Security Mechanisms over Delay Tolerant Infrastructures

Brian Angelo Adan Gonzales

This thesis has been submitted to the Auckland University of Technology in partial fulfilment of the requirements for the degree of Master of Information Security and Digital Forensics (MISDF)

August 2019

Attestation of Authorship

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a university or other institution of higher learning.

Brian Angelo Adan Gonzales

Date: August 2019

Abstract

The motivation of this research is to seek a flexible encryption and authentication method to facilitate the secure delivery of data through a Delay-Tolerant Network Infrastructure. This work will demonstrate a proof-of-concept, by using the blockchain and Delay-Tolerant technologies. These two technologies have the characteristics of being both decentralised and distributed and emphasise the data accessibility and delivery on any type of data through a Delay-Tolerant Infrastructure. Part of this motivation is to conduct an academic enquiry to look in-depth into providing cryptographic attribution of transferred data from source to destination in a distributed environment. This work conducted both an academic study and a proof of concept for securing digital exchange between nodes on Delay-Tolerant Infrastructures. This work will provide a conceptual proposal on delivering digital services to the rural and remote areas. The remote areas (e.g., rural towns and villages) can only connect to a limited number of base stations where they can store their electronic transactions. Once there is a successful direct connection to the Internet, all stored data and transactions will be processed and recognised. Creating a prototype of using blockchains can be used to protect sensitive information, identification management, and protecting the integrity of logging user activity.

The research focuses on the use of security mechanisms throughout the Delay-Tolerant Network Infrastructure. This work has adopted the Threshold Cryptography, in a developed prototype to observe both hardware and software utilisation and processes using Raspberry Pi versions 2 and 3. The prototype will have two sets of clusters based on hardware types, which includes observations based on (1) the length of time for encryption and decryption, (2) the performance of hardware, and (3) the performance of network connectivity through Bluetooth and Wi-Fi.

Contents

List of Figures

List of Tables

Acknowledgments

I would like to acknowledge the following people who have supported me through the process of the completion of my Postgraduate Degree.

Bryce Anthony Coad, for being an amazing, informative, and support person event before I started this research thesis. In times that I needed help on understanding some of the laboratory forensic tasks in class, he made sure that I personally understand the pure technicality of what is needed to be done.

Bumjun Kim and Ramon Lewis, two of my co-workers here in AUT University who have been very supportive of me since I decided to take up further study to complete this Postgraduate Degree in 2017. These two people have been a very instrumental part of my life chapter here in AUT University, to give me a space to let me grow and add points into my personal knowledge domain.

To my supervisor, William Liu, for being a supportive and understanding person throughout this research activity that I have chosen. The valuable exchange of ideas that have led into the result of this research, which for sure it will create a sense of motivation for me to develop and think of future research ideas around the concepts of Blockchains and Opportunistic Networks. Hence, I have more people that I would like to acknowledge here in this section, such as countless people within the School of Engineering, Computer and Mathematical Sciences that I have worked with and those who have been instrumental into my postgraduate life.

To my family, who have given their unconditional and emotional support since I have decided to pursue this postgraduate degree. Let alone several sleepless nights that I have put myself, to ensure that I finish what is needed to be done to cross the finish line.

Chapter 1 - Introduction

Delay-Tolerant Infrastructure (DTI) is a distributed and decentralised networking concept, which has been become USA’s NASA main communications method. This was used as a major part of the NASA’s space development programme experiment, called Deep Impact Network (DINET) Experiment. The DINET experiment’s purpose is to, demonstrate the DTI readiness for operational use in space missions (Wyatt, Burleigh, Jones, Torgerson, & Wissler, 2009).

This type of connectivity method is a special type of Intermittently Connected Networks (ICN). Such nodes that are under this type of networking method are featured as long delay, intermittent connectivity, asymmetric data rates, and high error rates. These are also, decentralised networks where mobile nodes cooperatively communicate to transmit application data from a source node to a destination node (Reina, Ciobanu, Toral, & Dobre, 2016). Such features are the ones that have set a challenge to routing and delay management of travelling data transmission and receiving. In which the determination of routing processes is done in such a way that data is being stored and forwarded to a nearest node possible. The general concept of security was not planned to be part of its initial design; hence this research will be focused on how security measures can be implemented. This thesis will be focusing on the following research aspects of identification of potential positive research benefits, identification of new approaches, and identification of new methods within the stated environment.

Since both security and Delay-Tolerant Infrastructures are very broad in nature, focusing more within the systematic implementation in rural environments. Focused on the implementation of rural areas with delay-tolerant infrastructures and blockchains is due to the demand of connectivity. Connectivity is essential for some important aspects for advancing rural development such as, banking, log tracing, social needs, and decision-making activities. In today’s world, there has been a shift of focus based on the decentralised technologies, in terms of research and production developments. All urban and several rural areas are technologically rapidly advancing. In the other side of the situation, several rural areas are trying their best to keep up with technological trends. Such as the essential use of broadband, a technology that should be accessible to all regardless in rural and urban area. Several industries have adapted the use of broadband technology, to modernise their workflows and other industrial based aspects. There has been an increasing challenge within the food and farming sectors, businesses are seeking to develop and grow their business activity by diversification (Bowen & Morris, 2019).

Certain areas that fall under this category are finding it difficult to maintain their connectivity to other areas via the Internet. Connectivity is not the only issue that needs to be addressed. This thesis also needs to address several challenges of having a decentralised (ad-hoc) networks, such as (1) verification management, (2) identity management, (3) revocation processes, and (4) digital encryption. Overall commonality between these four points that have been raised, another special challenge that this work will mention is the application of security and forensic techniques. Delay-tolerant (no internet connectivity) and decentralised approach of data, technical controls and applications mostly depend on the aspect of having a centralised and seamless real-time connectivity.

1.1. Delay-Tolerant Infrastructures

In today's environment there has been an increasing demand of rural areas being connected to the outside world via the Internet. Different methods have been used such as microwave and satellite technologies, in some instances that UAVs have been used to deliver Internet connectivity to other areas that are extremely remote or hard-to-reach in nature. Where the implementation of traditional and common modes of communications such as through the fibre, copper, and cellular methods which are in real time. Hence the implementation of this type of communication method can levitate network congestion issues on all traditional communications (such as TCP/IP). The theoretical application of

Internet-of-Things will also be mentioned on this research activity, as the delay-tolerant infrastructures falls under this special category.

This type of connectivity methodology has been proven in the past by a few organisations such as NASA (USA) and SpaceX (RocketLab, NZ). There are many other space exploration-based organisations that Delay-Tolerant Infrastructure technology use to gather and send data between earth and the outer space. Thus, the DTI has been successfully implemented for the purpose of interspace communications. While this thesis is to propose that the DTI technology can be also implemented for terrestrial communications with intermitted connectivity. The concept of "Contact in DTN" is the message exchange between two or more nodes when they are in transmission range of each other (C, CT, & K, 2018). Today's generation is more data-driven and soft application centric society in comparison with the previous generation. Depending more on data that the prototype had produced for the purpose of decision-making procedures, fostering collaboration of both decision makers and people who are living in rural areas. The challenge that this work has faced is applying security mechanisms, which traditional and common mechanisms in today's world cannot be applied.

1.2. Blockchain Technology

The concept of blockchains introduces collections and mechanisms of decentralised information storage. This work will apply and develop several sophisticated consensus rules and cryptographic algorithms. In the specific aspect of this research, this work explores the possibility of blockchain implementation for both cryptocurrencies and secure identity and logging management in rural areas.

Since the inception of Bitcoin in 2008 and the further cryptocurrency applications until this present day. There has been a hype of utilising cryptocurrencies and other decentralised applications, which are more like peer-to-peer network (ad-hoc) approached. Cryptocurrencies based on blockchain technology, and it is based on smart contracts concept between users and devices, which is a peer-to-peer (P2P) communication overlay network concept with no centralised authority (Hu, et al., 2018).

The proposed idea of using blockchain technologies, is due to a similar behaviour in comparison to DTI being decentralised in nature. But in the contrary, this work will be exploring and questioning the utilisation of this technology and it's so called fit for purpose to be used with DTI. By the incorporation of cryptographic key exchange with DTI is a challenging problem (Menesidou, Varadalis, & Katos, 2016). Hopefully by incorporating blockchains into DTI is to overcome that specific problem statement.

1.3. Research Questions and Motivations

The main goal of this research is to find out ways of implementing security mechanisms over delay-tolerant infrastructures. Since the two main concepts are very broad in nature, this thesis has outlined the following research questions as below:

Question 1: How can the security mechanisms can be implemented in a Delay-Tolerant Infrastructure?

Question 2: How can Delay-Tolerant Infrastructures be made for Forensic Ready?

Question 3: How delay-tolerant nodes can handle offline validation during data exchange?

The following research questions will complement this research, in terms of providing a hybrid-based (mixed with practical and theoretical) solutions, in terms of the implementation of Security Mechanisms over Delay-Tolerant Infrastructures. In relation to the established research questions will outline some of the issues that this work would like to overcome (items below are not ordered against criticality).

1. Unsecured ad-hoc network between nodes in the Delay-Tolerant Infrastructures.
2. No managed solutions for digital transactions and validation management.
3. The detection and segregation of unwanted (unverified) nodes.

As a solution, this work will be involved in the conceptual use of decentralised technologies such as (1) blockchains, (2) Internet of Things, (3) threshold cryptography, and (4) delay-tolerant networks

(Delay-Tolerant Infrastructures). The commonality of all the four technologies is the mobility and the decentralised nature.

The concept of Delay-Tolerant Infrastructures is not a new form of technology; this has been used as the primary medium by NASA to communicate with International Space Stations (ISS) and Rocket. As such in a Delay-Tolerant Infrastructures standard, data can be forwarded on any type of networks and nodes such as near-Earth satellite networks, with sporadic satellite-to-satellite and satellite-to-ground communication opportunities (Fraire, Madoery, Charif, & Finochietto, 2018).

Since the development release of this technology, the idea of including any security mechanism was not even part of the design process. This work will be focused on the using Delay-Tolerant Technologies to serve as an alternative medium for communications. Using this technology will eventually bring Internet to rural areas (including areas in emergency), and this work aims at proposing an idea of having a secure environment for communication and data exchanges.

The motivational idea of this research is based on the past activities conducted by previous researchers such as Sullivan & Burger (2017), and McGhin, Choo, Liu, & He (2019). There have been a few countries that have moved all its public services, an excellent example is the Government of Estonia. The Estonian Government with a population of just under two million (as of 2019), has been a global leader of digitalisation of its public sector services and the management of their electoral processes. This was developed and released in December 2014, in which they have built a platform to ease the management and transparency of their government entities. Henceforth, the security and accuracy of the information stored in the ledger (or blockchain) are maintained cryptographically (Sullivan & Burger, 2017)

Even though that this has been implemented in a wider scale using real-time networking methods, this is a complete opposite method of data connectivity. Trust management is one of the weak core aspects of the application of such technologies that full depend on security, encryption and digitalisation and centralisation of public services. This proposed work can also be utilised on a couple of scenarios such as (1) organisations that uses big data, and (2) to provide an alternative medium to send digital data by offloading current infrastructure.

1.4. Thesis Structure

This section will outline the overview content summary of this thesis and its key chapters. This thesis contains five key chapters, that this work will state several key points and components to put into discussion. In which will outline the importance of the implementation of security mechanisms to protect data processing and transmission on any current or future developed infrastructure.

Chapter 2 will discuss the use of the Design Science Research methodology, defending the use of this methodology due to the aspects of collection of data and prototyping activities which will be mentioned in this thesis. This chapter (Chapter 2) will also outline seven guidelines that have been adapted to ensure that discussion points in this thesis are valid. This part will complement the proposed solutions, which will gather the ideas with the support of quoting from different researchers and literature in Chapter 3. This work will be stating the importance of the principle idea of implementing security mechanisms over Delayed Tolerant Infrastructures. Such security mechanisms that will complement the decentralised nature and its sole importance to protect data integrity and privacy. Hence, to support the concept of fault-tolerant applications, decentralisation, and distribution of resources and systems to prevent and reduce the issue of single point of failure concepts. Then onwards, presenting a theoretical argument into the needs and challenges of forensics approaches and methodologies and how the idea this work would like to propose, should be able to attack these types of issues of cybercrime activities.

Afterwards, this work will then continue to Chapter 4, it will refer to the proposed ideas based on Chapter 3. This work will mention in this specific chapter, the idea of Security Mechanisms for Offline and Online Nodes, and it will set out theoretical ideas and methods of this specific implementation.

The ability to put forward an argument of blockchain platforms for different reasons such as cryptocurrencies, and the need of having a database of transactions, identity management, and user activities. This work will be also stating creating a prototype based on Threshold Cryptography methods. It will be using that specific cryptographic application, to control user and node read and write access to sensitive data-centric applications and blockchain platforms.

Chapter 5 will be focused on the results and findings from the developed prototype. It has evaluated the proposed ideas and the utilisation of low-powered hardware of Raspberry Pi versions 2 and 3 (Model B+), as well as the aspects of hardware resource behaviour and exploring different methods of communication mediums such as Ethernet, Wi-Fi, and Bluetooth. The conclusions and summary have been drawn on Chapter 6, and it also discusses the research limitations and layouts the future work.

The outcome of this work is to have a developed prototype that will benefit the rural communities, with one goal to understand this new method of connectivity. This type of connectivity method i.e., DTI can be more likely classified as providing services with a limited capability of connecting resources to the Internet.

This work could be applied to other situations or environments, such as in natural and man-made disaster events. The ideas mentioned in this thesis can also be used for developing an alternative communication infrastructure for people living both in urban and rural areas. Developing ideas that will be able either contribute to any event or needs such as natural or man-made disaster management, alternative point-to-point connection between locations. Having this alternative solution to be put in place on these mentioned types of scenarios, will start to flourish an idea that is less depended on the traditional networking methods. These traditional networks have been put in place are mostly real-time based methods that need a constant network connection.

It will also require having a methodology that will be able to cater for a diverse and multidisciplinary knowledge domain. This will have the aspect of covering many topics and problems that are both mixed and purely technical and social (Gluhak, et al., 2011). The specific methodology that will be applied into this research will mostly be focused on the Design Science Research. To support this work's developed prototype, it will be using and quoting academic based literature to support the proposed concepts. The academic based literature quoted in this thesis, will fully complement the mentioned concepts. It will also compliment the formulated research questions, which are mentioned on Sections 1.3 and 2.1. It will also be stating several popular research articles to support all the mentioned ideas.

Chapter 2 - Research Methodology

This chapter will seek the identification of methods, to be able to create requirements for researching and experimenting with cyber-physical systems. The developed prototype will be focused on setting up a sample community with delay-tolerant nodes. It will propose a security mechanism method using threshold cryptography and blockchains. Such results will be used to understand the idea of incorporating secure mechanisms in DTI. Having a research methodology will aid on tackling and understanding of a number of issues. One major point that needs to be put into consideration, is a number of methods of tackling a single issue could exist. Such as common methods can sometime be either applied or not applied, depending on the nature of that single issue. <<quote needed>>

The main research objective is to develop a prototype that will implement secure mechanism in DTI, and it needs to explore a methodology that is focused on conducting, collecting, and observing behaviours of this prototyped system. The application and choosing a research methodology have been a very challenging factor of this thesis, which will be detailed in section 2.3. It is important to have a methodology, to enforce uniformity on certain areas and solutions based to encountered problems to any research-based issue and to newly contributed ideas. Figure 2.1 demonstrates a more generalised process of dealing with proposed solutions and ideas using the Design Science Research methodology.

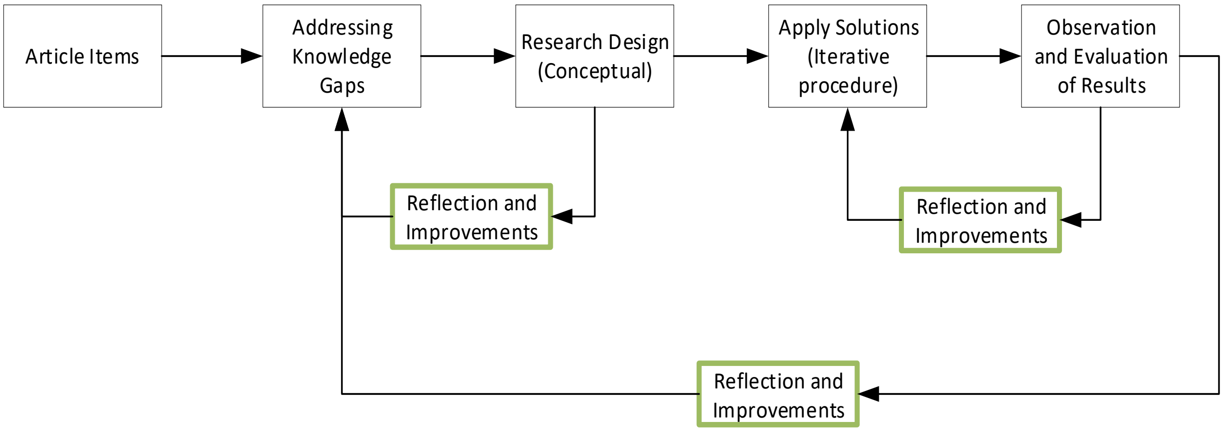
Article Items
Addressing Knowledge Gaps
Research Design (Conceptual)
Apply Solutions (Iterative procedure)
Observation and Evaluation of Results
Reflection and Improvements
Reflection and Improvements
Reflection and Improvements

Figure 2.1 General Diagram Summary of Design Science Research

The diagram (Figure 2.1) demonstrates a very iterative process of managing either issues or new ideas being introduced into this work. Processing each article will ensure the possibility of delivering meaningful outcomes and solutions in relation to this work. This procedure ensures that there is a strong correlation on types of outcomes and solutions, can be like either applied either fully or partially.

2.1. The Experimental Perspective

The developed prototype will be using Raspberry Pi's (versions 2 and 3 B+), wireless networking modules (Wi-Fi, and Bluetooth), and Raspbian operating system. The developed prototype will be focused on methods and techniques that complementing them on Chapter 3. Chapter 4 will discuss the results of the developed prototype as a basis of having an understanding approach into decentralised cryptography. Developed prototype will be used to evaluate the threshold cryptographic and blockchain processes and utilise the certain applications, such as available operating systems and its associated tools. The Chapter 5 will be focused on conducting the experiments, and discussions based on its performance studies. The network architecture of the prototyped testbed can be found on Figure 5.8 and their more detailed descriptions can be found in Chapters 4 and 5.

2.2. Chosen Methodology – Design Science Research

Design Science Research methodology (DSRM) is more appropriate against this work. By researching the aspects of, Secure Mechanism over Delay-Tolerant Infrastructures, it is demonstrated the dualistic nature of this thesis, a high assurance that the use of a Design Science Research methodology. All research articles quoted ensures the enough coverage on the topic and its related areas discovered in this study. Below are the six main points of discussions and objectives for the literature review section on Chapter 3.

1. General overview of blockchain technologies.
2. Reasons for using blockchain technologies.

3. The basis of having positive approaches to decentralised environments.
4. Threshold Cryptography application on DTI.
5. Attacks based on decentralised environments.
6. Digital Forensic Methodologies on decentralised environments using blockchain technologies.

Stated points will be making an important argument for the decentralised and distributed encryption and networking techniques, and conducting a comparison between DIT, blockchains, and threshold cryptography. It will theoretically discover the purpose of having these stated technologies integrated, on how they can be implemented to provide a solution to the specific cause of creating a secure environment. This work is to propose a solution to build a sense of trust into the distributed and decentralised network, while still support the secure routing and data exchange among the nodes. As such any new data generated by participating nodes and including other types of nodes that have been introduced and communicating with other nodes (Alguliyev, Imamverdiyev, & Sukhostat, 2018).

Being dualistic in nature, meaning that this method will complement certain supporting elements such as the theoretical proposal and the overall general concepts of the prototype. The approach of using Design Science Research complements, design and development of new or improved research methods (Venable & Baskerville, 2012). Hence, this thesis will be summarising the full aspect of this methodology which has been a sole guide for this thesis.

This specific mentioned methodology will sure be able to develop into having a much more rational and consistent. This means that being much more rational and consistent, is being able to complement its effectiveness and accuracy. As mentioned in the starting remarks of this chapter on how this work faced challenges in the selection of a research methodology. Until now that there is still a widespread interest in the method of empirical software engineering methods, considering that software engineering is a specific domain that is multi-disciplinary field both technological and social aspects (Easterbrook, Singer, Storey, & Damian, 2008).

Each of the proposed recommendations that have been stated on this work, have gone through the set guidelines. This methodology has seven guidelines, which are (1) design as an artefact, (2) problem relevance, (3) design evolution, (4) research contributions, (5) research rigor, (6) design as a search process, and (7) communication of research. These mentioned guidelines focused on the style of Design Science Research, relates to the aspect of the whole research as guidelines that must be followed to ensure the level of relativeness within the aspect of this work. As demonstrated on Figure 2.1, all proposed articles will need have gone through time can be in a repetitive process to address gaps and focus of this work.

2.2.1. Design as an Artefact (Guideline 1)

This methodology must create a sustainable artefact in the form of either a construct, model, method, or both countability and uncountability. Designing as an artefact is the first guideline that all proposal points had gone through, were in fact not only involves on certain product that will be used for research. Ensuring that these ideas that involved products, are mostly complemented with (1) creative processes, (2) modelling techniques, and (3) mathematical reasoning.

Proposed techniques and methodologies that are being introduced into a specific domain, this work must ensure it considers that Research and Development management strategies as a core component. Hence, certain proposed points of discussion must be focused more on being authentic, and this aspect of culture which complements the problem context of this research. In terms of this work and the guideline itself, ensures that there is a sensible artefact that will be substantive to the knowledge domain of this work. In relation to this guideline, this work ensured that articles that will be included will make sure have some sustainable relevance. In order for a specific article to be considered as part of this research, the process design includes the analysing of keywords stated on all of the quoted literature. The specific process also includes the methods that will bring benefit to this work, to which this specific guideline will complement to what has been required on guideline 2 (in section 2.2.2), were it talks about the problem relevance.

2.2.2. Problem Relevance (Guideline 2)

This guideline's focus is to establish objectives, having a develop technologically centric solutions to related problems. This specific guideline also is designed to investigate the aspects of the problem and explore on how important it can be done. The DSR method following the framework, will assure that the concept of splicing by researchers as a positive approach. By using this guideline, ensures that the major problems that this thesis is to focus and solve the issues that have been raised. Major issues will be focused upon the communication between nodes on times of disaster management, and the closing on the digital divide between rural and urban communities. The primary focus of this research is to ensure that it complements modern problems to be solved with current technologies and methods. The application of security mechanisms to protect the flow of information and data between source and destination. This guidance also ensures that the problems in terms of the application of secure mechanisms upon DTI are addressed properly.

2.2.3. Design Evaluation (Guideline 3)

This focuses on the utility, quality and efficacy of a designed prototype or product. Having the ability to recognise certain research limitations and metrics, based on the any tools, methods and techniques being used in this work. The use of currently established technologies and methods to complement the focus if this research. To which this work focuses more heavily depending on creating prototypes, which has been demonstrated via well-executed evaluation processes.

Creating a prototype and testing the specific aspects of its functions, that this work fully mentioned in detail the experimental research aspect in Chapter 5. The experimental research being focused on procedures, to observe and collect data on hardware and software capabilities. Testing of capabilities are in terms of the selected features provided by hardware and software, which can aid the provisioning of DTI technology. By developing (in Chapter 4) and interpretation of results (in Chapter 5), it can aid the evaluation process to help stating future work of this research and the capabilities of existing hardware and software.

2.2.4. Research Contributions (Guideline 4)

In respect of this research work and the approach to Design Science Research, this was more like and extension to Guideline 3. This work ensured that it complements within the basis of evaluation experiment results in Chapter 5, and the backing of literature articles in Chapter 3. The ability of having a positive contribution to the target knowledge domain, that is valuable for the target community or researchers. A positive contribution aspect, certain research contributions, making sure that anything that has been proposed in this thesis contributes and complements the stated research topic. Certain contributions that will be stated in this thesis must be at least unique in nature, or improvements on previous contributions from a similar research activity. Regardless of the nature of any research contribution items, these must always compliment the full aspects of Delay-Tolerant Networking methodology.

2.2.5. Research Rigor (Guideline 5)

Being scientifically rigor (or purely research rigidness), meaning that it is implying and making sure that standards and practices are applied to the highest standard. Being able to apply it to any specific research activities and tasks, to be able to discover the truth and reducing minimising any bias. This also comes to selecting research questions, which are part of any research work to set certain boundaries, and to be able to focus properly into the work set in this thesis. A rigorous researcher must also be able to articulate certain objectives within the research (Sovacoo, Axsen, & Sorrell, 2018). Having a clarity on what they want to achieve and being able to determine the best method to achieve a specific goal or outcome. in relation to this thesis, to be able to contribute to both Internet of Things and Delay-Tolerant Infrastructure domains in a positive outcome.

2.2.6. Design as a Search process (Guideline 6)

Designing a proposal or an idea is a very repetitive process to find an effective solution. Such as searching for a specific tool or method that is available, that its relevant and fit for intended purpose. Using these searched tools or techniques, this work ensured that two points have been observed such as, (2) discovering the feature capabilities of tools or techniques, and (2) ensuring that these can provide and tackle the stated research questions and problems.

