QATAR UNIVERSITY

COLLEGE OF ENGINEERING

IOTA VIABILITY IN HEALTHCARE INDUSTRY

BY

MAYS MOHAMMED ALSHAIKHLI

A Thesis Submitted to

the Faculty of the College of Engineering

in Partial Fulfillment of the Requirements for the Degree of

Masters of Science in Computing

June 2019

COMMITTEE PAGE

The members of the Committee approve the Thesis of
Mays defended on 18/04/2019.

Dr. Tarek Mohamed El-Fouly
Thesis/Dissertation Supervisor

Dr. Tamer Khattab
Committee Member

Dr. Sameh Sorour
Committee Member

Approved:

Abdel Magid Hamouda , Dean, College of Engineering

ABSTRACT

ALSHAIKHLI, MAYS, MOHAMMED, Masters: June: 2019, Master of Science in Computing.

Supervisor of Thesis: Tarek, Mohamed, El-Fouly.

The Internet of Things is a novel paradigm which involves the increasing prevalence of objects and entities supported with identifiers and the ability to exchange the data over a network. However, with all these advantages the risk comes, as the huge number of connected devices gives hackers more entry points. Distributed Ledger Technology (DLT) can stave off security threats to Internet enabled devices by providing a distributed ledger for their functioning, thereby eliminating the central node that networks usually depend on for management by their users. Internet of Things and Application (IOTA) is a new technology designed specifically for the Internet of Things (IoT) industry which depends on the distributed ledger for storing transactions.

The main contribution of this thesis is to study and run a set of test cases in healthcare industry to prove the effectiveness and viability of using IOTA in many healthcare applications using data, images or even videos. We will also do a comparative analysis with Blockchain to prove that IOTA technology could stand all odds in terms of feasibility, reliability and robust data security.

DEDICATION

I dedicate my work

To my parents for their affection, love, encouragement, and prayers that enabled me to achieve such success. Thank you, my beloved family.

ACKNOWLEDGMENTS

First and foremost, I would like to thank Almighty Allah who granted me the opportunity to work on this thesis (Alhamdulillah) guided me throughout my life and blessed me abundantly with notable achievements.

I extend my heartiest gratitude to my parents for their unconditional love, passionate encouragement, and continuous supplication to Allah. It gives me immense pleasure to thank my sister Huda, for everything she did for me. My brother Abdulwahhab, who was always available whenever I needed him. And for my best friend Massarat, who is my model of inspiration and for every help she did to me.

I would like to submit my sincere and deepest gratitude to my supervisor, Dr. Tarek El-Fouly. This thesis would not have accomplished success without his meticulous supervision, admirable patience, and constant support. I would not be who I am today without having the honor of being mentored by him. I am deeply indebted to him for his highly commendable efforts during my journey in research. Finally, I would like to acknowledge my co-supervisor Dr. Amr Mohamed for his support and help in different parts of this thesis.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

1.1 Overview

The revolutionary changes in the operations and robust systematic functioning—with the progress of time and applied science—in pursuit of the progression of technology and the expansion of business sectors has become the priority of the present.

The critical needs of the healthcare industry demand quality and reliable technology. The healthcare organizations are challenged to deliver quality healthcare while maintaining up-to-date technology. Keeping in mind the criticality, accessibility, availability, and accuracy of information exchange among various tiers of the system, a thorough, reliable, and real-time approach is an ultimate need. Having said that, confidentiality comes out on top as a key aspect of protecting information exchange against malicious attacks. Thus, a technology with great potential and multiple potential applications, from remote monitoring to medical device integration is highly required to benefit the healthcare industry.

1.2 Limitations of the Current Healthcare Systems

There are numerous limitations within the current health care system that need to be considered to enhance the functionality of healthcare protocols. In this section, we will discuss a few of them [67] and [68]:

• Expectations of healthcare users. Users expect an immediate and seamless flow of data in today's world. Many industries either have or are starting to adopt the technologies necessary to ensure instantaneous information for their users. Unfortunately, there has been a recession in the health sector. Legacy systems are heavy, sluggish, and often sensitive, and they play little part in the patient's life.

• Fragmented health services. Due to various formats and standards, health records contained in legacy systems are isolated and thus difficult to share. The current scope of data is fragmented and not suitable for modern users' instantaneous needs. Consequently, stakeholders are encouraged to maintain their own records.

• Lack of patient centricity (passive user). The relationship between health professionals and patients has been paternalistic for a long time now. However, a considerable change of authority has occurred in recent years. A second medical opinion is now considered reasonable, and patients are expected to help make decisions about their treatment options, according to Yeoman et al. [1]. Although patients have the right to choose where and when they receive their treatment, they must not only have control over their own data but must be provided with the best care as well.

• Informed clinical decision making: Medical staff and professionals rely on research and testing to decide on informed diagnoses and possible treatment plans for patients. Traditionally, such investigation and testing are requested only when it leads to alternative diagnoses or treatment plans. Unfortunately, although research and/or test results are reported, they are rarely shared among all the healthcare providers involved in the care of the patient and are normally confined to the hospital that originally requested them. This affects the patient's quality of care. When other institutions don't know the entire history of a patient, this can lead to wrong decisions for the patient and can also lead to delays and unnecessary costs. These types of medical errors can be fatal in the worst case.

Research by the National Health Center has found that medical errors are the third most prominent cause of death in the United States, as shown in Figure 1, and that "most errors are systematic, including poorly coordinated care" (Makary et al.) [2].

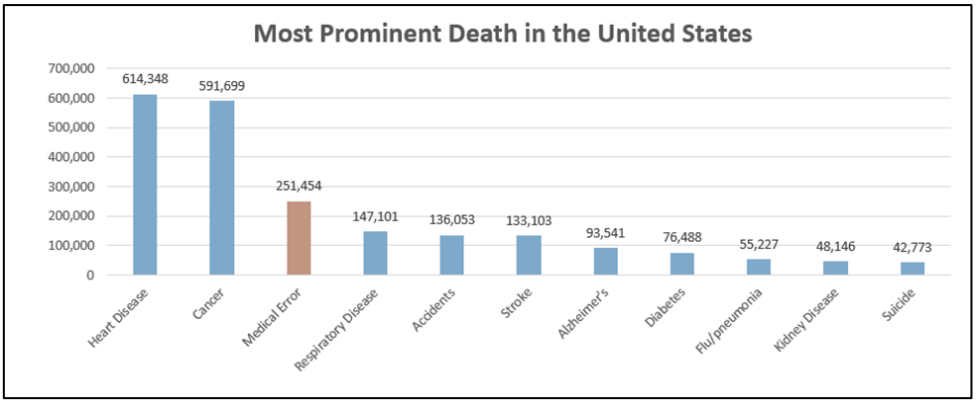

Figure 1 Most prominent death in the United States [2]

• Security risks to patient data: Electronic health records (EHR) are currently stored in a centralized database with largely non-portable medical records. Centralization increases the level of security risks and calls for confidence in a single authority. In addition, centralized databases cannot guarantee security and data integrity. Legal requirements force health institutions to have centralized health databases. Centralized health databases in most countries are legally necessary to improve portability and safety. In this context, they require an extra layer of technology.

Data security is paramount because medical data is more sensitive. In early 2017, this was underlined when a cyber-attack hit health institutions around the world. The attack showed the public that health systems are vulnerable to potential risks, and it served as a warning about the shortcomings of existing facilities. Many institutions have tried to overcome this issue, which is top on governments' agendas and causes both physician and patient frustration. Data security is a major part of the challenge noted by Collier [3].

• Increasing costs. The current system is unbelievably slow, inflexible, and unfortunately opaque for both patients and professionals. These problems are also apparent during the processing of health plan claims that require approval from health

plan providers and subsequent sharing of data with the providers in order to determine costs. This occurs only if the specific healthcare service has a health plan "in-network." To make a supplier an in-network supplier, it is necessary to negotiate a complex agreement that adds substantial cost to the supplier's management costs. Billing and insurance related (BIR) expenses include, among other things, the maintenance of benefit databases and the records for the services provided. Average BIR costs are expected to reach up to $315 billion by 2018 and take up to 3.9 hours, according to Yong et al. [4].

• Record tampering: Medical data should not only be considered as medical records but also as legal documents. It is a criminal offense to tamper with stored records, and any retrospective changes must be clearly marked, dated, and signed. Changing existing medical records or deleting or adding false records is a risk for healthcare professionals. Authentic and original clinical notes are required if a claim is made, and a claim cannot be made indefensible by failing to do so.

1.3 Thesis Objective

The goal of this thesis is to tackle the problem of lacking high-quality services in the field of e-health. The conflict between the use of EHR technology and patients' privacy in terms of their medical history remains a major problem in the healthcare sector. Doctors face ample issues (in terms of performance and security) with EHR, leading to unreliable and troubled results. To achieve this goal, IOTA is intended to give advanced trust to the community through the decentralized approach of the innovation itself. This approach inhibits records from being tampered with because there is no single central authority that by itself can alter data [60].

Working on a distributed guideline is important in the healthcare community, since IOTA can resolve the issues around the absence of a central node, arranging health records with the goal that they can be verified and recorded by all participants. This can possibly construct an efficient focused framework for patients. It doesn't, in any case, imply that IOTA is just utilized in a decentralized setting; rather, it is utilized with a constraint that the trust between healthcare entities is fundamental, with or without intermediaries. Its ability to conquer healthcare's most serious challenges, from identity and security to information integrity and access, just like interoperability, is too unexpected to ever be overlooked by our industry [61].

Indeed, it is the desire to stop losing trust in health records that has driven us to IOTA technology. By giving the precise idea of an unalterable health record empowered by IOTA, the potential for utilizing this progressive innovation for tracking purposes is also incredible. With the healthcare industry currently being very digitized and at the same time experiencing information weakness, utilizing an IOTA innovation-based framework makes sense to monitor this tremendous volume of information and provide the area with much-required relief.

The main objectives of this research can be summarized as:

1.Studying and running a set of test cases in healthcare industry to prove the effectiveness and viability of using IOTA in many healthcare applications using data, stream of continuous data, images or even videos.

2.We will also do a comparative analysis with Blockchain to prove that IOTA technology could stand all odds in terms of feasibility, reliability and robust data security.

1.4 Thesis Outline

In Chapter 2, we present the necessary background information and address some of the recent reviews of the related problems. Chapter 3 reviews the history of the IOTA model and its components and algorithms. Our proposed system and case studies for its evaluation are presented in Chapter 4. Chapter 5 concludes the thesis and presents some future work.

CHAPTER 2: BACKGROUND

2.1 Overview

Some important studies related to the proposed framework are discussed in this chapter. The work discussed is the main concept of a newly proposed framework that is presented in Chapter 3. The design and assessment papers discussed in this chapter are divided into two main subjects. The first set of research papers focuses on the overall concept of IoT, along with its benefits, risks, usage, device requirements, and security requirements. The second set of papers focus on blockchain technology, as it provides the baseline for IOTA technology because of the similarities in their concepts.

2.2 Internet of Things

The Internet of Things (IoT) impacts the way we interact with the world around us. Billions of internet-connected devices ("things") ranging from TVs, fridges, and cars to health monitors and wearables find their way into our personal lives, according to Pan et al. [5]. As Kumar et al. [6] point out, we are heading towards 20.6 billion connected things by 2020, according to the Gartner forecast. This pervasive technology materializes the concept of things being super-connected to the world and collecting information, as well as being monitored and controlled via the Internet to interact and interconnect with humans. Even with overestimates of the number of devices connected to the IoT world, there is no escaping that we are inside the IoT world and an unimaginably large number of IoT devices contain sensitive information, any disclosure of which will have serious consequences. IoT devices have several issues related to security due to their limited hardware and significant energy constraints according to Trappe [7]. Also, the characteristics of the IoT ecosystem have security implications with regard to the flow of information between the connected devices. A prime illustration of security's importance in the IoT environment is the 2016 Dyn

cyberattack that involved a distributed denial of service (DDoS) attack that targeted systems provided by Dyn, which affected millions of internet addresses as well as servers. According to Kolias et al. [8], countless IoT devices were infected and hijacked by this simple malware attack.

There is no clear plan for realizing the vision of the IoT. In a centralized "traditional platform" of cloud computing that acquires information from nodes in data acquisition networks and provides raw data and services to other nodes, the central platform controls the whole information flow. But the problem with the centralized model is that the infrastructure and its maintenance are costly, and as IoT devices proliferate, it will increase the cost substantially. Also, from a performance standpoint, centralized servers remain a bottleneck and failure point that could disrupt the whole network. On the other hand, in a distributed approach, different application platforms collaborate with each other, and all the intelligence is in the nodes (edge computing). However, there have been no explicit analyses for the most powerful security and performance mechanism, blockchain and IOTA, that were built using the distributed platform. In order to understand these techniques, it is necessary to understand the distributed approach and determine its actual value.

Today's IoT initiatives apply distributed computing concepts on a local level and collaborate with other network participants to achieve a common goal. Still, the development of decentralized architecture and edge computing is a critical issue discussed by Sunmaeker et al. [9]. In order to explore these factors, we need to study the specific requirements of applications.

Goiri and LopezdeIpina [10] discuss in their paper how to use web protocols to implement IoT successfully through semantic techniques that help with exchanging

knowledge in a distributed manner, where devices located in different locations can communicate with each other successfully.

Also, Liu [11] describes the U2IoT system, which is composed of two parts—the unit of the IoTs and the ubiquitous IoT—which control the communication between all nodes. Because of the nature of the distributed environment, many security threats are encountered. Zhou et al. [12] explain in detail the security issues and challenges in distributed IoT by focusing on the network entity, where un-traceability, authentication, and access control are the main security issues. The proposed technique is based on the robustness and scalability of the network and node mobility due to their dynamic behavior. Specifically, the node can travel from network to network safely due to the robustness of the node mobility.

As the IoT extends to be "Internet of everything," companies are increasingly interested in leveraging data-driven insights to generate value. This technology offers different ways to make more profit through increased resource efficiency and productivity. We need IoT in many fields, such as medical and healthcare systems, where the Internet of things is revolutionizing healthcare. As patients become more connected and generate more data, clinicians can identify and address their needs more efficiently than ever.

IoT can help in many ways: 1) It can make operations that once required ample time to execute instantaneous, and 2) it can provide comfort to patients because various in-hospital procedures and treatments such as electrocardiograms (ECGs) and blood pressure (BP) monitoring could be conducted remotely.

These systems would utilize devices to allow patients to monitor their health, share data with healthcare providers, and alert others when in need by embedding intelligent functionalities into homes. This would allow patients to be monitored around

the clock with built-in sensors that could track movement from inside the home and alert family members or emergency services when needed. These smart systems could be integrated with near field communication, radio frequency identification (NFC, RFID) and other wireless-based applications for data sharing, according to Amendola [13]. The deployment of such services would certainly displace invasive testing methods, thus saving time and money.

The crux is that with the advancement in biotechnology and its utilization in the healthcare industry, healthcare providers would significantly increase the success rate of patient comfort and survival, according to Hu [14].

