A STUDY ON BLOCKCHAIN SECURITY ISSUES AND CHALLENGES

Sayani Chandra
Assistant Professor
Dept. of Computer Science & Engg.
Guru Nanak Institute of Technology, Kolkata, India

Abstract- ***The successful adoption and operation of any new technology is dependent on the appropriate management of the risks associated with that technology. This is especially true when that technology is more than an application and is part of the organization's core infrastructure. And distributed ledger technologies (DLT) like blockchain technology have the potential to be the backbone of many core platforms in the near future. The blockchain is an undeniably ingenious invention – the brainchild of a person or group of people known by the pseudonym, Satoshi Nakamoto. It has become a focus of global attention since its development as banks around the world seek to understand and harness its disruptive potential. Many of the industries has been exploring how to use blockchains across a variety of internal and client facing issues. Blockchain has the potential to transform our world. However, leading into 2018 the focus will move from "how to use a blockchain" to "how to secure a blockchain". Experts insist the technology is "bigger than the internet," but we may want to take a beat before we put everything from our money to our health records on blockchains. According to a new study, the technology isn't nearly as secure as we thought.***

Index Terms- Bitcoin, Block, Blockchain, Consensus, Decentralized, Fork, Hash, PoS, PoW, Security.

I. INTRODUCTION

Blockchain isn't a household buzzword, like the cloud or the Internet of Things. It's not an in-your-face innovation you can see and touch as easily as a smartphone or a package from Amazon. But in a world where anyone can edit a Wikipedia entry, blockchain is the answer to a question we've been asking since the dawn of the internet age: How can we collectively trust what happens online?

Every year we run more of our lives—more core functions of our governments, economies, and societies—on the internet. We do our banking online. We shop online. We log into apps and services that make up our digital selves and send information back and forth. Think of blockchain as a historical fabric underneath recording everything that happens—every digital transaction; exchange of value, goods and services; or private data—exactly as it occurs. Then the chain stitches that data into encrypted blocks that can never be modified and scatters the pieces across a worldwide network of distributed computers or "nodes".

Back in 2009, Bitcoin set the blockchain revolution in motion giving any two parties, anywhere, a way to quickly and securely transfer money.

Some blockchains, most notably Ethereum, take the utility of Bitcoin to the next level by incorporating smart contracts, which automate the process.

II. WHAT IS BLOCKCHAIN TECHNOLOGY?

Blockchain technology was originally developed to facilitate the digital currency Bitcoin. But these are two separate technologies. While bitcoin is an encrypted currency, blockchain is the platform for peer-to-peer payment, supply chain tracking, and lots more. Consider this as an operating system for applications such as bitcoins and ethereum to function.

In the simplest words, blockchain technology is a shared and open ledger that keeps a record of the transactions and cannot be modified. And as the name implies, blockchain includes an ever-increasing blocks of data with each block containing transaction information.

The blockchain technology is based on decentralisation which means the data is accessible to everyone while the data is managed by a cluster of computers and not owned by a single person.

III. TOP FEATURES OF BLOCKCHAIN

Security

One of the major issues with today's digital economy is online security. Blockchain addresses that concern to a large extent.

The technology relies on a consensus from all network members for the validation of a transaction. And all validated transactions are permanently stored in the data blocks which cannot be altered or deleted by anyone.

"Blockchain uses strong cryptography to create transactions that are impervious to fraud and establishes a shared truth. Also, all the transactions are signed with the digital certificate." Microsoft explains in a note.

A decentralised system makes it difficult for hackers to breach the transaction by targeting one unit, a common pain point in a centralised system where the data is stored at a single core.

Immutability

Immutability refers to the fact that the blockchain is highly resistant to alterations. In a blockchain setup, the data blocks are linked and secured with a special cryptography, called hash.

For instance, hash for "Good Morning" is
E526F13918F16C1C65FC4AC51ABE8B5B991769AE6718495A7AD9984406A14A2C.

And the hash for "Good Mornin" is
551294185A8D2AD6A0C72EC63FF7D68F4C4AC538B334D3256AFE21DE001E7C26.

Increased Capacity

One of the remarkable things about peer-to-peer technology is that they can increase the capacity of an entire network. Having thousands of computers working together as a whole can have greater power than a few centralized servers.

