

A Survey on Blockchain and its Application Prospect

By

Zahiruddin Ahmed Chisty
ID: 181-25-654

This Report Presented in Partial Fulfillment of the Requirements for the
Degree of Master of Science in Computer Science and Engineering.

Supervised By

Md Zahid Hasan

Assistant Professor & Associate Head (In-Charge)
Department of CSE
Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

November 2018

APPROVAL

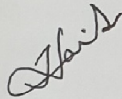
This Thesis titled “A Survey on Blockchain and its Application Prospect”, submitted by Zahiruddin Ahmed Chisty(ID:181-25-654)to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of M.Sc.in Computer Science and Engineering and approved as to its style and contents.

BOARD OF EXAMINERS

Dr. Syed Akhter Hossain
Professor and Head

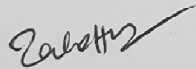
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Chairman



Dr. SheakRashedHaiderNoori
Associate professor and Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Md Zahid Hasan
Assistant Professor & Coordinator of MIS
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Dr. MohammadShorif Uddin
Professor
Department of Computer Science and Engineering
Jahangirnagar University

External Examiner

DECLARATION

I hereby declare that, this thesis has been done by me under the supervision of **Md Zahid Hasan, Assistant Professor, Department of CSE**, Daffodil International University. I also declare that neither this thesis nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

Md Zahid Hasan
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Submitted by:

Zahiruddin Ahmed Chisty
ID: 181-25-654
Department of CSE,
Daffodil International University

ACKNOWLEDGEMENT

First of all, our heartiest thanks and gratefulness to Almighty Allah for His divine blessing that makes us capable to complete this project successfully.

We would like to thanks to our honorable teacher & project supervisor **Md ZahidHasan, Assistant Professor, Department of CSE**, Daffodil International University for his endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior draft and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to **Dr. Syed Akhter Hossain**, Head, Department of CSE, for his kind help to finish our project and we are also thankful to all the other faculty and staff members of our department for their co-operation and help.

We must acknowledge with due respect the constant support and patients of our parents.

Finally, we would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

ABSTRACT

This thesis is on “**A Survey on Blockchain and its Application Prospect**”.Blockchain has proved its potential by implementing Bitcoin, a modern crypto currency network. However, Blockchain can do more than this. Traditional system architectures can be replaced by this architecture since it provides more security, persistence, transparency to the participants. Blockchain executes as a decentralized framework which thus brings more data security and safety. It has its own limitations and more research work on this is required. This paper provides a clear concept of Blockchain architecture and overview on major research work. Furthermore, it also presents a couple of new idea which can solve existing problems if the implementation is right. Future research scope and possibilities is also listed in this article.

TABLE OF CONTENTS

CONTENTS	PAGE
Approval	ii
Declaration	iii
Acknowledgements	iv
Abstract	v
Table of Contents	vi
List of Figures	viii
CHAPTERS:	
CHAPTER 1: INTRODUCTION	01-03
1.1 Background	01
1.2 Motivation	03
1.3 Objectives	03
1.4 Report Layout	03
CHAPTER 2: LITERATURE REVIEW	04-16
2.1 Introduction	04
2.2 Related Works	04-15
2.2.1 Proof of Work (PoW)	05
2.2.2 Proof of Stake (Pos)	06
2.2.3 Scalability	08
2.2.4 Anonymity	09
2.2.5 Smart Contract	10
2.2.6 Hawk Model – Privacy Preserving Smart Contract	12
2.2.7 Blockchain and IoT powered by Smart Contract	13
2.2.8 Music Industry	13
2.2.9 Selfish Mining	14
2.2.10 Attacks on Blockchain	14
2.3 Scope of Problems	15
2.4 Research Challenges	16
CHAPTER 3: ARCHITECTURE OF BLOCKCHAIN	17-25
3.1 Short History of Bitcoin	17
3.2 Blockchain Network	17-20
3.2.1 Architecture	17
3.2.2 Blocks	18
3.2.3 Types of Blocks	19
3.2.4 Chain	19
3.2.5 Digital Signature	20
3.2.6 Transactions	20
3.3 How Blockchain Works	21
3.4 What is Mining?	24
CHAPTER 4: RESEARCH SCOPES & RECOMMENDATIONS	26-29
4.1 Blockchain in Agriculture	26-28
4.1.1 Background	26

4.1.2	Problem Scope	26
4.1.3	Blockchain and Smart Contract Integration in Agriculture Sector	27
4.1.4	Detect and Resolve Illegal Actions	28
4.2	Distributed Database	28
4.3	Blockchain for Product History	37
4.4	Supply Chain Tracking	37
4.5	Secure Donation Transparency	37
CHAPTER 5: CONCLUSION & FUTURE SCOPE		38
REFERENCES		39

LIST OF FIGURES

FIGURES		PAGE NO
Figure- 2.2.2A	Screenshot of QuantumMechanic's suggestion of PoS in forum	14
Figure- 2.2.2B	Image of 51% attack	15
Figure-3.2.1A	A sequence of blocks in a Blockchain	26
Figure-3.2.2A:	A block structure	27
Figure-3.2.7A	Blockchain generation from unordered transactions	30
Figure-3.2.7B	Math race to protect transactions	31

CHAPTER 1

INTRODUCTION

1.1 Background

In a white paper[1] published in November 2008, Satoshi Nakamoto proposed Bitcoin as the first electronic payment system based on a decentralized peer-to-peer network, without the need for a trusted third party which was implemented in 2009. Blockchain, the core technology of this system, is widely acknowledged as a major invention in fault-tolerant distributed computing since researches were going on for decades.

Blockchain could be acknowledged as a **public ledger** and all valid and verified transactions are stored in a list of blocks. As new blocks append frequently, the chain grows continuously. The security is maintained by implementing **asymmetric cryptography** and **distributed consensus algorithms**. Each and every transaction is verified by the majority of participant's consensus algorithm through the system before storing in the public ledger. Each information is secured, so once a data entry performed, it can never be removed or tampered. The Blockchain contains the history of every action or transaction ever made in the system. To simply this observation Blockchain uses an analogy, it is easy to tamper/steal something in private whereas impossible when most people are monitoring it in a public place. So by making the system publicly available to the participants while they are observing and verifying every transaction/change request, the platform became more secure. This technology generally has key characteristics of decentralization, persistency, anonymity, and auditability. With these merits, Blockchain can greatly save the cost and improve efficiency.

Blockchain technology has worked flawlessly over the years and is being successfully applied to both financial and non-financial world applications. Marc Andreessen, the doyen of Silicon Valley's capitalists, listed the Blockchain ***distributed consensus model*** as the most important invention since the Internet itself. Johann Palychata from BNP Paribas wrote in the Quintessence magazine that Bitcoin's Blockchain, the

software that allows the digital currency to function should be considered as an invention like the steam or combustion engine that has the potential to transform the world of finance and beyond[3].

The current digital economy and online transactions are based on the **reliance** on a certain trusted authority. Email service provider confirms the email delivery; certification authority verifies that the digital signature is valid; bank tells us that our money is safe and our transaction is secured via their channel. The aforementioned examples can prove that the current world is relying on a third entity for the security and privacy of the digital assets.

These third-party entities can be hacked, manipulated or compromised. This is where the Blockchain technology works perfectly. It facilitates the *distributed consensus* any types of online transaction including digital assets, payments can be verified. It does this without compromising the privacy of the digital assets and parties involved. The *distributed consensus* and *anonymity* are two important characteristics of Blockchain technology.

The advantages of Blockchain technology outweigh the regulatory issues and technical challenges. One of the important emerging features of Blockchain technology involves **Smart Contracts**. Smart contracts are basically software programs that can automatically execute according to the terms of a contract. When a smart contract's predefined condition becomes true among participating candidates then the contract agreement executes automatically such as making payments or transactions to a specific entity as per the contract information.

