

An in depth exploration on Blockchain Technology using Cryptocurrency

Jahir Ahmed

Student Id: 011 143 040

Akib Bhuia

Student Id: 011 143 120

Rifat Ara Ahmed

Student Id: 011 143 119

Ambia Md. Hossain

Student Id: 011 143 114

A thesis in the Department of Computer Science and Engineering presented
In partial fulfillment of the requirements for the Degree of
Bachelor of Science in Computer Science and Engineering



United International University

Dhaka, Bangladesh

January 26, 2019

Declaration

We, Md. Jahir Ahmed, Akib Bhuia, Rifat Ara Ahmed and Ambia Md. Hossain, declare that this thesis titled, **An in depth exploration on Blockchain Technology using Cryptocurrency** and the work presented in it are ours. We confirm that:

- This work was done completely while in candidature for a Bachelor degree at United International University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at United International University or any other institution, this has been clearly stated.
- Where we have consulted the published work of others, this is always clearly attributed.
- Where we have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely our own work.
- We have acknowledged all main sources of help.
- Where the thesis is based on work done by us jointly with others, we have made clear exactly what was done by others and what we have contributed our self.

Md. Jahir Ahmed, 011 143 040, Computer Science and Engineering

Akib Bhuia, 011 143 120, Computer Science and Engineering

Rifat Ara Ahmed, 011 143 119, Computer Science and Engineering

Ambia Md. Hossain, 011 143 114, Computer Science and Engineering

Certificate

I do hereby declare that the research works embodied in this thesis entitled “**An in depth exploration on Blockchain Technology using Cryptocurrency**” is the outcome of an original work carried out by Md. Jahir Ahmed, Akib Bhuia, Rifat Ara Ahmed and Ambia Md. Hossain, under my supervision.

I further certify that the dissertation meets the requirements, and the standard for the degree of Bachelor of Science in Computer Science and Engineering.

Mohammad Mamun Elahi
Assistant Professor, Dept. of CSE
United International University

Abstract

Blockchain is a suite of distributed ledger that can be programmed to record and track any significant data. The most important use of blockchain technology is the Bitcoin Cryptocurrency. Blockchain records every Bitcoin transaction that has ever happened. This makes the transaction ever so secure and unchangeable. The most functional and paramount attributes of the blockchain are security, anonymity, and data integrity without any intermediaries to control the transactions. In this research we have demonstrated the Bitcoin Cryptocurrency through Blockchain technology. Blockchain can be programmed to record financial transactions, medical records or even land titles. Although we already have processes (like bank, clinic, etc.) in place to track data, blockchain stands to revolutionize the way in which we interact with each other. It is a peer-to-peer interaction with the data that modernize the way we access, verify and transact with one another. Many other blockchain quantifiable related challenges including throughput and latency have been left unstudied.

Acknowledgement

We give a special recognition to our thesis supervisor, Mr. Mohammad Mamun Elahi, whose contribution in stimulating suggestions and encouragement helped us to synchronize our Thesis, who gave us the permission to use all required equipments and necessary materials to complete the task. We have to appreciate the guidance our supervisor has provided the team in achieving the goal.

Furthermore we would also like to acknowledge with much appreciation the time and effort Mr. Mamun Elahi sir has invested on us. Even when all seemed to be fragmented, he never gave up and instead made us go further and work harder.

Table of Contents

List of Figures.....	viii
1. Introduction.....	1
1.1 Blockchain and Cryptocurrency Summary.....	1
1.2 Problem Statement.....	1
1.3 Organization of the Paper	2
2. Background and Literature Review	3
2.1 Financial Services.....	4
2.1.1 Insurance: Claims processing	4
2.1.2 Asset Management: Trade Processing and Settlement.....	4
2.2 Bitcoin.....	4
3. Blockchain Technology	6
3.1 History	6
3.2 Structures	6
3.2.1 Decentralized	6
3.2.1 Peer-to-Peer network	7
3.2.3 Immutability	7
3.2.4 Accessible	7
3.2.5 Tamper proof	7
3.2.6 No intermediaries.....	7
3.3 Block elements.....	7
3.3.1 Data.....	8
3.3.2 Hash value	8
3.3.3 Previous Hash	8

3.4 Mechanism.....	9
3.4.1 Hash value	10
3.4.2 Peer-to-Peer network	11
3.4.3 Transaction pool	12
3.4.4 Miners and Mining	12
3.4.5 Proof-of-work	12
3.4.6 Bitcoin reward	13
3.5 Hashes and Mining	13
3.5.1 Hash function.....	13
3.5.2 Procedure	13
3.5.3 Application in Blockchain	14
3.6 Blockchain Security.....	14
3.7 Types of Blockchain	14
3.7.1 Public Blockchain.....	14
3.7.2 Private Blockchain.....	15
3.7.3 Similarities among Private and Public blockchain	15
3.8 Application of Blockchain	15
4. Cryptocurrency	16
4.1 What is Cryptocurrency?	16
4.1.1 Cryptography	16
4.2 Singularity of Cryptocurrency	16
4.2.1 Decentralized & No Central Authority	16
4.2.2 Anonymous / Pseudo-anonymous	17
4.2.3 Irreversible & Immutable	17
4.2.4 Limited Supply & Scarcity	17

4.3 Crypto currencies in modern world	18
4.4 Blockchain and Cryptocurrency	18
5. Implementation	20
5.1 Create Node	21
5.2 Wallet Generate	21
5.3 Create Transaction	22
5.4 Mining Block	24
6. Conclusion	26
7. References.....	27

List of Figures

Figure 1: The progress of Bitcoin	5
Figure 2: A block in a block chain.....	8
Figure 3: Hash value of blocks	8
Figure 4: Illustration of a Blockchain.....	9
Figure 5: Hash value representation in a Blockchain	9
Figure 6: Block invalidity.....	10
Figure 7: Peer-to-Peer Network.....	11
Figure 8: Transaction pool.....	12
Figure 9: System block diagram	20
Figure 10: Node initiation.....	21
Figure 11: Wallet	22
Figure 12: Key generate.....	22
Figure 13: Create transaction.....	23
Figure 14: Confirmation	23
Figure 15: Mining	24
Figure 16: Transaction History	25

Chapter 1

Introduction

Blockchain is a new technology with strong proposition for the future currency transaction and information exchange as a global networked society. Since it is so topical there is relatively little academic work done on it, but this is shifting quickly. Majority of the population find it rather tricky to comprehend the facts about Blockchain technology and Cryptocurrency. Providentially this paper will alleviate the recognition among Blockchain technology and Cryptocurrency further enhancing the understanding between these two. The idea of Cryptocurrency comes from block chain.

1.1 Blockchain and Cryptocurrency Summary

To be precise, Blockchain is the technology that enables the existence of Cryptocurrency which is a means of transfer. The most known of Cryptocurrency is the Bitcoin which was invented by the blockchain technology. By means of this ingenious technology transaction is being more secured and it is difficult to track and tax.

A blockchain is a distributed ledger which is unlocked to anyone. A few interesting aspects of a Blockchain is that, once a data has been recorder in a blockchain, it becomes almost impossible to modify it. Cryptocurrency is a digital currency in which encryption systems are used to control the generation of units of currency and verify the transfer of funds, operating independently of a central bank. Now all Cryptocurrency transactions are being handled through the blockchain technology. The blockchain technology is a digital, decentralized public ledger. It is a secured fortress of data and information. In the usage of Cryptocurrency, the public ledger stores transaction information with acute precautions.

1.2 Problem Statement

Our project exhibits an in-depth peek into the blockchain technology and how the course in which this technology employs, has been demonstrated using the most popular application of that technology, which is Cryptocurrency. The report demonstrates how a digital wallet is generated, the manner in which a miner or node is connected in a peer to peer network system, how a transaction is initiated and transported, the job of miners and Bitcoin generation and collection.

1.3 Organization of the Paper

The chronological order of matter distributed in our report is as follows, Chapter 2 has the assessment of the background and literature review on blockchain technology and Cryptocurrency. In Chapter 3 a comprehensive study of blockchain technology is conferred, along with its property, mechanism, security, types of blockchain and future application. In Chapter 4, Cryptocurrency and cryptography is extensively studied. The understanding of Cryptocurrency and blockchain is revised in this chapter. The implementation of the Cryptocurrency is broadly analyzed in Chapter 5. The chronological procedure from the construction of digital wallet to transaction generation to mining block is stated in this particular chapter. Finally, Chapter 6 contains the conclusion about our report.

Chapter 2

Background and Literature Review

As blockchain is a subject undergoing intense study at the moment, many of people have scripted about it, done research or performed tests and evaluation. This chapter will try to give a small view into some of the aspects other people glanced.

