Secured IOTA Enabled Micropayment Transaction Crypto-Platform with Discretionary Mining Capabilities and Miner Nomination Based on First-Price Sealed Bid Auction Theory

by

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
Brac University
December 2019

Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

H.M Sadman Amin 16101008	Zahin Sufiyan 17201033
Nakhla Rafi 16101197	Syeda Afrida Anjum 16101059

Approval

The thesis/project titled "Secured IOTA Enabled Micropayment Transaction Crypto-Platform with Discretionary Mining Capabilities and Miner Nomination Based on First-Price Sealed Bid Auction Theory" submitted by

1. H.M Sadman Amin (16101008)
2. Zahin Sufiyan (17201033)
3. Nakhla Rafi (16101197)
4. Syeda Afrida Anjum (16101059)

Of Fall, 2019 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on December 24, 2019.

Examining Committee:

Supervisor:
(Member)

Dr. Golam Rabiul Alam
Associate Professor
Department of Computer Science and Engineering
BRAC University

Head of Department:
(Chair)

Dr. Mahbubul Alam Majumdar
Professor
Department of Computer Science and Engineering
Brac University

Abstract

The commercial utilization of cryptocurrency as a digital asset in being more and more sought-after on each successive year. Most of the well renowned crypto-platforms now-a-days are devised based on the premise of the concept of blockchain. These cryptocurrencies work as an alternative medium of exchange using cryptography to secure the transactions on a distributed ledger. For validating a rationally substantial transaction, all of the blockchain-based cryptocurrencies requires a miner who will execute the proof-of-work to secure network consensus even in the presence of malicious nodes. After solving the cryptographic hash puzzles, the mining nodes are then compensated with a block reward and a mining/transaction fee for their services. When using regular blockchain-based digital cryptocurrency such as bitcoin, ripple, etherium etc. most of the time the respected crypto-platforms discourages low valued transactions from being executed. Because often, the transaction fee may exceed the value of the product or service that are being purchased. As a result, for this particular reason, micropayment systems using digital crypto-platforms remains largely under developed. To solve this complication our thesis model was emanated from the notion of IOTA, which is considered as a minerless cypto-platform where the requisition of miners are disregarded thus enabling users to relish the advantages of microtransactions, however with the inclusion of "Discretionary mining". "Discretionary Mining" refers to the hypothesis of availability of mining capabilities at the discretion of the users. While using IOTA, the efficiency of the Tangle network largely depends on the computational power of nodes. Moreover, unconfirmed transaction node also known as "Tips" with low computational capability may not be able to validate it's previous two transactions in time which will result in the degradation of the entire Tangle. Hence, our research of Discretionary Mining was derived from the postulation of distributive computing where a low powered smart device can outsource complex computations while validating transactions such as solving cryptographic puzzle (Hashcash) which they cannot execute on their own. Thus enabling users to reap the benefits of microtransactions without the network being completely minerless.

Keywords: Crypto-Platform, Micropayment, Minerless, Discretionary Mining, IOTA, Tangle, Distributive computing.

Acknowledgement

First and foremost, praises and thanks to the Almighty Allah, for His gift of knowledge and good health that he bestowed upon us throughout our research. Our greatest and most sincere gratitude goes towards out research supervisor Dr. Golam Rabiul Alam for giving us the opportunity and immensely providing us with his invaluable guidance throughout the research. In addition to being an outstanding teacher his vision, integrity, resilience and sincerity have deeply inspired all of us. He has always challenged us to think outside the box and push ourselves to our absolute limit. Without his counsel, our thesis would not have turned out as we had hoped it would be. It was an outright privilege and honor to work under his guidance.

We would also like to thank our respected Brac University for always providing us with the necessary facilities, equipment and resources during our research period. We would like to extend our deepest thanks to all the faculty members of CSE department. Without their precious lessons they taught us throughout our entire undergraduate period, we would not have been here today.

Last but certainly not the least, we are beyond grateful and indebted to our beloved parents for their love, compassion and all the sacrifices they went through to give us a fighting opportunity in life and preparing us for the future. We are exceedingly thankful to all our peers and fellow classmates for their love, support and getting us through the all tears and hardship. Life wouldn't have been the same without their presence.

Table of Contents

List of Figures

Nomenclature

The next list describes several symbols & abbreviation that will be later used within the body of the document

BTC Bitcoin

DAG Directed Acyclic Graph

$FPSB$ First-Price Sealed Bid

LTC Litcoin

$P2P$ Peer to Peer

PoS Proof of Stake

PoW Proof Of Work

$SHA256$ Indian Premier League

TPS Ethereum

XRP Ripple

Chapter 1

Introduction

1.1 Background

The origination of cryptocurrency can be considered one of the most emerging and inescapable technologies of the 21st century. Cryptocurrency is basically an internet-based digital asset or a medium of transaction which uses cryptographic functions to ensure transactions between parties. In the early 1990s, the "Cypherpunks" who laid the first bricks to the foundation of the creation of cryptocurrency thought that the government and related governing organizations possess too much surveillance and authority over people's lives and their information. As certainly not being the admirer of centralized bureaucracy, these cypherpunks wanted to use cryptography to allow the people to have more control over their money and their own transaction information. It would have been much later in 2009, when the first ever decentralized digital cryptocurrency named bitcoin was introduced for the first time by satoshi nakamoto which was inspired by the early works of the cypherpunks and thus a new form of decentralized digitized form of transaction was inaugurated. So as we can all expect one of the most alluring aspects of cryptocurrency is that it is not controlled by any kind of governing body whatsoever. It does not have a central server or a point of control. As a result, it can be theoretically considered as immune to any kind of government interference and jurisdiction. This decentralization factor allows the entire network to be distributed among thousands of servers and computers. Another one of the other important characteristics cryptocurrency is it's P2P (peer to peer) nature. The transaction always takes place between only involved parties. There are no trusted third party such as a bank to accredit the transaction. Furthermore, all of the digital crypto-platforms are known for their pseudonymously. Pseudonymously basically means that users don't have to share their personal information in order to own a digital asset, although all of the transactions made by the user are made public to all the people in the network. Almost every cryptocurrency in the market today runs on the blockchain network. The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value [15]. A blockchain is a time-stamped chain of blocks. Each blocks hold a series of data according to it's usage and information about transactions. Apart from the engraved data a block also contains it's own unique identifier called the hash and also carries the hash of its previous block. So if a malicious user tries to tamper with a block in the blockchain, in the process he will change the identifier hash of the

affected block and as a result, the block ahead can identify the presence of malicious user. In addition to that, as blockchain is a distributed ledger which means all the documents about transactions are replicated several times with each update and are sent to every cryptocurrency holder in the network. Each user connected to the network has a copy of the entire chain. So if someone wants to tamper with any block the whole network will not reach consensus and as an output it will reveal that a hacker is trying to get in. One of the most significant key players of the blockchain are the miners. Each time a transaction is made between users, those transactions are tallied and verified by the crypto miners. Their responsibility is to authenticate if every information is in-order. This process involves solving some complicated puzzles involving cryptographic hash functions associated with each transaction block. The hash value is basically a fixed length numeric value. The miner uses various algorithms, in the case of bitcoin it is SHA 256 (Secured hashing Algorithm 256) to zero in on a hash value which is less than the target. After authentication, the miner then adds the block to the blockchain which contains a proof-of-work POW and updates the ledger. Lastly among all the miners, the first one to solve the puzzle and commence verification, is rewarded with a physically minted reward block also known as a transaction fee. This reward block is paid by the vendors who participated in the transaction. The reward of mining a block is currently 12.5 bitcoin [30].

1.2 Research Problem

After the successful invention of Bitcoin in 2009, the flood gates were opened ushering in a new wave of new cryptocurrencies to the digital currency market. Today, some of the most well-known cryptocurrency that has good share value are Bitcoin (BTC), Litcoin (LTC), Ethereum (ETH), XRP, Bitcoin cash, etherium classic etc. All of these digital currencies were constructed upon the concept of Blockchain structure described above. These blockchain based cryptocurrencies are bound to use the ministration of miners who will validate and verify a secured transaction between the users of the network and for theirs service the miners took a portion of the transacted bitcoin as their block reward also known as a transaction fee. Although most of the digital payment portals we use which are blockchain based are pretty efficient when we are considering large transactions because in these types of situation the mining fees are quite negligible. Be that as it may, these crypto-platforms face a crucial challenge when it comes to micropayment transaction.

By definition, a micropayment transaction refers to any sort of economic transaction that is relatively small in asset value. Typically these type of microtransaction can even be reduced to a value of a fraction of dollar. In terms of digital cryptocurrency, microtransaction is posing as a pivotal defiance because of the high transaction fees confiscated by the crypto-miners. When using regular blockchain-based cryptoplatforms such as ripple, ethereum and even bitcoin, the payment portals do not allow micropayment transactions. Because often, the transaction fee dictated by the miners may exceed the value of the product or service being purchased. For example, if a person wants to purchase a dozen eggs from a grocery store using cryptocurrency, the grand total value of the eggs may cost even less than the value of transaction fee he has to give to the miner for approval. Due to the blockchain distributed ledger

structure, when considering for a micropayment transaction, using blockchain based cryptocurrencies can consume large quantities of time, money and make the overall system obsolete. Currently, the average transaction fee on the bitcoin network in $1.21 USD [10]. In short, it becomes increasingly unfeasible to process microtransaction using established cryptocurrencies accessible in the market today.

On top of that, another predicament that has been looming over the concept of blockchain based crypto-platform is the term scalability. Scalability refers to the number of transactions a system can withstand per unit time. Generally, scalability is denoted by TPS (Transaction per second). A system's Transactions Per Second rating is the number of transactions it can run per second and deliver one-second response time to 95% of the requests. As of 2019, Bitcoin has the capability of processing 7 TPS [22]. As we speak, along with the increasing number of users the bitcoin network is being more congested and with the growth of each users, the TPS is deteriorating. As a result, transactions take a long amount of time to process and transaction fees are pilling up as well. If cryptocurrency is ever to become a viable substitute to contemporary payment systems, a payment portal with a higher transactional throughput is a must.

For the sole purpose of enabling microtransaction to the proposed model, our research came across the implementation of IOTA in the world of crypto-platforms. In short, IOTA is a next-generation distributed ledger which was derived from the concept of blockchain structure but it is not typically considered a blockchain based platform. Rather than using a blockchain based structure IOTA introduced a new network core which is known as Tangle. The tangle network is virtually minerless so to speak. As having the alluring advantage of being minerless, it can be used to the enactment of a micropayment transaction model which our research initially aimed for. In spite of having the sheer edge of being virtually minerless, the Tangle also has some pitfalls. Inside the tangle network, because of the absence of miners, the responsibility of verifying a valid transaction falls on to the shoulder of the IOTA users (nodes) itself. As a consequence, a number of the connected users with low computational-powered hardware might cost a significant amount of time and money thus making the entire tangle incompetent.

1.3 Research Objective

The predominant objective and aspiration of our thesis research are as follows:

1. To propose a decentralized digital crypto-platform framework which will legitimize micropayment transaction (IOTA).

2. To construct a crypto-platform which will not only be implemented on a virtually minerless environment but simultaneously will also have partial mining capabilities at user's discretion.

3. To develop FPSB Auction Theory based miner appointment and nomination scheme.

The section below briefly discusses about the objectives and the procedures by which those objectives were met:
First and foremost, for ensuring the basic premise of our objective the proposed crypto-platform model will operate on IOTA environment. IOTA is one of the most highly revolutionary and talked-about decentralized distributed ledger that has surfaced in recent years. IOTA incorporates the utilization of an innovative technology called Tangle at its core. The Tangle is fundamentally a Directed Acyclic Graph (DAG) with a new composite network data structure. Other cryptocurrencies which are based on blockchain consists of transaction information clustered into a sequential chain of blocks. On the other hand, in IOTA tangle transactions are stored as a stream of individual transactions with are later entangled. The main advantage that IOTA holds over all other data structure is that in this network no additional miners are needed. Instead the users themselves will take the responsibility of mining and the process of verification. On account of being minerless, which is the foremost requisite of sanctioning micropayment transaction, our thesis aims to be implemented on IOTA tangle to meet our primary goal.