Foldingcoin is a perfect example of increasing network capacity by using many computers. The project started at Stanford University and created a distributed supercomputer that simulates protein folding for medical research. It takes microseconds for a protein to fold, which is faster than the processing power of a regular computer. Normally a protein folding simulator requires building a multi-million dollar supercomputer but the Foldingcoin project managed to build it for cheap by using a distributed network.

So, any minute alteration generates a different hash and is immediately flagged. Also, it is impossible for one to trace back the older one.

Better Security

Blockchains tend to have better security because there is no single point of failure to shut down the network. Even the highest levels of our financial system are vulnerable to hacks. Bitcoin on the other hand, has never been hacked. Sure it's possible to hack individual private keys if they're not securely stored, but the network in and of itself remains fully secure.

Blockchains are secured by many computers that run nodes and confirm transactions on the networks. Public blockchains use their own currency as an incentive mechanism to reward miners for securing transactions on the ledger.

Faster Settlement

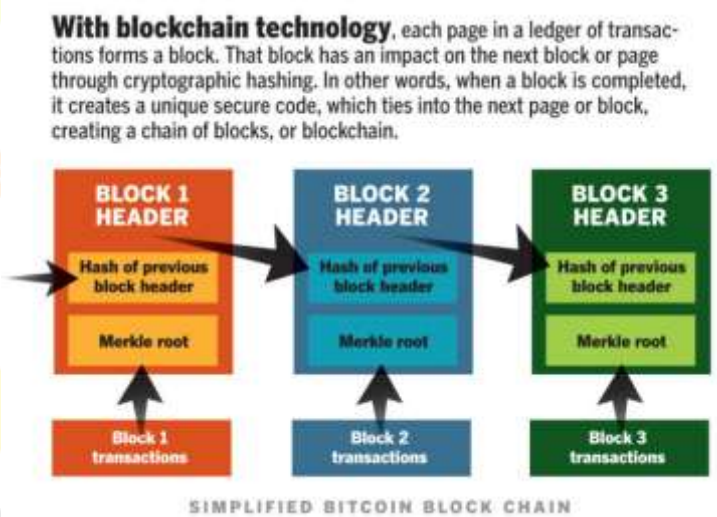
Traditional international banking can be very slow, with settlement times often taking days to process. This is the main reason why most financial institutions are looking to upgrade their systems. Blockchains can usually settle money transfers at near instant speed. This can save time and money for the entire financial industry.

IV. WHY IS IT CALLED BLOCKCHAIN?

A block is record of a new transactions. When a block is completed, it's added to the chain. Bitcoin owners have the private password (a complex key) to an address on the chain, which is where their ownership is recorded. Crypto-currency proponents like the distributed storage without a middle man—you don't need a bank to verify the transfer of money or take a cut of the transaction.

V. HOW DOES BLOCKCHAIN WORK?

When a new transaction or an edit to an existing transaction comes in to a blockchain, generally a majority of the nodes within a blockchain implementation must execute algorithms to evaluate and verify the history of the individual blockchain block that is proposed. If a majority of the nodes come to a consensus that the history and signature is valid, the new block of transactions is accepted into the ledger and a new block is added to the chain of transactions. If a majority does not concede to the addition or modification of the ledger entry, it is denied and not added to the chain. This distributed consensus model is what allows blockchain to run as a distributed ledger without the need for some central, unifying authority saying what transactions are valid and (perhaps more importantly) which ones are not.



VI. THE STRUCTURE OF BLOCKCHAIN

Generally in the block, it contains main data, hash of previous block, hash of current block, timestamp and other information. Figure 1 shows the structure of block [10].

Main data

It depends on what service, this blockchain applicate, for example: transaction records, bank clearing records, contract records or IOT data record.

Hash

When a transaction is executed, it had been a hash to a code and then broadcasted to each node. Because it could contain thousands of transaction records in each node's block, blockchain used Merkle tree function to generate a final hash value, which is also Merkle tree root. This final hash value will be recorded in block header (hash of current block), by using Merkle tree function, thus reducing data transmission and computing resources drastically.

Timestamp

Time of block generated.

Other Information

It means like signature of the block, Nonce value, or other data that user define.