Another emerging concept is Smart Property which is related to control property or asset ownership via Smart Contracts agreement. The asset can be non-physical or digital like company shares, bonds, equity; or physical like a home, car, land, or a smartphone. Digital currency like Bitcoin works like this, they are purely based on the concept of money.

1.2 Motivation

Blockchain is now being addressed as the best invention in this century after the internet. It has received significant attention from experts. The concept of decentralization security and removing the third-party trusted institutions from two parties changed the regular way of work. Moreover, Smart Contract implementation became simple and IoT devices are way smarter than the last decade. Combining these technologies, we can overcome major issues from various sectors.

1.3 Objectives

The main goal of this paper is to give a basic understanding of the Blockchain network to the general user. This paper combines previous research works and implementations with current issues. Blockchain as a technology can solve many existing problems and can open the doors of numerous opportunities. This paper focuses on the Blockchain framework and uses Bitcoin as an example since this is the major breakthrough of this architecture. Previous research articles, journal papers, blogs, wiki, Blockchain forum threads are used in this technical survey paper to present a clear concept to general people. This paper also provides suggestions and ideas to overcome known existing challenges.

1.4 Report Layout

This paper is divided into several sections. Chapter 1 presents the introductory information and objectives. Chapter 2 discuss the main literature review which includes the related work in the Blockchain domain. This presents the major research works summary on the Blockchain. Chapter 3 describes the Blockchain architecture, building blocks of this architecture, how things work and the underlying concepts. Chapter 4 focuses on future research scopes and recommendations. In that section, new ideas and possible solutions for existing issues, limitations will be discussed. Images are attached in different sections based on demand. The very last section contains the references of published research articles, journal papers, wiki pages, articles, blogs, forum threads etc which is used in this paper.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

In the recent world, Blockchain is becoming a new trend and replacing a lot of old systems with its architecture. Being a very reliable, distributed, public protocol, it addressed security, privacy related issues from a different angle which people didn't think about before. Continuous research work is going on now for further integration since people don't know what will be the global scope of this network can be in the future. Moreover, researchers are thinking that the latest trend, Internet of Things (IoT), has a great scope to improve its scalability, portability, security, and things can be automated using Smart Contract etc. In this chapter, recent and related works will be discussed in a brief manner.

2.2 Related Works

Satoshi Nakamoto, the inventor of Blockchain, focused on the peer-to-peer distributed network which resulted in implementing an electronic cash system. In his paper [1], he redefined the meaning of money and solve the core problem. Utilizing participating entity's computer power he managed to provide the full-fledged network architecture where people can participate and mine through Blockchain. The key issues introduced here is the concept of proof of work, public-private chain, a mathematical calculation to verify the block and transaction validity etc.

As transactions are taking place continuously and Blockchain tries to maintain a distributed public ledger, the nodes in the whole network need to agree on the transaction validity as well as the order of the transaction list. Each node keeps a local copy of the ledger. So data should be synced throughout the entire network. Otherwise, the individual copies will diverge and the network will face different lengths of data in different forks. A different fork will have a different view of the current state and no unique order will be there which will eventually lead to a failure of the network. Since there is no central node or authority to control this issue, a

distributed consensus mechanism is introduced to achieve that. There are different types of consensus mechanism [1].

2.2.1 Proof of Work (PoW)

Proof of work (PoW) is a consensus strategy. In a decentralized network, all nodes should agree on the order of transactions for the next block and would choose depending on the majority. But any single entity can join in an open network with multiple instances and can try to influence the network on its favor. This could be happened by a group of nodes as well. In other words, the minority can take control over a network. Satoshi Nakamoto addressed this issue by making the computation work of mining expensive. Since the computing power of a single entity is limited, multiple instances of it cannot do any better on its favor. Any node can append their next block in the chain if they can choose the right nonce in that block's header which will go through the SHA-256 hash algorithm to make a number of specific leading zeroes. The more leading zeroes are required, the more difficult the solution of the puzzle is. Each node needs to solve this mathematical puzzle which is the PoW. It can be verified the other nodes easily as checking this function is faster.

Sometimes it could happen that two competing nodes create blocks almost simultaneously which eventually can lead to a fork. This can be resolved by checking the next block since the PoW mechanism also chooses the longest fork as the main fork and it is very much unlikely that both fork again creates the next block simultaneously. If it is the case, it can be solved by checking the next block and so on. The network always chooses the fork which contains the longest chain. This allows the consensus to reach a solid conclusion. As a PoW, Blake-256 and scrypt hashing algorithm are used (Litecoin) beside SHA-256 [3][8].

2.2.2 Proof of Stake (PoS)

Proof of Stake (PoS) is an alternative to proof-of-work that requires far less CPU computation for mining. This works same like PoW but in a different manner. Instead of CPU power, participants are using their currency to vote the next block. On July 11, 2011, a user from Bitcoin forum with id *QuantumMechanic* proposed this architecture in a thread.

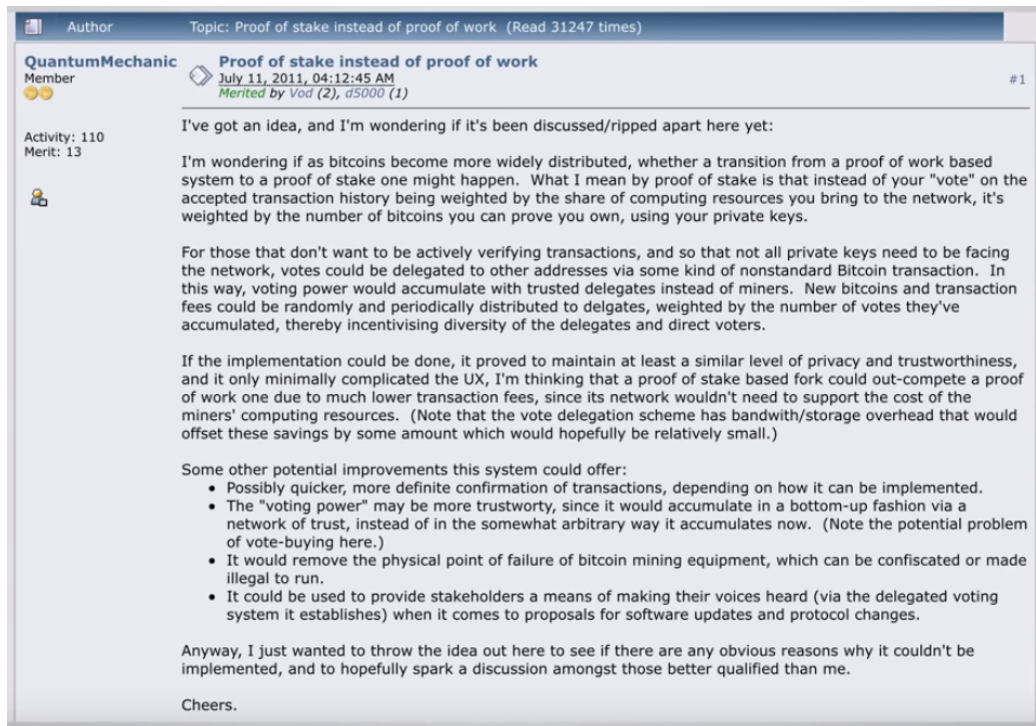


Figure- 2.2.2A: Screenshot of QuantumMechanic’s suggestion of PoS in forum

In PoS, the network chooses a validator node randomly for validating the next block. To become a validator, each node needs to deposit some reward point or currency in the network as a stake. Getting chance of being selected as a validator by the network is directly proportional to its deposited amounts. So, if miner A deposited 100 reward point and miner B deposited 1000, miner B has 10 times more chances of being selected as a validator by the network. This might seem like that the rich miner gets more chances than a poor miner, but this is fair compared to PoW. Since PoW uses electricity as an invest, rich can get a great deal on buying more electricity and powerful computation equipment. Hence, the more they buy the better prices they can get.