Some remarkable applications of blockchain alongside the highly regarded application of payments:

1. Voting system [1,2]

This can be used as one of the things of smart contracts on blockchain. Ethereum is already integrated in smart contracts which can be easily used for this purpose.

2. Supply Chain Sensors [3]

As the provided data on location and circumstance of the supplies is transported around the globe, sensors provide companies cross functional exposure of their supply chain. The blockchain administers stores, protects and transfers this smart information.

3. Administration of mass business of Emirate's using blockchain [4]

Dubai wants all its government services and transactions on blockchain, and almost all of its businesses will be operated through blockchain by 2020.

4. Loans [5]

Blockchain can be utilized for all sorts of loans, according to Microsoft.

The following examples below will be worked out in a bit more detail

5. Financial services [6]

Under this category we have insurance and asset management. The usage of blockchain technology will make the financial services much more reliable, easier and docile.

6. Bitcoin [7]

Bitcoin is a digital and global money system currency. It allows people to send or receive money across the internet. Money can be exchanged without being linked to a real identity or any middleman.

2.1 Financial Services

Traditional financial service systems tend to be ponderous, insecure and exasperatingly impeding. Frequently intermediaries are needed to mediate the process and resolve disagreements. Genuinely this costs stress, time, and money. On the contrary, users find the blockchain inexpensive, more transparent, and more efficacious. A mounting number of financial services are employing this system to introduce innovations

2.1.1 Insurance: Claims processing

Claims processing can be a hindering and unpleasant procedure. Insurance processors have to toil through fraudulent claims, fragmented data sources, or abandoned policies for users. This adds an enormous scope of error. The blockchain provides a perfect system for risk-free regulation and clarity. Its encryption properties allow insurers to capture the ownership of assets to be insured.

2.1.2 Asset Management: Trade Processing and Settlement

Traditional trade deals within asset which can be expensive and unreliable. Each faction or body in the process, such as broker, custodian, or the settlement manager, keeps their own records which create significant inefficiencies and scope for flaws. The flaws or errors are reduced via encrypting the records by the blockchain ledger. Simultaneously the ledger aids the process by omitting the need for any intermediaries.

2.2 Bitcoin

Bitcoin is a Cryptocurrency, a form of electronic cash. It is the very first crypto-valuta introduced by Satoshi Nakamoto. Beyond a doubt the most renowned application of blockchain is Bitcoin. It could be claimed that blockchain became so renowned because of Bitcoin. It is the first foreign currency with no bank or nation behind it to manage and maintain it.

In Figure 1 the course of Bitcoin in USD is shown since its launch in 2013. On account of the lack of intervention it is prone to a lot of fluctuation. Concurrently it can be seen that it elevates to new heights. Figure 1 below shows the progress or course of Bitcoin since its start in 2013 to 2018.

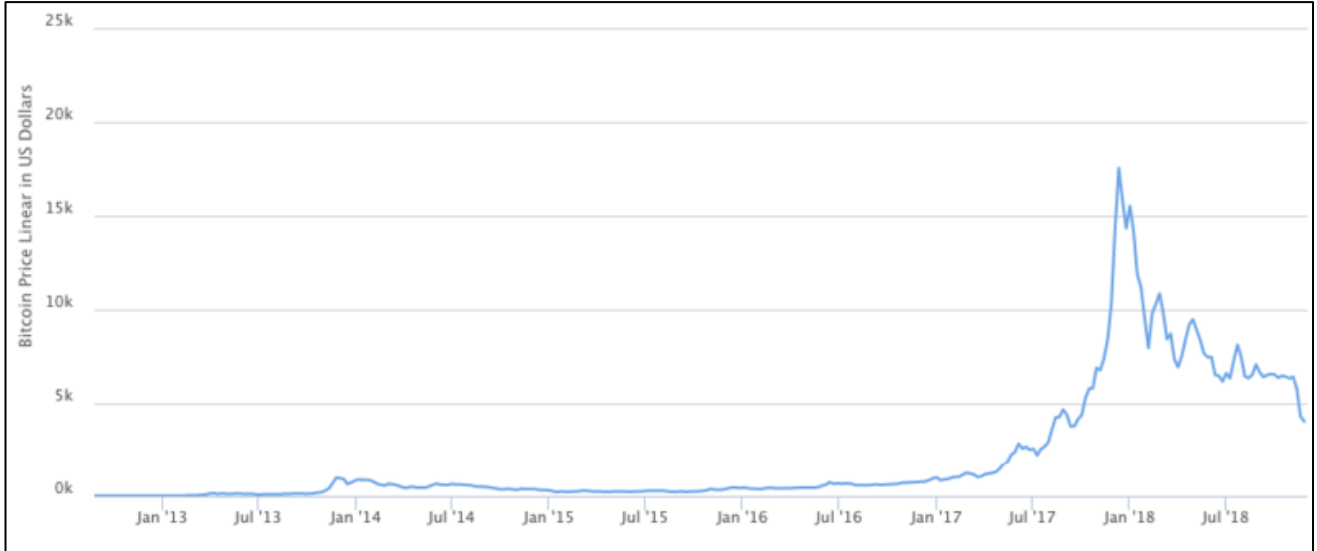


Figure 1: The progress of Bitcoin

Chapter 3

Blockchain Technology

Blockchain is a hierarchical structure that contains information or data while ensuring confidentiality, lucidity and decentralization. It is a sequence of blocks. While Bitcoin and other crypto currencies are the most popular examples of blockchain usage, this distributed ledger technology is finding a broad range of uses such as, data storage, financial transactions, real estate, asset management and many more uses are being discovered [8].

3.1 History

The blockchain mechanism was formerly introduced by a group of researchers in 1991 to timestamp digital documents so that the data cannot be meddled with. However, it was primarily pristine till it was reformed by Satoshi Nakamoto in 2009 to produce a digital crypto currency called Bitcoin.

The history of the blockchain began when it was used in Cryptocurrency. It had an unostentatious opening as a concept in computer science, predominantly in the province of cryptography and data structures. The very primordial form of the blockchain was the hash tree, also known as a Merkle tree [9]. The service provided by this procedure was to verify and handle data between computer systems. During transfer, validation of data in a peer-to-peer network was important to ensure no modification. It also facilitated to guarantee data integrity.

3.2 Structures

Blockchain is a suite of distributed ledger that can be programmed to record and track any significant data. It is a peer-to-peer interaction with the data that modernize the way we access, verify and transact with one another [10]. Any data or information plotted in a block is ineradicable and indestructible.

3.2.1 Decentralized

Blockchain was intended to be dispersed and distributed across a large network of computers. This means no one has the authority of the global network. Every node in the

network has a copy of the block being distributed to them; no one node specifically can change it. This unique attribute of blockchain ensures lucidity and safety.

3.2.1 Peer-to-Peer network

Blockchain uses P2P protocol which allows all the participants in the network to hold an identical copy of transactions, enabling sanction through a machine consensus. With the use of Blockchain, the interaction between two parties through a peer-to-peer model is easily accomplished without the requirement of any intermediaries [11].

3.2.3 Immutability

Any information or data that enters the blockchain network is prevented from being altered or modified. Not even the administrator of the network can modify any information or data.

3.2.4 Accessible

All the nodes in the network can easily access the information, that is the chain of block; also known as the distributed ledger book. Anyone who joins the network automatically receives the complete ledger book.

3.2.5 Tamper proof

The information on a blockchain is sheltered through cryptography. Network participants have their own private keys that are appointed to the transactions they make and exploit as a personal digital signature [12]. In any case, the bigger the network, the more tamper-resistant the blockchain will be.

3.2.6 No intermediaries

One of the game changing structures of blockchain is that we do not need any intermediaries. Thus, allowing us to spend less money and time on middleman, such as lawyers and banks.

3.3 Block elements

A blockchain is a distributed ledger that is open to anyone. They have some interesting properties; once a data has been recorder in a blockchain, it becomes very difficult to alter it. The method in which a blockchain works is explained below.