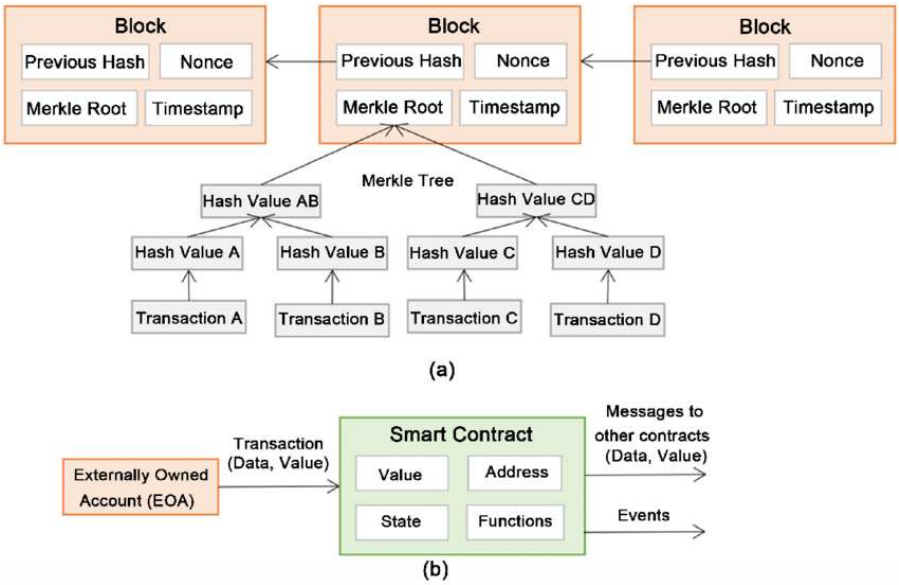


Figure 1: Structure of Block

VII. BLOCKCHAIN PROTOCOLS

Here we have included 6 major blockchain protocols, so as to embrace the technology and increase awareness among end users of blockchain.

Bitcoin

The starting of the bitcoin dates back to November 2008, when a thesis had been posted by Nakamoto on a US mailing list where the cryptographers share or exchange information. The thesis titled *"Bitcoin: A peer-to-peer electronic cash system"*, presented the following characteristics of this protocol:

- Enables transaction directly with no need of any trusted third party
- Enables the non-reversible transactions
- Decreases credit cost in minor casual transactions
- Decreases transaction fees
- Prevents double-spending

Bitcoins are virtual currency, also called cryptocurrency. These are distributed while exploring the value in the data managed by software. The start of 2016 witnessed the issuance of around 15.26 million BTC, equivalent to around 7 billion US Dollars. Major technologies that make Bitcoin include hash, digital signature, public-key cryptography, P2P and Proof of Work. This blend has developed a mechanism that prevents duplication of payments and data falsification, additionally a mechanism that prevents malicious users, which are critical for the operating system like the one for the electronic money, having no central authority.

Ethereum

Ethereum is a public, open-source and block chain oriented distributed computing protocol that features smart contracts (scripting) functionality. The protocol has provided a decentralized virtual machine called the Ethereum Virtual Machine (EVM), which carried out Turning-complete scripts by using a global network of public nodes and the token called ether, also referred to as gas. Gas is used for preventing the spam on networks and allocating the resources in proportion to the incentive provided by the request. Bloomberg explains Ethereum as shared software that is used by all; however, is tamperproof. Ethereum is also used as a protocol for decentralized applications, smart contracts and decentralized autonomous organizations, with a number of functioning applications developed on it by March 2016, New York Times says.

Ripple Consensus Network

The Ripple Transaction Protocol (RTXP), issued in 2012, has been developed upon an open-source distributed consensus ledger, Internet protocol, and native currency termed as XRP (ripples). Ripple enables instant, safe and almost free global financial transactions of any scale without any chargeback. The protocol is embraced being able to support tokens presenting cryptocurrency, fiat currency, commodity and any other value unit like mobile minutes, frequent flier miles etc. By the end of 2017, Ripple is expected to be the third-biggest cryptocurrency in terms of market capitalization, after the bitcoin and Ethereum.

Hyperledger

Hyperledger is the open source blockchain platform, began in 2015 by the Linux Foundation, in an effort to support the blockchain-based distributed ledgers. The protocol focuses ledgers developed to support international business transactions, catering leading financial, technological and supply chain businesses, with the objective of improving a lot of performance and reliability aspects. The project emphasizes on making collaborative efforts for making open standards and protocols, by offering a modular framework that backs various

components for diverse uses, including a range of blockchains having their own storage and consensus models, and the services for access control, contracts and identity.