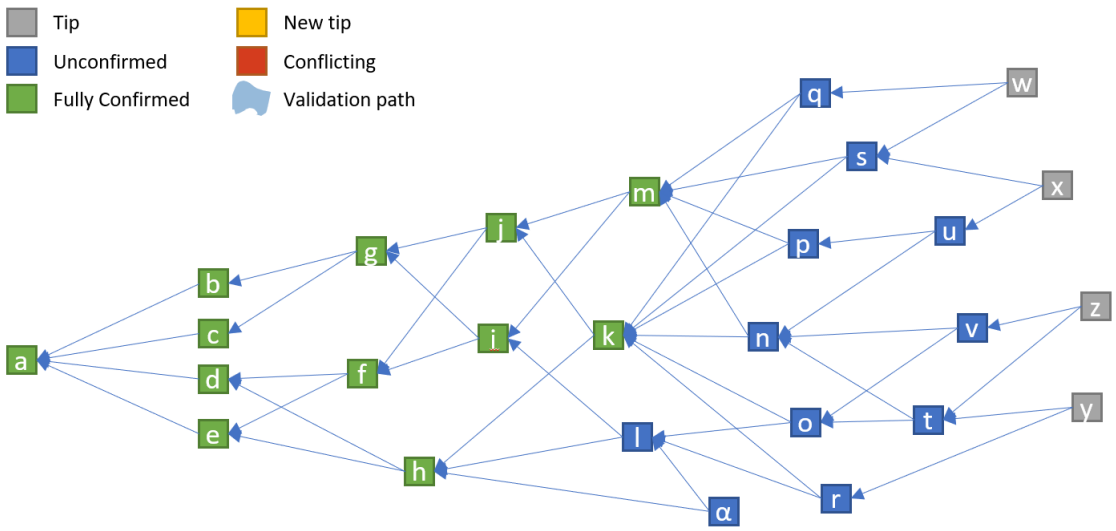

Figure 1.1: Visualization of IOTA Tangle[10]

The subsidiary aim of our thesis is to modify the IOTA Tangle by using the concept of distributive .computing. Distributive computing refers to a group of computers operating as a single system. This group of computers work as a combined team to solve complex problems quickly and efficiently. It consists of a Master Node (M) who will request the service of other Worker Nodes (W). The system can only operate under maximum one Master Node connected to several Worker Nodes Distributive computing allows nodes with comparatively low computational power to outsource complex computations which they cannot perform on their own. Utilizing distributed computing the proposed model will introduce miners on IOTA tangle.
Last but certainly not least, another one of the chief objectives of our thesis is the selection of miners from a vast group. Instead of outsourcing to an undefined number of miners, we tried to deplete the miner participation by defining specific number of required miners and a maximum amount of mining cost. The process of selecting miner was derived from FBSB auction theory. The FPSB auction theory refers to a type of auction theory where a maximum bid is published forehand. Bidders will

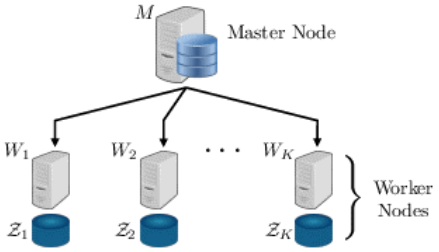

Figure 1.2: Visualizing Distributive Computing[29]

have access to the information of maximum bid and will submit their own bid in accordance. Submission of bid will be private and can only be done once, hence the name "First Price Sealed Bid". The bidder with the highest submitted bid will win. Inspired by FPSB auction theory, the proposed model suggests an algorithm which will entitle and nominate a specific number of miners.

1.4 Research Methodology

As designated in the title, this chapter covers the research methodologies implemented in the dissertation. Among numerous types of research, following only one dogma no longer served the purpose. As a result, the approach that we took is a sequential one. The main research methodology that was followed for the thesis was an inductive research that was later accompanied by a deductive one.

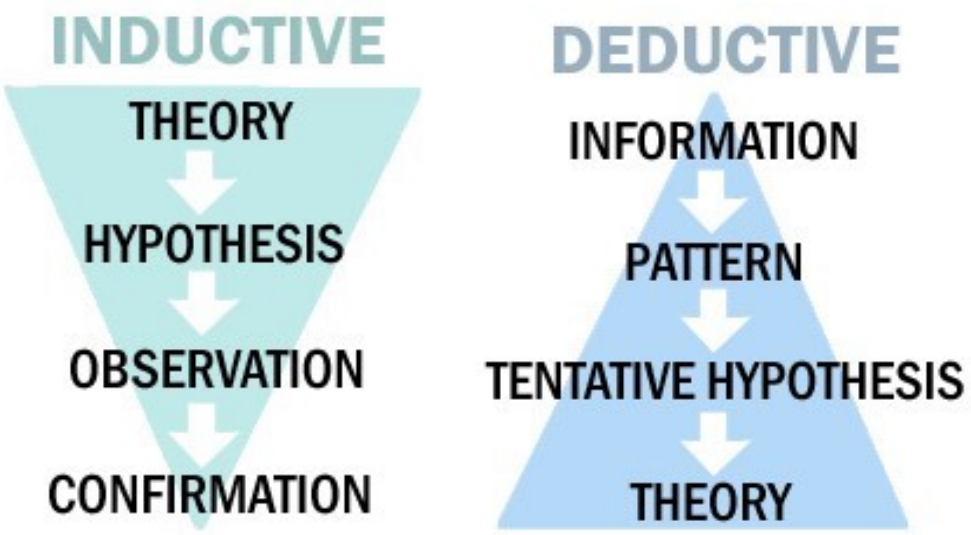

Figure 1.3: Sequential Research Process[36]

According to inductive research, researchers initiate their research based on specific observations. At the inauguration of our research, numerous pieces of previous papers that had a cryptocurrency background were thoroughly observed. At this point of research, our concepts regarding different current cryptocurrency such as bitcoin, litcoin, ripple and how they operate on a blockchain structured platform were legitimized. The research came across IOTA and the idea of introducing micropayment

transaction in crypto with help of a minerless Tangle network which was previously missing from other well established crypto-platforms. The main crucial objective of these inductive observations was to discover any drawbacks or limitation of the current cryptocurrencies. The second stage of inductive research was to observe a pattern among all of the previous academic researches based on the following dissertations. Consequently, the research realized a pattern of inefficiency in tangle network when it contains users with low powered smart devices. Afterwards, various conclusions were drawn from the inductive research and a generalized theory of "Discretionary mining" was developed.
At the second phase of our research, we took a rather deductive approach to solve the partial mining problem at hand. Deductive research/deductive reasoning begins with a theory, in our case that was the result of the inductive research. Deductive reasoning basically works to transform a theory from the more general to the more specific. Deductive research is also known as "top-down approach". At this stage, we started with the top which refers to the theory of "Discretionary mining' and attempted to develop a hypothesis based on the notion of distributive computing. Finally, an algorithm was formulated based on a popular auction theory named FPSB to execute the process of nominating miners as the outcome of our deductive research.

1.5 Scope and Limitations

To ordain the scope of the proposed system, the foremost task of our thesis model is to construct a microtransaction payment crypto-platform. The construction of such a crypto-platform necessitates a minerless environment. The reason behind making the proposed crypto-platform minerless was to eliminate transaction fee entirely. In search of such a minerless structure, our thesis scope expanded to a new project called "Project Amaranth" which was later renamed as IOTA. The solution that our proposed model desperately needed came in the form of a directed acyclic graph based data structure called the tangle. This allowed the research to break free from the existing blockchain based crypto-platforms. The tangle is a minerless network that works on CPU based mining. But instead of actual miners, the users are able to perform the task of mining to ensure their own transaction on the stream. Users only need to perform insignificant amount of hashing to verify two previous transactions which are also known as tips. In spite of having micropayment transaction enabled IOTA, it also contains some flaws. One of which is the reduction of TPS rate because of users with low powered hardware inside the tangle. The scope of the research extended furthermore as we found the principal contribution of the proposed thesis and that is to make alteration to IOTA in such a way that it will have partial mining capabilities with the help of external miners if the user with low computational power needs it.

To illustrate the limitations on the characteristics of design or methodology that impacted or influenced the interpretation of our thesis research, the prime candidate is the IOTA Corporation itself. After deducing the theory of "Discretionary mining based on FPSB auction" the thesis proposed a new algorithm to test it. Unfortunately the entire architecture upon which the tangle network operates on, was not made open-source by IOTA. As a result, when it came to the implementation of the

proposed algorithm instead of executing the algorithm on tangle network, our team had to experiment on a generalized blockchain network which was implemented with the help of JavaScript.

Another limitation the proposed crypto-platform faced is related to throughput limitation. Throughput limitation is directly connected to scalability issues. Other blockchain based cryptocurrencies are currently facing bottleneck issues with low TPS because of the increment of users. In a blockchain based cryptocurrency, a numerous amount of transactions are first inserted into a block that is inherently linear in fashion. After being verified by a miner each block is then added to the main chain every Y time. In terms of bitcoin, it currently takes about 10 minutes, and the amount of transactions that fit into each block only allows a current maximum of 7 TPS [5]. This creates a bottleneck issue. On the other hand, tangle does not have such a bottleneck issue in terms of the size of the network based on the increasing number of connected users. The tangle can be oversimplified by the term "the more the merrier" means the more users join the network it will become more and more efficient instead of causing a bottleneck. Because of this characteristic, theoretically it is considered that IOTA tangle can handle thousands of transactions per unit time. But there are some drawbacks to that theory as well. Among many differences with a blockchain based structure, one of the common factors between both structures is that both of them contains a distributed ledger. Each node in the tangle network has a copy of the ledger. Whenever a new transaction is added to the tangle, the network itself runs an algorithm to check and verify it against all the other ledgers of all the nodes of the tangle. When the data is consistent with all the other ledgers, only then can it reach complete consensus. As not all the nodes have similar computational capacity and suppose if there are a huge number of users in the tangle, it might take a considerable amount of time to finally process all the ledger for consistency and finally reach consensus. As a result, along with each increment of transaction the TPS will reduce more and more. This is known as throughput limitation. This is not necessarily a drawback of the tangle network rather it can be considered as a downside of the consensus algorithm which is followed by all of the distributed ledger based architecture.

1.6 Report Outline

The remaining section of the paper has been catalogued as follows. Chapter 2 presents related works and literature reviews loosely based on the dissertation. Moreover, the concepts of blockchain, byzantine Fault Tolerance Algorithm and the detailed process of consensus algorithm were thoroughly discussed on the section. Afterwards, the rise and pitfalls of various well established cryptocurrencies on the market today were described. Chapter 3 provides a thorough deep basic background of IOTA tangle. In this section, the core architecture of the tangle network and how it maintains a minerless environment are narrated considering all of the aspects. Afterwards, the working procedures of IOTA such as the process of validating a transaction by a user specific mining system and reaching consensus are also discussed. In addition to that, the chapter also focuses on distributive computing and how it can be used to outsource by a master node. Chapter 4 describes the platform we will use and it will further provide a detailed introduction and working proce-

dure of the proposed algorithm of "Discretionary mining Based on FPSB Auction Theory". Besides that this chapter illustrates the programming and implementation aspect of the algorithm. In chapter 5, a full representation of the evaluation of performance is recorded. This section basically portrays the experimental results and focuses on the higher throughput IOTA is gaining throughout the modification and implementation of introducing partial mining capability inside a minerless network. Finally, chapter 6 concludes with a discussion on some of the future limitations the system might face and also about further improvements that can be instigated.

Chapter 2

Literature Review

This chapter provides some basic knowledge about cryptocurrency, points out some widely accepted cryptocurrency, explains their mechanism and persisting problems related to these cryptocurrencies.