This guideline also complements that designing as a search process, can be in a repetitive procedure to ensure that tools and techniques are just and appropriate. This work also had encountered issues with search processes from the beginning, mostly depending on the tools that have been proposed to be used for the prototyping on Chapter 4 and Chapter 5.

2.2.7. Communication of Research (Guideline 7)

This work and complementing this guideline, ensuring that this work can be presented in a useful and effective manner. Which can be presented in to complement the needs and understanding of technical and non-technical alike. Communication of research guideline ensures that prior to the final publication of this work, that this work has presented with future directions (future work). So that when it comes to other researchers that may want to refer to this work, to give them ideas to what areas are still lacking.

2.3. Other considered methodologies

This section of this thesis will mention certain methodologies, which have been considered for the use of other methodologies for the sake of this thesis. In this section of this work, will discuss other alternative research-based methodologies that have been considered in detail. There are some points that are needs to be considered. The following five points that mentioned on the next paragraph are mentioned the research conducted by Sjøberg, Dybå, & Jørgensen (2007).

Firstly (1) having a full understanding of the applied methodology and how it can be able to relate to the research topic, also (2) having the implicit assumptions on arguments and proposals established. Another point that should be considered as important, is the (3) full confidence in the presentation of the work appropriately. Also, (4) having a work that is original and could refer or work from other researchers that may have focused their work on the same domain. Finally, (5) being able to accommodate of using an additional methodology into any work. In relation to this work, four out of the five points have been met. The fifth point, which talks about the additional methodology was not mentioned, since the chosen methodology on Section 2.2 is fully appropriate to complement both its theoretical reasoning and prototyping aspects.

This work also investigated other available methodologies that this work could incorporate, such as qualitative or quantitative, also even the combination of the two methodologies that can fully support this work. The detailed reason that this thesis did not choose either or both said methodologies, is because (1) they do not complement the dualistic approach of this work in terms of theocratic application of mentioned proposals. By using either or both methodologies, they cannot fully support or complement the prototype that was conducted on Chapter 5. In addition to what has been stated reason for not pick either or both said methodologies, is due to its very broad methodological approach, and being flexible and uncomplimentary approach within the domain of information systems and security.

Chapter 3 - Literature Review

3.1. Introduction

The initial design and development of delay-tolerant infrastructures was based on exchanging information between satellites and on both earth surface and space. The implementation of any security mechanism was not part of the development process, due to the accessibility was only restricted for organisations of space exploration such as NASA. There is a popularity of using this type of communication over traditional networking methods. This specific popularity will surely bring certain benefits such as providing an offloading solution to current real-time networking infrastructures, and to provide network connectivity to remote areas. On the other side of the scenario, there are several research challenges that delay-tolerant infrastructures are currently facing which needs to be addressed.

The challenges that are in need to be addressed such as: (1) the validity of all initiated transactions, (2) the revocation of malicious accounts. And lastly, (3) the encryption management of data across the delay-tolerant nodes. This thesis will focus on having a concept of validation of transactions in a limited connectivity environment where all communications are mostly passive. These mentioned design points are perfect with the conditions of rural and remote areas, where the implementation of solid communication infrastructure is nearly impossible. With the solution of DTI (or delay tolerant networks), the implementation of communication infrastructures to these areas can be achieved.

This work stresses the importance of peer-to-peer offline networking technology, which will be an alternative into building real time communication infrastructures in rural and remote areas. An offline networking technology that can be capable and trusted to offload current real time infrastructures. This type of networking technology should be able to deliver any type of information, also to serve as an alternative to connect rural and remote areas. This type of offline technological concept is commonly known as Delay Tolerant Networks, which focuses on store and carry forward approach of data from source to destination. This type of communication infrastructure approach does have some negative implications. One of the major negative implications will be, such as suffering from constant interruption especially when sending over large or very important data across the medium. To fully understand that in opportunistic networks such as Delay Tolerant Infrastructures are prone to, interrupted connectivity between nodes is normal (Ahmad, Doss, Alajeely, Rubeaai, & Ahmad, 2018). It means a number of or most communication activities within the opportunistic infrastructure, the participating nodes will be managing data in a delay tolerant approach.

Figure 3.1. demonstrates the approach of having an offline transaction or somewhat an exchange of data between persons A and B. In a perfect real-time scenario of no security and high degree of trust, a simple transaction can occur without the need of encryption and secure mechanisms. There are also some advantages of not having encryption and secure mechanisms, such as devices will be able to process data faster without delay. This will also be same when these users with certain scenarios such as, ease of trust mechanisms and processes when devices are regularly getting updates when connected.

In today’s not so perfect world, the concept of information security is paramount on any development of applications. It is unacceptable to have a developed application that does not being armed with requirements of data integrity and security processes. As shown in Figure 3.1, the diagram demonstrates that there is a trust between two users in exchanging data while on near contact. It is a perfect example of delay tolerant connectivity, where there is a type of intermittent connectivity between two or more nodes are in a short distance away from each other. Also, person A does not know what person B has in terms of active or dormant malicious applications (and vice versa). There can be some types of attacks such as discreet and not discreet approaches when it comes to attacks on privacy and devices used, this will be explained more in sections 3.3. and 3.4. of this Chapter.

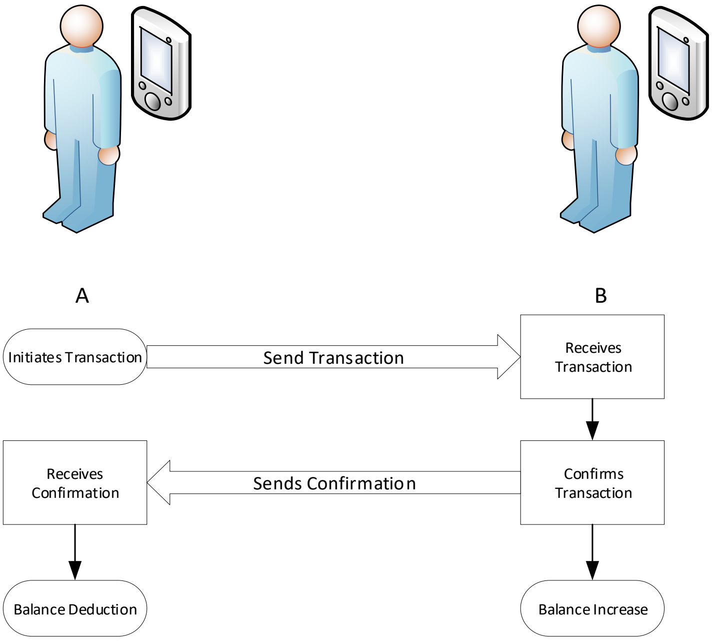

Figure 3.1 Normal Transaction without Secure Mechanisms

3.2. Delay Tolerant Infrastructures

Delay Tolerant Infrastructures have been one of the driving forces of the concept called Internet of Things, where sensors and other forms and methods of decentralised technologies are used. Focusing on having a decentralised environment where it can be trusted, transparent, and accountability approach. Which is the similar approach on having the concept of AAA (Authentication, Availability, and Accounting) on centralised environments. In which all nodes are required to be successfully authenticated and continually connected both virtually and physically. In this research activity, focuses more on the implementation of offline networking technologies on rural and remote areas. Basically, Delay Tolerant Infrastructures and including other types such as opportunistic networks, these are more like an end-to-end path among a set of nodes which cannot guarantee a good connection (C, CT, & K, 2018).

Considering such a scenario that some remote villages distribute in a region, in which there do not exist communication infrastructures (Jiang, Chen, & Shen, 2014). Referring to these people or nodes that are part of one village or specific area commonly known as communities or can be classified as message receivers. To completely understand that Delay Tolerant Nodes are mostly low-level graded specification designed. Which have limited bandwidth and computational capability (Li, Gao, Zhu, & Cao, 2012). Certain considerations are needed to be highlighted by understanding both of its full intent and function in terms of developing these types of opportunistic networks. This work stresses the three fundamental features of what Delay Tolerant Networks have, such as (1) no connected medium (wired or wireless) between nodes, (2) long transmission delays on mediums, and (3) high frequent packet drops (connection interruptions). Delay Tolerant Networks (Infrastructures) in general have emerged when, traditional TCP/IP protocol failed to work in environments that use acoustic or optical modulation with frequent interruptions (Dutt, 2015).

3.2.1. Demand for Connectivity

Where in fact that delay-tolerant infrastructures in general, effectively extends the network connectivity in the time domain, and endows communication devices with enhanced data transfer capabilities (Chen, Liu, Liu, Taylor, & Moore, 2015). As of now, there have been many recent developments of this connectivity method such as mobile sensors (Internet-of-Things), disaster recovery, and social networking. Chen, Liu, Liu, Taylor, & Moore (2015), have been studying the effects of the utilisation of network coding with Delay Tolerant Infrastructures.

Network coding method has been proven to be the perfect solution for all related to Delay Tolerant Networks. This has been supported and validated by other researchers such as Zhao, et al. (2012), where they have proven the Network Coding Techniques offer an emerging solution to efficient data transmission (Zhao, et al., 2012). The most simple and positive solution in terms of application and algorithmic approach than other data transmission methods, which can adapt to any dynamic change and growth within the Delay Tolerant Infrastructures.

As the demand for Internet connectivity grows, the need of having the Internet to rural and remote areas has also grown. The growth and demand of internet connectivity comes into play, due to the positive future growth and development of these rural areas, in terms of (1) productivity, (2) financial benefits, and (3) social impact. DTI has its benefits of less dependency on implementation of traditional infrastructures on rural and remote areas. Adapting the method of delay tolerant infrastructures will result into (1) less maintenance cost, and (2) easily expandable to other unreached or to improve connectivity. Another point that this work would like to raise is the (3) offloading of current real-time and traditional infrastructures. Such Delay Tolerant applications and their traffic allow much room for flexible scheduling and transmission (Laoutaris & Rodriguez, 2008).

3.2.2. Infrastructure Deployment

Even though the three points mentioned on section 3.2.1 are very attractive and promising, the important issue is to address, the long-term planning and implementation of secure and trusted DTI. Reflecting on a continual large-scale size fully operational and trusted DTI, without the issue of geographical location or the method of connectivity. Certain types of connectivity methods could be as follows below:

1. Bluetooth
2. NFC (Near-Field Communications)
3. RF (Radio Frequency)
4. The use of transportation modes (such as buses, trains, and cars)

DTI can be either implemented in hybrid (mixed with other medium methods) or homogeneous (by itself) approaches. These two types of implementation can be part of the long-term of the development of the Internet availability regardless of geolocation of devices and individuals. But in regards with development and delivering Internet to rural and remote areas, this work will sure highlight the sociotechnical issue of digital divide. Delay Tolerant Networks can be utilised to decrease or eliminate the current digital divide. Hence there has been a worldwide public policy movement, which is focused on providing digital connectivity infrastructure in remote areas, where some people in remote or rural areas remain digitally excluded (Pavez, Correa, & Contreras, 2017).

This work's motivation of delivering Internet connectivity to all rural and remote areas, of having to eliminate the global issues of digital divide. It also stresses the importance of the demand of a digital connectivity from these affected areas, in which we can all refer to them as (1) digitally motivated. People who are opposed to having or taking part of solving digital divide, can be called as (2) digitally disengaged. Reflecting towards on grasping the focus and motivation of these two groups, these points should help us on any long-term and short-term strategic efforts. The ability of solving the digital divide with the help of digitally motivated people, will enable us to provide Internet connectivity to rural and remote areas.

3.2.3. Other Possible Deployment Methods

Certain areas affected by natural and man-made disasters, can also be classified as hard-to-reach areas. Henceforth there have been some research activities and development in terms of practical application. Delayed Tolerant Networks concept, which has been used to aid and support post disaster management process and procedures. This is only to the fact that there have been some attempts to use DTI in disaster situations, such as Japan's 2011 earthquake and tsunami event. This particular event did demonstrate the importance of active communication links, that resulted into a limited or no available communication medium available to be used. The result of reduced or no communication mediums available, would have created a massive issue into planning and deployment of assistance to affected isolated areas. In this type of situation, the implementation of Multihop wireless access networks could have been the solution provide as a network solution to isolated areas (Minh, Shibata, Borcea, & Yamada, 2016). Minh, Shibata, Borcea, & Yamada (2016), did focused their research into the application of Multihop wireless access method called, tree-based disaser recovery access network

(TDRAN). TDRAN is a flexible and expandable networking method similar to a mesh peer-to-peer network, creating relay nodes (or relay stations) called Wireless Distribution Systems to extend the network coverage within remote areas.

Which can be used to send critical information to designated disaster management centres, such as deploying personnel have been assigned to observe affected areas to collect information by sending text or visual information. Firstly, this work has been focused on the reasons for people who are part of the digitally disengaged group. This group of people in rural and remote areas may have a list of issues and motivation points that need addressing. Group them out to which these people are not concerned or do not have any form of motivation to be online. Due to the level of understanding and education, another factor that this work is willing to consider is the age and generation gap and their slow reaction into using technology. For the purpose of this work, it focused towards people of these communities that have a very high concerns about two things such as, concerns about privacy and technological reliability (Pavez, Correa, & Contreras, 2017). Concerns of these types are needed to be addressed, as part of any short-term and long-term planning and development of DTI from now and to the future.

Seeing the huge impact on urban areas and how technology has transformed the way of life, on people who are currently living in urban areas. This work understands the purpose and levels of impact, which Delay Tolerant Infrastructures (and other Opportunistic and Ad-hoc Networking based methods) can change the way these communities interact. Designing infrastructures that can transform these communities, ensuring to remain focused around the developmental concepts of (1) security, (2) stability, (3) integrity, and (4) reliability. These four stated concepts, strictly following the concept of security, in which at times most people will take away for granted. In terms of meeting the four concepts that this work will discuss more in detail on Sections 3.3 and 3.4.

3.3. Importance of Security Mechanisms on Delayed Tolerant Environments (Opportunistic Networks)

Due to the nature of Opportunistic Networks such as Delay Tolerant Infrastructures, as such of no centralised control and can be dynamically placed geographically. The whole implementation approach of security mechanisms will be a huge technical challenge, as it’s characteristics of such an open medium, dynamic topology, no centralised management, and absent clear lines of defence (Alajeely, Doss, & Ahmad, 2017). These opportunistic nodes or delay tolerant nodes, as far as mentioned on this thesis, that they do a summary procedure of Store-Carry-Forward when nodes are in contact (nearby or at a certain long range). Delay tolerant nodes (and networks) are not part of any physical permanent infrastructure, compared to today’s conventional networks, where logging of transmission of data is possible. Hence, in delay tolerant nodes (and networks) and the transmission between the source and destination, there is not a proper or fixed path to the destination (Ahmad, Doss, Alajeely, Rubeaai, & Ahmad, 2018).

In reference to a delay tolerant node, these could be as follows such as a vehicle, smartphone (or any mobile device), and even as small or large programmable and embedded devices. Hence whatever the attack method utilised, and the size of any potential malicious devices as characterised as ad-hoc and geo-dynamic node (devices). Also, to understand as well that, with nodes being ad-hoc and geo-dynamic, this can cause several methodological ways to attack either a device or a community or clusters of nodes. Such attacks can be classified as active, passive, internal or external, or different attacks classified based on different protocols (Kaur, 2015). In ad-hoc and opportunistic networks, another challenges that this work stresses to highlight in this research activity is the possibility of having the application of forensic technique, which will be discussed in depth in Section 3.4.

3.3.1. Security Concerns of Delayed Tolerant Environments

There are some concerns that this work needs to address on delay tolerant infrastructures, is within the basis of security, data privacy, and in matters of digital forensic methods. There are some of the concerns that this work will present certain areas of concern about the application of delay tolerant infrastructures. Types of attacks and other malicious activities that can occur on delay tolerant network such as (1) the transmission of malicious packets, (2) to be able to view received data that can contain any private information. (3) No such ability or feature for protecting information during the procedural stages of store, forward, and carrying data.

Kaur (2015) on his research article within the basis of attacks in opportunistic networks, based his aim on the application of privacy mechanisms on opportunistic networks. He has recognised the challenging objectives due to opportunistic network does not have a permanent physical infrastructure. Also, he has highlighted a number of attacks that can be done in opportunistic networks, such as (1) blackhole attack, (2) grey hole attack, (3) wormhole attack, and (4) selective packet drop. These types of attacks can be used to disrupt the whole infrastructure's function, and the whole physiological of trust due to the breach of privacy. These specific malicious nodes' job, is to inject more packets into networks, but at times these nodes drop packets to encourage incidents to occur (Khalid, et al., 2018)

Other types of attacks that can happen on Opportunistic Type Networks (e.g., Delay Tolerant Networks) is the Sybil attack. This type of attack is similar and a combination of about grey hole and wormhole attacks, where there is a node that will do a false impersonation of a safe node. This attack methodology has been researched by Trifunovic & Hossmann-Picu (2016), which has highlighted that the sybil attack is one of the most disruptive form of attacks against any applied security mechanisms. In a perfect world where, there is increasingly more digital communication being routed among wireless, mobile computers over ad-hoc, and un-secured communication channels (Bucur & Iacca, 2017).

Providing the aspect of privacy, is one of the specific security concerns that will be addressed in this study. To which having a decentralised infrastructure (setup) such as delay tolerant networks, where the management of privacy can easily be compromised. In which the types of attacks mentioned in this section such as black hole and grey hole attacks. Privacy itself undertakes the trust and risk such associated with a specific node's data is collected, stored, and shared (Ahmad, et al., 2019). There has been an approach to which a specific method of certification can be achieved is by doing the method of Privacy by Architecture (PbA). The PbA method itself was introduced by the specifically by Ahmad, et al. (2019), to minimise and protect potential system user's or node's privacy, by only focusing on minimal information being sent for requesting a digital certificate.

3.3.2. Management of Malicious Delayed Tolerant Nodes

One of the major disadvantages of what opportunistic networks (Delay Tolerant Infrastructures), is the isolation of malicious nodes, which is also a common issue with conventional networks in today's world have put in place now. In these conventional (or so-called common methods of connectivity) networks, the advantage is that logging and monitoring systems can be established easily to isolate nodes within certain parts of the infrastructure. In opportunistic networks such as Delayed Tolerant nodes are near to impossible when it comes to logging and geotagging and locating of these types of nodes. There has been several research activities, when it comes to securing the routing protocols and mechanisms of Delay Tolerant Networks which is ones of its specific approaches for security mechanisms. More focused on the general use of routing applications, issues of routing are mostly covered on the integrity and confidentiality aspects of data being transmitted.

There has been a thought of using certain method that can be used to combat malicious node, which is by the node's time settings (such as time zone and clock settings). There have also been some studies to which the use of transmission nearby nodes, to transmit time zone and clock settings information from the transmitting node to the receiving node. This type of method can be as an easy way to associate and to certify a node with similar time settings, that can be considered as a safe node. But, using time settings as an attribute to certify that a node is a safe node, may not solve the issue of managing safe nodes. In which, time synchronisation has been classified as a challenging task for both wireless and decentralised networks such as delay tolerant networks (Hasan, Wang, Feng, & Tian, 2018).

There are at least two methods that can be considered are by (1) applying cryptographic methods and (2) the process of revocation of nodes in opportunistic networks. These two methods can also be considered as an additional method of managing malicious nodes, that do not cooperate within the rules of the whole delay-tolerant infrastructure or a specific part of the network. Threshold cryptography methods can be applied throughout the whole infrastructure, or in a specific topological part of the infrastructure itself. In which, a number of nodes can be given certain roles and responsibilities to provide a decentralised cryptographic and authentication service in the infrastructure itself (Djamaludin, Foo, Camptepe, & Corke, 2016).

The technology of threshold cryptography can be implemented very difficult, since most of the popular cryptographic methods that are common centralised in nature such as Public Key Infrastructures (PKI). Which are easy to set up, configure, and maintain, because this work only focuses on all the key and authentication management aspects centrally. Traditional (or common) methods of implementing Public Key Infrastructure (PKI) systems is always centralised, and its sole requirement is to have a centralised authentication and cryptographic server (or more commonly called a master node). Most of the time, it will need a powerful configuration of a central (or master) node within the whole infrastructure to ensure that it can handle as much requests for authentication and cryptographic processes.

Public Key Infrastructure (PKI) may not be compatible with systems and applications that are managed in a decentralised manner. Discovering the concept of MANETS (Mobile Ad-Hoc

Networks), a specific form of technology under delay-tolerant networks, these types of nodes have so much constrains in terms of processing power and available resources. Meaning that MANETs (or any form of nodes also including Vehicular Nodes or VANETs), may be inefficient to handle cryptographic techniques for key management due to high computational and communication node overhead, including highly dynamic and autonomous network (Cho, Chen, & Chan, 2016).

Mobile ad hoc networks are also a specific collection of autonomous nodes connecting between nodes through wireless environments without a proper infrastructure (Gharib, Moradlou, Doostari, & Movaghar, 2017). These nodes (such as delay-tolerant networks) are mostly dynamic, fragmented, and ephemeral network formed by a large number of highly mobile nodes (Djamaludin, Foo, Camptepe, & Corke, 2016). Having a highly dynamic (decentralised) network, which means that there are too many frequent key assignment (and reassignments) when a node leaves or enters a new community (cluster). The constant reassignment of keys and certificate or installation on nodes, this can contribute to a high level of resource utilisation of hardware capabilities. There are several points that this work need to consider, due to the specific networking ad hoc network the management of trust is very dispersed and can be very unorganised due to no centralised node to handle all node trust management.

Incorporating the method of trust in decentralised networks, looked into how the term trust in a sociological point of view. The terms of trust, reflecting on this as humans trying to establish a trust with other human beings a good way to explain trust in ad hoc networks. In which it will take some time between humans to establish trust, that can be defined as the specific subjective belief about the reactions and behaviours of a particular person or party (Cho, Swami, & Chen, 2010; He, Yu, Wei, & Leung, 2019). Just like same as humans, there are times that it will take time to establish the trust between ad hoc nodes. In that specific sociological example, expecting to have this similar type of scenarios that can happen in relations of both opportunistic networks and security mechanisms.

Without certain application of security mechanisms and the highly-socially demand of mobile technologies. These specific infrastructure-less networks will continue to have a specific considerable level of popularity since the inception of mobile technologies (Panos, Ntantongian, Malliaros, & Xenakis, 2017).

3.4. Forensic Approaches and Methods for Opportunistic Networks with decentralised cryptographic methods and challenges.

One of the major issues that this research can encounter with opportunistic networks (such as ad-hoc and delay tolerant infrastructure), is the incorporation of forensic techniques. Due to the name of certain opportunistic networks such as Delay-Tolerant Networks, in its decentralised nature. Nodes that are either isolated or decentralised and be able to capture them is a technical issue in a forensic sense. Living in a digital focused world, were there has been an increase demand of digital mobility and further development of other new technologies. Some of these new technologies that have developed, are at times having issues on lacking in testing capabilities in terms with security. Newly developed and emerging technologies overtime comes hand-on-hand with the rapid increase in cybercriminal activities. Hence this work will need to give importance of the need of digital evidence (Lone & Mir, 2017).

The development of these specific technologies, especially with the huge social demand of developed devices and applications and enables mobility and ad hoc networking approach presents a difficult challenge to forensic investigators. This specific social phenomena around forensic technicians and investigators in which they need, to find ways to retrieve and secure forensic data (MacDermott, Baker, & Shi, 2018). With the proposed provisioning of a blockchain technology for the purpose of protecting evidential data (chain of custody), if such legal requirement needed to fulfil any such investigation.

The importance and growth of providing and acquiring digital evidence will be able to give a new source to point out the origin of where an attack has been established. Lone & Mir (2017), did a study of proposal for developing of forensic-chain model in which can be used as a solution for tracing and maintaining the integrity of the digital forensics chain of custody process and practices. In which this work stresses the utilisation of blockchains, can fully protect the chain of custody process, assuring to protect the integral part of any such legal investigation processes and procedures, as long as all nodes that participate the blockchain accept and hash all evidences being supplied. By referring to this example, the aim of this thesis is to reduce or eliminate the issue of evidence being tampered or destroyed illegally.

As long as there has been a social need and demand of device mobility, both in research activities and continual development of current and new ad hoc devices (such as Internet of Things, Opportunistic Network Nodes, and Delayed Tolerant Infrastructure Nodes). There has been a prediction to which the number of these devices will exponentially increase, with a specific estimate of 50 billion devices that will be networked by the year 2020 (Botta, de Donato, Persico, & Pescapé, 2014). In which that specific statics estimate that Botta, de Donato, Persico, & Pescapé (2014) have stated, will need to have an attention to specificity must be considered for managing all of the data that have been generated by these devices. This specificity of having a digital solution will surely compliment, the development of mechanisms of acquiring the need of having a digital witness. This type of mechanism is a specific device that can handle certain forensic activities such as identification, collection, safeguarding, and communication of certain digital forensic evidence (Niteo, Roman, & Lopez, 2016).

Unlike centralised approached, logging of node activity is possible to be done because nodes within a cluster with a configured centralised master. To attract a user interaction within a newly designed system, this usually involves the aspects of security mechanisms. These specific security mechanisms are included to protect the transmission and exchange of data between such as cryptographic methods. To which cryptography is a common approach used to provide data confidentiality and integrity (Banerjee, Lee, & Choo, 2018).