R3's Corda

Corda by the Company R3 is the distributed ledger protocol that has been developed from the ground up for recording, supervising and synchronizing the financial agreements among regulated financial institutions. It is, by great deal, stimulated by, and captures the advantages of blockchain systems, with no design choices that turn blockchains unsuitable for a lot of banking scenarios. Corda's design came up as a result of heavy analysis and prototyping with team members. It is now an open sourced protocol since the code matured further.

Symbiont Distributed ledger

This protocol was announced in October 2016 as a software development kit for the Assembly, which is the permitted distributed ledger part of Symbiont's smart contracts system. Assembly is considered as the first distributed ledger suitable for institutional finance. It is a greatly secure, high performing Byzantine fault-tolerant distributed ledger, which can process a sustained 80,000 transactions every second in a local multi-node network. As stated by Co-founder of Symbiont, decentralized systems should no longer be slow and with Assembly, it has been fulfilled.

VIII. FIVE KEY CONCEPTS

In order to understand well blockchain one needs to grasp the following five key concepts, how they interrelate to one another, and how they might provide us with a new computing paradigm.

Those five concepts are:

- Blockchain
- Decentralized databases applications consensus
- Smart contracts
- Proof of work/stake
- Trusted advanced computing

Blockchain

As we all know blockchain technology started with the bitcoin. Bitcoin is a peer-to-peer electronic payments system, also known as a cryptocurrency, which allows people to make instant, anonymous transactions online.

The unique characteristic of bitcoin is that it records every single transaction made on its network in a public record. This is known as the "blockchain". A new blockchain is created every ten minutes. That blockchain is afterwards shared throughout the network. The chain is constantly growing, because each completed "blocks" is added to the public ledger. There are an infinite number of blocks on the blockchain, because as soon as one block gets completed, another is automatically generated. Each block though, contains a "hash", which is a unique fingerprint of the previous code.

Decentralised Databases Applications Consensus

Blockchain's potential for the development of decentralised database applications consensus is based on the unique characteristics of the technology, as outlined previously.

What is used to secure the authentication of the source of the transaction is cryptography, through the hash codes. There is never a duplicate recording of the same transaction. As such, the need for a central intermediary is not there anymore. This breaks with the paradigm of centralised consensus (when one central database is used to rule transaction validity). As John Reed, former chairman and CEO of Citibank acknowledges:

"A decentralised scheme, on which the bitcoin protocol is based, transfers authority and trust to a decentralized virtual network and enables its nodes to continuously and sequentially record transactions on a public "block," creating a unique "chain": this is the inception and keywords genesis for blockchain."

Another way to put it is to think of blockchain as a meta database where you store any data semi-publicly in a linear container space (the block). Anyone can verify that you've placed that information because the container has a given signature on it, but only the person that created that bloc or a program can unlock what's inside the container because only that person holds the private keys to that data, securely. So, the blockchain is sort of a database, except that part of the information stored — its "header" — is available to the public. Here the public, of course, means a computer scientist or software engineer, knowing how to use it and how to access its APIs and different flows.

William Mougayar, who wrote the book "The Business Blockchain" explains this with a great metaphor for Blockchain, which is how it is based on one' s own home address. One can publish hers or his home address publicly, but that doesn't give any information about what the home looks like on the inside. You'll need your private key to enter your private home, and since you have claimed that address as yours, no one else can claim the same address as theirs.

The value of decentralised databases applications consensus is enormous and it promises to disrupt the current ecosystem that tends to the monopoly. Companies like eBay, Facebook and Uber are very valuable because they benefit tremendously from the network effects that come from keeping all user information centralised in private silos and how they act as middle men taking a cut of all the transactions.

Decentralised protocols on top of the blockchain have the potential to undo every single part of the stacks that make these services valuable to consumers and investors. They can do this by, for example, creating common, decentralised data sets to which any one can plug into, and enabling peer-to-peer transactions powered by bitcoin and other cryptocurrencies.

A number of promising companies have already begun working on the protocols that will disrupt the business models of the companies above. One example is Lazooz, a protocol for real-time ride sharing and another is OpenBazaar, a protocol for free, decentralised peer-to-peer marketplaces.