So when the validator signs the block as a valid one and the new block appends on the chain, validator gets reward points from the network associated with that transaction. If any validator participant is not honest in his work, the deposited money will be taken off from his network. Hence, as long as the reward point is lower than the deposited money, other miners can trust the validator. In terms of how this works technically, the simplest setup is a model that has been called the “simulated mining

rig”: essentially, every account has a certain chance per second of generating a valid block, much like a piece of mining hardware, and this chance is proportional to the account’s balance. The simplest formula for this is:

$$SHA256(\text{prevhash} + \text{address} + \text{timestamp}) \leq 2^{256} * \text{balance} / \text{diff}$$

Here, prevhash is the previous block’s hash; the address is the validator miner’s address; timestamp is current Unix time in second; the balance is the stake miner’s account balance; diff is a global adjustable difficulty parameter. If any account satisfies this equation at any particular time, it may produce a valid block [9].

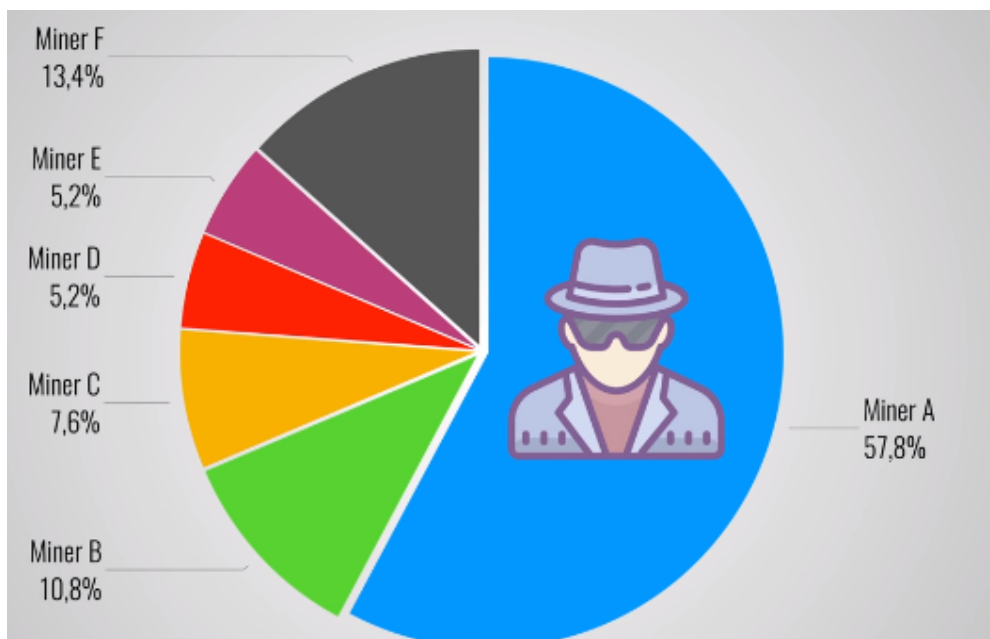


Figure- 2.2.2B: Image of 51% attack

But there is a chance that a single richest node or a group of nodes can create a monopoly situation and dominate the whole network and can create invalid blocks or transactions over time. This is called as 51% attack. To address this types of fraudulent actions, the network takes some actions. It holds the reward points for a certain period of time to verify the actions of the validators. If any other node or the network can detect any fraud action or invalid block in the chain, the reward point and deposited balance will be deducted as a penalty. Moreover, gaining 51% market capital is not possible at all since it is quite a large number.

Furthermore, to avoid fraudulent actions, the network will hold the reward point for a certain period of time since it wants to verify the actions of the validator for that period. If in this period, any other validator can prove a fraud action of any validator node, it will get a portion of the penalty money.

PoS certainly mitigate the overhead of using unnecessary electricity and computation power by using its scheme. Blockchain [11] uses randomization to predict the next generator. It uses a formula that looks for the lowest hash value in combination with the size of the stake. Peercoin favors coin-age based selection. It is another great way to choose the next validator. In Peercoin, older and largest sets of coins have a greater probability of mining the next block. Many Blockchains adopt PoW at the beginning and transform to PoS gradually. For example, Ethereum [12] is planning to move from Ethash (a type of PoW) to Casper (another type of PoS).

2.2.3 Scalability

Blockchain becomes bulky since it is continuously growing and appending new blocks. As because each node should have the ability to mine or verify any transaction, all the information of previous transactions need to be stored in their storage. But, the block size is limited and there is a fixed time interval for validating any transaction. For example, Visa handles on average 2000 transactions per second whereas PayPal 10 million a day. But Bitcoin still restricted to 7 transactions per second due to the restricted block size [13]. Hence, many transactions are delayed and fall in a queue. Additionally, miners prefer to work on big transactions since more reward point is involved in this work.

People were not concerned about this issue at the beginning. But, now in 2018, the size of the headers of the whole Blockchain is 186 Gigabyte (191,454 Megabyte to be exact) [14]. The core developers of Bitcoin tried to improve this situation by switching the database from Berkeley DB to LevelDb[15]. Berkeley DB is much slower compared to LevelDB and that switching resulted in a major performance boost in terms of synchronization and block verification speeds.

J.D. Bruce proposed a solution in his paper to address this by implementing mini Blockchain along with account tree. The account tree is a structure which will store all the non-empty addresses and the balances of those addresses. It is like a decentralized balanced sheet. If the balance of the addresses updated, the tree is also updated with new numbers. Since it is keeping only the addresses, the size will be relatively small. Additionally, the concept of mini Blockchain is it will be the same as normal Blockchain, except that the historical records will not be there. There will be a time limit as a security measure and after that period, the blocks will erase previous data [16].

Some researchers published a paper in 2016 introducing a new scalable Blockchain protocol named Bitcoin-NG with experiment data. They have shown that they gained huge performance improvement by decoupling Blockchain operation into two phases: *leader election* and *transaction serialization*. This protocol divides time into epochs. In each epoch, a single leader takes the ownership to serialize the transactions. The protocol introduces two types of blocks: *key blocks for leader election* and *micro blocks that contain the ledger entries*. Key blocks will contain previous block's reference data that previous block could be another key block but generally, it is a micro block. All the subsequent micro blocks use the key block's public key. In Traditional Blockchain implementation of Bitcoin, there is a waiting time between two block creations. But in NG, the leader block creates the micro block as soon as possible according to the network bandwidth. The PoW is implemented by the leader block only. No micro block keeps this data. Moreover, this micro block does not add weight to the chain [17].

2.2.4 Anonymity

Blockchain maintains the necessary privacy among the participants. Users participate in a transaction through asymmetric encryption and do not disclose the real identity. However, transactional privacy is not available in Blockchain since the transaction information is available to the entire network. Moreover, Barcelo's paper [28] shows that user's information can be achieved by using their transaction information. Biryukov also published a conference paper [29] showing that using user's id and IP address information, user's information can be gained even if the user is behind the

firewall. If there is no privacy and user information is available, then secret groups and illegal mining will gain advantages. In order to address this issue, various solutions are proposed.

Mixing is one of the proposed solutions which facilitates the privacy by doing the transaction in several phases. It divides the input to multiple instances and also the same for the output. Funds are transferred to multiple output addresses from multiple input addresses. For example, if user A wants to send fund to user B, they will not transfer directly since it will reveal their relationship. They will use another intermediate user C who will take the fund from user A in several inputs and transfer that to B in several outputs [30].

However, the intermediate user could be dishonest. It could reveal the privacy or transfer the fund to its own address. Mixcoin [31] solves this problem by using encryption. The fund amount and date is encrypted with the private key. Hence, if the intermediate user does not pay the money, anyone can verify that.

Zerocoin integrates another approach for anonymity. Instead of validating the transaction, miners just verify the coins if they belong to the valid list of coins or not. The information of paying entity is not available. However, receiving entity's information is still available in this system.

