e-government and a valuable addition to the literature on information system research in general. Therefore, hopefully, the findings of this research will have a positive impact on the research community and e-government service providers, acting as a valuable resource.

REFERENCES

Abrazhevich, D. (2004) *Electronic Payment Systems : a User-Centered Perspective and Interaction Design, Technische Universiteit Eindhoven*. doi: 10.6100/IR575913.

Acar, Y., Fahl, S. and Mazurek, M. L. (2017) ‘You are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users’, *Proceedings - 2016 IEEE Cybersecurity Development, SecDev 2016*, pp. 3–8. doi: 10.1109/SecDev.2016.013.

Adami, C. et al. (2011) ‘Severe Esophageal Injuries Occurring After General Anesthesia in Two Cats: Case Report and Literature Review’, *Journal of the American Animal Hospital Association*, 47(6), pp. 436–442. doi: 10.5326/JAAHA-MS-5690.

Ahmad, N., Shoaib, U. and Prinetto, P. (2015) ‘Usability of Online Assistance From Semiliterate Users’ Perspective’, *International Journal of Human-Computer Interaction*, 31(1), pp. 55–64. doi: 10.1080/10447318.2014.925772.

Aichholzer, G. and Strauß, S. (2009) ‘Understanding a complex innovation process: identity management in Austrian e-government’, *Proceedings of the 10th Annual International …*, pp. 230–239. Available at: http://dl.acm.org/citation.cfm?id=1556218.

Akers, D. et al. (2009) ‘Undo and erase events as indicators of usability problems’, *Proceedings of the International Conference on Human Factors in Computing Systems*, p. 659. doi: 10.1145/1518701.1518804.

Ali, H., For, H. L.-I. C. on H. A. of I. and 2016, U. (2016) ‘Designing a smart watch interface for a notification and communication system for nursing homes’, *Springer*. Available at: https://link.springer.com/chapter/10.1007/978-3-319-39943-0_39 (Accessed: 27 April 2019).

Alonso-Ríos, D., Mosqueira-Rey, E. and Moret-Bonillo, V. (2014) ‘A Taxonomy-Based Usability Study of an Intelligent Speed Adaptation Device’, *International Journal of Human-Computer Interaction*, 30(7), pp. 585–603. doi: 10.1080/10447318.2014.907463.

Alshamsi, A. and P. Andras (2019) ‘User Perception of Bitcoin Usability and Security across Novice Users’, *Elsevier- International Journal of Human-Computer*. Available at: https://www.sciencedirect.com/science/article/pii/S1071581918301459 (Accessed: 26 February 2019).

Alshamsi, A., Williams, N. and Andras, P. (2016) ‘The Trade-off Between Usability and Security in the Context of eGovernment: A Mapping Study’, *Proceedings of the 30th International BCS Human Computer Interaction Conference: Fusion!*, pp. 36:1--36:13. doi: 10.14236/ewic/HCI2016.36.

Amaratunga, D. et al. (2002) ‘Quantitative and qualitative research in the built environment: application of “mixed” research approach’, *Work Study*, 51(1), pp. 17–31. doi: 10.1108/00438020210415488.

Andreasen, M. S. et al. (2007) ‘What happened to remote usability testing?’, *Proceedings of the*

SIGCHI conference on Human factors in computing systems - CHI '07, p. 1405. doi: 10.1145/1240624.1240838.

Androulaki, E. et al. (2013) 'Evaluating user privacy in Bitcoin', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7859 LNCS, pp. 34–51. doi: 10.1007/978-3-642-39884-1_4.

Astrup, P., Jansen, E. and Aksic, N. (2016) 'Usability of Commercial mHealth Toolkits From a Developer Perspective-An Empirical Evaluation of Google Fit, Apple HealthKit and Samsung Digital Health'. Available at: https://brage.bibsys.no/xmlui/handle/11250/2406938 (Accessed: 27 April 2019).

Athey, S. et al. (2016) 'Bitcoin Pricing, Adoption, and Usage: Theory and Evidence', *Stanford University Graduate School of Business Research Paper*, 16(42), p. 70. doi: 10.1016/j.snb.2016.03.104.

Atzori, M. and Ph, D. (2015) 'Blockchain Technology and Decentralized Governance : Is the State Still Necessary ?', pp. 1–37.

Avison, D., Baskerville, R. and Myers, M. (2001) 'Controlling action research projects', *Information Technology & People*, 14(1), pp. 28–45. doi: 10.1108/09593840110384762.

Babaian, T., Lucas, W. and Oja, M.-K. (2012) 'Evaluating the collaborative critique method', *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems - CHI '12*, p. 2137. doi: 10.1145/2207676.2208366.

Baglin, F. (2015) 'Utilising a Human Centered Design (HCD) approach for Enhancing Government Systems in Saudi Arabia through Usability Evaluation from the user ' s perspective A thesis submitted for the degree of Doctor of Philosophy Department of Computer Science', (May).

Baker, D. L. (2009) 'Advancing E-Government performance in the United States through enhanced usability benchmarks', *Government Information Quarterly*. Elsevier Inc., 26(1), pp. 82–88. doi: 10.1016/j.giq.2008.01.004.

Bamert, T. et al. (2013) 'Have a snack, pay with Bitcoins', *13th IEEE International Conference on Peer-to-Peer Computing, IEEE P2P 2013 - Proceedings*, (c). doi: 10.1109/P2P.2013.6688717.

Barber, S. et al. (2012) 'Bitter to better - How to make bitcoin a better currency', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7397 LNCS, pp. 399–414. doi: 10.1007/978-3-642-32946-3_29.

Batubara, F. R. and Janssen, M. (2018) 'Challenges of Blockchain Technology Adoption for e-Government : A Systematic Literature Review'.

Baur, A. W. et al. (2015) 'Cryptocurrencies as a disruption? empirical findings on user adoption and future potential of Bitcoin and Co', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9373, pp. 63–80. doi: 10.1007/978-3-319-25013-7_6.

Beck, R. et al. (2016) 'Association for Information Systems AIS Electronic Library (AISeL) BLOCKCHAIN – THE GATEWAY TO TRUST- FREE CRYPTOGRAPHIC TRANSACTIONS', *ECIS 2016 Proceedings*. Available at: http://aisel.aisnet.org/ecis2016_rp%0Ahttp://aisel.aisnet.org/ecis2016_rp.

Ben-Asher, N. et al. (2009) 'Security and usability research using a microworld environment', *Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services - MobileHCI '09*, p. 1. doi: 10.1145/1613858.1613925.

Ben-Sasson, E. et al. (2014) 'Zerocash: Decentralized anonymous payments from bitcoin', *Proceedings - IEEE Symposium on Security and Privacy*, pp. 459–474. doi: 10.1109/SP.2014.36.

Bertot, J. C. and Jaeger, P. T. (2006) 'User-centered e-government: Challenges and benefits for government Web sites', *Government Information Quarterly*, 23(2), pp. 163–168. doi: 10.1016/j.giq.2006.02.001.

Bhattacharya, P. et al. (2014) 'Learning mobile security with labware', *IEEE Security and Privacy*, 12(1), pp. 69–72. doi: 10.1109/MSP.2014.6.

Bitcoin.org (2018) *Bitcoin*. Available at: https://bitcoin.org/en/, 2018. (Accessed: 11 August 2018).

Bob-Milliar, G. M. (2014) 'Party youth activists and low-intensity electoral violence in Ghana: A qualitative study of party foot soldiers' activism', *African Studies Quarterly*, 15(1), pp. 125–152. doi: 10.1191/1478088706qp063oa.

Böhme, R. et al. (2015) 'Bitcoin: Economics, Technology, and Governance', *Journal of Economic Perspectives*, 29(2), pp. 213–238. doi: 10.1257/jep.29.2.213.

Bohr, J. and Bashir, M. (2014) 'Who Uses Bitcoin? An exploration of the Bitcoin community', *2014 12th Annual Conference on Privacy, Security and Trust, PST 2014*, pp. 94–101. doi: 10.1109/PST.2014.6890928.

Bonneau, J. et al. (2015) 'SoK: Research perspectives and challenges for bitcoin and cryptocurrencies', *Proceedings - IEEE Symposium on Security and Privacy*, 2015-July, pp. 104–121. doi: 10.1109/SP.2015.14.

Boucher, P., Nascimento, S. and Kritikos, M. (2017) 'How Blockchain Technology Could Change Our Lives', *European Parliament*, pp. 4–25. doi: 10.2861/926645.

Brannen, J. (2005) 'Mixing Methods: The Entry of Qualitative and Quantitative Approaches into the Research Process', *International Journal of Social Research Methodology*, 8(3), pp. 173–184. doi: 10.1080/13645570500154642.

Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', *Qualitative Research in Psychology*, 3(2), pp. 77–101. doi: 10.1191/1478088706qp063oa.

Braz, C., Seffah, A. and M'Raihi, D. (2007) 'Designing a Trade-Off Between Usability and Security: A Metrics Based-Model', *Lecture Notes in Computer Science*, 4663, pp. 114–126. doi: 10.1007/978-3-540-74800-7_9.

Brereton, P. et al. (2007) 'Lessons from applying the systematic literature review process within the software engineering domain', *Journal of Systems and Software*, 80(4), pp. 571–583. doi: 10.1016/j.jss.2006.07.009.

Bruun, A. et al. (2009) 'Let your users do the testing', *Proceedings of the 27th international conference on Human factors in computing systems - CHI 09*, p. 1619. doi: 10.1145/1518701.1518948.

Bryman, A. (2016) *Social research methods*. Available at: https://books.google.co.uk/books?hl=en&lr=&id=N2zQCgAAQBAJ&oi=fnd&pg=PP1&dq=bryman+2001+social+research+methods&ots=doNxBVP2qg&sig=xb_j-kXHaW_pwtaqeyEMDyobnFs (Accessed: 23 April 2019).

Budgen, D. and Brereton, P. (2006) 'Performing systematic literature reviews in software engineering', *Proceeding of the 28th international conference on Software engineering - ICSE '06*, 2, p. 1051. doi: 10.1145/1134285.1134500.

Burch, M. I. (2010) 'Blurred vision: Marion on the "possibility" of revelation', *International Journal for Philosophy of Religion*, 67(3), pp. 157–171. doi: 10.1109/MSP.2010.60.

BusinessInsider (2018) *Cryptocurrency price.*

Cameron, C. (2007) 'Social pedagogy and the children's workforce', *Community Care*, 3(1685), pp. 24–25. doi: 10.1145/259963.260531.

Campbell-Verduyn, M. (2017) 'Bitcoin and beyond: Cryptocurrencies, blockchains, and global governance', *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*, pp. 1–207. doi: 10.4324/9781315211909.

Candiwan, Beninda, M. Y. D. and Priyadi, Y. (2016) 'Analysis of Information Security Audit Using ISO 27001:2013 & ISO 27002:2013 at IT Division - X Company, In Bandung, Indonesia', *International Journal of Basic and Applied Science*, 4(4), pp. 77–88. doi: 10.13140/RG.2.1.1483.3044.

