Algorithms and Security Concern in Blockchain Technology: A Brief Review

Article *in* SSRN Electronic Journal · January 2018

DOI: 10.2139/ssrn.3234933

CITATIONS
0

READS
114

3 authors:

Amer Kareem
University of Bedfordshire
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Rejwan Bin Sulaiman
Glyndwr University
4 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Muhammad Umer Farooq
University of Bedfordshire
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Algorithms And Security Concern In Blockchain Technology: A Brief Review

Amer Kareem (1436182)
School of Computer Science and Technology
University of Bedfordshire
Vicarage St, Luton LU1 3JU

Rejwan Bin Sulaiman (1436184)
School of *Computer Science* and Technology
University of Bedfordshire
Vicarage St, Luton LU1 3JU

Muhammad Umer Farooq (1435896)
School of *Computer Science* and Technology
University of Bedfordshire
Vicarage St, Luton LU1 3JU

***Abstract*—** The Blockchain is an ingenious and remarkable invention. This technology created the backbone of a new type of internet. It was originally designed for the digital currency, Bitcoin, in which you can send digital money to anyone, even a stranger. Originally, it transmits bitcoin. It is considered a revolutionary technology. Blockchain helps in creating the record whose authenticity can be verified by the entire community. To make centralized and distributed systems it stores the data over a network of computers, which anyone can use this system, no central organization or person owns a system. It contains a number of blocks that contain data. The database of Blockchain is not stored at a single location, it is an open source database which can be accessed by anyone and it is easily verifiable. No one owns the blockchain technology. As the blockchain's nature is distributed, there must be a simple way by which all the nodes reach an agreement; Consensus agreement is a way by which all the participants agree on the contents of the blockchain. Here we will tell you about the basic principles and characteristics of the Consensus Algorithms so that you can decide which of the algorithm the best one to work with is.

In this paper, we will research on the number of technical aspects of Blockchain technology, the pace in which this technology is booming and most importantly its implementation on the Bitcoin cryptocurrency which has totally revolutionized the financial infrastructure of the World. Along with this, we will also consider a number of security concerns, challenges and other technical vulnerabilities associated with the Bitcoin technology. The decentralized mechanism, distributed mechanism, scripted mechanism and the mechanism of the password related to Blockchain has opened a new view on the rapidly developing internet technology. There is no need for participants or any third party who are needed to be known to each other. The responsibility is included in the recording, transmission and the activities regarding transferring the storage by distributed technology. That is how the assurance is guaranteed by keeping these aloof from tampering and forged. With the assistance of asymmetric cryptographic algorithm, each and every participant can reach towards consensus on the information of the blockchain. The blockchain technology has the potential to play a key role in the case for the information security technology. Hence, in this paper we will also cover the impact of blockchain will ensure the expansion in the sphere of information security.

Keywords¬ Blockchain, Information security, Security, decentralized, distributed, blockchain, bitcoins, blockchain technology, Distributed ledger, cryptocurrency,
crypto contract

Table of Contents

INTRODUCTION

The basic concept of the blockchain technology is that it uses the process of the distributed database which performs a number of transactions that are entirely open to the participants. All the transactions that are made are verified by the blockchain system, and once the transaction is done, it keeps all the track of the transactions and it is not possible to destroy that records. The specification of the blockchain is that it gives the pure verification to all the transactions and keep a solid record which can never be misguided. In simple words, it is much easier to steal something which is placed in the specific place rather than stealing the same thing which is placed in front of thousands of people [1].

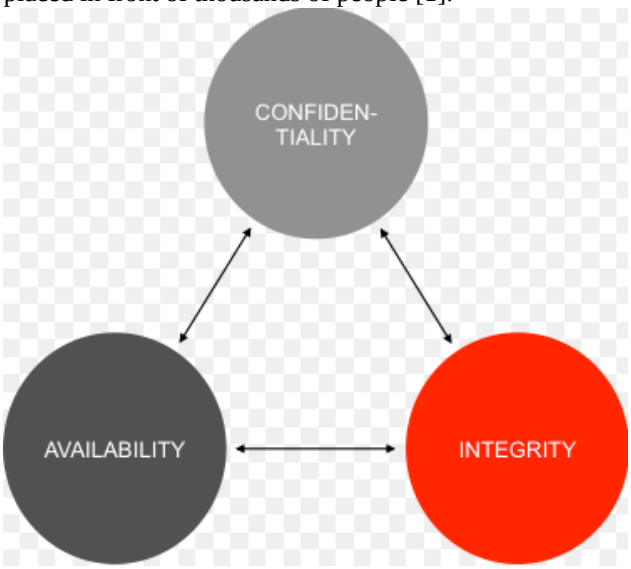


Figure 1: Blockchain features

If the concept of the blockchain technology is concerned, Bitcoin is one of the prominent examples which has introduced the World with the multi-billion market with all the transactions that are anonymous, and it doesn't involve any centralised control. It is one of the famous cryptocurrency which has attracted millions of people to participate but on the other hand, there are many controversies as well [2].

If we analyse the current situation of the digital economy, it will be clear that all of the vendors providing the services are based on the trustworthy source, like in simple words it will be clear that there is always a centralised medium for management and give the people confidence to rely on this trustworthy for their investment. For example, if we consider banking system, like in case of any transaction we do, bank confirms us if the transaction is processed successfully, that means there is always a third-party agent that plays a centralised. But here the compromised thing is that this third-party agent can be easily vulnerable to security threats and this creates a risk for the system to be hacked.

So, at this point blockchain technology has an important consideration, as this is one of the unique ways of securing all the relevant transactions of all time and it can be verified easily. And this verification is done based on the privacy of the Digital World and all the participants involved. In other words, the distributed nature of the blockchain technology and the anonymity are one of the unique features of this technology [1].

SECURITY CONCERN IN BLOCKCHAIN

Information security is involved with social life; whereas, it can run to the whole system of national informatization. The construction of national informatization is the central point of information security. People have invested vastly in information security due to security concerns in their social and work lives.

In the case for Bitcoin data structure as well as the transaction of information encrypted transmission, blockchain technology is the base upon which their construction is constructed [3]. Blockchain helps in order to operate and develop. In addition, it is bringing a revolutionary change in the information security and technology. This technology has the potential to identify and certify, staying strong against DDOS attack, assure data credibility and integrity to develop the information security technology.