2.2.1 Advantages and Disadvantages of IoT

The IoT is a future-oriented technology that proposes interconnected devices and the Internet to automate many daily jobs. The IoT digitizes the sensors, equipment, machinery, gateways, and network. It connects people in the real environment with devices. This opens opportunities for significant data creation and revenue generation and leads to a rapidly growing typical IoT network which expands the speed of variation and total volume of data. But how such a large amount of information from all sources will act in real-time situations in IoT environments is a real challenge to predict.

2.2.1.1 Advantages of IoT

As already discussed in the above section, IoT technology is rapidly emerging because of its incomparable structure and efficiency. The future depiction of IoT will certainly revolutionize various technological applications around the globe. Many of the benefits of this stringent and sturdy platform are discussed by Roman et al. [15] and Zhao et al. [16]:

• Communication: IoT technology's main role is to connect machine to machine (M2M) to make the commutation of devices more transparent and to stay in touch with one another. This will lead to greater efficiency, higher quality, and faster results.

• Automation and control: Replacing much of human intervention with IoT devices is an aim of IoT technology. Automation will increase the quality, reliability, and security of services. This will allow machines to be able to communicate with each other without human intervention.

• Access to information: Ease of access to any information regardless of the location of the data by IoT platforms will make it very convenient for people to do their work, even if they are not physically present at their workplace.

• Monitoring: Taking into consideration the surgical aspects of healthcare industry monitoring have always been a challenge to healthcare professionals. IoT will ensure that the critical data required during surgical interventions is stored and accessed efficiently.

• Cost effectiveness: The financial aspect is also one of IoT's greatest advantage for money saving and optimum use of energy and resources. Where IoT devices provide a relatively cheap way to increase efficiency considerably.

2.2.1.2 Disadvantages of IoT

With the huge list of advantages of IoT, we need to look at the technology from a wider perspective to look for its weaknesses, if any: Here is a compiled list of the disadvantages of IoT discussed by Roman et al. [15] and Zhao et al. [16]:

• Compatibility: Different types of devices could require installing extra hardware to make it possible to communicate between the IoT devices.

• Complexity: Even though the huge number of interconnected devices is an added advantage for IoTs because of its nature, as far as security is concerned, this advantage brings a flaw in the system. For example, as more nodes get added to the network, dealing with data congestion becomes a challenge.

• Privacy and security: The privacy of IoT is a major concern. The safety risks associated with IoT are becoming more complex and may have serious consequences. All information between IoT devices should be encrypted to keep information confidential, which obviously demands extra effort and infrastructure.

2.2.2 IoT Security Requirements

The Defense Advanced Research Projects Agency (DARPA) has identified the Internet of Things security shield as one of four projects with a potentially wider impact than the Internet itself, according to Sfer et al. [17]. The security requirements of IoT devices are divided into four principle areas (authentication, confidentiality, integrity, and availability) to ensure security between different devices. Security should be implemented during the development lifecycle of all IoT devices. Here we will discuss the principles requirement in more detail as explained by Leo et al. [18] and Weber [19]:

• Authentication: Weak links in today's computing world can sometimes be networks. They are one of the most vulnerable sections of the whole configuration. Each IoT node must recognize any node that attempts to connect. The node credentials

are verified, identified, and validated to determine whether the user is authentic in using the resources. IoT users can use double-way authentication, digital certificates, and biometrics based on the needs of the IoT user for easy or complex and much more secure authentication. IoT authentication does not require human authentication intervention because the sensors and the machine-to-machine interactions are highly embedded in IoT. Therefore, you will have to go in with a different mindset when authenticating IoT devices. However, it's very challenging to achieve authentication due to the nature of the IoT environment with many nodes connected to the network (e.g., devices, humans, services, processing units, and service providers) as discussed by Roman et al. [12]. In 2015, Rizzardi et al. published a research paper, "Security, privacy and trust in Internet of things: The road ahead" [20], to assert the opinion that a set of IoT devices communicates to accomplish a common goal. Their vision considered that IoT deployments involve distinct technologies, architectures, and implementations to build a successful and secure communication. They divided their work in terms of security into three main categories: security requirement (authentication, access control, and confidentiality), trust, and privacy.

• Confidentiality: Confidentiality and privacy are always interchangeable in our lives. They refer to how users share information with other users which generally cannot be divulged without getting the authorization to access the data. On the other hand, privacy refers to freedom from intrusion into another user's information. Confidentiality is designed to prevent sensitive data from going to the wrong node. Key methods to achieve confidentiality are cryptography, strong passwords, and encryption technologies. One example of confidentiality is making sure that the sensors reveal the collected data to the correct node, as explained by Farooq et al. [21] and Roman et al. [22].

• Integrity: This refers to the "property that data has not been altered or destroyed in an unauthenticated manner." The main goal of the IoT system is to exchange data between different IoT devices, and this is an extremely important factor to ensure the integrity, consistency, and accuracy of the data. It is the assurance that the data received at the receiver node is sent without tampering while in transit or modified through collisions (e.g., breaches of confidentiality), according Airehrour [23].

• Availability: IoT devices and services should be available at any time and from anywhere in order to achieve the goal of IoT technology. Availability is important to keep systems upgraded, ensure that they remain functional despite hardware issues and security attacks, and to let data be capable of retrieval, according to Abdmeziem [24].

It's important to analyze the possible threats to IoT systems and choose the appropriate defense accordingly based on the type of data and its sensitivity. Also, it's important to start thinking about security in the design phase and define security requirements regarding risk evaluation. During the design phase, it should be understood how an attacker could gain access to the system and compromise it.

2.2.3 IoT Device Requirements

IoT device requirements stem from the heterogeneous nature of IoT devices. The prerequisites of IoT are many, but the main ones can be classified into three categories:

• Low resource consumption: The IoT is already estimated to generate hundreds of zettabytes (trillions of gigabytes) of data each year, so the biggest challenge for IoT devices is to minimize power consumption. The design requirement for IoT is to increase the lifetime of devices and maximize the capacity of on-board batteries. Operating within a battery's lifetime translates into lower power needs with

ramifications for both average and peak power consumption. In the case of wearable medical devices such as pacemakers, battery failure is not an option. Therefore, it is essential to understand the power consumption pattern and battery life of these devices. A prime example of the importance of low resource consumption is a wireless sensor that would do some job for an extended period of time—maybe months or years—while powered by a battery, as explained by Perera et al. [25].

• Widespread interoperability: IoT is an unbelievably diverse area that includes a wide range of hardware and software ecosystems. All technologies are linked together within the IoT, including smart watches, drones, cameras, and thermostats. Billions of IoT devices, sensors, actuators, and smart devices are connected to the Internet for collecting and maintaining data through connected communication networks in a heterogeneous way. Interoperability is the ability to make all the devices that are connected to a network work together and achieve a specific need, according to Cheung et al. [26].

• Billions of Nano-transactions: IoT devices generate and maintain transactions over the Internet. Hence, IoT devices need a model to deal very efficiently with hundreds of billions of transactions between IoT devices, according to Cooper et al. [27]. Because IoT devices send data very frequently, the IoT device should use an application/model that takes into consideration the above requirements.

2.3 Blockchain Model

Blockchain is a fully distributed and trusted database (ledger) cryptocurrency technology that is used to maintain a tamper-proof record of transactional data to achieve transparency, integrity, and verifiability of transactions, as discussed by

Shaheen et. al. [28]. Blockchain was founded in 2009 by Satoshi Nakamoto as Bitcoin [29].

Blockchain functions as a decentralized public ledger, and it disregards the need for any central authority between network devices to maintain the network. Blockchain is structured as a peer-to-peer (P2P) network, according to Lemieux [30]. It allows the network participants through the nodes to share a public ledger, which is tamper-proof and becomes a permanent record once the transaction is confirmed and added to the blockchain. The transaction cannot be deleted or modified, and each node will be egalitarian in the network. Furthermore, each node stores a copy of the public ledger, which is updated simultaneously to prevent data loss due to a single point of failure (SPoF), according to Banerjee et al. [31].

2.3.1 How Blockchain Works

As shown in Figure 2, when a new transaction is issued, it is represented as a block in the shared ledger and is immediately broadcast to all participants. Generally, most of the nodes must execute algorithms to confirm and validate the history of the new individual block; a public key encryption technique is used to ensure the security and privacy of the distributed ledger content, according to Desmedt [32].

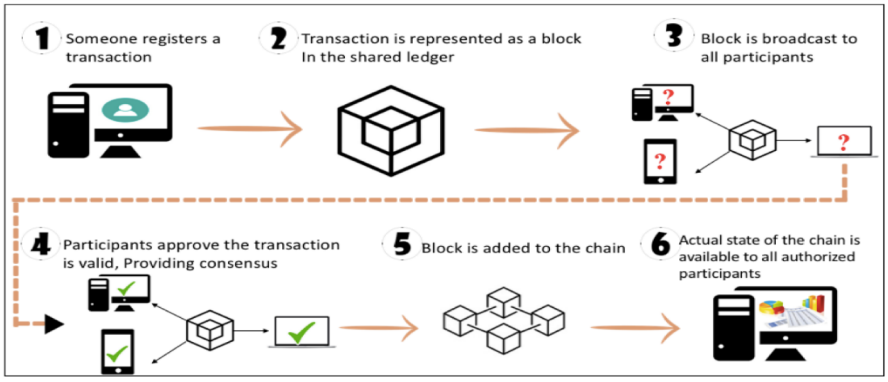

Figure 2 The blockchain process

In the beginning of the blockchain, the first block (the "genesis block") created contains a header of the block and data transactions. The block's timestamp is used to create the hash algorithm (e.g., SHA256). After the blockchain is started, any new transaction issued comes into a blockchain and calculates its own hash from the previous block hash, and all the network participants that are connected to the network must execute algorithms to confirm and validate the new transaction. This process is called "consensus," as shown in Figure 3, according to Sleiman et al. [33] and Righi et al. [34]. At this point in the process, the network participants must verify whether the hash has been calculated correctly. The distributed consensus process ensures that all network participants have the same copy between them and share the same state without the need for a centrally governing, unifying authority to determine which transactions are valid and which are not. Once a block is added to the ledger, it will not be deleted nor modified, since the main characteristic of the ledger is that it is tamper-proof. If anyone attempts to modify the block or swap it out, the hashes of the previous block will also change, which will lead to an error state during the consensus process. When the error state is reached, other network participants will not receive any new blocks unless the problem is solved by discarding the block that caused the error, and the consensus process will be repeated again, according to Zheng et al. [35].

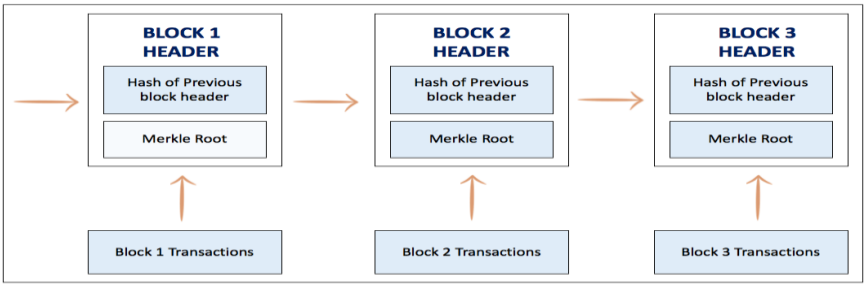

Figure 3 Blockchain from inside

Blockchains can be classified into two platforms: permission-less blockchains or permissioned blockchains, according to Meng [36]. In permission-less blockchains, also called public blockchains, any network participant can conduct transactions and participate in the consensus process. Examples of permission-less platforms are Bitcoin by Nakamoto [29], Zerocash by Sasson et al. [37], and Ethereum by Wood [38].

2.3.2 Validation Algorithms

The development of decentralized architecture and edge computing remains a main issue needed to be discussed. Determining which blockchain platform will be used is perhaps the most important part of the consensus algorithm. There are four standard protocols for blockchains which are used to arrive at consensus, according to CERP-IoT [39] and Wright et al. [40]:

• Proof-of-work (PoW) algorithm: The main innovation by Satoshi Nakamoto is doubtless the proof-of-work algorithm, which is used to solve the problem of double-spending (e.g., in Bitcoin, spending the same money twice). PoW requires network participants to perform some work that will simplify the work to the network. For the block to be accepted, it should solve the puzzle, “guess the zeros,” which is generated by the network to be solved in a specific time. The miners that don’t solve the puzzle

will try to guess the new puzzle. In general, proof-of-work always accompanies public platforms because though it consumes lot of power to compute, it is also the easiest algorithm to verify, according to Zheng et al. [41].

• Proof-of-stake (PoS) algorithm: This method uses another way to achieve consensus. Instead of solving the puzzles of PoW, the creator of a new block is chosen in a deterministic way. Depending on the number of stakes, there is no block reward, and the miners take the transaction fees. This algorithm allows for the building of a trusted and distributed network with high-stake node (loyal node), as explained in [42] by Borge.

• Practical Byzantine fault tolerance (PBFT) algorithm: PBFT is a replication algorithm that can handle up to 1/3 byzantine replica attacks and is used to build consensus in blockchain systems; it is just one of those possible solutions. Among all other algorithms, it requires less effort than others, according to Lamport et al. [43]. Three examples of blockchains that depend on PBFT for consensus are Hyper-ledger by Hyperledger Project [44], Stellar by Mazieres [45], and Ripple by Schwartz et al. [46].

• Delegated proof-of-stake (DPoS) algorithm: To achieve consensus, it uses a reputation system by preventing non-trusted nodes from participating. The trusted nodes can create blocks but cannot change the transaction details. However, they can also prevent non-trusted nodes from being included in the next block, according to Sankar et al. [47].

2.3.3 Limitations of Blockchain

The core benefit from blockchain is that it uses a decentralized database to be directly shared without a central authority. However, some researchers have pointed out that blockchain has some real challenges that need to be overcome:

• Scalability: Scalability is one of the principal criticisms of blockchain. Because of the blockchain's inherent decentralization platform characteristic, each network participant processes the transaction and maintains a copy of the entire state, according to Conoscenti et al. [48]. In fact, the blockchain gets weaker as more network participants are added to its network because of the inter-node latency that logarithmically increases with every additional participant node, as explained in [49] by Huumo.

• Storage and bandwidth: As the blockchain increase in size, the storage requirement cryptographic proof also increases the bandwidth and power needed by the network's fully participating nodes. It becomes somewhat difficult for the few nodes that can provide resources for blocks, which leads to the risk of centralization, according to Zyskind et al. [50].

• Fees: In each block, several transactions are bundled and then checked by miners. This means more jobs will be validated for miners by increasing transactions, meaning higher transaction fees as well, according to Buterin [51].

• Data privacy: Blockchain data is shared by everyone on the system intrinsically. This level of openness is not always a secure way to store data, as discussed in [52] by Aitzhan et al.

• Network size: It requires a large number of nodes knowing that each user is a node, which means that the bigger the network is, the stronger it responds to attacks while the risk of internal defects remains. Specially in IoT devices, the size really

matters. Moreover, it does have a physical limit, since all the data needs physical storage, according to Karame [53].

However, the growth of blockchain still hits bottlenecks and impediments at present, which prevent it from being used as a generic platform for cryptocurrencies across the globe. So, the IOTA comes as a next generation of blockchain to solve the drawbacks of this technology with different infrastructure as explained.