Carson, D. et al. (2001) *Qualitative marketing research*. Available at: https://books.google.co.uk/books?hl=en&lr=&id=L8nSK5QEeGEC&oi=fnd&pg=PP1&dq=Carson,+D.,+Gilmore,+A.,+Perry,+C.,+and+Gronhaug,+K.+(2001).+Qualitative+Marketing+Research.+London:+Sage&ots=I0iqhBcuqG&sig=yIlIFbJH42lYrVJi4Toxuo1lM1A (Accessed: 23 April 2019).

Carter, L. and Ubacht, J. (2018) 'Blockchain applications in government', *Proceedings of the 19th Annual International Conference on Digital Government Research Governance in the Data Age - dgo '18*, (September), pp. 1–2. doi: 10.1145/3209281.3209329.

Catalini, C. et al. (2016) 'We are thankful to'. Available at: http://www.nber.org/papers/w22952.

Cecchinato, M. E., Cox, A. L. and Bird, J. (2017) 'Always On(line)?', *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*, pp. 3557–3568. doi: 10.1145/3025453.3025538.

Chan, Y. Y. and Wei, V. K. (2009) 'Teaching for conceptual change in security awareness: A case study in higher education', *IEEE Security and Privacy*, 7(1), pp. 68–71. doi: 10.1109/MSP.2009.22.

Chiasson, S., Oorschot, P. van and Biddle, R. (2007) 'Even experts deserve usable security: Design guidelines for security management systems', *SOUPS Workshop on Usable IT Security Management*, (July), pp. 7–10. Available at: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Even+Experts+Deserve+Usable+Security+:+Design+guidelines+for+security+management+systems#0.

Chilana, P. K. et al. (2011) 'Post-deployment usability', *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*, p. 2243. doi: 10.1145/1978942.1979270.

Chilana, P. K., Wobbrock, J. O. and Ko, A. J. (2010) 'Understanding usability practices in complex domains', *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*, p. 2337. doi: 10.1145/1753326.1753678.

Chin, J. P., Diehl, V. A. and Norman, L. K. (1988) 'Development of an instrument measuring user satisfaction of the human-computer interface', *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '88*, pp. 213–218. doi: 10.1145/57167.57203.

Choi, J. (Jong U. et al. (2013a) 'SecureGov: Secure Data Sharing for Government Services', *Proceedings of the 14th Annual International Conference on Digital Government Research*, pp. 127–135. doi: 10.1145/2479724.2479745.

Choi, J. (Jong U. et al. (2013b) 'SecureGov', *Proceedings of the 14th Annual International Conference on Digital Government Research - dg.o '13*, p. 127. doi: 10.1145/2479724.2479745.

Choi, J. (Jong U., Ae Chun, S. and Cho, J.-W. (2014) 'Smart SecureGov', *Proceedings of the 15th Annual International Conference on Digital Government Research - dg.o '14*, pp. 91–99. doi: 10.1145/2612733.2612756.

Choi, J. and Kim, S. (2016) 'Is the smartwatch an IT product or a fashion product? A study on factors affecting the intention to use smartwatches', *Computers in Human Behavior*, 63(October 2016), pp. 777–786. doi: 10.1016/j.chb.2016.06.007.

Chowdhury, S., Poet, R. and Mackenzie, L. (2014) 'Passhint', *Proceedings of the 32nd annual*

ACM conference on Human factors in computing systems - CHI '14, pp. 2917–2926. doi: 10.1145/2556288.2557153.

Chuah, S. H. W. et al. (2016) 'Wearable technologies: The role of usefulness and visibility in smartwatch adoption', *Computers in Human Behavior*. Elsevier Ltd, 65(August), pp. 276–284. doi: 10.1016/j.chb.2016.07.047.

Chun, J. et al. (2018) 'A qualitative study of smartwatch usage and its usability', *Human Factors and Ergonomics In Manufacturing*, 28(4), pp. 186–199. doi: 10.1002/hfm.20733.

Churchill, E. F. (2015) 'Why should we care about Bitcoin?', *Interactions*, pp. 20–21. doi: 10.1145/2810199.

Cicoria, S. et al. (2014) 'Several Emerging Information Technology Topics and Related Doctoral Dissertation Ideas', *pdfs.semanticscholar.org*, pp. 1–8. Available at: https://pdfs.semanticscholar.org/403e/7f3631cb0b76bc83bc135afc1a5f9df0dca0.pdf (Accessed: 27 April 2019).

Clarke, A. (1999) *Evaluation research: An introduction to principles, methods and practice*. Available at: https://books.google.co.uk/books?hl=en&lr=&id=-gmjRF1KM2oC&oi=fnd&pg=PP1&dq=Clarke+%26+Dawson+1999&ots=Cu9KvAaiNv&sig=WDqxNqSFPakhV3Sm1Y58_pnNMA0 (Accessed: 24 April 2019).

Coín-Mejías, M. A. et al. (2007) 'Personality disorders and emotional variables in patients with lupus', *Salud Mental*, 30(2), pp. 19–24. doi: 10.1038/141613a0.

Collis, J. and Hussey, R. (2013) *Business research: A practical guide for undergraduate and postgraduate students*. Available at: https://books.google.co.uk/books?hl=en&lr=&id=uPgcBQAAQBAJ&oi=fnd&pg=PP1&dq=Collis+and+Hussey,+2009&ots=haTo3lSbdw&sig=Q5X4zuOprTKiEMGHLdxxpOfk2m4 (Accessed: 23 April 2019).

Conoscenti, M. et al. (2016) 'Blockchain for the Internet of Things : a Systematic Literature Review'.

Coursaris, C. and Kim, D. (2006) 'A Qualitative Review of Empirical Mobile Usability Studies A Qualitative Review of Empirical Mobile Usability Studies'.

Coutu, O. (2014) 'Privacy in Bitcoin through decentralized mixers'.

Cranor, L. F. and Buchler, N. (2014) 'Better together: Usability and security go hand in hand', in *IEEE Security and Privacy*, pp. 89–93. doi: 10.1109/MSP.2014.109.

Crosby, M. et al. (2016) 'Applied Innovation Review', *Applied Innovation Review*, (2), pp. 5–20.

currency, D. Y.-H. of digital and 2015, undefined (2013) 'Is Bitcoin a real currency? An economic appraisal', *Elsevier*, Working Pa. Available at: https://www.sciencedirect.com/science/article/pii/B9780128021170000023.

Custard, W., Magnus, B., & Yakubu-Sam, T. (2015) *Apple Watch User Testing Unboxing & First-Use, SOMoGlobal*. Available at: http://www.somoglobal.com/wp-content/uploads/2015/05/Somo-Apple-Watch-UX-Report.pdf.

Davie, N. and Hilber, T. (2016) 'Smartwatches As a Learning Tool: a Survey of Student Attitudes', pp. 117–122.

Dhamija, R. and Dusseault, L. (2008) 'The seven flaws of identity management: Usability and security challenges', *IEEE Security and Privacy*, 6(2), pp. 24–29. doi: 10.1109/MSP.2008.49.

van Dijk, J. A. G. M., Peters, O. and Ebbers, W. (2008) 'Explaining the acceptance and use of government Internet services: A multivariate analysis of 2006 survey data in the Netherlands', *Government Information Quarterly*, 25(3), pp. 379–399. doi: 10.1016/j.giq.2007.09.006.

Do, Q., Martini, B. and Choo, K.-K. R. (2017) 'Is the data on your wearable device secure? An Android Wear smartwatch case study', *Software: Practice and Experience,* 47(3), pp. 391–403. doi: 10.1002/spe.2414.

Donalek, C. et al. (2008) 'New approaches to object classification in synoptic sky surveys', *AIP Conference Proceedings*, 1082(2), pp. 252–256. doi: 10.3390/fi5020237.

Dontamsetti, M. and Narayanan, A. (2008) *Impact of the human element on information security, Social and Human Elements of Information Security: Emerging Trends and Countermeasures*. doi: 10.4018/978-1-60566-036-3.ch003.

Dumas, J., Dumas, J. and Redish, J. (1999) *A practical guide to usability testing*. Available at: https://books.google.co.uk/books?hl=en&lr=&id=4lge5k_F9EwC&oi=fnd&pg=PR9&dq=Dumas+and+Redish+1999&ots=vrhc9Fj3wI&sig=aBgkJA_05O3YfYvO8QLtNkchO4k (Accessed: 27 April 2019).

Dwivedi, Y. K. and Williams, M. D. (2008) 'Demographic influence on UK citizens' e-government adoption', *Electronic Government, an International Journal*, 5(3), p. 261. doi: 10.1504/eg.2008.018874.

Dzida, W., Herda, S. and Itzfeldt, W. D. (1978) 'User-Perceived Quality of Interactive Systems', *IEEE Transactions on Software Engineering*, SE-4(4), pp. 270–276. doi: 10.1109/TSE.1978.231511.

Egelman, S. et al. (no date) 'You've been warned: an empirical study of the effectiveness of web browser phishing warnings', *dl.acm.org*. Available at: https://dl.acm.org/citation.cfm?id=1357219 (Accessed: 27 April 2019).

Eskandari, S. (2015) 'Real-world Deployability and Usability of Bitcoin', (October).

Eskandari, S. et al. (2018) 'A first look at the usability of bitcoin key management', (February). doi: 10.14722/usec.2015.23015.

Finck, M. (2017) 'Blockchains and Data Protection in the European Union', *Ssrn*, pp. 17–35. doi: 10.2139/ssrn.3080322.

Fine, D. M. (1998) 'The violence against women act of 1994: The proper federal role in policing domestic violence', *Cornell Law Review*, 84(1), p. 252. doi: 10.1525/sp.2007.54.1.23.

Fogg, B. et al. (2003) 'How do users evaluate the credibility of Web sites?: a study with over 2,500 participants', *dl.acm.org*. Available at: https://dl.acm.org/citation.cfm?id=997097 (Accessed: 2 September 2019).

Følstad, A., Law, E. L. and Hornbæk, K. (2012) 'Analysis in Practical Usability Evaluation : A Survey Study', *CHI 2012 Proceedings*, pp. 2127–2136. doi: 10.1145/2207676.2208365.

Frandsen-Thorlacius, O. et al. (2009) 'Non-universal usability?', *Proceedings of the 27th international conference on Human factors in computing systems - CHI 09*, p. 41. doi: 10.1145/1518701.1518708.

Frissen, A. V. et al. (2007) *The Future of eGovernment for the EU in 2020*.

Fujii, K. et al. (2006) *Serine racemase binds to PICK1: Potential relevance to schizophrenia, Molecular Psychiatry*. doi: 10.1038/sj.mp.4001776.

Gao, X., Clark, G. D. and Lindqvist, J. (2016) 'Of Two Minds, Multiple Addresses, and One Ledger', *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*, pp. 1656–1668. doi: 10.1007/978-981-10-1926-5_82.

Garcia-Alfaro, J. et al. (2015) 'Data privacy management, autonomous spontaneous security, and security assurance', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8872(September), pp. 1–14. doi:

10.1007/978-3-319-17016-9.

Gibbon, J. D. (1985) ‘Nonparametric Methods for Quantitative Analysis, 2nd ed’. Holt, Rinehart and Winston. doi: 10.1038/ng.790.