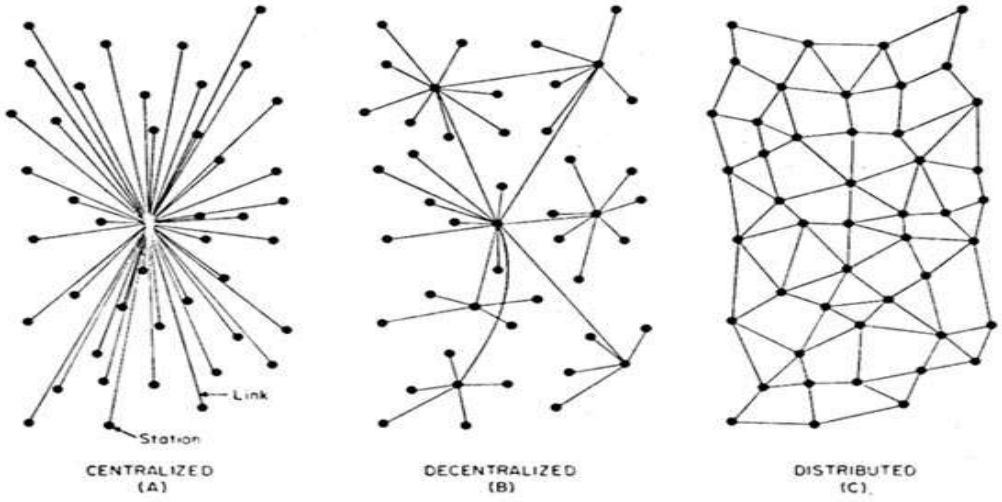


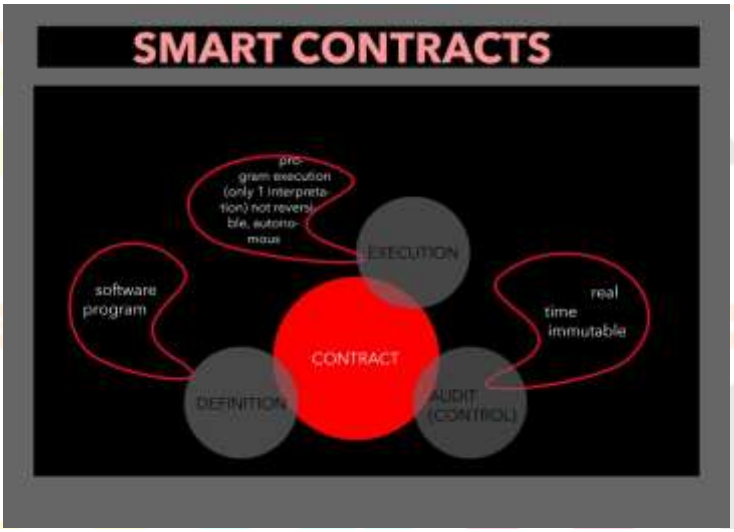
Figure 2: Types of Networks

Smart contracts

A scaled blockchain is something that starts proving a new global (somehow still science fiction) ecosystem. For this the smart contracts are the building blocks for decentralized applications.

Smart contracts are contracts whose terms are recorded in a computer language instead of legal language. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system. The potential benefits of smart contracts include low contracting, enforcement, and compliance costs; consequently it becomes economically viable to form contracts over numerous low-value transactions.

So the question behind Bitcoin and Blockchain is why depend on a central authority when two (or more) parties can agree between themselves, and when they can bake the terms and implications of their agreement programmatically and conditionally, with automatic money releases when fulfilling services in a sequential manner, or incur in penalties if not fulfilled?



Proof of work/stake

Proof of stake (PoS) is a method by which a cryptocurrency blockchain network aims to achieve distributed consensus. While the proof of work (PoW) method asks users to repeatedly run hashing algorithms or other client puzzles to validate electronic transactions, proof-of-stake asks users to prove ownership of a certain amount of currency (their "stake" in the currency). Peercoin was the first cryptocurrency to launch using proof-of-Stake. With Proof of Work, the probability of mining a block depends on the work done by the miner (e.g. CPU/GPU cycles spent checking hashes). With Proof of Stake, the resource that's compared is the amount of Bitcoin a miner holds – someone holding 1% of the Bitcoin can mine 1% of the "Proof of Stake blocks". According to Bitcoin wiki Proof of Stake is one way of changing the miner's incentives in favour of higher network security.