CHAPTER 3: IOTA MODEL

3.1 Overview

Internet of Things Applications (IOTA) is a cryptocurrency distributed open-source ledger that will be the foundation for the growing technological concept known as the Internet-of-Things (IoT) and aims to mark the age of the machine economy, as is explained in Popov's white paper [54]. IOTA is doing this by applying its new and innovative tangle protocol.

3.2 IOTA History and Evaluation

The evolution of IOTA began in 2015. Marked as a "third-generation cryptocurrency," IOTA was launched by David Sonstebo in 2015, and all tokens were issued by the end of the year. By 2017, the tokens had been used for beta-testing [54]. Rumors swirled that all tokens were seized by the community that established the IOTA Foundation, a non-profit organization seated in Germany, while the developers got nothing [55].

The number of devices to be connected to the network will reach 20.6 billion in the coming years [6]. According to experts, this type of network fits perfectly with IOTA's original purpose: to be a means of data transfer. The data are pre-mined and inseparable, and to be able to use the network, users do not need them. A total of 2,779,530,283,277,761 tokens are in circulation at this point.

There is no other cryptocurrency that has the strength of micro-transactions as of today. Micro-transactions (i.e., sending small volumes) became a substantial part of the internet once they were resolved by IOTA developers. In 2016, massive investment in this project was made by Outlier Ventures Capital Project [56].

A huge advantage is that no fees are required for this cryptocurrency, regardless of the size of the transaction. Nodes are motivated to be involved in the creation and

confirmation of other node transactions. The system uses a weight mechanism to avoid hacker attacks and spam. All transactions are confirmed in terms of their weight. The weight corresponds to the amount of "work" invested in a transaction by each node.

Unlike other cryptocurrencies, IOTA has always primarily focused on the Internet of Things. This global concept includes network elements such as medical systems that can communicate with data and can be monitored and remotely controlled.

3.3 Advantages of IOTA

The idea of IOTA stands out from other technologies because of its scalability. This next-generation technology will certainly go way ahead in terms of its robust architecture, which is much more sophisticated than other distributed ledger technologies.

• Distributed Ledger Technology: IOTA is an open-source cryptocurrency created for IoT projects seeking to build a distribution ledger for the Internet of Things, different from most of other cryptocurrencies, which use blockchains technology to store transactions. A distributed ledger is a database that can store and updated independently by each node in a large network. The broadcasting is unique, where the transactions are not distributed to various nodes that govern by a central authority but instead are independently built and held by every node. Each node on the network validates two previous transactions, and the majority must come to a consensus. The main idea of IOTA is the ability to communicate through a tangle graph, which gives the advantage of establishing secure, fully authenticated, and tamper-proof communications between the IoT devices and sensors [57].

• Micro-transactions and Zero Fees: IOTA provide real-time micro-transactions as well as an ecosystem that is ready and flexible for scaling with no mining and no

blocks. The security and consensus of the network are maintained by all the nodes that are attached to the network and generating transactions. Micro-transactions are enabled for the first time in tangle technology, which gives developers new business opportunities for their applications in IoT devices. Besides transferring money between users, IOTA allows the transfer of transactions between IOTA devices to request a service. To implement this service, you need to pay for the data with a small value of IOTAs, which is called “micro-payment.” Zero fees for each transaction is another interesting advantage that comes with IOTA, as there is no requirement to pay miners, which is a purposive accomplishment in the tangle technology [58].

• Scalable Distributed Ledger: There is no limit to scalability. Each transaction requires the sender to verify two previous transactions on the tangle in order to broadcast to neighbors, so more transactions can be confirmed as the number of users sending them increases, which makes IOTA scale proportionally to the number of transactions. Also, IOTA can achieve high transaction throughput: Even if more IOTA transactions are created, the confirmation rates will become better, as explained by Martin et al. [59].

3.4 How IOTA Works

IOTA cryptocurrency is based on the tangle technology, just as Bitcoin and Ethereum are based on blockchain. The Direct Acyclic Graph (DAG) of the tangle differs in several key aspects from the blockchain. The tangle uses a ledger in the tangle protocol to store transactions. These transactions are connected via edges, which represent validated transactions within the tangle network. The rule of the tangle is to validate at least two previous transactions before a new transaction that takes place on the network can be validated.

The procedure for validating transactions in the tangle network differs from the procedure carried out in the blockchain network. There are no miners on the tangle network in the same sense that Bitcoin miners are made available. Each user who operates on the tangle network is, instead, a miner. In sending x IOTAs onto Bob's mobile phone, Alice performs an order to verify two previous transactions with a proof-of-work calculation. IOTA uses Hash-cash as a test algorithm, but with considerably less difficulty. This allows the tangle network to join regular devices such as Alice's mobile telephones, internet routers, and laptops.

3.5 The Tangle

We must learn what computer scientists call a "directed acyclic graph" in order to understand the tangle. A "directed acyclic graph" is a group of vertices (squares) that are linked by edges (arrows) without forming a loop. Figure 4 is a directed diagram example:

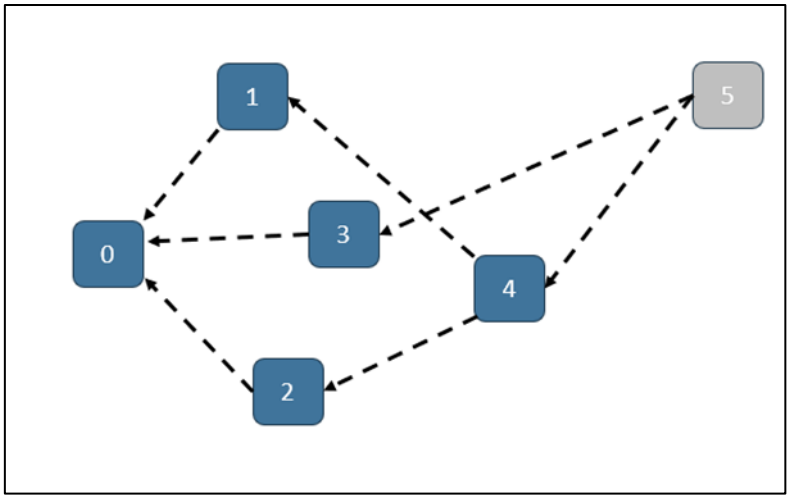

Figure 4 Directed acyclic graph

A directed graph is a data structure behind IOTA that holds transactions in the

“tangle”. Figure 4 shows each transaction as a vertex. The first transaction created, called the genesis transaction, is the one on the left, and the latest transactions are located on the right. The transaction with no approvals is called the tip which is marked with a gray square. If a new transaction is included in the tangle, two previous transactions will be selected for approval, and two new edges are added. In the above example, transaction 5 validates two previous transactions ‘number 3 and 4’ (unapproved transaction tips). Transaction number 5 is a tip in this example, as no one has approved it yet.

3.6 Tip Selection Algorithms

Two tips must be selected for approval for every incoming transaction. It is extremely important to choose the two tips to be approved, and it is essential for IOTA to function appropriately. Although there exist many algorithms that can be used for tip selection, we will start with the simplest of them:

• Uniform Random Tip Selection Algorithm: For each incoming transaction, all transactions that are not currently approved will be considered and could be selected for approval. We simply select two of them randomly. But this will raise a serious problem: lazy tip approval. A lazy tip validates old tips rather than recent ones. It is lazy because it doesn’t keep the state of the tangle up to date and only diffuses its own transactions based on old data. This issue will not help the network, as there is no confirmation of new transactions. In the example shown in Figure 5, transaction 14 is a lazy tip because it has approved transaction 1 and transaction 3, which are quite old transactions. In this example, because of the unweighted walk, transaction 14 is being randomly approved as any other transaction.

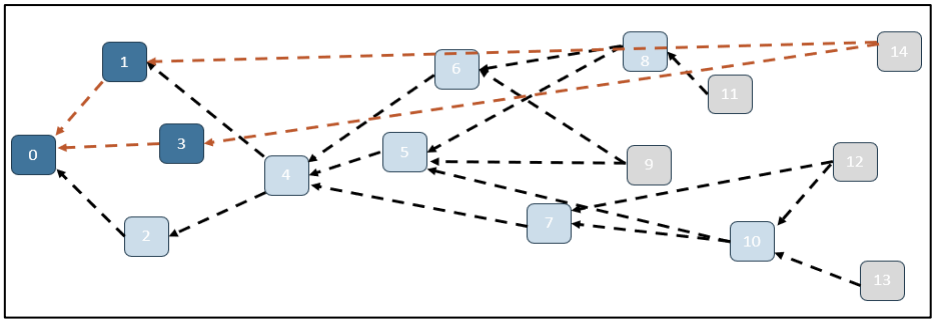

Figure 5 Lazy tip example

This issue needs to be addressed, but at the same time, we cannot strictly let any new transaction accept only the recent tip transactions because this would counter the concept of decentralization. We need to work on a solution to discourage the lazy walk so that the lazy tips won't be selected.

• Random Walk Algorithm: Selects two unapproved transactions ("tips"). One thing this algorithm needs to address is avoiding lazy tips when selecting. We will accomplish this by using a favourite strategy, wherein we will be partial in choosing the lazy tip in such a way that it will be ignored during the random walk. The calculation of cumulative weight will give us the real picture of how important a transaction is. As we will be biased in selecting the transactions, we will try to walk toward the transaction with the heaviest weight only. This algorithm is best for avoiding laziness. In our example shown in Figure 6, we calculate the cumulative weight of transaction 3. It has a cumulative weight of 5 = 1 + 1 + 1 + 1 + its own weight (1). Transactions 7, 8, and 10 are indirect transactions, while 5 is the direct transaction.

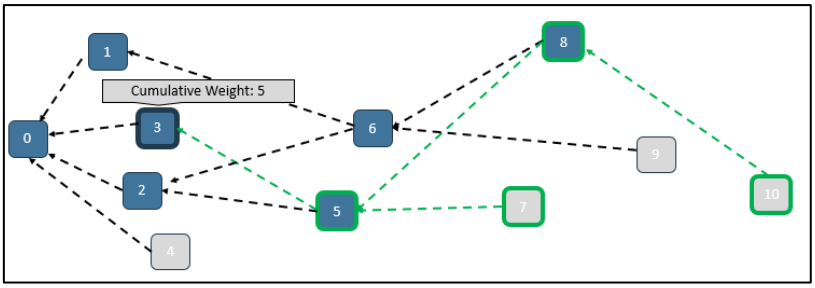

Figure 6 Cumulative weight example

• Super-Weighted Random Walk: Here, we need to halt for a moment to understand if we really need a random walk, as we can create a super-weighted random walk, where we can pick the heaviest weight transaction at each crossing with less probability involved. Then we'll get a situation like the one shown in Figure 7:

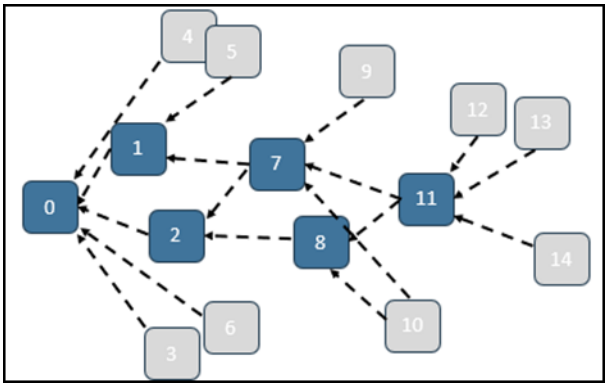

Figure 7 Super-Weighted random walks

The squares in gray are the tips, which have no approver and won't be approved in future. This is the effect of the bias strategy where we were partial in our walk. This will leave a large percentage of tips stagnant, and it will leave behind many of the tips, which will never be approved in the future. The forgotten tips will be side-lined around the schema. We need a strategy with a parameter α, which determines the importance of the transaction according to its cumulative weight, rather than being partial at any

junction.

3.7 Transaction Rates, Latency, and Random Walks

The transactions are not evenly spread out over time, but some periods are "heavier" than others. This randomness is attained by using a Poisson point process to structure how transactions arrive.

The Poisson point process model is very common for analyzing how many customers walk into, for example, a hospital in rush hours or how many requests are sent for ambulances in a given period of time. Some transactions, as can be seen in Figure 8, arrive at almost the same time (Transactions 4, 5, and 6). There is a long delay between transactions 6 and 7.

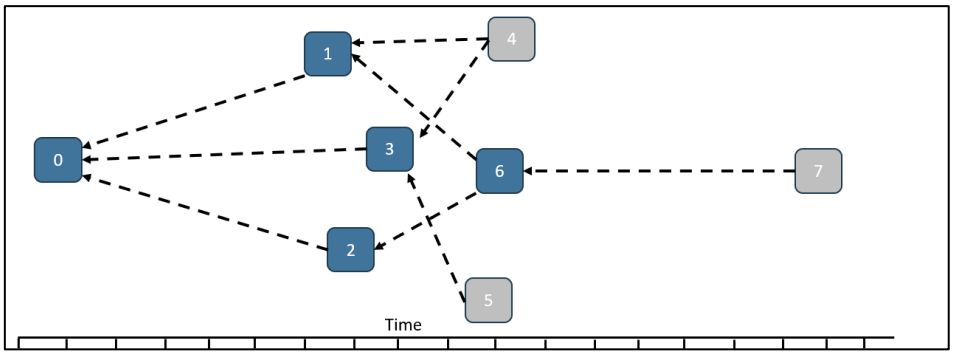

Figure 8 Applied Poisson Point model on tangle

The Poisson point process help us to determine that the average rate of incoming transactions is constant. Per this method, the constant β gives us the probability of patients visiting a hospital during a given period of time. As an example, if we fixed β = 4 and the number of transactions to be 200, the total execution time will be about 50-time units.

3.8 Approvers, Balances, and Double-spends

In the above sections in this chapter, we explained random walks, DAG, and other tip selection methods. Now, we will discuss in monetary terms what it depicts when we say that transaction A validates transaction B.

Each transaction is in form of "Alice paid Bob 50 [Mi]." It is the validator's job to make sure that Alice really had those 50 [Mi] in her account to give.

Discussing Alice and Bob further, consider the example shown in Figure 9. The rectangle here represents a transaction. The blocks inside the rectangle have the current balance in Alice's account and current balance in Bob's account before and after the transaction. We see that before the payment, Alice had 50 [Mi], which she paid it to Bob, after which Bob has 50 [Mi] and Alice has none.

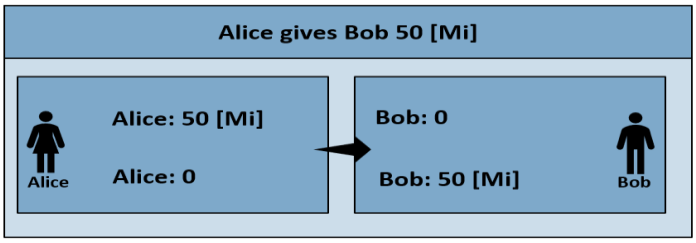

Figure 9 Example of Alice gives Bob 50 [Mi]

Finally, someone announces that Carol needs to send his own payment. He executes the tip selection algorithm, and the results show that he needs to validate Alice's transaction. He will make sure that Alice really had the 50 [Mi] she spent. Carol must be cautious about the fact that if he approves a malicious transaction, his own transaction will be in trouble and never be approved!