Goetz, J. P. and LeCompte, M. D. (1981) ‘Ethnographic Research and the Problem of Data Reduction’, *Anthropology & Education Quarterly*, 12(1), pp. 51–70. doi: 10.1525/aeq.1981.12.1.05x1283i.

Goldfeder, S., Felten, E. W. and Kroll, J. A. (2015) ‘Securing Bitcoin wallets via threshold signatures’. Available at: https://freedom-to-tinker.com/blog/stevenag/new-research-better-wallet-security-for-bitcoin/.

González Martínez, S. et al. (2011) ‘Comparing usability of government web portals during governor change of terms’, *Proceedings of the 12th Annual International Digital Government Research Conference on Digital Government Innovation in Challenging Times - dg.o ’11*, p. 327. doi: 10.1145/2037556.2037609.

Gouscos, D. et al. (2007) ‘A general model of performance and quality for one-stop e-Government service offerings’, *Government Information Quarterly*, 24(4), pp. 860–885. doi: 10.1016/j.giq.2006.07.016.

Greiner, L. (2007) ‘Usability 101’, *netWorker*, 11(2), p. 11. doi: 10.1145/1268577.1268585.

Grossman, T., Fitzmaurice, G. and Attar, R. (2009) ‘A survey of software learnability’, *Proceedings of the 27th international conference on Human factors in computing systems - CHI 09*, p. 649. doi: 10.1145/1518701.1518803.

Guest, G., MacQueen, K. and Namey, E. (2011) *Applied thematic analysis*. Available at: https://books.google.co.uk/books?hl=en&lr=&id=Hr11DwAAQBAJ&oi=fnd&pg=PP1&dq=Applied+Thematic+Analysis&ots=Xi1xxJyKvE&sig=EHqZoc4DaV_9kWucdHzbO-UVmMU (Accessed: 5 March 2019).

Guest, G., MacQueen, K. and Namey, E. (2012) ‘Applied Thematic Analysis’, in *Applied Thematic analysis*, p. 11. doi: 10.4135/9781483384436.

Gutmann, P. and Grigg, I. (2005) ‘Security usability’, *IEEE Security and Privacy*, 3(4), pp. 56–58. doi: 10.1109/MSP.2005.104.

Ha, T. et al. (2017) ‘Examining user perceptions of smartwatch through dynamic topic modeling’, *Telematics and Informatics*. Elsevier Ltd, 34(7), pp. 1262–1273. doi: 10.1016/j.tele.2017.05.011.

van den Haak, M., De Jong, M. and Jan Schellens, P. (2003) ‘Retrospective vs. concurrent think-aloud protocols: Testing the usability of an online library catalogue’, *Behaviour & Information Technology*, 22(5), pp. 339–351. doi: 10.1080/0044929031000.

Han, F. and Luximon, T. (2016) ‘Examining the Usability of Message Reading Features on Smartwatches’, *International Journal of Humanities and Social Science Invention ISSN (Online*, 5(4), pp. 2319–7722. Available at: www.ijhssi.org.

Hankerson, D. et al. (2016) ‘Does technology have race?’, *dl.acm.org*. doi: ISBN 978-1-4503-4082-3/16/05...$15.00. DOI: http://dx.doi.org/10.1145/2851581.2892578.

Hayati, D., Karami, E. and Slee, B. (2006) ‘Combining Qualitative and Quantitative Methods in the Measurement of Rural Poverty: The Case of Iran’, *Social Indicators Research*, 75(3), pp. 361–394. doi: 10.1007/s11205-004-6299-9.

Heale, R., Forbes, D. and Heale, R. (2013) ‘Understanding triangulation in research’, 16(4), p. 101494.

Heller, B. et al. (2010) ‘Ripcord’, *ACM SIGCOMM Computer Communication Review*, 40(4), p. 457. doi: 10.1145/1851275.1851261.

Heo, S. (2017) ‘No Need to Stop What You ’ re Doing : Exploring No-Handed Smartwatch Interaction’, *CHCCS/SCDHM ACM*, pp. 107–116.

Herley, C. (2014) ‘More is not the answer’, *IEEE Security and Privacy*, 12(1), pp. 14–19. doi: 10.1109/MSP.2013.134.

Hern, A. (2013) (2013) *Missing: hard drive containing Bitcoins worth£ 4m in Newport landfill site*, *Missing: hard drive containing Bitcoins worth£ 4m in Newport landfill site*. Available at: www.theguardian.com/technology/2013/nov/27/hard-dr.

Hertzum, M. (2010) ‘Images of usability’, *International Journal of Human-Computer Interaction*, 26(6), pp. 567–600. doi: 10.1080/10447311003781300.

Hite, D., Fontana, P. and Williams, R. G. (2015) ‘Wide azimuth towed streamer: applications for exploration as well as development’, *ASEG Extended Abstracts*, 2007(1), p. 1. doi: 10.1071/aseg2007ab163.

Holzinger, A. (2005) ‘Usability engineering methods for software developers’, *Communications of the ACM*, 48(1), pp. 71–74. doi: 10.1145/1039539.1039541.

Hornbæk, K. and Frøkjær, E. (2005) ‘Comparing usability problems and redesign proposals as input to practical systems development’, *Proceedings of the SIGCHI conference on Human factors in computing systems*, p. 400. doi: 10.1145/1054972.1055027.

Hornbæk, K. and Frøkjær, E. (2008a) ‘Making use of business goals in usability evaluation’, *Proceeding of the twenty-sixth annual CHI conference on Human factors in computing systems - CHI ’08*, (January), p. 903. doi: 10.1145/1357054.1357197.

Hornbæk, K. and Frøkjær, E. (2008b) ‘Making use of business goals in usability evaluation’, *Proceeding of the twenty-sixth annual CHI conference on Human factors in computing systems - CHI ’08*, p. 903. doi: 10.1145/1357054.1357197.

Hornbæk, K. and Law, E. L.-C. (2007a) ‘Meta-analysis of correlations among usability measures’, *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI ’07*, 1, p. 617. doi: 10.1145/1240624.1240722.

Hornbæk, K. and Law, E. L.-C. (2007b) ‘Meta-analysis of correlations among usability measures’, *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI ’07*, p. 617. doi: 10.1145/1240624.1240722.

Houben, S., ACM, N. M.-P. of the 33rd A. and 2015, U. (2015) ‘Watchconnect: A toolkit for prototyping smartwatch-centric cross-device applications’, *dl.acm.org*. Available at: https://dl.acm.org/citation.cfm?id=2702215 (Accessed: 27 April 2019).

Howitt, D. (2016) *Introduction to qualitative research methods in psychology*. Available at: https://books.google.co.uk/books?hl=en&lr=&id=aRyKDwAAQBAJ&oi=fnd&pg=PT12&dq=Introduction+to+qualitative+methods+in+psychology+2010&ots=af89G2O-4f&sig=9bbRT5WlkUjQZoSDdITcAzUfWr4 (Accessed: 24 April 2019).

Huang, Z. and Benyoucef, M. (2014) ‘Usability and credibility of e-government websites’, *Government Information Quarterly*. Elsevier Inc., 31(4), pp. 584–595. doi: 10.1016/j.giq.2014.07.002.

Hudson, L., Research, J. O.-J. of consumer and 1988, U. (1998) ‘Alternative ways of seeking knowledge in consumer research’, *academic.oup.com*. Available at: https://academic.oup.com/jcr/article-abstract/14/4/508/1811971 (Accessed: 23 April 2019).

Hung, S. Y., Chang, C. M. and Kuo, S. R. (2013) ‘User acceptance of mobile e-government services: An empirical study’, *Government Information Quarterly*. Elsevier Inc., 30(1), pp. 33–44. doi: 10.1016/j.giq.2012.07.008.

Hyvärinen, H., Risius, M. and Friis, G. (2017) 'A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services', *Business and Information Systems Engineering*, 59(6), pp. 441–456. doi: 10.1007/s12599-017-0502-4.

Inglesant, P. G. and Sasse, M. A. (2010) 'The true cost of unusable password policies', *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*, p. 383. doi: 10.1145/1753326.1753384.

Ioannidis, E. (2017) 'Design an iOS application to promote medication adherence in adults'. Available at: https://repository.ihu.edu.gr/xmlui/handle/11544/15298 (Accessed: 27 April 2019).

Jakobsson, M. et al. (2008) 'Love and authentication', *Proceeding of the twenty-sixth annual CHI conference on Human factors in computing systems - CHI '08*, pp. 197–200. doi: 10.1145/1357054.1357087.

Jhajharia, S. et al. (2014) 'Wearable computing and its application', *Citeseer*. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.637.3781&rep=rep1&type=pdf (Accessed: 27 April 2019).

Ji, Y. G. et al. (2010) 'International Journal of Human- A Usability Checklist for the Usability Evaluation of Mobile Phone User Interface A Usability Checklist for the Usability Evaluation of', *International Journal*, 20(September 2011), pp. 37–41. doi: 10.1207/s15327590ijhc2003.

Johnson, M. E. and Willey, N. (2011) 'Usability failures and healthcare data hemorrhages', *IEEE Security and Privacy*, 9(2), pp. 35–42. doi: 10.1109/MSP.2010.196.

Johnson, R. B. and Onwuegbuzie, A. J. (2004) 'Mixed Methods Research: A Research Paradigm Whose Time Has Come', *Educational Researcher*, 33(7), pp. 14–26. doi: 10.3102/0013189X033007014.

Johnston, E. and Hansen, D. L. (2011) 'Design lessons for smart governance infrastructures', *American Governance*, pp. 1–30. Available at: https://books.google.co.uk/books?hl=en&lr=&id=Aru5CAAAQBAJ&oi=fnd&pg=PA197&dq=Johnston+%26+Hansen+(2011)&ots=0vxp_mtkuZ&sig=eWebCU1RX36xh-gflmTOrGdqtVo (Accessed: 27 April 2019).

Johnston, J. et al. (2003) 'Security and human computer interfaces', *Elsevier*. Available at: https://www.sciencedirect.com/science/article/pii/S0167404803000063 (Accessed: 25 September 2019).

de Jong, M. and Lentz, L. (2006) 'Scenario evaluation of municipal Web sites: Development and use of an expert-focused evaluation tool', *Government Information Quarterly*, 23(2), pp. 191–206. doi: 10.1016/j.giq.2005.11.007.

Jr, V. S. (2019) 'The Feasibility of Wearables in an Enterprise Environment And Their Impact on IT Security', pp. 1–17.

Just, M. (2004) 'Designing and evaluating challenge-question systems', *IEEE Security and Privacy*, 2(5), pp. 32–39. doi: 10.1109/MSP.2004.80.

Kainda, R., Flechais, I. and Roscoe, A. W. (2010) 'Security and usability: Analysis and evaluation', *ARES 2010 - 5th International Conference on Availability, Reliability, and Security*, pp. 275–282. doi: 10.1109/ARES.2010.77.

Karakaya, M., Bostan, A. and Gökçay, E. (2016) 'How Secure is Your Smart Watch ?', *INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE*, 5(4), pp. 90–95.

Karlsson, F. (2016) 'Assessing usability evaluation methods for smartwatch applications'.