2.1 Literature Background

2.1.1 Concept of cryptocurrency

Cryptocurrency is a form of digital money that does not depend on the third party for it's process of transaction. It is totally a new concept and our modern economy is heavily dependent on it to make transactions more secure and efficient. Cryptocurrencies are not controlled by any central authority which allows two parties to make transaction directly without the need of any transaction fees. In the paper "Crytocurrencies: Market analysis and perspective" Giudic mostly focused on the emerging phenomenon of crytocurrencies Most of the cryptocurrencies depends on blockchain technology to gain transparency, decentralization and immutability. In a decentralized network, every node have a ledger that contains the list of all the transactions made previously on the network to determine whether the future transactions are valid or not [12]. In any peer to peer network, there are four big concerns- confidentiality, integrity, non-repudiation and authentication. These four concerns are maintained with the help of digital signature. To maintain confidentiality and integrity in cryptocurrencies, asymmetric key cryptography, which is also known as public key cryptography is used. To maintain integrity, the data is firstly signed. When node-1 wants to make transaction with node-2, at the very beginning node-1's hashed data is encrypted with it's own private key. Since node-1's public key can be attained by all nodes, node-1 later encrypt it with node-2's public key. When node-2 receive the data, it can decrypt with it's private key and again decrypt the data with Node-1's public key. These way of double encryption and decryption helps to provide confidentiality and authentication[17] [32]. The process is shown in figure 2.1:

2.1.2 Blockchain Technology Architecture

A blockchain is a continuous sequence of blocks which contains the list of all the transactions occurred in the network. Each block contains data and there is a

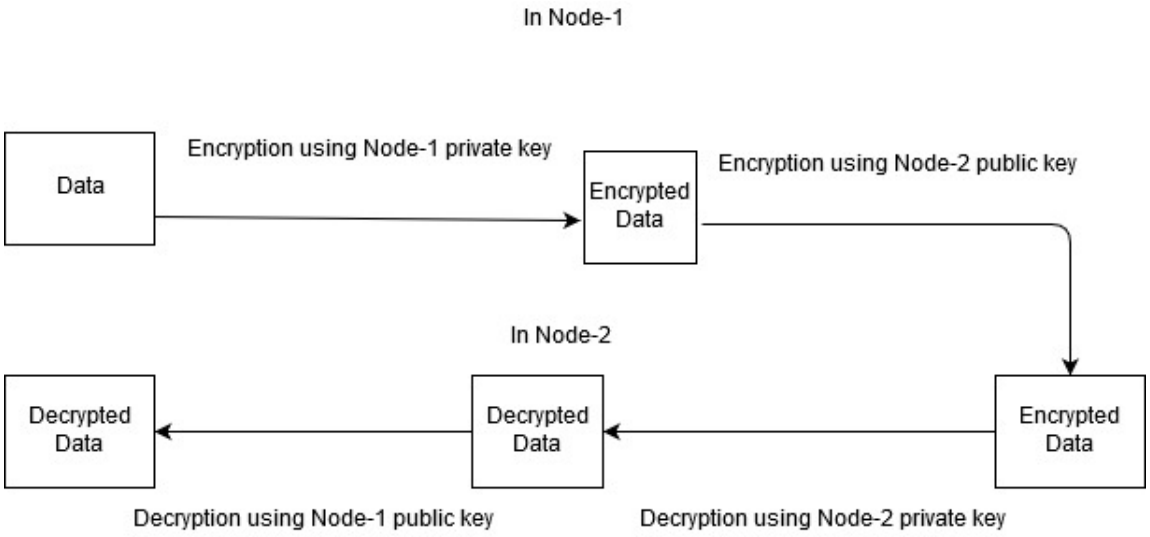

Figure 2.1: Digital Signature

separate block header for each block to uniquely identify the block. The block header which is exactly 80 bytes contains information like-timestamp (4 byte), version(4 byte), Merkle root(32 byte), difficulty target(4 byte), nonce(4 byte) and previous hash(32 byte). The timestamp is used to denote the time when the block was created. The concept of hash function is used in blockchain. Basically a hash function converts any length of data to a fixed length of numerical data. This fixed length of output depends upon which type of algorithm is used in the hash function, like- message digest (MD), Secure Hash Algorithm (SHA) etc. Every block contains transactions and each transaction has an individual hash value for it. With the help of Merkel Root Tree it is possible to generate a unique hash for every block. The very important property of hash is that even if the smallest part of the data change within a block, it produce a completely different hash output. In blockchain, every block contains the hash of the previous block to create a chain of blocks and the very first block in the blockchain is the genesis block whose previous hash value is 0. A very important property of blockchain which is immutability can be obtained with the help of hash, since if data of any block within the chain is change, the hash of that block also changes. This is return effect the later blocks as the hash of the later blocks need to be regenerated again to make it work properly[29][27].

2.1.3 Byzantine Fault Tolerant Algorithm

It was important to solve how the nodes within a distributed network agree on a decision when some of the nodes fail or act dishonestly. Byzantine General problem was explained simply with a group of generals attacking a city and need to have proper communication and agreement among them. If only a part of generals attack the city, the attack would fail. As blockchain is a distributed network and all the nodes have the same power in the absence of any central authority, Byzantine Fault Tolerant Algorithm ensures consistency is maintained in ledger of different nodes [18].

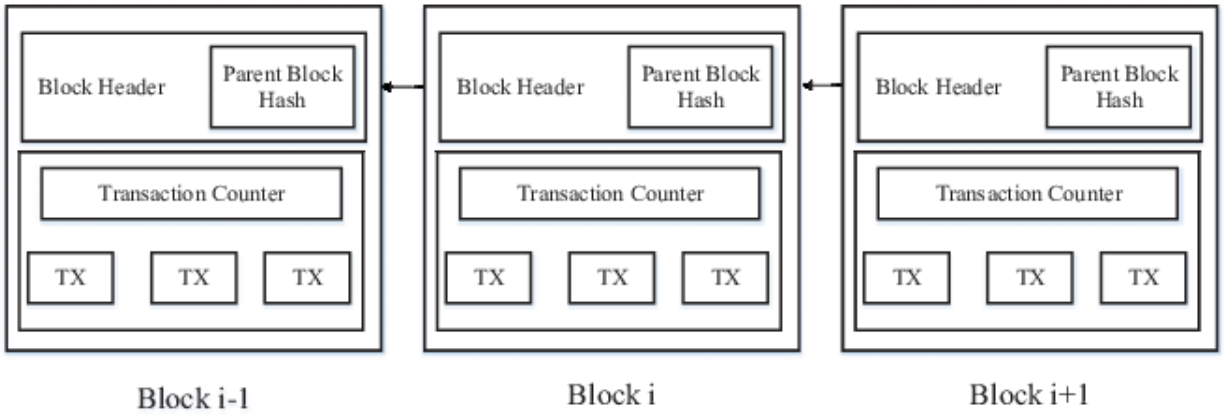

Figure 2.2: Sequence of blocks in a blockchain

2.1.4 Consensus

The concept of consensus comes when it is required to determine which node will add a new block in the blockchain among huge number of miners within a network and to ensure that the chosen one is not a malicious miner. There are different types of consensus like Proof-of-Work (POW), Proof-of-Stake (POS), Proof-of-Authority (POA) etc [29].

Proof-of-Work (PoW)

Proof-of-Work algorithm is the main basis of bitcoin. According to this algorithm, all the nodes within the network will have to perform some mathematical computation or solve cryptographic puzzle and the node which have the highest computational power and able to solve the puzzle will get the chance to add the new block. The miner will not only add a new block but will also be rewarded with some bitcoins according to bitcoin theory. This process of adding new block is called mining. If a node is using huge amount of computational power to add a new block, than the chances goes down that the node is a malicious software. The mathematical problem given to solve to the miners depends upon the size of the network, users active and blockchain size. In POW, the miners are basically calculating the hash value by changing the nonce frequently to get different hash value. There might be a case that two or more miners are able to generate the target value at the same time which would eventually lead to having branches within the blockchain. To avoid branching or fork problem, POW made a protocol denoting that the longest branch among them will be considered as the most authentic one and the other validated blocks within the shorter branches will switch to the longest one. In short it can be said that, mining requires a lot of work to be done, but it is ever easy to validate it. While mining, the miners try to find the hash of the block header by changing the nonce value and compare to check if it is smaller than the difficulty target[18][27].

Proof-of-Stake (PoS)

Proof of stake protocol is basically used in ethereum. In PoS, the nodes having more currencies get the chance to add block in the network. It is assumed that nodes having more currencies are less likely to attack the network. In Proof-of-Stake, a

validator is selected based on the combination of staking age, randomization and node's wealth. Cryptocurrencies using PoS usually start with PoW, later switch to PoS. Those nodes interested to be a validator, need to have certain amount of stake in the network. In order to prevent only wealthiest nodes in the network to become a validator certain method like Randomized Block Selection and Coin Age Selection are used. In Randomized Block Selection method a validator is chosen among nodes which have highest stake and lowest hash value. Again the Coin Age Selection method, node selection depend upon how long the token have been staked for. Coin age is calculated by multiplying the stake with the number of years they have been staked for. Once a validator has forged a block their coin age is set to zero and must wait for a certain period to forge a block again. If a node is chosen to be a validator in PoS, the node needs to check if all the transaction within the block is valid or not. The node receives reward which is basically the transaction fee, after adding the block on the blockchain. But the validator will have to lose a part of their stake if they approve any fraudulent transaction. For this reason, it can be said that executing attack is much more expensive in PoS. Moreover, this also helps to create trustworthy validators. Again if a node stops being a validator, then the stake and all the transaction fees that the node owned previously will be released after a certain time[12][7].

Proof-of-Authority (PoA)

Proof-of Authority provides an efficient solution for private blockchain network. It focuses on the validator's reputation rather than staking coins like PoS. In PoA, there are a limited number of validators and blocks are verified by preapproved nodes. According to this consensus, a validator need to disclose their real identity, invest money and put their reputation at stake. Although PoA is able to make more transactions per second compared to PoW or PoS, it sacrifices decentralization within the system. On the other hand, since the validator's identities are public, there is a scope for third party manipulation [21].

2.1.5 Ethereum and smart contract

Smart Contracts are applications or programs that contains a specific set of rules which are predefined by computer code. These codes are needed to be executed by all the nodes to keep the network secure. Blockchain smart contract use trustless protocol which ensures that if any condition within the smartcontract is not followed, the contract will not execute. A smartcontract is responsible to execute blockchain operation in an ethereum network. Ethereum is a blockchain based decentralized platform to run applications. Ethereum can process 15 transactions per second which is double than that of bitcoin. To run applications on ethereum network there is a separate type of cryptocurrency called ether. Ether is used to pay for transactions as well as to run computational services. Ethereum consumes tokens called gas to execute any operation on blockchain. So in short it can be said that ether buys gas to fuel up the EVM. Smartcontract of an ethereum network is made up of two public keys, one of which is made by the creator of the smartcontract and the other is the contract itself, and the contract code [18][8].

2.1.6 IOTA

IOTA (MIOTA) is a cryptocurrency based on a new data structure. This new data structure is known as "Tangle". It does not require blocks, chains and miners. Internet of Things(IOT) is one of the main applications of IOTA.

The main goal of the project was to create a convenient means of payment for the implementation of the futurological concept of the Internet of Things (IoT, "Internet of Things").

Developers created the "Tangle", a unique block-less technology. Which is miner free and thus IOTA can be a great way to solve things without miners.

The Tangle

Tangle works in a different way. There is a DAG(Directed Acyclic Graph) which is here called the Tangle. It uses a simplified version of blockchain. You have to verify two other transactions first, to send a transaction in the network. It needs a ledger for storing transactions. The transactions issued by nodes establish the site set of the tangle graph. Obtaining the edge sets are done in some different steps. First, as soon as a new transaction arrives it has to approve two previous transactions. The direct edges show the approvals(Figure 1). We say that A indirectly approves B if there is not a directed edge between A and B, but there is a directed path of at least two from A to B. There is a transaction which is called the "genesis" transaction. It is directly or indirectly approved by all other transactions(Figure 2). The genesis is described in the following way. In the beginning, the genesis transaction sent an address with a balance that contained all of the tokens which was sent by the genesis transaction to several other "founder" addresses. We say that all of the tokens were created in the genesis transaction. No tokens will be created in the future. Moreover, there will be no mining in the sense that miners receive monetary rewards "out of thin air".
Sites are basically the transactions represented on the tangle graph. Nodes issue and validate transactions. The user must work to approve other transactions and thus they are contributing to the network's security. It's also checked by the nodes if the approved transactions are having any conflict. If there are any conflicts including their previous activities, the node will not approve anything. When a transaction has received additional approvals, it is accepted by the system with a higher level of confidence. It becomes very tough to accept a double-spending transaction.There is no rules for choosing which transaction a node will approve.
For issuing a transaction a node has to follow some rules. Those are:

- Node has to choose two other transactions to approve according to an algorithm.
- The node checks if two transactions are conflicting. According to the negative results, it does not approve conflicting transactions.
- A cryptographic puzzle must be solved by the node for generating a valid transaction.

