**Project report**

*(Review-II)*

**Decentralized Application for**

**Digital Certification**

**Personnel:**

1. Aravind G

2. Varun K

**Introduction:**

Democratic voting is a crucial and serious event in any country. The most common way in which a country votes is through a paper based system, but is it not time to bring voting into the 21st century of modern technology? Digital voting is the use of electronic devices, such as voting machines or an internet browser, to cast votes. These are sometimes referred to as e-voting when voting using a machine in a polling station, and i-voting when using a web browser. Security of digital voting is always the biggest concern when considering to implement a digital voting system. With such monumental decisions at stake, there can be no doubt about the system’s ability to secure data and defend against potential attacks. One way the security issues can be potentially solved is through the technology of blockchains. Blockchain technology originates from the underlying architectural design of the cryptocurrencybitcoin. It is a form of distributed database where records take the form of transactions, a block is a collection of these transactions. With the use of blockchains a secure and robust system for 4 digital voting can be devised. This report outlines our idea of how blockchain technology could be used to implement a secure digital voting system

**Problem statement:**

A number of digital voting systems are currently in use in countries around the world. We researched some of these systems to familiarise ourselves with current implementations, particularly Estonia. Estonia has had electronic voting since 2005 and in 2007 was the first country in the world to allow online voting. In the 2015 parliamentary election 30.5% of all votes were made though the nation’s i-voting system (VabariigiValimiskomisjon, 2016). The bases of this system is the national ID card that all Estonian citizens are given. These cards contain encrypted files that identify the owner and allows the owner to carry out a number of online and electronic activities including online banking services, digitally signing documents, access their information on government databases and i-voting. (Electronic ID Card, no date) In order to vote, the voter must enter their card into a card reader and then access the voting website on the connected computer. They then enter their PIN number and a check is made to see if they are eligible to vote. Once confirmed, they are able to cast/change their vote up until four days before election day. The voter may also use a mobile phone to identify themselves for ivoting if they do not have a card reader for their computer. However, this process requires a specialised SIM card for the phone. (Estonian Ministry of Foreign Affairs, 2015) When a voter submits their vote, the vote is passed though the publicly accessible vote forwarding server to the vote storage sever where it is encrypted and stored until the online voting period is over. Then the vote has all identifying information cleaned from it and is transferred by DVD to a vote counting server which is disconnected from all networks. This 7 server decrypts and counts the votes and then outputs the results. Each stage of this process is logged and audited. During the 2013 Local Election, researchers observed and studied the i-voting process and highlighted a number of potential security risks with the system. One such risk is the possibility of malware on the client side machine that monitors the user placing their vote and then later changing their vote to a different candidate. Another possible risk is for an attacker to directly infect the servers though malware being placed on the DVDs used to set up the servers and transfer the votes. (Springall et al., 2014) However, this report has also come under criticism from the Estonian Information Systems Authority.

**(Paper1)**

**Blockchain:** Technology and Applications

*Report by Christian Muller and Dalmir Hasic*

Department of Computer Sciences University of Salzburg

July 29, 2016

This report focuses on explaining the blockchain technology and its application ﬁelds. They distinguish between multiple types of blockchains and explain the two biggest platforms, namely Bitcoin and Ethereum. While introducing those two platforms they explain the most important technology, algorithms and some of the security issues and solutions are also covered.

**Blockchain Overview**

In this chapter we explore the basics of the blockchain technology and mainly its role in cryptocurrencies. Even though the idea of a blockchain as an underlying architecture is relatively new, there are recent developments which suggest applications of the blockchain in other domains apart from cryptocurrencies.

There are three main categories of blockchain applications:

• Blockchain 1.0: Currency

• Blockchain 2.0: Smart contracts

• Blockchain 3.0: Areas in government, health, science etc.

**Blockchain 1.0**

Because the cryptocurrencies are the ﬁrst real application of the blockchain technology, it is often referred as Blockchain 1.0 [2]. Since the blockchain had its ﬁrst big breakthrough with Bitcoin protocol and cryptocurrency, it is often diﬃcult to distinguish those three main components shown in Figure 1: blockchain, protocol and currency.