2.2.5 Smart Contract

The term Smart Contract was first used by Nick Szabo which he described as “it is a computerized transaction protocol that executes the terms of a contract” [18]. Later, he proposed to replace the contractual conditions by programming language codes and embed them into hardware and software entity so that they can apply them by their own upon meeting the conditions [19]. This approach can minimize the involvement of third-party trusted organizations in transactions. As a basic example, we can take a ATM machine or Coca-cola vending machine which only verifies the debit/credit card or valid money as an input; returns the cash or product as an output.

In the context of a Blockchain, smart contracts improved the scenario a lot. They are like some scripts stored in the Blockchain. People can think this as a stored procedure script in SQL Server or any relational database management system [20]. Each contract has a unique address and it is stored in the Blockchain. Hence, the contract is distributed among all the participants when it is released in the chain. Anyone can create a contract and release it in the Blockchain. If any transaction triggers the contract condition, it will execute its code and apply changes in the Blockchain.

To make this more clear we can think of an example like this- A, B, C are three participants and there are different types of digital assets like p,q,r etc in a Blockchain. A now deploys a smart contract *Contract-ZZ* on the network defining these:

- *Store function*: this function gives a user an option to store some p types asset into that contract.
- *Trade function*: this function allows a user to trade to anyone with 1 p asset to 3 q type asset. So, $1p=3q$ and $2p=6q$ etc.
- *Encash function*: this function allows a user to retrieve all the asset he has from the contract.

Now, user B can call Store function by 5 p types assets and store them in the contract. Later, user C who owns 50 q type assets, can call the trade function with 15 q assets and get back the 5 p assets. Before executing this operation, the contract checks and validates its conditions. After a successful execution, user B and C can retrieve the asset by using the Encash function. The whole transaction is stored in the network. This is very secured since the operations are executing in a distributed manner. Everyone is validating these transactions and verifying it [3].

Bitcoin first used the basic smart contract to send some currency from one person to another. But it has its own limitation as it can only use currencies for use cases. Ethereum first facilitates a way to implement its own program with Solidity programming language which can be used for any types of transactions [23]. In Ethereum white paper [24], they are naming it as “autonomous agents”. One smart

contract can work with other smart contracts and can provide utility function to other contacts.

Smart Contract runs in a deterministic fashion. Hence in any circumstances, the same input will result in the same output. In a valid Blockchain, it is not possible to write a contract which is non-deterministic. Programming language Solidity is used to write a contract, which itself does not support any non-deterministic constructor [21]. If somehow any user manages to write a non-deterministic contract, he will not be able to deploy that in the network. The platform will reject that on its own [22].

Smart contracts are immutable, thus it is not possible to modify the criteria and output clauses after a successful deploy. Since it is distributed, everyone is validating the clauses for a smart contract transaction. Hence, it is not possible to tamper the transaction data [25].

2.2.6 Hawk Model – Privacy Preserving Smart Contract

Since the transactions of smart contracts are visible to the entire network, there is no way to keep the anonymity of related parties. Hawk Model, a framework for preserving the privacy of smart contracts was published in 2016 from Maryland and Cornell University to address this issue [26]. Anyone can write a Hawk program without knowing programming and this framework will take care of the cryptography protocol, privacy measurement itself. It gives 2 types of security assurance:

- On-chain privacy: It will guard the transaction from the public. So, only parties involved in the transaction can know each other. Data is not visible to the whole network.
- Contractual security: By using this, the contractual parties in a transaction can protect their information from each other. Hawk will manage the necessary information for the transaction.

Transactional privacy is sometimes necessary since it hides the identity of different parties which eventually restrict themselves to communicate via other channels. Hawk provides additional contractual security measures like this:

- Secured Input: If the contracts takes arguments from different users and choose a specific one based on some condition, it does not reveal other user's information. For example, if the contract is for highest bidding then one user will not be able to see others bid information.
- Posterior privacy: If the manager doesn't unveil the bid, the information will be kept private after the auction as well.
- Financial Security: Involved parties may want to abort at an early stage after gaining some asset. This is solved by imposing a financial penalty from the framework to those parties. This penalized amount will be distributed among the honest parties.

2.2.7 Blockchain and IoT Powered by Smart Contract

IoT devices need regular updates from their manufacturer company. Maintaining this from the manufacturer side is very costly since there are millions of devices worldwide which they might have discontinued for years. If all these devices can stay in their own Blockchain network, they can trust each other. Manufacturer company can release a new firmware update by deploying a Smart Contract. Devices which has the minimum requirement can install the updates [3].

As Blockchain supports peer-to-peer communication, it is also facilitates the communication between IoT devices. Smart devices have the ability to work alone and work on demand. By using some smart contracts, these smart devices can communicate and share their work when necessary. For example, some smart solar panels generate extra resources whereas some don't fulfill the required portion. This total bandwidth can be distributed among the whole network by maintaining some smart contract clauses.

2.2.8 Music Industry

The music industry is worth an estimated USD 45 billion globally. This sector is facing more challenges every day with the copyright issue, recording issue etc. Middlesex University published a paper in 2016 which proposed to maintain a network database for music copyright information [27]. According to the researcher, there will not be one single database that documents ownership of all song and

recording copyrights. Instead of this, there will be a large number of databases, none entirely comprehensive. This architecture will support:

- A networked database for music copyright information.
- Fast, frictionless royalty payments.
- Transparency through the value chain
- Access to alternative sources of capital.

2.2.9 Selfish Mining

Selfish mining is a process in which a miner or a group of miners keep their newly created block private for a period of time. They don't broadcast it to the network. Instead, they keep mining on it and thus create a private chain fork. After a while, when they have grown up enough long chain, they reveal the entire chain to the network. Since this new branch is longer than the public chain, all the miners will accept this chain and merge to their system. When the integration is done, the selfish miners will take the reward points.

This is not fair to the honest miners since their work on the public Blockchain goes in vain and all the resources they have used are wasted. They put their work on a useless branch while selfish miners are mining privately without any kind of competition. Selfish miners can gain using this technique but the honest miners lose resources without any gain.

Heilman proposed a technique to the honest miners to choose the right branch on a Blockchain. They should choose more fresh blocks using the timestamp. However, this will not work if the timestamp is not available. Zeroblock scheme gives a good solution to this. There will be a strict time limit and new blocks should be revealed to the network within this time frame. The network will not accept a long chain all of a sudden. In this scenario, selfish miners gain the same usual reward.

2.2.10 Attacks on Blockchain

Previously we discussed the 51% attack which is very easy for a small chain. Although smart contracts are very helpful, it could cause vulnerable situations in some scenario. In Ethereum, the implementation of the smart contract is error prone.

Solidity, the programming language supported by Ethereum has a good amount of share on this. Some of its semantics are not properly aligned and a programmer can use it in a wrong fashion. Solidity is a Javascript alike language which supports exceptions, functions, delegates etc. Some of its architectural code is a bizarre.

Till now the most successful attack managed to steal almost \$60M from a contract. However, its effects were canceled later.

2.3 Scope of Problems

Blockchain as a technology has its own problems sets and limitations. It has been improved a lot compared to the first version since Bitcoin has grown popularity and a solid user base. Swan [32] published a paper where he pointed out seven technical challenges for Blockchain:

- **Throughput:** The current maximum throughput of Bitcoin Blockchain is 7 tps (transactions per second). Comparing to other transaction networks like VISA (2000 tps), Twitter (5000 tps), Paypal (10M in a day so 115 tps approx) [13], Bitcoin is very slow. If the transaction frequency increase to this level, the throughput of Blockchain will cause trouble.
- **Latency:** More time is spent to a block to minimize the risk of double spending attack. It takes almost 10 minutes to complete a single transaction now. Such time is taken as Blockchain verifies the validity of spent money in the transaction, if it is already sent or not etc. This is a major concern for Blockchain architecture.
- **Size and bandwidth:** As of now, the size of Bitcoin Blockchain network is approximately 185 gigabytes (September, 2018). If Blockchain can achieve a throughput like VISA, its size will be 214 petabytes in a year [33]. Since the size of Bitcoin block is 1 MB, at max 500 transactions can handled at a time. Hence, if the Blockchain wants to handle more transactions, the size and bandwidth issue needs to be addressed.
- **Security:** The 51% attack is still a great threat to Blockchain network. Moreover, proper anonymity is not implemented yet in real world.
- **Wasted resources:** Almost \$15M worth energy is wasted in a day for Blockchain mining. PoW (proof of work) is the main reason for this. New

technology like PoS (proof of stake) has come to solve this issue, but it brings its own limitations. In PoS, miners with more points get more chances than a poor miner.