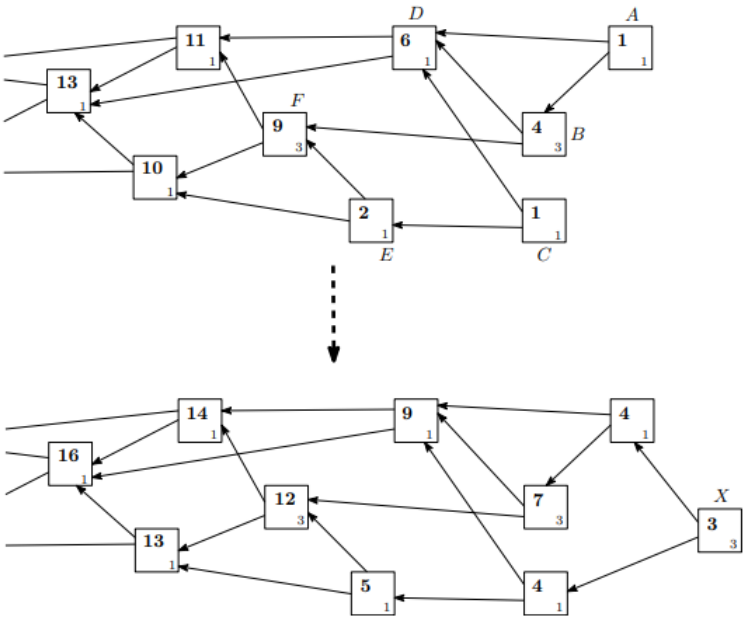

Figure 2.3: DAG with weight assignments before and after a newly issued transaction, X. The boxes represent transactions, the small number in the SE corner of each box denotes own weight and the bold number denotes the cumulative weight.[22]

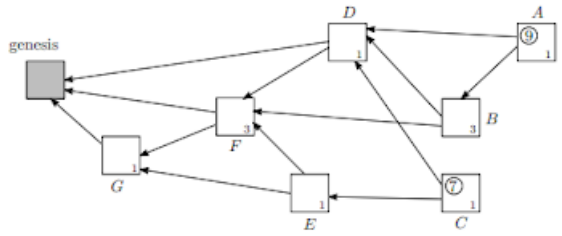

Figure 2.4: DAG with own weights assigned to each site, and scores calculated for sites A and C.[22]

One thing we need to know is iota network is asynchronous. Nodes do not see the same set of transactions. On the other hand, we already learned that the tangles may have conflicting transactions. The nodes don't necessarily need to know to have the consensus on which valid transactions can be in the ledger. All of them can be in the tangle. But, when there are conflicting transactions, the nodes need to decide which transactions will become a parentless child in which transactions are not indirectly approved by incoming transactions anymore. Nodes calculate how many new transactions are received from a neighbor. Neighbors drop a node if it is lazy. That is why a node still has incentive to participate even if it does not issue a transaction and has no direct incentive to share a new transactions.

A basic mathematical model can be used to describe Tangle. Let card(A) be a set. A graph be T = (V, E) where V is the set of vertices, E is the set of edges and $v \epsilon V$. For any u,v V, we say that u approves v is u,v E and there must be a directed path

from u to v. If degin(w) = 0 it means no edges point to w. Then, w V can be said to be a tip. Any vertex should have at most two outgoing edges, i.e degout(v) = 2. degout() = 0 (this vertex is called the genesis or start node). All v V have an oriented path with .

The state of tangle at time $t >= 0$ is T(t) = (VT(t), ET(t)). Initially, VT(0) = and ET(0) = null. Tangle grows with time such that VT(t1) VT(t2) and ET(t1) ET(t2) whenever 0 t1 ¡ t2. If a new transaction v arrived at time t', then VT(t'+) = VT(t') v and ET(t'+) = ET(t') U (u,v'),(u,v"). [8] How does a new arrived transaction choose which two vertices in the tangle will it approve? Tangle uses Random Walk Monte Carlo algorithm to do this task.

Weights

The weight of a transaction is proportional to the amount of work that the issuing node invested into it. . In the IOTA model implementation, the weight may only assume values 3n̂. Here "n" is a positive(n¿0) integer that belongs to some nonempty interval of acceptable values. Every transaction has an attached positive integer, its weight. Transaction with a larger weight is the most important thing. There is no need to worry about the smaller weight. To avoid spamming and other attack styles, it is assumed that no entity can generate a bunch of transactions in a short period of time with weights.
"Cumulative weight" of a transaction is defined as the weight of a particular transaction plus the summation of all transactions' own weights that directly or indirectly approve this transaction. In figure 1 the boxes are basically the transactions and the small-sized numbers inside the boxes are basically the own weights of the transactions. For instance, transaction F is approved by transactions A, B, C, E. It can be directly or indirectly. Here, the cumulative weight of F is 9 = 3 + 1 + 3 + 1 + 1.

Tips

The unapproved transactions are called the tips. For example, in fig:3.3 transaction number 6 is a tip. The reason is that it is not approved yet. Each incoming transaction needs to choose two tips to approve. This is a very important step.

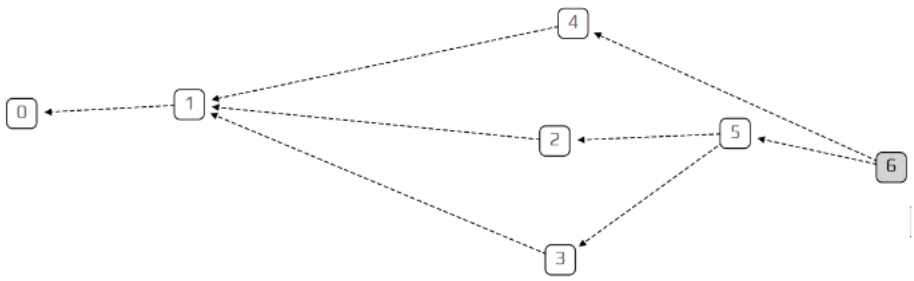

Figure 2.5: [37]

Current IOTA Structure

In the current IOTA network, the Coordinator plays an important role. In the following we describe the main tasks implemented in the current main network:

- Manual peering. In order to join the Tangle, a node is needed to be connected to some nodes that are already existing. The current IRI (IOTA reference implementation) software only permits manual peering, Node has to manually look for the other nodes. To propagate transactions and to synchronize to the current status of the ledger peering is a fundamental way. A node is probably lagging behind If a node's latest solid milestone is much older than its peers.

- Rate control mechanism. Proof of work must be done to issue a transaction. It is necessary to guarantee that nodes do not spam or to avoid that they inject more transactions beyond network capability.

- Tip selection strategy. Approving transactions leads to the DAG structure of the Tangle. To approve a transaction, a node must verify there are no inconsistencies in the ledger. IOTA white paper suggests a tip selection algorithm based on a random walk which: (i) Suggests approving fresh tips; (ii) It merges small branches to a single large branch, which increases confirmation rate; (iii) In case of conflicts, kills off the conflicting branches.

- Consensus. Milestones determine the consensus. A transaction is confirmed if and only when it is referenced by a milestone. Furthermore, we also want to highlight that milestones are used to optimize the IRI code: For instance, rather than compute the full ledger state starting from the genesis, an intermediate state is saved for each milestone; similarly, milestones are used in local snapshots, i.e., the IRI pruning mechanism, which allows nodes to avoid storing older parts of the Tangle.

Choosing Neighbor

Half of the neighbors are chosen by the nodes themselves and let the other half be comprised of neighbors that choose them. These groups of neighbors are consequently called:

- Chosen neighbors- The neighbors that the node proactively chooses from his list.

- Accepted Neighbors- The neighbors that choose the node as their peer.

In order to select chosen neighbors from the list of potential peering partners, we measure the distance between two nodes through the distance function d defined as-

$$d(nodeId1, nodeId2, \zeta) = hash(nodeId1 + \zeta) \oplus hash(nodeId2)$$

In order to connect to new neighbors, each node with ID $ownId$ and public salt ζ keeps a list of potential peers sorted by their distance $d(ownId, ., \zeta)$. Then, the node sends them peering requests in Then in ascending order the node sends them peering requests containing its own node ID, its current public salt and its address (i.e., IP + port). Then, the requested node can either accept or reject the network. The

connecting node repeats this process and stops whenever a connection is established. Those neighbors make up their list of chosen neighbors. Similarly, in order to accept neighbors, a private salt must be generated by the ownID node. When it receives a peering request from a node with ID remoteID, it measures d(ownID, remoteID,) and only accepts the request if one of the conditions above is done:

1. An existing accepted neighbor distance is not less than the connecting node.

2. The connecting node does not have the required or enough neighbors.

If a node rejects the request it is because the above requirements are not fulfilled.

2.1.7 Auction Theory in Mining

The very first consensus algorithm that came into account was Proof of Work which was introduced by Satoshi Nakamoto in his paper "Bitcoin: A peer to peer electronic cash system" [3]. Later on, many other consensus algorithms emerged onto the world of blockchain like Proof of Stake, Proof of Authority, Proof of Transaction and many others which were briefly discussed in the Literature Review chapter. To reduce the mining power consumption and wastage of resources, a new concept for consensus is explained in this paper. The newer algorithm will be based on Auction Theory with a mixture of Proof of Work for a limited amount of miner. The theory of auctions is one of the most impactful modern economic theories. An auction can be defined by one of its central properties as a market-clearing mechanism to equate demand and supply. [2] Auctions mostly happen when the seller is not quite sure of what should be the value of the item be or when ownership changes from public to private entities. This can include natural resources, seized goods, rare items, land, government contract procurement, etc. Auctions can be both universal and anonymous which implies that an auction is skeptic to what object is for sale and that the identities of the bidders should not affect the final of the result of the auction.
Although we have a popular concept of Auctions, there are many auction formats available in the market [28]. Some are mentioned below.

- English Auction: The most popular format of auction is the English one where the auction starts from a low price. It increases upwards based on the bidder's bid. The highest bidder wins the auction and pays for the item. This is a public auction where everyone knows about the bids.

- Dutch Auction : Also known as Reverse Dutch, this auction starts from an artificially high fee where in most cases no bidders are willing to bid. It decrements in order until a willing bidder emerges. The auction ends at that point and the bidder pays the whole amount. Gnosis uses this format in their ERC-20 crypto named as Dutchx. By using this format, all of their token was sold in 15 minutes only.

- First-price sealed bid auction (FPSB) - Although the previous two theories were public, which means all other bidders can see the bid others are bidding, First Price sealed bid auction is a private one. In this format of auction, bidders submit their bids in a private manner; in an envelope. A bidder can

only participate once. The highest bidder wins the auction and pays the highest submitted bid. Both English and Dutch auctions have to take place in a specific location. However, due to the asynchronicity of FPSB, it can be conducted from any place.

- Vickrey Auction (second-price sealed bid auction) - In a Vickrey auction, the participants submit their bids in a private order like the FPSB. It carries a different structure than FPSB. Although the highest bidder wins, he doesn't pay what he bade. Rather, he pays the second highest submitted bid. Vickrey auctions are also known as truthful auctions, because there is no benefit in bidding less than what someone value the good at. In a FPSB auction, which is not truthful, if someone's value is $2000 and they bid $1900 and win, they make $100 even though they risk losing the good to another bidder. If I win a Vickrey Auction, I'll still pay less than what my value is so my dominant strategy is simply to bid what I value, or to bid "truthfully". Vickrey auctions are used for domain name bidding in the decentralized domain name protocols Handshake and ENS.

- Channel Auctions - In a channel auction, both a minimum and a maximum price are set. Someone who chooses to remain in the auction commit to their willingness to purchase at the minimum price, and may purchase at the maximum price at any point during the auction. The minimum price and maximum price intersect until a symmetry in price is reached. Channel auctions are inspired by the efficacy of binary search algorithms where a solution is found by honing in from two sides of the problem.