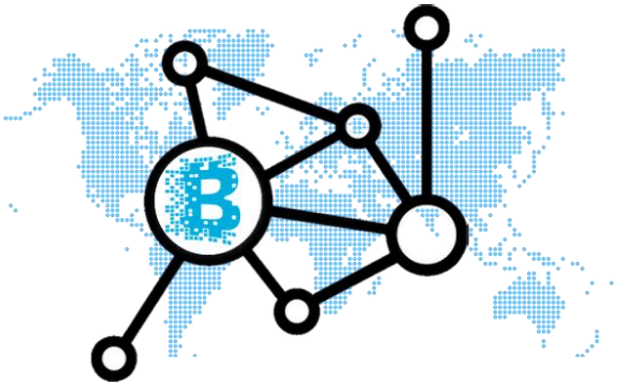


Figure 2

Blockchain technology uses a form of math called cryptography and provides an open decentralized database of every transaction involving value, money, goods, property, work or even notes. Cryptography ensures that the records cannot be changed by anyone. It was usually developed as the accounting method for Bitcoin and is used in many of the commercial applications today. The main purpose of the blockchain is to verify the transactions. It is very easy to digitize code and insert any document into the blockchain. [4]

The blockchain is made up of a vast network of nodes. The computers of blockchain network use a different client that executes the transactions i.e. validating and relaying transactions. When you join the blockchain network the node automatically gets the complete copy of the blockchain. Every

node is regarded as the administrator of the blockchain and every person can participate in this network and gets the chance of winning bitcoins. Each node in the network updates the record independently. [5]

The blockchain is a type of database which can be accessed by the public holding encrypted ledger; this means a block is the current part of the blockchain which records the recent transactions. Once it is verified, it becomes a permanent part of the growing blockchain. The people who run the system use a computer to hold bundles of records made by others, known as "blocks", as a chronological chain. The "block" is the main and important part of the blockchain, which verifies and records all of the recent transactions. After the completion of the block, it saves in the permanent database of the blockchain. Whenever a block gets completed, it overrides the previous one. In this way, numbers of blocks are connected to each other in a blockchain. The blockchain carries with it the complete set of information about specific users' addresses from the starting block till the last completed block.[5] [6]

Every block contains some information, some of the new block and some of the last block.

- **Data:** Each information that presents in the block depends on the type of blockchain. [7]
- **Hash:** The block contains hash in it, you can compare a hash to a fingerprint. It always unique and It identifies the block. If you make changes in inside the block it will cause the hash to change. Hash is very useful in detection and upgrading in the block. [7]
- **Hash of the previous block:** This effectively creates chains of the block and makes the blockchain secure. The first block is known as the genesis block. If the hash of previous blocks changes, it will make the following blocks invalid. [7]

MINING IN BLOCKCHAIN

The blockchain is particularly the technological innovation of Bitcoin mining. The transaction which has been completed gets recorded into the blocks and then automatically into the blockchain, where first it is verified then is used by other Bitcoin users. On average, in every 10 minutes, a new block is generated in the blockchain using mining process. Bitcoin is just the beginning for blockchain. In the future, blockchain will manage and verify the online data.

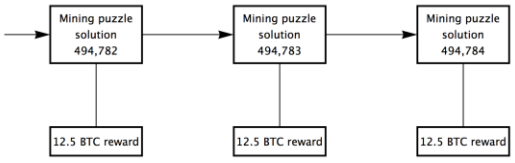


Figure 3

Blockchain network lacks the centralized points that computer hackers can easily exploit. The internet today has many security issues that are almost familiar to everyone in this world, as we all rely on simple "username/password" to protect our personal identity.[8] For security, blockchain uses the encryption technology. You can store your data on Blockchain without any fear. It solved the stock transaction in a few seconds if this transaction took place on a blockchain-based system. It could never get manipulated or hacked because of the basic structure of blockchain. It is very difficult to update the information, once the information has been saved inside a blockchain.[7]

The most transformative application of blockchain is the "Smart Contracts". These automate the payments and safe transfer of currency as negotiated conditions are met. A company could signal via blockchain that a good has been received which triggers the payment automatically.[8] The implications of the Blockchain Technology are fascinating. Many of the tech companies are adopting the blockchain technology with the goal of disrupting a variety of industries. According to research, this technique would be used to embed the Bitcoin mining chips into IoT devices and cell phones. Some of the established firms are also interested in using this technology such as Microsoft Corporation. Blockchain also offers P2P network, everyone can join this network, when he joins this network he get a full copy of the blockchain, the node can use this to verify that everything is in order, when someone creates a new block, that block is sent to everyone in the network, each node verifies the block to ensure it has not been tampered with. Then every node adds the block to their blockchain. [9]

The uses of Blockchain Technology are endless. You only have to download this app on your computing device, then you can transact with it without paying a single transaction fee. Some expect that in less than 10 years it will be used to collect taxes. It will make easy for the immigrants to send money, back to countries where access to financial institutions is limited. It could also enable us to launch the companies that are entirely run by algorithms making the self-driving car safer. It can also track the billions of devices on the internet of things. These innovations will change our lives forever and it's all just beginning. [10] The Blockchain technique can add up to serious cost savings. The blockchain serves as a financial institution and each block in the blockchain is like an individual bank statement.

INNOVATION OF BITCOIN

[This part is written by Amer kareem (1436182)
Blockchain technology is the public ledger that is responsible for keeping all the records that have started from the very first stage and it makes the transactions information available for keeping records as well as for the verification purpose. The backbone of the blockchain is comprised of a number of blocks that are linked to each other and every new block is generated

and added to the chain in a sequence. For the authentication purpose bitcoin uses the special digital signatures i.e. ECC. [11]And for verification, there are certain vendors in the bitcoin linked network known as miners. These miners are based on the specially programmed software that utilises the computer power for verification of the transactions. It utilises the bandwidth and the electric power, and this where Blockchain comes into an action.

Every time repeatedly block is generated throughout the Bitcoin system with the help of a miner. In this way replicated copies of all the Bitcoin transaction is generated across the network for the last ten minutes. So, in this way miner utilises the computer power to ensure that the transition is taken place effectively between the two parties without any issue. This is how Bitcoin is different than the normal traditional banking system. The largest amount of Bitcoin that can ever exist is 21 million. Due to this, all the payments that are made is like taking the currency free of limitation. That is how a transmission control protocol which is based on the 'communication' protocol is different than the Blockchain protocol which is based on the 'value exchange'. So, the only way to add more Bitcoin in the network is to use the process of mining. [12]

Now a day, World is leading towards using the new version of Blockchain technology which actually indicates the other ways of using this technology which s not just limited to transfer money. There is a number of new protocols have been introduced i.e. Multichain or Ethereum etc. that can be considered for using this technology in a better way. Most of them are normally based on the similar concept of distribution system i.e. ledger and some of the better features are added like smart-contract and many other applications. Work is continuously being done to increase the boundaries of this technology and many new techniques and application are been introduced. [11][12]

BITCOIN

It is one of the famous forms of digital currency that is run over the entire network. It basically points to a point-based system of payment that doesn't constitute of any central medium. According to the report, there are around 110 types of cryptocurrency, but Bitcoin constitutes of about 77 % of the total market of the cryptocurrency due to the highest number of available active users [12].