- Usability: The API for development is not developer-friendly.
- Multiple chains: A small Blockchain with small number of blocks possesses a greater probability of 51% attack.

2.4 Research Challenges

A lot of research work is pending and needs to be resolved to address the limitations of Blockchain technology. A few of them is pointed out below:

- A better consensus technique is necessary which can replace the PoW, PoS functions. That new idea should resolve the limitations of these aforementioned techniques.
- Better throughput needs to be supported by Blockchain architecture.
- Block size needs to be increased so that more transactions can be handled at a time. This will improve the total bandwidth.
- The current solution to stop double spending (10 minutes time break to check the validity) is not a good implementation since this is affecting the network latency. A proper solution is needed for this issue.
- Since the 51% attack is still a great threat, necessary measure needs to be taken to solve this problem. Currently, honest miners are believing the fact that this large number of share is not possible now. But, it can change anytime.
- The anonymity of every user needs to be secured and privacy must be reserved. There is a huge research gap in this section.
- Though smart contract facilitates numerous possibilities, it is possible to attack the network using this technique if not developed carefully. The network itself should take care of the security like apple store server.
- More programming languages, tools needs to be released to develop smart contract function. The current language, Solidity, has some limitations and gives developer freedom to write buggy codes.
- Though Zerocoin addressed the Selfish Mining attack by using a strict time frame, more research work is necessary to address this attack on existing Blockchain network like Bitcoin.

CHAPTER 3

ARCHITECTURE OF BLOCKCHAIN

3.1 Short History of Bitcoin

In 2008, an individual (or group) writing under the name of Satoshi Nakamoto published a paper entitled “Bitcoin: A Peer-To-Peer Electronic Cash System”. This paper introduced a peer-to-peer distributed electronic cash network which will allow the participants to do transactions directly from sender to receiver without any support of financial organizations. Bitcoin was the first outcome of this concept. Now the word **cryptocurrency** is used to describe all distributed networks and mediums of exchange that uses cryptography to secure transactions where they don't use any third-party trusted authority.

The author of the first paper wanted to remain anonymous and hence no one knows Satoshi Nakamoto to this day. A few months later, an open source program implementing the new protocol was released, beginning with the **Genesis block** of 50 coins. Anyone can install this open source program and become part of the Bitcoin peer-to-peer network. It has grown in popularity since then. The popularity of the Bitcoin has never ceased to increase since then. Moreover, the underlying Blockchain technology is now finding a new range of applications beyond finance.

3.2 Blockchain Network

3.2.1 Architecture

Blockchain is a chain which consists of a sequence of blocks which represents a sequence of transaction information like a general public ledger. Figure-1 represents an example of a simple Blockchain. Every block of a Blockchain contains its previous block's hash in its block header. Each block has only one parent block. The very first block of a Blockchain is called **genesis block** which has no parent block.

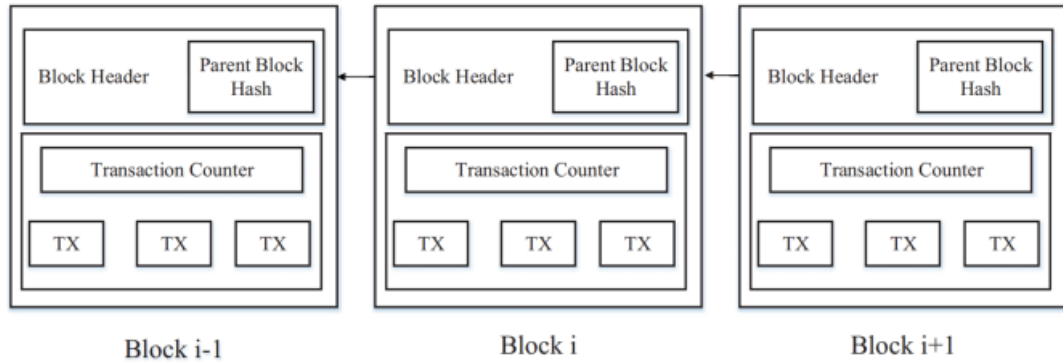


Figure-3.2.1A: A sequence of blocks in a Blockchain

Every block can be represented as a node and each one keeps a local copy of the ledger. In a large system, the nodes collectively belong to an organization. Each block can communicate with each other to transfer knowledge and agreement purpose. There is no central authority in this system. Each block is monitoring and validating every transaction and also verifying every event [6].

3.2.2 Blocks

A block is the smallest unit in the whole network. Each one contains a block Header and a block Body as shown in Figure-2.

A block Header contains metadata which helps to verify the validity of that block. It includes:

- Block version: the current version of the structure.
- Merkle Tree Root Hash: a hash value of all the transactions in this block.
- Timestamp: the creation time of that block.
- nBits: the current *difficulty* that was used to create this block
- Nonce ("number used once"): a 4-byte field, which usually starts with 0 and increases for every hash calculation
- Parent block hash: a 256-bit hash value that points to the previous block.

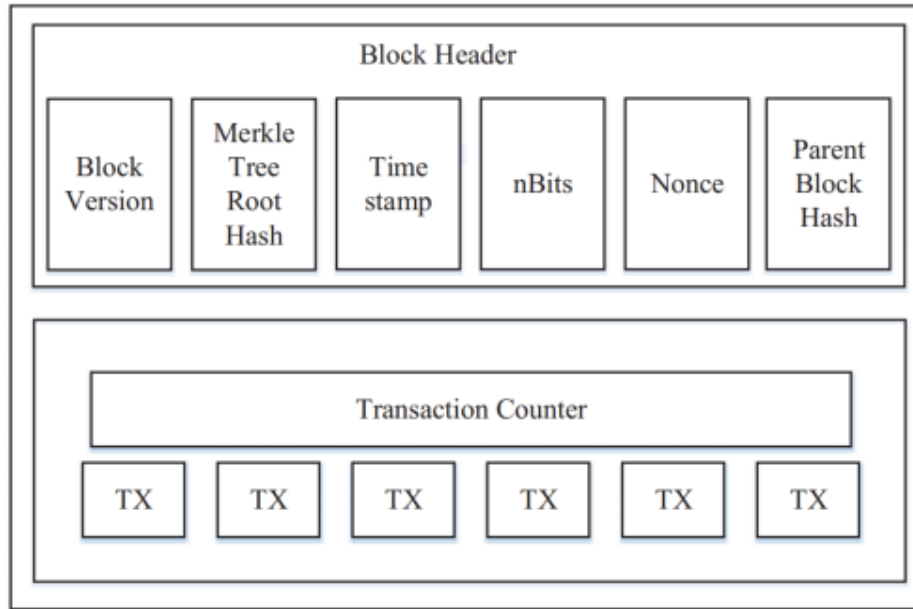


Figure-3.2.2A: A block structure

The block Body is composed of a transaction counter and transaction data. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction [5] [6].

3.2.3 Types of Blocks

There are different types of blocks such as [5]:

- Main branch blocks: Blocks which simply extend the current main Blockchain.
- Side branch blocks: Some blocks reference a parent block that is not at the current Blockchain tip.
- Orphan blocks: Some blocks reference a parent block that is not known to the node processing the block.