2.2 Related Works

2.2.1 Bitcoin

Bitcoin is a type of virtual currency that runs on a peer-to-peer network. In 2008, it was invented by Satoshi Nakamoto as the first cryptocurrency [10]. Satoshi Nakamoto, in his paper proposed a solution to the double spending problem using a peer to peer network. When transactions are made in bitcoin networks, all the transactions are firstly verified by the nodes in the network. In this step, the bitcoin account history is checked. Later, the valid and unconfirmed transactions are passed to memory pool to be added in the block. When the miner add the transactions in the block, the transactions are said to be confirmed and the process of sending funds is complete. It is found that the reward for bitcoin mining is halved after every four years. At the beginning, in 2009 mining 1 block a miner could earn 50 BTC. In 2012 and 2016, the value was halve again to 25 BTC and 12.5 BTC respectively. It is assumed that in 2020 the value will become 6.25 BTC. As the price of bitcoin was about $9,300 per bitcoin in November 2019, this means that one can earn $116,250 (12.5 x 9,300) for completing a block[11] Bitcoin is the most versatile cryptocurrency which can be used to purchase goods (companies like Expedia, Overstock.com etc), exchanged with other users for services and can be swapped to other traditional or virtual currencies. However, it is also used to facilitate in illegal activities in dark web marketplace like SilkRoad. As bitcoin runs on blockchain, it is affected by some weakness in blockchain technology[34][33]. These are mentioned below-

- In the paper 'A model for Bitcoin's security and the declining block subsidy' there is some mention of some vulnerable attacks that fatal to the whole concept. Each blockchain address has their own private key which are needed to access their funds. There exists a chance of theft if these private keys are stored in public repositories like personal storage drives[14].

- In [4], [25] Karame thoroughly investigate double-spending attacks in Bitcoin. The proof-of-work algorithm that protects bitcoin blockchain is found to be inefficient since this type of consensus may lead to 51% attack. This type of attack may occur if a group of malicious nodes attain more than 50% of a network's hashing power, which will ultimately lead them to intentionally modify the transactions. It is shown through the paper that double spending attack still prevails even after the measures taken by the blockchain developers.

- Again from the paper 'Comparison Between PoW and PoS Systems Of Cryptocurrency' it is pointed out that as only one miner is able to add a block after solving a cryptographic puzzle for 10 minutes,so the work of other miners are wasted. Again the consumption of energy by the bitcoin network is significantly high, as all the miners are continuously increasing their computational power to find the hash value quickly[19].

- Visa can make 24000 transactions per second whereas Bitcoin can process on average 7 transactions per second. Bitcoin need to have much higher speed in order to replace credit or debit cards[1].

- It is also pointed out in different papers that as there is a concept of mining, there is an additional cost known as mining fee in bitcoin. The mining fees are comparatively high, as there is a limited space and high demand in the bitcoin network. A low mining fee may take days or months for a transaction to be added in the blockchain or may even reject the transaction and send the fund back to the owner's wallet[5].

- Another big issue with bitcoin is the value of bitcoin is fluctuating all the time according to demand. In June 2011 the value of 1 bitcoin was $9.9, whereas 6 months ago 1 bitcoin was valued less than $1. As bitcoin is a highly volatile currency, bitcoin accepting site continuously need to change prices. It also creates a great confusion when refunding for a product[1].This type of volatility is shown through figure 2.3.

2.2.2 Ripple

Ripple is a digital currency designed for banks. As banking sectors do not have connecting network with same set of rules, in order to transfer money between banks the money would need to go through several intermediary banks with which they have common connection with. Currency conversion might also be required. This makes the process slow and costly.Frederik Armknecht is his paper thoroughly discussed about Ripple [9]. Ripple network (RippleNet) aims to create internet of value to transfer money as quickly as it is possible to transfer information through internet. They use RTXP (Ripple Transaction Protocol) which have a unique set of

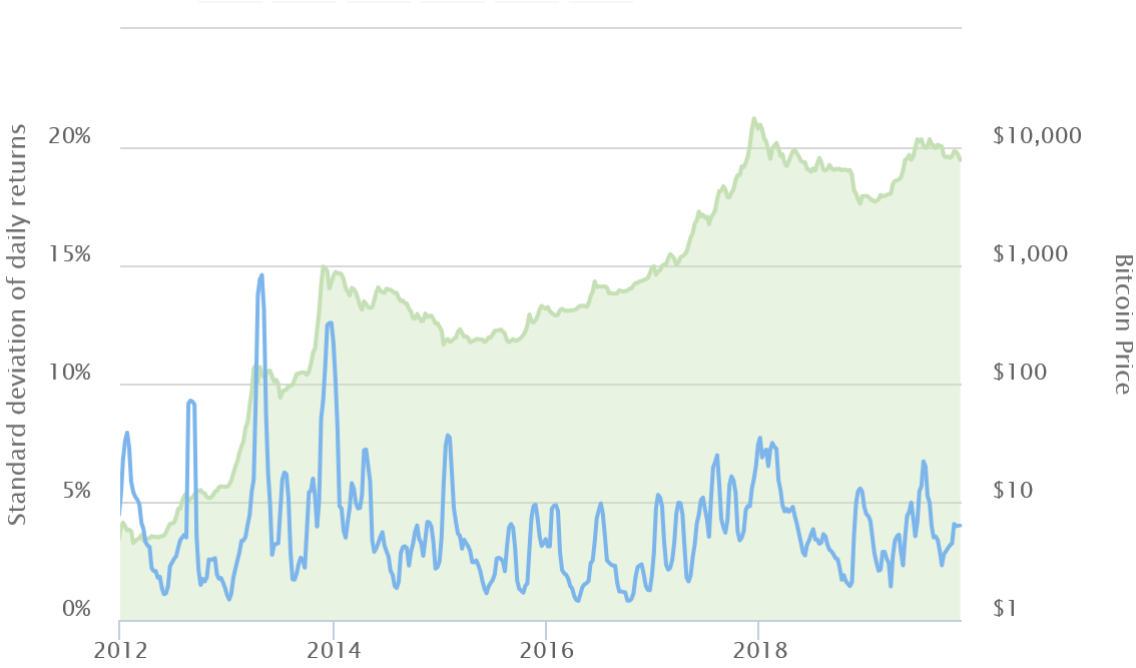

Figure 2.6: Bitcoin historical data[37]

rules for the network. The validators within the network maintain a shared ledger and determines if all the transactions are following RTXP. In order to access the network by any company, they need to use gateways. Ripple has two types of currencies- IOUs and XRP. The name of each IOU has two parts representing who issued it and what it represents. It can be issued for any real world asset. Again XRP is a cryptocurrency used in Ripple network to transfer funds. The sender bank can convert the money in XRP and send to recipient bank directly. In this case, they only need IOUs. In the network there are two types of node- server, nodes which are participating in the consensus process and clients, nodes which transfer funds. Each server has Unique Node List (UNL), which they use to query nodes.Shailak Jani in his paper made a clear distinction between the two mostly popular cryptocurrency- Bitcoin and XRP [35]. When a transaction is broadcasted in the network, if 80% of the validators vote that the transaction is valid, only than the transaction is added in the ledger. There is no separate reward for the validators like bitcoin. The tokens in the Ripple network is already pre-mined. In order to prevent multiple accounts of a single user in the Ripple network, one must have a wallet to support the currency and deposit 20 XRP in their account. XRP can handle 1500 transactions per second which is much higher than that of bitcoin[21].Transactions can settle in less than 4 seconds. It requires minimum transaction cost 0.00001 XRP or a fraction of a cent. There are certain drawbacks for Ripple Cryptocurrency XRP. These are-

- Since Ripple is pre-mined only a few validators are required to run the network which is not really distributed.
- Again since XRP are created all at once and the Ripple company holds 61% of it, many consider Ripple as a central bank of XRP, which opposes the decentralized property of any cryptocurrency[6].
- Ripple has not prioritized privacy and security of the network like other cryp-

tocurrencies.

2.2.3 Tron

Tron is the youngest cryptocurrency exchanges which has earned a lot of trust within a very short time. It is a decentralized entertainment and content sharing platform based on blockchain and peer-to-peer network. All the content creators in Internet must go through big companies like Apple, Google, YouTube etc. which act as the middle men, to broadcast and sell their contents. In return these companies in return takes a part of the profit created by these contents and have control over the contents. Tron facilitates content creators by providing them a platform to sell their contents at a much lower commission fees without the involvement of any middle men. The whitepaper of Tron discussed briefly about the facilities provided by Tron. Tronix (TRX) is the official cryptocurrency for Tron. TRX handles 2000 transactions per second 24*7. TRX cannot be mined and is used for trading in exchange platform of Tron. The main features are it is highly scalable, available and more secure. Tron is quite similar to ethereum. Tron uses delegated Proof of Stake consensus algorithm where there are 27 Super Representative who generate new blocks and maintain the network. Every 6 hours, 27 new SRs are selected on a voted election basis and to vote for SR, other candidates must freeze their accounts. In order to win votes, participant must please the voters by keeping the transaction throughput level up and maintain the network smoothly. This helps to create democratic decentralized ecosystem. Tron system consists of three layers. The first layer is spatial layer which collects the data and process them. The second layer is application layer which is completely decentralized and the last layer is core layer where the mechanism of DPoS occurs. The Tron network can generate each block in 3 seconds and for generating 1 block the SRs are rewarded 32 TRX. Each block takes 3 seconds to be generated in the blockchain and after 19 blocks are added on a Tron network, a transaction is confirmed. The only problem with tron is that exchanges can be made only with other cryptocurrencies but not with real world cash [31].

Chapter 3

Proposed IOTA Based Model for Microcredit Transaction

With the advent of the 4th Industrial revolution, Blockchain plays a huge role in making it a success. Its unique feature of decentralization and cryptographic security in the database has a huge impact on the future of the digital world. Although the term blockchain focuses on its applications in cryptocurrency, other sectors like finance and energy including artificial intelligence are exploring new and exciting ways to leverage blockchain technology. However, with an increasing impact comes an increasing number of users - where the big problem arises. Most of the existing blockchain systems are not made for handling bulk users. As mentioned in the above chapters, Blockchain technology has several flaws among which scalability is the thing to work on for which the advent of IOTA came into reality. IOTA emerged in late 2015[20] and it aims to overcome some of blockchain's core problems. IOTA addresses these issues and offers an entirely new technology, which is still decentralized but can process an infinite amount of transactions as well. This technology is called Tangle. Using their Random Walk Monte Carlo algorithm inside Tangle[16], IOTA can theoretically process an infinite amount of transactions and grows its network strength if more nodes join the tangle. This capability of IOTA was one of the important factors for choosing it in this microtransaction model.

From our research findings, we have found that the sole purpose of the microcredit system is hampered. The reason is that mining fee sometimes crosses the amount transacted. For this reason, we choose IOTA which is a miner free system that can solve the problem of what typical blockchain systems failed.[13] We are trying to get rid of the transaction fees so that the problem of paying a fee larger than the amount of value being transferred is gone. It is not easy to get rid of transaction fees in the blockchain system. Two types of participants in the blockchain system does those distinct operations. One is the person who issue transaction and the other person approve the transactions. It sometimes leads to unavoidable discrimination of some participants. For solving this problem we found something essentially different from blockchain technology, the basis for Bitcoin and other cryptocurrencies. And we found IOTA as a solution.In order to complete a micropayment transaction, the first thing that is needed is a Cryptocurrency that will be transferred from one user to another. As mentioned earlier, popular cryptocurrency platforms like Bitcoin, Ethereum, Litecoin, etc have several issues that hinder the basic concept

of micropayment. For this reason, we choose IOTA's Tangle as the decentralized database that stores both data and value transactions.[24] IOTA supports flash transactions where the value and the price execute simultaneously as opposed to the traditional blockchain technology.[26] This very feature of IOTA ensures the scalability of our Micropayment model. In order to transfer crypto, we will use IOTA Tokens which set its foot into the world of Cryptocurrency in recent times.