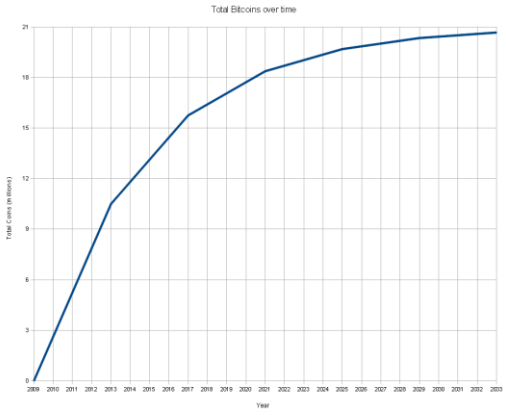


Figure 4

The major backbone of the bitcoin is the blockchain technology. And this technology comprises of all the available features for the Bitcoin currency. The foundation of the Bitcoin was proposed by one of the Australian businessman named Satoshi back in 2008 [13]. In figure 4 we can see that the rapid increase of the bitcoin. The paper, which he has published gives the overview of using the blockchain technology for the Bitcoin.

BACKGROUND TECHNOLOGIES

All the individuals who want to add the block must follow up with some work. So, for the proof of work is in the way that it requires the big amount of computational power which is involved in giving the proof, like in this way all the participants in the network can know that the work is done for generating more blocks in the chain. Therefore, this can lead to the prevention of the bad users to manipulate the chain, thus ensuring the integrity of the system.

Hash-cash is of the function that is used to promise the verification of the system based on the proof of work. It doesn't involve any kind of central medium, rather it is distributed across effectively. It uses the method of symmetric key cryptography i.e. SHA-1 or SHA256. [14]

The major function of the hash value is that, it takes the data that can possibly be any alternative size and because of that input, it transforms the data in the way that it is not possible to reserve it and makes it into the special string. In case of any changes in the data received, the hash function is changed very randomly. Thus, no one can make the same hash value with the various blocks of data. So, every hash match with the specific data, while in case of Bitcoin, all the input data is more than the SHA 256 hash value. [14] Therefore, Bitcoin doesn't require any serial number as each block is identified by the specific hash value, and this strategy doesn't only provide the identification but also promises the integrity of the data. By adopting this kind of strategy, it allows us to verify the real ownership of the Bitcoin and it ensures the distributed database of a number of available transactions which avoids the user for wrong spending.

POINT TO POINT NETWORK

In the Bitcoin framework, there are 'nodes' that are involved in the operation of the whole system. In the P2P network, all the parties that are involved hold the similar opportunities to star up the communication process. SO, for this, there is the way in which are involved in the processing of transactions, keep the record updated in the system and to ensure that all nodes in the network get the information effectively. [15]

There is one special protocol that is used in the Bitcoin system and is known as Gossip protocol, the major functionality of this protocol is that it informs about the data to each node and in return, it also receives data as well. By adopting this protocol strategy, the whole important information is spread out throughout the whole network. Another major consideration about this protocol is that it follows up with the fault-tolerant mechanism. So, that means in case of any node failure in the network would not affect the availability of information via multiple places. Other than that, it is worth to consider about this protocol, it is highly scalable which can consider all the various nodes and it adjusts itself in the network irrespective of the changes while performing the configurations in the network. [16]

CRYPTOGRAPHY IN BITCOIN

In case of public key cryptography, every coin is linked with the real owner public key, that means when the Bitcoin is sent to anyone, a message is created in terms of the transaction and as a result, the public key is attached to all the available Bitcoins and these are verified by the private key. So, as a result, when it is publicly broadcasted, this will cause other users to know that the owner of the Bitcoin is the same owner of the key as well. The signatures that are done by the owner is the solid evidence that the message produced is trust-worthy. All the previous record of transactions is held by everyone, so this strategy makes it possible to identify the real owner of the coins at any time. [17]

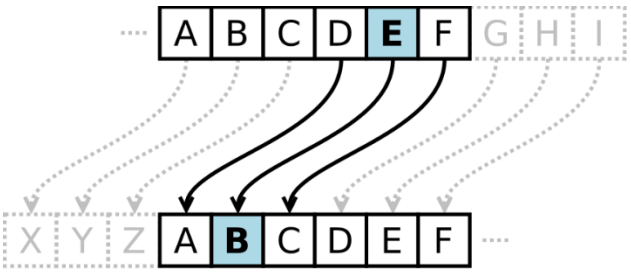


Figure 5

To ensure the integrity of the whole Blockchain system, every block in the chain promises the integrity of the last block (previous). And this process continues till back to the first block. This process is a bit expensive as it is quite hard to fulfil all the special requirements. So, in this way, no one can over-write any one of the available records.

CHALLENGES ASSOCIATED WITH BITCOINS

As the fact in the Bitcoin is that, it doesn't involve any kind of central medium or authority for the transaction control, instead, it is public, and this fact brings up certain security concerns.[18] So, while considering this scenario, the following are some of the security aspects that should be considered:

TWICE SPENDING ON COINS

This term means that the user shouldn't be able to use the similar coins two times and it shouldn't be able to use the same coin for another user at once. Through the Blockchain infrastructure, spending twice is prohibited, so for this everyone over the Bitcoin network must agree for the certain transaction prior to its confirmation. While adopting this strategy, it can be assured that the user didn't use the coin and it assured if the user is the actual owner of the coin as well. This identification is possible because the Blockchain system keeps the record of all the available history of transactions, therefore the real ownership of the Bitcoin can be traced easily. So, it can be concluded that the double spending of the coin at the same time is not practically possible. In case if anyone is managed to spend two blocks, in that case just one of the transactions will work in accordance with the nature of Algorithm designed [19] [20].

ACCESS TO THE NETWORK

In case of anyone, who managed to get access to most of the network, this will cause him to do anything as he intended to do so, and this may result in the failure of the entire network. This can be possibly avoided by adopting the proof of work technique assuring that none of the people would alter the entire Bitcoin network while considering the computational power. Though it is very difficult to consider the whole network while using the computational power. This process can possibly be adopted if a large number of people make a big pool and until, yet this never happened.

The algorithm that is used in the Block hash is made in such a way that each block constitutes the hash value of the last block of the chain.

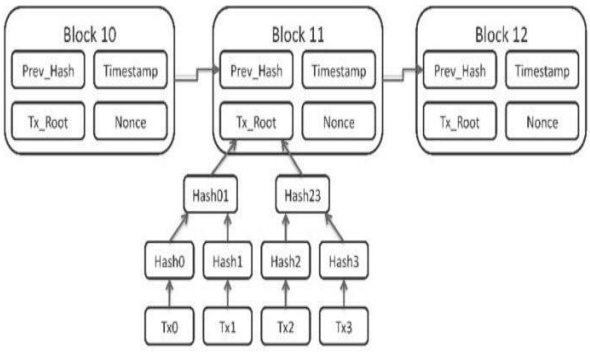


Figure 6: Block Configurations

In case if someone wants to alter the data in the transaction, then they have to follow up with the Proof of work for that specific block and this follows up with all he interconnected blocks while considering the computational power, so that they

could create the prof of work of all the previous blocks and in the same way create the similar one for the newly generated blocks while they are added into ledger. Well, the only case in which the probability of success can be possible when the overall controlling is more than 51 % of the total value of computational power.[21]

In usual circumstances, no one has authority to get access to the private key information, but in case of having the higher computational power, the access for changing the transaction can alternatively be possible. While, along with this, due to higher computation power, the creation of a big amount of crypto-currency can also be possible by utilising the process of mining.[21]

ANONYMOUS USERS

This is one of the vital considerations in the Bitcoin technology that the anonymity of all the participant is promised. Although the functionality of the Bitcoin is based on publicly, however keeping the user identity confidential and private is necessary. In the usual situation, this situation is achieved at a certain level by considering the utilisation of public-key as the address, therefore it becomes difficult instead impossible for anyone to explore the relationship among the certain key and of course the person which is behind the key.