3.2.4 Chain

Multiple blocks make a sequence or chain which represents the Blockchain. After creating a new block, the newly created block will append at the end of the chain. Before that, all the verification and validation process execute to maintain the data authenticity. Every node or block in the network participates in that process. If there

are multiple chains from to choose, the network always chooses the longest one. There are 2 types of chain:

- **Public Blockchain:** This network is a Blockchain network without permission. Anyone can join this network to participate in the process without any kind of permission since it is open publicly. Everyone can execute the consensus protocol, and access the shared ledger.
- **Private Blockchain:** This network requires specific permission for every user. Hence, everyone needs a valid invitation from someone. They have to maintain the rules/conditions of the network creator. This is the main and only difference between public and private network.

3.2.5 Digital Signature

Using asymmetric encryption, each user owns a pair of private key and public key. The private key should be kept secured which is used to sign the transactions. The public key is used to verify the encryption. The digitally signed transactions are broadcasted throughout the whole network. The typical digital signature can be divided into two phases: *signing phase* and *verification phase*. For instance, a user A wants to send another user B a message.

- In the signing phase, user A encrypts his data with his private key and sends user B the encrypted result and original data.
- In the verification phase, user B validates the value with user A's public key. In that way, user B could easily check if the data has been tampered or not. The typical digital signature algorithm used in Blockchains is the elliptic curve digital signature algorithm (ECDSA) [10].

3.2.6 Transactions

Transactions are the smallest building blocks of a Blockchain system. It generally consists of a recipient address, a sender address, and a value. This is similar to a standard credit card transaction.

A transaction changes the state of the Blockchain. A Blockchain is a shared, decentralized, distributed state machine. Each node keeps a local copy of their own Blockchain, and the current known state is calculated by processing the transactions

in the same order like the chain. Transactions are bundled and delivered to each node in the form of a block. As new transactions are executed and distributed throughout the network, they are independently verified and "processed" by each participant.

3.2.7 How Blockchain Works

We will explain the concept of the Blockchain by explaining how Bitcoin works since it is intrinsically linked to the Bitcoin. However, the Blockchain technology is applicable to a lot of other applications which require safe and secured transactions. It can be separated in below steps:

1. Validate Entries
2. Safeguard Entries
3. Preserve Historic Record

Bitcoin uses cryptographic proof which is protected through a digital signature, is sent to the "public key" of the receiver, and is digitally signed using the "private key" of the sender. In order to spend money, the owner of the crypto currency needs to prove his ownership of the "private key".

The entity receiving the digital currency then verifies the digital signature, which implies ownership of the corresponding "private key", by using the "public key" of the sender on the respective transaction.

Each transaction is broadcasted to every node in the Bitcoin network and is then recorded in a public ledger after verification. Every single transaction needs to be verified for validity before it is recorded in the public ledger. The verifying node needs to ensure two things before recording any transaction:

1. Spender owns the crypto currency, through the digital signature verification on the transaction.
2. Spender has sufficient crypto currency in his account, through checking every transaction against the spender's account or "public key", that is registered in the ledger. This ensures that there is sufficient balance in his account before finalizing the transaction

However, there is a question of maintaining the order of these transactions that are broadcasted to every other node in the Bitcoin peer-to-peer network. The transactions do not come in order in which they are generated, and hence there is a need for a system to make sure that double-spending of the cryptocurrency does not occur. Blockchain solves this problem. The transactions are placed in groups called blocks and then linking these blocks to make a chain or line. The transactions in one block are considered to have happened at the same time. These blocks are linked to each other like a chain in a proper linear order with every block containing the hash of the previous block.

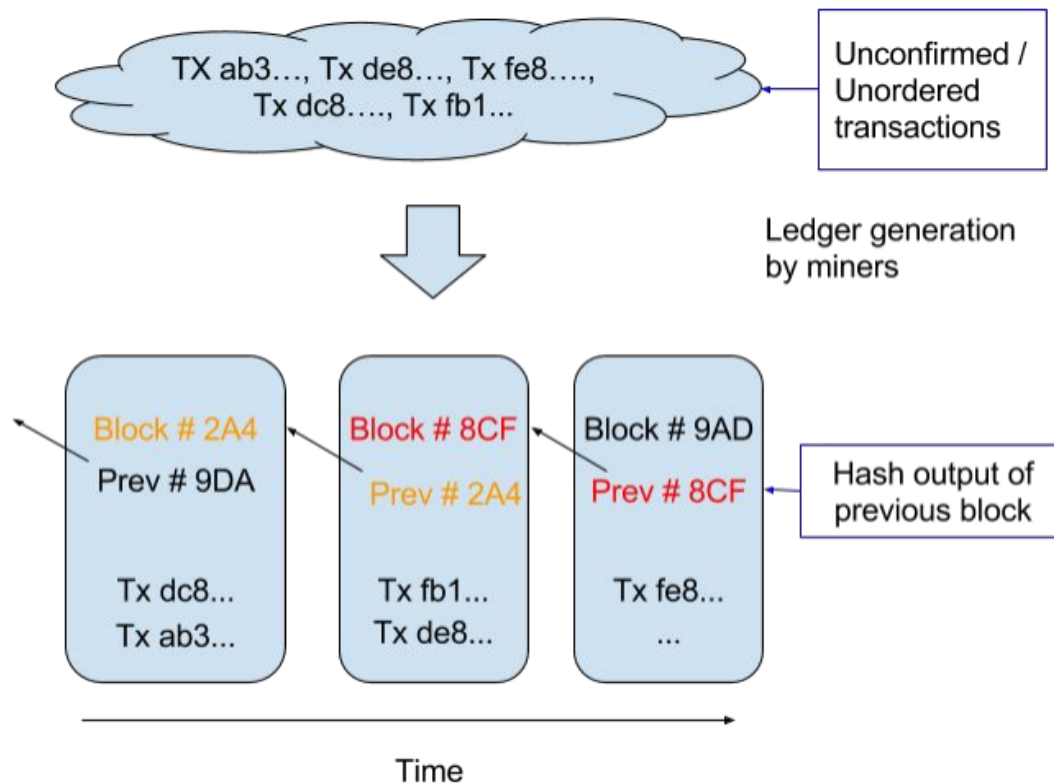


Figure-3.2.7A: Blockchain generation from unordered transactions

Still, there could be some issues like multiple blocks can be created by different nodes at the same time. One can't rely on the order since blocks can arrive at different order at a different stage in the whole network. This is solved by introducing a mathematical puzzle: each block will be accepted in the Blockchain if it contains an answer to a very special mathematical problem. This is also known as *proof of work*.

So, a node generating a block needs to prove that it has put enough computing resources to solve a mathematical puzzle. For example, a node can be required to calculate a *nonce* which when hashed with both transactions and hashes of previous blocks produces a hash with a certain number of leading zeroes.

This mathematical puzzle is not trivial to solve and the complexity of the problem can be adjusted so that on average it takes ten minutes for a node in the Bitcoin network to make a right guess and generate a block. There is a very small probability that more than one block will be generated in the system at a given time. The first node, to solve the problem, broadcasts the block to rest of the network. Occasionally, however, more than one block will be solved at the same time, leading to several possible branches. However, the math of solving is very complicated and hence the Blockchain quickly stabilizes, meaning that every node is in agreement about the ordering of blocks a few backs from the end of the chain. The nodes donating their computing resources to solve the puzzle and generate block are called **miner nodes** and are financially awarded for their efforts.