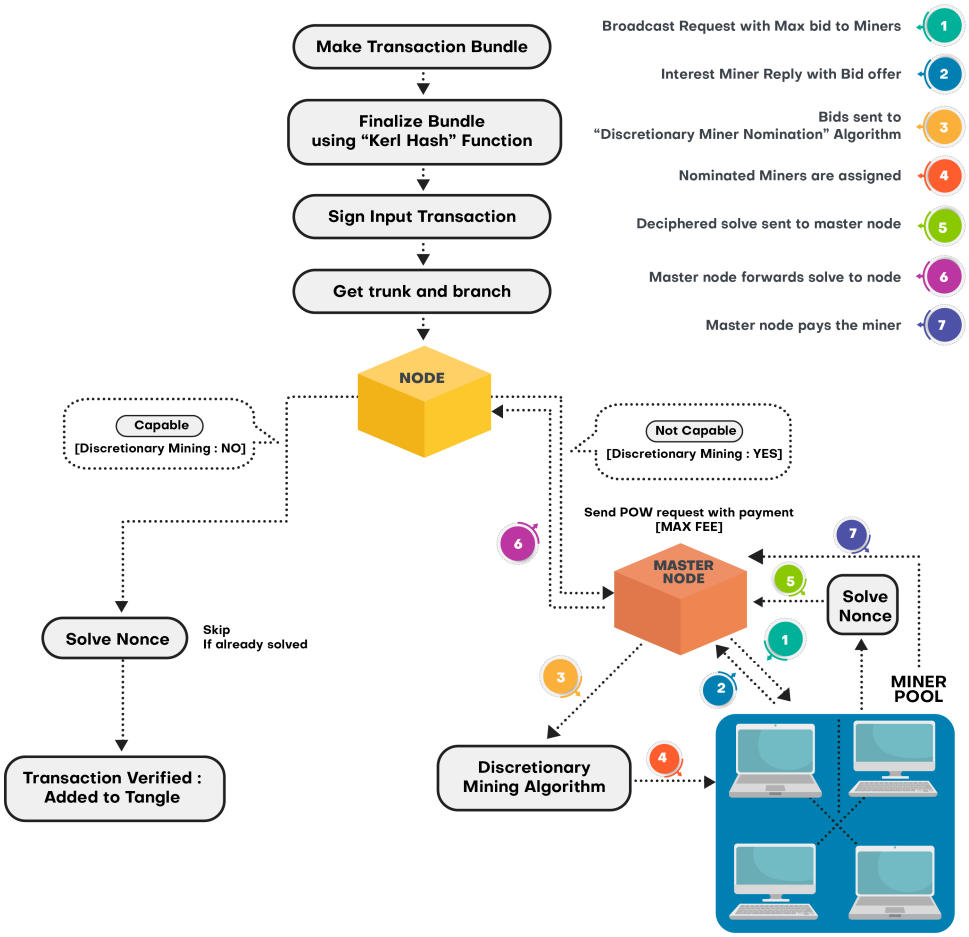

Figure 3.1: Proposed Model

When two devices interact with each other in an IOTA Token transfer, the device or nodes computation power comes into question. Although IOTA is for smaller IoT devices, one might need a more powerful machine to compile from source code as most of its code is written in Java. First and foremost, IOTA tangle evidently has a higher rate of TPS than any other blockchain based cryptocurrency. Other blockchain based cryptocurrencies are currently facing bottleneck issues. After transactions are recorded inside a block it remains inside the queue as unverified. After being verified by a miner, it currently takes about 10 minutes to be added to the main blockchain identified as a valid transaction. This drawback leakage creates a considerable amount of delay. IOTA tangle on the other hand, overcomes this

bottleneck issue by being completely miner-less. Nevertheless, IOTA is also based on the concept of distributed ledger just like other blockchain based portals. On a brief perspective, a distributive ledger is basically a shared ledger that possesses all the documentation and records of all the digital transactions which are synchronized across several ledgers of every node inside the network. Essentially, every user connected to the IOTA tangle network has access to an identical public record of all the transactions. The primary difference between a centralized transaction portal and a decentralized distributed ledger is that the ledger is immutable after recording data. If a malicious attacker wants to tamper with a transaction information, it requires them to successfully penetrate all other ledgers and simultaneously hacking them as well. Basically, whenever a new transaction is made, the participant's ledgers are updated. After that, the updated information is passed down throughout the entire tangle and all the ledger copies of every user reflects the changes that are made. When the record of all the distributed ledgers matches and synchronizes only then can the network reach complete consensus. Generally, each device (node) connected to the network has a certain amount of limitations when it comes to processing the log of consensus algorithm. Nodes within a tangle which has lowered computational power will take a considerable amount of time to update it's own copy of ledger and pass the updated information down the line to ensure consistency. As a result, the procedure of reaching complete consensus will be slackened and the whole tangle will become further inefficient. Moreover, a tip node with a low powered hardware may not be able to handle the complex cryptographic problems that needs to be solved. As a consequence, the verification process of the previous two transactions may come to a halt. This creates a throughput limitation to the tangle which will result in a lower rate of TPS.

3.1 Proposed Model

In a micro transaction, the amount transferred from one person to another or one device to another could be really small or it could be a large transaction. Depending on the amount of transaction, time and computing ability may vary. Keeping that in mind, our model is divided into two parts -

- Transaction of IOTA
- Discretionary mining using the proposed consensus algorithm

3.1.1 Transaction of IOTA

Transaction inside IOTA happens in several steps.[23] To help the audience visualize the steps, examples have been used below.

1. Suppose person A will have a transaction with person B. A have a secret seed named as A_SECRET_SEED and contains 100i (i= IOTA Token) in four different address which are related to the seed (figure 3.2).

   Person B have a secret seed named as B_SECRET_SEED and it has 0i in its related addresses (figure 3.3).

   Person A wants to send 80i to person B's address[0] QQQQQ...QQQ

seed: A_SECRET_SEED
address[0]: AAAAAA.....AAA, balance: 10
address[1]: BBBBBB.....BBB, balance: 5
address[2]: CCCCCC.....CCC, balance: 25
address[3]: DDDDD.....DDD, balance: 60
address[4]: EEEEEE.....EEE, balance: 0

Figure 3.2: Addresses of A
[23]

seed: B_SECRET_SEED
address[0]: QQQQQQ.....QQQ, balance: 0
address[1]: QQQQQQ.....VVV, balance: 0

Figure 3.3: Addresses of B
[23]

2. Transactions occur in a bundle. Bundle is the unit of a transaction, which includes three kinds of transaction: Input, Output and Meta Transactions. First, output transaction needs to be prepared which means 80i will be sent to B's address (figure 3.4).

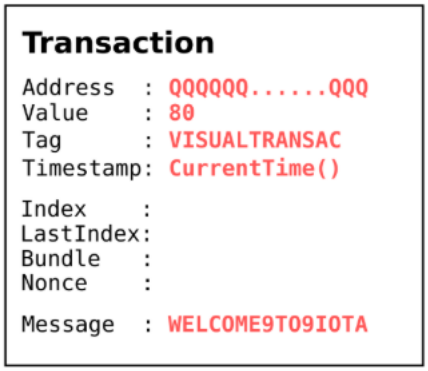

Figure 3.4: Output Transaction[21]

Next, input transaction need to be prepared which means 80i needs to be deducted from A's addresses. This happens in a sequence. Balance of address will be summed until it becomes equal or greater than the required value. In this case, it is 10+5+25+60¿80 to fill up 80i. But the input transaction need to contain transaction signature, default address security level is 2, that means an additional meta transaction need to be carried with every address to carry the transaction signature. Thus, each address will have two transaction - One with amount deducted by sending negative transaction, another with a meta transaction with a 0 value to carry out security level 2 signature (figure 3.5).

However, the bundle is unbalanced. It contains 20 additional IOTA Tokens. Hence, A will receive 20i which will happen in a new transaction. A new address will be generated from A's seed and the residue amount will be sent to that address shown in figure 3.6.

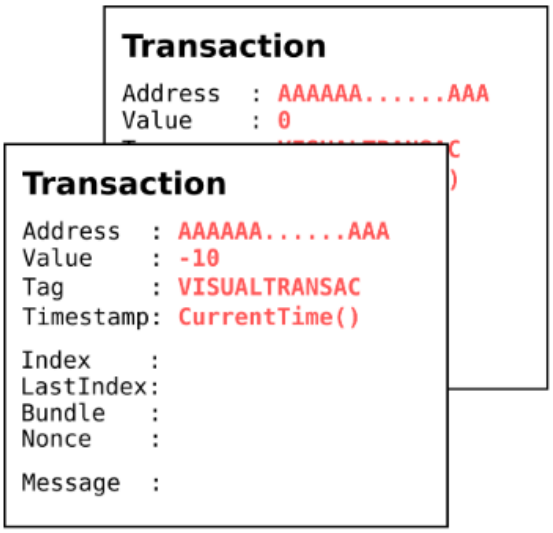

Figure 3.5: Output with meta transaction[21]

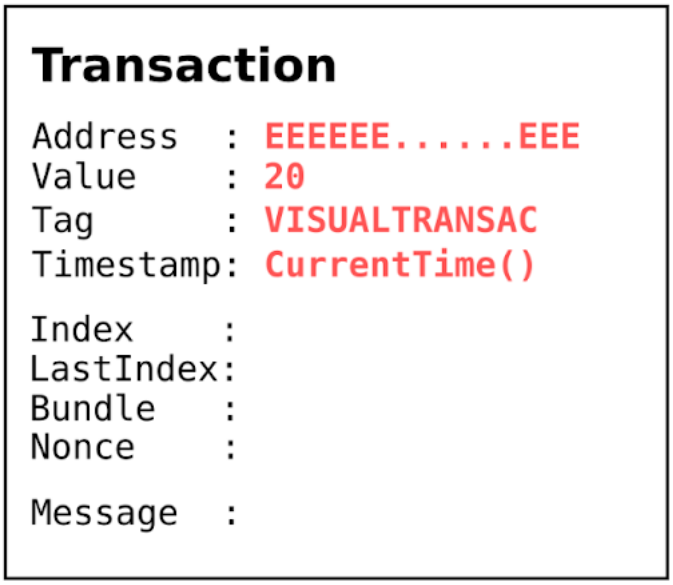

Figure 3.6: Returning remaining amount[21]

Bundle is now complete. Bundle hash and other information will be added.

3. Using Kerl Hash function, transaction index, last index and bundle hash will be generated. Transaction validate items include: Address, value, obsolete tag, timestamp, index, and last index. Using sponge constructor, Kerl hash will absorb transaction validate item one by one (order is important), and then squeeze out the result(figure 3.7).

   After this step, the bundles are ready with Bundle hash and they look like the following in figure 3.8

   Next, input transaction need to be signed with corresponding address's private key. The address private key comes from the secret seed. In this case, it comes from A_SECRET_SEED. From the address private key, Signature Fragment Generator gives the transaction signature using Private Key and Bundlehash

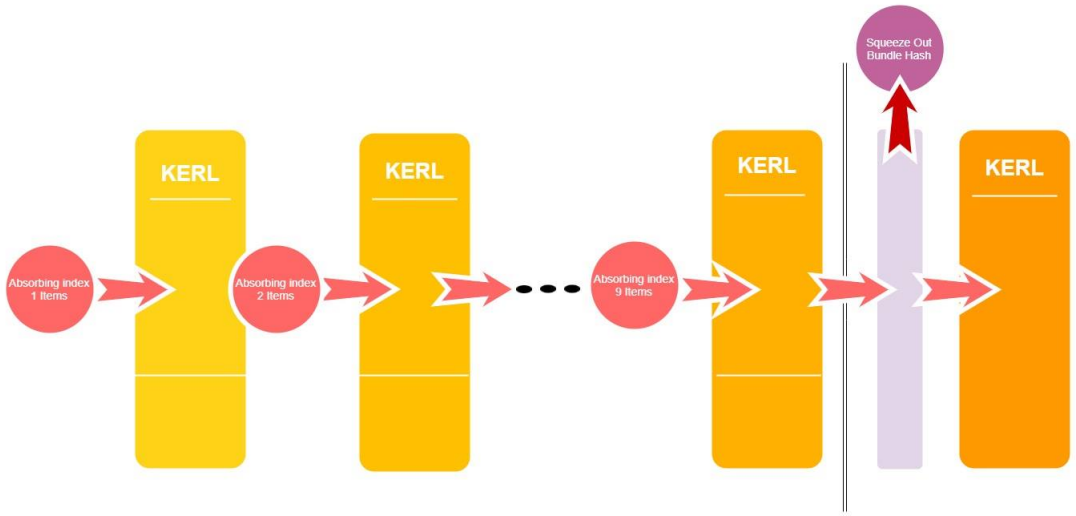

Figure 3.7: Bundle hash using Kerl Hash Function[21]