Kaye, J. et al. (2014) '#CHImoney', *Proceedings of the extended abstracts of the 32nd annual ACM conference on Human factors in computing systems - CHI EA '14*, pp. 111–114. doi:

10.1145/2559206.2559221.

Keijzers, J., den Ouden, E. and Lu, Y. (2008) ‘Usability benchmark study of commercially available smart phones’, *Proceedings of the 10th international conference on Human computer interaction with mobile devices and services - MobileHCI ’08*, p. 265. doi: 10.1016/S0168-9002(02)01787-4.

Kerber, F., Krüger, A. and Löchtefeld, M. (2014) ‘Investigating the effectiveness of peephole interaction for smartwatches in a map navigation task’, *Proceedings of the 16th international conference on Human-computer interaction with mobile devices & services - MobileHCI ’14*, pp. 291–294. doi: 10.1145/2628363.2628393.

Khairuddin, I. E. et al. (2016) ‘Exploring Motivations for Bitcoin Technology Usage’, *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems - CHI EA ’16*, pp. 2872–2878. doi: 10.1145/2851581.2892500.

Kim, K., Research, D. S.-I. and 2015, U. (2015) ‘An acceptance model for smart watches: implications for the adoption of future wearable technology’, *emeraldinsight.com*. Available at: https://www.emeraldinsight.com/doi/abs/10.1108/IntR-05-2014-0126 (Accessed: 27 April 2019).

Kirschner, J. (2018) ‘Mind and Matter: (Re)membering, Performing, and Being’, in *Creative Selves / Creative Cultures*. Cham: Springer International Publishing, pp. 93–100. doi: 10.1007/978-3-319-47527-1_6.

Kokini, C. M. et al. (2012) ‘Considering Context: The Role of Mental Workload and Operator Control in Users’ Perceptions of Usability’, *International Journal of Human-Computer Interaction*, 28(9), pp. 543–559. doi: 10.1080/10447318.2011.622973.

Kornmesser, S. (2008) ‘Theoretizität im logischen empirismus und im strukturalismus - Erläutert am fallbeispiel des neurobiologischen konstruktivismus’, *Journal for General Philosophy of Science*, 39(1), pp. 53–67. doi: 10.1007/s10838-008-9062-0.

Koshy, P., Koshy, D. and McDaniel, P. (2014) ‘An analysis of anonymity in bitcoin using P2P network traffic’, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8437, pp. 469–485. doi: 10.1007/978-3-662-45472-5_30.

Kotamraju, N. P. and Van Der Geest, T. M. (2012) ‘The tension between user-centred design and e-government services’, *Behaviour and Information Technology*, 31(3), pp. 261–273. doi: 10.1080/0144929X.2011.563797.

Koteska, B., Karafiloski, E. and Mishev, A. (2017) ‘Blockchain implementation quality challenges: A literature review’, *CEUR Workshop Proceedings*, 1938, pp. 11–13.

Krombholz, K. et al. (2016) ‘The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy’, *Financial Cryptography and Data Security 2016*, 9604, pp. 555–580. doi: 10.1007/978-3-662-54970-4.

Krueger, R. and Casey, M. (2014) *Focus groups: A practical guide for applied research*. Available at: https://books.google.co.uk/books?hl=en&lr=&id=tXpZDwAAQBAJ&oi=fnd&pg=PT7&dq=Focus+groups:+A+practical+guide+for+applied+research.&ots=Psp48Rgq7y&sig=GvKoNXBu7vqvoJJDx4D3bw3hjVs (Accessed: 20 February 2019).

Kuo, C. and Perrig, A. (2009) ‘Security configuration for non-experts: A case study in wireless network configuration’, *igi-global.com*. Available at: https://www.igi-global.com/chapter/security-configuration-non-experts/29052 (Accessed: 25 September 2019).

Law, I. T. (2017) ‘B Lockchain 101 for G Overnments’, *The Committee of Experts on International Cooperation in Tax Matters: Fifteenth session*, (October). Available at:

http://www.un.org/esa/ffd/wp-content/uploads/2017/10/15STM_Blockchain-101.pdf.

Lee, S. and Koubek, R. J. (2010) 'Understanding user preferences based on usability and aesthetics before and after actual use', *Interacting with Computers*. Elsevier B.V., 22(6), pp. 530–543. doi: 10.1016/j.intcom.2010.05.002.

Leon, P. G. et al. (2012) 'Why Johnny Can't Opt Out : A Usability Evaluation of Tools to Limit Online Behavioral Advertising', *Carnegie Mellon University, Pittsburgh, PA*, 2011(12), pp. 589–598. doi: 10.1145/2207676.2207759.

Lesemann, E., Woletz, N. and Koerber, S. (2007) 'Combining methods to evaluate mobile usability', *Proceedings of the 9th international conference on Human computer interaction with mobile devices and services - MobileHCI '07*, pp. 444–447. doi: 10.1145/1377999.1378051.

Lewis, J. R. (1995) 'IBM Computer Usability Satisfaction Questionnaires: Psychometric Evaluation and Instructions for Use', *International Journal of Human-Computer Interaction*, 7(1), pp. 57–78. doi: 10.1080/10447319509526110.

Lewis, J. R. (2014) 'Usability: Lessons Learned. and Yet to Be Learned', *International Journal of Human-Computer Interaction*, 30(9), pp. 663–684. doi: 10.1080/10447318.2014.930311.

Lichtman, M. (2012) *Qualitative research in education: A user's guide: A user's guide*. Available at: https://books.google.co.uk/books?hl=en&lr=&id=bg-r3sW1PH0C&oi=fnd&pg=PR5&dq=Lichtman,+M.+(2006),+Qualitative+research+in+education:+A+user%27s+guide.+Thousand+Oaks,+CA:+Sage&ots=dxlOcFub3s&sig=3HyjsDRCeiIFqhX_lhW2rzZBK_8 (Accessed: 23 April 2019).

Lindgaard, G. and Chattratichart, J. (2007) 'Usability Testing : What Have We Overlooked?', *CHI 2007 Proceedings*, pp. 1415–1424. doi: 10.1145/1240624.1240839.

Link, C. et al. (2019) 'iCalm : Wearable Sensor and Network Architecture for Wirelessly Communicating and Logging Autonomic Activity'.

Liu, X. et al. (2017) 'Characterizing Smartwatch Usage in the Wild', *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services - MobiSys '17*, pp. 385–398. doi: 10.1145/3081333.3081351.

Looper, C. de (2016) *Why smartwatches need bots Bots could do for smartwatches what apps did for smartphones*. Available at: https://www.wareable.com/smartwatches/bots-smartwatches-2628 (Accessed: 18 December 2018).

Lu, T.-C. et al. (2016) 'Healthcare Applications of Smart Watches', *Applied Clinical Informatics*, 7(3), pp. 850–869. doi: 10.4338/ACI-2016-03-R-0042.

Lundell, J. and Bates, C. (2016) 'Understanding user experience journeys for a smart watch device', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9752, pp. 424–433. doi: 10.1007/978-3-319-39399-5_40.

Luther, W. J. and Olson, J. (2013) 'Bitcoin is Memory', *Ssrn*, p. 18. doi: 10.2139/ssrn.2275730.

Mainelli, M. and Smith, M. (2015) 'Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)', *The Journal of Financial Perspectives: FinTech*, 3(3), pp. 1–47. doi: 10.1016/j.ijfatigue.2009.12.013.

Mankoff, J., Fait, H. and Tran, T. (2005) 'Is your web page accessible?', *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '05*, p. 41. doi: 10.1145/1054972.1054979.

Markova, M. et al. (2007) 'MoBiS-Q', *Proceedings of the 9th international conference on Human computer interaction with mobile devices and services - MobileHCI '07*, pp. 238–245. doi:

10.1145/1377999.1378013.

Marvasti, A. (2018) ‘Research methods’, *The Cambridge Handbook of Social Problems*, 1, pp. 23–37. doi: 10.1017/9781108656184.003.

Maurer, B., Nelms, T. C. and Swartz, L. (2013) ‘“When perhaps the real problem is money itself!”: The practical materiality of Bitcoin’, *Social Semiotics*, 23(2), pp. 261–277. doi: 10.1080/10350330.2013.777594.

McHugh, M. L. (2003) ‘Descriptive Statistics, Part I: Level of Measurement’, *Journal for Specialists in Pediatric Nursing*. Edited by A. M. Villarruel, 8(1), pp. 35–37. doi: 10.1111/j.1744-6155.2003.tb00182.x.

McMillan, D. et al. (2017) ‘Situating Wearables’, *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI ’17*, pp. 3582–3594. doi: 10.1145/3025453.3025993.

Meiklejohn, S. et al. (2016) ‘A fistful of Bitcoins’, *Communications of the ACM*, 59(4), pp. 86–93. doi: 10.1145/2896384.

Miers, I. et al. (2013) ‘Zerocoin: Anonymous distributed e-cash from bitcoin’, *Proceedings - IEEE Symposium on Security and Privacy*, pp. 397–411. doi: 10.1109/SP.2013.34.

Mitnick, K. D. and Simon, W. L. (2003) *The Art of Deception: Controlling the Human Element in Security*, *John Wiley & Sons*. John Wiley & Sons. doi: 0471237124.

Moser, M., Bohme, R. and Breuker, D. (2013) ‘An inquiry into money laundering tools in the Bitcoin ecosystem’, *eCrime Researchers Summit, eCrime*. doi: 10.1109/eCRS.2013.6805780.

Nguyen, T. and Memon, N. (2017) ‘Smartwatches Locking Methods : A Comparative Study’, pp. 2–6.

Nielsen, J. (1992) ‘FINDING USABILITY PROBLEMS THROUGH HEURISTIC EVALUATION’, pp. 373–380.

Nielsen, J. (1993) ‘Usability Engineering, First’. Available at: https://scholar.google.co.uk/scholar?hl=en&as_sdt=0%2C5&q=Nielsen%2C+J.%2C+1993.+Usability+engineering.+Morgan+Kaufmann%2C+San+Francisco%2C+CA.&btnG= (Accessed: 13 February 2019).

Nielsen, J. (1995) ‘Heuristic evaluation of user interfaces’, *Proceedings of the SIGCHI conference on 1995*. Available at: https://dl.acm.org/citation.cfm?id=97281 (Accessed: 27 April 2019).

Nordman, E. et al. (2017) ‘The Growing Impact of Wearable Technology 2’. Available at: https://www.naic.org/cipr_newsletter_archive/vol23.pdf (Accessed: 27 April 2019).

Nylander, S., Lundquist, T. and Brännström, A. (2009) ‘At home and with computer access’, *Proceedings of the 27th international conference on Human factors in computing systems - CHI 09*, p. 1639. doi: 10.1145/1518701.1518951.

Oakley, I. and Lee, D. (2014) ‘Interaction on the edge’, *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI ’14*, pp. 169–178. doi: 10.1145/2556288.2557138.

Olalere, A. and Lazar, J. (2011) ‘Accessibility of U.S. federal government home pages: Section 508 compliance and site accessibility statements’, *Government Information Quarterly*. Elsevier Inc., 28(3), pp. 303–309. doi: 10.1016/j.giq.2011.02.002.