Each block has 3 elements as shown in Figure 2:

1. Data
2. Hash value
3. Hash of the previous block

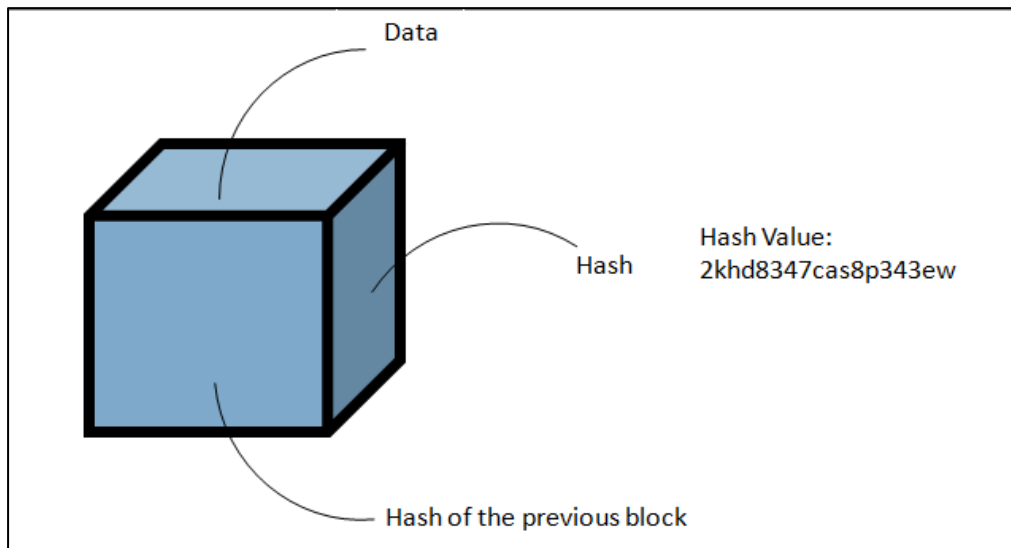


Figure 2: A block in a block chain

3.3.1 Data

The data in the block depends on the type of the blockchain. The Bitcoin blockchain for example, stores the information about the exchange or transaction. So only the details about the sender, receiver and the amount are stored.

3.3.2 Hash value

Each block has a hash. The hash is like a fingerprint; therefore each hash of the block is unique. It identifies the block and all its contents. Once a block is created the hash is calculated and if the content of the block is altered the hash changes as well. It is very useful if we want to detect any changes within a block [14].

3.3.3 Previous Hash

The last element is the hash value of the previous block [14]. This creates a chain of blocks and this is also the very method that makes a blockchain so secure, as shown in Figure 3.

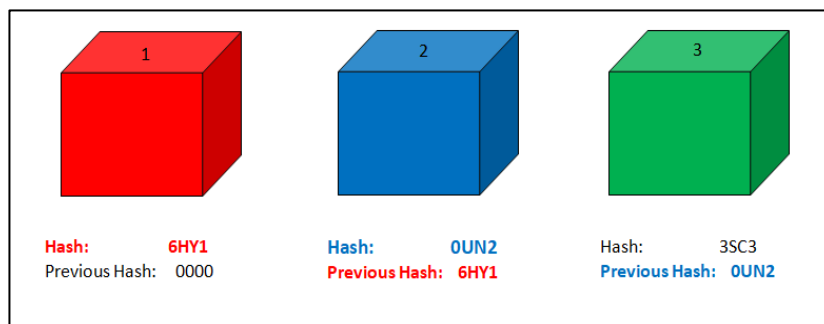


Figure 3: Hash value of blocks

3.4 Mechanism

The following description and illustrations are employed to simply comprehend the blockchain mechanism using Bitcoin transaction.

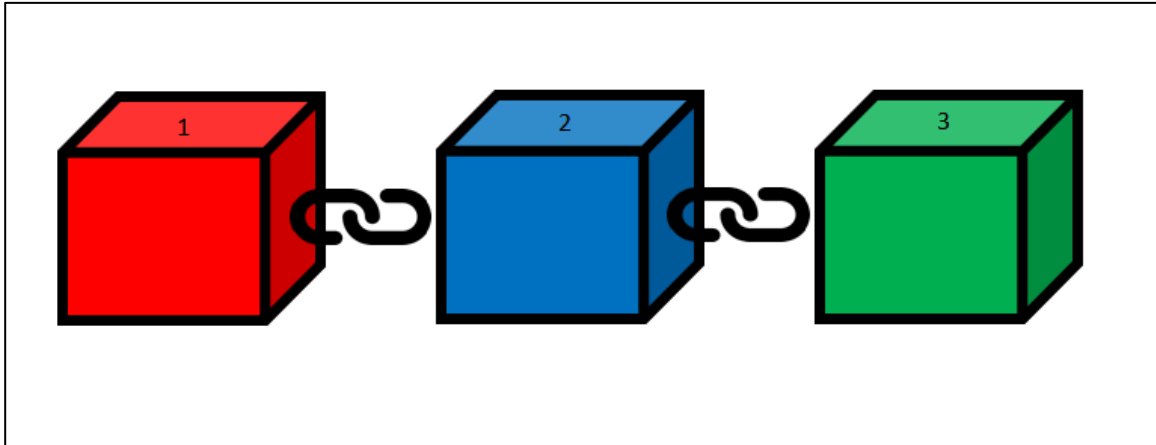


Figure 4: Illustration of a Blockchain

Figure 4 exhibits the representation of a Blockchain. All data blocks are linked to each other in the form of a chain.

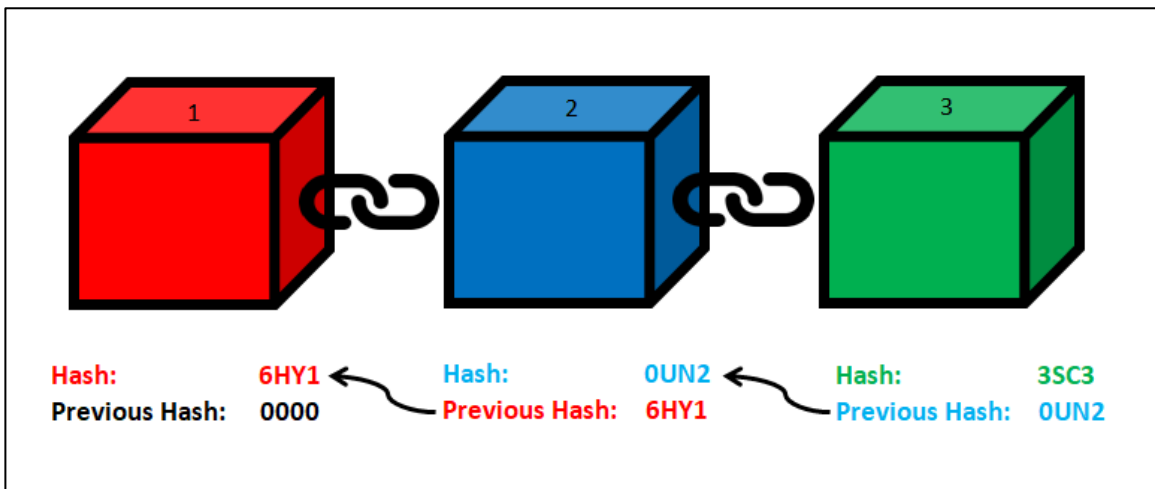


Figure 5: Hash value representation in a Blockchain

3.4.1 Hash value

Figure 5 demonstrates three blocks that are displaying how the hash value of the previous blocks forms a chain of blocks. Every block has a hash and the hash of the prior block. Block 3 points to block 2. Block 2 points to block 1. The first block, as you can see cannot point to the previous block since it is the first block. This block is called the **Genesis block** [15].

If the contents of the second block in Figure 6 are altered then the hash of the respective block also changes unconditionally. This will make block 3 and all following blocks invalid because they no longer store the valid hash of the previous block. Subsequently changing a single block will make all following blocks null or invalid.

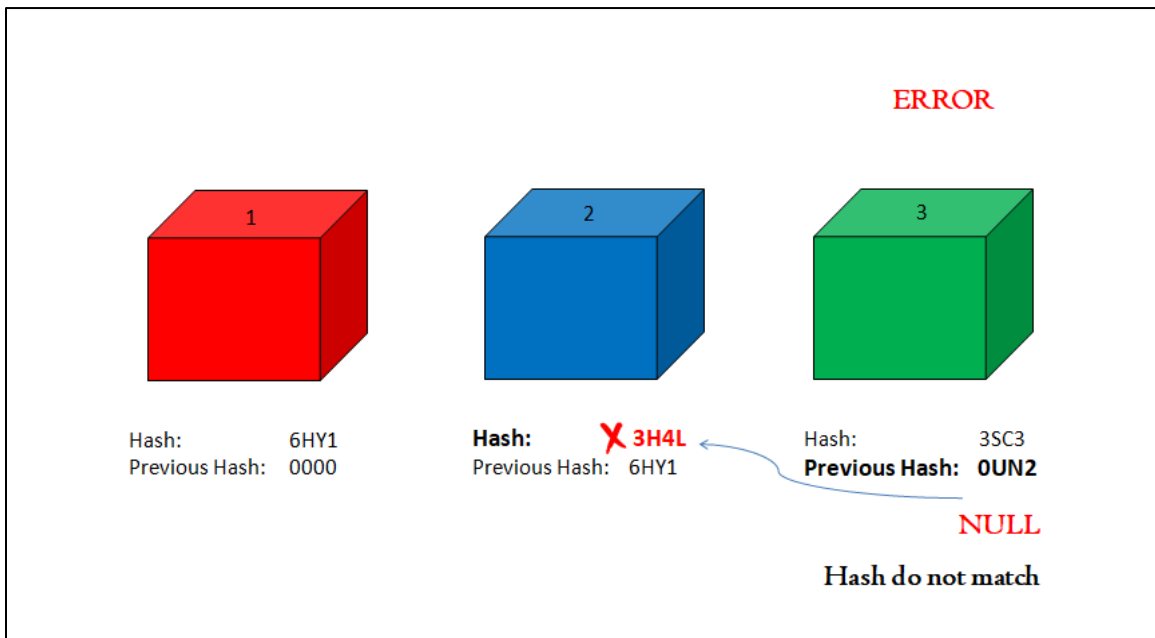


Figure 6: Block invalidity

3.4.2 Peer-to-Peer network

The blockchain technology uses the peer-to-peer network. Anyone can join this network. Figure 7 demonstrates how the network is connected.