In which overtime, bridging the gap with ad-hoc measures has become increasingly infeasible (Roussev, Quates, & Martell, 2013). This work needs to constantly remember that Delay-Tolerant Network is a part of the general concept of Internet-of-Things (IoT). In which methods that are under this methodology, can communicate with billions of things simultaneously (Atlam, Alenezi, Alassafi, & Wills, 2018). In different types of configurable methods, which is good since most or all communication methods are dynamic. But this introduces a range of issues when it comes to capturing important data, such as performing forensic tasks on post incidental.

This work stresses the importance of the features and characteristics of blockchain, can solve the reputation of any offline transactional as a post-transactional checker. Hence stated application throughout the whole transactional procedure will be more sensible approach. Using blockchain in the method of, logging as a service-oriented application, will ensure that all logging of transactions is on a valid state and cannot be tampered. This can be demonstrated in Figure 3.2, it shows a demonstration, to which blockchain applications can be used for two purposes of providing a digital currency and logging of user transactions and activities platforms. In which digital currencies (or cryptocurrencies) can be used to handle digital monetary services. To make all nodes top can be able to participate in a blockchain environment for all logging activities. Even storing some information for later and having them transmitted the specific information into the blockchain environment.

The other blockchain platform that has been demonstrated on Figure 3.2, for the purpose of storing and logging user transactions and activities, this has been depicted of having this platform on the cloud as its primary storage. The reason behind in having this on the cloud is (1) to protect that specific blockchain from illegal data tampering, (2) reduce the issue of physical maintenance of the blockchain system. Due to the increasing of cybercriminal activities, having this type of blockchain system will also enable a secured and fool- and tamper- proof system. To which this work proposes to have a systematic approach of validation of transactions that have occurred between digital currency services.

Considering that digital currency (financial) data, will require the same high degree of privacy intensive requirements as of Healthcare. Where large amounts of data are created, disseminated, stored and accessed daily by users (Esposito, De Santis, Tortora, Chang, & Choo, 2018). Not only healthcare that will require that high degree of privacy, also some autonomous nodes such as portable devices and specific attacks if these nodes are not protected properly.

Noticing this happens on delay-tolerant network nodes when interacting with each other. No internet connection, hence, the only method of communication is a nearby approach transmission method between nodes. These nodes will be required to have their transactional information updated, once they have been connected to the Internet or to a device that can act as an intermediary. Meaning that all logged activity can be traced down easily by following a chain. It is also a composed of verifiable records for each single transaction ever made (Jiang, Guo, Liang, Lai, & Wen, 2017). For each verifiable logged record and transaction will not be able to be changed, due to all information stored in a blockchain system will be protected. The full cooperation of all participating nodes within a network or cluster, node participants can perform a decentralised verification method of logged data into a blockchain system. If by chance there is a need to be a change on a block, that change will need to go through the whole network of nodes to agree on the change. In an event that there is no consensus, in any event such as creating a block within the blockchain system cannot be initiated.

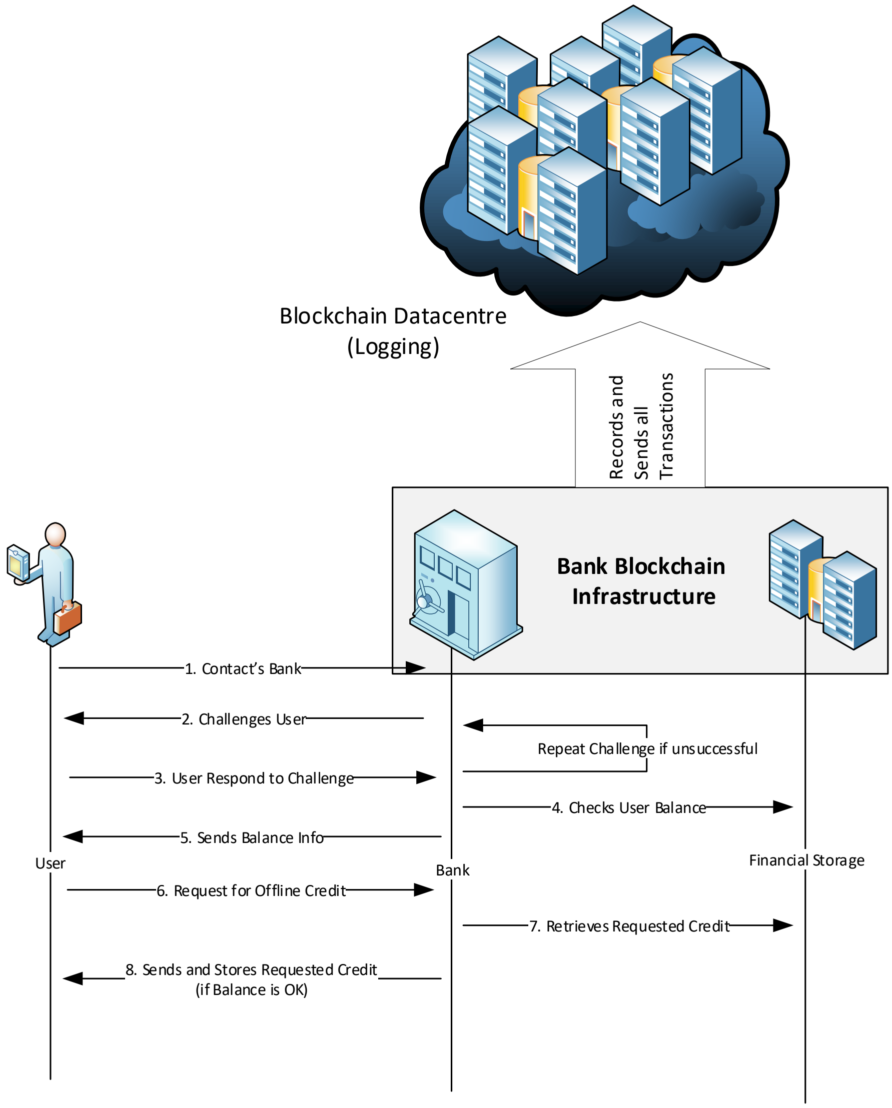

Figure 3.2. User Transaction for Offline Withdrawing Digital Currency

As far as this work goes further into the need of forensic approaches, the use of the blockchain technology for logging as a type of live forensics methodology. Where everything will be logged and collected in real-time. This type of blockchain can be described as the method of Proof-of-Work, where all the logged actions are being used, through the aiding technology of blockchain to validate all activities (referring to Figure 3.2.). Meaning all activities from requesting, acquiring, depositing, will be logged in a separate blockchain. Such participating nodes will be used for the purpose of having to follow this process. In comparison to other logging database activities that are purely centralised under on server. Blockchain itself is a form of a decentralised database which distributes the workload of all data between nodes (that participate in the transaction), and nodes that are configured to facilitate al transactions of the whole ledger (McGhin, Choo, Liu, & He, 2019).

There has also been a study for the use of blockchain in the process of revocation of nodes and digital certificates. Example of this could be the use of the algorithm of Proof-of-Work (or consensus algorithms), to which all aspects of security and privacy of blocks are protected by this specific algorithm. The purpose of Proof-of-Work does in the blockchain system makes it better against any network failure which is caused by nodes disconnecting overtime (Lei, et al., 2019). That specific consensus algorithm of Proof-of-Work is mostly used by big cryptocurrencies such as Bitcoin. Revocation of nodes is purely essential to the overall management of any delay-tolerant networks, and this includes also some other forms of decentralised networks. A specifically configured revocation system where it can protect data by (1) the access control of data, (2) authentication, (3) non-repudiation, and (4) availability of services.

VANETs (which are under the Delay Tolerant Infrastructures), aims to promote safe self-driving methods, with great benefits of improving the flow of traffic and decrease incidents (Hasarouny, Samhat, Bassil, & Laouiti, 2017). Lei, et al. (2019), have conducted a study to which they have contributed for using blockchain as a basis of certificate revocation using VANETs.

The certain exchange of messages using pseudonym (meaning aliases), then using the exact identity of the participating nodes. The use of aliases, meaning partial information that will be used for the encryption processes. Participating nodes in reference to the study of Lei, et al. (2019), in which they proposed that nodes will be the ones that will manage all of the aspects of key management and distribution to affected nodes within the specific infrastructure. Meaning that there will be no certain central node or server that will handle all the key requests and revocation. As the specific system further develops, as this reaches maturity. It will require both strong management aspects of security and key management for the purpose of having a secure environment. This specific key exchange has also been explored and studied by Hasarouny, Samhat, Bassil, & Laouiti (2017), they have incorporated on their study is the use of Public Key Infrastructure (PKI) method. The use of PKI has been known as a popular method of security mechanisms due to its support both distribution and identification of public encryption keys.

Expanding more on pseudonym method of digital key management, the needs to understand that that using very minimal information for key enrolment is a good idea to protect good nodes. Having a pseudonym system in place for cluster of nodes (or referring to them as security domains), this can give an opportunity to nodes to be able to exploit the system. In which that specific scenario may happen if there is an issue of having security domains are not somewhat cooperating with each other. Remembering that, these nodes have the freedom to move anywhere due to its decentralised focused.

One exemplar scenario domain to consider is to take is the emergency response management situations. In this specific scenario can be provoked by either natural, or man-made, in which this thesis has observed. These are mostly wireless network sensors have been used to protect us from certain disasters, these wireless networks are also been used for the purpose of monitoring activity and aiding the assessment of damage inflicted. Such real effective emergency management response requires to protect all communication channels, and protecting is by the means of us need to consider the aspects of strong communication networks. These strong communication networks have been put in place need to make sure that, an effective information sharing and decision support systems in place (Seba, Nouali-Taboudjemat, Badache, & Seba, 2019). Ensuring that these network nodes (could either be a VANET, MANET, or UAV), are protected from certain network-based or node-based attacks of compromising data.

Leading us back into the issues of certain delay-tolerant infrastructure attacks of blackhole and grey hole attacks, were supposed malicious nodes can freely move in and join with other domains (or clusters) in self disguise as a good node. Regardless of the sensitivity of the transmitted or exchanged data, treating all data with the specific security aspects of non-repudiation, integrity, and availability. Bucur & Iacca (2017) have identified on their research certain attacks that can occur within these networks such as (1) black-hole, and (2) flooding attacks. In the case of a black-hole attacks, the specific attacker can have the ability to drop packets in the duration of the transmission process, which prevents data being both stored and forwarded. A black-hole attack methodology can be considered as a type of attack based on keeping the forwarded data stored. For the purposes of node prevention (or elimination) of the attack impact, highly considering to put in place such detection mechanisms.

Due to the autonomous and ad hoc characteristics of Opportunistic Networks (or Delay-Tolerant Networks) and no security mechanisms in place, all nodes that are participating in the network or cluster are in some sort of so-called a blind trust. In reference again to the characteristics of delay tolerant networks and its routing protocols, without the inclusion of security mechanisms. Hence in a forensic standpoint, this will become an issue itself if the malicious node is needed to be contained away to prevent future attacks. With the rapid growth (in terms of manufacturing and demand) of having these smart devices (such as Internet of Things and Delay Tolerant Networks). This has highly gained a wider acceptance and popularity as the main standard for low-power lossy network (LLNs) having such constrained resources (Khan & Salah, 2018).

Figure 3.3 demonstrates to us the demonstration of this type of attack. It is noted that this work needs to consider all the nodes or persons within the same cluster to demonstrate that attacks can occur easily within. The source person wants to send a data to destination Y, but the Source node does not have an idea on how to reach Destination Y. So, the Source node’s only way is to contact the node Destination X. The Source node does not have an idea that the node Destination X is a malicious node. So being the node Destination X being the silent malicious node, decided to have the data that supposed to be for node Destination Y to be dropped.

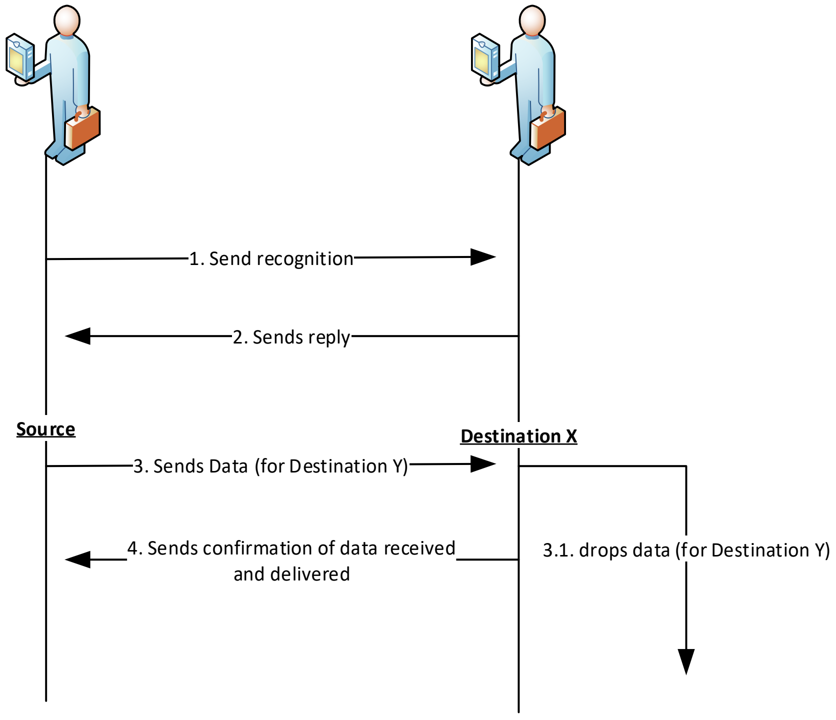
Source
Destination X
Destination Y
1. Send recognition
2. Sends reply
3. Sends Data (for Destination Y)
4. Sends confirmation of data received and delivered
3.1. drops data (for Destination Y)

Figure 3.3. black-hole packet dropping

Flooding attack methodology is were an attacker could disguise as a non-malicious node. to which it silently attacks all the nodes by injecting and sending fake messages to flood a network. The main objective of this flooding attack method is to perform an attempt of Denial-of-Service attack. To which this specific attack method, also can make false transmission paths (as such as routing tables) to mislead nodes within a cluster of nodes. To which a study of Denial-of-service attacks, conducted by Mamolar, Pervez, Calero, & Khattack (2018), to which they have proposed a system to which is focused on validation and prevention of such Denial-of-Service attack in a specific cluster of nodes. To which their specific proposed solution system in such following two main design objectives as such as (1) modular design and (2) extendable data modelling.

Nodes such as either Internet of Things or Delay Tolerant Networks, which are set up for personal security, financial, governmental, and healthcare. A successful attack on its system can have a serious consequence on the users that may full depend on it (Hossian, Hasan, & Zawoad, 2018). Such consequences are more common sense focused such as issues on data privacy and such attacks can be used as an open backdoor to other network attack methods. Banerjee, Lee, & Choo (2018), on their study that focuses on the application of Internet of Things nodes with blockchains in a military scenario. They have highlighted the benefits of blockchain integrity for the purposes of improving the security of ad hoc items used. To which this has matched with the study that was conducted by Reyna, Martín, Chen, Soler, & Díaz (2018). If the common goal of these security mechanisms to protect the flow all personal data throughout the built infrastructure.

3.5. Blockchain Technologies Integration Challenges and Opportunities

The general overview of blockchain technologies has been the hype of since the inception of cryptocurrencies. But in general, blockchains are also used in different forms such as identification, logging and tracing services, digitalised democratic elections, and many others who want to have a less centralised applications. In a form of decentralised environment, enabling systems and applications to have a degree of independency from configured centralised authority and decentralisation of trust management. Nonetheless, due to the decentralised architecture and nature of blockchain technologies, it has bought us a system of a distributed database that has a high degree of fault-tolerance and non-repudiation. The cryptographic security benefits such as pseudonymous identities, data integrity and authentication (Makhdoom, Abolhasan, Abbas, & Ni, 2019).

There has been a study that was covered by Reyna, Martín, Chen, Soler, & Díaz (2018), where they conducted a study into the challenges and opportunities of integration of blockchains and Internet of Things. Certain issues that they have identified such as (1) security (weaknesses and threats), (2) storage capacity, (3) storage scalability, (4) anonymity and data privacy, (5) smart contracts, and (6) legal issues. But regardless about the stated disadvantages Reyna, Martín, Chen, Soler, & Díaz (2018), have stated on their study that the integration of Internet-of-Things and Blockchain has some great benefits. The advantages of integrating of both of these technologies as such as (1) decentralisation and scalability support, (2) identity, (3) autonomy, (4) reliability, (5) security, (6) market of services, and (7) secure code deployment.

In which the same advantages can be applied with blockchain and delayed tolerant networks in both financial and logging. In which the development of applications and other digital products can be controlled and secured without a centralised authority, all nodes and its transactions can be identified. This in fact that both blockchains and Internet-of-Things as concerned both having the similar characteristics. Blockchains can be extremely beneficial to the Internet-of-Things by providing a trusted platform for sharing service, were such information is reliable and traceable (Reyna, Martín, Chen, Soler, & Díaz, 2018). Which means all transactions will be transparent and all certain modifications can be tracked and traced, to the fact that it can be used for the improvement of systems security (Banerjee, Lee, & Choo, 2018).

This means all types of data sources that are required to conform with the blockchain network itself, can be identified and undisputable. To which can also open up several new development opportunities, as this research goes deeply into the integration between Blockchain and Internet-of-Things in comparison with integrating blockchains and delay-tolerant networks. Another sector to which the blockchain technology can benefit is the enhancing and creating a resilient supply chain processes. Incorporating blockchain technology into the specific process intensive such as supply chain management, which can cause a high mitigation of risk, prevent disruptions (either one-off or repetitive), improving flexibility, and a change in the culture of the organisation. It can also protect digital systems from cybersecurity threats, to which the management of supply chains can be regarded very sensitive (with Healthcare and Finance). Due to the high demand of digitalisation of processes and data mobility, to which can remove the risk of a single point of failure with its end-to-end encryption, visibility and privacy (Min, 2019). This means that deliveries and the management of supplies can be easily be done, it can also be traced if there has been some sort of issues within the process. Hence the recording of all involved assets, the courier company in-charge of the delivery, and right to the person that has been intended to receive that specific delivered item. These stated activities (and including other related activities that have been mentioned) can be added into the blockchain application of tracking the movement of items within the supply chain process.

This was previously stated on Section 3.4 about the forensic approaches and methods for opportunistic networks and decentralised cryptographic methods. But this type of infrastructure approach, has been designed to cope with the challenging conditions in restricted networks with sparse density, intermittent disruption and limited energy (Guo, Wang, Cheng, & Huang, 2017). Routing protocols on networks such as Delayed Tolerant Infrastructures is important for the purpose of delivering information within the whole network.

Guo, Wang, Cheng, & Huang (2017), in their paper have introduced the concept of LACS (or Location-Aided Controlled Spraying). This is an algorithm designed as a scheme (or as representative overview) over appropriate routing algorithms based on delayed tolerant or opportunistic networks. Which this type of routing algorithm is only based on the event when many nodes are connected and sensed each other. LACS have two main methods were introduced such as (1) node contact (a unicast direct contact communication), and (2) controlled spraying stage (a unicast nearby communication contact). Both main methods are executed that the time when there has been a near to close contact with any configured nodes that are able to receive that specific message.

3.6. Chapter Summary

DTN technology which has a promising future on rural and remote areas to be able to use the Internet. Having the Internet being available to such areas, will ensure rural and remote users the ability to access information available. Since most services now are depended on the use of the Internet, users through DTN technology will have the ability to access such services. Hence, DTN can be deployed using either using land-based and air-based vehicles, equipped with sensors, NFC, and Bluetooth modules. To which data can be passed between nodes depending on how near or far between nodes are between each other. Deployment of DTN can be done either in a full or hybrid approach similar to Figure 4.1, where there is a mixture of both real-time and delay tolerant networks being converted into one topology. Delay tolerant networks are far more scalable and can be dynamically and strategically geographically placed, without the dependent use of a constant physical connection between nodes.

This chapter had highlighted the importance of the implementation of secure mechanisms and how they can be applied to opportunistic networks. As mentioned, opportunistic nodes have the ability to store information without of the technologies that have been mentioned, such as blockchains and threshold cryptography. These two technologies mentioned in this work, have highlighted the benefits it can bring to securing DTN and other opportunistic type networks. It has been highlighted in this chapter is the importance of having the application of secure mechanisms. The use of these secure mechanisms, especially blockchains, where it needs a cluster of nodes required to do a certain function, to create a block. It can also be used not only for cryptocurrencies, there are so much more to which blockchains can be used for identification of legitimate nodes within the cluster.

A blockchain identification management system will be handy to identify legitimate nodes within a cluster or a number of clusters. Easing off the administration tasks of ad-hoc nodes on any communities these nodes have associated themselves. Threshold Cryptography does work similarly to what blockchains have in nature in terms of encryption, which can control the number of nodes that can share compute a key request within a community. Clearly an issue has been identified, in terms with the management of nodes that handle the computation of shared keys. Such basics such as IP address groupings have been mentioned, to easily identify which are the requestor nodes and the nodes that compute share encryption keys.

Chapter 4 - Security Mechanisms for Offline and Online Transactions

This chapter has proposed three ideas including (i) the incorporation of blockchains on delay-tolerant infrastructures, (ii) the application of threshold cryptography, and (iii) the hybrid (online and offline) validation techniques. These three concepts are to complement the ideas that have been stated on the literature review (on Chapter 3). These specific ideas aim to synthesize the Internet of things, Delay Tolerant Networks, Blockchains and Threshold Cryptography technologies and their associated methods. The main goal of these proposed ideas is to achieve the full goal of having security mechanisms on delay tolerant networks. This chapter aims to address the stated research questions that have been mentioned in Section 1.3. It introduces the developed prototype, and primarily validate the key ideas.

4.1. Overview of the Idealistic System

This work demonstrated the idealistic system to be proposed. Referring to Figure 3.1, showing the specific exchange of financial data without security mechanisms implemented. Without security mechanisms, any attacker within the delay tolerant infrastructure will be able to illegally tamper, store, or listen to communication channels that have been established. In this scenario, it will be demonstrating the implementation of security mechanisms over digital currency and a hybrid delayed tolerant infrastructures. As current wireless data transfer among everyday devices will continue to improve and succeed as a specific technological phenomenon of modern computing (Gupta, et al., 2019).

Figure 4.1 shows a diagram example of the implementation of having a digital currency and logging of all user transactions. The diagram depicts two zones have been drawn up to represent the well-connected and the limited-to-non-connectivity zones. Alternatively, the diagram demonstrates that the well-connected zone represents areas that have been urbanised. The well-connected zone, there is a high degree of network connectivity and variety of network mediums are available to be used such as Wi-Fi, Cellular network, and even Personal Area Network mediums such as Bluetooth and NFC. The full purpose of having a blockchain based logging is to aid different banks for transactional verification. In reference to the diagram in Figure 4.1, if the main type of currency is only based on blockchain technology, all digital transactions will be transparent and can be easily traced. This can also mean that all users will be required to be under one currency, through using one application to manage all transactions. This specific application will be required to be installed on any user's mobile phone where they can transact using NFC or Bluetooth. If a specific user is in the Full Data Connectivity Zone, they can perform such transactions over the Internet or still have the option to perform transactions over NFC or Bluetooth mediums.

This specific cloud based blockchain banking system can establish the validity of any occurred transaction. Users once they have either visited their bank, or have a degree of strong connectivity, they will be able to perform transactions in real-time and update all stored offline transactions. Within this specific scenario, forcing all users to participate within the blockchain environments. Users who participate within this distributed network of blockchains, can have an ability to trace and verify their own transactions. Any transaction that occurs between other users in the limited-to-non-connectivity zone, they will be able to update and verify any occurred offline transactions.

If by chance there are nodes classified as VANETs, passes by a digital user heading to a zone with full connectivity. The configured vehicle will be able to grab all the stored offline transaction, afterwards will be able to upload and update those specific transactions on behalf of the user that performed that offline transaction. This specific type of transaction can be done with a user performing an offline transaction if there has been a VANET node that has gone pass the specific user. This type of action, to classify as an offline hybrid approach for the validation and logging of all digital transactions. The hybrid approach and method of validation and logging can be done with the purpose of using either Ubiquitous Sensor Networks (USN).

As defined in the study conducted by Perez, Zeadally, & Jabeur (2017), that USNs are (1) more powerful and can handle more data than Wireless Sensor Networks (WSN). Lastly, other characteristics of USNs have (2) the ability of use TLS to create a point-to-point secure communication medium. Such secure communications to which could have certain activities within that medium such as, key distribution and other specific cryptographic protocols in Internet-of-Things devices (Perez, Zeadally, & Jabeur, 2017). Sections 4.2, 4.3, and 4.4 of this chapter will cover an in-depth analysis of technological methods and applications, in which these will complement the idealistic requirements. Hopefully in future some of these ideas that have put in this chapter, will open more research questions and opportunities. It will be able to improve or create the new methods, services, and applications, with a goal to make all services that are highly available on the urban areas. Such applications and methods are to reach out to the minor population centres who have either limited to no change of reaching such services.