So, Carol should check all the transactions that had been validated directly and indirectly by Alice's transaction, all the way back to the genesis. The list that ends up with:

Genesis creates 60 [Mi]

Genesis paid Bob 10 [Mi]

Genesis paid Alice 40 [Mi]

Genesis paid Carol 10 [Mi]

Bob paid Alice 10 [Mi]

This is only one option; any list that finishes in Alice's account with 50 [Mi] and Bob's with 0 is acceptable. Also, in order to ensure they are not less than zero, Carol must monitor all other accounts in the system: If any balances of the previous or following sections are negative, its transaction shall be invalid.

Now, let's look at another scenario, as shown in Figure 10, where Alice pays more IOTAs than she has in her account:

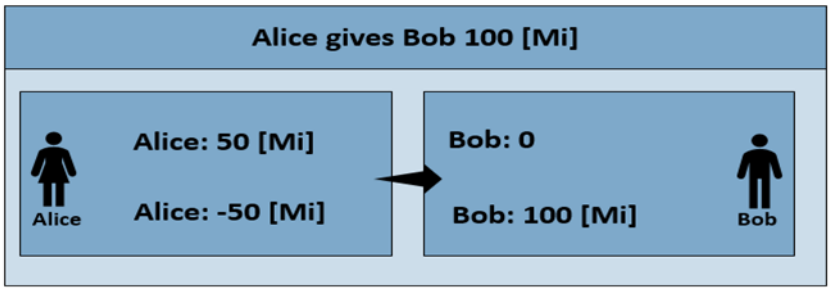

Figure 10 Example of Alice gives Bob 100 [Mi]

Alice gives Bob 100 [Mi] even though she only had 50 [Mi]. Alice's transaction will be disapproved because of the negative balance. Now, if we validate two previous transactions rather than one, shown in Figure 11:

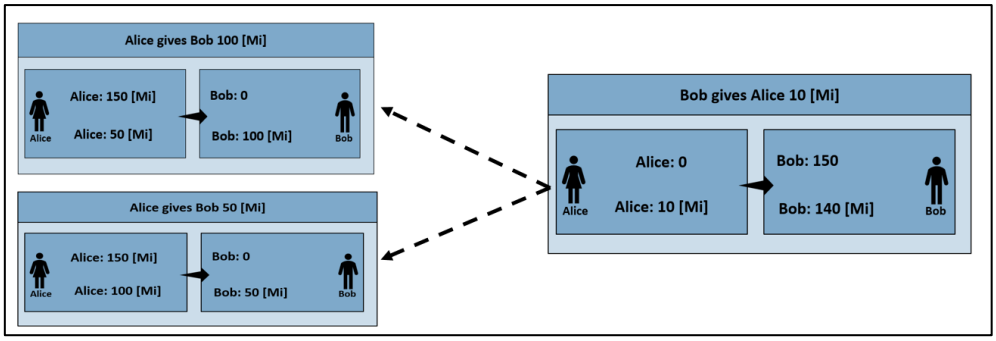

Figure 11 Example of transaction with two approvals

Bob verified Alice's transactions, because she has enough balance in her account to pay both the transactions without her balance going negative. If we take the scenario shown in Figure 12, where the total is more than she has, then Bob cannot validate both of Alice's transactions, because the total goes negative.

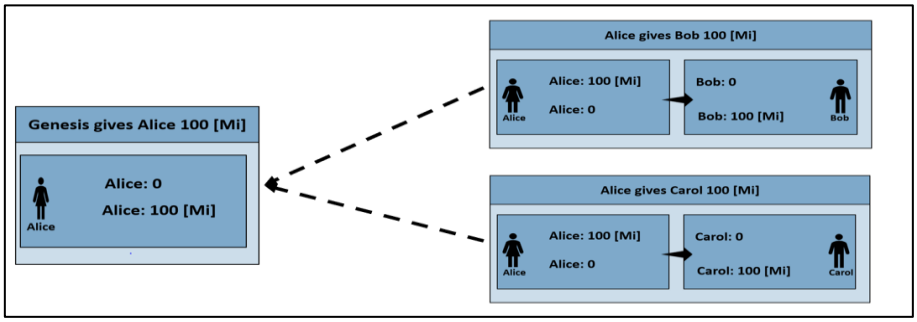

Figure 12 Example of invalid transaction

Alice has 100 [Mi], which she pays to both Bob and Carol. But this is obviously a problem: Both transactions cannot be treated as valid. We cannot have an upcoming transaction with tangle terminology that will approve them both, as it will end up with Alice's account having a negative balance.

The last scenario discusses the double spending problem, where Alice spends her money twice, as shown in Figure 12. Here, Alice still follow the protocol, because

she had sufficient balance for each transaction. It may be that by mistake her transaction sent twice and she did not even mean to double-spend. However, create two branches in the tangle that cannot be agreed. This creates a confusion for honest users in which branch should they follow and validate?

The solution of double spending problem is the weighted walk that we discussed above in this section. Finally, one of these branches will have more weight and grow more than the other, and the lighter one will be ignored.

3.9 Masked Authenticated Messaging

IOTA is the first distributed ledger, free transaction architecture designed for Internet of Things or Web 3.0 to allow devices to communicate securely and autonomously. IOTA uses a gossip protocol in its core to spread transactions across the network. This method allows for efficient dispersal of all data with enough weight on the tangle. These transactions can contain an amount or information sent by a sensor, a car, or an application installed on your phone, allowing any person's small jobs, microscopic data, and nano-payments to flow around the globe. An IOTA user is always able to publish a message. It only makes a lightweight calculation for proof of work to let the data spread through the tangle (this is required to prevent network spamming). If the channel ID (= address) is heard by nodes in real time, when the subscriber reaches the subscriber's node, the message is received (gossiped through the network).

These messages may be large, but a heuristic assessment will show smaller messages with a higher data integrity potential. Other concepts which would be very useful in MAM include remote control transmission and update orchestration.

Because these MAM transactions are stored inside the distributed ledger, they both contribute to the network's security through a help in calculating the hashing power and

benefit from the network's data integrity properties because other businesses still reference them indirectly. MAM covers the application layer of the network layers, as shown in Figure 13.

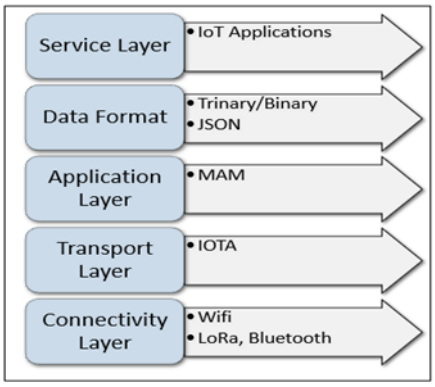

Figure 13 IOTA network layers

In order to sign the digest of an encrypted message, MAM uses a Merkle tree signature method. The root is used as a channel ID for this Merkle tree. Each message covers the root of the next Merkle tree, given that a tree only persists for a short period of time. Because previous trees are not mentioned, a forward secrecy element could be added to a channel.

A one-time pad is used to encrypt all the messages, each of which contains the channel ID and the key's index that used to sign the message for its encryption. A reversible encryption key may be used as a supplementary nonce. The resulting hash is signed with the private key of one of the leaves. The encoded payload, the signature, and the siblings of the sheet are then released to the network, which can be found and deciphered by anyone who knows the symmetrical key.

The message is authenticated during use of the MAM stream by validating the signature and checking that the signature is one of the leaves of the tree, and then it is revealed.

The entire message is deemed invalid if the signature check fails.

3.9.1 Privacy and Encryption Modes

The MAM method can be used to monitor the state and access in several different ways. Here, I will describe some of those forms that offer nuanced MAM applications far from a simple encrypted message stream.

3.9.1.1 MAM Channel

MAM also has a channel like YouTube where owners publish, and viewers meet. Viewers can subscribe to the data available in the channel, which the channel owner publishes. This ownership is secured by seed in tangle. Seed has every right to privacy and property.

• Public Mode: The Merkle tree root in public mode uses the root as the transaction address at which the message is published. A random user can then decrypt a message by using the message address. This mode is like amateur radio. It can be used by a device or individual for public announcements, but you now have the added immutability and data integrity properties.

As shown in Figure 14, NextRoot is the next message connecting pointer. When one generation's masked message is decoded, the unmasked message includes NextRoot, which is used by requester to find the next-generation message on the channel. Simply put, it's as if you find the key to open the second generation in the first generation. Once again, one could trace all messages from the channel's genesis on the chain. However, if the middle generation is given to you, you can only decrypt and start reading from that middle point, you can't trace past messages back.

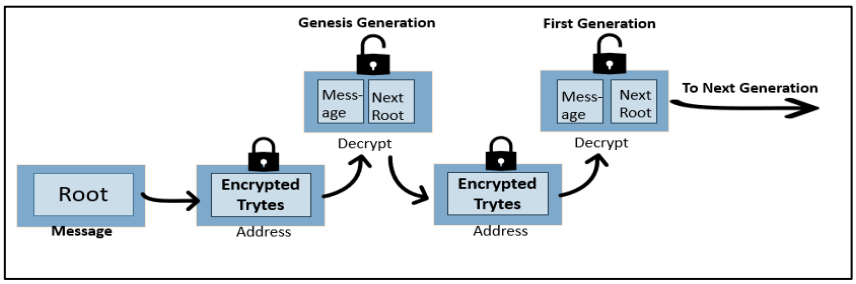

Figure 14 Public mode

• Private Mode: Private mode may be used for encoded or private streams that are not intended for public use. The Merkle root hash is used as an address in private mode. This prevents random users from decrypting your message if it stumbles because they cannot obtain the root from the hash. This makes a MAM data stream readable only by those who have the root. This mode is more similar to an encoded radio stream, everyone can see it, but only those who have the root can decode it. Private mode is useful for private communication between owned devices.

• Restricted Mode: Restricted channel adds an authentication key to private channel. The address used to attach to the network is the hash of the authorization key and the Merkle root. A message publisher could stop using the authorized key without changing its Channel ID (that is, the Merkle tree), so access could be revoked from subscribers if desired. When a key change event occurs, the new authorized key needs to be distributed to the parties that are allowed to follow the stream. In other ways, it is the same as public mode. The only difference is that sideKey is used to decrypt masked messages, as shown in Figure 15. People without sideKey can find a message's location with the root but can't understand what's loaded there.

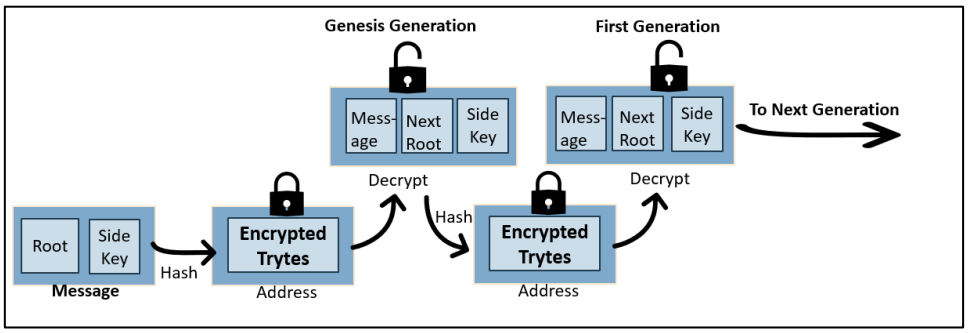

Figure 15 Restricted mode

3.9.2 Message Chain

As with many other cryptos in IOTA technology, nodes can send arbitrary messages with the transactions. But for IOTA, it restricts the sender to only attach one message at a time, and one cannot publish successive related messages in an arbitrary context.

For example, if you want to send the current heart rate data every 5 minutes, you must send each message at the same address without MAM. Since the nature of DLT, including the tangle, is reachable by the public, it is easy for attackers to recognize the address that making the updates every 5 minutes and interfere with it with spam transactions. If you decide to change your address each time you send new data, you should keep in track all the addresses used. And controlling them is relatively expensive in terms of online data storage.

However, we can keep our channels safe from any disturbing spam transactions with the message chain and thereby free ourselves from cumulative address management.

MAM sends each message from a different address. Older messages always lead to new ones in this message chain, from one generation to the next. Its flow is in one

direction.

3.9.3 Basic Structure of MAM Bundle

The MAM bundle has two sections, the signature section and the MAM section, the details of which will be explained later in this chapter. Their data is saved in the bundle as a signature fragment of transactions. The signature is used to check the ownership of MAM and therefore its validity. And the address is where the actual masked message is being stored and is hashed from the root, as shown in Figure 16.

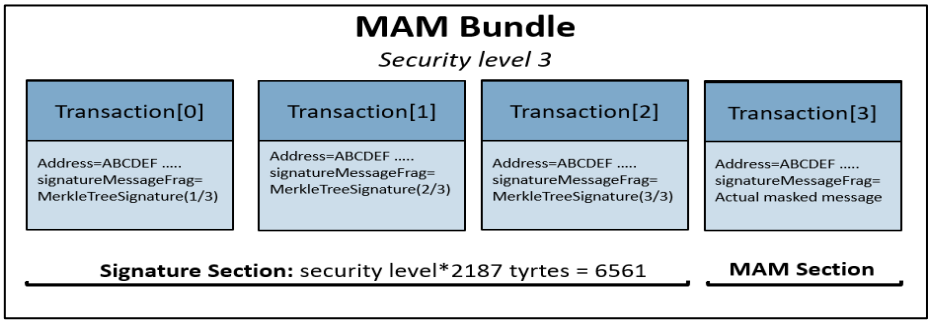

Figure 16 MAM bundle

3.9.4 Private Key and Digest

The seed is an arbitrary string of 81 trytes, which users can freely choose. However, the private key isn't the same, it's just a result of complicated seed hashing calculations. The digest is the next private key by-product. Figure 17 shows what is happening.

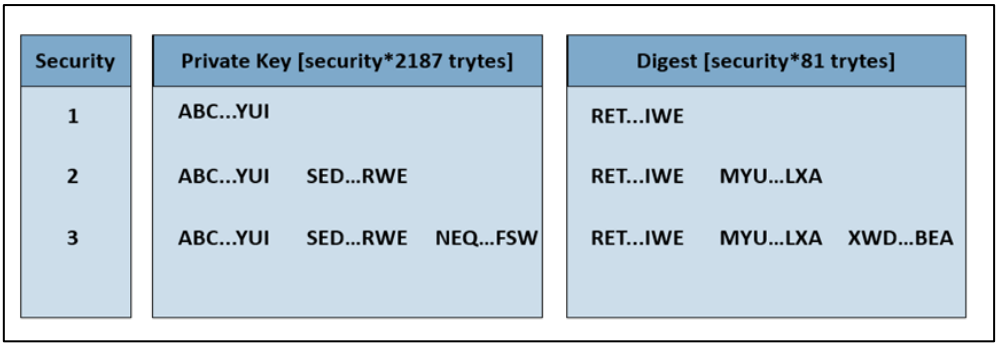

Figure 17 Security, private key, and digest

The higher the security, apparently, the longer the length. And just what has changed is added to the next chunk by changing the security level. There is a partial overlap between different security levels in the private key.