LEGAL ISSUES IN BITCOIN

The basic system blockchain technology in Bitcoin is that there is no central system of management, therefore the whole system will only stop working if the overall network is shut which is practically not possible. Following are some of the legal considerations in the bitcoin network.

- Practically, all the legal enforcement parties including government are failed to take control over the Bitcoin networking system. All the transactions and number of activities that are performed over the Bitcoin network cannot be traced over the normal circumstances. This has promoted some illegal things over this network. This can be understood by considering the example of buying of drugs that can probably not possible by buying via normal credit or debits cards etc. but here the cryptocurrency is the solution which can be used due to its feature of un-traceability [22]. So, these kinds of issues made it impossible to use this platform under the legal boundary [2].

- There are certain other legal concerns about the Bitcoin platform which are very confusing for example if the Bitcoin is treated as money or property, other than that if the owner of the Bitcoins is liable of paying tax, if 'yes' what are the possible ways this can be implemented as there is no central controlling mechanism in Bitcoin [23].
- Another strange thing about the Bitcoin is that its value or price changes frequently and in a wild way, and this trend is possible because of a limited number of participants and the transactions, and because of social media. None of the government of any country including the number of Banks would like to base their economy where there is no centrally controlled structure.

TECHNICAL ISSUES IN BITCOIN

Other than legal and security concerns in the Bitcoin technology, there is a number of technological constitute in the Bitcoin network. Following are some of the issues based on Bitcoin technology.

- One of the big challenges in the operation of the Bitcoin network is the power consumption used by the feature of proof of work in Bitcoin which requires a big amount of computational power to transaction verification. Therefore, it doesn't worth to waste this much power for a small task.
- 21 million coins are the total number of Bitcoins that can be possibly achieved and according to forecasting this will take place by 2140 [23]. Afterwards, there won't be any mining payment, and during this situation, the only possible way is the fee that is charged during the transaction and that will be the sole mean for mining blocks by the miners. So, in this scenario, the Bitcoin system will be useless, when the transaction payment will be the same as other centralized systems.
- In terms of safety, Bitcoin overall network is quit safe and secure, however in case of anyone or maybe some group get control over the major computation power, then this might cause the overall system to come down. Although this condition is quite impossible to achieve as mentioned before.
- Another major technical concern about the Bitcoin network is that, if someone commits any mistake that might be unconscious, there is no way to get that fixed. In one way this is an advantage, as this enhances the security of the network, as no one will able to perform any alterations or changes, however, on the other hand, this can create a problem when something is done just by the human error.

In the Bitcoin infrastructure, there is a number of concerns that are causing the privacy issues which includes the removal of sensitive personal data from the Bitcoin system. While considering the other Blockchain technologies, there is a number of situations where it keeps the data of the users at a certain time, but when there are alterations in the circumstances, this personal data is not kept in the same way as before. This can be easily understood by considering the example, that US has recently published the law that the name of company's CEO and date of birth must not be published at company's website, However, other information like licence holder etc. can also be changed in a similar way. All this data is under the control of the government, however, block-chain technology gives the best chance to people to get together and make their own data-sets throughout the end to end network without the involvement of any central medium [24].

THE CONSENSUS ALGORITHM IN BLOCKCHAIN:

[This part is written by Umer Farooq (1435896)]

A consensus Algorithm is a process in computer science which is used to achieve agreement among distributed processes or systems. There are various Consensus algorithms like Paxos, Google implemented a distributed lock service called Chubby (based on Paxos), Proof of work etc. Two of the general problems arises in blockchain technology which needs to be solved these are double spending problems and Byzantine General Problems. [25]

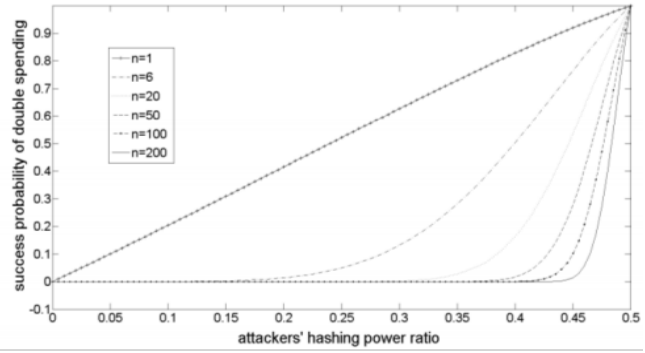


Figure 7: Relationship between hashing power ratio and double spending

Double- spending is an error in a digital cash scheme in which the same digital token is spent twice or more. This is possible because a digital token consists of a digital file that can be duplicated or falsified. The prevention of double- spending has taken two general forms: centralized and decentralized. It is usually implemented using an online central trusted third party that can verify whether a token has been spent. This normally represents a single point of failure from both availability and trust point of views. The second problem is the Byzantine General Problem. We all know that Blockchain is a decentralized network, in a decentralized network, there is no central authority and each node does not trust any other nodes. The question is that how all the nodes can agree on what the correct state of shared data is, this is known as the Byzantine General's Problem. This problem is described as a group of generals of the Byzantine army camped with their troops surrounding an enemy city. The generals must agree upon a common battle plan and they can only communicate with each other using messengers. However, one or more of the generals may be traitors who will try to confuse the others. The problem is to find an algorithm that ensures the loyal generals will reach an agreement on the battle plan regardless of what the traitors do.[25]

characteristics	consensus algorithms				
	PoW	***PoS***	***DPoS***	***PBFT***	***RAFT***
Byzantine fault tolerance	50%	50%	50%	33%	N/A
crash fault tolerance	50%	50%	50%	33%	50%
verification speed	>100s	<100s	<100s	<10s	<10s
throughput(TPS)	<100	<1000	<1000	<2000	>10k
scalability	strong	strong	strong	weak	weak

Figure 8: COMPARISON OF THE FIVE CONSENSUS ALGORITHMS

The characteristics of the Consensus Algorithm include the following:[26]

POWER OF WORK (POW):