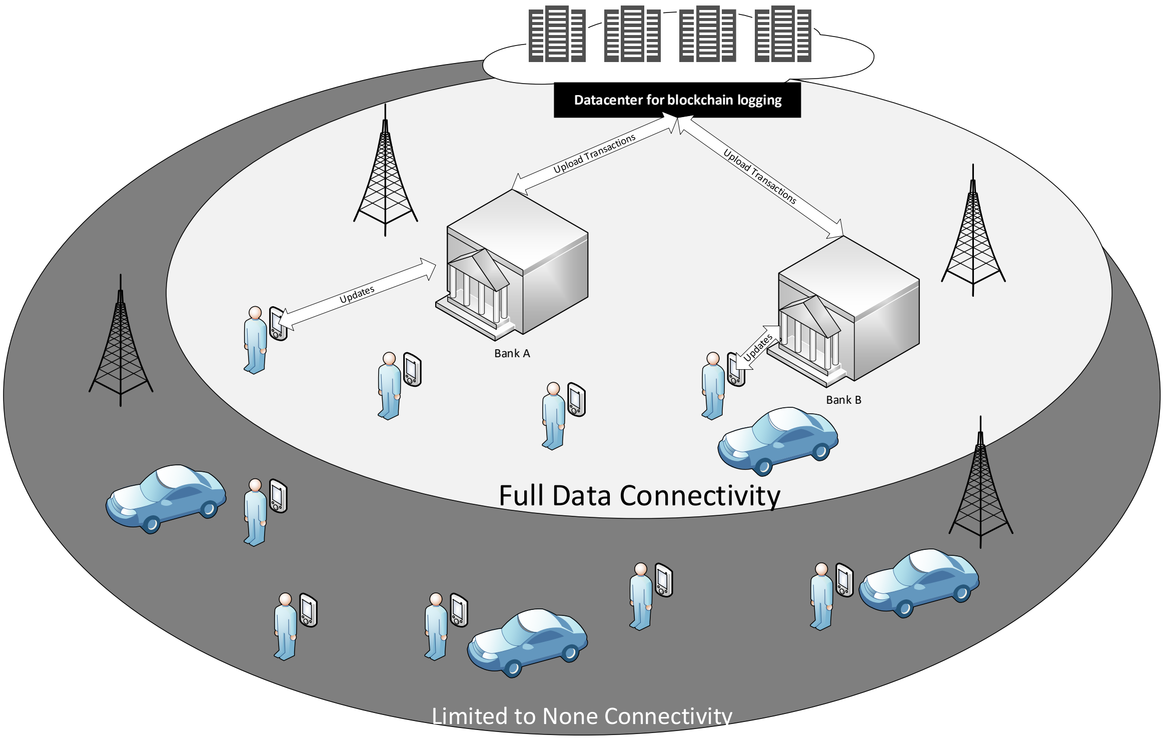

Figure 4.1. Conceptional diagram of digital currency and logging through blockchains

The specific applications of having certain technology and methods of blockchains and threshold cryptography, these will be further discussed in the following sections 4.2, 4.3 and 4.4. The specific aim of these stated discussions is to go within the technical processes of these technology and methods.

These specific ideas that this work proposes, are to have a conceptual system that will has the ability to accommodate a variety of users from urban and non-urban areas. Even though in today's environment, where connectivity to the Internet has been come the necessity, over having the Internet as a privilege. In some parts of the world, there are still a number of rural and remote areas, where there are several habitants that have either little to no Internet connection, commonly called the "Digital Divide". This has been the strongest factor that there are still some number of people that are not able to get the information and the level of connectivity that they want or what these people (in rural and remote areas) desire to have.

The VANETs (Vehicular Autonomous Networks) or UAVs (Unmanned Autonomous Vehicles) can be deployed to reach out to the remote areas of isolated communities. Henceforth, we need to highlight the real problem is the digital divide and exclusion, from mostly rural and remote areas to which there have been either non-existent or less existent systems. Governments can in fact benefit from forming sensible strategies, guidelines and policies, to be able to bridge identified and potential digital divides which has been a core challenge when forming an inclusive and participatory digital democracy and society (Wihlborg & Engstrom, 2017). This in fact will remain as a specific challenge, which are both social demand and the specific demand of security mechanisms.

Knowing that Information Technology and its applications and processes have benefited all aspects of society. As such that this work proposes the need to have a thought of including a conceptual need of implementation of information security, having a specific assurance of data being taken care. Also having a good mind into having information security within these areas of concern with the issue of digital divide, will be a positive factor of attracting users to use the specific system. Having in mind and putting into practice of such, identification of critical success factors that are vital for the maturity of the system's security posture (Chisanga & Ngassam, 2017). Without the assurance of these measures to bridge the digital gap, anyone will not be able to achieve such full participation of all users of both rural and urban population clustered groups.

4.2. The Incorporation of Blockchains on Delay-Tolerant Infrastructures

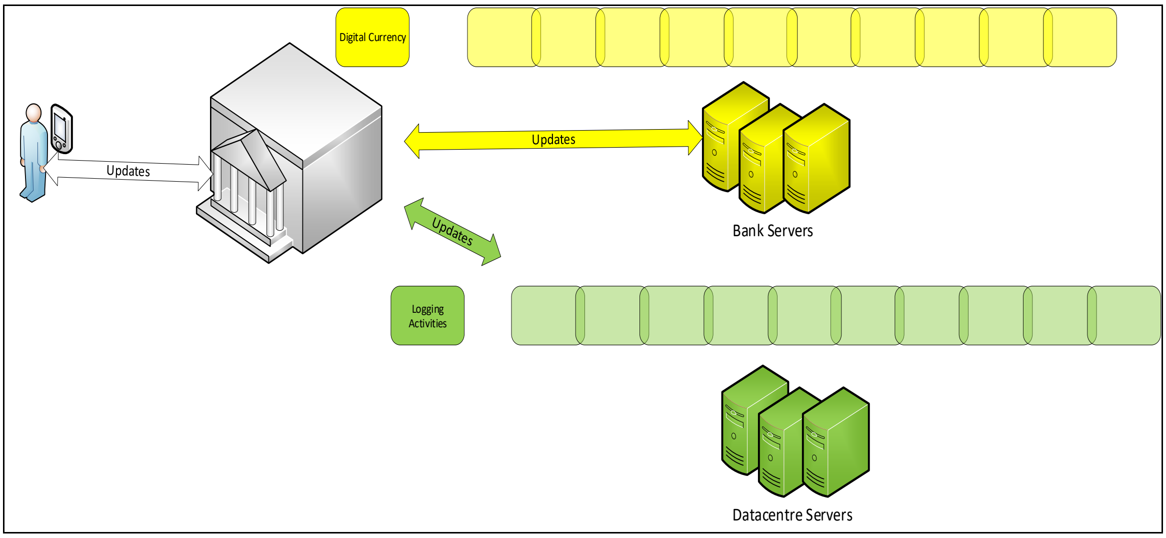

Figure 4.2. Depiction of blockchains for both as distributed ledger and activity logging

Firstly, having a full understanding the need the use of blockchains for both on digital currency and logging of transactions. Blockchains in general covers the whole aspect of having three general main points that are needed to be achieved prior development and implementation of these technologies, such as (1) trust, (2) transparency, and (3) accountability.

A blockchain system, as iterated in this thesis, as being distributed, decentralised, corruption-free, and consensus-based application to protect all stored information within this distributed database. As along as all nodes that are within the blockchain agree with the entered data, this specified agreed data will be hashed and stored. The hashing of any specified stored data will be able to create an environment, that provides only approved and trusted source of data, in which can be resulted into having a method source of distributed truth.

For the purpose of this research, this work proposes the implementation of a dual blockchain process for storing digital currency and for logging activities and transactions. Aiding us into understanding why this work stresses the use of blockchain technology for the sole purpose of this specific research activity, this work has stated several justified reasons in Table 4.1 (about Digital Currency) and Table 4.2. (about Logging Activities).

To justify the reason of proposing the implementation of two blockchain system, is due to the need and to complement the forensic aspects of this research. The main reason to which this work proposes of having blockchains for logging user transactions and activities is to provide a forensic enabled data collection system that does not need to compromise the function of the other blockchain that is used for digital currency services. Other activities and tasks that people can also accomplish, as such achieving uniformity of all stored and to be stored data within any decentralised data structure.

Table 4.1. Reasons for blockchain technology for Digital Currency

Blockchain Features	**Digital Currency Reasons**
Trust	1. Provided the digital currency can be used for exchanging such financial transactions, in which can be done in both offline (passive) and online (active). Giving users of this proposed idea that all transactions can be trusted. 2. The specific digital currency can be trusted and treated as an official currency. Meaning that this will be able to offer the same experience has doing a manual transaction on using physical money
Transparency	1. To be able to view digital currency transactions from different users, and movement of the digital currency from one account code to another. 2. To be able to monitor personal privacy of the accounts and the user of the digital currency. In which can be done by the person that have the account that contains personal digital currency data.
Accountability	1. To provide a platform for digital currency users, of making them accountable of any created or initiated transactions. 2. To be able to have a tracking mechanism for digital currency blockchains. The specificity of liability of storing of digital currency data and user digital transactions and activity. 3. Ensuring that all associated blockchain data for digital currency are being accounted and open for circulation and public use.

Table 4.2. Reasons for blockchain technology for Logging Activities and Transactions

Blockchain Features	**Logging Activities and Transactions Reasons**
Trust	1. To be able to have a mechanism of trust for all digital transactions and activities within the blockchain developed from digital currency. 2. To have the ability of having a blockchain, that is forensic ready and actively enabled. To which that specific blockchain application can provide an automatic management and safeguarding from revoked or misbehaving nodes.
Transparency	1. The ability to have a transparent process and accepting of logging of transactions both malicious and not malicious. 2. A system to which have a specific logging or records and protecting the privacy of the users. The users in return can view their logged activities and transactions within the blockchain technology.
Accountability	1. To put the specificity of accountability on nodes do participate in the process of ensuring that all logged activities related to specific transaction and activity have been logged. 2. Data that will be required to be used to store information of transactions and other activities. Through the application of blockchain, sets or rules on governing the data requirements of this blockchains. 3. If the data to be store in the blockchain platform follows the rules, then it should be good to go for that node to continue loading the blockchain with more transactional data.

Blockchains have been popularised with the development of bitcoin and including all other types of cryptocurrencies. This thesis will not be focusing its discussion of blockchains on the aspect of digital currencies (or commonly called cryptocurrencies). In fact, blockchains itself can be used as a form of a distributed database, with rules that can be implemented on how data can be used and stored (the concept of pseudonym method). Though remembering that, these are full-stack systems where security is a critical factor for their success (Homoliak, Venugopalan, Hum, & Szalachowski, 2019). In this type of technology, all blocks are created and completed through reusing of hashes from the previous block, within a specific consensus rules on how data can be created as part of a new block, nodes that are part of this specific block can be used (as such as monetary transaction and logging of activities).

In the diagram that has been demonstrated on Figure 4.2, two types of blockchain have been shown to demonstrate the specific need of blockchains, in which one will be focused on as a digital currency services (or cryptocurrency, being coloured yellow). Digital currency users can have the ability to perform transactions with other users, regardless these users' banking organisations. The incorporation of blockchain technologies will have the ability to make sure that they will be able to trust such digital currencies.

The green chain on the Figure 4.2, focuses on the purpose of audit trailing and logging of transactional financial activities. Referring to the supply chain scenario of integrating blockchains on Sections 3.5 and 3.4. in which this thesis mentions the use of this specific technologies for the use of blockchains for the purpose of protecting digital evidence, chain of custody, and supply chain processes. This work can also replicate this with having a blockchain system to be able to store the log of user transaction activities. Such banks (both current and new) that will be offering digital currency servers, can have this type of blockchain information stored offsite. For example, planning and proposing the use of such cloud as a typical solution to store information of user transaction activities.

4.3. The Application of Threshold Cryptography

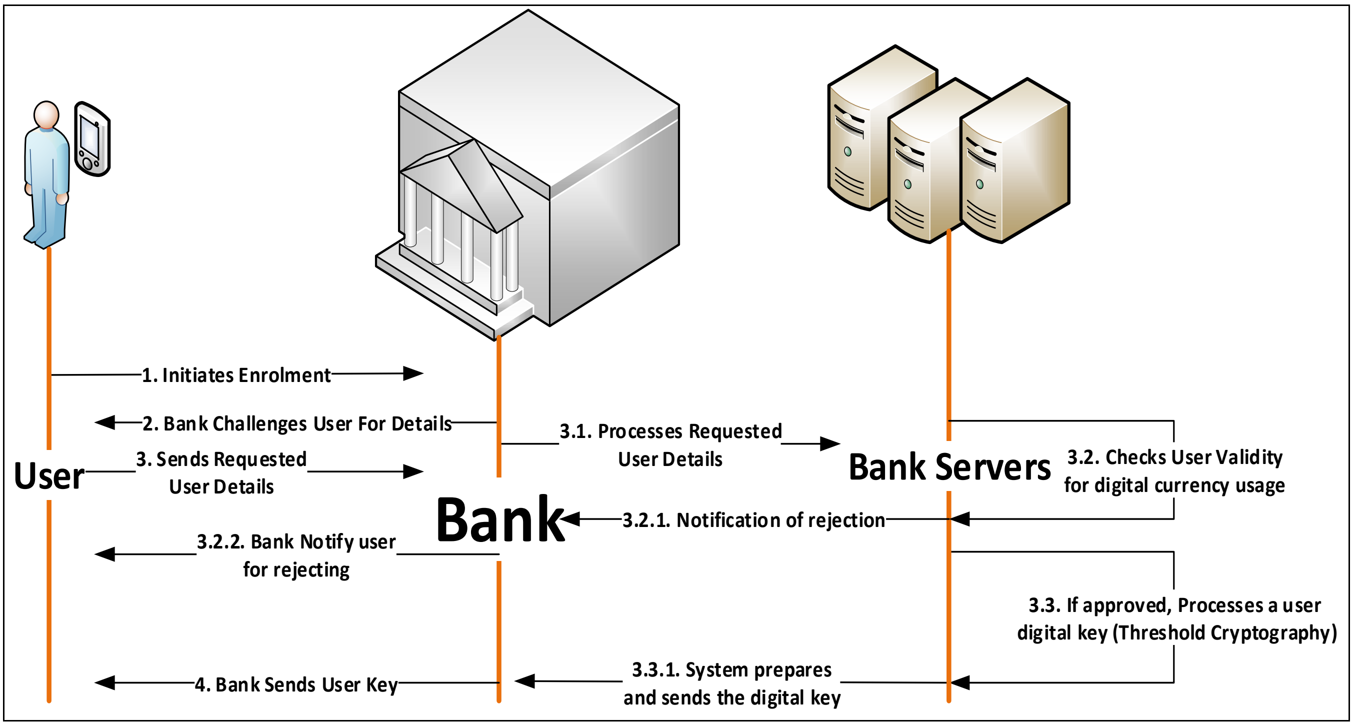
1. Initiates Enrolment
2. Bank Challenges User For Details
User
3. Sends Requested User Details
3.1. Processes Requested User Details
Bank Servers
3.2. Checks User Validity for digital currency usage
Bank
3.2.1. Notification of rejection
3.2.2. Bank Notify user for rejecting
3.3. If approved, Processes a user digital key (Threshold Cryptography)
3.3.1. System prepares and sends the digital key
4. Bank Sends User Key

Figure 4.3. The idealistic process of applying Threshold Cryptography for managing bank user registrations

Threshold cryptography is another type of distributed cypher system application, considering the use for user device enrolment method. This type of cryptographic method also has the mechanism to put in place controls, in relation to its decentralised nature in which the realistic implementation can be seamlessly be accomplished. Hence, this specific cypher is not a brand-new security mechanism application, this has been used in several research activities that have been conducted by the following academics such as Ahmad, et al. (2019), Stathakopoulou & Cachin (2017), Gharib, Moradlou, Doostari, & Movaghar (2017) and Goldfeder, et al. (2015).

The application of threshold cryptograph upon DTI, opportunistic and other ad-hoc networks and applications require security service aspects of privacy, anonymity, authentication, and non-repudiation (Avramidis, Kotzanikolaou, Douligeris, & Burmester, 2012). But yet, this is impossible for the implementation of these security service aspects, due to the fact that DTI, opportunistic networks, and ad-hoc networks are not hierarchical network based applications.

Since threshold cryptography, uses a specific shared key procedure and as previously iterated within this thesis. That introduces the distributed systematic of trust between nodes that are part of the cryptographic process. In which follows a scheme of (t, s) ratio system, meaning that t value represents the number of included parties, and the s value represents the minimum number needed to decrypt a secret. This specific encryption method and application is a specialised cryptographic methodology and algorithm, which has derived from the Public Key Infrastructure. To which have been extensively studied by Adi Shamir, a person who have introduced the threshold cryptographic ratio definitions which have been mentioned in the literature. This specific rationed system, will then have the share of encryption key generation being shared between nominated nodes. Referring to this, by following the formula 1 < t < s, as such knowledge of any t shares will allow the secrete k to be reconstructed, however, the knowledge of t – 1 share will reveal no information (Ahmad, et al., 2019). That mentioned formula tells us that, it is needed that more than 1 node will be required to generate keys

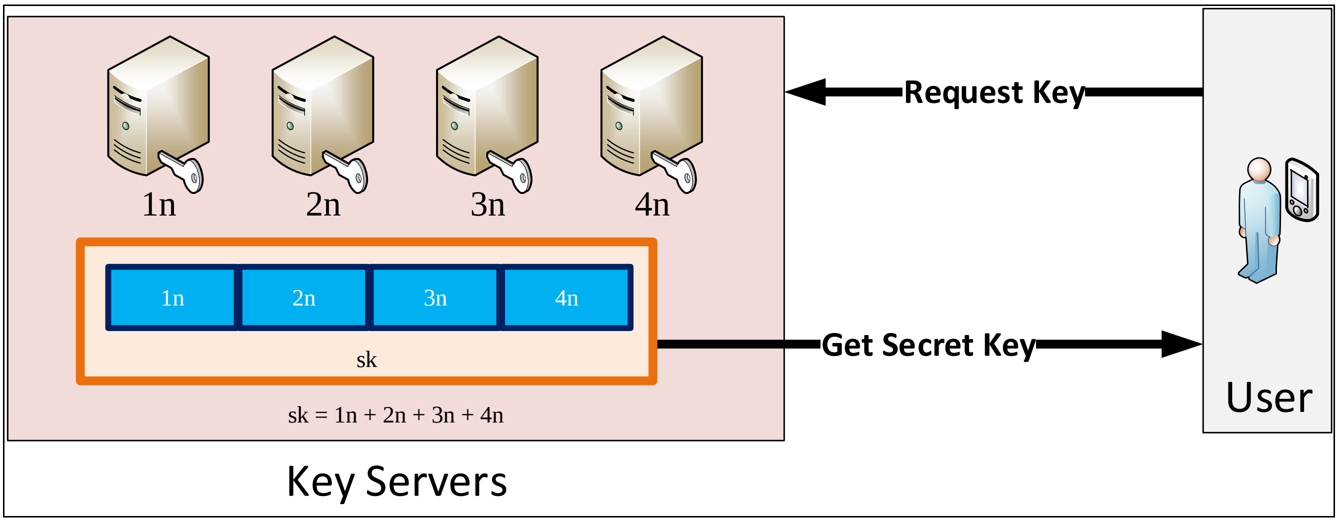

Figure 4.4. Key Request Summary Process

for the specific requesting node. So, in this specific scenario, there is only one node available and active within a cluster, then they may be asked to join a different cluster or network, which can provide this application service.

The descriptive nature of its algorithm is a distributed, ad-hoc, and disruptive-tolerant cryptographic algorithm, which is a perfect algorithm for opportunistic nodes (such as delay-tolerant network nodes). All nominated nodes that have been configured to handle all cryptographic processes of decryption and encryption and including the management and allocation of encryption keys. In today's digital environment, this work must consider the apply security mechanisms of any applications (hardware and/or software) that are desired to be used. This thesis has mentioned the implementation of encryption, is to protect the integrity of data being transmitted from its source to its intended destination also to facilitate the need of having authentication. The concept of authentication has been used in the past for both encrypted and non-encrypted environments to complement the issues of identity of users and nodes.

Such stated researchers have been able prove to us, this specific implementation can be achieved, by incorporating Threshold Cryptography, with Delay Tolerant Infrastructures and Blockchains. Figure 4.3 has demonstrated the proposed user device enrolment. Having a method of user device enrolment, as a major requirement resulting into having a digital user identity system. This work stresses its importance and a purpose of what has been demonstrated in Figures 4.3 and 4.4, which is a layer of protecting users from malicious transactions and users. Threshold cryptography's nature also complements the decentralised nature of all ad-hoc nodes, for the purpose of implementation of cryptography on any non-centralised and disruptive environment. Referring to what has been demonstrated on Figure 4.4, it can be the first line of defence against that attacks performed both from real-time and delay tolerant nodes regardless of its transaction methods. The implementation of threshold cryptography and to what has been demonstrated on Figures 4.1, 4.2, 4.3, 4.4, and 4.5, requiring a number of clusters to have certain number of nodes needed for approval of certain activities. The number of nodes can be configured to be able to serve encryption services in a distributed and ad-hoc approach. Having a number of nodes configured for handling encryption services, will be similar to configure nodes on real-time networks.

The advantages of encryption services being partly distributed throughout several nodes within a cluster, is to distribute and share the load of all encryption methods and processes. All nodes that have been configured to process such key generation requests, each nominated node will compute their own part of the key generation process. In duration of the process, all nodes will be able to agree on a certain consensus, if the node that has specifically requested to have a key will be able to have it. If all required nodes agree, then the specific node will be able to get the requested key. Which means that specific key, can be only used for that specific device only.

Using Figure 4.4 as an example, a cluster of nodes will be required to have at least four nodes to perform key generation, these nodes will be required to take part on the management of both key distribution and node participation within the cluster. The implementation of threshold cryptography, would require nodes to have a key installed on their device, which the device (or the user) will be able to participate within the community or cluster of nodes. That specific cluster or network of nodes, in which the node (and its user) have been required to be able to take part into, to be able to exchange data to other nodes within the specific cluster or network.

The user request of having a digital key, that user can use that specific key to participate in any digital transaction process within the community, or as long as both users are within the same digital bank. In respect to the rule of concept of this cryptographic application, having each server to be placed in each digital bank (banking organisations). This means that all banks will be required to have at least one bank server can participate within several other key servers (from different digital banks). If this idea of having at least one server per each bank been adopted, technically having a facility of simplistic transaction between users regardless they participate or take part of any bank (cluster, or community).

Hence the sharing of encryption processes between configured number of nominated nodes, each of these specific nodes must compute their own part of the encryption process. So, in relation of Figures 4.3 and 4.3, which depicts to the enrolment process of a user to be registered into having and requesting a digital key for securing such digital transaction scenarios. Figure 4.4 show the high-level process of the whole process of the user requesting for a key and gets the key once all four nodes have generated their part of the key. In Figure 4.3, however is similar and show on how this can be done throughout the whole process of having an approval scheme system. A specific systematic process that allows banks to facilitate the approval and key generation, to which it is up to the banking organisations for them to decide on certain policy parameters on nodes (or users, or both) to be accepted into using digital currency services.

These policy parameters can be defined as by setting a score standard based on both or either node or user activity. Parameters can be defined as (1) the number of successful transactions, (2) the number of reported illegal transactions, (3) the number of legitimate transactions, or (4) any other parameters as defined by the digital bank on how either users or devices can participate. Figure 4.3 demonstrated the process of facilitating an approval on potential users and nodes that want to be part of this digital network. The user who desires to use the digital currency bank feature, with following the process that have been demonstrated on Figure 4.3

Since threshold cryptography, uses a specific shared key procedure and as previously iterated within this thesis. That introduces the distributed systematic of trust between nodes that are part of the cryptographic process. In which follows a scheme of (k,n) ratio, meaning that n value represents the number of included parties. The k value represents the minimum number needed to decrypt a secret. Elaborating more on Figure 4.3, in terms of approval the enrolment of nodes and users into utilising the facilitated digital currency system. Between the users and the bank, there will be a challenge process in which the bank will initiates once a user initiates the enrolment process.

It is up for the bank on point 2 of the diagram on Figure 4.3, on what type of details that the bank will use to challenge the node and the user. In this conceptual diagram, the bank can ask for the following details. For example, such as (1) device ID, (2) User Full Name, and (3) User Contact Details (e.g. phone number(s), email, physical address). If the information that the bank wants to challenge (or request) to the specific user, is very minimal, to which to keep up with the aspect of psedunomity aspect of both blockchains and threshold cryptography applications.

Once an enrolment has been initiated, the bank prior the user challenge and with the information collected from the node used for the user challenge, the bank and its servers will use the information to initiate the approval process. Referring on the diagram demonstrated on Figure 4.3, which depicts of having a blockchain that contains logging of user activity and transactions. The points of 3.2 to 3.3.1 depitcted in Figure 4.3, The bank and its servers can use this specific blockchain to trace down, and to aid the process of approval of the user who initiated the enrolment process. That specific blockchain for logging user activity and transactions, in which can be used as the one source of truth to aid the validation of user digital enrolment process. This has been further explained in Section 3.5 in this thesis, discusses the integration of blockchain technologies.