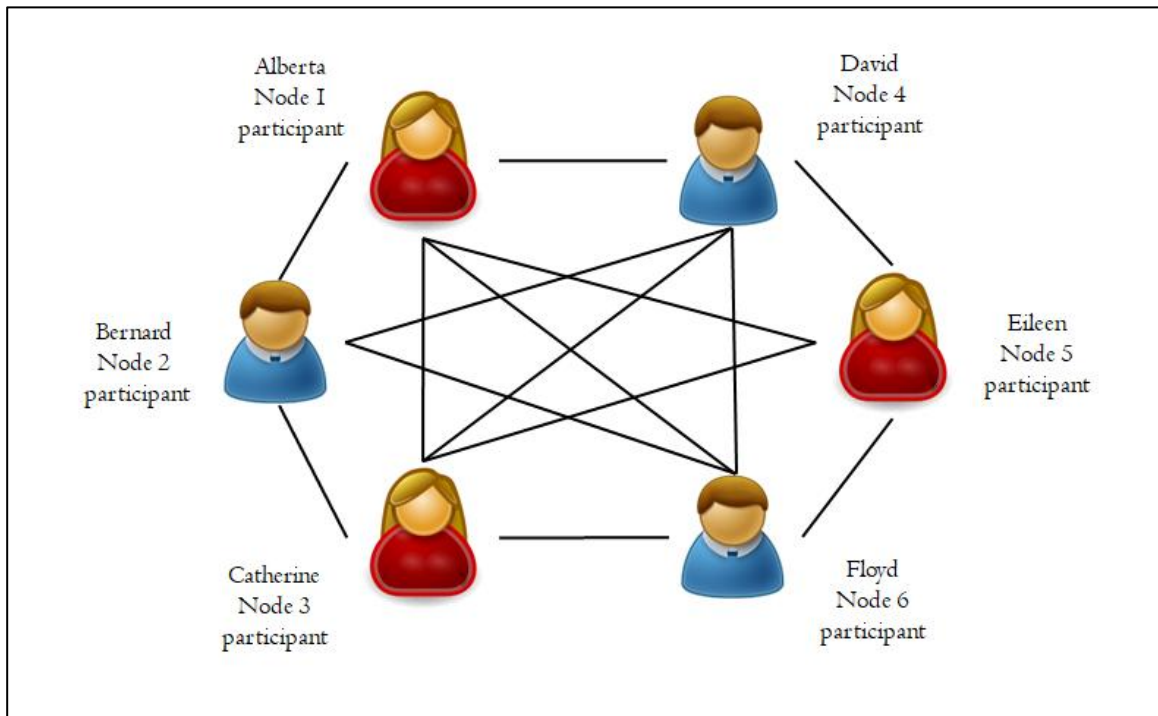


Figure 7: Peer-to-Peer Network

When a transaction is made, the message of the transaction is distributed in the peer to peer network. That is, the transaction message is passed on to all the network participants, as shown in Figure 7, also known as the nodes. All the nodes in the network creates a consensus, they agree about which block is valid and invalid. This peer-to-peer network prevents fraudulency in Bitcoin crypto currency known as double spending [16].

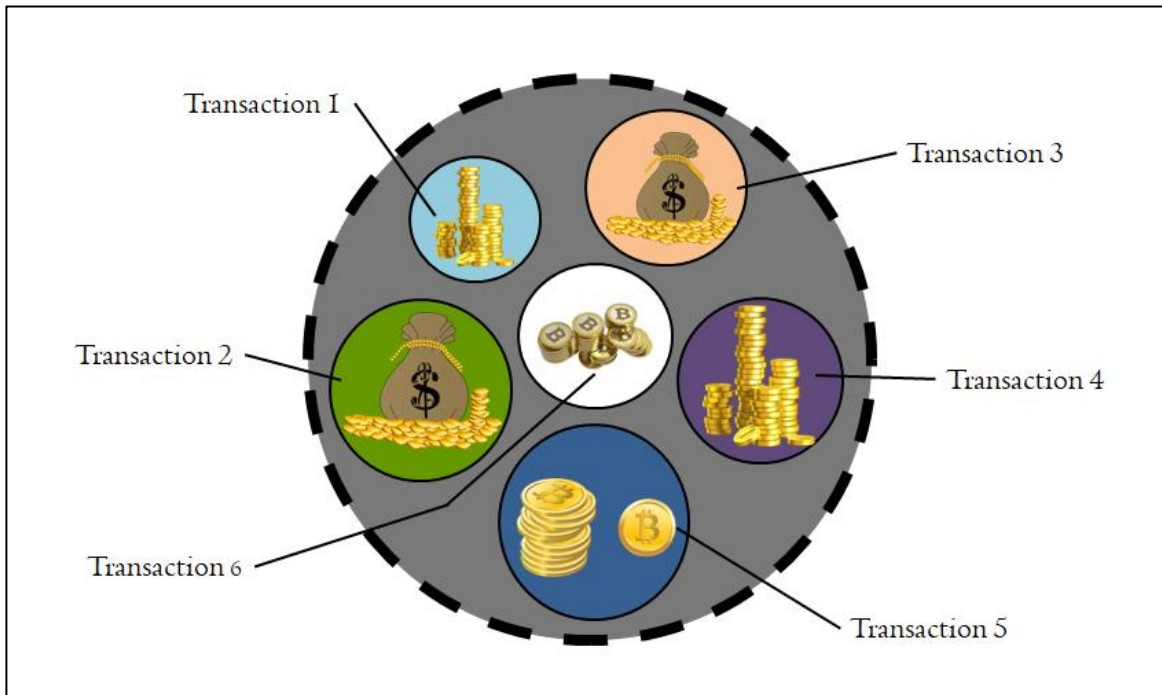


Figure 8: Transaction pool

3.4.3 Transaction pool

Currently the transactions reside in an invalidated state in the transaction pool as shown in Figure 8. All the transactions that exist in the transaction pool remain in an unauthenticated state [17].

3.4.4 Miners and Mining

Miners are the network participants who validate a transaction and record that transaction on the global ledger of a blockchain. This pursuit is called mining.

3.4.5 Proof-of-work

Clearly using only hashes is not enough to prevent block tampering. Computers these days are incredibly fast and can gauge hundreds of thousands of hashes per second. One could effectively tamper with a block and can recalculate all the hashes of other blocks to make the blockchain valid again. So to mitigate this, blockchain has something called the proof-of-work [18].

The miners aim to confirm the transaction from the transaction pool and add the transaction block to the blockchain. In order to add they will have to solve a complex algorithm. This procedure is known as the proof-of-work. The miner who can solve the algorithm the fastest gets to add the block to the public ledger. Each confirmation represents addition of new block. The average time to confirm each block is about 10 minutes. This means it takes about 10 minutes to calculate the required proof of work and add a new block to the chain.

3.4.6 Bitcoin reward

Once the confirmed block is added to the public ledger blockchain, the miner is awarded a transaction and block cost that is, Bitcoin. New Bitcoins are created every time a miner adjoins a new transaction block to the blockchain as an incentive for approving the transactions [19]. Block rewards are reduced every year and in the end only the transaction cost will remain as no new Bitcoin will be generated.

In present there are 998 confirmed blocks in the blockchain public ledger.

3.5 Hashes and Mining

Proof-of-Work is the unique consensus algorithm in a Blockchain network. In Blockchain, this algorithm is used to confirm transactions and create and insert new blocks to the chain. With Proof-of-Work, miners contest against each other to conclude transactions on the network and get rewarded [19]. Earlier it was mentioned that accumulation of new blocks in a blockchain requires the need to solve a complex algorithm. This complex algorithm is a **hash function** [20].