3.9.5 Ownership of Channel

To prove ownership of the channel, so that only the actual publisher can publish in his or her channel and keep the message chain from being edited, a signature is used.

3.9.6 Publish Masked Message

At this point, each section of publishing will be explained separately for ease of understanding:

3.9.6.1 Publish Root

Root address is the Merkle tree's root address. To know this root address, we need to construct the Merkle Tree. And the seed is used for the creation of Merkle tree. The Merkle tree has start and size integer parameters. These represent the index of addresses generated from the seed. Also, when we

generate addresses, we take the index as one of the parameters (seed, index, security). As shown in Figure 18, A, B, C, and D, are index keys with values equal to 0, 1, 2, 3, respectively. And A', B', C', and D' are all the hash of private index keys, which represent the addresses. Then, the process will continue to hash the address up to the root, then start to combine the pairs of hashes to narrow them down to get to the root. We cannot get back from the root.

Now, we got the root. This root is used directly in public mode as the MAM address; while in other modes, address = hash(root).

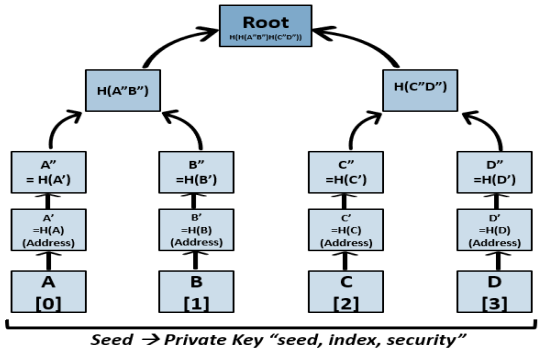

Figure 18 Merkle tree's root

3.9.6.2 Publish MAM Section

The MAM section consist of masked message that the publisher is about to publish his message, and the arbitrary-length ASCII code string. But it must be converted to tryte and stored as a tryte message before it is attached.

3.9.6.3 Publish MAM Section – Next Root

To post a message chain of masked messages of one generation, two Merkle trees must be created. The first Merkle tree is for the current generation, and the second one is for the next generation, as shown in Figure 19.

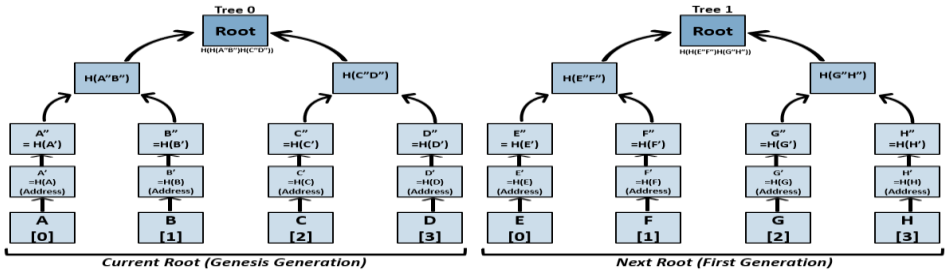

Figure 19 Publishing of next root

3.9.6.4 Publish MAM Section – Branch Index

The branch index is selected from the leaves' indices of the current generation's Merkle tree. In the illustration shown in Figure 20, the branch index will be index 0, 1, 2, or 3.

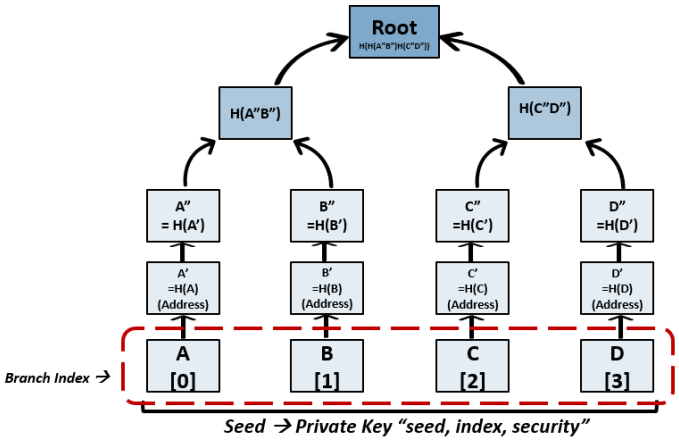

Figure 20 Publishing of branch index

3.9.6.5 Publish MAM Section – Siblings

As shown in Figure 21, if we assume branch index = 0, from the address (A') we can obtain the root without knowing all other leaves B', C', and D'. In leaf A', B" and H(C"D") are required to find the root. Those B" and H(C"D")

are named siblings of A'. Different branch indices have different siblings according to them.

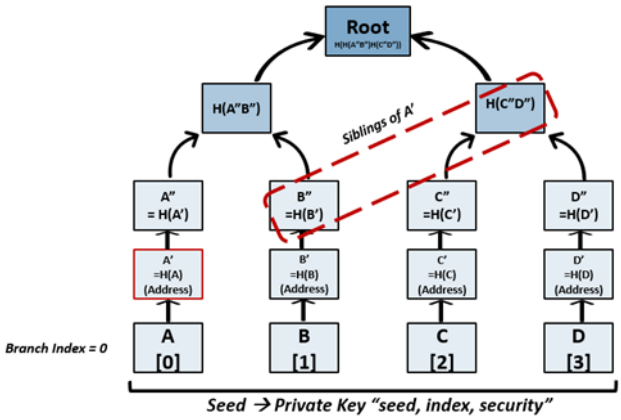

Figure 21 Publishing of siblings

3.9.6.6 MAM Completed

In the MAM section, the message trytes consist of NextRoot, siblings, and branch index. These message trytes are encrypted with the root if they are in the public mode or encrypted with the sideKey if they are in restricted mode. Figure 21 is an example of the restricted mode encryption section in MAM.

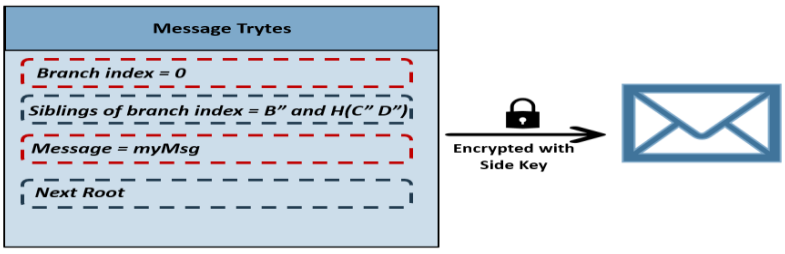

Figure 22 Restricted mode encryption section

3.9.6.7 Signature Section – Signing

As mentioned earlier, publishers add their signatures to the bundle to

check the validity of the MAM section. The signature is located inside the message fragment, and the transactions are named in the signature section inside bundle. The signature of the masked message is a private key that created from key (seed, branch_index, security). The messageTrytes of the MAM section is the signed data. The signing process consists of the following points:

1) Create a private key from the seed

2) The length of private key = security * 2187 [trytes].

3) Private Key is partitioned into N segments, where N = security * 27 [trytes]. So, each segment would be 81 [trytes].

4) Each segment is hashed 26 times.

5) Hash all segments in their entirety. The product is known as the digest. Every chunk of 27 segments is hashed and concatenates everything precisely. There are thus two chunks for security = 2, each containing 27 segments, thus we have segments from 1–27 and from 28–54. They are separately hashed to produce two 81 [trytes] digests, then concatenated to obtain one final 162 [trytes] digest.

6) Hash the digest once. The product is called the address, as shown in Figure 22.

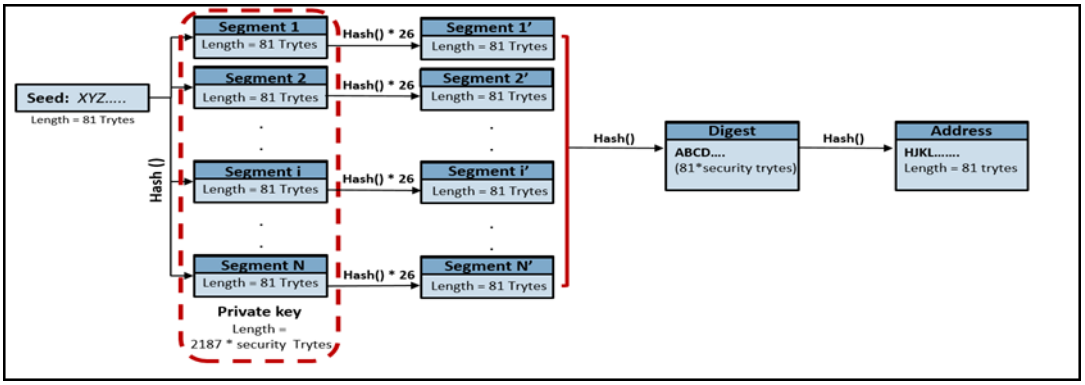

Figure 23 Generating address from seed

3.9.6.8 Multi-sig

Multi-sig only differs in the length and creation of the signature. If large amounts of money are transferred, especially those involving exchange security, it is worrying that only one seed is responsible for the transfers. Multi-signature transfers are sent securely by requesting multiple co-signers. Although multi-sig transfers are created differently from ordinary individual transfers, they appear to be the same when attached to the tangle, and people cannot distinguish between multi-sig attached transfers (= bundle) and others. The address generation in multi-sig is the same as the basic address generation mechanism described in the previous section.

3.9.6.8.1 Multi-sig Address

Figure 24 shows an example of a multi-sig mechanism where Alice and Bob want to create an account for their balance. Neither knows the other's own unique seed. First, they create the Multi-sig Address, which looks like 81 trytes to any tangle viewers, but which is generated differently. In this case, two digests, one for Alice and one for Bob, are used when generating a multi-sig address (of two people). They can select their own index and security level

individually and then submit their own digest.

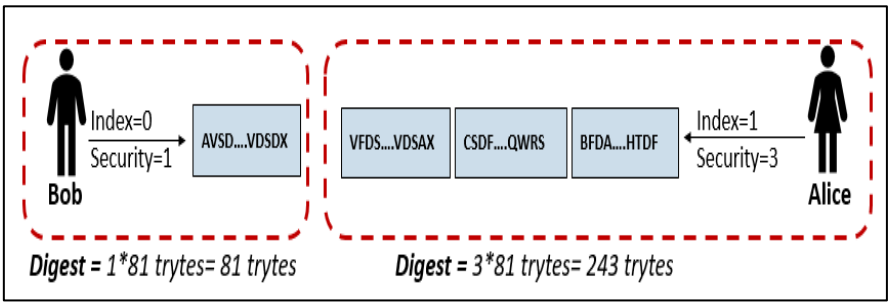

Figure 24 Generating multi-sig address

Be aware that you can share your digests publicly. But, like always, never share seeds. They can combine the two digesters submitted for a longer digest. The new digest appears as a security digester with value equal 4. Then, the digester must create an address using the same method as used in ordinary address generation. Remember that the final address always has 81 trytes, regardless of how long the original digest is. This is a multi-sig address. In short, two different digests, each created by two separate seeds, are seen as one digest. And from the digest the address will be generated. You can generate an address that requires more than two co-signers if you concatenate more than two digests.

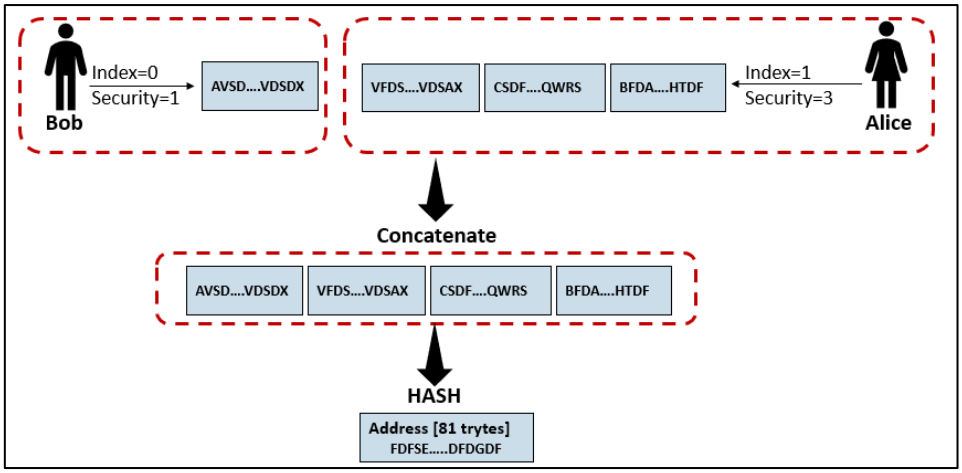

Figure 25 Combining two digesters

3.9.6.8.2 Signing Multi-sig

Assume we want to send from a multi-sig address. Sending from a multi-sig address is just the same as ordinary sending, except that sending from an ordinary address requires a single signature, while a multi-sig address literally requires multiple signatures. Multi-sig is produced with the private key itself. This process is no different from the normal signing procedure described in this thesis. A bundle hash (normalized hash of bundles) is generated by signed data. Co-signers create the same bundle hash signature. Let's assume that we are sending x [Mi] IOTAs from a multi-sig address "XYX..." with y [Mi] IOTAs total balance to the address "ABC..." of a receiver, as shown in Figure 26. The change of balance used to receive the change is not automatically generated by a multi-sig transfer, as one needs to have several digests from different individuals to produce the next address. So, we have to make sure all the next digests with the next index of co-signers are ready to create the next address before transferring the multi-sig address input. We can also choose any ordinary address if we no longer need our modification to be sent to multiple numbers.

Now, we have the signatures of two co-signers. In Figure 26, Alice's signature is 6561 Trytes and Bob's is 2187, so Alice has Security equal to 3. In total, four signatures are stored in the bundle object "8748(6561 + 2187) Trytes." Four comes from 8748/2187, where every signatureFragment is 2187 Trytes for one transaction object. And the order is important because Alice's digest is before Bob's digest, so the bundle should be signed into the order. For the actual tangle, viewers cannot distinguish between security equal to 4 from two multi-sig co-signers (security equal 1and 3) and security equal to 4 (two security equal to 1 and a security equal to 2) from three co-signers.

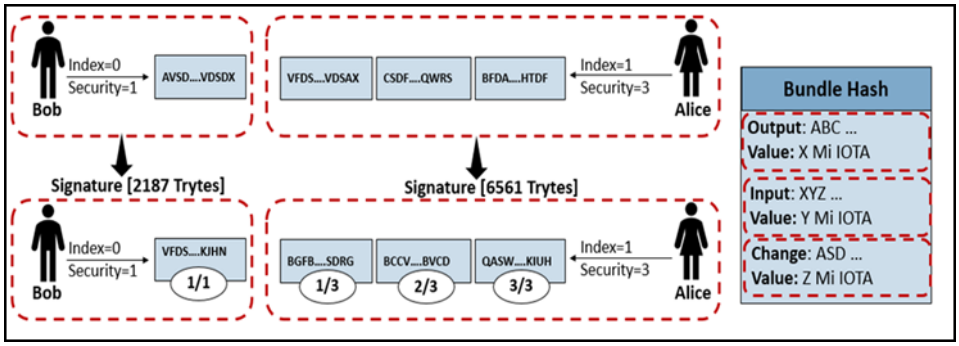

Figure 26 Signing multi-sig address

3.9.6.8.3 Validate Multi-sig Address

On the tangle, it seems as if the multi-sig bundle created from the single signature is attached. Only the length of the signature part is different. The multi-sig bundle of people whose security equal (1, 3) may be validated as one signature bundle of security equal to 4 (1 + 3) when validating, where a different level of security creates a different length of the signature (security level × 2187 Trytes).