Ølnes, S. and Jansen, A. (2018) ‘Blockchain technology as infrastructure in public sector’, (1), pp. 1–10. doi: 10.1145/3209281.3209293.

Olsen, W. (2004) ‘Biographical Note’, pp. 1–30.

Orlikowski, W. J. and Baroudi, J. J. (1991) ‘Studying Information Technology in Organizations:

Research Approaches and Assumptions', *Information Systems Research*, 2(1), pp. 1–28. doi: 10.1287/isre.2.1.1.

Ormrod, J. E. and Leedy, P. D. (2005) *Practical research: Planning and design*. Internatio, *New Jersey, Pearson Merill Prentice hall*. Internatio. Pearson Education International.

Papadomichelaki, X. and Mentzas, G. (2012) 'E-GovQual: A multiple-item scale for assessing e-government service quality', *Government Information Quarterly*. Elsevier Inc., 29(1), pp. 98–109. doi: 10.1016/j.giq.2011.08.011.

Patton, M. Q. (2005) 'Qualitative Research', in *Encyclopedia of Statistics in Behavioral Science*. Chichester, UK: John Wiley & Sons, Ltd. doi: 10.1002/0470013192.bsa514.

Peng, S. (2013) 'BITCOIN : Cryptography , Economics , and the Future'. doi: 10.1097/01.shk.0000209554.46704.64.

Petrie, H. et al. (2006) 'Remote usability evaluations With disabled people', *Proceedings of the SIGCHI conference on Human Factors in computing systems - CHI '06*, p. 1133. doi: 10.1145/1124772.1124942.

Petrie, H. and Power, C. (2012) 'What do users really care about?', *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems - CHI '12*, p. 2107. doi: 10.1145/2207676.2208363.

Pizza, S. et al. (2016) 'Smartwatch in *vivo*', *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*, 2(1), pp. 5456–5469. doi: 10.1145/2858036.2858522.

Plotnick, L., Hiltz, S. R. and Burns, M. (2013) '"You've Been Warned?"', *International Journal of Information Systems for Crisis Response and Management*, 5(3), pp. 37–62. doi: 10.4018/ijiscram.2013070103.

Ramon Llamas, Jitesh Ubrani, M. S. (2018) *New Wearables Forecast from IDC Shows Smartwatches Continuing Their Ascendance While Wristbands Face Flat Growth*. Available at: https://www.idc.com/getdoc.jsp?containerId=prUS440 (Accessed: 28 January 2019).

Rawassizadeh, R. et al. (2015) 'Lesson Learned from Collecting Quantified Self Information via Mobile and Wearable Devices', *Journal of Sensor and Actuator Networks*, 4(4), pp. 315–335. doi: 10.3390/jsan4040315.

Rawassizadeh, R., Price, B. A. and Petre, M. (2014) 'Wearables: Has the Age of Smartwatches Finally Arrived?', *Commun. ACM*, 58(1), pp. 45–47. doi: 10.1145/2629633.

Reeder, B. and David, A. (2016) 'Health at hand: A systematic review of smart watch uses for health and wellness', *Journal of Biomedical Informatics*. Elsevier Inc., 63, pp. 269–276. doi: 10.1016/j.jbi.2016.09.001.

Reid, F. and Harrigan, M. (2013) 'An analysis of anonymity in the bitcoin system', *Security and Privacy in Social Networks*, pp. 197–223. doi: 10.1007/978-1-4614-4139-7_10.

Reid, J. M. et al. (1999) 'Metabolic activation of dacarbazine by human cytochromes P450: The role of CYP1A1, CYP1A2, and CYP2E1', *Clinical Cancer Research*, 5(8), pp. 2192–2197. doi: 10.1126/science.Liquids.

Renaud, K. (2012) 'Blaming Noncompliance Is Too Convenient : What Really Causes Information Breaches ? Why People Don ' t Comply', *Security*, 10(June), pp. 57–63. doi: 10.1109/MSP.2011.157.

Reynaga, G., Chiasson, S. and van Oorschot, P. C. (2015) 'Heuristics for the evaluation of captchas on smartphones', *Proceedings of the 2015 British HCI Conference on - British HCI '15*, pp. 126–135. doi: 10.1145/2783446.2783583.

Riihiaho, S. (2017) 'Usability Testing', *The Wiley Handbook of Human Computer Interaction Set*, 1, pp. 255–275. doi: 10.1002/9781118976005.ch14.

Rinaudo, J.-L. (2018) ‘Robots de téléprésence et intersubjectivation’, *L’Évolution Psychiatrique*, 11(4), pp. 323–336. doi: 10.1016/j.evopsy.2018.01.001.

Robertson, J. (2001) ‘Know your enemy’, *Ecos*, 22(1), pp. 96–101. doi: 10.1080/00139157.1971.9930601.

Rohnke, A. T. and Yahner, R. H. (2008) ‘Long-term effects of wastewater irrigation on habitat and a bird community in central Pennsylvania’, *Wilson Journal of Ornithology*, 120(1), pp. 146–152. doi: 10.1207/s15327590ijhc1803.

Sas, C. and Khairuddin, I. E. (2015a) ‘Exploring Trust in Bitcoin Technology’, *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction on - OzCHI ’15*. Elsevier B.V., 4(1), pp. 338–342. doi: 10.1145/2838739.2838821.

Sas, C. and Khairuddin, I. E. (2015b) ‘Exploring Trust in Bitcoin Technology’, *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction on - OzCHI ’15*, pp. 338–342. doi: 10.1145/2838739.2838821.

Sasse, A. (2015) ‘Scaring and Bullying People into Security Won’t Work’, *IEEE Security and Privacy*, 13(3), pp. 80–83. doi: 10.1109/MSP.2015.65.

Sasse, M. A., Flechais, I. and Famed Hacker Kevin, S. (2005) ‘Chapter 2 Usable Security Why Do We Need It? How Do We Get It? “THE WEAKEST LINK IN THE CHAIN” OF SYSTEM’, pp. 13–30.

Saunders, M., Lewis, P. and Thornhill, A. (2017) *Research Methods for Bus Stds 5th Edition 2017*.

Sauro, J. and Kindlund, E. (2005) ‘A method to standardize usability metrics into a single score’, *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI ’05*, p. 401. doi: 10.1145/1054972.1055028.

Schedler, K. and Summermatter, L. (2007) ‘Customer orientation in electronic government: Motives and effects’, *Government Information Quarterly*, 24(2), pp. 291–311. doi: 10.1016/j.giq.2006.05.005.

Schivinski, B. and Dabrowski, D. (2012) ‘The Effect of Social Media Communication on Consumer Perceptions of Brands’.

Schrack, J. A., Gresham, G. and Wanigatunga, A. A. (2017) ‘Understanding physical activity in cancer patients and survivors: new methodology, new challenges, and new opportunities’, *Cold Spring Harbor molecular case studies*, 3(4). doi: 10.1101/mcs.a001933.

Seebacher, S. and Sch, R. (2017) ‘Blockchain Technology as an Enabler of Service Systems : A Structured Literature Review’, pp. 12–23. doi: 10.1007/978-3-319-56925-3.

Sekaran, U. and Bougie, R. (2016) *Research methods for business: A skill building approach*. Available at: https://books.google.co.uk/books?hl=en&lr=&id=Ko6bCgAAQBAJ&oi=fnd&pg=PA19&dq=Sekaran+%26+Bougie&ots=2B2RU0JViL&sig=MMK891MApx82PvwmdEOJ0qbyX78 (Accessed: 24 April 2019).

Shannon, S. E. (2005) ‘Three Approaches to Qualitative Content Analysis’, (December 2005). doi: 10.1177/1049732305276687.

Shay, R. et al. (2014) ‘Can long passwords be secure and usable?’, *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI ’14*, pp. 2927–2936. doi: 10.1145/2556288.2557377.

Shirazi, A. S. and Henze, N. (2015) ‘Assessment of Notifications on Smartwatches’, *International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct*, (September), pp. 1111–1116. doi: 10.1145/2786567.2794338.

Siegel, S. (1956) ‘Nonparametric statistics for the behavioral sciences.’, *Nonparametric Statistics for Behavioral Sciences*, pp. 213–214. doi: 10.1017/CBO9781107415324.004.

Sieger, H. and Möller, S. (2012) ‘Gender differences in the perception of security of mobile phones’, *Proceedings of the 14th international conference on Human-computer interaction with mobile devices and services companion - MobileHCI ’12*, p. 107. doi: 10.1145/2371664.2371685.

Silva, P. F. et al. (2016) ‘Wearable textile bioinspired antenna for 2G, 3G, and 4G systems’, *Microwave and Optical Technology Letters*, 58(12), pp. 2818–2823. doi: 10.1002/mop.30150.

Simpson, A. (2014) *Who will drastically innovate the usability of Bitcoin, Quara.com*. Available at: https://www.quora.com/profile/Arianna-Simpson (Accessed: 30 December 2017).

Singh, P. et al. (2013) ‘Performance comparison of executing fast transactions in bitcoin network using verifiable code execution’, *Proceedings - 2nd International Conference on Advanced Computing, Networking and Security, ADCONS 2013*, pp. 193–198. doi: 10.1109/ADCONS.2013.42.

Skudnov, R. (2012) ‘Bitcoin clients’, *Instructor*, 3(12), p. 32. Available at: http://bitcoinmalaysia.com/wp-content/uploads/2012/12/Bitcoin_Clients_Thesis_Skudnov_Rostislav.pdf.

Sousa, R., Smeets, J. B. J. and Brenner, E. (2012) ‘Does size matter?’, *Perception*, 41(12), pp. 1532–1534. doi: 10.1068/p7324.

Spinnewijn, W. (2009) ‘Undercover’, *Huisarts en Wetenschap*, 52(7), p. 311. doi: 10.1007/BF03085655.

Strauss, A. and Corbin, J. (1990) *Basics of qualitative research*. Available at: https://genderopen-develop.cms.hu-berlin.de/bitstream/handle/25595/12/whatsnew7.pdf?sequence=1 (Accessed: 24 April 2019).

Sultan, N. (2015) ‘Reflective thoughts on the potential and challenges of wearable technology for healthcare provision and medical education’, *Elsevier*. Available at: https://www.sciencedirect.com/science/article/pii/S0268401215000468 (Accessed: 27 April 2019).

Swan, M. (2015) *Blockchain BLUEPRINT FOR A NEW ECONOMY*.

T Cohen - US Patent 9, 870,357 and 2018, undefined (2013) ‘Techniques for translating text via wearable computing device’, *Google Patents*. Available at: https://patents.google.com/patent/US9870357B2/en (Accessed: 7 February 2019).

Tabane, E., Zuva, T. and Ngwira, S. M. (2015) ‘The Socio-Economic Impact of Internet of Things towards Smart Cities’, *researchgate.net*, pp. 102–109. Available at: https://www.researchgate.net/profile/Natalie_Walker4/publication/280027642_Proceedings_of_the_Third_International_Conference_on_Digital_Information_Processing_E-Business_and_Cloud_Computing_Reduit_Mauritius_2015/links/55a4739208ae00cf99c902bf.pdf#page=104 (Accessed: 27 April 2019).