Currency

Protocols

Blockchain

Figure 1: Success rates

The blockchain in its basic form can be seen as the distributed, decentralized, transparent and chronological database of transactions, sometimes also called the ledger. The data in the blockchain (e.g. transactions) is divided into blocks. Each block is dependent on the previous one. The system in which a blockchain serves as the database comprises of nodes or workers. These workers are responsible for appending new blocks to the blockchain. A new block can only be appended after all nodes in the system reach a consensus, i.e. all agree that this block is legit and contains only valid transactions. How the validity of transactions is determined and how the nodes compute new blocks, is regulated by the protocol. We will explain Bitcoin protocol in later sections. Blockchain is shared among all nodes in the system, it is monitored by every node and at the same time controlled by none. The protocol itself is responsible to keep the blockchain valid. An illustration of the blockchain can be seen in Figure 2.

Bn

B2

B1

B0

Figure 2: Blockchain

**Beyond Cryptocurrency: Blockchain 2.0**

Almost since the introduction of Bitcoin and its underlying blockchain ledger, researchers began to explore other ﬁeld where a blockchain technology might be of great use. In Chapter 4 we explore Blockchain 2.0 in detail but here, as an introduction, we introduce additional types of blockchains and reason about their potential in other ﬁelds beyond cryptocurrency. Some of those potential applications are:

• General (bonded contracts, multiple signature transactions)

• Financial transactions (pensions, stocks ...)

• Public records (land titels, vehicle registrations ...)

• Identiﬁcation (driver’slicense, ids ...)

• Private records (loans, contracts ...)

• Physical asset keys (home, hotel rooms, rental cars)

• Intangible assets (patents, trademarks...)

In literature [3] two main categories of block chain are distinguished:

• Permission less Blockchain

• Permissioned Blockchain

**Permission less Blockchain**

Permission less blockchains are the ones where anybody can join the network to be a veriﬁer without obtaining any prior permission to perform such network tasks. Since anybody can join, special types of incentive mechanisms are necessary in order for veriﬁers to participate. It has advantage that it can accommodate both anonymous and pseudo anonymous actors. Bitcoin and Ehtereum are examples of permission lessblock chains.

**Permissioned Blockchain**

The other type is the so-called permissioned blockchain where special permission is needed from an authority to become a veriﬁer in the system. Permissioned blockchains are intended to be purpose-built, and can thus be created to maintain compatibility with existing applications (ﬁnancial or otherwise). An advantage of a permissioned blockchain is scalability. In permission less blockchain, the data is stored on every computer in the network, and all nodes verify all transactions.

**Bitcoin**

In this chapter we explore the concrete usage of the blockchain with the most prominent example, namely the Bitcoin. Bitcoin itself presented a revolution in 2009, when it was introduced by Satoshi Nakamoto because it introduced peer-to-peer transactions without the need of an intermediary. The users involved in transactions do not need to trust each other but they trust the system (more precisely the protocol) which comprises of decentralized nodes which verify and validate the transactions. Bitcoin represents the ﬁrst decentralized cryptocurrency in the world and it is the largest of its kind in terms of market value.

**Overview and key technology**

The main parties in the Bitcoin protocol are:

• Sender: the one who initiates the transfer of currency.

• Receiver: the recipient of the transfer

• Miners: Independent nodes which verify and conﬁrm the transactions, also sometimes called as workers. The security of the system is guaranteed by these nodes.

• Blockchain: Decentralized ledger shared among all miners where all transactions are stored (the complete history since the Bitcoin creation)

The system has following characteristics:

• Decentralized: The work is done by miners which are located around the world. Moreover any individual who possesses a device capable of performing computation can participate.

• Pseudo-Anonymous: Users are identiﬁed via public keys in the system and there is no way to know to whom the public key belongs unless it is made public by the owner of the key.

As mentioned above the public-key cryptography is used to identify and verify the users, that are for signing the transactions. Also cryptographic hash functions play a crucial role. Their unique properties of one-wayness (there is no way of knowing what is the string that produced a given hash) and collision resistance (it is highly improbable to ﬁnd two messages m1 and m2 which have the same hash or for a given m1 to ﬁnd m2 with the same hash value) are used in the so-called proof of work concept. More about this concept in subsequent sections. The last part are digital timestamps, which can be issued by the 3rd party to specify the time when a transaction is included in the block.