3.9.7 Fetch Message

To get a masked message, root and sideKey are needed in the case of restricted mode, or only the root in the case of public mode. First, find the root's address and search for the address bundle. Then, use method to decrypt the messageTryte that is found in bundle's MAM section. The decryption key in public mode is the root itself; in restricted mode is the sideKey. Now, we have several messages (decrypted data, NextRoot, siblings, and branch index). The next step is to check the decrypted message's validity by using the section of signature to verify the messageTryte of the bundle's MAM section as signed data. The process of validation was already discussed in the previous section. After the validation process, the address you get is the leaf address of the branch index of the Merkle tree, which is combined with the siblings to calculate the tree's root, called the temporary root. If the temporary root is the same as the given root, this decrypted message is a valid channel message. If not, the owner (= seed owner) will not publish it.

3.10 MAM Conclusion

Masked Authenticated Messaging method is the most powerful module in IOTA and opens a new area of use in IOTA technology use-cases. The security and control of data integrity is a required for such things as data markets, fog analysis, verifying the supply chains, insurance company services, etc...

CHAPTER 4: CASE STUDIES AND EVALUATION

4.1 Overview

To model the functionality of IOTA and its behavior, I captured various use case scenarios for testing the viability of IOTA. The first case study, “Preliminary Investigation in Healthcare Community”, shows the difference between two different technologies with the same concept of decentralization (IOTA and Blockchain). The other case studies implement the MAM technology as a second-layer data communication protocol that is discussed in Section 3.9 with different data types (data, images, and videos), which allows users to transmit and access an encrypted data stream that consist of messages through zero-value transactions in the tangle.

4.2 Proposed System and Technical Details

The IOTA tangle is an important technology where its innovatory work in data supervision and share can solve some of healthcare’s looming problems. In healthcare, critical information is broadcasted across many nodes, and sometimes these nodes may not be available when one requires it the most. The existing healthcare structure has often been observed as insufficient to hold information exchange.

According to my research, one of the major things that makes the use of the IOTA tangle revolutionary in healthcare is a weak central administrator. If the database is stored in the physical drives of a specific system, anyone gaining access to that system could tamper with the database. When the IOTA tangle comes up, there will be no requirement for a central administrator, but the information will be distributed across the nodes due to IOTA technology’s distributed approach.

Since healthcare systems interact with private patient records that requires quick actions, and mostly works in a critical and real-time environment, the efficiency, security, and speed of accessing records are key factors when designing any healthcare

system. All of these factors can be achieved through IOTA tangles.

Overall, an IOTA system designed for accessing, monitoring, and storing healthcare providers information is implemented in a laptop computer with the following system specifications:

• Intel® Core™ i7-6600U CPU 2.60 GHz processor;

• 8.00 GB installed memory;

• 64-bit Windows 10 operating system;

• 7.03/4.14 (Download/Upload) Mbps link speed; and

• IPv6, among others.

Table 1 summarizes these properties.

Table 1 Operating System Properties

Property	Type
Processor	Intel Core i7
RAM	8 GB
System Type	64-bit

4.3 Case Study 1: Preliminary Investigation in Healthcare Community

The decentralized Tracking System is a great use case for deploying the distributed ledger technology as a based solution that can help in streamlining the process. Since patient records are still not used in an efficient manner by previous technologies, they lead to procedural incurring in time and costs. Accordingly, by executing the IOTA technology solution over blockchain technology, all the parties included will gain the benefits in terms of time, cost, and better organization of the

valuable medical services records.

4.3.1 Case study

First, the concerned General Doctor will open the communication link between parties by adding them as neighbors to the list of neighbors to his node in order to broadcast the transaction, as shown in Figure 27. In this case study, the General Doctor sends a request to the Laboratory for the required preliminary test as per his diagnosis for a specific patient using the patient address/seed. This address/seed is an identity for this patient inside the tangle/blockchain. Subsequently, the Laboratory sends the test results back to the tangle/blockchain on the same patient seed/address. Accordingly, the General Doctor can refer the patient either to the required Specialist or to the Surgeon for further investigation.

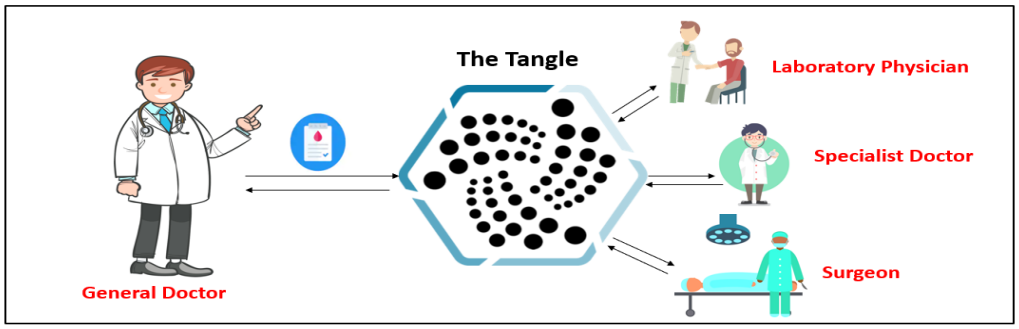

Figure 27 Preliminary investigation use case

4.3.2 Results

I applied the case study in two different DLTs: IOTA and Blockchain and recorded the results in Table 2. The average time it takes to send and fetch a particular transaction to/from the tangle, as shown in Table 2, is approximately 1.9 seconds, while the average time to send and fetch a particular transaction to/from the blockchain, as

shown in Table 2, is approximately 21.3 seconds.

The difference in the execution time of this test case between the two technologies clearly shows that the IOTA technology is a viable as well as a feasible technology that undoubtedly can change the operations of the healthcare industry for a better future in terms of speedy and reliable operations.

Table 2 Comparison Between IOTA and Blockchain in Terms of Sending/Fetching Transaction.

Trial No.	IOTA Execution Time (sec.)	Blockchain Execution Time (sec.)
1	3.7	52.0
2	2.4	13.0
3	2.0	9.0
4	1.8	11.0
5	2.2	32.0
6	1.3	27.0
7	1.1	10.0
8	1.2	15.0
9	1.7	21.0
10	1.5	23.0

Figure 28 shows the huge difference between the two technologies in one plotted graph.

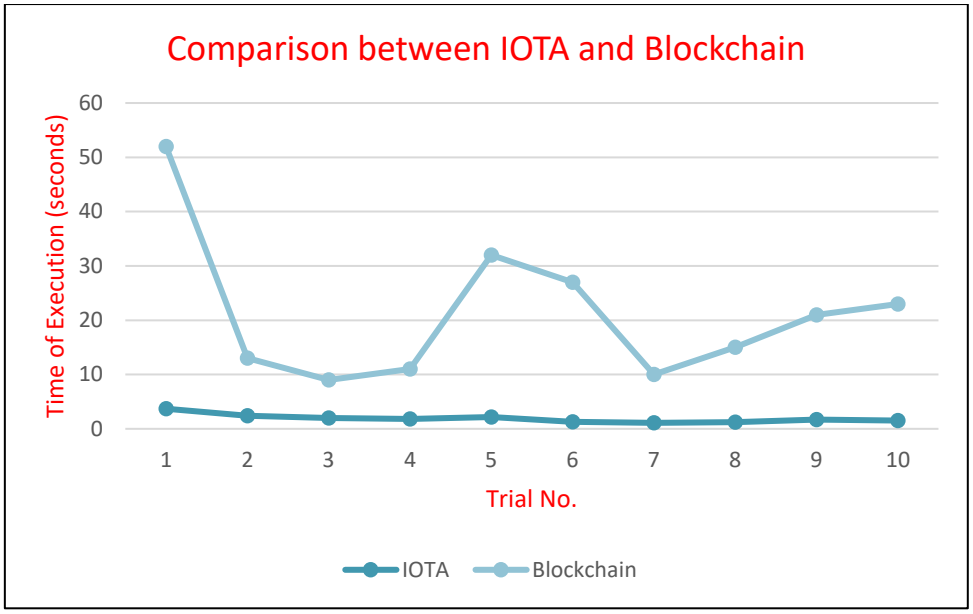

Figure 28 Comparison between IOTA and blockchain

Also, Table 3 shows the difference in terms of cost, where the Ethereum transaction involves a transaction fee of 0.01 USD based on the last reading on 5 April 2019.

Table 3 Comparison Between IOTA and Blockchain in Terms of Cost

Cryptocurrency	Cost (USD)
IOTA	0
Ethereum (Blockchain)	0.01/transaction
Bitcoin (Blockchain)	0.44/transaction

As discussed in Chapter 3, the tangle is built on a DAG data structure, which means that instead of constructing a chain of blocks where blocks are added after collecting a number of confirmations, the tangle can achieve transactions with no transaction fees. Also, as the tangle grows and more users perform transactions, the

entire system becomes faster and more secure. Further, a consensus in Blockchain is achieved through a very complex mechanism whereby parties are competing with each other and the goal is to add the next block to the Blockchain to win the reward, which in this case is requires some transaction fees. This mechanism involves the client server approach of blockchain technology, making it dependent on the specific route and database (centralization). When it comes to IOTA, instead of having everyone competing to generate a new block on the blockchain to win the reward, IOTA allows every participant in the network to actively participate in the consensus by letting every node reference two previous transactions directly and indirectly access the sub-tangle. All of this allows IOTA to have concurrent validation and keep the network decentralized. This also allows for no mining and no transaction fees.

4.4 Masked Authenticated Messaging Case Studies

Given that MAM is a lightweight protocol for data transmission over a distributed ledger, used for broadcasting sensitive data. A system that could transmit different types of data from wearable devices and unwearable devices using the MAM method was implemented. Finally, the MAM JavaScript wrapper was used to populate the MAM dataset structured in JSON format.

Every use-case was configured to spread data through a restricted MAM mode with sideKey that could be defined by a patient. If a patient would like to give permission to the doctor(s), he could share his channel keys with them. In return, the doctor could request the associated data stream(s) from the tangle. If a patient would like to cancel the access to his channel, he could simply change his MAM channel's sideKey and share it to his healthcare provider. In the following sections 4.4.1, 4.4.2, 4.4.3, and 4.4.4, four different case studies of the MAM method are presented.

4.4.1 Case Study 2: Broadcasting and Retrieving Blood Pressure (BP) Data for Home-Patient Tracking Through the Tangle

High blood pressure affects approximately 1 billion people and is assessed to cause 7.5 million deaths worldwide, but about 18.5% of people with high blood pressure are ignorant of their condition [62]. Blood pressure normally rises and falls throughout the day, but it may lead to heart and other related health problems if it remains high for a long time.

4.4.1.1 Case Study

I have created a clean interface using the JavaScript programming language to view a patient's blood pressure using historical patient data, as shown below. This specific study allows the systolic and diastolic blood pressure to be tracked in a real-time environment.

The MAM method fits best here, as it will save all records with their time stamps and without any manipulation. This optimal privacy mechanism lets the doctor easily monitor the records via the chain root, as shown in Figure 29.

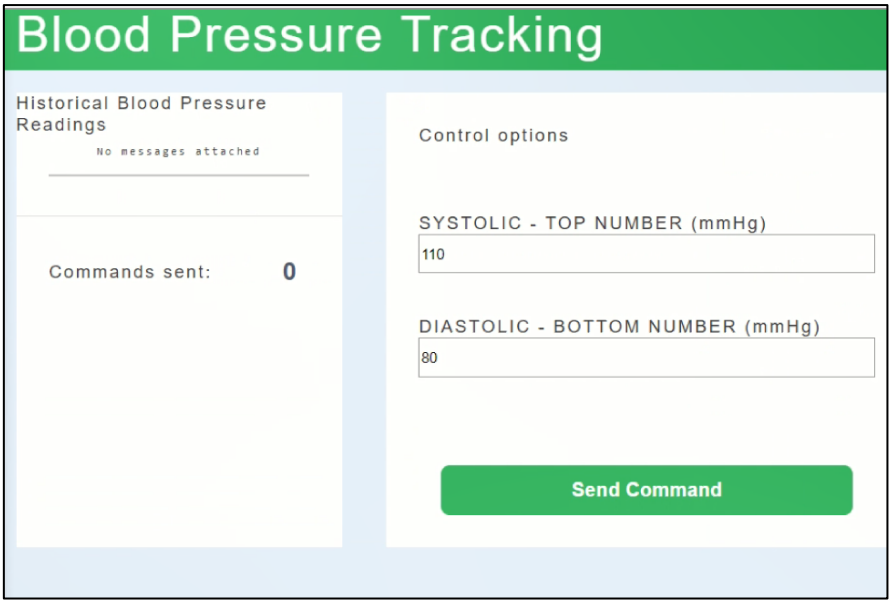

Figure 29 Blood pressure tracking interface

As shown in Figures 30 and 31, the total number of readings entered into and attached to the tangle is 4, and the root address of each transaction is displayed in the Doctor's node side for the retrieval of the results. As the doctor picks the transaction root address, he will be able to see the specific record as well as its succeeding ones. Further in, comes a particular scenario as shown in Figure 31, in which there are four total transactions, but the total number of root addresses shown in the Doctor's node is 5. This is precisely due to the fact that the last address to access the future transactions is already available.

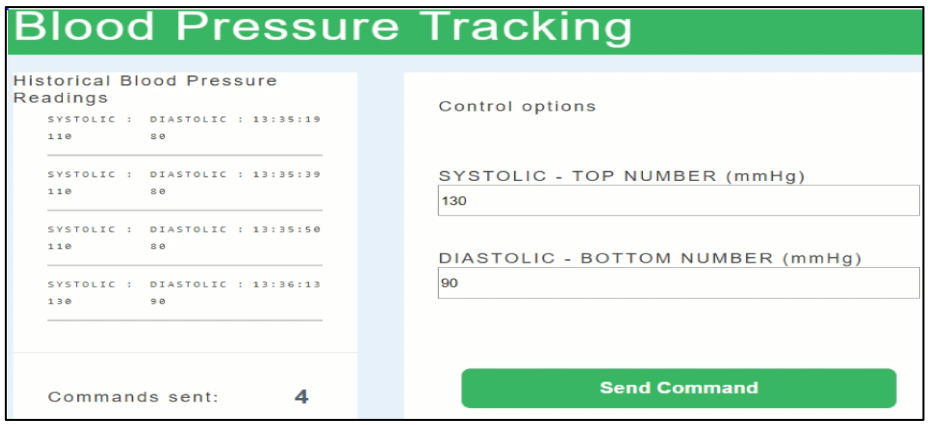

Figure 30 Blood pressure with patient entries

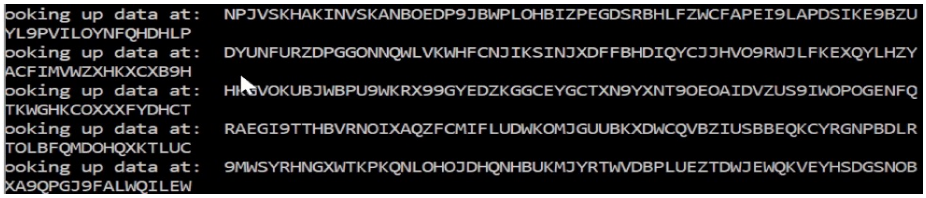

Figure 31 Root address of each entry in doctor's side

4.4.1.2 Results

This test case was run almost 10 times to validate the practicability of using MAM to get the expected results. The findings were excellent in terms of execution time and performance, as shown in Table 4. The average time of sending/fetching transactions to/from the tangle was 0.71s.