The banking system itself has the right to ensure that the user initiated the enrolment process, notifying either their enrolment requests have been approved or not approved. Specific banks that do offer this specific digital currency, must always record all user (customer and employee) transactions and actions on a blockchain dedicated application. To ensure that it continually complements the positive social aspect of ensuring that both accrual financial practices and readiness to forensic approaches, a technology-based platform is ready for any digital forensic investigation event to solve any such digital crime that may occur.

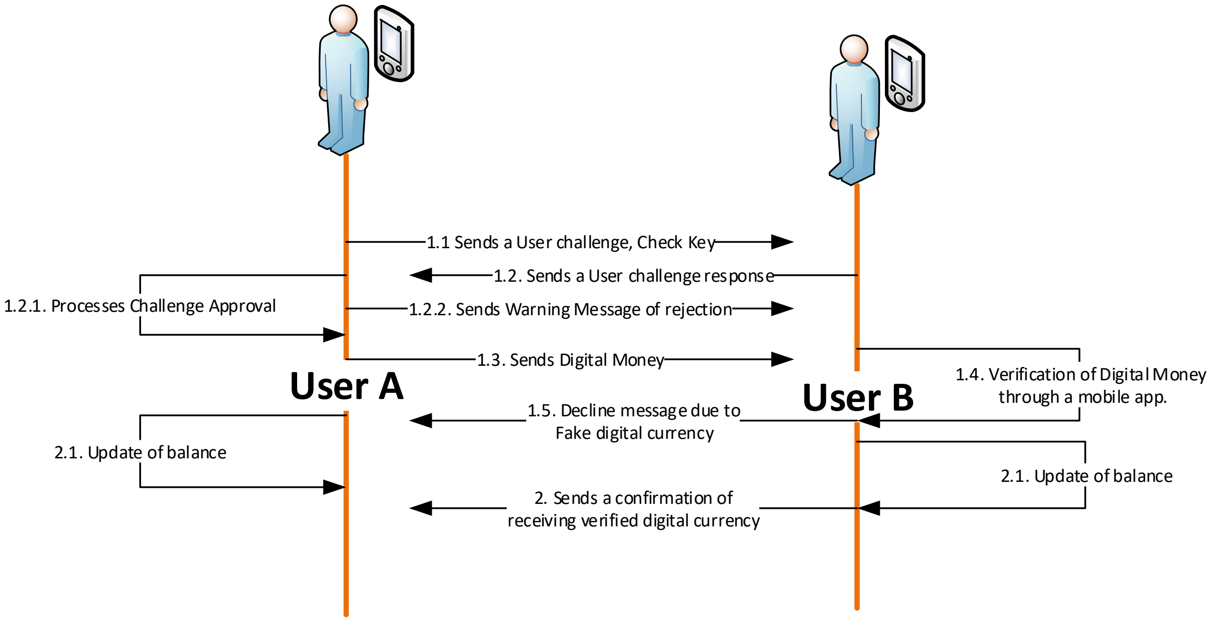
User A
User B
1.1 Sends a User challenge, Check Key
1.2. Sends a User challenge response
1.2.1. Processes Challenge Approval
1.2.2. Sends Warning Message of rejection
1.3. Sends Digital Money
1.4. Verification of Digital Money through a mobile app.
1.5. Decline message due to Fake digital currency
2.1. Update of balance
2.1. Update of balance
2. Sends a confirmation of receiving verified digital currency

Figure 4.5. Process of verification of digital currency transaction, in an offline base scenario.

These example types of activities can be as such as, protecting digital currency transactions and to have a facilitation of providing and digital identification. Figures 4.4 and 4.5 depict the process of a need of having threshold cryptography for the purpose of digital identity. Iterated in this thesis (in Chapters 3 and 4), in which this work proposes an idea of having a specific node a user identification procedure with threshold cryptography. The specific application of this technology will purely solve some issues into malicious actions, and will act as a first line of defence against basic false identity and resources utilisation.

Hence, this can be done through just purely technology of blockchain, There are some instances of blockchains being compromised and cybercrime activities can occur. To be mindful that all transactions and data within the blockchain can be made public. Figure 4.5 depicts the transaction exchange between two users where it shows an exchange of keys. The high important point in this thesis, this work had iteratedly stated the requirement of having digital keys, that can be used as a digital identification for nodes and users. If users that do not have such digital key generated for the purpose of facilitation of digital transactions, then users must not be able to imitate such transactions unless users have been enrolled through their nominated bank.

Figure 4.5 on point 1.1 demonstrated a user being challenged by the receiver of the digital currency if the person has a key (or the person has been enrolled). Being mindful that this specific process will be done on an offline scenario, all transactions will be a type of a pseudo validation status. All pseudo transactions will still be required to be uploaded through an online medium. In reference to User B in Figure 4.5, were the transaction activity ends and has managed to connect to an Internet connection, they will be able to complete the final validation of the pseudo validated transaction. For converting any pseudo validated transactions, is required either going to the bank, or having an encrypted communication medium to send all transactions to the bank servers. VANETs can also be used as another type of communication medium, to which they will be able to provide a connectivity medium between the remote user and their bank.

If in a scenario that the User A has encountered a rejection of the created challenge between two users conducting transactions. Main reasons are: (1) the failed challenging process of the specific user due to no digital identification, and another reason for transaction rejection can also be (2) such digital identification keys have been revoked. Such revocation of nodes is another procedural defence against

(1) the specific issues of misbehaving (or malicious) users and (or) nodes, and (2) nodes that have been suspected of being classified as misbehaving (or malicious). This specific concept is similar the management of digital certificates, were it can be revoked, assigned, produced, and be installed.

4.4. The use of VANETs as Mediums to Aid Transaction Synchronisation

The VANETs (Vehicular Autonomous Networks), have been used as alternative mediums of communications and transmission of data between source and destination. VANETs themselves as iterated on this thesis, have been a positive social contribution to bring connectivity to rural and remote areas, also in areas that have declared as disaster zones. These type of delay tolerant nodes (in the form of vehicles), have been a type of technology that have been able to emerge to bridge the gap of issues with the digital divide. In which the issue of digital divide, as iterated in this thesis that has been an issue that most rural and remote areas have been facing. VANET technology has not only been used as an alternative form of communication medium, but also it has been used to improve autonomous vehicular safety functions. Such safety aspects and functions must be considered, especially for vehicles that will route and carry data.

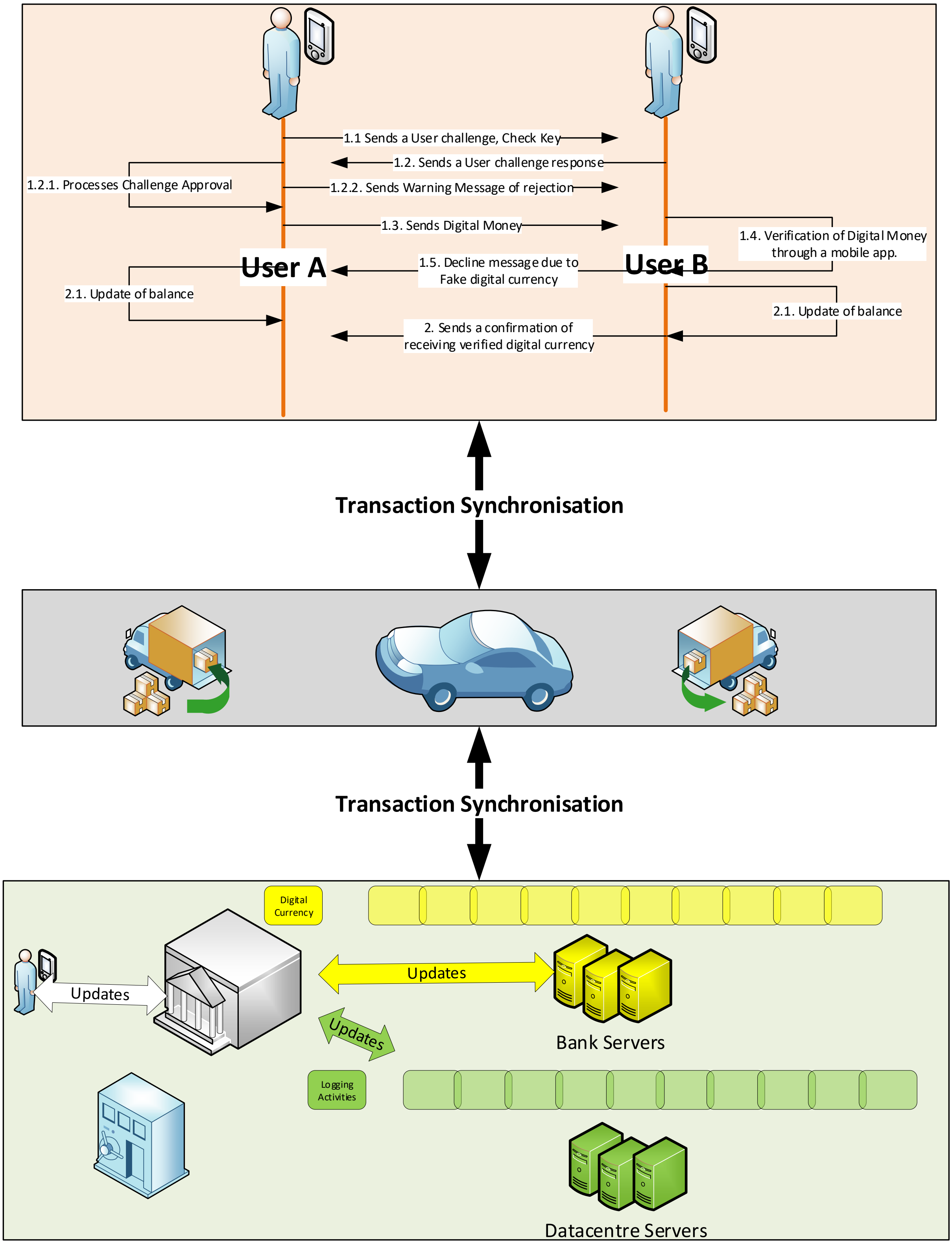
1.1 Sends a User challenge, Check Key
1.2. Sends a User challenge response
1.2.1. Processes Challenge Approval
1.2.2. Sends Warning Message of rejection
1.3. Sends Digital Money
1.4. Verification of Digital Money through a mobile app.
User A
1.5. Decline message due to Fake digital currency
User B
2.1. Update of balance
2.1. Update of balance
2. Sends a confirmation of receiving verified digital currency
Transaction Synchronisation
Transaction Synchronisation
Digital Currency
Updates
Updates
Updates
Bank Servers
Logging Activities
Datacentre Servers

Figure 4.6. Inclusion of VANETs for the purpose of being an additional medium to update transactions

In which VANET technology has been design, with the aim to ensure a safe drive and improving traffic flow and therefore significantly reducing accidents (Hasarouny, Samhat, Bassil, & Laouiti, 2017). In which the aspect of safety has been highly considered, as such as if the vehicles equipped with wireless sensors. If such aspects of safety cannot be guaranteed, it will cause a specific issue in the safety standpoint, and it will also have a negative impact on the technological contribution to the full aspect of delay tolerant infrastructures.

The diagram that has been demonstrated on Figure 4.6, shows the relationship of using VANETs being the source of medium between the two users that have done the digital transaction offline. The other side of the VANET medium, the bank and its servers where there is a good and solid Internet connection. VANETs in this type of scenario, will serve as the delivery communication medium between the users that have performed the offline exchange, and the bank and its servers that have some sort of Internet connection. The VANET nodes in this scenario will be equipped with automated wireless sensors, or to be able to connect to the VANET node by either a wired or wireless connection in a form of Personal Area Network (PAN). This specific idea in which digital banks could introduce of having an idea of mobile rural banking services, this which could solve the issues of managing demand of banking rural services.

Another point to consider is the cybersecurity aspect of these VANETs, in such scenario of using technological aspect of delay tolerant infrastructures. Nodes that are in a specific type of VANETs can cause packet transmission issues between the offline and disconnected users, and to its desired destination. These as such as will not be able to distinguish which nodes are selfish or be able to mask themselves as fake nodes. This thesis would like to argue is the need of VANETs to be able to take part into the node validation process, in which this specific validation process has been iterated on section 4.3. This will result into having all nodes that will participate, into the node verification processes, as a first defence to protect all participating nodes within the cluster.

Since some VANETs are based within the use of controller components, such as Electronic Control Units or ECUs for short and commonly known. These VANETs and Control Units, uses the concept of Controller Area Networks (CAN) as their primary source of communication methods. Hence this may not sound related to this research activity. But having such ECUs on some configured VANETs to be able and encounter issues when its component(s) are attacked by malicious attacks. Such attacks can be deadly, especially if that Vehicle is a public utility vehicle and configured with sensors to carry, store, and forward data. For example, if by chance an attacker manages to find out the data is stored in that specific VANET node, the specific attacker will try to attempt to control any components installed on the suspected node.

CAN nodes (VANET node), are mostly configured with storage memory such as FLASH (non-volatile) and/or RAM (volatile) for primarily storing data (Pan, et al., 2017). In which, authentication is not fully supported, so any event occurred was such attack of the CAN node (VANET node), there will be a probability a node will reset the RAM. Alternatively, the worst specific event that can occur, is when an attacker can program the node to erase and reset all contents both FLASH and RAM components. Such attacks that are common, for example (1) injection with hoaxed messages and (2) replay attacks. To which these specific common events, can stop the ability of the routing and transmission of data within the delay tolerant infrastructure nodes. The specific attacker not only attacks the vehicle and the driver and its passengers, it can also retrieve all data that are being transported and transmitted without prejudice.

There must be some sort of dynamic equivalence, into the application of trust models that this work is aiming of implementing and having a reliable data acquisition method. Implementing the purpose of, dynamic entity-centric based trust model that is based on the weight of the reliability of data according to any type of application (Yao, Zheng, Ning, & Li, 2017). Just like with other applications and security, this thesis has continued to iterate the importance of security measures to protect user data (of any kind) from malicious activities.

VANETs are an excellent alternative to extend Internet connectivity, and they can also be used with the routing data to aid its transmission. Another concept of vehicular networks that have been talked about are FANETs, or commonly known as Flying ad hoc networks, were every UAV can be set up as routers and consequently exchange data packets between each FANET node (Oubbati, et al., 2017). These FANET (a variation of VANETs) can be deployed anywhere flexible to any geographic location. This can aid to have the ability to extend network (Internet) connectivity, and to be able to bridge the gap of the digital exclusion issue.

4.5. Chapter Summary

The importance of utilising security mechanisms is paramount when implementing systems (which could be either on any hardware or software applications). Especially in decentralised networks, having no security mechanisms, it is easier for attackers to steal or grab data that should not be accessed. Since DTI is a decentralised networking concept, means that other traditional and centralised security mechanisms cannot be implemented into DTI. The result into having no security mechanisms, will also cause issues on any digital forensic work, meaning that the protection of custody and relative path of the specific data can be easily tampered. In section 4.2, where the discussion around the need of implementing of two sets of blockchains, one of each for storing cryptocurrencies and logging user activity. This for sure will enable the ability having forensic based approach to aid any digital investigations for the purpose of having a fail-proof and tamper-proof system.

In the event of a failure in the cryptocurrency blockchain system, and having the blockchain for logging user activities separately, the method of tracing back will be easier. Threshold Cryptographic technology implementation can also add security within the ad-hoc approach of device (or user) identity. On the other hand, user identification can also be done on blockchain systems, since most hardware involved in DTI are lightweight. Threshold cryptographic approach on DTI nodes is the correct approach, using blockchain technologies can still be used, but it may cause issues on the performance of DTI devices. Identification management on threshold cryptography can also be done in a much quicker approach when two nodes are trying to identify in a two-way handshake approach with less resources involved. This is a perfect solution not only for nodes within clusters, but for nodes that do travel from one place to another, such as VANETs as a good example. VANETs are nodes that mostly have low powered networking devices, based around configured controller units, and are mostly used to transport data. This type of nodes can also act selfish in a way that it will not transmit the data that needs to be delivered to its indented destination.

Threshold cryptography can also aid into creating policies into encryption protocols and node participation rules within a cluster. This technology can also be used control malicious nodes from being part of any clusters available. Ensuring that all transmissions between two nodes

Chapter 5 - Experiment and Results

This chapter demonstrates the experimental aspects of the threshold cryptography, which is a partial concept that has been stated in Chapter 4. The items have been involved for the purposes of this experiment as by using Raspberry Pi 3 (B+ Model) & Raspberry Pi 2 (B+ Model). The purpose of using Raspberry Pi is to have a device to be able to physically simulate in an Internet-of-Things hardware scenario, demonstrating cryptographic process on low powered devices. The reason of ensuring that low powered devices have been considered in this experiment, is to consider such scenarios and situations of limitation to budget, and resource flexibility of being able to not rely on centralistic approach for networking. This has reduced the overall cost of the experiment so as to meet the project budget. A system prototype has been designed to study the behaviours of threshold cryptography. By observing the developed prototype, we have found several points that can be beneficial as part of the future work. The developed prototype and its results which will be represented and complement to have been discussed in this chapter.

5.1. Technology Specifications and Diagram

The prototype has used the hardware of Raspberry Pi 3 and 2, in which its hardware specification can be found on Table 5.1. It has the ability to conduct the experiment and observe the utilization and resource performance on any performed task within the built prototype. The experimental tasks are including cryptographic processes, connecting between nodes, and high spikes in CPU usage.

5.1.1. Hardware Components

This section has provided a comparison table (Table 5.1), to firstly show the hardware specifications that both Raspberry Pi hardware components that have been used for this experiment. The differences between version 3 and version 2 are mostly the CPU, GPU and RAM hardware available, which is faster on version 3. Version 3 hardware also comes with Bluetooth and Wi-Fi (IEEE 802.11) on board. If the prototype has Wi-Fi and Bluetooth on version 2 hardware, it will be required to have USB external devices connected to the version 2 Raspberry Pi. Having at least two versions of the specified device, can be the best approach to discover that any device can participate as part of the threshold cryptography processes.

Table 5.1. Raspberry Pi 2&3 Specifications

	Raspberry Pi 2 Specifications	Raspberry Pi 3 Specifications
CPU (Processor)	Quad-core 900MHz quad-core ARM Cortex A7	Quad-core 1.4GHz Broadcom BCM2837B0 quad-core A53 (ARMv8) 64-bit
GPU (Graphics Processing Unit)	VideoCore IV chipsets (4th Gen) (clocked at 250MHz)	VideoCore IV chipsets (4th Gen) (clocked at 400MHz)
RAM (Memory)	1GB (450MHz) LPDDR2	1GB (900MHz) LPDDR2
Wi-Fi	N/A	2.4GHz/5GHz – 802.11b/g/n/ac
Ethernet	10/100Mbps	Ethernet over USB (max throughput 300PMbps), PoE (Power over Ethernet) Ready
Bluetooth	N/A	Version 4.2 BLE (Bluetooth Low Energy).
Storage	Using Micro-SD Card (32GB)	Using Micro-SD Card (32GB)

Within this developed prototype, the following diagrams in this section (Figures 5.1 and 5.2) demonstrate the creation of the prototype (or test bed) evaluation of how this specific encryption application will behave on low powered devices. The demonstrated diagrams will also include other technologies, such as wireless (using Bluetooth, and Wi-Fi), physical Routers and Switches which are common in centralised hierarchical networking. Reasons on having a wireless switch on the developed prototype, is because it is impossible to emulate the use of cellular data.

But with the wireless switch and a physical switch as part of the implementation of the prototype, this should still not defeat the purpose of the encryption key application of threshold cryptography. Unlike other encryption applications such as the RADIUS services, which needs a more sophisticated hardware and associated applications to enable a more secured, controlled, and stabled server. In addition to that, RADIUS services are far more hierarchical and centralised services approach into the overview of nodes. Please note that this specific experiment mostly focuses on the diagrams depicted on Figures 4.3 and 4.4, where the threshold cryptography has been used.

The clusters depicted on diagrams on Figures 5.1, 5.2, and 5.3, represents the banking system’s user and node approval process that has been deeply mentioned in Chapter 4. Even though blockchains can be used for managing the membership of nodes into the proposed digital currency services, with threshold cryptography, limiting and controlling the number of nodes that can participate within the key sharing generation exchange. In contrary with blockchains, there were all nodes (infinite number of nodes) participating within the computation and validation of data that goes through the whole network being constantly connected.

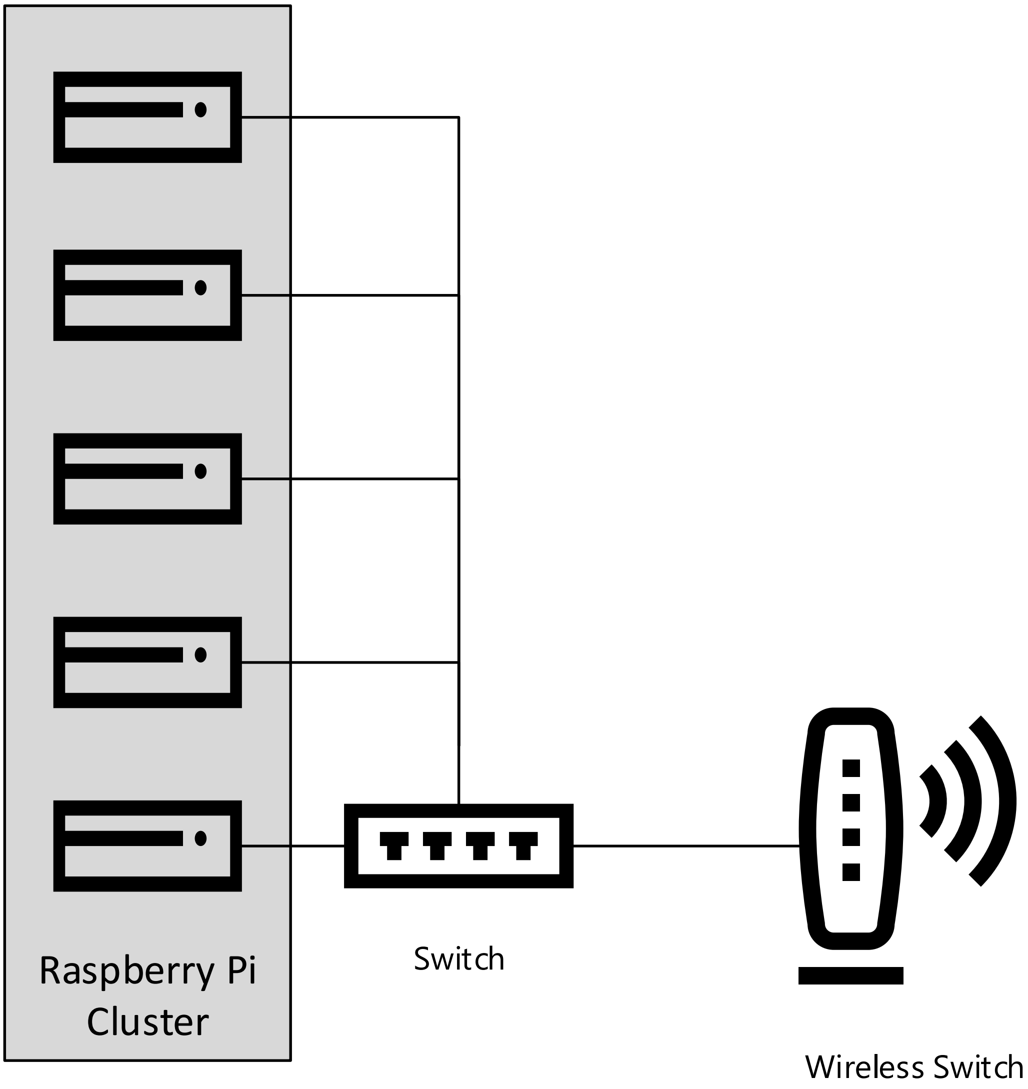

Figure 5.1. Raspberry Pi 2 cluster with a switch and a wireless switch.

The Figure 5.1 demonstrates the purpose of having a far more generic set up this prototype has initially been designed. Due to technical features of Raspberry Pi 2, they must be connected to a physical switch so that the nodes would be able to use the wireless services to connect with other nodes. Wi-Fi USB dongles can be considered if there is a need of changing the Raspberry Pi version hardware network connectivity via a wireless connection. The aspect of using wireless networks for node communications can still be configured as a primary alternative device for networking. The prototype did not have the cluster nodes connecting through Wi-Fi due to the fact of may impede the performance of the wireless switch due to connection overload.

That specific diagram on Figure 5.1 is what can be done on security intensive environments such as banks. For example, were there needs to be an awareness to secure digital currency and all different types of data, this means that in sensitive environments all data must be treated as confidential. Even though in this present day, there has been an improvement of connectivity and security mechanisms on wireless communications and components. In a real-world scenario, decision makers of computer systems will still depend on actual physical and wired node connections. This could be done by user awareness training or closing/switching off services and ports that are underutilised.

The configured cluster that are shown in both Figures 5.1, 5.2, and 5.3, will be the nodes that will be configured to be part of the process of the inclusion of threshold cryptography. In which these nodes will be using the security approach of poor man's Hardware Security Module (pmHSM). The pmHSM is a signed (distributed based) system, which Munoz, Montoto, Cifuentes, & Bustos-Jimenez (2017), have done their contribution and research activity. This was achieved into utilising the use of the API of PKCS11, in which their work have mentioned that it is easy to implement this interface. It is solely transparent between the applications and any associated systems. The reason of aquiring low powered and low cost hardware, was the sole approach of the developed prototype. To which it can deliver the same experience, rather than aquiring expensive hardwares.