Tashakkori, A. and Teddlie, C. (1998) *Mixed methodology: Combining qualitative and quantitative approaches*. Available at: https://books.google.co.uk/books?hl=en&lr=&id=qtW04-pRJZ0C&oi=fnd&pg=PR9&dq=Tashakkori+and+Teddlie,+1998&ots=6gbsmw8atK&sig=eKlh-NUIKEqAF6wjbyYV5CmhopQ (Accessed: 23 April 2019).

Tohidi, M. et al. (2006) ‘Getting the right design and the design right’, *Proceedings of the SIGCHI conference on Human Factors in computing systems - CHI ’06*, 1, p. 1243. doi: 10.1145/1124772.1124960.

Trochim, W. M. . K. . (2006) *The Research Methods Knowledge Base Author : Second Edition*, *Knowledge Creation Diffusion Utilization*. Available at: http://www.socialresearchmethods.net/kb/.

Tullis, T. and Albert, B. (2013) 'Background', *Measuring the User Experience*, pp. 15–40. doi: 10.1016/B978-0-12-415781-1.00002-9.

Valaei, N. and Rezaei, S. (2016) 'Job satisfaction and organizational commitment: An empirical investigation among ICT-SMEs', *Management Research Review*, 39(12), pp. 1663–1694. doi: 10.1108/MRR-09-2015-0216.

van Velsen, L. et al. (2009) 'Requirements engineering for e-Government services: A citizen-centric approach and case study', *Government Information Quarterly*. Elsevier Inc., 26(3), pp. 477–486. doi: 10.1016/j.giq.2009.02.007.

Venkatesh, V. and Agarwal, R. (2006) 'Turning Visitors into Customers: A Usability-Centric Perspective on Purchase Behavior in Electronic Channels', *Management Science*, 52(3), pp. 367–382. doi: 10.1287/mnsc.1050.0442.

Venkatesh, V., Chan, F. K. Y. and Thong, J. Y. L. (2012) 'Designing e-government services: Key service attributes and citizens' preference structures', *Journal of Operations Management*, 30(1–2), pp. 116–133. doi: 10.1016/j.jom.2011.10.001.

Venkatesh, V., Hoehle, H. and Aljafari, R. (2014) 'A usability evaluation of the Obamacare website', *Government Information Quarterly*. Elsevier B.V., 31(4), pp. 669–680. doi: 10.1016/j.giq.2014.07.003.

Verdegem, P. and Verleye, G. (2009) 'User-centered E-Government in practice: A comprehensive model for measuring user satisfaction', *Government Information Quarterly*. Elsevier Inc., 26(3), pp. 487–497. doi: 10.1016/j.giq.2009.03.005.

Virzi, R. A. (1992) 'Refining the Test Phase of Usability Evaluation: How Many Subjects Is Enough?', *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 34(4), pp. 457–468. doi: 10.1177/001872089203400407.

Virzi, R. A., Sorce, J. F. and Herbert, L. B. (1993) 'A Comparison of Three Usability Evaluation Methods: Heuristic, Think-Aloud, and Performance Testing', *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 37(4), pp. 309–313. doi: 10.1177/154193129303700412.

Wahyuni, D. (2012) 'The Research Design Maze : Understanding Paradigms , Cases , Methods and Methodologies', *JAMAR*, 10(1), pp. 69–80. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103082 (Accessed: 24 April 2019).

Walsham, G. (1995) 'The Emergence of Interpretivism in IS Research', *Information Systems Research*, 6(4), pp. 376–394. doi: 10.1287/isre.6.4.376.

Wang, G. et al. (2009) 'Effect of enhancement of catalyst-oil mixing heat on residue catalytic cracking', *Shiyou Xuebao, Shiyou Jiagong/Acta Petrolei Sinica (Petroleum Processing Section)*, 25(3), pp. 313–318. doi: 10.1080/10556781003625177.

Welle Donker-Kuijer, M., de Jong, M. and Lentz, L. (2010) 'Usable guidelines for usable websites? An analysis of five e-government heuristics', *Government Information Quarterly*. Elsevier Inc., 27(3), pp. 254–263. doi: 10.1016/j.giq.2010.02.006.

Wells, J. D. et al. (2010) 'The Effect of Perceived Novelty on the Adoption of Information Technology Innovations: A Risk/Reward Perspective', *Decision Sciences*, 41(4), pp. 813–843. doi: 10.1111/j.1540-5915.2010.00292.x.

Whalen, T. (2011) 'Security as if people mattered', *IEEE Security and Privacy*, 9(4), pp. 64–67. doi: 10.1109/MSP.2011.92.

White, M., Killmeyer, J., and Chew, B. (2019) *Will blockchain transform the public sector?* Available at: https://www2.deloitte.com/insights/us/en/industry/public-sector/understanding-basics-of-blockchain-in-government.html (Accessed: 28 February 2019).

Whitten, A. and Tygar, J. D. (2005) 'Why Johnny Can't Encrypt: A Usability Evaulation of PHP 5.0', *Designing Secure Systems that People Can Use*, 1999(October), pp. 679–702. doi: 169-184.

Wich, M., Kramer, T. and Kramer, T. (2015) 'Enhanced Human-Computer Interaction for Business Applications on Mobile Devices : A Design-Oriented Development of a Usability Evaluation Questionnaire Devices : A Design-Oriented Development of a Usability Evaluation Questionnaire', (February 2016). doi: 10.1109/HICSS.2015.63.

Wiig, A. and Wyly, E. (2016) 'Introduction: Thinking through the politics of the smart city', *Urban Geography*, 37(4), pp. 485–493. doi: 10.1080/02723638.2016.1178479.

Wong, S. et al. (2017) 'Assessing the usability of smartwatches for academic cheating during exams', *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services - MobileHCI '17*, pp. 1–11. doi: 10.1145/3098279.3098568.

Wright, A. and De Filippi, P. (2015) 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia', *Ssrn*. doi: 10.2139/ssrn.2580664.

Wu, L. H., Wu, L. C. and Chang, S. C. (2016) 'Exploring consumers' intention to accept smartwatch', *Computers in Human Behavior*. Elsevier Ltd, 64, pp. 383–392. doi: 10.1016/j.chb.2016.07.005.

Wüst, K. and Gervais, A. (no date) 'Do you need a Blockchain ?', pp. 1–7.

Xu, C., Pathak, P. H. and Mohapatra, P. (2015) 'Finger-writing with Smartwatch', *Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications - HotMobile '15*, pp. 9–14. doi: 10.1145/2699343.2699350.

Yelowitz, A. et al. (2015) 'The Acceptance of Bitcoin in Indonesia: Extended TAM with IDT', *Journal of Business and Management*, 4(1), pp. 28–38. doi: 10.1145/2838739.2838821.

Yelowitz, A. and Wilson, M. (2015) 'Characteristics of Bitcoin users: an analysis of Google search data', *Applied Economics Letters*, 22(13), pp. 1030–1036. doi: 10.1080/13504851.2014.995359.

Yeratziotis, A., Pottas, D. and van Greunen, D. (2012) 'A Usable Security Heuristic Evaluation for the Online Health Social Networking Paradigm', *International Journal of Human-Computer Interaction*, 28(10), pp. 678–694. doi: 10.1080/10447318.2011.654202.

Yin, X., Zhang, J. and Wang, X. (2004) 'Sequential injection analysis system for the determination of arsenic by hydride generation atomic absorption spectrometry', *Fenxi Huaxue*, 32(10), pp. 1365–1367. doi: 10.1017/CBO9781107415324.004.

Yli-Huumo, J. et al. (2016) 'Where Is Current Research on Blockchain Technology?-A Systematic Review.', *PloS one*, 11(10), p. e0163477. doi: 10.1371/journal.pone.0163477.

Yu, L. and Yu, L. (2016) 'A System View of Financial Blockchains', (March). doi: 10.1109/SOSE.2016.66.

Zaharias, P. and Poylymenakou, A. (2009) 'Developing a usability evaluation method for e-learning applications: Beyond functional usability', *International Journal of Human-Computer Interaction*, 25(1), pp. 75–98. doi: 10.1080/10447310802546716.

von Zezschwitz, E., Dunphy, P. and De Luca, A. (2013) 'Patterns in the wild', *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services - MobileHCI '13*, p. 261. doi: 10.1145/2493190.2493231.

Appendix A

<u>Bitcoin Wallet Questionnaire</u>

Please choose the one most appropriate response to each statement

Personal information					
No	**Please select the most appropriate answer**				
1	Please select your gender:	Male	Female	Other	Prefer not to say
2	Please select your age:	19-24	25-29	30 -34	35 -39
3	Please select your educational level:	1^{st} year	2^{nd} Year	3^{rd} Year	Bachelor degree
4	How do you access Internet services?	Smartphone	Tablet	Laptop	Desktop computer

Usability Evaluation						
	Learnability	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
To what extent do you agree with the following statements?						
5	I can easily create and setup my own Bitcoin Wallet account	Δ	Δ	Δ	Δ	Δ
6	I can easily find my Bitcoin Wallet address.	Δ	Δ	Δ	Δ	Δ
7	I can easily locate the names and functions on Bitcoin Wallet	Δ	Δ	Δ	Δ	Δ
8	The help messages of Bitcoin Wallet are **NOT** helpful.	Δ	Δ	Δ	Δ	Δ
9	I can easily view my coin balance.	Δ	Δ	Δ	Δ	Δ
10	I can easily view my Bitcoin address book.	Δ	Δ	Δ	Δ	Δ
11	I can easily find the confirmed transactions in my Bitcoin wallet.	Δ	Δ	Δ	Δ	Δ
12	I can easily and quickly send money.	Δ	Δ	Δ	Δ	Δ
Efficiency		**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
To what extent do you agree with the following statements?						
13	I can create a Bitcoin Wallet account in no time.	Δ	Δ	Δ	Δ	Δ
14	I find the sequence of screens when creating my wallet account confusing.	Δ	Δ	Δ	Δ	Δ
15	I can efficiently send	Δ	Δ	Δ	Δ	Δ

	payment using the Quick Send option.					
16	I can efficiently create a payment request.	Δ	Δ	Δ	Δ	Δ
17	I can efficiently enable two factor authentications on my wallet account.	Δ	Δ	Δ	Δ	Δ
18	I can efficiently send coins by mail and SMS.	Δ	Δ	Δ	Δ	Δ
19	I found the Bitcoin Wallet fast to use.	Δ	Δ	Δ	Δ	Δ
20	I can efficiently back up my wallet using the available options.	Δ	Δ	Δ	Δ	Δ
21	On average, I have to do many clicks to navigate my wallet	Δ	Δ	Δ	Δ	Δ
22	Overall, I can efficiently change my account settings.	Δ	Δ	Δ	Δ	Δ
23	Overall, I was able to complete the tasks and scenarios quickly and accurately.	Δ	Δ	Δ	Δ	Δ
Memorability		**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
To what extent do you agree with the following statements?						
24	I can easily remember the steps required to create a Bitcoin Wallet account.	Δ	Δ	Δ	Δ	Δ
25	I can easily remember the steps required to change the settings of my Bitcoin Wallet account.	Δ	Δ	Δ	Δ	Δ
26	I can easily remember the steps required to send a payment through my Bitcoin Wallet account.	Δ	Δ	Δ	Δ	Δ
27	I can recall the steps required to change my Bitcoin Wallet address.	Δ	Δ	Δ	Δ	Δ
28	I can recall the steps required to change my Bitcoin Wallet security settings.	Δ	Δ	Δ	Δ	Δ
29	I can recall the steps needed to change the time of inactivity logout.	Δ	Δ	Δ	Δ	Δ
30	I can remember the steps required to change notification options when a payment is sent or received from my wallet.	Δ	Δ	Δ	Δ	Δ
	It is hard to remember the	Δ	Δ	Δ	Δ	Δ