Table 4 Sending BP Records to Tangle

Trial No.	IOTA Execution Time (sec.)
1	1.0
2	0.6
3	0.9
4	0.6
5	0.8
6	0.7
7	0.4
8	0.6
9	1.0
10	0.5

4.4.2 Case Study 3: Broadcasting and Retrieving Instantaneous Activity of ECG Signals from Wearable Devices Through the Tangle

An ECG signal is a sequence of time series that clarifies the electrical impulses from the myocardium. An ECG signal is recorded from many conductors that are attached over the skin. Using MAM in this test case proved to be an efficient solution. Calling the root of any transaction will retrieve the ordered sequence of all the following transactions as a chain without the need to use an extra algorithm for ordering the ECG signals.

4.4.2.1 Case Study

The case study of an ECG signal was programmed in JavaScript and compiled as a JSON file. The ECG reading were stored in the same file, and the

records were retrieved from the 12 wearable sensor patches on a patient. This file was called every 10 seconds through the tangle, as shown in Figure 32. Each transaction contains information of 12 channels' readings, plus the root address, which can be used later by the Doctor. If the Doctor uses the first root address, the result of this test case will return the information of this particular address and all the subsequent information that comes after this address, as shown in Figure 33.

Figure 32 Sending ECG records from 12 channels to tangle

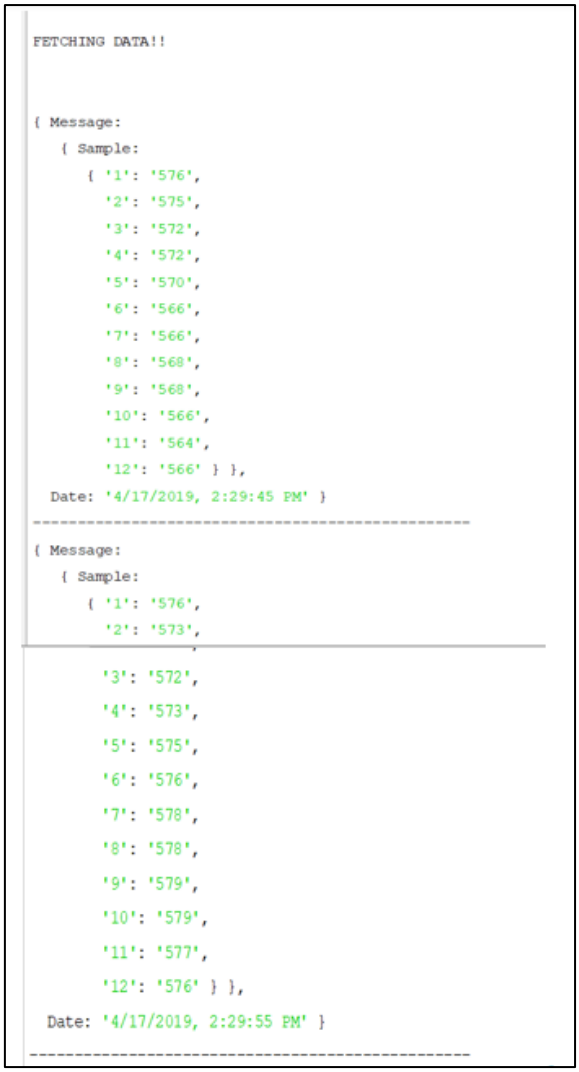

Figure 33 Fetching ECG records from tangle

4.4.2.2 Results

It was observed that the time taken to store the transactions (ECG patient data) in the tangle was the same as the time taken to call any specific record with required appended records, as shown in Table 5. The average time of sending/fetching ECG signals to/from the tangle in 10 trials was 0.6s.

Table 5 Sending/Fetching ECG Records to/from Tangle

Trial No.	IOTA Execution Time (sec.)
1	0.8
2	0.6
3	0.7
4	0.9
5	0.6
6	0.4
7	0.5
8	0.5
9	0.6
10	0.8

The same scenario was conducted in blockchain by Shen et al. [66] and on the Azure cloud platform by Hsieh et al. [65]. Figure 34 shows the comparison between Blockchain, Cloud and IOTA in terms of cost required.

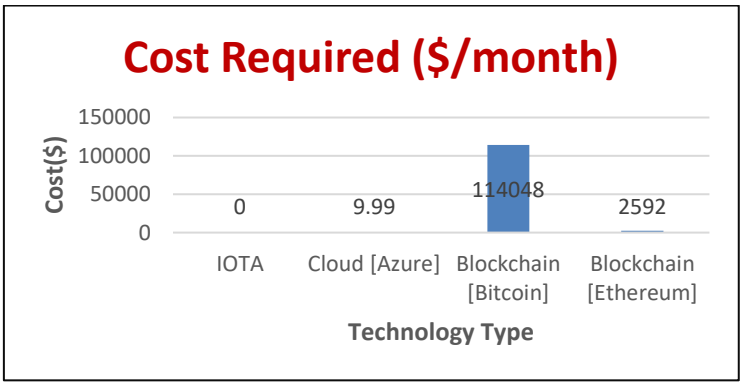

Figure 34 Comparison in terms of cost required

It is noticeable that IOTA has a much lower execution time compared to the other platforms, and it is the most cost-effective. And in terms of security, it also has an advantage because of MAM's nature. Also, a comparison was conducted between the platforms in terms of their scalability, as shown in Figure 35. The scalability issue is conceptually fixed with IOTA, in that the more transactions there are, the more the system can handle [48,63,64].

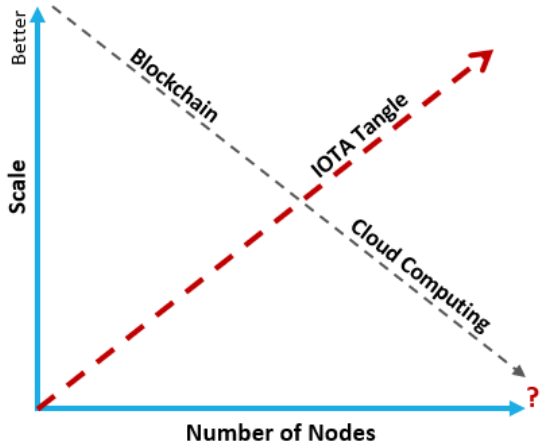

Figure 35 Comparison in terms of scalability

Also, as shown in Figure 36, I tested the same test case for different time intervals and found that the longer the time interval, the lower the percentage of failure for a transaction to attach to the tangle. The y-axis shows the percentage of failed transactions to attach to the tangle in 10 trials, while the x-axis shows the time interval between sending two transactions to the tangle. The blue line represents the feasibility of IOTA over time. However, a failed transaction will not come to a halt; rather, it will immediately reattach itself to the tangle. In this test case, all the failed transactions attached themselves to the tangle on the second attempt only, as shown in Figure 37.

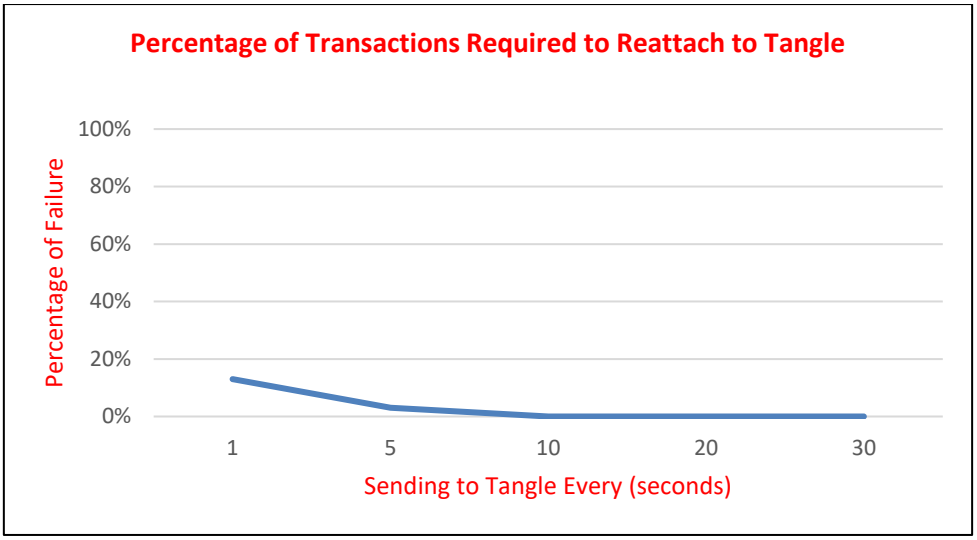

Figure 36 Percentage of transactions required to reattach to tangle

Figure 37 Failed to attach message

4.4.3 Case Study 4: Broadcasting and Retrieving of Medical Imaging Services Through the Tangle

Because of the centralized approach of client-server technology that the healthcare community is currently following, storage space has always been an issue. Unfortunately to make the work smooth and hassle-free requires frequent maintenance and upgrading of the systems. This of course demands more effort and a larger budget. Also, due to the distributed/parallel architecture of the servers laid out, the information remains scattered, which in turn adds to the processing time for any transaction. For

example, primary care providers, physicians, and imaging services are rarely located in the same place, which makes it more difficult to compile and access the information about a specific patient.

This presents a series of challenges for security and performance. Also, the lack of a better system has even resulted in the sharing of medical images through physical media. However, sending physical storage media by mail or in the patient's hands poses an obvious risk of loss or theft, which compromises the patient's privacy. In addition, proprietary wrappers and encryption can make the DICOM-standard files useless when received on the provider's side. For all these concerns, switching to a reliable technology through decentralized systems, especially to the MAM method, could be one of the best if not the best solution.

4.4.3.1 Case Study

Figure 38 explains how IOTA could help in storing images in the tangle by converting images to base 64 and then applying a segmentation process that includes N chunks. Each chunk contains 1600 bytes, as the IOTA transaction accepts up to a 1600-byte transaction size. Each chunk of text data will be broadcasted as an independent transaction. The root of the first transaction will be sent to the Doctor's node, and this particular root will help him retrieve the rest of the chunks of data and order them into the actual transmitted image.

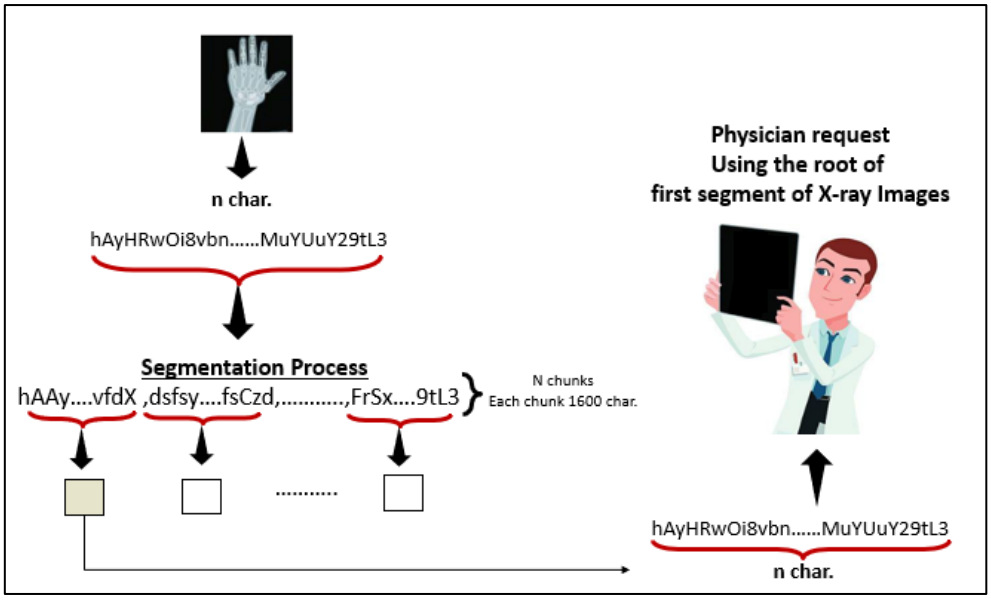

Figure 38 Storing/Retrieving images in/from tangle

4.4.3.2 Results

Table 6 shows the time required to fetch an x-ray image from the tangle and execute it. The same case study was repeated 10 times in order to guarantee the consistency of the results obtained from this use case. This analysis found evidence of how IOTA is viable in this sector.

Table 6 Sending/Fetching Images to/from Tangle

Trial No.	IOTA Execution Time (sec.)
1	0.7
2	0.4
3	0.9
4	0.8
5	0.9
6	0.6
7	0.5
8	0.6
9	0.7
10	1.1

The average time required to send/fetch images from the tangle, including the process of segmentation/combination, is 0.7 seconds, which is very efficient.

4.4.4 Broadcasting and Retrieving Activity of Video Streaming Through the Tangle

The existing video-streaming methods have incrementally increased the expenses to store all those massive video files on servers. This is due to the fact that these companies are using huge amounts of resources to store the data. Thus, these companies are in real need of a solution to significantly decrease the cost incurred and to design a robust solution for the security of the highly sensitive data. The DLT is a good solution to tackle this issue but using the blockchain technology will not be an effective solution to hold the video-streaming due to the long confirmation time needed

for each block and limited computing capacity. Hence, IOTA with the MAM method is the best fit.

4.4.4.1 Case Study

Tangle technology using the MAM method promises to reduce these expenses and provide content makers direct access to their income. The tangle also pledges to provide a multitude of avenues for storing the video data and distributed under a strongly encrypted and secure system. This case study was programmed in the JavaScript programming language.

As Figure 39 shows, the video will be divided into frames. Each 10 milliseconds, the program will take a snapshot from the video stream, then each frame will be converted into base-64 format and get appended to the JSON file inside the program. This process will apply to all the content/frames. Finally, the JSON file will contain all frames in base-64 format. A segmentation algorithm will be applied to this JSON file, and each segment will be sent as a standalone transaction. Foremost, when the Doctor requests this part, he will call the first segment of the first frame; then, the inverse process will start to compile the chunks of data together. After that, the segmentation process will be applied to the combined string to separate the file into frames. These segments will contain the common string that will aid in rearranging the segment to its original form. This will happen by searching the common string (img/jpeg;base64,). Finally, a conversion from base-64 format to images will be processed.