A proof of work is a remarkable piece of data which is very difficult to produce to satisfy some of the basic requirements. It is a random process to generate proof of work with low probability and efficiency so that the number of trials and errors is required before a valid proof of work is produced. This mechanism could be used to reach consensus between many nodes on a network and he used it to secure the bitcoin blockchain. However, the proof of work algorithm works by having all nodes to solve a cryptography puzzle. This cryptography puzzle is solved by all the miners and the first one to solve it gets the miner reward. Proof of work gives more rewards to people with better equipment's. The higher your hash rate is the higher is your chance of creating the next block and getting the miner reward. To increases chances any further, the miners can come together and can form the mining pole, they combine their hashing power and distribute the rewards evenly across everyone in the pole. One of the disadvantages of proof of work is that it uses a large amount of electricity. With proof of work, rich people are more likely to enjoy the power of economics at scale. [26]

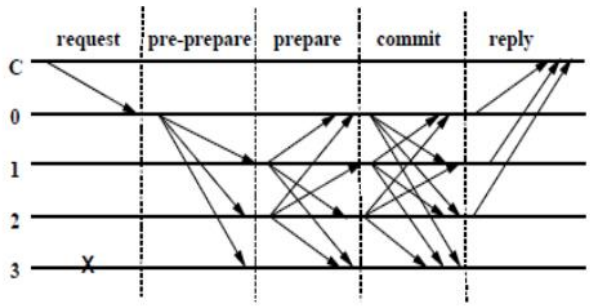


Figure 9: Steps of PBFT

This method forces miners to have a stake in the bitcoin network. Proof of stake does not have miners but instead validators. It does not allow people to mine new blocks but instead mint or forge blocks. For a person to become a validator, a node must deposit a certain amount of coins into

the network as stake. The size of the stake determines the chances for the validator to be chosen to forge the next block. The validator which is chosen to validate the next block will check whether the transactions in the block are correctly made and if everything checks out the node signs off the block and add it into the blockchain. As a reward, the node receives the fees associated with the transactions associated inside this block. If node no longer remains as the validator, his stake as well all of his transaction fees which he has got will be released after a certain period of time. Proof of stake is more environmental friendly as compare to proof of work because it does not utilize a large amount of electricity.[26]

DELEGATED PROOF OF STAKE (DPOS):

Delegated Proof of Stake users conducts a reputation system and real-time voting to create a panel of limited trusted parties, they are called as witnesses. Witnesses have the right to create blocks to add it into the blockchain. You can consider this as a representative democracy, citizens electing officials to represent them when making decisions. In the model people worth strength depends on how many tokens they hold. This means the people who have more tokens will influence the network more than people who have very few tokens. The voting for the witnesses is a continuous process, therefore, the witnesses must carry out their functions to the higher standard or they will lose their position. The delegated proof of stake is a decentralized consensus model Which has a high transaction rate and consumes low energy.[26]

Practical Byzantine Fault Tolerance (PBFT):

It was a breakthrough in distributed computing that comes out in 1999. Basically, it is a replication algorithm that is able to tolerate Byzantine faults and achieve variable consensus in a distributed computing network. It is used in many distributed networks such as Ripple, Stellar and Hyper ledger. It is a multi-stage verification process where at the beginning the verification is done by a selected number of nodes and as it progresses through the verification process it needs more and more confirmation.

RAFT:

The raft is a characteristic of the consensus algorithm which I just like Paxos in fault tolerance and performance. The main function of Raft is that each entire node in a group agrees upon the same transitions. In Raft, a person is selected from the group which acts as the leader. The leader's job is to accept the requests made by the clients and then manage he replication of the log to other servers. The data flows in one direction from the leader to the server.[26]

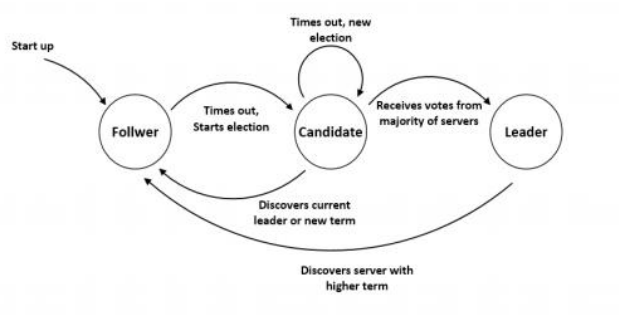


Figure 10

Technology Behind Blockchain

[This part is written by Rejwan Bin Sulaiman (1436184)]

The technology has originated from a mathematical problem that is known as Byzantine failures. This is a basic issue that has been developed by Lesley Lambert to have a proper communication system between peer-to-peer [27]. The point of Byzantine question is to formulate consistency with a view to messaging via the channel of information. Hence, the anticipation is that the channel is always reliable to communicate.

The blockchain technology is also known as the technology of distributed ledger and it also has an underlying technology that confirms the operation of the Bitcoin. In the Bitcoin Forum, an essay written by Satoshi Nakamoto has been published in which the name "Bitcoin" first appeared in "Bitcoin: A Peer-to-Peer Electronic Cash System" [28]. The technology is an amalgamation of numerous technologies. The technologies are integrated into a database where they maintain the reliable and unique database. This is a database technology that is distributed through the internet. Storage is being done in a data-centre that is centralized in nature. In blockchain technology, any person in this system has the capability to participate in working of the data centre. This technology has the capability of integration, being continuous and consistent through password verification of asymmetric mechanism. [26]

Aspects of Blockchain Technology

The blockchain technology is one of the evolutionary technologies on the internet. The core of blockchain is consisting of data structure that is block-based, the architecture of decentralized open source, cryptographic asymmetric mechanism. [29]

The blockchain is a distributed database technology that is entirely different from the traditional structure of the

database. This technology is equipped with the innovative block as an important component of the data. Information of the data is being kept in the data record and that file that keeps and stores the data is known as a block.

Nakamoto has created a genesis block where every single block is responsible for recording the value in the case of the creation. The structure of the block keeps a header of the block and that block creates a link with the prior block.

The genesis blocks, as well as the block structure, is given in Figure 11.

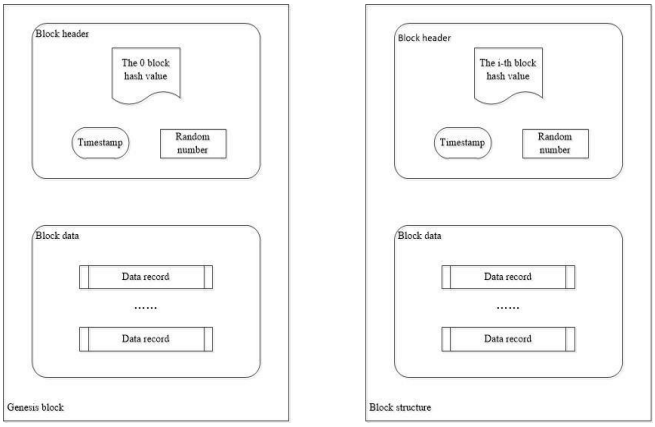


Figure 11: Genesis block and block structure

That is why the structure of the block is consisting of two distinctive characteristics. At first, the information of the data inside the block is an exchange of the activity that is recorded while the creation of the prior block takes place to the creation of the whole block to ensure the integrity of the database blockchain. Next, in the case of creating and linking to the ending point of the blockchain, the block data is ready to have assurance as well as the consistency of that database of the blockchain.