31	secret phrase that is used to help verify my identity in case of losing the wallet identifier.					
Error & Recoverability		**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
To what extent do you agree with the following statements?						
32	It is difficult to make errors in an action because Bitcoin Wallet does not allow me to skip or ignore any of the steps.	Δ	Δ	Δ	Δ	Δ
33	It is easy to miss out notifications or messages when using Bitcoin Wallet frequently.	Δ	Δ	Δ	Δ	Δ
34	It is easy to see errors because the Bitcoin wallet indicates a highlighted message around errors.	Δ	Δ	Δ	Δ	Δ
35	It is easy to fill in the Bitcoin address in address field when transfer coins to other address.	Δ	Δ	Δ	Δ	Δ
36	I can clearly see the progress in an action as the whole process is indicated.	Δ	Δ	Δ	Δ	Δ
37	It is easy to recover my Bitcoin Wallet login password.	Δ	Δ	Δ	Δ	Δ
38	It is hard to recover my Bitcoin Wallet login password.	Δ	Δ	Δ	Δ	Δ
39	It is not easy to reverse any transaction with Bitcoin wallet	Δ	Δ	Δ	Δ	Δ
40	Error messages are easy to read and understand.					
	Help & Training	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
To what extent do you agree with the following statements?						
41	I can easily use the online help to find the relevant answer to solve the problems.	Δ	Δ	Δ	Δ	Δ
42	It is easy to find the help option when I needed.	Δ	Δ	Δ	Δ	Δ
43	It is easy to switch between the online help and my current work while using Bitcoin Wallet.	Δ	Δ	Δ	Δ	Δ
44	The training provided to use	Δ	Δ	Δ	Δ	Δ

	Bitcoin Wallet is useful and easy to understand.					
45	Overall, the information provided with Bitcoin Wallet (such as online help, on-screen messages, and other documentation) is clear.	Δ	Δ	Δ	Δ	Δ
Security		**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
To what extent do you agree with the following statements?						
46	I can easily learn to use the security functions of Bitcoin wallet.	Δ	Δ	Δ	Δ	Δ
47	I can easily find the security functions grouped into logical zones, and there are headings used to separate the zones.	Δ	Δ	Δ	Δ	Δ
48	I can easily find and change the security selection defaults.	Δ	Δ	Δ	Δ	Δ
49	I can easily change the level of security detail.	Δ	Δ	Δ	Δ	Δ
50	I can easily change between novice and expert security levels.	Δ	Δ	Δ	Δ	Δ
51	Bitcoin Wallet grants me access to my account based on various authentications, such as password, biometrics and SMS one-time passwords (OTP).	Δ	Δ	Δ	Δ	Δ
52	I feel in control over the situation when using Bitcoin Wallet.	Δ	Δ	Δ	Δ	Δ
53	I can easily access protected or confidential areas without certain passwords.	Δ	Δ	Δ	Δ	Δ
54	Bitcoin Wallet warns me if I am about to do any security breaches.	Δ	Δ	Δ	Δ	Δ
55	Bitcoin Wallet notifies me about my access privileges.	Δ	Δ	Δ	Δ	Δ
56	I can easily cancel any security operations in progress.	Δ	Δ	Δ	Δ	Δ
57	I can easily understand the language used relating to security functions.	Δ	Δ	Δ	Δ	Δ
58	Overall, I am satisfied with the security options provided by Bitcoin Wallet.	Δ	Δ	Δ	Δ	Δ
59	Overall, I am satisfied with	Δ	Δ	Δ	Δ	Δ

	the level of security provided by Bitcoin Wallet.					
60	Overall, I am satisfied with the protection provided by Bitcoin Wallet to ensure my privacy.	Δ	Δ	Δ	Δ	Δ
61	Overall, I am satisfied with the anonymity provided by Bitcoin Wallet.	Δ	Δ	Δ	Δ	Δ
Subjective Satisfaction		**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
To what extent do you agree with the following statements?						
62	Overall, I am satisfied with the level of anonymity provided by Bitcoin Wallet.	Δ	Δ	Δ	Δ	Δ
63	Overall, I am satisfied with how easy it is to use Bitcoin Wallet.	Δ	Δ	Δ	Δ	Δ
65	It is simple to use this system.	Δ	Δ	Δ	Δ	Δ
66	I could effectively complete the tasks using Bitcoin Wallet.	Δ	Δ	Δ	Δ	Δ
67	I am happy about the speed and accuracy to complete the tasks using Bitcoin Wallet.	Δ	Δ	Δ	Δ	Δ
68	I felt comfortable using Bitcoin Wallet.	Δ	Δ	Δ	Δ	Δ
69	It was easy to learn to use Bitcoin Wallet.	Δ	Δ	Δ	Δ	Δ
70	I believe I could become productive quickly using Bitcoin Wallet.	Δ	Δ	Δ	Δ	Δ
71	The Bitcoin Wallet client shows error messages that clearly indicate how to fix problems.	Δ	Δ	Δ	Δ	Δ
72	Whenever I made a mistake using the Bitcoin Wallet, I could recover easily and quickly.	Δ	Δ	Δ	Δ	Δ
73	It was easy to find the information I needed.	Δ	Δ	Δ	Δ	Δ
74	The information provided for Bitcoin Wallet was easy to understand.	Δ	Δ	Δ	Δ	Δ
75	The information was effective in helping me complete the tasks.	Δ	Δ	Δ	Δ	Δ
76	The organisation of information on Bitcoin Wallet screens is clear.	Δ	Δ	Δ	Δ	Δ
77	The interface of Bitcoin	Δ	Δ	Δ	Δ	Δ

	Wallet is pleasant.					
78	I liked using the interface of Bitcoin Wallet.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
79	Bitcoin Wallet client has all the functions and capabilities I expect it to have.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
80	Overall, I am satisfied with Bitcoin Wallet.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**

Appendix B

Credit card questionnaire (Part two)

Personal information					
No	**Please select the most appropriate answer**				
1	Please select your gender:	Male	Female	Other	Prefer not to say
2	Please select your age:	19-24	25-29	30 -34	35 -39
3	Please select your educational level:	1st year	2nd Year	3rd Year	Bachelor degree
4	How do you access Internet services?	Smartphone	Tablet	Laptop	Desktop computer

.Usability Evaluation						
	Learnability	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
To what extent do you agree with the following statements?						
5	I can easily conduct online payment transactions using my credit or debit card.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
6	I can quickly conduct online payment using my credit or debit card.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
7	I can easily fill in the credit or debit card online form to make payment.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
8	I can easily fill in various online forms to make online payments using my credit or debit card.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
9	I find it easy to understand credit or debit card online payment forms.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
10	The help messages for credit or debit cards are helpful.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
11	I know if the online transaction is successful or not when I conduct a transaction using my credit or debit card.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
12	I can easily cancel any online transaction when using my credit or debit card.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
13	It is easy to find out about my confirmed transactions when using my credit or	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**

	debit card.					
Efficiency		**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
To what extent do you agree with the following statements?						
14	I can efficiently conduct any online transaction with my credit or debit card.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
15	I find filling in forms when conducting online payments using my credit or debit card confusing.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
16	I can efficiently conduct small amount online payment (e.g. £1) using my credit or debit card.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
18	I can efficiently follow the sequence of the filling in forms when conducting online transactions with my credit or debit card.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
19	On average, I have to do many clicks to conduct an online payment using my credit or debit card.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
20	Overall, I find it convenient to transact online with my credit or debit card over another payment method because it’s easier to use.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
21	Overall, I can transact and conduct online payment using my credit or debit card easily.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
Memorability		**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
To what extent do you agree with the following statements?						
22	I can easily remember the steps required to conduct online payment using my credit or debit card.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
24	I can easily remember the sequence for conducting online transactions using my credit or debit card.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
25	I can easily remember the pin code of my credit or debit card to authorise transactions.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
26	I can recall the steps required to change the pin number of my credit or debit card.	**Δ**	**Δ**	**Δ**	**Δ**	**Δ**
Error & Recoverability		**Strongly**	**Agree**	**Neutral**	**Disagree**	**Strongly**

		Agree				Disagree
To what extent do you agree with the following statements?						
27	It is difficult to make errors in filling in the online form when conducting online transactions by credit or debit card.	Δ	Δ	Δ	Δ	Δ
28	It is easy to miss out notifications or messages when conducting online transactions using my credit or debit card.	Δ	Δ	Δ	Δ	Δ
29	It is easy to see errors when filling in the online credit or debit card form and a highlighted message is shown around errors.	Δ	Δ	Δ	Δ	Δ
30	It is easy to fill the in the right data in a data entry field because the number of character spaces available in a field is indicated.	Δ	Δ	Δ	Δ	Δ
31	I can clearly see the progress in an action as the whole process is indicated.	Δ	Δ	Δ	Δ	Δ
32	It is easy to recover my credit or debit card security number.	Δ	Δ	Δ	Δ	Δ
33	It is hard to reverse any payment or transaction conducted by debit or credit card.	Δ	Δ	Δ	Δ	Δ
	Help & Training	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
To what extent do you agree with the following statements?						
34	I can easily use online help to find the relevant answer to solve any problems.	Δ	Δ	Δ	Δ	Δ
35	It is easy to find the help option while conducting transactions using my credit or debit card.	Δ	Δ	Δ	Δ	Δ
36	The training provided to conduct online transactions and filling in the credit or debit card form is easy to understand.	Δ	Δ	Δ	Δ	Δ
37	Overall, the information provided related to conducting online transactions using credit or debit cards (such as online help, on-screen messages,	Δ	Δ	Δ	Δ	Δ

	and other documentation) is clear.					
Security		**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
To what extent do you agree with the following statements?						
38	I trust the total security provided by my bank when conducting online transaction using my credit or debit card	Δ	Δ	Δ	Δ	Δ
39	I am very aware that banks or shops can keep records about my payments when I conduct transactions using my credit or debit card.	Δ	Δ	Δ	Δ	Δ
40	I am comfortable with the security level that is provided by my credit or debit card issuer.	Δ	Δ	Δ	Δ	Δ
41	I feel in control over the situation when conducting online transactions using my credit or debit card.	Δ	Δ	Δ	Δ	Δ
42	When conducting online transactions using my credit or debit card, I get alerted about any security issues.	Δ	Δ	Δ	Δ	Δ
43	I can easily cancel any security operations in progress.	Δ	Δ	Δ	Δ	Δ
44	I can easily understand the language used relating to security issues.	Δ	Δ	Δ	Δ	Δ
45	Security awareness is provided when I conduct online transactions or fill in the credit or debit card form.	Δ	Δ	Δ	Δ	Δ
46	Overall, I am satisfied with the security level provided by my credit or debit card issuer.	Δ	Δ	Δ	Δ	Δ
47	Overall, I am satisfied with the level of control provided when I transact using my credit or debit card.	Δ	Δ	Δ	Δ	Δ
48	Overall, I am satisfied with the protection provided by my credit or debit card to ensure my privacy.	Δ	Δ	Δ	Δ	Δ
Subjective Satisfaction		**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
Subjective Satisfaction						
49	Overall, I am satisfied using	Δ	Δ	Δ	Δ	Δ