**Blockchain Security**

In this section we explore how Blockchain makes it highly improbable for someone to cheat the system or to do fraudulent actions. One of the biggest potential problems is the so-called double spending problem. This means that a user can try to spend coins twice or more times. That is: initiate multiple transactions with the same Bitcoins as an input. Of course this should not be allowed and only one transaction should go through and others should fail. From section 3.2 we know that when a transaction is created it gets broadcasted to all nodes in the system which, before incorporating the transaction in the blockchain, actually checks whether the user who initiated the transaction is owner of the Bitcoins and whether he tried to double spend them. If a user would attempt to do this, the second transaction would fail and everybody in the system would know that the user, Alice, is not honest and would not trust her anymore. But there is one other problem and that is the possibility of multiple blockchains to exist, or multiple versions of the history. We know that everybody should work on one chain, but it is possible that some users did not receive notiﬁcation that a new block is created or they want to create their own version of the chain with bad transactions in it etc. and then multiple versions could exists at some point.

**Blockchain 2.0: Applications**

After the rise of the Bitcoin protocol people started to think about application domains other than cryptocurrency. The nature of the blockchain network has the potential to enable the development of a wide range of diﬀerent applications that are decentralized. Decentralized applications are becoming more and more important in recent years. In this context not only the architectural decentralization is important but the politcal one as well. Blockchain based applications cannot be stopped censored or controlled and they ensure transparency and trust between all parties involved in the interaction. The discussion about whether these are arguments for or against the use of decentralized application often depend on the context of the usage too. Because every information on the blockchain is public, one will not ﬁnd many people thrilled to use a medical blockchain application and feed it with their personal medical history for example. The focus of a new generation of the blockchain applications is not on the transfer of money via transactions on the blockchain but on carrying out serious computation on a decentralized network of computers. Despite the fact that the use of the blockchain as a ledger for decentralized applications oﬀers a seemingly unlimited amount of potential, many concerns regarding the use of the blockchain exist. One of the largest problems with blockchains is the issue of scalability. As for now the use of the blockchain for applications requieres every full network node to perform every calculation to reach consensus. Before the blockchain technology is able to become a mainstream this is a problem that certainly needs to be solved. This is a problem among many others. In section 5.5 we will try to shed light on a few of them.

Blockchain shows potential to be used in many diﬀerent ﬁelds and some of them are:

• Domain registration (Namecoin)

• Trading Assets (Colored Coin)

• Cloud Storage

• Voting

• Crowdfunding

• Car sharing

• Gambling and prediction markets

• Internet of Things

**Ethereum**

Ethereum is a project which attempts to build the generalised technology; technology on which all transaction-based state machine concepts may be built. Moreover it aims to provide to the end-developer a tightly integrated end-to-end system for building software on a hitherto unexplored compute paradigm in the mainstream: a trustful object messaging compute framework.

Our research on Ethereum suggests that there are as many opinions on what Ethereum actually is, as there are people trying to answer that question:

• Public blockchain-based distributed computing platform, featuring smart contract functionality

• multipurpose protocol built for decentralised applications on the blockchain

• Operating system enabling the development of decentralized application

• ﬁrst (slow and expensive to use) decentralised computer

• Bitcoin 2.0 and many more

**Problems and future directions**

Scalability turns out to be a huge issue in all blockchain applications. The throughput of mainstream payment networks exceeds the current throughput of Bitcoin by a factor of roughly 300. In order to increase the number of transactions per second, a simple change of the block size limit would be enough. A bigger block size (beside multiple other negative eﬀects) would lead to the situation that it would be hard for an average user to run a full node. At the time of writing this report the size of the Bitcoin blockchain is about 75GB with a growth of 6 MB per hour. A bigger block size could lead to a faster growth of the blockchain. Depending on the development of storage cost it is quite possible that the blockchain outpaces the average HDD capacity and only a small set of businesses would be able to manage this load, which would defy the entire idea of Blockchain. The problem of scalability is still subject of ongoing discussions in the Bitcoin community. Ethereum faces basically the same problem.