Trusted advanced computing

The integration of all the different concepts outlined here, namely, the blockchain, decentralised consensus and smart contracts, enables the spreading of the resources and transactions laterally, in a flat, peer to peer manner, and in doing that, they are enabling computers to trust one another at a deep level.

If institutions and central organizations are necessary nowadays as trusted authorities, in the future, a certain number of their central functions can be codified via smart contracts that are governed by decentralised consensus on a blockchain.

Namely, due to the blockchain's role as the unequivocal validator of transactions, each peer can proceed and trust one another, because the rules of trust, compliance, authority, governance, contracts, law, and agreements live on top of the technology.

If you fast forward to a not-too-distant future, smart contracts and smart property will be created, dispensed or executed routinely between consenting parties, without either of them even knowing that blockchain technology was the trusted intermediary. "Trusted computing" on the Web seems to be a key tenet of the new crypto-driven paradigm.

IX. TYPE OF BLOCKCHAIN

There are basically three types of blockchains.

Public blockchains

In a public blockchain, a user can become a member of the blockchain network. This means they can store, send and receive data after downloading the required software on their device. Allowing anyone to read and write the data stored on the blockchain as it is accessible to everyone in the world.

A public blockchain is completely decentralised. The permissions to read and write data onto the blockchain are shared equally by all connected users, who come to a consensus before any data is stored on the database.

The most popular example of a public blockchain is Bitcoin. The digital currency allows users to use a platform for making transactions directly between them.

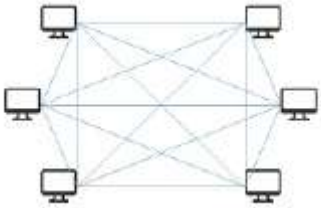


Figure 3: Public blockchain

Private blockchains

In a private blockchain, permission to write, send and receive data is controlled by one organisation. Private blockchains are typically used within an organisation with only a few specific users allowed to access it and carry out transactions.

The organisation in control has the power to change the rules of a private blockchain and may also decline transactions based on their established rules and regulations.

An example of this is a blockchain deployed by a corporation to collaborate with other divisions or a few permissioned participants.

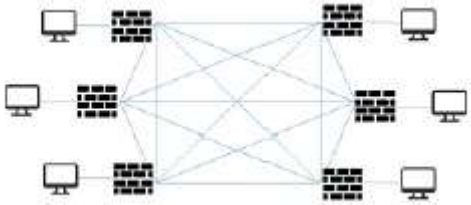


Figure 4: Private blockchain

Consortium blockchains

A consortium blockchain, also called permissioned blockchain can be considered as a hybrid model between the low-trust offered by public blockchains and the single highly-trusted entity model of private blockchains. Instead of allowing any user to participate in the verification of the transaction process or on the other side just allowing one single company to have full control, in a consortium blockchain a few selected parties are predetermined. It only allows a limited number of users the permission to participate in the consensus process.

For example, imagine a group or network of ten banks, each of which is connected to the blockchain network. In this example, we could imagine that for a block to be valid, seven of the ten banks have to agree.

Although there is some degree of centralisation in this structure, users can grant permissions to read or write to other users. This leads to the partially decentralised design of consortium blockchains. Similar to private blockchains, the consortium blockchains keep the privacy of the data, without consolidating power within a single organisation.

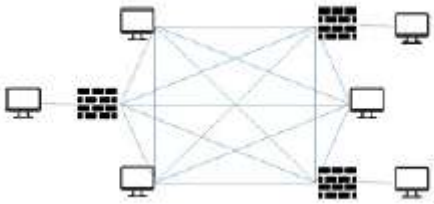


Figure 5: Consortium blockchain

X. SECURITY ISSUES AND CHALLENGES

So far, blockchain has got many attention in different areas, however, there exists some problems and challenges that needs to be faced [1, 2, 10].

The Majority Attack (51% Attacks)

With Proof of Work, the probability of mining a block depends on the work done by the miner (e.g. CPU/GPU cycles spent checking hashes). Because of this mechanism, people will want to join together in order to mining more blocks, and will become "mining pools", a place which holds most computing power. Once it holds 51% computing power, it can take control of this blockchain. Apparently, it cause security issues [3, 4, 10].