	my credit or debit card to do online transactions					
50	Overall, I am satisfied with how easy it is to use my credit or debit card for online transactions	Δ	Δ	Δ	Δ	Δ
51	It is simple to fill in and use credit or debit card online forms.	Δ	Δ	Δ	Δ	Δ
52	I can effectively transact using my credit or debit card.	Δ	Δ	Δ	Δ	Δ
53	I am able to efficiently complete my online transactions using credit or debit card.	Δ	Δ	Δ	Δ	Δ
54	I felt comfortable using credit or debit card.	Δ	Δ	Δ	Δ	Δ
55	It is easy to learn to use credit or debit cards for online transactions.	Δ	Δ	Δ	Δ	Δ
56	I believe I could become productive quickly using credit or debit cards for conducting online transactions.	Δ	Δ	Δ	Δ	Δ
57	It is clearly indicated how to fix problems when conducting online transactions using my credit or debit card.	Δ	Δ	Δ	Δ	Δ
58	It is easy and quick to recover from any errors when conducting online transactions using credit or debit card.	Δ	Δ	Δ	Δ	Δ
59	It is easy to find the information I need to conduct online transactions using credit or debit card.	Δ	Δ	Δ	Δ	Δ
60	The information provided when conducting online transactions using credit or debit card is easy to understand.	Δ	Δ	Δ	Δ	Δ
61	Information is effective in helping me to conduct online transactions using credit or debit card.	Δ	Δ	Δ	Δ	Δ
62	The organisation of information required to conduct online transactions on the screens is clear.	Δ	Δ	Δ	Δ	Δ
63	Paying with credit or debit	Δ	Δ	Δ	Δ	Δ

	card online is pleasant.					
64	I like using credit or debit cards to conduct online transactions.	Δ	Δ	Δ	Δ	Δ
65	All the functions and capabilities I expect it to have to conduct online transactions using credit or debit card are useful.	Δ	Δ	Δ	Δ	Δ
66	Overall, I am satisfied with paying online using credit or debit card.	Δ	Δ	Δ	Δ	Δ

Appendix C

Table: Chi-Square results

No	Main Feature	Sub-Feature	**User views**	**Groups**		**Chi**	**df**	**P-value**
				Novice	**Expert**			
1	Design	Watch Size	Positive	22(71%)	12 (31%)	11.173	1	0.001
			Negative	9(29%)	27 (69%)			
		Main Menu	Positive	6 (67%)	9 (41%)	1.697	1	0.193
			Negative	3 (33%)	13 (59%)			
		Icon colours & Graphics	Positive	3 (33%)	12 (57%)	1.429	1	0.232
			Negative	6 (67%)	9 (43%)			
		Watch faces	Positive	6 (60%)	11(34%)	2.077	1	0.15
			Negative	4 (40%)	21 (66%)			
		Total Design	Positive	37 (46%)	22 (24%)	9.081	1	0.003
			Negative	44 (54%)	70 (76%)			
2	Applications & usefulness’	Built-in Apps	Positive	57(51%)	29(37%)	3.49	1	0.062
			Negative	55(49%)	49 (63%)			
		Third party Apps	Positive	3(33%)	4 (20%)	0.603	1	0.438
			Negative	6(67%)	16(80%)			
		Apps Usefulness	Positive	8 (16%)	17(33%)	4.292	1	0.038
			Negative	43(84%)	34 (67%)			
		Total	Positive	68(40%)	50(34%)	1.227	1	0.268
			Negative	104(60%)	99(66%)			
3	Notification Centre	Text Messages	Positive	18 (78%)	14(40%)	8.215	1	0.004
			Negative	5 (22%)	21(60%)			
		Weather	Positive	17(74%)	8(38%)	5.74	1	0.017
			Negative	6(26%)	13(62%)			
		Calendar	Positive	11(61%)	13(31%)	4.775	1	0.029
			Negative	7(39%)	29(69%)			
		E-mails	Positive	13(59%)	7(29%)	4.182	1	0.041
			Negative	9 (41%)	17(71%)			
		Social Media	Positive	13(57%)	8(29%)	4.073	1	0.044
			Negative	10(43%)	20(71%)			
		Total	Positive	72(66%)	50(33%)	27.127	1	0.001
			Negative	37(34%)	100(67%)			
4	Screen	Size	Positive	8 (33%)	17 (63%)	4.464	1	0.035
			Negative	16 (67%)	10 (37%)			
		Resolution	Positive	7 (30%)	13(68%)	6.019	1	0.014
			Negative	16(70%)	6 (32%)			
		Readability	Positive	5 (26%)	8 (28%)	0.009	1	0.923
			Negative	14 (74%)	21(72%)			
		Total	Positive	20(30%)	38(51%)	6.012	1	0.014
			Negative	46(70%)	37(49%)			
5	Health & Fitness	Heart Rate	Positive	9(39%)	7(27%)	0.827	1	0.363
			Negative	14(61%)	19(73%)			
		Fitness Tracking	Positive	20(80%)	17(55%)	3.908	1	0.048
			Negative	5 (20%)	14 (45%)			
		Total	Positive	29(60%)	24(42%)	3.495	1	0.062

			Negative	19(40%)	33(58%)			
6	Battery & Performance	Battery life	Positive	8 (35%)	11(31%)	0.115	1	0.735
			Negative	15(65.5 %)	25(69%)			
		Performance	Positive	5 (22%)	14(38%)	1.699	1	0.192
			Negative	18(78%)	23(62%)			
		Storage	Positive	7 (30%)	5 (31%)	0.003	1	0.957
			Negative	16 (70.3%)	11 (69%)			
		Total	Positive	20(29%)	30 (34%)	0.401	1	0.527
			Negative	49 (71%)	59(66%)			
7	Connectivity	WiFi	Positive	16(70%)	5 (20%)	11.959	1	0.001
			Negative	7 (30%)	20 (80%)			
		Bluetooth	Positive	13(57%)	9 (27%)	4.861	1	0.027
			Negative	10(43%)	24(73%)			
		Total	Positive	29 (63%)	14 (24%)	16.012	1	0.001
			Negative	17 (37%)	44(76%)			
8	Dependency	iPhone dependency	Positive	0	7	NA	1	NA
			Negative	0	23			
		Apple Store dependency	Positive	0	3	NA	1	NA
			Negative	0	17			
		Universal Compatibility	Positive	0	0	NA	1	NA
			Negative	0	13			
		Total	Positive	0	10		1	NA
			Negative	0	53			
9	Interaction	Keypad	Positive	0	0	NA	1	NA
			Negative	11	7			
		Siri	Positive	13 (57%)	4 (16%)	7.302	1	0.007
			Negative	10 (43%)	21 (84%)			
		Force Touch	Positive	14 (61%)	6(26%)	5.662	1	0.017
			Negative	9 (39%)	17 (74%)			
		Digital Crown	Positive	13 (57%)	8 (27%)	4.851	1	0.028
			Negative	10 (43%)	22 (63%)			
		Total	Positive	40 (50%)	18 (21%)	14.089	1	0.001
			Negative	40 (50%)	67 (79%)			

Appendix D

Smart Watch Users Responses

No	Main Feature	Sub-Feature	Novice Perception		Expert Perceptions	
			Positive	Negative	Positive	Negative
1	Design	Watch Size/shape/style	22	9	12	27
		Menu Icons	6	3	9	13
		Icon Colour & Graphics	3	6	12	9
		Watch faces	6	4	11	21
		Total Design	37	22	44	70
2	Applications & usefulness	Built-in Apps	57	55	29	49
		Third party Apps	3	6	4	16
		Apps Usefulness	8	43	17	34
		Total	68	104	50	99
3	Notification Centre	Text Messages	18	5	14	21
		Weather	17	6	8	13
		Calendar	11	7	13	29
		E-mails	13	9	7	17
		Social Media	13	10	8	20
		Total	72	37	50	100
4	Screen	Size	8	16	17	10
		Resolution	7	16	13	6
		Readability	5	14	8	21
		Total	20	46	38	37
5	Health & Fitness	Heart Rate	9	14	7	19
		Fitness Tracking	20	5	17	14
		Total	29	19	24	33
6	Battery & Performance	Battery life	0	13	5	8
		Performance	2	21	9	32
		Storage	6	17	5	13
		Total	8	51	19	53
7	Connectivity	WiFi	1	6	7	11
		Bluetooth	3	8	6	9
		Pairing	2	7	9	11
		Total	6	21	22	31
8	Interaction	Keypad	0	11	0	7
		Siri	13	10	4	21
		Force Touch	14	9	6	17
		Digital Crown	13	10	8	22
		Total	40	40	18	67
9	Dependency	iPhone dependency	0	0	7	23
		Apple Store dependency	0	0	3	17
		Universal compatibility	0	0	0	13
		Total	0	0	10	53

Appendix F

Ethical Approval

Keele University

Ref: ERP1289

2nd September 2016

Abdulla Juma Abdulla Alshamsi
School of Computing and Mathematics
Keele University

Dear Abdulla,

Re: Trade-off between usability and security in the context of egovernment

Thank you for submitting your revised application for review.

I am pleased to inform you that your application has been approved by the Ethics Review Panel. The following documents have been reviewed and approved by the panel as follows:

Document(s)	Version Number	Date
Process Flow Chart	1.1	14-06-2016
Invitation to Participate	1.2	23-08-2016
Participant Information Sheet	1.3	31-08-2016
Consent Form	1.3	31-08-2016
Consent for the use of quotes	1.3	31-08-2016
Pre-screening Questionnaire	1.1	14-06-2016
Bitcoin Wallet Questionnaire	1.1	14-06-2016
Credit Card Questionnaire	1.1	14-06-2016
Task Sheet	1.1	14-06-2016

If the fieldwork goes beyond the date stated in your application, **30th February 2017**, or there are any other amendments to your study you must submit an 'application to amend study' form to the ERP administrator at research.erps@keele.ac.uk stating **ERP1** in the subject line of the e-mail. This form is available via http://www.keele.ac.uk/researchsupport/researchethics/

Directorate of Engagement & Partnerships
T: +44(0)1782 734467

Keele University, Staffordshire ST5 5BG, UK
www.keele.ac.uk +44 (0)1782 732000

If you have any queries, please do not hesitate to contact me via the ERP administrator on research.erps@keele.ac.uk stating **ERP1** in the subject line of the e-mail.

Yours sincerely

pp C H Bannerman

Dr Jackie Waterfield
Chair – Ethical Review Panel

CC RI Manager
Supervisor