3.5.1 Hash function

A hash is a one way function that has several utilizations in blockchain and decentralized systems [21].

3.5.2 Procedure

A hash function takes any digital media like documents, and runs an algorithm on it to produce a unique fixed length digital output known as the hash. This fixed length output is usually much smaller than the initial input. Every time the same digital media is put through the hash function it produces the same digital output or hash. When just a single bit of data in the digital media is altered and passed on to the hash function, the digital output, the hash, is completely changed compared to the original one [22,23].

The mathematics behind the hash function guarantees that there is no way to originate the initial digital media content from its generated hash thus making the hash function one way.

3.5.3 Application in Blockchain [24]

In a blockchain, the concept of mining entails miners to solve a problem with a known partial input derived from the latest state of the blockchain to create a hash target. The miners must aim to presume the digital input that can create the hash target therefore solving the problem. As a hash is a one way function, the miners have to evaluate many combinations of input to create the hash target and solve the problem. This consumes a computer's resources like CPU and memory. The first miner to answer the problem wins.

3.6 Blockchain Security

Blockchain is like a fortress and like any other fortress it has guards to shield anything inside it. The hash value, proof-of-work mechanism and the distributed peer-to-peer network acts as the guards of the blockchain public ledger [25].

So in order to tamper with a block in blockchain one must tamper all the blocks on the chain, redo the proof-of-work for each block, take control of more than 50% of the peer-to-peer network. This is almost impossible to do.

3.7 Types of Blockchain

There are two extensive categories in which blockchains can be classified [26].

3.7.1 Public Blockchain

A public blockchain is an unauthorized ledger and can be accessed by any and every one. Anyone with the access to the internet is qualified to download and read it. In addition, one can also check the complete history of the blockchain along with making any transactions through it. Public blockchains typically reward their network contributor for executing the mining process and preserving the immutability of the ledger .

The Bitcoin Blockchain is an example of the public blockchain.

Public blockchains sanction the communities worldwide to trade information explicitly and securely. However, a palpable disadvantage of this type of blockchain is that it can be compromised if the regulations around it are not executed strictly.

3.7.2 Private Blockchain

Private Blockchains are the ones which are shared only among the trusted participants, contrary to the public blockchain. The entire control of the network is in the hands of the owners. Furthermore, the regulations of a private blockchain can be altered according to different levels of authorizations, revelation, number of members, consent etc.

Private Blockchains can run autonomously or can be integrated with other blockchains as well. These are usually employed by enterprises and organizations. Hence, the level of trust required amongst the participants is superior in private blockchains.

3.7.3 Similarities among Private and Public blockchain

1. Both Public Blockchain and Private Blockchain have peer-to-peer decentralized networks.
2. All the participants of the network uphold the copy of the shared ledger with them.
3. The network retains facsimiles of the ledger and synchronizes the latest update with the help of consensus.
4. The rules for immutability and safety of the ledger are resolved and channeled on the network so as to avoid malicious attacks.

3.8 Application of Blockchain

1. Bitcoin and crypto currency
2. Smart contracts
3. Government election
4. Identity Management
5. Intellectual property protection

Chapter 4

Cryptocurrency

Let us consider an example of an online transaction; Amanda is sending money to Bill. The money is being sent using online transaction method, but there is a central authority which is in the middle to operate this transaction. Now there is a probability that the transaction might be successful or not. The transaction may fail due to any technical issue at the bank, like improper system execution or server failure. The account of Bill could be hacked, compromising the transaction or identity theft may occur or the transfer limits for the account could be exceeded, even a central point of failure could take place. That is why the future of currency lies with Cryptocurrency, to avoid all these impediments.

4.1 What is Cryptocurrency?

A Cryptocurrency is a digital or virtual currency that is meant to be a medium of trade. Now Cryptocurrency is quite similar to real world currency except that it has no physical personification. It is a decentralized systems based on Blockchain technology, works in peer to peer network so that it is simple to authenticate the transfer of funds.

4.1.1 Cryptography

In order to fully understand Cryptocurrency, one must be able to comprehend cryptography.

Cryptography is a method of using encryption and decryption to secure in the presence of third parties with ill intent. Like, third party wants to steal your data or eavesdrop on your conversation .Cryptography usually requires a computational algorithm like SHA256 [27], a public key – which the user shares with everyone and a private key which acts like a digital signature of the user.

4.2 Singularity of Cryptocurrency

4.2.1 Decentralized & No Central Authority

In traditional paper currencies, central authorities and banks, manage the financial system. However, with Bitcoin and other crypto currencies, these transactions can be processed and validated by a distributed and open network which is owned by no-one. Unlike centralized banking systems, most Crypto currencies are decentralized on distributed networks of computers that are spread around the world, also known as nodes. Transactions are corroborated by network participants through cryptography and recorded in a public distributed ledger called a blockchain. The transaction is circulated across the

peer-to-peer network and is copied by every node, attaining a large percentage of the nodes within a few seconds.

4.2.2 Anonymous / Pseudo-anonymous

Since there are no requisition for a central authority, users does not require identifying themselves when transacting with Cryptocurrency. When a transaction request is submitted, the decentralized peer-to-peer network will examine the transaction and verify it and record it on the blockchain accordingly. Crypto currencies, like Bitcoin, work with a private key and public key system to authenticate these transactions. Meaning users can create anonymous digital identities and digital wallets to transact on the decentralized system and still manage to authenticate their transactions with assurance.

4.2.3 Irreversible & Immutable

Cryptocurrency transactions are permanent and absolute. The permanent and absolute features of Cryptocurrency means that it is not viable for anyone but the owner of the respective private key to move their digital assets, and that transaction is consistent once it is recorded on the blockchain. While it is not impossible to modify the transaction, secure cryptography makes it very difficult for adjustment, because it entails to alter most nodes in the blockchain. In order to preclude fraudulent transactions, all transactions are transparently recorded on the blockchain and open to the public.

4.2.4 Limited Supply & Scarcity

Fiat currencies, also known as paper currencies (e.g. Dollars, Euros) have an infinite supply, as the central banks can issue as much fiat currencies as they require. Central banks often maneuver the value of the countries' currencies as part of its economic policies. Most countries often control their currency to be inflationary over a period of time. The inflationary nature of paper currencies would mean a decrease in the value of the currency over time. Therefore, paper currency holders might suffer the cost of the decrease in value and also face the uncertainty of currency manipulation. Alternatively, most Crypto currencies have a limited and pre-determined supply of the Cryptocurrency that is coded into its underlying algorithm when it is produced. For instance, Bitcoin has a maximum supply of 21 million, and once this limit is reached, no new Bitcoin can be mined. Cryptocurrency deliberately creates insufficiency to prevent currency manipulation and the decrease of value over time.

4.3 Crypto currencies in modern world

In 21st century, technology is growing rapidly through internet. People all over the world are trying to acclimatize with these technologies rapidly. But in terms of crypto currencies, it becomes dissimilar. The word “Cryptocurrency” refers to a digital currency that is used for making digital transaction, which has no imperative system. Actually, crypto tokens are not created to govern since there is no existence of third party (Bank, Government). This is why it becomes difficult for the government (or countries) to authorize these currencies. Apart from this issue, countries of North America (Canada, US, Mexico), Europe (Germany, France, Malta, Holland, Belarus), Asia (Vietnam, Singapore, Thailand, India) and many countries of South America have shown positive interests in crypto currencies and legalized it [28]. According to COINRIVET, there are 2.503 recognized crypto currencies as of November 21st, 2018. What even more incredible is that there is one Cryptocurrency, Bitcoin (BTC), that makes up 59% of the total market capitalization [29]. As for the rapid growth of crypto currencies now-a-days, world’s leading futurists predict that, crypto currency is going to change the future of finance. [Thomas Frey](#), Google’s top rated futurists’ speaker predicts that “crypto currencies are going to displace roughly 25% of national currencies by 2030. They are much more efficient the way they run.” [30]. The rise of crypto currencies over the past couple years represents “the legitimization of a new asset class emerging alongside the traditional global economy,” according to [Dr. James Canton](#) of the Institute for Global Futures. “I would state that one can expect an exponential increase of new investment vehicles to come from crypto finance.” [31]. Slovenia, one of the smallest countries in Europe, has introduced the first digital crypto currency shopping complex, also called as “Bitcoin City”, located in the capital of Ljubljana where every store (over 500 retail stores) and venture will accept crypto currency and operate via blockchain technology [32]. Holland (another country of Eastern Europe), also hosts a “BITCOIN CITY” where all kinds of transaction including retail purchases, trading, business are completely done by BITCOIN crypto currency. Moreover others countries like Czech Republic, Argentina, United States, Colombia, United Kingdom and France are also developing Bitcoin city following the trend of Cryptocurrency [33].