If someone has more than 51% computing power, then he/she can find Nonce value quicker than others, means he/she has the authority to decide which block is permissible.

What it can do is:

1. Modify the transaction data, it may cause double spending attack [5, 6, 10].
2. To stop the block verifying transaction.
3. To stop miner mining any available block.

A majority attack was more feasible in the past when most transactions were worth significantly more than the block reward and when the network hash rate was much lower and prone to reorganization with the advent of new mining technologies [7, 10].

Fork Problems

Another issue is fork problem. Fork problem is related to decentralized node version agreement when the software upgrades. It is a very important issue because it involves a wide range in blockchain.

- *Types of Forks*

When the new version of blockchain software gets published, the new agreement in consensus rule also changed to the nodes. Therefore, the nodes in blockchain network can be divided into two types, the New Nodes and the Old Nodes. There can be four situations:

- The new nodes agree with the transaction of block which is sent by the old nodes.
- The new nodes don't agree with the transaction of block which is sent by the old nodes.
- The old nodes agree with the transaction of block which is sent by the new nodes.
- The old nodes don't agree with the transaction of block which is sent by the new nodes.

Because of these four different cases in getting consensus, fork problem happens, and according to these four cases, fork problems can be divided into two types, the Hard Fork and the Soft Fork. In addition to distinguish the new nodes and the old nodes, we have to compare the computing power of new nodes with old nodes, and assume that the computing power of new nodes are more than 50.

- *Hard Fork*

Hard Fork means when system comes to a new version or new agreement, and it wasn't compatible with the previous version, the old nodes couldn't agree with the mining of new nodes, so one chain became two chains. Although new nodes' computing power were stronger than old nodes, old nodes will still continue to maintain the chain which it thought was right. Figure 6 shows the hard fork problem.

When Hard Fork happens, we have to request all nodes in the network to upgrade the agreement, the nodes which haven't been upgraded will not continue to work as usual. If there were more old nodes which weren't upgraded, then they will continue to work on the other completely different chain, which means the ordinary chain will fork into two chains.

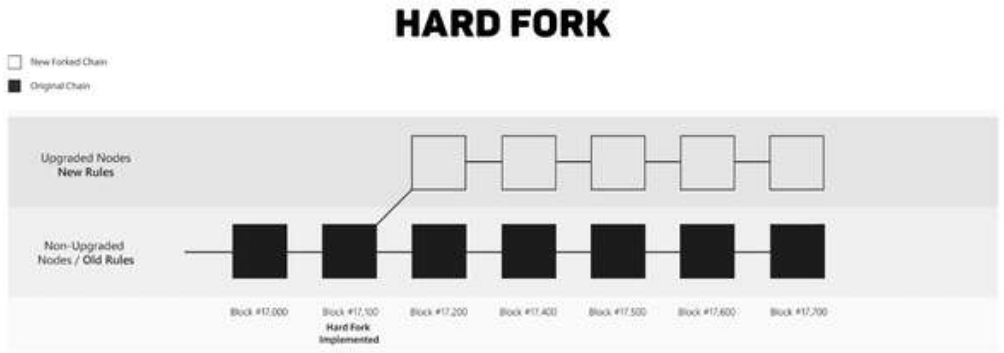


Figure 6: Hard Fork

- *Soft Fork*

Soft Fork means when system comes to a new version or new agreement, and it wasn't compatible with previous version, the new nodes couldn't agree with the mining of old nodes. Because the computing power of new nodes are stronger than old nodes, the block which is mining by the old nodes will never be approved by the new nodes, but new nodes and old nodes will still continue to work on the same chain. Figure 7 shows the soft fork problem.

When Soft Fork happens, nodes in the network don't have to upgrade the new agreement at the same time, it allows to upgrade gradually. Not like Hard Fork, Soft Fork will only have one chain, it won't affect the stability and effectiveness of system when nodes upgrade. However, Soft Fork makes the old nodes unaware that the consensus rule is changed, contrary to the principle of every nodes can verify correctly to some extent.