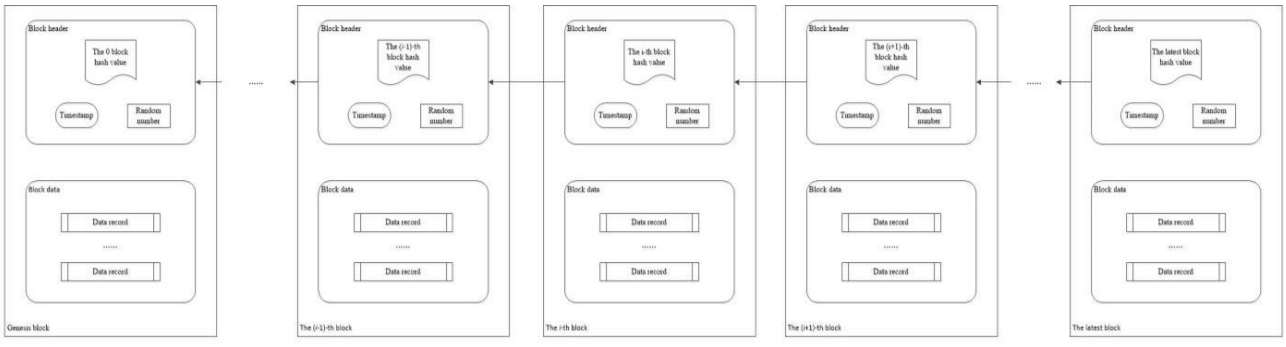
The block acts like a node that is based upon the value exchange agreement to create a blockchain. The index must have been known before to generate the latest block with the prior block. That is why each block is needed to be linked with the prior block. Hence, it can be said that index of prior block creates the head of the following block as well as the data information creates the data block and here, the timestamp has to be fixed to the end [29].

"The magic of blockchain data structure: a block (complete history) + chain (full authentication) = a timestamp, which is the maximum innovation of the blockchain technology" [30]. Blockchain technology database can store complete data information starting from genesis block and it goes to the last block in the structure. Every data, as well as messages, can be traced as well as can be validated. You can find the figure 9.0 of the data structure of the blockchain is given below.

Since blockchain technology differs from many technologies, it does not record as well as store data in a data centre that is centralized in nature. In lieu of different nodes that are bound to work altogether. To begin with, the blockchain technology is constructed with different sets of protocol mechanisms. Different nodes are used to do different tasks. One is used for maintaining the data information for its node whereas the other is responsible for verifying other nodes.

The block data information is dependent on a fact that almost all the nodes in that network has the potential to consider information in a correct manner and later, comparison of the result as well as the authenticity is considered. In this technology, all data are regularly and spontaneously updated. In addition, they are also stored in different nodes of the network that participate while the recording is going on. Though it is possible that some of the nodes might be tampered or damages, it would not put any impact on the recording of the database. The network system is purely stood upon the principles of volunteering. It also tries to establish a spread-out network system. Here, all persons can have accessibility to each other. By having so, total networking system will be decentralized as well. Data information is being validated as well as disseminated throughout the distribution network. In the case of the blockchain technology, a different type of transactions is needed to be distributed in the structure of distribution. With respect to the P2P protocol, the messages are delivered to different nodes from a single node in the whole network. This is fully a decentralized architecture that is updated real-time in a single network node to assure the security of the blockchain database.

The accounting distribution, storage and the dissemination of the blockchain depict that it is not possible for an organization to have absolute control over this. The procedures regarding the storage of the data, transmission of the information and the verification of the transaction are kept decentralized.



The technology of the blockchain can validate the ownership regarding the information that is purely based on the algorithms of asymmetric encryption. Two distinctive keys are required to encrypt and decrypt such as a public key and a private key. The public key is used to have the blockchain encrypted and that remains open to anyone in the entire network. Anyone can use their own public key in the case of encrypting data. On the contrary, the private key can only be owned by the information owner. To encrypt information, a private key can decrypt it to ensure the security and privacy of the data. There are some common encryption algorithms such as RSA, ElGamal, D-H, ECC and many more. In the case of the blockchain technology transaction, the public key is responsible for encrypting the transaction whereas the private key is responsible for decrypting it to utilize the value of the original data that it has. [32]

In a decentralized environment, all agreements of the blockchain are required to stay ahead of where the script is being taken as a programmable smart contract. This technology utilizes a script and in return, it ensures flexibility, practicability as well as adaptability. The scripts are the files that can be executable in some formats. This can also provide a list of different instruction for holding value on each exchange job.

EXHUMATION OF BLOCKCHAIN TECHNOLOGY IN THE CONCERN OF INFORMATION SECURITY

I. Authentication of Identity

The process of authentication is a system that examines an identity of the user's. It gives a mechanism for confirming the identity of the users' [32]. The normality of the technology is to protect the users' who are legitimate.

The technology of authentication is regarded as the pillar of the security protocols like accessibility to the control, detection of the intrusion, security audit etc. These are the important components of the information security. The authentication technology has the inclusion of different password-based technology, smart card-based authentication technology, PKI based authentication technology. In addition, different authentication technology has been introduced that is based on different biological characteristics of human [33]. Traditional authentication technology has already adopted the authentication method that is centralized in nature. The Certificate Authority (CA) is responsible for executing the authentication technology with a view to realizing the

functions in terms for issuing, revoking, updating as well as for certificates verification. Nowadays, web-based application systems like the email system, portal website and the messaging application system are purely standing upon the CA mode. On the other hand, it is a big risk since the crackers can have an intention to crack the CA centre to crack the encrypted information.

The authentication process of the identity is purely situated on the technology of blockchain. It has different characteristics of different decentralized authentication whereas it does not create any threats to the CA. In addition, by releasing a key of the blockchain, can surely disrupt any action of the fake secret key. Now, a project from MIT named by "certain" is one of the best examples of implementing PKI that is totally created upon the blockchain technology. The certain has the capability to remove the centralized CA; meanwhile, can replace the spread-out accounts by utilizing the blockchain. Moreover, Pomcor has already marketed an implementation of PKI that is based on the blockchain.

The approach permits the users to authenticate certification via decentralized as well as transparent sources of the user. IOTA project is used in the case for leveraging a lightweight, Tangle, block less and a scalable account and acts like the standing pillar of the Internet of Things (IoT). [34]

II. Protection of the Infrastructure

Distributed Denial of Service, known as DDoS, is responsible for attacking different computers as a form of the platform with assistance provided by the Client/Server (C/S) technology [35].