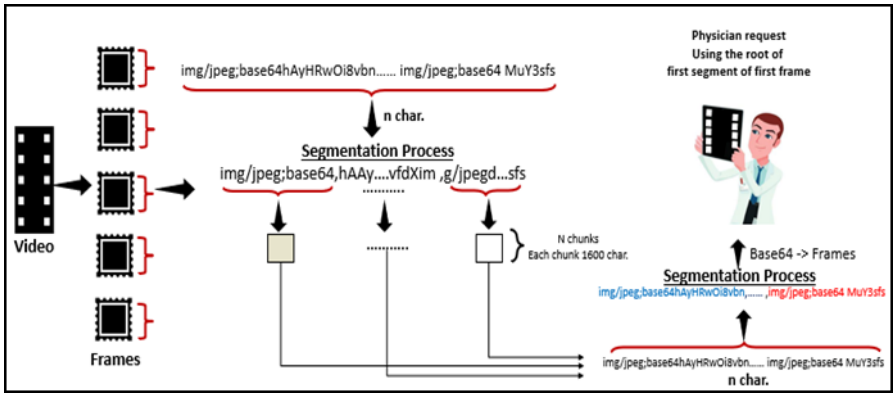

Figure 39 Storing/Retrieving videos in/from tangle

4.4.4.2 Results

Table 7 shows the execution time of fetching the frames from the tangle and compiling them back to their original state. As shown in the table, the average time taken to fetch all the required frames from the tangle was approximately 2.27 seconds, which means the audited section will be received on average 2.27 seconds later.

Table 7 Sending/Fetching Video to/from Tangle

Trial No.	IOTA Execution Time (sec.)
1	2.2
2	1.3
3	2.3
4	3.1
5	3.3
6	1.7
7	1.9
8	3.1
9	2.0
10	1.8

4.5 Results Conclusion

Until now, IOTA has been in its initial state of development and deployment, but if utilized and implemented in communities that require efficiency, reliability, and security, it will certainly revolutionize the technology of such sectors or communities.

CHAPTER 5: CONCLUSION, CONTRIBUTION, AND FUTURE WORK

5.1 Main Conclusion

IOTA distributed ledger networks are an opportunity to overcome the interoperability challenges that medical professionals in the electronic healthcare community are currently facing. Along with the applications suggested by the research results, IOTA is well positioned to tackle complex issues ranging from insurance processing to sharing digital healthcare data in a reliable and secure manner. This is made possible because of the nature of IOTA in using a quantum-proof cryptography that even quaternary computers cannot break. This research could very well be the first step toward achieving a distributed ledger based EHR infrastructure with the potential for a reduced transaction rate, scalability, the ability to realize micropayments, efficiency, verifiable security against manipulation, etc.

5.2 Contribution

Though the idea of using the IOTA technology in the healthcare industry is yet in the incubation stage, preliminary analysis suggests that tangles are worth implementing as an upcoming technology. Comparatively, the test cases run across the platforms proved that the IOTA technology could stand against all odds in terms of feasibility, reliability, and robust data security.

Usually, with the advent of a new technology, the focus is on its practicability in a manner that would help in overcoming the flaws of the technologies currently being used. I experienced the same flaws in the healthcare industry, and after thorough research, I was moved by IOTA's immense distributed ledger and tamper-proof scalability. Obviously, it wasn't easy to try a technology in its initial phase of deployment, but it was the essence of this technology that made me explore it to its

fullest.

IOTA being a brand-new platform, the resources for its implementation were quite scarce. It was an uphill task for me to get the resources intact, but my motivation led me to explore more into the core library of IOTA, and the results were satisfying.

5.3 Future Work

Seeing the remarkable results of this technology in this phase of implementation in the healthcare sector, I am planning to extend this application to wrap up all the annexes of healthcare.

REFERENCES

[1] Guy Yeoman, Patricia Furlong, Michael Seres, Helena Binder, Helena Czhung, Vincenzo Garzya, and Rachel RM Jones. *Defining patient centricity with patients for patients and caregivers: a collaborative endeavor*. BMJ Journal, 3(2). 2017.

[2] Martin Makary, and Michael Daniel. *Medical error—the third leading cause of death in the US*. BMJ Journal, 535. 2016.

[3] Roger Collier. *NHS ransomware attack spreads worldwide*. CMAJ Journal, 189 (22). 2017.

[4] Pierre Yong, Robert Saunders, and LeighAnne. *The Healthcare Imperative Lowering Costs and Improving Outcomes*. 1 edition. 2011.

[5] Jianli Pan, and James McElhannon. *Future Edge Cloud and Edge Computing for Internet of Things Applications*. IEEE Internet of Things Journal, 5(1). 2017.

[6] Saurabh Kumar, Sneha Poddar, R. Marimuthu, S. Balamurugan, and S. Balaji. *A review on communication protocols using internet of things.* ICMDCS, INSPEC No. 17448507. 2017.

[7] Wade Trappe. *The Challenges Facing Physical Layer Security*. IEEE Communications Magazine, 2015.

[8] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffery Voas. *DDoS in the IoT: Mirai and Other Botnets.* IEEE Computer Society, 50(7). 2017.

[9] Harald Sunmaeker, Patrick Guilemin, Peter Friess, and Sylvie Woelffle. *Vision and Challenges for Realizing the Internet of Things*. CERP-IoT. 2010.

[10] Aitor Goiri, and Diego Ipona. *On the complementarity of triple spaces and the Web of Things.* WoT ’11, Article No. 12. 2011.

[11] Hong Liu, and Huansheng Ning, *Cyber-Physical-Social Based Security Architecture for Future Internet of Things*. Advances in Internet of Things, 02(01).

2012.

[12] Rodrigo Roman, Jianying Zhou, and Javier Lopez. *On the features and challenges of security and privacy in distributed internet of things*. Computer Network, 57(10). 2013.

[13] Sara Amendola, Rossella Lodato, Sabina Manzari, Cecilia Occhiuzzi, and Gaetano Marrocco. *RFID Technology for IoT-Based Personal Healthcare in Smart Spaces*. IEEE Internet of Things Journal, 1(2). 2014.

[14] Fang Hu, Dan Xie, and Shaowu Shen. *On the Application of the Internet of Things in the Field of Medical and Health Care*. 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, INSPEC No. 13972209. 2013.

[15] Rodrigo Roman, Jianying Zhou, and Javier Lopez. *On the features and challenges of security and privacy in distributed Internet of Things*. Computer Networks, 57(10). 2013.

[16] Kai Zhao, and Lina Ge. *A Survey on the Internet of Things Security*. 2013 Ninth International Conference on Computational Intelligence and Security, INSPEC No. 14128983. 2013.

[17] Arbia Sfar, Enrico Natalizio, Yacine Challal, and Zied Chtourou. *A roadmap for security challenges in the IoT*. Digital Communication and Networks, 4(2). 2018.

[18] Marco Leo, Federica Battisti, Marco Carli, and Alessandro Neri. *A federated architecture approach for IoTs security*. 2014 Euro Med Telco Conference. INSPEC No. 14838150. 2014.

[19] Rolf Weber. *Internet of Things – New security and privacy challenges*. Computer Law & Security Review, 26(1). 2010.

[20] S. Sicari, A. Rizzardi, L. Grieco, and Coen-Porisini. *Security, privacy and trust*

in Internet of Things: The road ahead. Computer Networks, 76(15). 2015.

[21] M. Farooq, Muhammad Waseem, Anjum Khairi, and Pakistan Mazhar. *A critical Analysis on the Security Concerns of Internet of Things (IoT)*. International Journal of Computer Applications, 111(7). 2015.

[22] Rodrigo Roman, Pablo Najera, and Javier Lopez. *Securing the Internet of Things*. Computer Journal, 44(9). 2011.

[23] David Airehrour, and Jairo Gutierrez. *An analysis of secure MANET routing features to maintain confidentiality and integrity in IoT routing*. International Conference on Information Resources Management. 2015.

[24] Mohammed Abdmeziem. *Data Confidentiality in the IoT*. Phd dissertation. 2016.

[25] Charith Perera, Prem Jayaraman, Arkady Zaslavsky, Peter Christen, and Dimitrios Geo. *MOSDEN: An Internet of Things Middleware for Resource Constrained Mobile Devices*. 2014 47th Hawaii International Conference on System Sciences. INSPEC No. 14179146. 2014.

[26] Mahmoud Elkhodr, Seyed Shahrestani, and Hon Cheung. *The Internet of Things: New Interoperability, Management and Security Challenges*. Networking and Internet Architecture. 2016.

[27] Joshua Cooper, and Anne James. *Challenges for Database Management in the Internet of Things*. IETE, 26(5). 2009.

[28] Safdar Shaheen, Muhammad Yousaf, and Mudassar Jalil. *Temper proof data distribution for universal verifiability and accuracy in electoral process using blockchain*. 2017 13th International Conference on Emerging Technologies (ICET). 2017.

[29] Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system*. Ed, White Paper, 2008.

[30] Victoria Lemieux. *A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation*. 2017 IEEE International Conference on Big Data (Big Data). INSPEC No. 17504673. 2017.

[31] Agniva Banerjee, and Karuna Joshi. *Link Before you Share: Managing Privacy Policies Through Blockchain*. Cryptography and Security. 2017.

[32] Yvo Desmedt. *Public Key Cryptography - PKC 2003*. 6th International Workshop on Practice and Theory in Public Key Cryptography. 2003.

[33] Matthew Sleiman, Adrian Lauf, and Roman Yampolskiy. *Bitcoin Message: Data Insertion on a Proof-of-Work Cryptocurrency System*. 2015 International Conference on Cyberworlds (CW). INSPEC No. 15757432. 2015.

[34] Roehrs A, Costa CA, and Rosa Righi. *OmniPHR: A distributed architecture model to integrate personal health records*. Journal of Biomedical Informatics. Vol. 77. 2017.

[35] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*. 2017 IEEE International Congress on Big Data (BigData Congress). INSPEC No. 17188683. 2017.

[36] Weizhi Meng, Elmar Tischhauser, Qingju Wang, Yu Wang, and Jinguang Han. *When Intrusion Detection Meets Blockchain Technology: A Review*. IEEE Access, Vol. 6. 2018.

[37] Eli Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Lan Miers, Eran Tromer, and Madars Virza. *Zerocash: Decentralized anonymous payments from bitcoin*. 2014 IEEE Symposium on Security and Privacy. INSPEC No. 14773620. 2014.

[38] D. Wood. *Ethereum: A secure decentralised generalised transaction ledger*.

EIP-150. 2016.

[39] CERP-IoT cluster. *Visions and Challenges for Realising the Internet of Things.* European Commission. 2010

[40] Aaron Wright, and Primavera Flippi. *Towards Blockchain-Based Intelligent Transportation Systems*. IEEE 9th International Conference. 2016.

[41] Zibin Zheng, Shaoan Xie, Hong Dai, and Xiangping Chen. *Blockchain challenges and opportunities: A survey*. Work Pap. 2016.

[42] Maria Borge, Eleftherios, Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, and Bryan Ford. *Proof-of-Personhood: Redemoctratizing Permissionless Cryptocurrencies*. IEEE European Symposium. 2017.

[43] Leslie Lamport, Robert Shostak, and Marshall Pease. *The Byzantine generals problem.* ACM Trans. Programming Language, vol. 4. 1982.

[44] Hyperledger Project, 2015.

[45] David Mazieres. *The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus*. Stellar Development Foundation. 2015.

[46] David Schwartz, Arthur Britto, and Noah Youngs. *The Ripple Protocol Consensus Algorithm*. White Paper. 2014.

[47] Lakshmi Sankar, M. Sindhu, and M. Sethumadhavan. *Survey of Consensus Protocols on Blockchain Applications*. Advanced Computing and Communication Systems, 4th International Conference. 2017.

[48] Marco Conoscenti, Antonio Vetro, and Juan Martin. *Blockchain for the internet of Things: A systematic literature review*. AICCSA. 2017.

[49] Jesse Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. *Where Is Current Reseach on Blockchain Technology?- A Systematic Review*. PLOS ONE. 2016.

[50] Guy Zyskind, Oz Nathan, and Alex Pentland. *Decentralizing Privacy: Using Blockchain to Protect Personal Data*. Security and Privacy. 2015.

[51] V. Buterin, *Ethereum White Paper*. Ethereum White Pape. 2009.

[52] Nurzhan Aitzhan, and Davor Svetinovic. *Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams*. IEEE Transactions on Dependable and Secure Computing. 15(5). 2016.

[53] G. Karame. *On the security and scalability of Bitcoin's Blockchain*. 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016.

[54] Serguei Papov. *The Tangle*. White paper V.1.4.3. 2018.

[55] J. Pro. *IOTA, a popular cryptocurrency: the growth sustains*. Cryptocurrencies, ICO-Initial Coin Offerings. 2019.

[56] Outlier Ventures. *Token Ecosystem Creation*. Project. 2016.

[57] Marcella Atzori. *Blockchain-based architectures for the Internet of Things: a Survey*. SSRN Electronic Journal. 2017.

[58] Guald, Ancoina, and Stadler. *An Arbitrary Scalable, Energy Efficient and Anonymoud Transaction Network Based on Colored Tangles*. CryptoGuru PoC SIG. 2017.

[59] Bridget Martin, Frank Michaud, Don Banks, Arsalan Mosenia, Riaz Zolfonoon, Susanto Irwan, Sven Schrecker, and John Zao. *OpenFog Security Requirements and Approaches*. 2017 IEEE Fog World Congress. 2017.

[60] Rafi Hanifatunnisa, and Budi Rahardjo. *Blockchain based e-voting recording system design*. TSSA. 2018.

[61] Junaid Chaudhry, Ahmed Ibrahim, and Ali Bashir. *Internet of Threats and Context Aware Security: Part Two*. IEEE Internet Initiative eNewsletter. 2017.

[62] George Papathanasiou, Efthimia Zerva, Ooannis Zacharis, Maria Papandreou,

Effie Papageorgiou, Christina Tzima, Dimitris Geogakopouls, and Angelos Evangelou. *Association of High Blood Pressure with Body Mass Index, Smoking and Physical Activity in Healthy Young Adults.* Cardiovascular Medicine Journal. 2015.

[63] Shoaib Hassan, Asim Kamboh, and Farooque Azam. *Analysis of Cloud Computing Performance, Scalability, Availability, and Security*. ICISA. 2014.

[64] Laurence Tennant. *Improving the Anonymity of the IOTA Cryptocurrency*. White Paper. 2017.

[65] Jui-chien Hsieh, and Meng-Wei Hsu. *A cloud computing based 12-lead ECG telemedicine service*. BMC Med Inform Decis Mak. 2012.

[66] Bingqing Shen, Jingzhi Guo, and Yilong Yang. *MedChain: Efficient Healthcare Data Sharing via Blockchain*. Applied sciences. 2019.

[67] Kurt Stange. *The Problem of Fragmentation and the Need for Integrative Solutions*. Annals Family Med. 2009.

[68] Bozena Poksinska. *The current state of Lean implementation in health care: literature review*. Iww journals. 2010.