Another main concern is the proof of work approach, which is taken by Ethereum consensus algorithm Ehtash. Although Ethash is ASICs resistant and solves the problem of centralized mining, it does not address the fact that proof of work based mining can be seen as a competition about who can waste the most energy in a certain amount of time. Ethereum tries to develop a consensus algorithm which is fuelled by coins and not real energy. This approach is often called proof of stake. Every single account has a chance of being the creator (owner) of the next block. The chance of an account being chosen to be the owner of the next block is proportional to the amount of coins this account owns.

**Ethereum Applications:**

* DAO
* Augur

**The Rise and fall of theDAO**

The DAO is a Decentralized Autonomos Organization that lives as a smart contract on the Ethereum blockchain. There are actually many DAO’s on Ethereums blockchain. This section is going to focus on a DAO called ”theDAO”. In its ﬁrst stage (initial creation phase) the DAO sells tokens for Ether. After a certain amount of time the DAO stops collecting money and starts to operate. People in possession of tokens can now make proposals on how to spend the money. Needless to say that the DAO itself does not realize projects but transfers Ether to an accepted (by the token holders) contractor. If the voted projects end up becoming proﬁtable, people will get their fair share of the proﬁt.

The concept worked quite well and the DAO managed to collect over 150 Million Dollars in its ﬁrst funding period. Because of that and the fact that DAO was actually hacked right after its ﬁrst funding period we chose to write about this particular Ethereum application. The hack of DAO shows that even if we make the assumption that there are no attack vectors against the Ethereum system itself (which of course nobody can do), the contracts will always be the weak spot of Ethereum. The hacker managed to exploit a software bug in the contract and stole about a third of the money the DAO had managed to collect (60 Million Dollars).

**Augur**

Augur offers a decentralized platform that enables people to make predictions

about the future. After the event occured those who forecasted the event correctly win money,while the people who guessed wrong will lose money. An interesting fact about Augur however is that, unlike many other blockchain

Application, Augur works with external variables. It is necessary that participants

Of the market report the outcome of the event in question back to the

market.

**Conclusion**

This report tried to give an introduction into the wide spectrum of use cases of the blockchain. With Bitcoin and Ethereum we discussed probably the two most prominent state of the art representers of the blockchain technology. We saw that in recent years, people started to move away from building only economic systems on top of the blockchain. In times of a quite centralized Word Wide Web (Facebook, Google, Amazon etc.) this development seems quite refreshing. If successful, decentralized block chain applications could play a major role in the redemocratisation of the internet, by shifting the power from the big players back to the users. On the other hand this ﬁeld is still pretty young, prone to problems and seemingly quite far away from being able to replace the big players. Only time will tell how this battle turns out.

**A Review on Consensus Algorithm of Blockchain**

Du Mingxiao\*, Ma Xiaofeng\*, Zhang Zhe\*\*,

Wang Xiangwei\*, Chen Qijun\*

\*Department of Control Science and Engineering,

Tongji University Shanghai, China

\*\*Fintech Laboratory,

QianBao Financial Services Company Beijing, China

Blockchain is the basic technology of bitcoin. Blockchain has the characteristics of decentralization, stability, security, and non-modifiability. It has the potential to change the network architecture. The consensus algorithm plays a crucial role in maintaining the safety and efficiency of blockchain. Using a right algorithm may bring a significant increase to the performance of blockchain application. In this paper, we reviewed the basic principles and characteristics of the consensus algorithms and analyzed the performance and application scenarios of different consensus mechanisms.