Denial of Service (DoS) is responsible for targeting the availability of three components related to the security of the information such as usability, confidentiality and integrity. The mode of the attack uses the defect in the system network that is responsible for consuming the resources. Therefore, the target stays unable to give expected service to users.

The basic type of DoS attack can require huge resources to implement by utilizing the requests of the service. By doing so, the legitimate users might not be able to have the prompt response of the service [34]. The attack might have a target on the memory, CPU, and bandwidth where the indicator of the performance is relatively low. The attack of DoS is done on a one-on-one respectively. Since the network and computer technology is developing day by day, DoS attacks are seen as less likely to take place. The reason behind that is the increasing power of the computer processor, increased memory as well as the bandwidth.

DATA SECURITY IN BLOCKCHAIN

Data is being built on the exact foundation of that application system. With respect to the method of the cryptography, the digital signature creates a new set of information that depicts the integrity and the identity of the signer that is embedded into the data file [36]. The user is responsible for the confirmation of the signature by using the public key of the signers to authenticate the information.

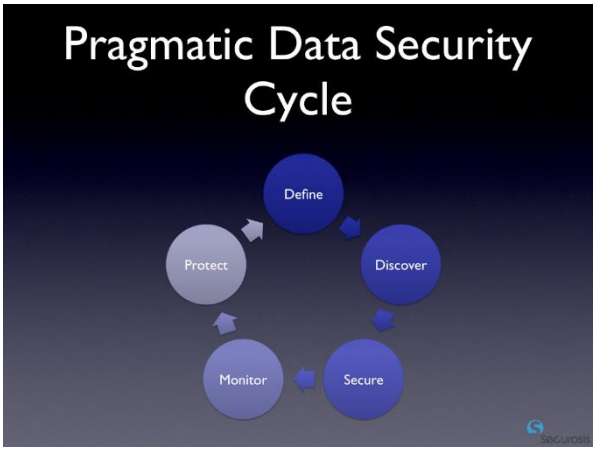


Figure 13

Generally, the intention of using private key is done because of the digital signature technique in the case for the recipients. A problem is there such as the private key is needed to be verified as well to see it has not been fabricated or tampered. As the blockchain technology is developing, usage of this technology to replace signature of the data can help to replace the classified information with total transparency. That can increase the cost of the tampered data; hence, it comes to an impossible task to alter data without being sought.[36]

DISCUSSION

The blockchain is one of the leading and emerging technology in the 21st century. The overall theory of the Blockchain technology has given us the insight of this decentralized technology and number of previous literature reviews has helped us to identify the number of possible improvements and concerns that can be taken in consideration in the future. No doubt that the Bitcoin technology has been researched and investigated on the broader scale and this has given an opportunity to study further on this technology towards the future perspective while considering the number of Blockchain applications.

Blockchain technology has already been implemented on the larger scale in cryptography and other sectors of information technology. According to the researcher and investigators, this technology the constitutes of a number of characteristics that are composite of many advantages which are fairly well to be used in the financial sector, however, there are still limitations of implementing this technology over the large scale during this era of the modern World. The experts are still hopeful for the Blockchain technology to perform the future contribution due to the immense advancements and the development in the Internet industry.

This technology was designed for the digital currency such as bitcoin, ripple, we can send this digital money to anyone. It doesn't have any physical worth. It stores information or data over the network to make it centralized or distributed system, so anyone can access it. There is a number of blocks in blockchain technology which contains all data. The blockchain technology uses a cryptography to make a system more secure and transparent. For transactions, it provides an open decentralized database like for money, goods or work. Blockchain has a vast network of nodes and for execution of transactions, it uses different clients, transactions like relaying and validating. The blockchain is one of the emerging technologies of this century, and many researchers and investigator are putting their efforts to get the best possible deal out of it. Its tremendous advantages and useful implications in a number of different areas can never be ignored.

ALGORITHMS

The blockchain technology uses different consensus algorithms. The consensus algorithm is a technique or a process in the computer field to attain the goal among distributed systems. There are different consensus algorithms that are used to achieve the results i.e. Paxos, Chubby (it is a google implemented distributed service) and Proof of Work. The Proof of Work algorithm is used in blockchain technology to secure the bitcoin blockchain and it can be used to get consensus between different nodes. There are some other methods and algorithms that are used in blockchain technology for getting a good result which is, Proof of Stake, Delegated Proof of Stake and Practical Byzantine Fault Tolerance. Proof of Stake method is used to mine the transactions according to your holding coins. It means that you have more power in mining if you have more coins. We can say that Proof of Stake method works directly proportional to the coins you have. Peercoin was the first coin that used Proof of Stake method. Delegated Proof of Stake method is used to solve the scalability issues that faced the users in the blockchain. EOS, BitShares and Steam used this method. Delegated Proof of Stake is also sped up the transactions and creation of blocks. Byzantine Fault Tolerance defines the system which permits the class of failure from Byzantine Generals' Problem. The most difficult class of failure modes is a Byzantine failure because a node can generate any garbage value during the transactions which are very difficult to handle.

USER ROLES IN BLOCKCHAIN PROJECT

There are three different types of user roles in Blockchain project which are Application Developer, Solution Administrator and Business Network Participant. Application Developer is developing the application that interacts with the ledger, modelling the business network and Implementing the script files that define transaction behaviour. The Solution Administrator is provisioning the target environment, deploying the business application and managing the blockchain.

The Business Network Participant running an end-user application that invokes transactions, aware of business concepts: assets, participants and transactions and may not be aware of blockchain underpinning.

DEVELOPER CONCEPTS

Developer concepts of applications, models and scripts. The Applications concepts provide front-end for the user and may require different applications per participant. Furthermore, it interacts with the registries to add, delete, update, query and registries persisted on the blockchain. It also connects to blockchain via JavaScript client libraries (SDK) or REST. The model concept provides a domain specific language (.CTO) that defines the type structure of assets, participants and transactions. Moreover, it aims

to match how we talk about business networks in the real world. The script concept provides the implementation of transaction processor logic and it specified in JavaScript. Further, it is designed for any reasonable JavaScript developer to pick up easily.

In terms of security, blockchain technology constitutes a number of vulnerabilities, which must be considered. Although this technology is decentralized from the government agencies, however in terms of its dependence on the technology, it depends on the Internet platform for getting access to the resources like database and another authentication system. While blockchain technology has given a big confidence to the people during its features of very strong cryptography, as once the whole process of performing transactions the process is unchangeable or it is not possible to reverse.

Another major consideration about the Blockchain infrastructure which also includes the Bitcoin system, that the system is highly available as the reason lies in the fact that the blockchain system is decentralized, it doesn't hold any centralized server which makes it resistant to the DDoS attacks. Therefore, this technology is highly acceptable for the people.

CONCLUSION

This technology has the potential to devise a new perspective on trading technologies like the security of the password, decentralized coherence, sharing the public accounts and the visibility of the control as well as the permissions. It surely can create a new society by exchanging different assets that are tangible or intangible in nature. Due to its security features, it is getting better each day in terms of its acceptance towards the people and it is booming the confidence of the users to get themselves involved.