The specific diagram shown on Figure 5.2, is what the aim of the prototype to have as a specific implementation or full concept to which a node (or external node) will be able to communicate with the physically connected cluster. Most of the hardwares that have been used for this experiment are mostly low graded equipment, which means light applications and security mechanisms can be applied easily. Decentralised applications and networks do not require the need of having high graded and specified hardware and software configuration, unlike hierarchical and centralised networks.

Discussing further into what has been demonstrated in Figure 5.2, the ability of creating an implementation plan and need for the digital key management approach. Figures 5.2 and 5.3 depicts the same aspect of the implementation of digital key assignment, based on the user for requesting to be part of the digital currency exchange (either offline or online). This will be able to depict on what this work has conceptually demonstrated in Figures 4.3 and 4.4. The stated diagrams (Figures 4.3 and 4.4), are to introduce the aspect of having threshold cryptography for approving and securing clients as a first base defence for malicious attacks. To prevent the illegal tampering of data during the computational generation of the shared key, Figure 5.2 depicted the cluster nodes connected through a physical switch. As previously iterated in this chapter, these cluster nodes will compute any shared tasks on banks that provide digital currency services.

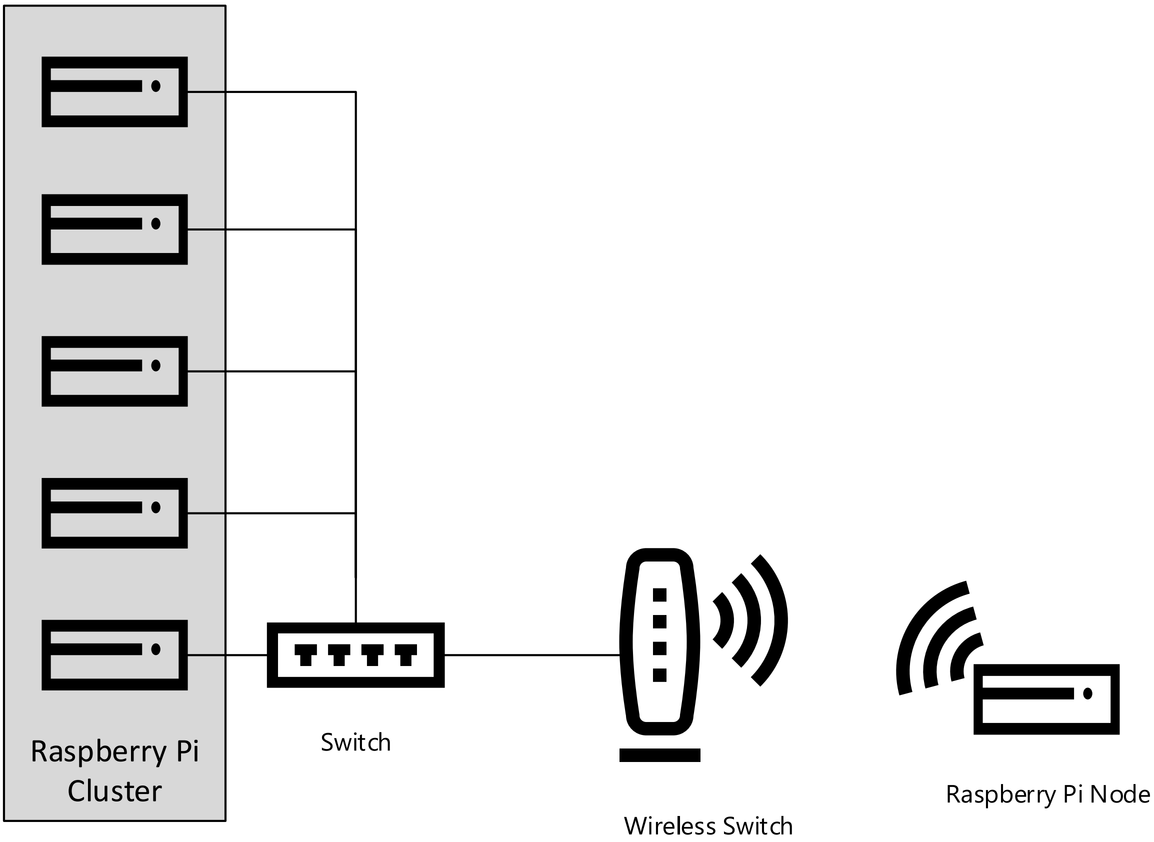

Figure 5.2. Raspberry Pi Cluster and external node interaction

The main differences between Figures 5.2 and 5.3, are the differences of data transmission and exchanges between the external node and the configured cluster by computing the shared secret key. Figure 5.2 depicts the use of IEEE 802.11 standard (Wi-Fi) for connecting to the cluster for encryption and decryption. With an alternative method, the Figure 5.3 depicts the use of Bluetooth technologies as a medium to transfer data between the cluster and the external node. In this prototype, planning to demonstrate such different options that this thesis would like to perform in this experiment in terms of providing of a cryptosystem aspect.

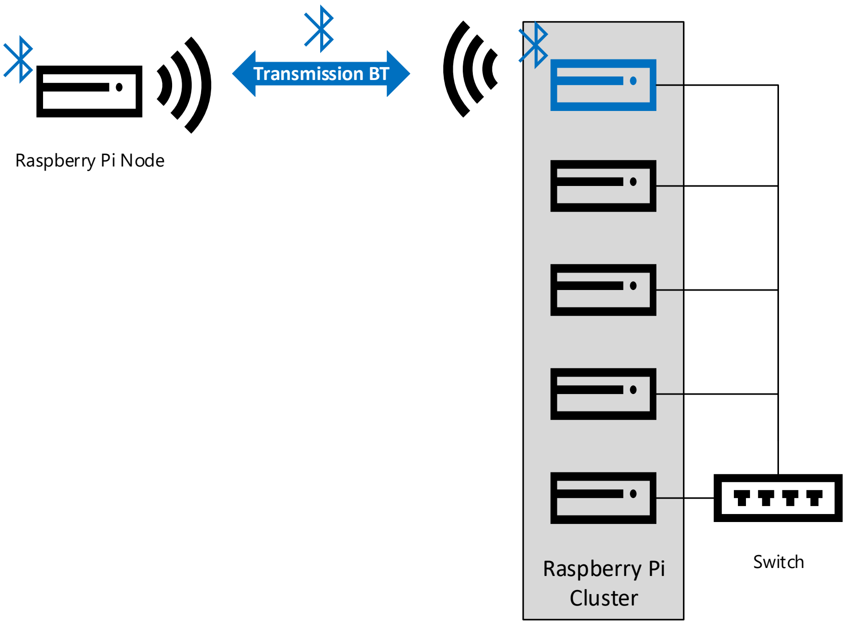

Figure 5.3. Bluetooth Transmission between external node and the Raspberry Pi Cluster

The differences between Figures 5.2 and 5.3, is the data medium either via Wi-Fi or Bluetooth between the cluster server and the client nodes. If users (or nodes) have been configured or made a manual or automatic decision, to adopt the method on Figure 5.3 (using Bluetooth), then a Raspberry Pi 3 node must be part of that cluster. That Raspberry Pi 3, having both Bluetooth and Wi-Fi embedded on board, must be configured in such a way that it is the gateway to receive all requests for a shared computed key encryption and decryption. The specific standard of Bluetooth can be implemented in these experiments such as having to follow the standard of IEEE 802.15.2 (Bluetooth with Wi-Fi).

Bluetooth medium standard that can be considered, is by following the standard of IEEE 802.15.6, were it is focused on the wireless BAN (Body Area Network) approach, for shorter distance communications. In general, Bluetooth communications can be the primary source of short-distance communication method for exchanging data between the source and destination. In this specific experimental scenario, considering the type of medium as the primary mode of data exchange between other nodes.

If a node has been configured to be part of the cluster for transmitting key management requests, the specific node will be configured in such a way that it will act as a middleman. The specific middleman node (to be configured), will be able to configure in such a way that in will act as a transparent node to pass requests between the nodes inside the cluster and the node(s) outside of the configured cluster. In a perfect world scenario, users of this specific digital currency in terms of registering for the specific service will be able to create.

Alternatively, if Figure 5.2 (using Wi-Fi) has been used as the main source of requesting a key, decrypting, and encrypting the key. Nodes that have preferred to this method, may need to enter in a shared key passcode of the wireless network to participate to communicate with the cluster. Alternatively, this will give the ability to such nodes to be able to update offline transactions depending on their geographical locations.

Hence, users (or nodes) that have preferred to use this specific communication medium, must ensure that physical security controls are implemented, to make sure that data can travel safely through the Wi-Fi medium. This specific method of a wireless medium can be established like Bluetooth medium communication methods. NFC (Near Field Communications) methods can also be considered as specific communication medium for transferring data between nodes.

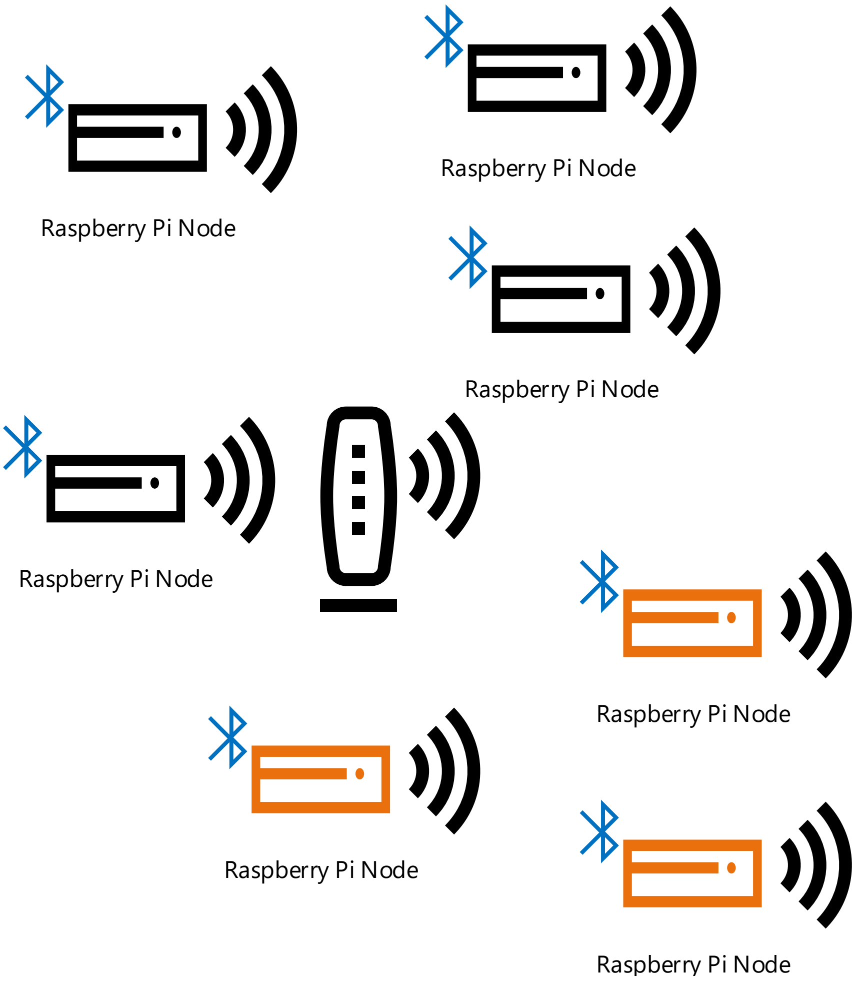

Figure 5.4. Wireless communication between threshold cryptography nodes and ad-hoc clients

In comparison to some of the stated mediums of either Bluetooth, NFC, or Wi-Fi, there is a possibility to create a specific dynamic cluster of nodes. As stated on Chapter 4, were all nodes will be required to have a digital identification or a digital key enabling communications and transactions between nodes. Figure 5.4 shows that these nodes can initiate communication within each other over Wi-Fi or Bluetooth connections, assumed that all the nodes in this diagram are using Raspberry Pi 3 hardware. Alternatively including some of the Raspberry Pi 2, acquiring the use of plugins such as a USB Wi-Fi stick and a Bluetooth module. In such scenario that Wi-Fi switch (or cellular mobile coverage) goes out, the Bluetooth can be utilised to transmit and exchange information.

All nodes that have been shown on the diagram in Figure 5.4, shows that all the nodes within the specific cluster will be able to communicate with each other using the Bluetooth and Wi-Fi. The orange nodes depicted on Figure 5.4, these nodes are configured to compute and generate a shared key to be used for the encryption and identification processes. As such, nodes that are on orange must be protected from malicious root attacks and be able to handle large numbers of requests. All data exchanges between the nodes on Figure 5.4, can only communicate with each other since the generated key is for the purpose of communication between nodes on the same cluster.

In this specific situation, the prototype is aiming to demonstrate in Figure 5.4, the need of having wireless networking to have a facility of such digital transmission of data between nodes. The nodes within the specific cluster depicted in the mentioned diagram, can exchange data which can be done via Wi-Fi networks. In the real scenario, it is expected that nodes will be able to have connectivity to the Internet via mobile cellular network. In this specific scenario as such that the prototype had depicted the use of a wireless network using Wi-Fi switch (or router), in which will be used to be depicted such as a dummy cellular network tower. The most important aspect that needed to demonstrate in this developed prototype, were there has a lot of transmission of data between the participating nodes.

5.1.2. Software Tools

Since most of the software tools in this experimental part of the research will need to be as light as possible. The prototype will mostly be using Open Source applications, that are available to use. There will be no such Closed Source applications that will be included, for the specific part of the experimental research. This specific prototype being created, were there may be a possibility for such mentioned software tools may not work as expected as planned.

Raspbian Stretch (2018 version) has been used as the primary Operating System, since it is one of the available operating systems available that can bare the hardware required for both raspberry pi versions 2 and 3. Using Python based programmable APIs, and available off-the-box encryption tools such as OpenPGP or GNUnet, these are the tools that are available for use through the operating system. These specific tools are either included on the installation of the operating system. These tools are also available to be downloaded online for both Open Source and Proprietary software tools and operating systems. Other tools will be used in consideration for this specific practical research to which will be able to satisfy the results, presented in this chapter.

5.2. Experiment Setup

5.2.1. Bluetooth Connectivity

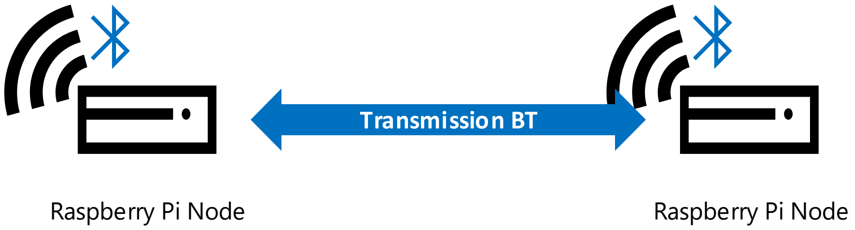

Figure 5.5. Exchange of data between nodes

The prototype had encountered some points of the software tools that have been used in this experiment. Firstly, as depicted on Figure 5.5, it is to establish communication between two Raspberry Pi 3 nodes over the Bluetooth connection. In which Bluetooth communications, in a real environment scenario in which this prototype will be able to use that specific medium to exchange data. At this point of the experiment, the diagram on Figure 5.5 did the exchange of data without the encryption methods that have mentioned in this thesis. This is done to ensure to monitor the behaviour of the Bluetooth medium feature that the Raspberry Pi 3 offers. Before this specific exchange occurs, running a command to install Python application for Bluetooth communications.

The command used for installation and enabling the service as stated below:

```
$ sudo apt-get install bluez python-bluez
```

The application installed called Bluez is the official Linux Bluetooth stack protocol service, which provides full support to a number of application and features, such as (1) complete implementation module, (2) safe multi-processing (symmetric), (3) data processing (multithread), (4) a wide range of supported devices, (5) hardware abstraction, and most important (6) device hardware and application security support.

After the installation and enabling the service for Bluetooth communications, the following sets of commands were running as a script:

```
$ import bluetooth
$ def receiveMessages ():
$ server_sock=bluetooth. BluetoothSocket( bluetooth.RFCOMM )
$
$ port = 1
$ server_sock.bind(("",port))
$ server_sock.listen(1)
$
$ client_sock,address = server_sock.accept()
$ print "Accepted connection from " + str(address)
$
$ data = client_sock.recv(1024)
$ print "received [%s]" % data
$
$ client_sock.close()
$ server_sock.close()
$
$ def sendMessageTo(targetBluetoothMacAddress):
$ port = 1
$ sock=bluetooth.BluetoothSocket( bluetooth.RFCOMM )
$ sock.connect((targetBluetoothMacAddress, port))
$ sock.send("hello!!")
$ sock.close()
$
$def lookUpNearbyBluetoothDevices ():
$ nearby_devices = bluetooth.discover_devices()
$ for bdaddr in nearby_devices:
$    print str (bluetooth.lookup_name( bdaddr )) + " [" + str(bdaddr) + "]"
$
$
$lookUpNearbyBluetoothDevices ()
```

Bluetooth is perfect to be used in this prototype for ad-hoc based models, which will be same as managing Bluetooth devices on smartphones. implementing an associative approach for device trust management, to mark certain connected devices to be as both added and trusted. Nodes can communicate with each other automatically, if the specific device has been marked as added or trusted devices. That specific information of added and trusted devices can be helpful where data can be routed, if the receiving device knows where to send the information to its desired destination node.

Bluetooth communications on the Raspberry Pi version 3, the developed prototype is based on Python which enables the use and possible automation of transmission of data between the nodes. In a defined scenario, Bluetooth communications can be used in an offline scenario where digital currency can be exchange without the need of Internet services. As such as users and nodes in a rural or remote area, will be able to set and currency exchange environment. Users will be able to make a withdrawal of any amount of their digital currency, in which they can be done using the wallet application installed on their mobile devices. All transactions will be stored and encrypted, the node will keep the transaction data available for automatic synchronisation once connecting to the Internet or a VANET passes by. Either of these methods, it will update transactions and activities blockchain through their bank. Were the node will be able to perform a validation check of transactions if they are legitimate or not.

5.2.2. Creating node cluster (TetraPi Server)

The specific diagrams on Figures 5.2 and 5.3, demonstrates the configuration of the distributed cluster. The prototype has been able to demonstrate this, but to configure at least four nodes to be able to act as one cluster. The created prototype based on a TetraPi distributed node server, that enabled all four nodes to share resources for threshold cryptography exchange.

In each of the nodes that will be used to be part of the cluster and external node. With the server node (or the client node), system preparation commands of all external node will be needed to be done, such as enabling the use of service resource. The system preparation processes are repeated to all four nodes, these are the only ones need a constant network connection. Let alone the client node which has the option to not connect or even be connected to a constantly live network system.

These specific service resources such as (1) dispy, (2) nmap, and (3) psutil, which are fully compatible with the used and available for Python 3. The table (referring to Table 5.2) describes the function of all three service resources required to use for creating the TetraPi. In which, making sure that these four service resources and applications are fully installed from using the terminal command below:

```
$ #installation of the distributed and parallel component (dispy)
$ python -m pip install dispy
$ #installation of nmap (Network Mapper)
$ sudo apt-get update #forces the update of available Debian libraries
$ sudo apt-get install nmap
$ #installation of psutil
$ sudo apt-get update
$ sudo apt-get install python3-pip

$ sudo pip-3.2 install psutil
```

If any of these three software tools and services, have been able to be established that these are installed on all the node that will be used as server clusters. Without the applications installed on supposed server nodes, some of the distributed and parallel processes and computations may not be able function properly.

For the nodes within the cluster to communicate, Secure Shell (or SSH) will be required to be enable a secured communication between nodes that have been configured. This will ensure that nodes will be able to exchange data, such as to be able to generate and compute key for the node and user that have requested to do so.

Table 5.2. Service Resources Description Table

Service Resources	**Description**
dispy	An API command module that is used for distribution of computation for all configured nodes. In which enables the use of other commands such as JobCLuster and SharedJobCluster to be able to distribute jobs and request. Perfect for the use of generating keys.
nmap	This command specifically used for port scanning of nodes within the network, or a specific node within the network.
psutil	Commonly called as process and system utilities tool which is a cross-platform based application for getting information of active processes, and system utilisation in Python. This is also a common application tool for Operating systems as such as Windows and Linux based systems.

The developed prototype on each node will have static IP addresses, in which the IP address assignment (based on IPv4) are depicted on Figure 5.6 (complementing Figures 5.2 and 5.3). The main reason of using static IP addressing, is the ability to identify nodes within the cluster system. Identification methods as such, if nodes are within the static range, knowing that these nodes are configured for network services and applications.

The DHCP range will aid the identification of client nodes connected on the network via wireless network. Ensuring that these specific nodes with static IP, can be connected to the network instantaneously in case of a network outage and due to DNS CNAME Records on the network. In

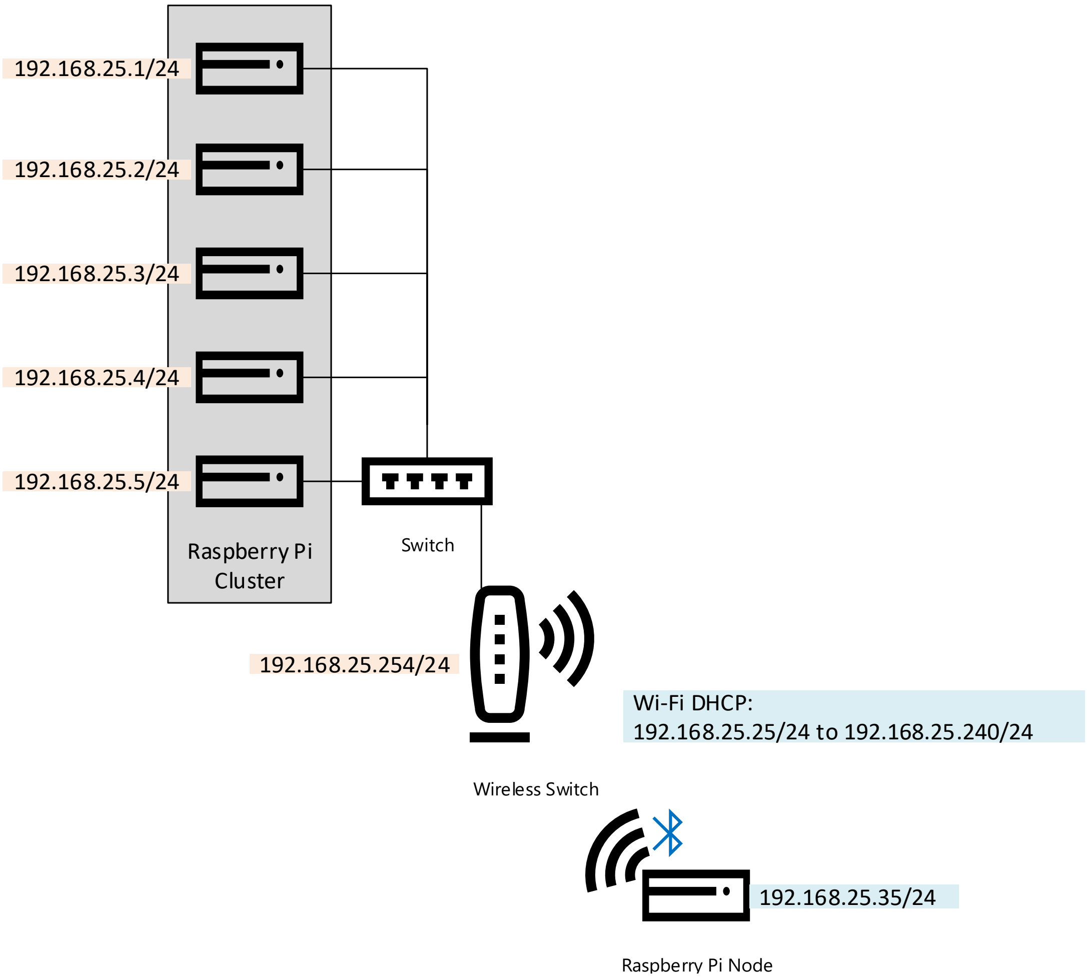

Figure 5.6. IP Address Assignment of nodes

terms of the DNS and DHCP configurations of this cluster, depending on the running of all these services from the Wireless Switch itself. Conducting such minimal node management activities within the Wireless Switch, such as (1) IP assignment management tasks, (2) creation of DNS records, and (3) device security management. Managing nodes that are by permitting and blocking node access to the network.

5.3. Explanation of Results (Chapter Summary)

The following three points of the developed prototype have been tested for observing the performance and system reactions,

1. Bluetooth connection and transmission.
2. Cluster resources.
3. Threshold Cryptography key generation, encryption, and decryption.