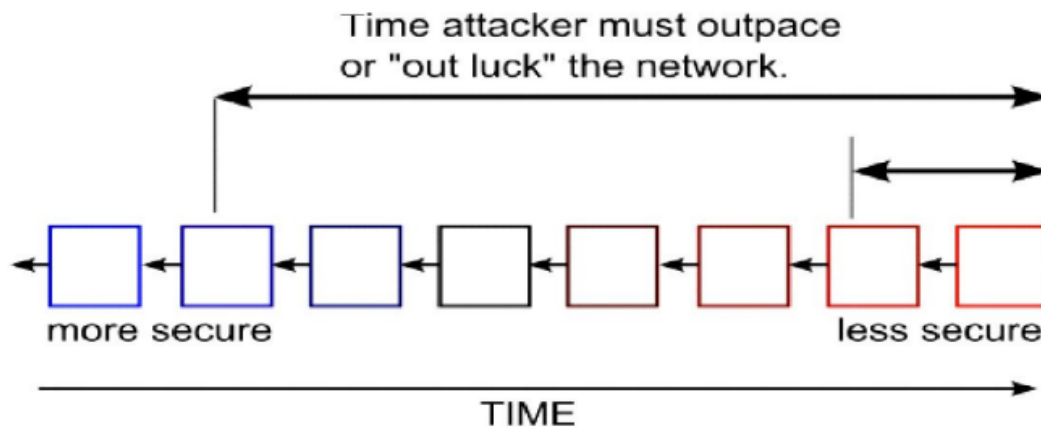


Figure-3.2.7B: Math race to protect transactions

The network only accepts the longest Blockchain as the valid one. Hence, it is next to impossible for an attacker to introduce a fraudulent transaction since it has not only to generate a block by solving a mathematical puzzle but it has to at the same time mathematically race against the good nodes to generate all subsequent blocks in order for it make other nodes accept its transaction & block as the valid one. This job

becomes even more difficult since blocks in the Blockchain are linked cryptographically together.

3.2.8 What is Mining?

Mining is the actual process where real work takes place. The result of this task is the creation of a valid block which will be validated and accepted by the entire network.

Miners are the equivalent to the credit card processing network. They take information of a transaction as an input and then verify the whole information whether it is cryptographically accurate or not, compute the new hash, create a new block, append the block to the chain, and update the public ledger in the Blockchain system.

The processing involves a couple of tasks like- computing the new hash, check the hash if it passes all the difficulty rules and if it fails then recalculate the hash by changing the **nonce**.

Due to hashing, editing even a single bit of the block header will result in a different hash. Therefore, changing the nonce will create a new hash value with the current difficulty rules. This process should repeat continuously for each new potential block until a valid hash is found. When a miner finds the perfect data configuration that results in a valid block hash, it's relatively easy for all other nodes to perform the same hash operation on that block, and verify that it does, in fact, result in a valid hash.

Miners must have some rewards, for doing the calculation and processing work, to find a valid block. In Bitcoin, this incentive is the creation of new coins via the coinbase transaction. This is a special transaction that exists in every block, which has no inputs, and has a single output pointing to an address that (presumably) the miner controls. If a miner's block is accepted by the network, their address is credited with this new Bitcoin.

As the network grows, mining difficulty is adjusted over time. The difficulty is a consensus rule, defines the amount of workload which is required to create a valid block. A block can be validated by checking the hash of their header which informs if enough work has been done or not. Bitcoin block 488485 (source-<https://Blockchain.info>), for example, has a hash of *000000000000000000000000000000008c8aa76452c5b0b422be963b1f9813538ec374178a6826*. This is a hash that begins with 18 zeros. Considering the properties of hashing functions defined above, it is extremely difficult to find a resultant hash from an arbitrary block structure that begins with the current difficulty level of 18 zeros.

Any other actor in the network can trust that if they receive this block, it must have taken lots of computing power to find the right combination of data to generate it. To compensate the miner(s) for their time and energy, the overall network agrees that the miner is allowed to include a coinbase transaction minting new coin as their reward.

CHAPTER 4

RESEARCH SCOPES & RECOMMENDATIONS

Blockchain combining with Smart Contracts opens a new era in the modern world. IoT devices enhanced the possibilities in a dramatic way. Things which were impossible to think of can be implemented using these tech stacks. This section will discuss some new idea which can address existing limitations in the agriculture sector, pension scheme, donation system, product history etc.

4.1 Blockchain in Agriculture

4.1.1 Background

Agriculture has been playing a major role in reducing poverty since 2005. According to the World Bank report article [34], almost 90% of poverty mitigated by agriculture between the timespan of 2005 and 2010. More than 70% of the total population lives in rural areas and a total of 87% of them is directly dependent on the agriculture economy. Bangladesh has made immense progress over the last 40 years and achieved food security (food production increased from 9.8M to 34.4M tons) and supported by public investments in technology, scientific researches, human capital etc.

Latest scientific approaches in agriculture are very promising and can increase the overall food production. One article of the World Bank [35] presented some research data of agriculture which is listed below:

- 1.31M farmers applied new scientific approaches to their land.
- Over 16K farmers adopted post-harvest technologies.
- 14.1% increase in Maize production, 15.8% increase in Wheat, 16.3% increase in Mungbean, 20.5% increase in Clean Rice and 19.6% increase in Mustard is the direct result of the implementation of scientific technology.

4.1.2 Problem Scope

However, scientific methods and its implementation are costly. It needs more money and land for its application. Since the majority of the farmers are poor, only rich farmers can adopt this technology to their field and thus increase their production. The

poor farmers are not able to experience this features as because the setup cost is quite high and is not fruitful for small land.

Bangladesh Journal of Agricultural Research published a research paper focusing on how poor farmers can be benefited via sharecropping [36]. This study reveals the output of sharecropping on paddy field which is applied in some areas of Khulna district. This is beneficial for a group of poor people but it has its own limitations. Maintaining the tenure agreements, distribution of profit, different sizes of land area, types of crops etc is difficult and often this leads to a chaotic situation. As a result, small landowners cannot agree to a specific conclusion and thus no fruitful decision is made.

4.1.3 Blockchain and Smart Contract Integration in Agriculture

Sector

Blockchain can be a good solution to address the aforementioned issue. Smart Contracts made this more secure and automated. If we can build a Blockchain network where each block will represent a farmer node and the nodes will belong to a single network then we can have a distributed ledger of ownership data of the lands in that architecture. Not only the small landowner but also the rich farmer can also participate in this network.

Here each block will contain its own information like land ownership data, land size data, land type data etc. Using NG model [17], all the blocks can elect a leader based on their requirements and that newly elected leader block can do the further work.

Leader block can calculate the costing for the scientific approach of agriculture and verify that if the aggregated land is a ideal fit for this approach. Then the leader block calculates the total cost of the implementation and divides them into phases. This process will be a bit complicated since the land area of each block is different and the cost needs to be adjusted depending on each block's situation. Later the leader block will ask for money from each node block based on their cost function. Each block will validate these transactions and verify. Upon successful transaction, the total amount balance will be shifted and stored in the network.

Smart Contract can enhance this situation by breaking down the processing tasks into small chunks of instructions. The leader block can deploy this contracts into the network. These contracts will ensure that implementation of work, marketing, selling is done properly. Moreover, profit distribution can also be done using the same cost function ration used previously to the entire network. Hence, the small landowners can also get the benefit of modern agriculture technology in a distributed secured way.

4.1.4 Detect and Resolve Illegal Actions

Since there is a chance to write buggy Smart Contracts, illegal actions can happen in the network. In order to address this issue couple of steps needs to be taken. Giving the complete authority to write the contracts to the leader block only is not a good idea. But, every block should not also deploy this since it will be a waste of energy. So, a group of blocks should be selected again by the network randomly who will validate the conditions of the contracts before deploying. Since this is a completely random process and executed by the Blockchain network itself, no additional overhead will be there.

4.2 Distributed Database

We can also use the Blockchain network as a distributed database. The concept of ownership will be easier by implementing this technology. The system will describe ownership of everything. Since data is immutable and everyone is agreeing with this information, security is achieved. Additionally, it will overcome lot of other third-party dependencies such as banks, NGOs, Introducers etc while doing any financial transaction related task.

We can give a more accurate example if we take the case of current situation of village farmers of Bangladesh. Most of the farmers don't have the legal documents of their land to claim ownership since they have inherited their property through inheritance. However, they don't get any financial support from Banks or other third-party organizations as they cannot provide any legal ownership documents. This issue can be resolved easily using a separate Blockchain network.