In the past Bitcoin technology used to be considered as the only innovation in the Bitcoin platform, however during the current era it can be seen very clearly that the Blockchain technology is expanding its horizon towards many other sectors which is bringing the innovation to many areas. This technology has shown a great transformation of conventional industry into a much better technological platform where there are features of security, persistence and accuracy. Decentralization and anonymity also remained the best features of this technology.

Currently, blockchain technologies are booming up in an exponential rate and there is still research and investigations that are carried out to ensure the maximum confidence of people towards this technology. Its applications are expanding in various areas of IT which typically include the sector Internet of Things (IoT) and other financial and trading sectors. Instead of having some challenges and issues related to the Blockchain network, ultimate advantages can never be ignored. The World is seen to be moving towards this technology to get more optimal solutions and researchers are putting more effort to make this platform more organized and secure such that any kind of illegal activities could be possibly prevented.

ACKNOWLEDGEMENT

This research paper is an outcome of our mutual collaboration of participating actively towards all the tasks. We would really like to thank our lecturers for their outstanding guidance and concerns throughout our work, who remained the guiding star for us, without their engagement and personal interest, this wouldn't have been possible.

We are also very grateful to rest of the university staff members, who have given us environment and space where we can get access to the modern learning recourses whether it is a library or the virtual platform of University Breo. We would also like to thank our rest of the classmates, who has guided us time to time where we have required any help in anything.

References

[1] "Beyond Bitcoin: Emerging Applications for Blockchain Technology", NIST, 2018. [Online]. Available: https://www.nist.gov/speech-testimony/beyond-bitcoin-emerging-applications-blockchain-technology. [Accessed: 05- Jul- 2018].

[2] E. Zukerman, "Bitcoin Reviewed: Clever, Controversial Financial/Social Experiment", PCWorld, 2018. [Online]. Available: https://www.pcworld.com/article/230594/Bitcoin.html. [Accessed: 02- Jul- 2018].

[3] Yuan Yong, Wang Fei-Yue. Blockchain: the state of the art and future trends. Acta Automatica Sinica, J. 2016, 42(4): 481−494.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Consulted, 2009.

[5] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in 18th IEEE International Conference on High Performance Computing and Communications, 14th IEEE International Conference on Smart City and 2nd IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2016, December 12, 2016 - December 14, 2016, 2016, pp. 1392-1393.

[6] P. T. S. Liu, "Medical record system using blockchain, big data and tokenization," in 18th International Conference on Information and Communications Security, ICICS 2016, November 29, 2016 - December 2, 2016, 2016, pp. 254-261.

[7] Y. Xiao, H. Wang, D. Jin, M. Li, and J. Wei, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control," Journal of Medical Systems, vol. 40, p. 218, 2016.

[8] D. Kraft, "Difficulty control for blockchain-based consensus systems," Peer-to-Peer Networking and Applications, vol. 9, pp. 397-413, 2016- 01-01 2016.

[9] M. Vukoli, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in IFIP WG 11.4 International Workshop on Open Problems in Network Security, iNetSec 2015, October 29, 2015 - October 29, 2015, 2016, pp. 112-125.

[10] F. Idelberger, G. Governatori, R. Riveret, and G. Sartor, "Evaluation of Logic-Based Smart Contracts for Blockchain Systems,", Cham, Switzerland, 2016, pp. 167-83.

[11] L. Lamport, R. Shostak and M. Pease, "The Byzantine Generals Problem," Acm Transactions on Programming Languages & Systems, vol. 4, pp. 382-401, 1982.

[12] A. Back, "Hashcash - A Denial of Service Counter-Measure," in USENIX Technical Conference, 2002.

[13] S. King and S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake,", 2012.

[14] Nxtwiki, "Whitepaper:Nxt,", 2015.

[15] P. Vasin, "BlackCoin's Proof-of-Stake Protocol v2,".

[16] "https://bitshares.org/,".

[17] "https://bitshares.org/technology/delegated-proof-of-stake-consensus/,".

[18] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in Symposium on Operating Systems Design and Implementation, 1999, pp. 173--186.

[19] L. Lamport, "The part-time parliament," Acm Transactions on Computer Systems, vol. 16, pp. 133-169, 1998.

[20] L. Lamport, "Paxos Made Simple," Acm Sigact News, vol. 32, 2001.

[21] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," Draft of October, 2013.

[22] Brennon Slattery. (Jun 2011) U.S. Senators Want to Shut Down Bitcoins, Currency of Internet Drug Trade, URL:http://www.pcworld.com/article/230084/

[23] Jonathan Todd Barker. (May 2014) Why Is Bitcoin's Value So Volatile?, URL:http://www.investopedia.com/articles/investing/052014/whybitcoins-value-so-volatile.asp

[24] Jeni Tennison. (Nov 2012) What is the impact of blockchains on privacy? URL:https://theodi.org/blog/impact-of-blockchains-on-privacy

[25] N. M. Hamza, R. A. Sarker, D. . Essam, K. . Deb and S. M. Elsayed, "A constraint consensus memetic algorithm for solving constrained optimization problems," Engineering Optimization, vol. 46, no. 11, pp. 1447-1464, 2014.

[26] J. . Zhang, V. S. Sheng, Q. . Li, J. . Wu and X. . Wu, "Consensus algorithms for biased labeling in crowdsourcing," Information Sciences, vol. 382, no. , pp. 254-273, 2017.

[27] Yuan Yong, Wang Fei-Yue. Blockchain: the state of the art and future trends. Acta Automatica Sinica, J. 2016, 42(4): 481−494.

[28]MEI Haitao, LIU Jie. Industry present situation, existing problems and strategy suggestion of blockchain, J. Telecommunications Science. 2016, 32(11):134-138.

[29]Nakamoto S. Bitcoin: A peer-to-peer electronic cash system, J. Consulted, 2008.

[30]Melanie Swan, Xiao Feng. Blockchain: New Economy Blueprint and Guide, M. NEW STAR PRESS. 2016: 1-4.

[31] Lin Xiaochi, Hu Yeqianwen. A summary of blockchain technology, J. Financial Market Research. 2016(2):97-109.

[32]Liang Liu. Information security technology research in B2B e-commerce application system, D. North China University of Technology. 2013.

[33]Kong Gongsheng. Advances on secure authentication and trusted admission protocols for cloud computing, J. Journal of Henan University, 2017.

[34]ZHANG Yi-fan, DONG Xiao-ju. Visualization analysis and design of DDoS attack, J. Chinese Journal of Network and Information Security. 2017, 3(2):53-65.

[35]LI Yang, XIN Yonghui, HAN Yanni, LI Weiyuan, Xu Zhen. A survey of DoS attack in content centric networking, J. Journal of Cyber Security. 2017, 2(1):91-108.

[36]Lu Rongbo. Analysis and design of proxy signatures and group signatures, D. Southwest Jiaotong University. 2006