5.3.1. Bluetooth connection and transmission

Firstly, the Bluetooth connection and transmission exchanges between nodes, the prototype had encountered some minor performance issues. The approach and process used to test the transmission is by using a few files that to exchange data between the source and destination nodes. Such file sizes that have been considered in stress testing this developed prototype such as 10MB, 500MB, and 1GB file. The file node connection and transmission exchange has been done using Raspberry Pi version 3 hardware, were the type of Bluetooth component associated is a low powered. The reason to which have conducted the testing in this approach, is because to accommodate the theoretical domain of this research which includes blockchains (in terms of having digital currency, or cryptocurrency) and the exchange of keys. The prototype itself encountered some communication processes and exchanges, which may have either stalled or dropped. This in fact is a very common issue of other Bluetooth devices interfering on other established Bluetooth connections. Table 5.3 shows the results of the files being transmitted within the Bluetooth (Low Powered) medium.

Table 5.3: Bluetooth exchange results

	10MB	500MB	1GB
Time (minutes)	2mins	20min to 25min (max)	40min (max)

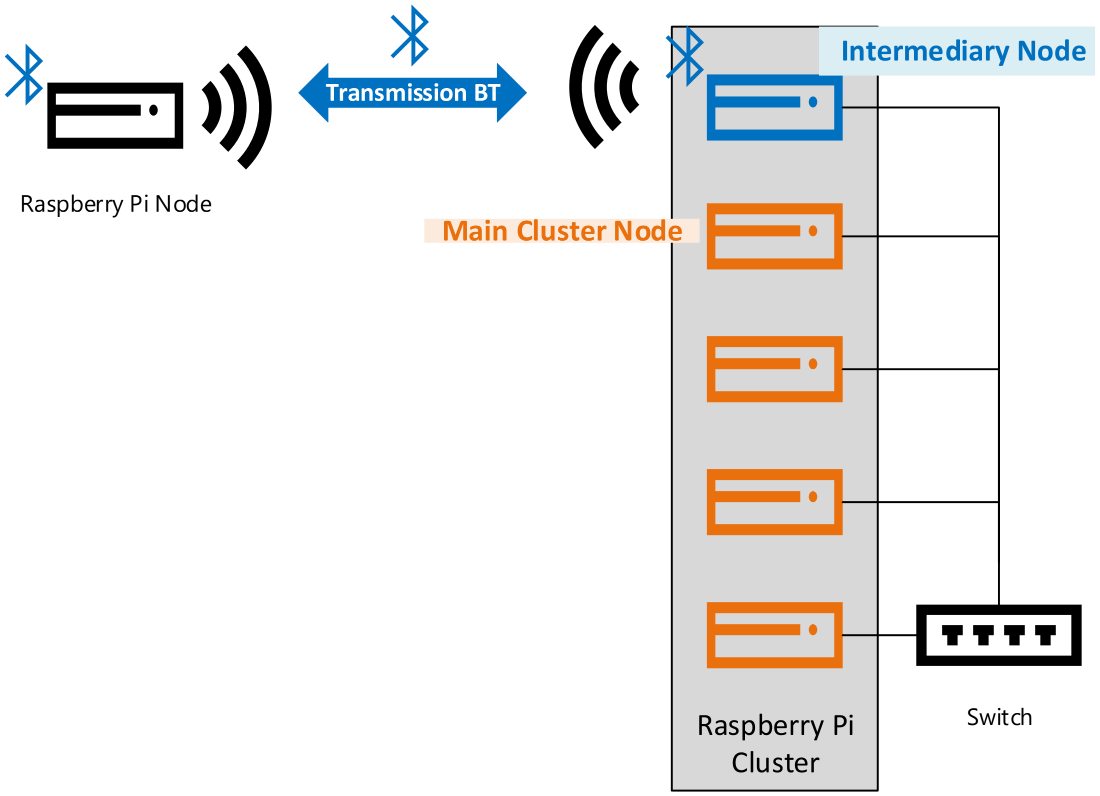

Figure 5.7. Using Bluetooth as intermediary node for cluster

The diagram on Figure 5.7, using the prototype between the client node and cluster to exchange data using Bluetooth. Configuring the intermediary node to be able to automatically move all data, to the main cluster node. The main cluster node's responsibility to ensure any such key request are distributed equally to all clusters so that distributed and parallel processes can commence immediately. After all the necessary processes that are needed to generate the key, this key is then passed back to the intermediary node so that the newly generated key can be generated to the node that have requested it. The generation key request processes are done depicted on Figures 4.3 and 4.4, were the developed prototype has demonstrated the purpose and detailed request process of key generation. In relation to the diagram on Figure 5.7., all the security challenges and request will be handled by the intermediary node.

What has been depicted on Figure 5.7, is by using Raspberry Pi version 3 as the intermediary node, and Raspberry Pi version 2 has been used for the setting up of the node cluster configuration. Due to the requirements for acquiring a key (as depicted on Figures 4.3 and 4.4), configuring the intermediary node to set some challenge questions such as a series of challenge questions to the client node in terms of hardware address (such as a, MAC Address), user information details (such as username use to access the client node). Sharing only minimal information details, to keep within full concept of pseudonym, to ensure the privacy of the intended user of the shared key.

The commands that have been mentioned below is the small script that has been used to move files from the intermediary node to the main cluster node.

```
$ scp *.* user@192.168.25.1:/home/clusterSystem
$ rm *.* #remove file
```

The used commands below are part of the small script that has been used to transmit files between the intermediary node and the resting node via the Bluetooth medium.

```
$ sudo hciconfig hci0 piscan #scanning of BT devices
$ hcitool scan
$ sudo l2ping -c 1 ab:00:67:89:11:34 #pinging BT device
$ sudo obexpushd -B -n #sends files
```

5.3.2. Cluster Resources

Since the prototype is only based on a TetraPi cluster approach, consisting of four Raspberry Pi version 3 hardware nodes. In this developed prototype, also created a similar cluster based on four Raspberry Pi version 2 hardware. The specific reason of comparing two sets of hardware, is the purpose of testing the specific utilisation impact of these resources. In terms of the behaviour, and how these two different sets of hardware types generate and compute a shared key (Threshold Cryptography). By having two combination sets of hardware (Raspberry Pi version 2 and Raspberry Pi version 3), a greater understanding of the hardware setup configuration maybe different between two versions of Raspberry Pi.

If all the cluster nodes are using the Raspberry Pi version 3 hardware, this will have more flexibility options in terms of the hardware implementation. The Wi-Fi medium can be used to as a medium for communicating with other nodes in the cluster. Alternatively, the developed prototype can utilise the feature of Power-over-Ethernet, in which means that the developed prototype will be required to have a physical switch to support Power-over-Ethernet. Having a physical switch, that can handle powering and switching data between nodes such as having an expensive Level 3 switch. This specific result of having two sets of hardware available for this prototype, sums up the total resources that are available in this parallel and distributed system. The summary and total available resources of Raspberry Pi version 2 can be found by referring to Table 5.4, and for Raspberry Pi version 3 can be found by referring to Table 5.5.

This prototype that have been able to expect some difference on system performance utilisation and capabilities. In this practical situation, expecting that there will be a change and differences in the specific resource utilisation behaviours. In this developed prototype, testing the application of Threshold Cryptography created an opportunity to gather experimental data in terms with common hardware utilisation. Such as the amount and size of data that it needs to encrypt or decrypt data, since the cluster nodes job is to perform such encryption processes. None of the encryption and decryption, will be performed on the client node side. Also, this includes how it manages the generation of shared key computation, were the calculation of the shared key will be distributed between nodes within the cluster.

Table 5.4 Summary of Resources on Raspberry Pi 2 Cluster

Raspberry Pi 2 Cluster (using four nodes)		Total Resources
CPU (Processor)	Quad-core 900MHz quad-core ARM Cortex A7	4 x 4 = 16 cores @ 900MHz
GPU (Graphics Processing Unit)	VideoCore IV chipsets (4th Gen) (clocked at 250MHz)	x4 GPU Chipset Units @ 250MHz
RAM (Memory)	1GB (450MHz) LPDDR2	4GB @ 450MHz
Wi-Fi	N/A	
Ethernet	10/100Mbps (RJ-45)	10/100Mbps x4 components
Bluetooth	N/A	
Storage	Using Micro-SD Card (32GB)	32GB x 4 = 128GB

Table 5.5. Summary of Resources on Raspberry Pi 3 Cluster

Raspberry Pi 3 Cluster (using four nodes)		Total Resources
CPU (Processor)	Quad-core 1.4GHz Broadcom BCM2837B0 quad-core A53 (ARMv8) 64-bit	4 x 4 = 16 cores @ 1.4GHz
GPU (Graphics Processing Unit)	VideoCore IV chipsets (4th Gen) (clocked at 400MHz)	x4 GPU Chipset Units @ 400MHz
RAM (Memory)	1GB (900MHz) LPDDR2	1GB x 4 = 4GB @ 900MHz
Wi-Fi	2.4GHz/5GHz – 802.11b/g/n/ac	x4 Wi-Fi modules
Ethernet	Ethernet over USB (max throughput 300Mbps), PoE (Power over Ethernet) Ready	x4 PoE enabled RJ-45 ports @ 300Mbps
Bluetooth	Version 4.2 BLE (Bluetooth Low Energy).	x4 BLE modules
Storage	Using Micro-SD Card (32GB)	32GB x 4 = 128GB

Table 5.6. Duration including Bluetooth Transmission with Encryption Process (Raspberry Pi 2)

Using cluster nodes based on Raspberry Pi 2 Cluster for encryption			
Duration of Process Time in minutes	10MB	500MB	1GB
BT Transmission	2.5 mins	27 mins (max)	40mins (max)
Encryption Process	2.5 min	5min (min)	30 min (max)
Total Process (BTT x 2) + Encrypt	= (2.5 x 2) + 2.5 = 7.5 mins	= (27 x 2) + 5 = 59 mins (max)	= (40 x 2) +30 =110 mins

Table 5.7. Duration including Bluetooth Transmission with Decryption Process (Raspberry Pi 2)

Using cluster nodes based on Raspberry Pi 2 Cluster for decryption			
Duration of Process Time in minutes	10MB	500MB	1GB (or more)
BT Transmission	2 mins	20 min to 25 mins (max)	40min (max)
Decryption Process	1 min	5mins (min)	30 mins (max)
Total Process (BTT x 2) + Decrypt	= (2 x 2) + 1 = 5 mins	= (25 x 2) + 5 = 55 mins	= (40 x 2) +30 =110 mins

Table 5.8. Duration including Bluetooth Transmission with Encryption Process (Raspberry Pi 3)

Using cluster nodes based on Raspberry Pi 3 Cluster for encryption			
Duration of Process Time in minutes	10MB	500MB	1GB
BT Transmission	2 mins	15 mins (max)	17 mins (max)
Encryption Process	1 min	2.5 mins (min)	10 min (max)
Total Process (BTT x 2) + Encrypt	= (2 x 2) + 1 = 5 mins	= (27 x 2) + 5 = 59 mins (max)	= (40 x 2) +30 =110 mins

Table 5.9. Duration including Bluetooth Transmission with Decryption Process (Raspberry Pi 3)

Using cluster nodes based on Raspberry Pi 3 Cluster for decryption			
Duration of Process Time in minutes	10MB	500MB	1GB (or more)
BT Transmission	2 mins	15 mins (max)	17 mins (max)
Decryption Process	1 min	5mins (min)	30 mins (max)
Total Process (BTT x 2) + Decrypt	= (2 x 2) + 1 = 5 mins	= (25 x 2) + 5 = 55 mins	= (40 x 2) +30 =110 mins

In reference between the results collated on Tables 5.6., 5.7., 5.8., and 5.9. These file sizes that were mentioned on Table 5.3. The values presented are mostly the averages of doing the process of decryption and encryption of the three types of file size. As such, the averages that show on the Tables 5.6., 5.7., 5.8., and 5.9, are based on the encryption and decryption processes that have occurred within the cluster, that have been repeated 4 times. In each of those four files, ensured that the four files that included to produce a meaningful average, are different file type associations (either a PowerPoint, email, video, or software installer file). Since several files regardless with the amount of noted attributes on any given file types, the number of associated file attributes within the file type, may create the probability of a longer encryption and decryption process. Hence, that specific information will be needed to be part of the encryption and decryption process.

In each of the Tables (referring to Tables 5.6., 5.7., 5.8., and 5.9) monitoring the total length of the process using a timer. For example, the developed prototype processed through by decrypting a 10MB file with the use of a Raspberry Pi 3 took five minutes in average. This type of systems development in the future, similar to what had been done, a lot more can still be added and as iterated in this thesis, that this is only a prototype. This will be needed to further understand the behaviour of encryption and encryption processes with low powered devices and components. This prototype also had events, that have shorter processing times for encryption processes, regardless of the file sizes.

In comparison between the two sets of mentioned hardware in this section of Chapter 5, the conducted experiment shows that the use of Raspberry Pi version 3 hardware will be the most efficient option. With Raspberry Pi version 3, the ability to build a cluster node with fast processing time for encryption and decryption. This prototype work also had an observation of the nature on how the processor (CPU Cores) has behaved through all the conducted tests. It is obvious that Raspberry Pi version 3's CPU cores are able to perform faster, processing the data feed through to all cores. Raspberry Pi version 3

CPU Cores (referring to Table 5.9), runs at 1.4GHz maximum, in comparison to Raspberry Pi version 2 which runs at 900MHz.

One point this experimental work has uncovered, is the CPU utilisation between the hardware versions, complementing the installed Operating System that the encryption processes for Raspberry Pi version 2 hardware only stays around 80% used. Alternatively, in Raspberry Pi version 3, CPU utilisation is somewhat between 77.5% and 85%, which totally varies due to the CPU processing speeds, that each of the four CPU cores can reach up to 1.4GHz. This prototype can also put into argument that the CPU utilisation can be high, is due to the way that some of these CPU hardware items have been developed. This prototype work can also conclude that the CPU utilisation and resources, can be at somewhat more or less same between the two versions of hardware used in this developed testbed.

RAM (Memory) utilisation behaviour can also be the catalyst for having a correlation result of some hardware performance results. In generic computing knowledge, expected that there will be some instances that processes can be passed on the memory and especially on the GPU components. For instance, based on the data collected during to one of the encryption processes that there was a memory utilisation of 70% (using a 500mb file) on Raspberry Pi version 2 hardware. The memory utilisation behaviour is somewhat likely similar on using Raspberry Pi version 3 hardware, even though there are some variances between the transactional speed of the memory hardware. Observing the developed prototype based on the hardware utilisation for encryption and decryption processes, most of the time, This experimental work have been able to see the memory utilisation level at times have reached its peak, due to the fact from all of the requests of shared keys, and encryption and decryption processes.

In summary, this prototype work has created a new area of discussion, in terms the importance of low-powered hardware utilisation. Highlighting the importance for decentralised and distributed applications. The hardware components, that this created prototype will enable us to understand the statements that have been proposed in this thesis. Low-powered devices in this present time, have been used in other scenarios such as testing and data collection, and for general purpose such as replacing personal computers. This section of the thesis will be able to make us understand deeply, on how to improve the implementation of hardware, and to make sure that services based on low-powered hardware components. Data that had been mentioned on this section of the thesis, will be able to aid us into decision making.

5.3.3. Threshold Cryptography (using the OpenPGP standard tool)

OpenPGP was being used for the purpose of this demonstration. In fact, this developed prototype will be using GnuPG version 2 (gpg2) to which, follows that full stack standard what has been defined on OpenPGP encryption mechanism protocol. GnuPG offers the feature in order this developed prototype in terms of using of asymmetric encryption of using key pairs such as public and private key pairs.