The blockchain was firstly introduced in the treatise [1] “Bitcoin: A peer-to-peer electronic cash system” by Satoshi Nakamoto in 2008. It is the underlying technology of bitcoin. The traditional transactions require a centralized trusted institution. The confirmation and record of the transactions depend entirely on the trusted institution, which may cause many problems of transaction cost, efficiency, and security. Decentralization is the core feature of blockchain and it can be used to solve these problems. All the nodes in the blockchain have equal status. These nodes achieve consensus by using the prior agreement of the rules and following the principle of majority dominance. They implement the functions of data distributed storage and transaction information recognition in the situation that the other nodes are not fully trusted. So we can effectively solve the transaction problems. Bitcoin is the first blockchain application in the financial field. With the development of the blockchain technology, blockchain has been concerned by the government, financial institutions, and technological enterprises

All major banks in the world are actively exploring the application of blockchain technology. In August 2016, UBS, Deutsche Bank, Bank of Santander and Bank of New York Mellon jointly developed a digital currency system with blockchain technology to help financial markets improve the speed of payment. Bank of Santander, the largest bank in Spain, believes that if all banks in the world use the blockchain, they can save about $20 billion every year. World Economic Forum predicts that 10% of the world's GDP will be stored on the blockchain network by 2027 [3].

In the academic field, the blockchain technology is also attracting more and more attention. The study of blockchain can be divided into three categories. Firstly, study on the digital currency that based on blockchain, including the decentralized and centralized digital currency [4]. Secondly, study on the application of blockchain technology in non-digital currency scenarios such as the application of blockchain in smart city [5] and medical information security management [6, 7]. Thirdly, study on underlying blockchain technology. More and more researchers realize that the blockchain can be stripped out from the digital currency to create a revolutionary technical architecture in other areas. Some researchers have begun to study the underlying technologies such as the difficulty control of mining[8], the scalability of consensus algorithms [9] and the smart contract [10].

Blockchain technology includes the point-to-point(P2P) communication, consensus algorithms, distributed storage technology, encryption algorithms, and so on. But at present, the research on blockchain is mainly focused on the application of Bitcoin or blockchain in different areas.

THE CONSENSUS ALGORITHMS

In the applications of blockchain, we need to solve two problems- double spending and Byzantine Generals Problem [11]. Double spending problem means reusing the currency in two transactions at the same time. The traditional currency is the entity, so we will not face the problem of double spending while using traditional currency. We can also solve the double spending problem in the Internet transactions with the centralized trusted institutions. Blockchain solves this problem with the method of verifying the transactions by many distributed nodes together. Byzantine Generals Problem is the problem in the distributed system. The data can be delivered between different nodes through peer-to-peer communications. However, some nodes may be maliciously attacked, which will lead to the changes of communication contents. Normal nodes need to distinguish the information that has been tampered and obtain the consistent results with other normal nodes. This also needs the design of the corresponding consensus algorithm. The consensus algorithm has been studied for many years in distributed system. There are some transplantable consensus algorithms applied in blockchain. Those principles are :

A. PoW (Proof of Work)

PoW is the consensus algorithm used in bitcoin. Its core idea is to allocate the accounting rights and rewards through the hashing power competition among the nodes. Based on the information of the previous block, the different nodes calculate the specific solution of a mathematical problem. It’s difficult to solve the math problem. The first node that solves this math problem can create the next block and get a certain amount of bitcoin reward. Satoshi Nakamoto used HashCash to design this mathematics problem in bitcoin [12]. The specific calculation steps are as follows:

1) Get the difficulty: After the production of every 2016 blocks, bitcoin mining algorithm will dynamically adjust the difficulty value according to the hash rate of the whole network.

2) Collect transactions: Collect all pending transactions on the network after the production of the last block. Then calculate the Merkle Root of these transactions and fill in the block version number, the 256-bit hash value of the previous block, the current target hash value, Nonce random number and other information.

3) Calculating: Traverse the Nonce from 0 to 232 and calculate the double SHA256 hash value in step 2. If the hash value is less than or equal to the target value, the block can be broadcasted. The node complete accounting After the verification of other nodes.

4) Restarting: If the node can't work out the hash value at a certain time, it repeats step two. If any other node completes the calculation, then it restarts from

step 1. PoW takes the workload as the safeguard. The newly created block is linked to the blocks in front of it. The length of the chain is proportional to the amount of workload. All nodes trust the longest chain. If anyone wants to tamper with the blockchain, he needs to control more than 50% of the world's hashing power to ensure that he can become the first one to generate the latest block and master the longest chain. The gains from tampering can be much greater than the cost. So the PoW can effectively guarantee the safety of the blockchain.