4.4 Blockchain and Cryptocurrency

Often, people confuse blockchain and Cryptocurrency as being the same, even though the two are different innovations on their own, they both work hand in hand. It is worth noting that Blockchain can be used in other areas other than the decentralized nature it provides to crypto currencies. In recent times, many institutions and governments are contemplating the possibility of making any good use of Blockchain technology. Businesses are now proposing the use of private blockchains to augment work. Blockchain has been devised to keep records of all transactions that take place across a peer to peer network; it works as an anonymous ledger. Although the details of transactions are surreptitiously stored, the ledger is made public. Hence, one can see it to confirm that a transaction took place. The Blockchain technology assists to decrease cost, enhance transparency and allows efficiency. Satoshi Nakamoto created the blockchain to serve the purpose of recording transactions made with bitcoins, thus becoming a public

transaction ledger. This made Bitcoin the first Cryptocurrency to make use of the blockchain in recording all transactions without the hindrance of an outside party or central authority.

Crypto currencies most of the time depend on the blockchain. To mine crypto's such as Bitcoin, the blockchain is inexorable. Blockchain holds a set of blocks with each of the block containing details of transaction data or transactions made with crypto currencies. Each of the individual blocks is made up of puzzles that are being solved by miners to authenticate transactions. After successfully solving the problem, a new block is created and broadcasted to other nodes, and the miner is then rewarded for completing the task. As mentioned earlier, blockchain functions as a ledger for recording all transactions made with crypto currencies, and it may take up to 30 minutes or more for Bitcoin transaction to be recorded. When this happens, details of the transaction are all confirmed and established within a short period across all the nodes. Once a transaction has been recorded, it becomes impossible for the data or information to be modified. The blockchain also ensures that crypto currency wallets gauge their spendable balance so that new transactions can be confirmed, and also ensures that there is no multiple spending.

Chapter 5

Implementation

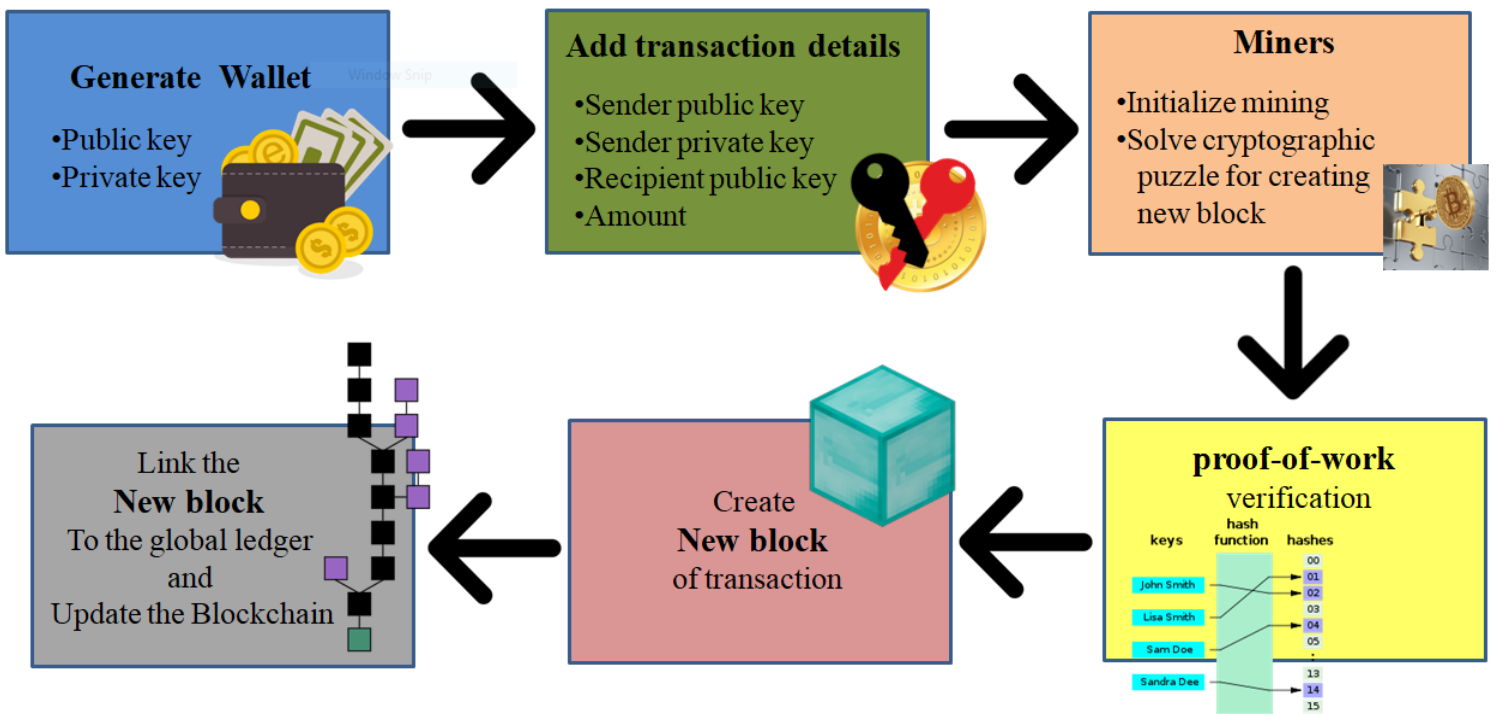


Figure 9: System block diagram

The block diagram of the Cryptocurrency implementation is exhibited in Figure 9. Step 1 is to generate the digital wallet. Once the wallet is produced, the transaction details are added to the “Add transaction details” block as shown in Figure 9. The miners then add the block to the public ledger by solving a cryptographic puzzle. Subsequently the proof-of-work follows. This is the verification of annexation of new block to the distributed public ledger. After the verification the block is validated and added to the chain and the ledger is updated.

5.1 Create Node

Node is an essential part of Blockchain technology that refers to a device connected on blockchain network, which helps to complete the operation of blockchain. An electronic device, maybe it's a computer, phone or printer, as long as it is connected to the Internet, we can mention them as node. In simple words, node is the identity of each user in the vast network of blockchain. The prime function of a node is to maintain a ledger of all transaction processes through the blockchain network from its beginning. Almost all Cryptocurrency uses its own nodes for maintaining the transaction record of their especial token.

Below is the representation of what be falls when a user registers into a blockchain network. To demonstrate our work, we are creating multiple nodes manually in our local host as shown in Figure 10.

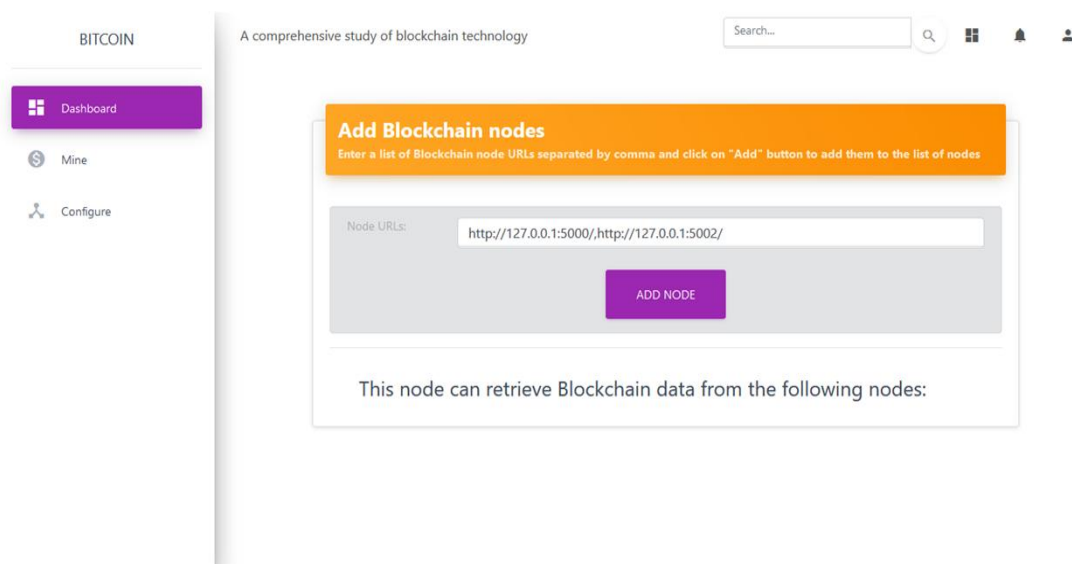


Figure 10: Node initiation

5.2 Wallet Generate

A Bitcoin wallet is used to store bitcoins in your account. Basically there are four types of Wallets:

1. Software based Wallet
2. Mobile Application Wallet
3. Online Based Wallet
4. Paper Based Wallet

As for our demonstration, we have developed online based wallet for our system. Initially a user needs to create a wallet for transactions as shown in Figure 10. A wallet consists of

two keys: public key, private key. The public key and private key comprise two uniquely related cryptographic keys (basically long random numbers). The public key is what its name suggests- Public. It is made available to everyone via a publicly accessible repository or directory. On the other hand, private key must remain confidential to its respective owner. This key pair is mathematically related, whatever is encrypted with a public key may only be decrypted by its corresponding private key. We used RSA cryptographic algorithm to generate public and private keys as shown in Figure 11.