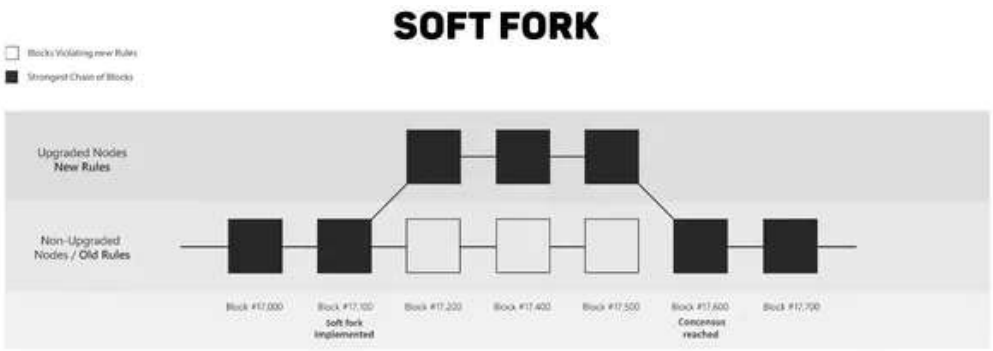


Figure 7: Soft Fork

Scale of Blockchain

As blockchain is growing, data becomes bigger and bigger, the loading of store and computing will also be getting harder and harder and it takes plenty of time to synchronize data. At the same time, data still continually increase, and bring a big problem to client when running the system [8, 10].

Simplifed Payment Verification (SPV) is a payment verification technology, without maintaining full blockchain information, it only uses block header message. This technology can greatly reduce user's storage in blockchain payment verification, and lower the user's pressure when transaction will drastically increase in the future.

Time Confirmation of Blockchain Data

Compared to traditional online credit card transaction, which usually takes 2 or 3 days to confirm the transaction, bitcoin transaction takes about 1 hour to verify. It's much better than the usual, but it's still not good enough to the extent to what we want it to be. **Lightning Network** is a solution to solve this problem [9, 10].

Lightning Network is a proposed implementation of Hashed Timelock Contracts (HTLCs) with bi-directional payment channels which allows payments to be securely routed across multiple peer-to-peer payment channels. This allows the formation of a network where any peer on the network can pay any other peer even if they don't directly have a channel open between each other.

Current Regulations Problems

If we use Bitcoin for example, the characteristics of decentralized system, will weaken the central bank's ability to control the economic policy and the amount of money, which makes government be cautious of blockchain technologies. Authorities have to research on this new issue, accelerate formulation of new policy, otherwise it will have risk on the market.

Integrated Cost Problem

Of course it will have a lot of cost including time and money to change an existing system, especially when it's an infrastructure. We have to make sure this innovative technology not only create economic benefits, meet the requirements of supervision, but also bridge with traditional organization, and it should always encounter difficulties from internal organization which is existing now.

XI. CONCLUSION

Blockchain technology has many benefits. In many cases, these benefits are worth those resources, which will be used to integrate it. However, there are also some disadvantages that we should not ignore and which the upcoming blockchain projects should try to either solve or avoid.

REFERENCES

[1] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, “Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in IEEE Symposium on Security and Privacy, pp. 104-121, May 2015.

[2] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, “Eclipse attacks on bitcoin's peer-to-peer network," in 24th USENIX Security Symposium, pp. 129-144, Washington, D.C., 2015.

[3] N. T. Courtois and L. Bahack, “On subversive miner strategies and block withholding attack in bitcoin digital currency," CoRR, vol. abs/1402.1718, 2014.

[4] I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable," CoRR, vol. abs/1311.0243, 2013.

[5] G. O. Karame, “Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin," in Proceedings of Conference on Computer and Communication Security, pp. 1-17, 2012.

[6] M. Rosenfeld, “Analysis of hash rate-based double spending," CoRR, vol. abs/1402.2009, 2014.

[7] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Capkun, “Tampering with the delivery of blocks and transactions in bitcoin," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS'15), pp. 692-705, New York, NY, USA, 2015.

[8] G. Karame, “On the security and scalability of bitcoin's blockchain," in Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS'16), pp. 1861-1862, New York, NY, USA, 2016.

[9] Y. Sompolinsky and A. Zohar, Secure High-Rate Transaction Processing in Bitcoin, pp. 507-527, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[10] Iuon-Chang Lin, Iuon-Chang Lin and Tzu-Chun Liao, A Survey of Blockchain Security Issues and Challenges, PP. 653-659, International Journal of Network Security, Sept. 2017.