4.3 Blockchain for Product History

Through a Blockchain network we can keep the history of any kind of product whether it is a banana or a medicine. Each product will have a own history by a chain of blocks. Since these blocks are connected through hash data, we can easily trace back to know what the origin of any product is and what other processes have applied in its lifecycle.

4.4 Supply Chain Tracking

We also can track any supply chain management by implementing a Blockchain network. The same hash data chain of blocks can solve the problem here.

4.5 Secure Donation Transparency

CHAPTER 5

CONCLUSION & FUTURE SCOPE

Blockchain is a promising technology in the modern era, featuring secured peer-to-peer transactions in a distributed fashion. It has great potential in future industries since it possesses some key characteristics which can solve limitations in traditional systems. In this paper, we present a systematic overview of Blockchain technology. At first, we discuss the summary of previous research works with their problem scope. We then present the Blockchain architecture in detail along with its limitations which can become a bottleneck in future. Later, we propose some solutions to existing problems which can be addressed by implementing the Blockchain network along with Smart Contracts. We have also discussed the possibility of illegal actions with this new proposals. We have suggested solutions for some of them in theory and left other issues for future contribution.

REFERENCES

- 1 S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf> (Access Date: Nov 20, 2018)
- 2 "State of blockchain q1 2016: Blockchain funding overtakes bitcoin," 2016. [Online]. Available: <http://www.coindesk.com/state-of-blockchain-q1-2016/>(Access Date: Nov 20, 2018)
- 3 KonstantinosChristidis, Michael Devetsikiotis(Fellow, IEEE); Blockchains and smart contracts for the Internet of Things; IEEE Access(Access Date: Nov 20, 2018)
- 4 G. W. Peters, E. Panayi, and A. Chapelle, "Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective," 2015. [Online]. Available: <http://dx.doi.org/10.2139/ssrn.2646618>(Access Date: Nov 20, 2018)
- 5 Borenstein, Joram. "A Risk Based View of Why Banks Are Experimenting with Bitcoin and the Blockchain." Spotlight on Risk Technology. N.p., 18 Sept. 2015. Web. 03 May 2016(Access Date: Nov 20, 2018)
- 6 Crosby, Nachiappan, Verma; "BlockChain Technology Beyond Bitcoin"; <https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf>(Access Date: Nov 20, 2018)
- 7 Pluralsight Resource Library, <https://www.pluralsight.com/guides/blockchain-architecture>(Access Date: Nov 20, 2018)
- 8 ZibinZheng, ShaoranXie, Hongning Dai, Xiangping Chen, Huaimin Wang; An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends; Conference Paper, June 2017(Access Date: Nov 20, 2018)
- 9 VitalikButerin; On Stake; <https://blog.ethereum.org/2014/07/05/stake/>(Access Date: Nov 20, 2018)
- 10 D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ecdsa)," International Journal of Information Security,vol. 1.(Access Date: Nov 20, 2018)
- 11 P. Vasin, "Blackcoins proof-of-stake protocol v2," 2014. ; <https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf>(Access Date: Nov 20, 2018)
- 12 G. Wood, "Ethereum: A secure decentralisedgeneralised transaction ledger," Ethereum Project Yellow Paper, 2014(Access Date: Nov 20, 2018)
- 13 Bitcoin wiki, Scalability; <https://en.bitcoin.it/wiki/Scalability>(Access Date: Nov 20, 2018)
- 14 Blockchain Size; <https://www.blockchain.com/charts/blocks-size>(Access Date: Nov 20, 2018)
- 15 Gavin Andresen; Bitcoin-Qt / bitcoind version 0.8.0 released; <https://bitcointalk.org/index.php?topic=145184>(Access Date: Nov 20, 2018)
- 16 J.D. Bruce; "The Mini-Blockchain Scheme", March 2017, Rev-3. Available: <http://cryptonite.info/files/mbc-scheme-rev3.pdf>(Access Date: Nov 20, 2018)
- 17 IttayEyal, AdemEfeGencer, EminGünSirer, and Robbert van Renesse; Cornell University; "Bitcoin-NG: A Scalable Blockchain Protocol"; <https://www.usenix.org/system/files/conference/nsdi16/nsdi16-paper-eyal.pdf>(Access Date: Nov 20, 2018)

- 18 Nick Szabo (1994); Smart Contracts; Available: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>(Access Date: Nov 20, 2018)
- 19 Nick Szabo (1997); The Idea of Smart Contracts; Available: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html(Access Date: Nov 20, 2018)
- 20 Stored Procedures and Run-Time Contexts; https://docs.oracle.com/cd/F49540_01/DOC/java.815/a64686/01_intr2.htm(Access Date: Nov 20, 2018)
- 21 Solidity Documentation, Available: <http://solidity.readthedocs.org/en/latest/>(Access Date: Nov 20, 2018)
- 22 Christian Cachin, Simon Schubert, Marko Vukolić; Non-determinism in Byzantine Fault-Tolerant Replication; IBM Research; <https://arxiv.org/pdf/1603.07351.pdf>(Access Date: Nov 20, 2018)
- 23 How Do Ethereum Smart Contracts Work?; <https://www.coindesk.com/information/ethereum-smart-contracts-work/>(Access Date: Nov 20, 2018)
- 24 A Next-Generation Smart Contract and Decentralized Application Platform; <https://github.com/ethereum/wiki/wiki/White-Paper>(Access Date: Nov 20, 2018)
- 25 Savjee.be; Smart Contracts; <https://www.savjee.be/videos/simply-explained/smart-contracts/>(Access Date: Nov 20, 2018)
- 26 Kosba, Miller, Shi, Wen, Papamanthou; Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts; University of Maryland & Cornell University; 2016 IEEE; <https://ieeexplore.ieee.org/document/7546538>(Access Date: Nov 20, 2018)
- 27 O'Dair, Beaven, Neilson, Osborne, Pacifico; Music On The Blockchain- Blockchain For Creative Industries Research Cluster; Middlesex University, London.(Access Date: Nov 20, 2018)
- 28 JaumeBarcelo; User Privacy in the Public BitcoinBlockchain; <https://pdfs.semanticscholar.org/549e/7f042fe0aa979d95348f0e04939b2b451f18.pdf>(Access Date: Nov 20, 2018)
- 29 A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, NY, USA(Access Date: Nov 20, 2018)
- 30 M. Moser, "Anonymity of bitcoin transactions: An analysis of mixing services," in Proceedings of Munster Bitcoin Conference, Munster, Germany, 2013(Access Date: Nov 20, 2018)
- 31 J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014(Access Date: Nov 20, 2018)
- 32 Swan M. Blockchain: Blueprint for a New Economy. " O'Reilly Media, Inc."; 2015(Access Date: Nov 20, 2018)
- 33 Jesse Yli-Huumo (Lappeenranta Uni, Finland), DeokyoonKo, Sooyong Park, Sujin Choi(SogangUni, Seoul, Korea), Kari Smolander (Aalto Uni,Helsinki,Finland); Where Is Current

- Research on Blockchain Technology?—A Systematic Review; <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477>(Access Date: Nov 20, 2018)
- 34 Bangladesh: Growing the Economy through Advances in Agriculture; The World Bank (Oct 9, 2016); <http://www.worldbank.org/en/results/2016/10/07/bangladesh-growing-economy-through-advances-in-agriculture>(Access Date: Nov 20, 2018)
- 35 Pairing Agriculture with Technology in Bangladesh; Feature Story- The World Bank (June 23, 2014); <http://www.worldbank.org/en/news/feature/2014/06/23/pairing-agriculture-with-technology-in-bangladesh>(Access Date: Nov 20, 2018)
- 36 MF Ahmed, MM Billah; Impact of sharecropping on rice productivity in some areas of Khulna district; <https://www.banglajol.info/index.php/BJAR/article/view/38390>(Access Date: Nov 20, 2018)