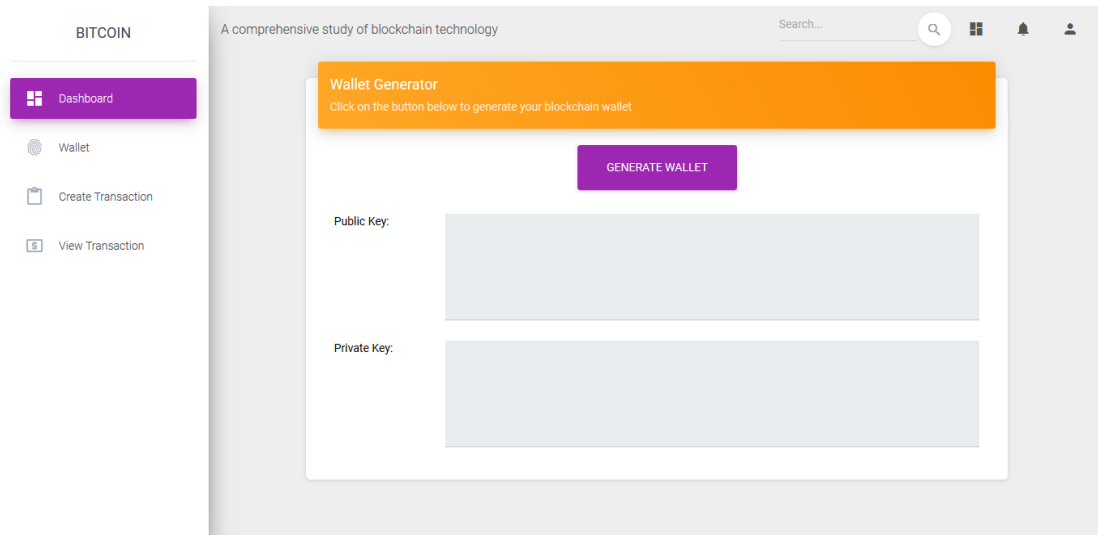


Figure 11: Wallet

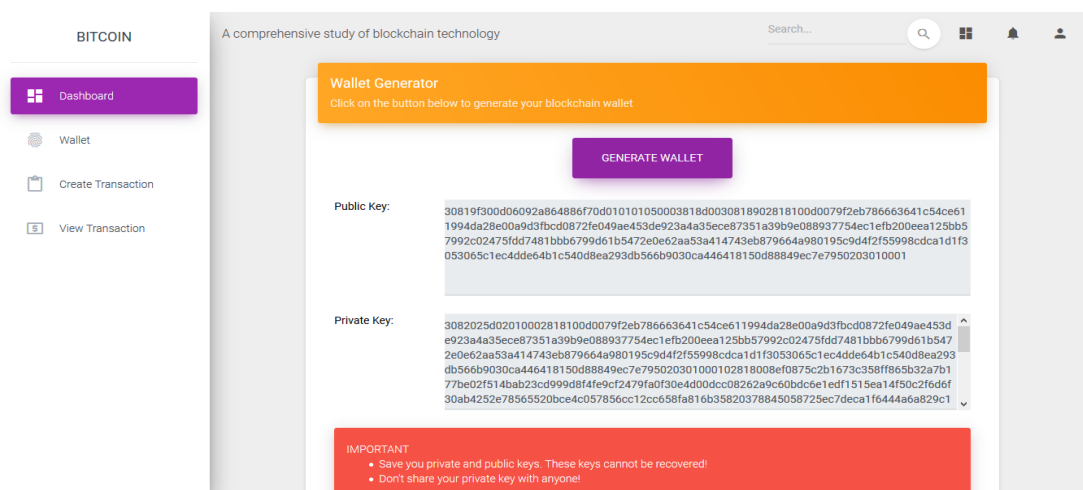


Figure 12: Key generate

5.3 Create Transaction

After having a wallet, a user can send or receive transaction through the Bitcoin network. Have a look at Figure 12, for making a transaction, sender must input his public key, private key, recipients public key (whom you want to send Bitcoin), and the amount of transaction. After fulfilling all credentials, sender is ready to make transaction over the network.

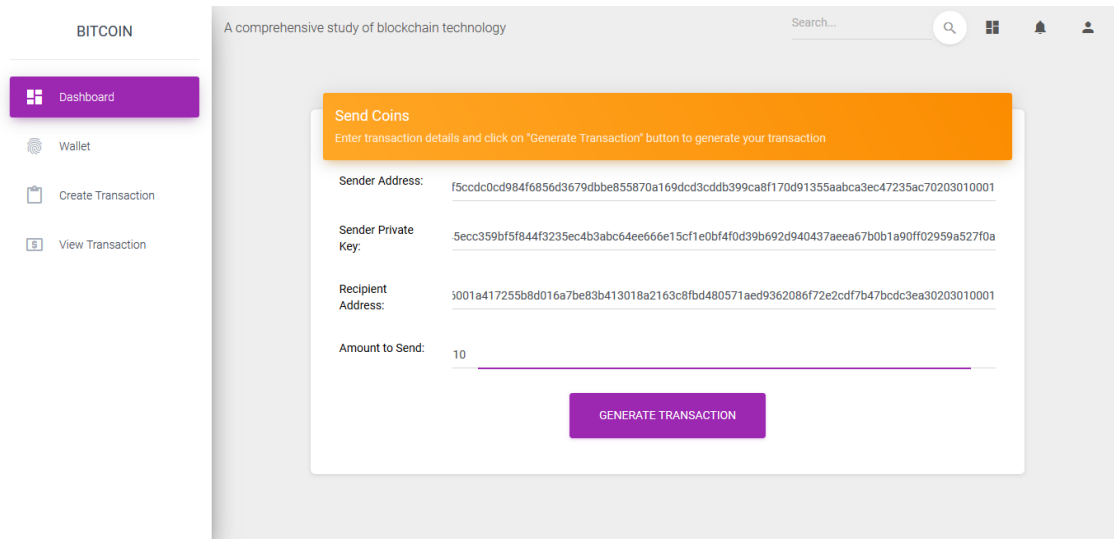


Figure 13: Create transaction

After generating transaction, sender will receive a prompt message to make sure about the transaction and send it to the recipient’s address as shown in Figure 13. To be exact, this is just the conformation of the transaction as shown in Figure 14.

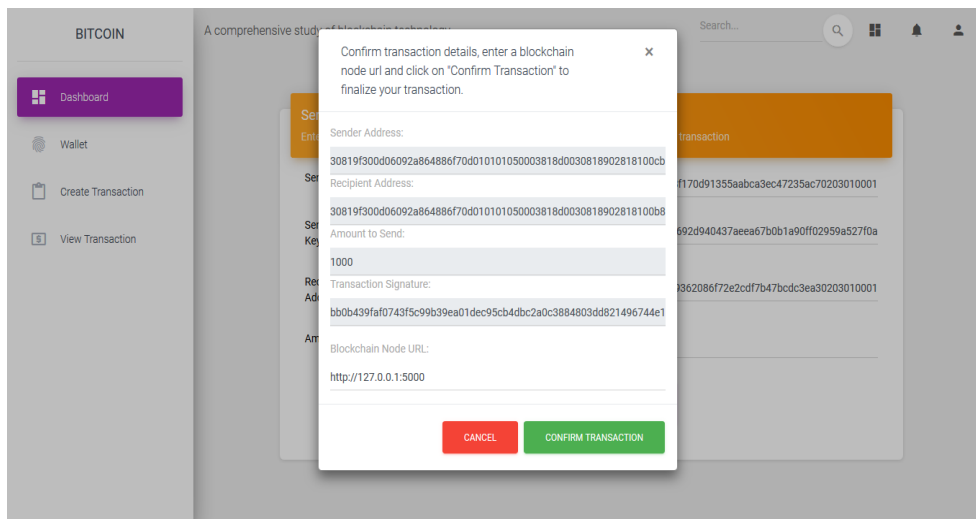



Figure 14: Confirmation

5.4 Mining Block


Mining is the process of verifying new transaction as well as adding the newly created transaction information to Bitcoin's public ledger along with older transactions. This public ledger has all information of each transaction, which is referred to as the Blockchain. Every transaction will need to be verified through the network after the mining process, then it will be added to the blockchain as a new block. Bitcoin uses a consensus algorithm to prevent the double-spending problem of this virtual currency that has already been used anywhere, which makes it more secure and trustworthy among cryptocurrency users. The mining process is premeditatedly made difficult so that the total number of blocks found by miners every day remains stable. When a new transaction comes, miners begin to solve the mathematical puzzle to add the new block into the chain as shown in Figure 15.