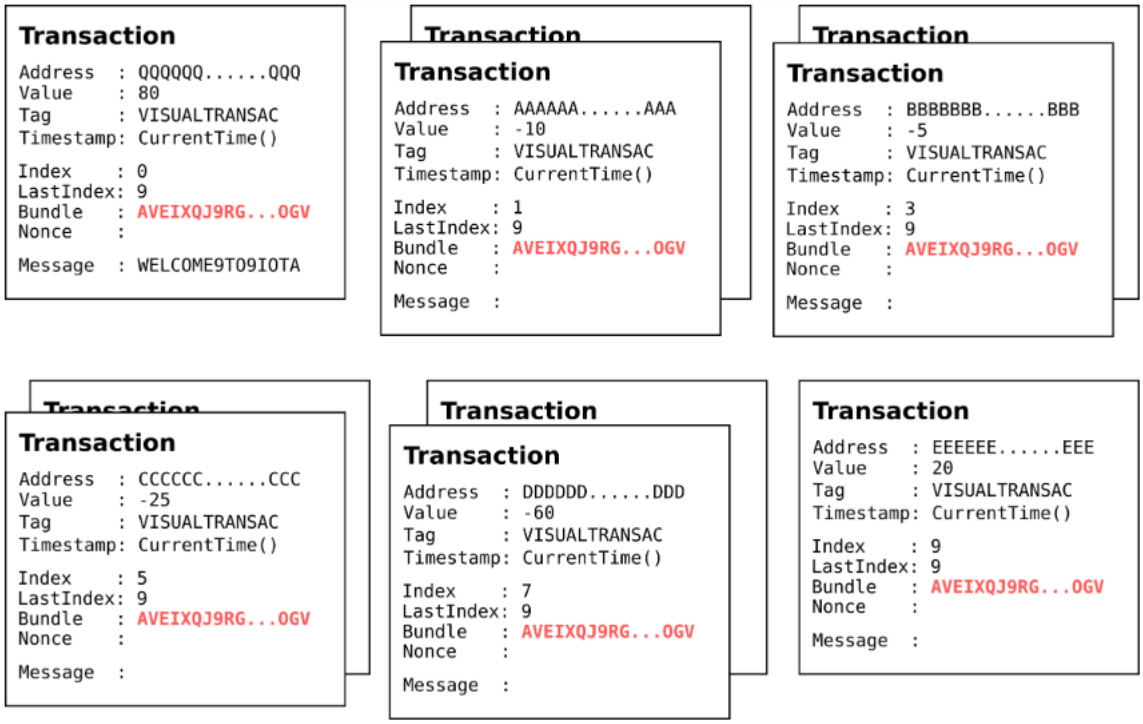

Figure 3.8: Fill up bundle hash

(figure 3.9, 3.10).

4. Afterwards, Trunk and Branch hash are calculated. All transactions but the last one contain the same branch hash. This branch hash is the hash of an almost randomly selected, unrelated transaction. Branches confirm tip transactions from the tangle and integrate the transaction into the tangle. Each individual transaction has its own individual transaction hash. The trunk hash chains each transaction to the next one inside the bundle. This means that the transaction with the index 0 will have in its trunk the hash of the transaction with the index 1. The transaction with the index 1 in its

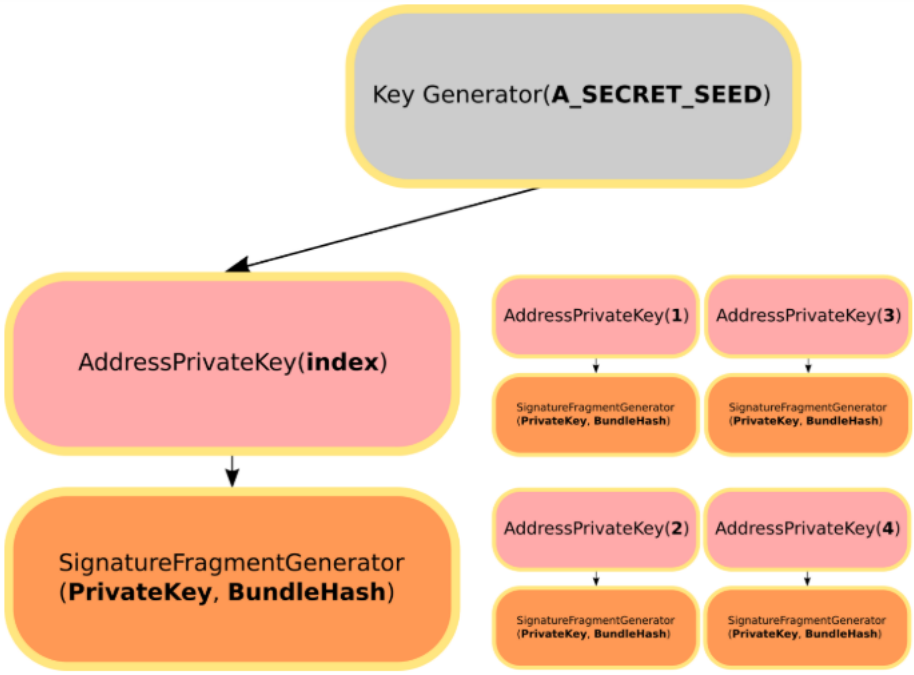

Figure 3.9: Signature Fragment Generator[21]

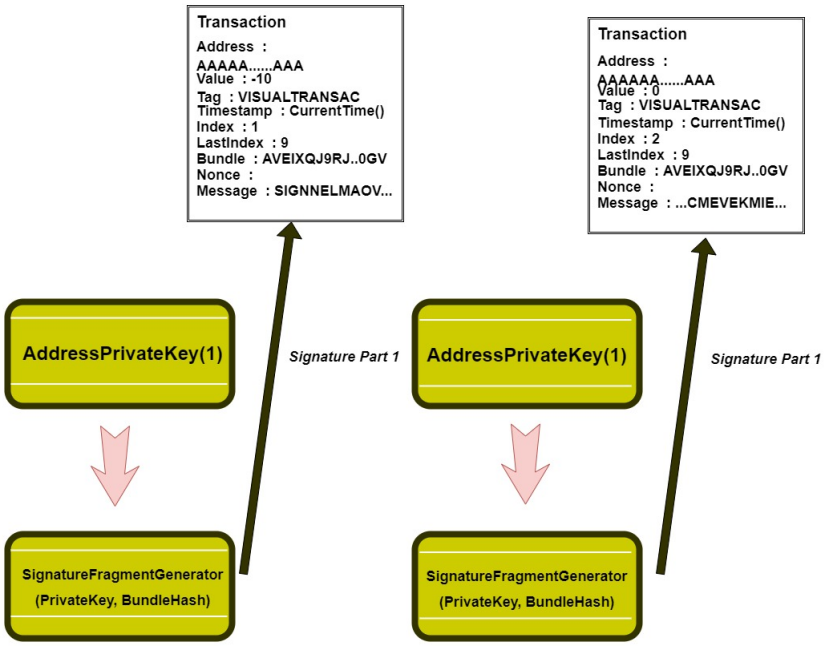

Figure 3.10: Fill Signature Fragment Generator to each transactions

trunk the hash of the transaction with the index 2, and so on (figure 3.11).

5. In the final step, Proof of Work(PoW) is done which means finding the nonce for the bundle which thereby concludes a transaction (figure 3.12).

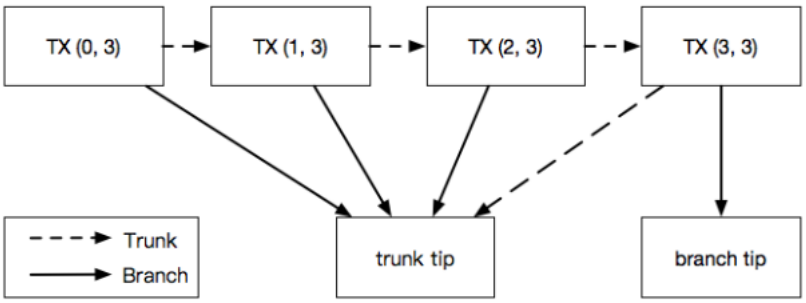

Figure 3.11: The diagram of transaction trunk and branch[21]

Transaction

Address : EEEEEE.....EEE

Value : 20
Tag : VISUALTRANSAC
Timestamp : CurrentTime()
Index : 9
LastIndex : 9
Bundle : AVEIXQJ9RJ..0GV
Nonce : CVYMVLE.....DIC
Message : 999999999....999
Trunk : HTQSF9C.....OIA999
Branch : QUVMZBE.....E999

Figure 3.12: Final Look of a Transaction Info

3.1.2 Discretionary mining using the proposed consensus algorithm

Although, IOTA aims to be a miner free platform, there arises a situation where one of the several nodes might not have the ability to complete the transaction but they want to stay inside IOTA network to avail the other features of IOTA. In that case, they can opt for discretionary mining where they will assign an optional miner to complete the task of inserting the transaction inside tangle. The process will follow the proposed consensus algorithm shown below.

- A client node or participant will send a mining request the parent node mentioning the maximum amount of fee it is willing to pay for some computation and the minimum computation power that it needs.
- Parent node upon receiving the request, will check the validity of the request and then broadcast it towards other miner available inside the network.
- Miners will send their bid following the First-Price Sealed Bid auction (FPSB) where other miners cannot see the request a miner is sending.
- Parent node will verify the miner's capability as per the request initiated by the client node and sort them according to their fee and timestamp.
- A limited number of miners from the sorted list will receive a broadcast of competing for the mining.
- Miners will perform computation steps of IOTA Transaction and solving the Proof of Work of IOTA, one miner will add the bundle to the Tangle and get its respective fee that it requested.

- The process completes upon adding the transaction trytes inside Tangle.

3.1.3 Algorithm

Algorithm 1: Nominating the Miner

Result: Miners will be assigned
$request = false$;
$payWill, payAmount$;
if $request$ **then**
  if $checkValidity$ **then**
    $participantMiners = broadcast(maxFee, noOfMiners)$;
  else
    $break$;
  end
  $getReplies[] = getReply(participantMiners)$;
  $chosenMiner = discretionaryMining(getReplies[])$;
  $givePermission(chosenMiner)$;
else
  $break$;
end

Algorithm 2: Discretionary Mining

Result: Miners selected based on Discretionary Mining
$miners[]$;
sort($getReplies$);
insert($getMiners$);
return $miners$;

Chapter 4

Implementation and Result

IOTA is an open-source distributed ledger technology that allows data transfer and IOTA token among Connected devices for zero fees. This network is made of nodes and clients. Although, a client can be a node and a node can be a client too in the public IOTA networks. The devices that are connected to the network and have read and write access to the Tangle are called Nodes. Clients are the nodes to transact or store data on the Tangle. Although the world of technology is formed mostly on Binary Numeral System, IOTA follows a Ternary Numeral System which consists of trits and trytes. In comparison to binary, ternary is considered to be more efficient as it contains 3 states. The states are 1,0 and -1. These values are called trits, and three of them are equal to one tryte, which can have 27 possible values.

4.1 IOTA Language and Environment

Although the source code of IOTA is written in Java, it can be implemented in four languages

- Java
- Go
- Javascript
- Python

4.1.1 Environment

For testing the proposed model, Java was used. Development environment had three stages to get activated and listen to live transaction on the Tangle.

- Setting up a developer environment: For Java Client Library, some set of programming tools was need to set up. Any operating system can be used. However, in this model, Linux was used using Virtual Machine. OpenJDK 11 was used as the Java compiler.
- Installing IOTA Java Client Library and its dependencies using Gradle. 'https://jitpack.io' needs to be inserted to build.gradle file.

- Connecting to a node of The Tangle. There are two networks where one can get connected - Devnet and Mainet. Inside Devnet, there is private tangle which can be set up for private testing without hampering the public one. In this case, private tangle was used.

4.1.2 Private Tangle

A private Tangle is an IOTA network that is controlled by someone and contains only nodes that are privately known. A private Tangle uses the same technology as the public IOTA networks, except someone controls it by running an open-source implementation of the Coordinator called Compass. Compass can be used to allow nodes to reach a consensus on transactions attached to a private Tangle. If Compass stops, no transactions in your IOTA network will be confirmed until it starts again.

To run a private Tangle, a device must meet the following requirements

- A new installation of an Ubuntu 18.04 Server / Virtual Machine
- At least 8GB RAM
- Preferably 4+ CPU cores, the more cores the faster the Merkle tree will be generated.
- At least a 10GB SSD

For the basic setup, IRI Node and Compass should be installed on the same server or virtual machine with configuration settings as the Devnet. The steps for setting up a private tangle are as follows:

1. Install the dependencies
2. Compute the Merkle tree
3. Run an IRI node
4. Run Compass (Coordinator's Private Form)
5. Test the network as http://localhost:14265.
6. Connect to the network through a wallet
7. Add several nodes

After the setup, IOTA Apis can be used for transactions.