B. PoS(Proof of Stake)

PoShas been mentioned in the first bitcoin project, but it was not used because of the robustness and other reasons. The earliest application of PoS is PPCoin [13]. In PoS, the digital currency has the concept of coin age. Coin age of a coin is its value multiplied by the time period after it was created. The longer one node holds the coins, the more rights it can get in the network. Holders of the coins will also receive a certain reward according to the coin age. In the design of PPCoin, mining is also needed to get the accounting rights. The formula is proofhash< coin age \* target. The proofhash is a composed hash value of the weight factor, the unspent output value and the fuzzy sum of current time. PoSlimits the hashing power of each node. The difficulty of mining is inversely proportional to coin age. PoSencourages the coins holders to increase the holding time. With the concept of coin age, the blockchain is no longer entirely relying on the proof of work. That effectively solves the resource wasting problem in PoW. The security of the blockchain using PoS improves with the increasing value in the blockchain. The attackers need to accumulate a large number of coins and hold them long enough to attack the blockchain. This also greatly increases the difficulty of attack.

C. DPoS(Delegated Proof of Stake)

In the initial design stage of bitcoin, Satoshi Nakamoto hoped that all the participants can use the CPU to mine. So the hashing power can match the nodes and each node has the opportunity to participate in the decision-making of the blockchain. With the development of technology and the appreciation of bitcoin, the machines that are specially designed for mining are invented. The hashing power is grouped in the participants that have large numbers of mining machines. The ordinary miners rarely have the opportunity to create a block.

BitShares is an example of DPoS [16]. In the blockchain with DPoS, each node can select the witnesses based on its stake. In the whole network, the top N witnesses that have participated in the campaign and got the most votes have the accounting right. The number N of witnesses is defined such that at least 50% of voting stakeholders believe there is sufficient decentralization [17]. The elected witnesses create new blocks one by one as assigned and get some rewards. The witnesses need to ensure adequate online time. If a witness is unable to create its assigned block, the activity of that block will be moved to the next block and the stakeholders will vote for a new witness to replace it. The blockchain using DPoS is more efficient and power-saving than PoW and PoS.

D. PBFT(Practical Byzantine Fault Tolerance)

In distributed systems, Byzantine Fault Tolerance can be a good method to solve the transmission errors. But early Byzantine system requires exponential operations. Until 1999, the PBFT(Practical Byzantine Fault Tolerance) system [18] was proposed and the algorithm complexity was reduced to a polynomial level, which greatly improved efficiency. The process of PBFT is shown in figure 1. It consists of five states:

1) Request: The client sends a request to the master server node, the master node gives the request a timestamp.

2) Pre-prepare: The master server node records the request message and gives it an order number. Then the master node broadcasts a pre-prepare message to the other following server nodes. The other server nodes initially determine whether to accept the request or not.

3) Prepare: If a server node chooses to accept the request, it broadcasts a prepare message to all the other server nodes and receives the prepare messages from the other nodes. After having collected 2f+1 messages, if a majority of nodes choose to accept the request, then it will enter the commit state.

4) Commit: Each node in commit state sends a commit message to all the other nodes in the server. At the same time, if a server node receives 2f+1 commit messages, it could believe that most nodes reach a consensus to accept the request. Then the node executes the instructions in the request message.

5) Reply: the server nodes reply to the client. If the client does not receive a reply because of the network delay, the request is resent to the server nodes. If the request has been executed, the server nodes only need to send the reply message repeatedly.

E. Raft

Lamport proposed Paxos algorithm to solve the consistency problem in certain conditions. The Paxos occupies the dominant position in the field of consistency algorithm. Many other algorithms are derived from it. But Paxos algorithm is too theoretical. The people have great difficulty in understanding it and engineering implementation. In 2013, Standford’sOngaro and others published the paper and proposed Raft algorithm[21]. Raft achieves the same effect as Paxos and is more convenient in engineering implementation and understanding. Raft cluster generally contains 5 server nodes. Up to two nodes are allowed to crash at the same time. The server node as shown in figure 2 has three states: leader, follower, and candidate. There is only one leader in a term and the leader is responsible for handling all clients’ requests.