Mine Block

Refresh the button for block update & enter Mine for mining a block

Transactions to be added to the next block 

Show entries Search:

# 	Recipient Address	Sender Address	Value
1	30819f300d06092a864886f7...	30819f300d06092a864886f7...	10

Showing 1 to 1 of 1 entries Previous Next




Figure 15: Mining

When mining is completed, it will verify by others (nodes) on the network and then new block is created and added into the chain as Shown in Figure 16.

Show entries
Search:

#	Recipient Address	Sender Address	Value
No data available in table			

Showing 0 to 0 of 0 entries
Previous Next

MINE

Transactions on the Blockchain

↻

Show entries
Search:

#	Recipient Address	Sender Address	Value	Timestamp	Block
1	30819f300d06092a864886f7...	30819f300d06092a864886f7...	10	Jan 25, 2019, 3:22:13 PM	2
2	612e3f0893c341228d0fae99...	Miner Rewarded	1	Jan 25, 2019, 3:22:13 PM	2
3	30819f300d06092a864886f7...	30819f300d06092a864886f7...	20	Jan 25, 2019, 3:23:06 PM	3
4	612e3f0893c341228d0fae99...	Miner Rewarded	1	Jan 25, 2019, 3:23:06 PM	3
5	30819f300d06092a864886f7...	30819f300d06092a864886f7...	15	Jan 25, 2019, 3:27:13 PM	4
6	612e3f0893c341228d0fae99...	Miner Rewarded	1	Jan 25, 2019, 3:27:13 PM	4

Showing 1 to 6 of 6 entries
Previous 1 Next

Figure 16: Transaction History

Chapter 6

Conclusion

Blockchain technology runs the Bitcoin Cryptocurrency. All the transaction of blockchain is recorded into a public ledger which is visible to everyone because its environment is decentralized. Blockchain ambition is to provide anonymity, security, privacy, and transparency to all its users. The uses of blockchains are appearing in a variety of commercial applications today. It is useful to understand in the context of Bitcoin. Blockchain is the advanced technology that maintains the Bitcoin transaction ledger. Bitcoin is the first attempt at maintaining a decentralized, public ledger with no formal control or governance. On the other side, private distributed ledger and blockchains can be deployed to solve the several problems. Every sector has pros and cons and they are tradeoffs to each solution. Consider these individually for each individual use case. Though, Cryptocurrency is not in any way a monetary investment in a real currency. Alternatively, buying into Cryptocurrency is an investment into a possible future where it can be exchanged for goods and services—and that future may be arriving sooner than expected.

References

- [1] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, “Blockchain-Based E-Voting System”.
Available: <https://skemman.is/bitstream/1946/31161/1/Research-Paper-BBEVS.pdf>
- [2] Algemene info van pro-Ethereum Available: <http://www.bestebank.org/ethereum/>
- [3] “The blockchain stores, manages, protects and transfers this smart information”
Available: <https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu-blockchain-internet-things-supply-chain-traceability.pdf>
- [4] NIKHIL LOHADE, “Dubai Aims to Be a City Built on Blockchain”, 24-4-2017”
Available: <https://www.wsj.com/articles/dubai-aims-to-be-a-city-built-on-blockchain-1493086080?prclt=DyD2kRRG>
- [5] COMPUTABLE, “Microsoft levert gratis blockchain-testomgeving”, 10-02-2017”
Available: <https://www.computable.nl/artikel/nieuws/finance/5951836/250449/microsoft-levert-gratis-blockchain-testomgeving.html>
- [6] The New York Times, “What Is Bitcoin, and How Does It Work?” Available: <https://www.nytimes.com/2017/10/01/technology/what-is-bitcoin-price.html>
- [7] BLOCKGEEKS. Available: <https://blockgeeks.com/guides/blockchain-applications/>
- [8] Cory Sarver, Intro to Blockchain and Cryptocurrency. [online]
Available: <https://www.igrad.com/articles/intro-to-blockchain-and-cryptocurrency>
- [9] Khudnev and Evgenii, "BLOCKCHAIN: FOUNDATIONAL TECHNOLOGY TO CHANGE THE WORLD".
Available:
https://www.theseus.fi/bitstream/handle/10024/138043/Evgenii_Khudnev_Thesis.pdf?sequence=1
- [10] Satoshi Nakamoto “Bitcoin: A peer to peer electronic cash system”.
Available: www.bitcoin.org
- [11] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi*, Sooyong Park and Kari Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review"
Available:
https://www.researchgate.net/publication/308877750_Where_Is_Current_Research_on_Blockchain_Technology-A_Systematic_Review
- [12] Sam Yang, “The Blockchain: Tamper-Proof Technology”.
Available: <https://medium.com/@stufffromsam/the-blockchain-tamper-proof-technology-3544969c222d>
- [13] Coindesk “Bitcoin Hash Functions Explained”.
Available: <https://www.coindesk.com/bitcoin-hash-functions-explained>
- [14] Lisk Academy “Hashing”.
Available: <https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/what-is-hashing>
- [15] Investopedia “Genesis Block”
Available: <https://www.investopedia.com/terms/g/genesis-block.asp>
- [16] Marc Pilkington, "Blockchain Technology: Principles and Applications".
Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660
- [17] CoinSutra, “What Is The Bitcoin Mempool & Why It Matters??”, Available: <https://coinsutra.com/bitcoin-mempool/>

- [18] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" Available: <https://bitcoin.org/bitcoin.pdf>
- [19] CoinDesk, "How bitcoin Mining Works?", Available: <https://www.coindesk.com/information/how-bitcoin-mining-works>
- [20] Sukant Khurana, A very basic introduction to Blockchain In Cryptocurrencies [online] Available: <https://medium.com/@sukantkhurana/a-very-basic-introduction-to-blockchain-in-cryptocurrencies-974be2914d96>
- [21] Global Information Assurance Certification Paper, "A study on hash functions for cryptography". Available: <https://www.giac.org/paper/gsec/3294/study-hash-functions-cryptography/105433>
- [22] Article in The Computer Journal · March 1975, "Hashing Functions". Available: <file:///C:/Users/Ambia/Downloads/hashingfcts.pdf>
- [23] Mahdi H. Miraz and Maaruf Ali, "Applications of Blockchain Technology beyond Cryptocurrency ",Annals of Emerging Technologies in Computing (AETiC),Vol. 2, No. 1, 2018. Available: <https://arxiv.org/ftp/arxiv/papers/1801/1801.03528.pdf>
- [24] IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July 2013, "Broad View of Cryptographic Hash Functions". Available: Broad View of Cryptographic Hash Functions
- [25] Garrick Hileman and Michel Rauchs, "2017 Global Blockchain Benchmarking Study". Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224
- [26] BlockchainHub, "Blockchains & Distributed Ledger Technologies", Available: <https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/>
- [27] Movable Type Scripts, "SHA-256 Cryptographic Hash Algorithm", Available: <https://www.movable-type.co.uk/scripts/sha256.html>
- [28] List of Countries Where Bitcoin/Cryptocurrency Is Legal & Illegal [online] Available: <https://blog.sagipl.com/legality-of-cryptocurrency-by-country/>
- [29] How many cryptocurrency are there? [online] Available: <https://coinrivet.com/how-many-cryptocurrencies-are-there/>
- [30] Cryptocurrency will replace National Currencies by 2030. [online] Available: <http://money.com/money/5178814/the-future-of-cryptocurrency>
- [31] Slovenia Plays Host to the World's First "Bitcoin City" by Nick Marinoff [online] Available: <https://bitcoinmagazine.com/articles/slovenia-plays-host-worlds-first-bitcoin-city>
- [32] Alexandra Talty, The Top 10 Bitcoin Cities In The World. [online] Available: <https://www.forbes.com/sites/alexandratalty/2018/07/31/the-top-10-bitcoin-cities-in-the-world/#3279fb384565>
- [33] List of Countries Where Bitcoin/Cryptocurrency Is Legal & Illegal [online] Available: <https://blog.sagipl.com/legality-of-cryptocurrency-by-country/>