This experimental work used the following command (calling the command on terminal, gpg) supplied below to check if the specific application version. the need to installation of gpg tool into the four server nodes. After installation process completes, checking the version of gpg installed on all four nodes that will be part of the specific configured nodes.

```
$ brew install gpg #installation of gpg tool
$ gpg –version #grabbing gpg version, with the version details below
gpg (GnuPG) 2.2.3
libgcrypt 1.8.1
Copyright (C) 2017 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

The specific command above of `gpg –version` was executed on all Raspberry pi nodes involved regardless of their role and configuration. There is another version of gpg, called gpg2, but since the encryption protocol will be done on the server nodes, and including some of the embedded systems. The command class of gpg2 (gpg version 2) can be used for desktop encryption processes and using some of the switches may require installation of addons.

5.3.4. Theoretical Alternative Experiment Setup and Conclusion

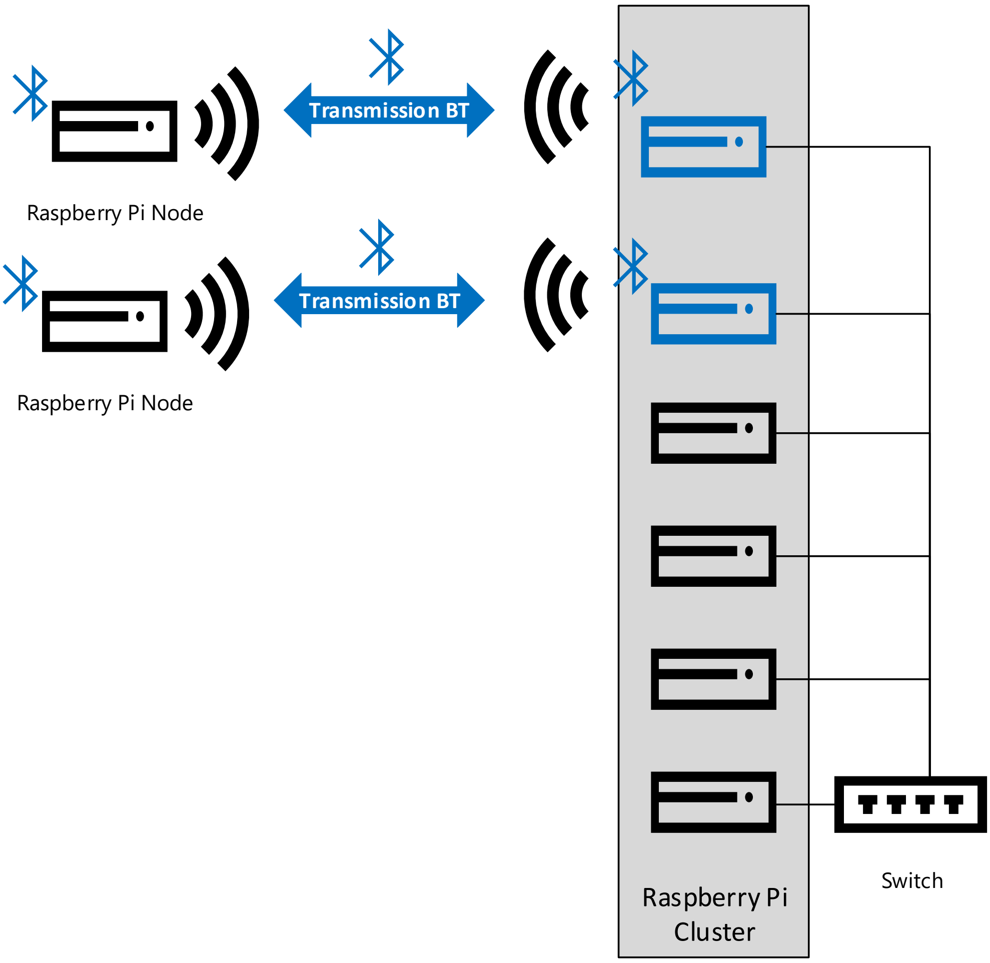

Figure 5.8. The alternative solution of using Bluetooth communications

To conclude this practical experimental part of this research activity, this work had discovered a few very interesting points of discussion. Such discussion points about future work with the knowledge domain of this specific research with Delayed Tolerant Infrastructures, Blockchains, and Threshold

Cryptography. This work discovered that incorporating both technologies, can create a beneficial use of decentralised and distributed networks and applications. Also, this can aid the use of having such future development of decentralised and distributed software tools and hardware applications.

In a real-world scenario, that this type of development work depicted on Figure 5.7, which includes the use of an intermediary node for sole Bluetooth communications. Bluetooth communications nowadays can be used to connect and share Internet connection in an ad-hoc approach Hence, if that specific idea has been literary decided for production environments, it will be slow to process due to Bluetooth technology is not a one to many (broadcast) communication when two Bluetooth devices are connected. This means that the specific more than two intermediary nodes, will be needed to faster the speed of handling key share requests, encryption and decryption.

In reference to the depicted diagram on Figure 5.8, the developed prototype theoretically demonstrated the use of more than one intermediary node. The intermediary node must be able to handle Bluetooth communications between the cluster and the node. Just imagine, like entering a bank and going to the service counter for depositing, seeking account enquiries, and requesting for loans. If there is only one counter to serve all customers, this will cause a service delivery issue, expecting the result of having long and a service that is not at a satisfactory level.

Having a conceptual plan like the developed prototype, were the social demand for more decentralised applications and networks. Specific applications will be able to be developed, where a thriving need of having applications that are intelligently configured to find its way in terms of data exchanges. That can be used for environments such as any event that will be needing anyone’s personal and private information, for registering services, controlling of sensitive and process-centric and process intensive tasks and applications. Providing a database of information that can be distributed and stored in a decentralised manner, avoiding the issues of replication methods that most of the time fails. In which these specific decentralised applications, can solve the issues of data being store centrally, that introduces a single point of failure for managing data.

Referring to what has been depicted on Figure 5.9, imagining in a real-world scenario that has mostly decentralised networks and applications. Imagining a world, such decentralisation and distribute technologies, will be able to solve issues that have occurred within centralised and hierarchical applications and networks. These have caused a sense of distrust and belief, due to how they are able to be accessed and unauthorised usage of mostly personal and private information. Hence, developing training and awareness programmes on how to teach users to act and stay alert against cyber activity. The concept of decentralisation can be a good approach and start to be able to protect user personal and private information. Continuing referencing to what has been depicted on Figure 5.9, the ability to create and imagine a world, being decentralised.

The process of data will be smooth and can be routed around between nodes and their clients. So, if depicting the concept to which the two are mostly banks, which offering digital currency to its users (who have enrolled for the service). If a node received a digital money from a different bank, then the cluster of nodes shall forward it to a different other cluster of either encryption or decryption. Once done, the information then will be sent back to source requested node, then in turn, sends the processed data to the source node. Yet again, to fulfil to what has been depicted on Figure 4.2 and Figure 4.3, were to ensure all the transactions and user activities will be logged using blockchain platform

As iterate in this research activity, and especially on this chapter, more work in terms of research will needed to be conducted. Especially on relationship between Blockchain and Threshold Cryptography technologies. Being able to take chances and be able to build and develop a distributed, parallel, and decentralised applications and security mechanisms. In that chance it can be developed into catering different needs and be able to contribute a positive social impact and drive.

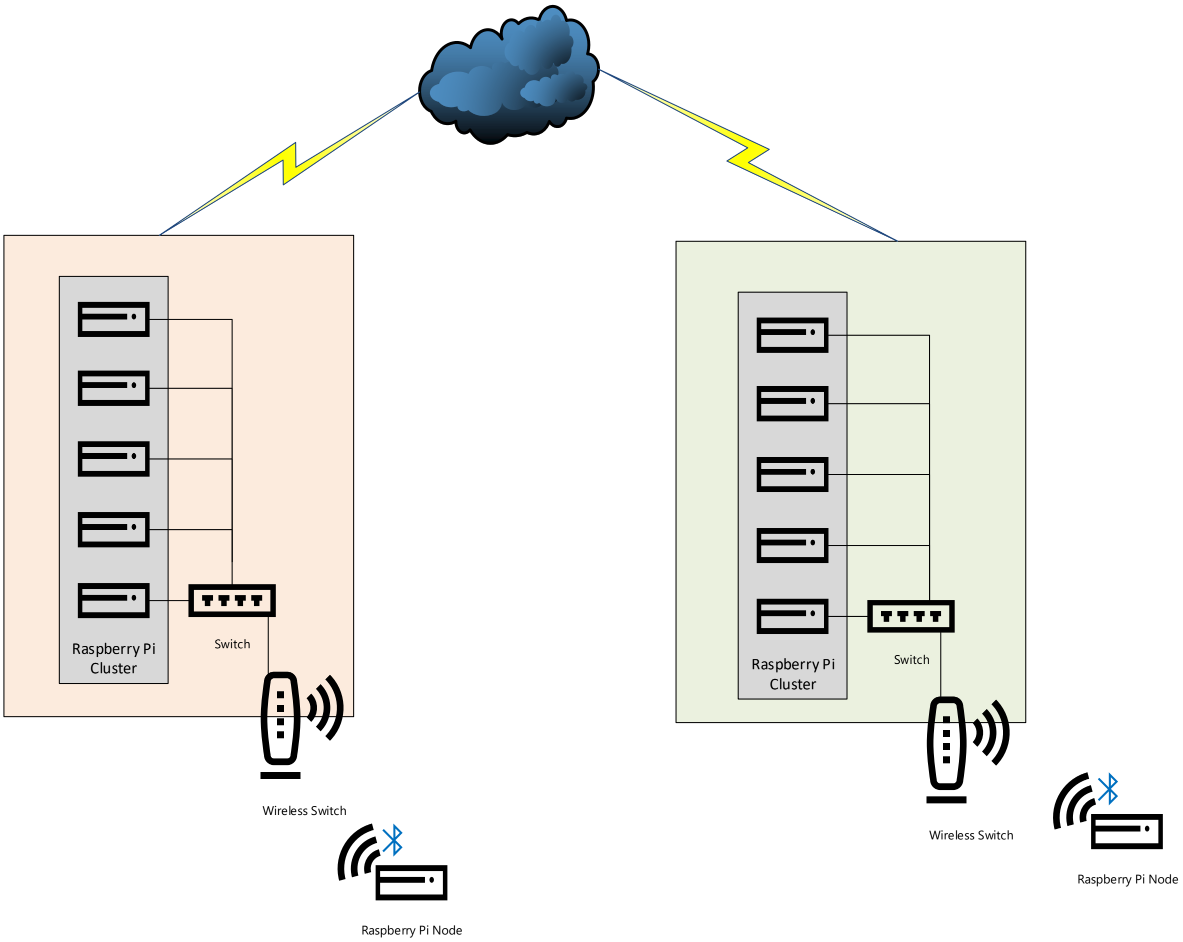

Figure 5.9. Communication between clusters nodes

Chapter 6 – Conclusion

This work did both practically and theoretically established the utilisation of blockchains both in digital economy (digital currency) and the use of for logging of user transactions and other activities. Stating the fact that blockchains are not mostly for cryptocurrencies, but the blockchain technology can be utilised with any medium to highly intensive processes and workflows. This particular platform can also be used all kinds of industrial work types and activities, to provide a high availability, fault-tolerant, highly distributed database collection. The process of data verification can be done, with an unlimited number of nodes connected through the blockchain network. Reducing (or eliminating) the issues of single point of failure incidents, were it can be an issue mostly with centralised and hierarchical database structures.

Nodes that do participate within the creation of blocks, within any of the blockchain system, will be able to part on the process of following validation rules and computation of new blocks. This work has discovered the use of opportunistic network methods, such as delayed tolerant infrastructures, were it has commonly known for its purpose to bridge the digital divide. These approaches and methods of utilisation of delayed tolerant infrastructures, having to discover that delay tolerant infrastructures can aid to bridge that digital gap.

6.1. Conclusion Summary

DTI methods of using mobile and vehicular nodes, in which mobile and vehicular nodes can be configured in a way data routing and bi-directional transmission of data. Implementation of security mechanisms have been extensively discussed in this thesis. Considering the use threshold cryptography, as a method of key assignment and revocation management for ad-hoc nodes. This is due to the specific number of digital data related incidents that could possibly occurred with ad-hoc and opportunistic networks. These specific digital data related incidents, as such as greedy nodes that will not aid into the transmission and routing of data to its intended destination. As mentioned on Chapter 5 of thesis, were this work had developed a prototype involving threshold cryptography on low powered devices. As acquiring the use of two versions of Raspberry Pi devices (versions 2 and 3). This chapter (Chapter 5) referring to the prototype concerned, this work has uncovered the truth and some unhidden processes on how applying generic cryptographic applications and tools. This includes proprietary and Open Source based Internet of Things application tools, operating systems, and hardware, such these tools are widely available in today's Internet.

In which blockchains have been sued a solution for the application of securing and protecting the data ownership, transparency, and being able to be audited. Such as any sensitive and personal data, that anyone must not trust certain third-party systems and nodes that can expose data to a range of malicious attacks and misuse (Zyskind, Nathan, & Pentland, 2015). As iterated on this thesis, the use of a third party can be eliminated since all verification and consensus of inputted data, can be done by infinite number of participated nodes. Stated the fact, that blockchain technologies can also be used for forensic purposes, to protect the integrity of court cases an investigation. Which is mostly important, especially the use of this technology (blockchains), on investigating decentralised and distributed nodes within opportunistic infrastructures, Internet-of-Things, and participating nodes within the blockchain network.

This work has discovered the ability of acquiring some decentralise services and application, which can cooperate to provide security mechanisms. In relation to the created prototype, acquiring expensive hardware can be considered as optional in nature due when it has been developed. Ad-hoc and fault tolerant application do not require such sophisticated software or even hardware depending on the scenario that will be developed in the future. In today's environment, some of these sophisticated software and hardware resources, do require constant network connectivity and mostly hierarchically dependent, on other services and application tools. These application tools where the developed prototype can apply security mechanisms, on ad-hoc, opportunistic, and fault tolerant based networks.

6.2. Future Work

The developed prototype as mentioned on Chapter 5, still have some points within the implementation process for improvement. Most stated application tools in this thesis are open-sourced, to which all based on Linux systems. Some of these mentioned application tools have been used, aided to what had been done on the developed prototype. As a result, Chapter 5 brought a lot of challenges and more overview of the aspects of having a decentralised network of nodes. The concept of decentralisation of cluster nodes, has been a popular trend for some time, due to the trust issues that centralised networking methods have created. The outcome of the experiment did consider several points of future work and improvements, in terms with the further development and inclusion of blockchains and threshold cryptography. These two technologies (blockchains and threshold cryptography) provides a feature of decentralisation, which complements the social need of decentralised controls and management of data. Blockchains have not been part of Chapter 5, due to the time constraints faced at the time when the experiment work was conducted.

In the past, there have been more research activities conducted, since the inception and popularity of blockchains. These research activities are more towards the improvement of cryptocurrency systems. But in this present time, there are more research activities that have been conducted based on the implementation of blockchains for securing network devices and mediums. Blockchains will introduce the concept of rules-based approach to data management, democratisation, distribution, and data decentralisation. Such as the variant of Delay Tolerant Networks of Wireless Sensor Networks, they will be configured to operate as self-regulated networks of static and transient devices behaving as autonomous colonies (Carbajo & Mc Goldrick, 2017).

The following points below are some of the points that this work to mention in terms of the future work of this research as follows below:

1. Blockchain technology for data security.
2. Cross compatibility of hardware for cluster nodes for threshold cryptography.
3. Revocation of poisoned threshold cryptography server nodes.

Utilising blockchains for both security and protection of data, but the specific issue that may occur infinite number of nodes can be network participants. This specific aspect can be investigated as a special future work, were there is a designed mechanism to control and vetting of users and nodes to be able to participate. One of the specific research arguments that this work would like to raise in this thesis. Blockchain and Threshold Cryptographic implementation and utilising these two technologies with a mechanism control processes base on the number of nodes being able to participate.

This could lead us into being out of the specific general domain that this research has set itself to be. A good example of Device-to-Device is cellular communications, Atat, et al. (2017), had focused their work on around the argument of set challenges of enabling Cyber-Physcial communications. In which this work is closely related to the matter of having secure channels for communcations and exchanging data. The proposal points that have been discussed in this document did go to the direction of securing communication channels using threshold cryptography and blockchains. Believing that more work needs to be discovered around this area. most likely the future and future development of this research more into introducing a tool that will control node participation of creating blocks. Hence, the decentralised and distributed in nature of this technology, that facilitates any node without security checks can cause the integral aspect of blockchain platform implementation. If this issue has been raised by different researchers and technology-based enterprises, applying different methods into application of user and node access controls into a blockchain.

Cross compatibility of hardware for cluster nodes for threshold cryptography, is one of the identified common points. To which the direction of this thesis topic, by planning into incorporating this aspect into the research, but due to the time constraints this has been neglected and put as a future work. Being able to have a flexible hardware requirement for nodes to be used for threshold cryptography. Such requirements based on the computation of secret keys, decryption, and encryption can be done using different number of nodes from different types of hardware configurations with no limitations.

Since this thesis stressed the importance and positive use of threshold cryptography, there has been a bit less research in general on revoking server nodes. The concept of server nodes is a term used for nodes the does most of the generation and calculation of shared keys for client nodes in a distributed and decentralised approach. This means that the importance the need of revocation in the sever level on Threshold Cryptography. Revoking server nodes which have been poisoned and infected by other malicious nodes, will mean the need of re-keying of previously computed keys. As such after the revocation of a server node, is to ensure that there is still more than one server node available to compute a shared key. Considering that processing of data no matter regardless of any format is very critical, heavily depending on the use of data, more importantly the aspect of decision making. Data being broken down into workflows, so that they can be easily distributed among data storages (Atat, et al., 2017). Having a strong and resilient cyber-physical system is essential for the purpose of ensuring that mostly on Device-To-Device communications. In respect to Delay-Tolerant Infrastructures and reflecting on the prototype Chapter 5, were this thesis was focused on the aspect of Device-to-Device communications.

References

Ahmad, A., Doss, R., Alajeely, M., Rubeaai, S. F., & Ahmad, D. (2018). Packet integrity defence mechanism in OppNets. *Computers & Security, 74*, 71-93. doi:10.1016/j.cose.2018.01.007

Ahmad, N., Cruickshank, H., Cao, Y., Khan, F., Asif, M., Ahmad, A., & Jeon, G. (2019). Privacy by Architecture Pseudonym Framework for Delay Tolerant Network. *Future Generation Computer Systems*, 979-992. doi:10.1016/j.future.2017.11.017

Alajeely, M., Doss, R., & Ahmad, M.-H. V. (2017). Defense against packet collusion attacks in opportunistic networks. *Computers & Security, 65*, 269-282. doi:10.1016/j.cose.2016.12.001

Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2018, September). Cyber-physical systems and their security issues. *Computers in Industry, 100*, 212-223. doi:doi.org/10.1016/j.compind.2018.04.017

Atat, R., Liu, L., Chen, H., Wu, J., Li, H., & Yi, Y. (2017). Enabling cyber-physical communication in 5G cellular networks: challenges, spatial spectrum sensing, and cyber-security. *IET Cyber-Physical Systems: Theory & Applications, 2*, 49-54.

Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2018). Blockchain with Internet of Things: Benefits, Challenges, And Future Directions. *I.J. Intelligent Systems and Applications*, 40-48. doi:10.5815/ijisa.2018.06.05

Avramidis, A., Kotzanikolaou, P., Douligeris, C., & Burmester, M. (2012). Chord-PKI: A distributed trust infrastructure based on P2P networks. *Computer Networks*, 378-398. doi:10.1016/j.comnet.2011.09.015

Banerjee, M., Lee, J., & Choo, K.-K. R. (2018). A blockchain future for internet of things security: a position paper. *Digital Communications and Networks*, 149-160. doi:10.1016/j.dcan.2017.10.006

Botta, A., de Donato, W., Persico, V., & Pescapé, A. (2014). On the Integration of Cloud Computing and Internet of Things. *2014 International Conference on Future Internet of Things and Cloud* (pp. 23-30). Barcelona, Spain: IEEE. doi:10.1109/FiCloud.2014.14

Bowen, R., & Morris, W. (2019, December). The digital divide: Implications for agribusiness and entrepreneurship. Lessons from Wales. *Journal of Rural Studies, 72*, 75-84. doi:10.1016/j.jrurstud.2019.10.031

Bucur, D., & Iacca, G. (2017). Improved search methods for asessing Delay-Tolerant Networks vulnerability to colluding storng heterogeneous attacks. *Expert Systems with Applications, 80*, 311-322. doi:10.1016/j.eswa.2017.03.035

C, S. C., CT, L., & K, D. C. (2018). An Efficient method for Secure Routing in Delay Tolerant Networks. *8th International Conference on Advances in Computing and Communication (ICACC-2018)* (pp. 820-826). Kochi, India: ScienceDirect. doi:10.1016/j.procs.2018.10.384

Carbajo, R. S., & Mc Goldrick, C. (2017). Decentralised Peer-to-Peer data dissemination in Wireless Sensor Networks. *Pervasive and Mobile Computing*, 242-266. doi:10.1016/j.pmcj.2017.07.006

Chen, Y., Liu, Z., Liu, J., Taylor, W., & Moore, J. H. (2015). Delay-tolerant networks and network coding: Comparative studies on simulated and real-device experiments. *83*, 249-362. doi:10.1016/j.comnet.2015.04.002

Chisanga, E., & Ngassam, E. K. (2017). Towards a conceptual framework for information security digital divide. *2017 IST-Africa Week Conference (IST-Africa)* (pp. 1-8). Windhoek, Namibia: IEEE. doi:10.23919/ISTAFRICA.2017.8102398

Cho, J.-H., Chen, I.-R., & Chan, K. (2016). Trust threshold based public key management in mobile ad hoc networks. *Ad Hoc Networks*, 58-75. doi:10.1016/j.adhoc.2016.02.014

Cho, J.-H., Swami, A., & Chen, I.-R. (2010). A Survey on Trust Management for Mobile Ad Hoc Networks. *IEEE Communications Surveys & Tutorials*, 562-583. doi:10.1109/SURV.2011.092110.00088

Djamaludin, C., Foo, E., Camptepe, S., & Corke, P. (2016). Revocation and update of trust in autonomous delay tolerant networks. *Computers & Security*, 15-36. doi:10.1016/j.cose.2016.03.008

Dutt, I. (2015, June). Issues in Delay Tolerant Newtorks: A comparative study. *International Journal of Advanced Research in Computer Science and Software Engineering, 5*(6), 534-542. Retrieved from http://ijarcsse.com/Before_August_2017/docs/papers/Volume_5/6_June2015/V5I6-0311.pdf

Easterbrook, S., Singer, J., Storey, M.-A., & Damian, D. (2008). Chapter 11, Selecting Empirical Methods for Software Engineering Research. In F. S. al., *Guide to Advance Empirical Software Engineering* (pp. 285-311). Springer. Retrieved from http://maveric0.uwaterloo.ca/~migod/846/papers/easterbrookChapter.pdf

Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K.-K. R. (2018, January/Feburary). Blockchain : A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Could Computing*, pp. 32-37. Retrieved from https://pdfs.semanticscholar.org/7f8f/4ff1377ebf0a084c44dbf6926af03dd2cdd8.pdf

Fraire, J. A., Madoery, P. G., Charif, A., & Finochietto, J. M. (2018, November). On route table computation strategies in Delay-Tolerant Satellite Networks. *Ad Hoc Networks, 80*, 31-40. doi:10.1016/j.adhoc.2018.07.002

Gharib, M., Moradlou, Z., Doostari, M. A., & Movaghar, A. (2017). Fully distruibuted ECC-based key mananagement for mobile ad hoc networks. *Computer Networks*, 269-283. doi:10.1016/j.comnet.2016.12.017

Gluhak, A., Krco, S., Nati, M., Pfisterer, Mitton, N., & Razafindralambo, T. (2011). A Survey on Facilities for Experimental Internet of Things Research. *IEEE Communications Magazine*, pp. 58-67. doi:10.1109/MCOM.2011.6069710

Goldfeder, S., Gennaro, R., Kaloder, H., Bonneau, J., Felten, E. W., Kroll, J. A., & Narayanan, A. (2015). Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme . Retrieved from http://stevengoldfeder.com/papers/threshold_sigs.pdf

Guo, H., Wang, X., Cheng, H., & Huang, M. (2017, November). A location aided controlled spraying routing algorithm for Delay Tolerant Networks. *Ad Hoc Networks*, 16-25. doi:10.1016/j.adhoc.2017.08.005

Gupta, A., Anpalagan, A., Carvalho, G., Khwaja, A. S., Guan, L., & Woungang, I. (2019). Prevailing and emerging cyber threatds and security practices in IoT-Enabled smart girds: A survey. *Journal of Network and Computer Applications*, 118-148. doi:10.1016/j.jnca.2019.01.012

Hasan, K. F., Wang, C., Feng, Y., & Tian, Y.-C. (2018). Time synchronisation in vehicular ad-hoc networks: A survey on theory and practice. *Vehicular Communications*, 39-51. doi:10.1016/j.vehcom.2018.09.001

Hasarouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. (2017). VANet security challenges and solutions: A Survey. *Vehicular Communications*, 7-20. doi:10.1016/j.vehcom.2017.01.002

He, Y., Yu, F. R., Wei, Z., & Leung, V. (2019). Trust Management for secure cognitive radio vehicular ad hoc networks. *Ad Hoc Networks*, 154-165. doi:10.10.16/j.adhoc.2018.11.0006

Homoliak, I., Venugopalan, S., Hum, Q., & Szalachowski, P. (2019, April 15). A Security Reference Architecture for Blockchains. *ArXiv*. Retrieved from https://arxiv.org/pdf/1904.06898.pdf

Hossian, M., Hasan, R., & Zawoad, S. (2018). Probe-IoT: A Public Digital Ledger Based Forensic Investigation Framework. *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 1-2). Honolulu: IEEE. doi:10.1109/INFCOMW.2018.8406875

Hu, Y., Manzor, A., Ekparinya, P., Liyange, M., Thilakarathna, K., Jourjon, G., . . . Ylianttila, M. E. (2018). Delay-Tolernat Payment Scheme Based on the Ethereum Blockchain. *Computers and Society*. Retrieved April 9, 2019, from https://arxiv.org/abs/1801.10295v1

Jiang, G., Chen, J., & Shen, Y. (2014). Delivery ratio- and buffered time-constrained: Multicasting for Delay Tolerant Networks. *Journal of Network and Computer Applications, 44*, 92-105. doi:10.1016/j.jnca.2014.05.004

Jiang, P., Guo, F., Liang, K., Lai, J., & Wen, Q. (2017). Searchain: Blockchain-based private keyword search in decentralized storage. *Future Generation Computer Systems*. doi:10.1016/j.future.2017.08.036.

Kaur, M. (2015). Attacks in Opportunistic Networks. *International Journal of Computer Science and Mobile Computing, 4*(3), 21-26. doi:https://pdfs.semanticscholar.org/c2c1/cfe00b185b887e60b3c5f3fdfd9aeab0894f.pdf

Khalid, W., Ullah, Z., Ahmed, N., Cao, Y., Khalid, M., Arshad, M., . . . Cruickshank, H. (2018). A taxonomy on misbehaving nodes in delay tolerant networks. *Computers & Society, 77*, 442-471. doi:10.1016/j.cose.2018.04.015

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 395-411. doi:10.1016/j.future.2017.11.022

Laoutaris, N., & Rodriguez, P. (2008). Good Things Come to Those Who (Can) Wait. Retrieved from http://conferences.sigcomm.org/hotnets/2008/papers/20.pdf

Lei, A., Cao, Y., Bao, S., Li, D., Asuquo, P., Cruickshank, & Sun, Z. (2019, April 5). A blockchain based certificate revocation scheme for vehicular communication systems. *Future Generation Computer Systems*. doi:10.1016/j.future.2019.03.039

Li, Q., Gao, W., Zhu, S., & Cao, G. (2012). A routing protocol for socially selfish delay tolerant networks. *Ad Hoc Networks, 10*, 1619-1632. doi:10.1016/j.adhoc.2011.07.007

Lone, A. H., & Mir, R. N. (2017). Forensic-Chain: Ethereum Blockchain Based Digital Forensics Chain of Custody. *Scientific and practical cyber security*, 21-27. Retrieved March 19, 2019, from https://pdfs.semanticscholar.org/50fa/aef8e3af200e58fc2c38be37b6041fd0640a.pdf

MacDermott, A., Baker, T., & Shi, Q. (2018). Iot Forensics: Challenges for the Ioa Era. *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS).* Paris, France: IEEE. doi:10.1109/NTMS.2018.8328748

Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications*, 251-279. doi:10.1016/j.jnca.2018.10.019

Mamolar, A. S., Pervez, Z., Calero, J. M., & Khattack, A. M. (2018). Towards the transversal detection of DDoS network attacks in 5G multi-tenant overlay networks. *Computers & Security*, 132-147. doi:10.1016/j.cose.2018.07.017

McGhin, T., Choo, K.-K. R., Liu, C. Z., & He, D. (2019, June 1). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Networkl and Computer Applications*, 62-75. doi:10.1016/j.jnca.2019.02.027

Menesidou, S. A., Varadalis, D., & Katos, V. (2016). Automated key exhange protocol evaluation in delay tolerant networks. *Computers & Security*, 1-8. doi:10.1016/j.cose.2016.02.006

Min, H. (2019). Blockchain technology for enhancing supply chain resilience. *Business Horizons*, 35-45. doi:10.1016/j.bushor.2018.08.012

Minh, Q. T., Shibata, Y., Borcea, C., & Yamada, S. (2016, April). On-site configuration of disaster recovery access networks made easy. *Ad Hoc Networks*, 46-60. doi:10.1016/j.adhoc.2015.12.008

Munoz, C., Montoto, F., Cifuentes, F., & Bustos-Jimenez, J. (2017). Building a Threshold Cryptographic Distributed HSM with Docker Containers. *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)* (pp. 1-5). Pucon, Chile: IEEE. doi:10.1109/CHILECON.2017.8229747

Niteo, A., Roman, R., & Lopez, J. (2016). Digital Witness: safeguarding Digital Evidence by using Secuire Architectures in Personal Devices. *IEEE Network*, 2016. doi:10.1109/MNET.2016.1600087NM

Oubbati, O. S., Lakas, A., Zhou, F., Günes, M., Lagraa, N., & Yagoubi, M. B. (2017). Intelligent UAV-assisted routing protocol for urban VANETs. *Computer Communications*, 93-111. doi:10.1016/j.comcom.2017.04.001

Pan, L., Zheng, X., Chen, H., Luan, T., Bootwala, H., & Batten, L. (2017). Cyber security attacks to modern vehicular systems. *Journal of Information Secuiryt and Applications*, 90-100. doi:10.1016/j.jisa.2017.08.005

Panos, C., Ntantongian, C., Malliaros, S., & Xenakis, C. (2017). Analyzing, qualifying, and detecting the blackhole attack in infrastructure-less networks. *Computer Networks*, 94-110. doi:10.1016/j.comnet.2016.12.006

Pavez, I., Correa, T., & Contreras, J. (2017). Meanings of (dis)connection: Exploring non-users in isolated rural communities with internet access infrastructure. *Poetics, 63,* 11-21. doi:10.1016/j.poetic.2017.06.001

Perez, A. J., Zeadally, S., & Jabeur, N. (2017). Investigating Security for Ubiquitous Sensor Networks. *The 8th International Conference on Ambient Systems, Networks and Technologies (ANT 2017)* (pp. 737-744). Madeira, Portugal: ScienceDirect. doi:10.1016/j.procs.2017.05.432

Reina, D. G., Ciobanu, R. I., Toral, S. L., & Dobre, C. (2016). A multi-objectiveoptimization of data dissemination in delay tolerant networks. *Expert Systems with Applications, 57*, 178-191. doi:10.1016/j.eswa.2016.03.038

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On Blockchain and its integration with IoT. Challeneges and opportunities. *Future Generation Computer Systems*, 173-190. doi:10.1016/j.future.2018.05.046

Roussev, V., Quates, C., & Martell, R. (2013). Real-time digital forensics and triage. *Digital Investigation*, 158-167. doi:10.1016/j.diin.2013.02.001

Seba, A., Nouali-Taboudjemat, N., Badache, N., & Seba, H. (2019). A review on security challenges of wireless communications in disaster emergency response and crisis management situations. *Journal of Network and Computer Applications*, 150-161. doi:10.1016/j.j.nca.2018.11.010

Sjøberg, D. K., Dybå, T., & Jørgensen, M. (2007). The Future of Empirical Methods in Software Engineering Research. *Future of Software Development*, 358-378. doi:10.1109/FOSE.2007.30

Sovacoo, B., Axsen, J., & Sorrell, S. (2018, November). Promoting novelty, rigor, and style in energy social science: Towards codes of practice for appropriate methods and research design. *Esnergy Research & Social Science, 45*, 12-42. doi:10.1016/j.erss.2018.07.007

Stathakopoulou, C., & Cachin, C. (2017). Threshold Signatures for Blockchain Systems. *IBM Research.* Zurich, Switzerland: IBM. Retrieved from https://pdfs.semanticscholar.org/2300/3bfc73e8d2fde9a465f4054f55ad1f2e8113.pdf?_ga=2.197884198.861987980.1563449230-1364988749.1563449230

Sullivan, C., & Burger, E. (2017). E-residency and blockchain. *Computer Law & Security Review, 33*, 470-481. doi:10.1016/j.clsr.2017.03.016

Trifunovic, S., & Hossmann-Picu, A. (2016). Stalk and lie - The cost of Sybil attacks in opportunistic networks. *Computer Communication, 73,* 66-79. doi:10.1016/j.comcom.2015.04.007

Venable, J., & Baskerville, R. (2012). Eating our own Cooking: Toward a More Rigorous Design Science Research Methods. *The Electronic Journal of Business Research Methods, 10*(2), 141-153. Retrieved from http://www.ejbrm.com/issue/download.html?idArticle=276

Wihlborg, E., & Engstrom, J. (2017). Bridging Digital Divides through Digital Media Buses: An Action Research Study on Digital Inclusion in Sweden. *2017 Conference for E-Democracy and Open Government (CeDEM)* (pp. 260-270). Krems, Austria: IEEE. doi:10.1109/CeDEM.2017.30

Wyatt, J., Burleigh, S., Jones, R., Torgerson, L., & Wissler, S. (2009). Disruption Tolerant Networking Flight Validation Experiment on NASA's EPOXI Mission. *2009 First International Conference on Advances in Satellite and Space Communications* (pp. 187-196). Colmar, France: IEEE. doi:10.1109/SPACOMM.2009.39

Yao, X., Zheng, X., Ning, H., & Li, P. (2017). Using trust model to ensure reliable data acquisition in VANETs. *Ad Hoc Networks*, 107-118. doi:10.1016/j.adhoc.2016.10.011

Zhao, B., Peng, W., Song, Z., Su, J., Wu, C., Yu, W., & Hu, Q. (2012). Towards efficient and practical network coding in delay tolerant networks. *Computer and Mathematics with Applications, 63*, 588-600. doi:10.1016/j.camwa.2011.10.001

Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *2015 IEEE Security and Privacy Workshops* (pp. 180-184). San Jose: IEEE. doi:10.1109/SPW.2015.27