4.2 Consensus Algorithm

Since IOTA development is not yet open sourced, its consensus mechanism and internal structure couldn't be changed to implement the proposed algorithm. For this reason, the algorithm was set up on a separate platform and tested using artificial miners. The tools that were used to implement the algorithm are as follows:

- Visual Studio (IDE)
- Language - Javascript
- Environment - NodeJS
- API Library - ExpressJS
- Server - Nodemon
- SSH Client - Putty

4.3 Result

First and foremost, among several differences IOTA and Blockchain based cryptos share a common trait and that is both of them are distributive ledger. Because of the way the consensus algorithm is designed inside IOTA tangle, while issuing a transaction it is essential for a user to verify the preceding two node's transactions. IOTA basically assumes that all the devices connected to the tangle network has approximately equal computational power. But that is not the case in reality. A user connected to tangle network may have low powered hardware. As we know, the verification process are executed by the users instead of the miners. So it is of utmost importance that all the users have a stable percentage of computational power. In contrast to that, if any user does not possess an equal amount of computational capability the verification process will slow down and the entire system will come to a sedation. As a result, the introduction of discretionary mining will enable the users to outsource computational abilities of other miners.

As already mentioned, IOTA is not a fully open sourced platform, many implementation could not be tested on the Main Network of IOTA. For this reason, the Discretionary Mining was tested on a local network platform. The key points to note during testing are stated below:

- Transaction Fee
- Transaction Time

Platform	Bitcoin	Ethereum	Ripple	Litecoin	IOTA
Transaction Fee ($)	0.332	0.083	0.0019	0.0017	0.00

Table 4.1: Transaction Fee of various Crytocurrencies

4.3.1 Transaction Fee

Transaction Fee for this micropayment will not hamper the current Fee structure of IOTA which is zero fee for transaction as stated in Table 4.1. Although, during Discretionary Mining, a fee is present, this fee will not effect the users. Clients who

will be transferring there IOTA token from one address to another will not pay this fee. However, this fee will be paid by the node which is willing initialize partial mining.

Platform	Bitcoin	Ethereum	Litecoin	IOTA	IOTA with D.Mining
Transaction Time (min)	10	5	2	1.5	<1.5

Table 4.2: Transaction Time of various Cryptocurrencies

4.3.2 Transaction Time

During testing, miners were artificially set using Ports of Network Socket. Each port was assigned as a different miner. Each transaction took 0.1 millisecond on an average. However, these ports were assigned in a localhost environment and so bandwidth was not as issue which resulted in faster output. On a second test, two laptops were connected using an Open Source SSH Client named Putty. This testing showed that the transaction time varies a lot which depends on the bandwidth of network. In general, IOTA takes an average of 90 second transaction time including the bottlenecks created by slow nodes. If discretionary mining comes into action inside IOTA Tangle, bottlenecks will be removed by powerful nodes and it will result in lesser transaction time than the current one as stated in Table 4.2.

4.4 Complexity

Best case : Suppose there are 50 nodes present on the tangle at a given time. In a best case scenario, all the 50 nodes have the required computational power needed to solve the nonce. At this point, the average TPS of IOTA is 700-800.

Average Case : Among 50 nodes suppose m nodes doesn't have the required computational power needed to solve the nonce. For each node, it requires a request (constant) that it will be broadcasted to T number of miners(constant). Suppose the number of interested miners who will reply with a bid offer is O. The master node will then receive all the offers and afterwards will use the "Discretionary Mining" algorithm to sort the bid and nominate the specific number of miners.
So, for each node the complexity of the algorithm is ONlog(N).
For M number of users the final complexity on average is MNOlog(N)

Chapter 5

Conclusion and Future Work

5.1 Conclusion

The primary incentive of this research was inspired by the founding fathers of cryptocurrency. The "cypherpunks" were solely motivated by the thought of breaking barriers and being confined by any central authoritative figure. Their purpose was to give the right to withhold personal information back to the people. Our journey began with the single motivation of planning and designing a new form of modification inside the current crypto platforms which will bring the entire system more closer to the people and will make it more viable for day to day usage. Subsequently, the absence of micropayment transaction on blockchain based cryptocurrency caught our attention. To eliminate this posing blockade, our research was based upon the concept of IOTA, a crypto platform that introduced the network Tangle. Tangle inaugurated a vast number of new edges over the current blockchain based platforms. Among which the most lucrative is it completely eliminating the miners. As a consequence of eliminating the miners, the transaction fees were vastly reduced. So to speak, the model became micropayment transaction enabled. However, the usage of iota tangle introduced some new challenges as well. One of the primary reasons for using a tangle network was to increase the number of transactions per second. The reason behind this is the degradation of TPS with each new user added in a blockchain based portal. At present, quite a huge number of digital transaction portal such as bitcoin, litcoin, ripple etc can only process 7 - 20 transactions per second due to restrictions in block size in comparison to millions of transaction handled by centralized banks.On the other hand, IOTA tangle can currently successfully handle 700 to 800 transactions and it has shown an increment of TPS equilibrium with the growth of users. But the posing challenge that the network is facing is a holt of verification timing also known as throughput limitation. In a minerless tangle, the users act as an intermediary miners themselves. To have their own transaction validated, each new tip needs to verify it's previous two nodes. As a result, a low powered hardware connected to the tangle can slow down the process of verification and it will take more and more amount of time for the network to reach consensus with every added node. For the sole purpose of resolving the matter our thesis designed and simulated a new algorithm called "Discretionary Mining" which was based on distributive computing. The algorithm was inspired by a mining auction theory named FBSB. Whenever a user won't have the necessary tools to solve the complex cryptographic problem, the node can outsource with the help of a master node. A

master node will be connected to a pool of miners. Our algorithm will work between the layer of master node and miner pool. The discretionary mining algorithm will nominate a specific number of miners according to the lowest bid that was offered by a miner. Furthermore, the specific number of miners will be appointed the task. The miner who will solve nonce the quickest will get the transaction fee. With the introduction of discretionary mining capabilities to IOTA, the tangle will achieve the intended well structured efficiency our research aimed for at the beginning.

5.2 Future Work

In the future, the discretionary mining algorithm can be further tweaked and tuned to incorporate more catalogued filtration characteristics in the nomination process of miners from the pool. Currently, using the algorithm the selection of a miner is completely based on the lowest bid made by a miner, the timestamp and the specified number of miners mentioned by the user. The algorithm can be improved more by adding additional filtration characteristics such as the computational power of the miner. The reason behind adding computational power to the equation is because low powered miners may always bid lower to get the assignment. Basically the sorting will work in such a way that the selected miners will possess the best computational power with the lowest bid. Furthermore, though we are partially allowing the concept of miner to be present in a virtually miner-less tangle network to make it more efficient, at the same time it is highly recommended to stick to the basic core of IOTA as well. Otherwise, the quality of a crypto platform that has micropayment transaction enabled might get demeaned over time. In a nutshell, the iota could customize the tangle in such a way that simultaneously at a time, only a few number of users can enjoy discretionary mining capabilities. Hence, we can ensure that tangle sticks to its roots.

Bibliography

[1] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail", in *Annual International Cryptology Conference*, Springer, 1992, pp. 139–147.

[2] F. M. Menezes and P. K. Monteiro, *An introduction to auction theory*. OUP Oxford, 2005.

[3] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system", 2008.

[4] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin", in *Proceedings of the 2012 ACM conference on Computer and communications security*, ACM, 2012, pp. 906–917.

[5] A. M. Antonopoulos, *Mastering Bitcoin: unlocking digital cryptocurrencies.* " O'Reilly Media, Inc.", 2014.

[6] D. Schwartz, N. Youngs, A. Britto, *et al.*, "The ripple protocol consensus algorithm", *Ripple Labs Inc White Paper*, vol. 5, p. 8, 2014.

[7] P. Vasin, "Blackcoin's proof-of-stake protocol v2", *URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf*, vol. 71, 2014.

[8] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger", *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[9] F. Armknecht, G. Karame, A. Mandal, F. Youssef, and E. Zenner, "Ripple: Overview and outlook", vol. 9229, Aug. 2015. DOI: 10.1007/978-3-319-22846-4_10.

[10] Y. Sompolinsky and all, "Secure high-rate transaction processing in bitcoin", in *International Conference on Financial Cryptography and Data Security*, Springer, 2015, pp. 507–527.

[11] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman, *et al.*, "Blockchain technology: Beyond bitcoin", *Applied Innovation*, vol. 2, no. 6-10, p. 71, 2016.

[12] J. Manning, "Proof-of-work vs. proof-of-stake explained", *ETHNews, November. Available at: https://www. ethnews. com/proof-of-work-vs-proofof-stake-explained (Accessed: 6 January 2018)*, 2016.

[13] S. Popov, "The tangle", *cit. on*, p. 131, 2016.

[14] Y. Sompolinsky and A. Zohar, "Bitcoin's security model revisited", *arXiv preprint arXiv:1605.09193*, 2016.

[15] D. Tapscott and A. Tapscott, *Blockchain revolution: how the technology behind bitcoin is changing money, business and the world*. Penguin, 2016.

[16] B. Kusmierz, "The first glance at the simulation of the tangle: Discrete model", *IOTA Found. WhitePaper*, pp. 1–10, 2017.

[17] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges.", *IJ Network Security*, vol. 19, no. 5, pp. 653–659, 2017.

[18] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends", in *2017 IEEE International Congress on Big Data (BigData Congress)*, IEEE, 2017, pp. 557–564.

[19] M. Alahmad, A. Al-Saleh, and F. AlMasoud, "Comparison between pow and pos systems of cryptocurrency", *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 10, pp. 1251–1256, Jun. 2018. DOI: 10.11591/ijeecs.v10.i3.pp1251-1256.

[20] R. Alexander, "Iota-introduction to the tangle technology: Everything you need to know about the revolutionary blockchain alternative", 2018.

[21] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain", 2018.

[22] *Iota's scalability solution*, 2018. [Online]. Available: https://helloiota.com/iotas-scalability-solution/.

[23] L. Lu, *In-depth explanation of how iota making a transaction (with picture)*, 2018. [Online]. Available: https://medium.com/@louielu/in-depth-explanation-of-how-iota-making-a-transaction-with-picture-8a638805f905.

[24] G. Ruiz, *Distributed data management in internet of things networking environments: Iota tangle and bitcoin blockchain distributed ledger technologies*, 2018.

[25] L. Singh, *Cryptocurrencies: Is bitcoin the future for a cashless society*, Feb. 2018. DOI: 10.13140/RG.2.2.18428.23684.

[26] D. Strugar, R. Hussain, M. Mazzara, V. Rivera, J. Y. Lee, and R. Mustafin, "On m2m micropayments: A case study of electric autonomous vehicles", in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, IEEE, 2018, pp. 1697–1700.

[27] A. Tar, "Proof-of-work, explained", *Retrieved Feb*, vol. 19, p. 2018, 2018.

[28] J. Wang, *An introduction to auction theory: Blockchain edition*, 2018. [Online]. Available: https://medium.com/crypto-economics/an-introduction-to-auction-theory-blockchain-edition-cf09b005b1cc.

[29] B. Academy, *How does blockchain work?*, 2019.

[30] M. Beedham, *85% of the world's bitcoin has been mined*, "https://thenextweb.com/hardfork/2019/08/01/85-percent-bitcoin-mined-cryptocurrency", 2019.

[31] M. Borkowski, P. Frauenthaler, M. Sigwart, T. Hukkinen, O. Hladk, and S. Schulte, *Cross-blockchain technologies: Review, state of the art, and outlook*, 2019.

[32] G. Giudici, A. Milne, and D. Vinogradov, "Cryptocurrencies: Market analysis and perspectives", *Journal of Industrial and Business Economics*, pp. 1–18, 2019.

[33] J. Daw and Babu, *What is ripple (xrp) and is it a good investment in 2020?* [Online]. Available: https://99bitcoins.com/ripple/.

[34] *Disadvantages*. [Online]. Available: https://cs.stanford.edu/people/eroberts/courses/cs181/projects/2010-11/DigitalCurrencies/disadvantages/index.html.

[35] S. Jani, "An overview of ripple technology & its comparison with bitcoin technology",

[36] *The amazing galileo abstraction: Logic, critical thinking, research methods, critical thinking*. [Online]. Available: https://www.pinterest.com/pin/518758450802920820/.

[37] *The bitcoin volatility index*. [Online]. Available: https://www.buybitcoinworldwide.com/volatility-index/.