ANALYSIS OF THE CONSENSUS ALGORITHMS

All the consensus algorithms have their own characteristics. In this chapter, we analysis the safety, verification speed, throughput (transactions per second, TPS), fault tolerance, scalability and shortcomings of the consensus algorithms and the usage in different scenarios. A. Performance PoW and PoS solve the safety problem by using the share ledger of the whole network. The system is stable as long as the longest chain is guaranteed by the honest nodes. We take PoW as an example to provide a proof of safety. Hypothesis: the total hashing power in the network is H0, the average time for creating a new block is T0, the total hashing rate of honest nodes is pH0 and the total hashing rate of malicious nodes qH0. The difficulty is changeless when calculating the double spending probability. One transaction is verified after n blocks.

B. Limitation

PoW also has weaknesses such as waste of resources, slow speed of transaction verification and concentration of hashing power:

1) Waste of resources: the nodes which have high hashing power can get the corresponding bitcoins as rewards. This is the main way to get the bitcoin, which forces people to upgrade the hardware. Participants need to spend a lot of money to buy the special mining machines and the machine needs to consume a large amount of electricity in the process of calculation. These characteristics also make the application of PoW some limitations.

2) The slow speed of transactions: In order to reduce the production of single block or branch of the chain, the calculating time of each block must not be too short. The average calculating time of the block is 10 minutes. But the time interval between the two blocks is not sure. The largest interval in history is more than one hour while the minimum interval is less than one second. This time has a great limitation in the application of instant payment.

3) The concentration of hashing power: With the increase of mining difficulty, it’s hard for a single one to figure out the math problem. In order to solve this problem, some organizations have set up the "mining pool", and the miners in a mining pool solve the math problem together. After a pool solving the math problem and obtaining the bitcoin as rewards, the miners allocated the bitcoin according to their contribution. But because of the existence of the mining pool, the global hashing power become concentrated. If the hashing power of one pool or some combined pools is more than 50%, they can easily have a monopoly on accounting. The monthly hashing power rankings. At present, the global top six mining pools’ hashing power has been more than 50% of global hashing power.

In Raft, the leader occupies an absolute dominance. It’s very important to defend the safety of the leader. Once the leader is maliciously controlled, the system will be completely destroyed. In addition, the system performance is limited by the maximum throughput of the node.

C. Application Scenarios

The blockchain can be divided into three categories: Public blockchain, private blockchain, and permissioned blockchain. According to the previous section, it is better to use the corresponding consensus algorithm in different scenarios. A public blockchain means that it is accessible to all the people in a public area. Everyone can become one of the nodes and make contributions to obtain the rewards following the rules. There are no trust relationships among the nodes. Public blockchain is completely open and decentralized. All transactions on the public blockchain can never be changed or revoked. PoW, PoS, and DPoS consensus algorithms are common choices of public blockchain.

Private blockchain means that the owner of the blockchain has the highest authority to change the information. The rest of the nodes have limited access to read. Compared to the public blockchain, the private blockchain has the characteristics of easy modification and low transaction cost. Transaction verification of the private blockchain only need some designated high credit nodes. Private blockchain is applied to more closed networks such as the intranet. It is more important to solve the crash faults than Byzantine faults. We can use PBFT and RAFT consensus mechanisms according to the network size. Permissioned blockchain means that the blockchain is composed of many parties and the main nodes are pre-specified by the participants. The members of the permissioned blockchain do not fully trust the others. Each participant selects its own consensus node according to the rules. Transactions need to be recognized by most consensus nodes. The degree of openness and centralization of the consortium blockchain lies between the public and private blockchain. The permissioned blockchain is suitable for the semi-closed network, which is built by different enterprises. There may be conflicts among different enterprises and some nodes can become malicious nodes, so it is better to use PBFT in this scenario.

SUMMARY

Blockchain has the characteristics of decentralization, stability, security, non-modifiability and so on. With the development of technology, the blockchain is attracting more and more attention in different areas. This paper makes a systematic review of the usual consensus algorithms used in the blockchain. Consensus algorithm is the core technology of blockchain, but current research of the consensus mechanism is still in its infancy. The consensus algorithm specially designed for different scenarios is still very rare. How to make the blockchain performance better in a particular scenario? We still need further research.