A Review on BlockChain Security

IOP Conf. Series: Materials Science and Engineering **396** (2018) 012030 doi:10.1088/1757-899X/396/1/012030

A Review on BlockChain Security

Remya Stephen
PG Scholar, St.Joseph College of Engineering and Technology, INDIA
E-mail: remyastephen93@gmail.com

Aneena Alex
Asst.Professor, St.Joseph College of Engineering and Technology,INDIA
E-mail: aneenaalex@gmail.com

Abstract. Blockchain is a decentralized technology. It has extensive power to solve business problems. Cryptography secures the records in a blockchain transaction and each transaction is tied to previous transactions or records. Blockchain transactions are validated by algorithms on the nodes . A single entity cannot create a transaction. Finally, blockchains provide transparency, giving each participant the ability to monitor the transactions at any time. Smart contract make secure transaction which helps to avoid third party disruption .Ethereum is a decentralized platform that runs smart contracts. This enables developers to create markets move funds in accordance with instructions given long in the past. The main features of blockchain are Decentralization, Immutability Faster dealings, Transaction and validation happens in seconds etc..

1. Introduction

Blockchain technology has huge potential with a variety of applications and provides wide opportunities for various infrastructure. The technology encourage resource management and makes communication both secure and efcient. Trust is increased when conducting nancial transactions among parties using Blockchain, as it reduces the chances of swindle and automatically produces a record of activities. Creating an automated background check of any member of the system. Due to its decentralized properties, Blockchain creates reliability and reduces the risk faced when looking to enter a business agreement with an unfamiliar party.

Today all people were using advanced technology for communication through internet. Voice call, video call, messages, pictures, are travel directly from sender to receiver over the internet. For this transaction, must maintain a trusted third party between these sender and receiver. When it comes in the case of money transaction, people have to trust a third party for complete this, in traditional system. But in the case of blockchain it will give a perfect security in transaction. A block should record every transaction, it will act like a record book. Once completed a transaction a block goes into the blockchain as a permanent database. If a block is completed a new block is added with this or a new block is generated. Every block carry a hash of the previous block.

2. KEY ATTRIBUTES OF BLOCKCHAIN TECHNOLOGY

2.1. Decentralization

Decentralization is completely different from centralization. It provide more security and exibility than the centralized application. Quick decision making is required and therefore many organizations opted for decentralization[4]. In the centralized environment everything is done in the same location. Where decentralized environment works in different location. It has the ability to provide both efciency and innovation. Efciency deals with saving cost and time ,should provide a better result. Innovation provide new idea. That should be a new benets.

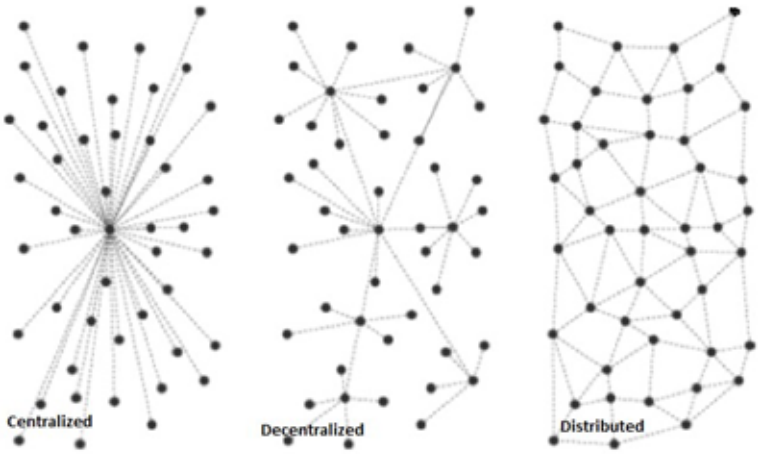

Figure 1. Network Comparison

2.2. Trust

In Blockchain technology each block contain information about the previous block. It will provide an authentication mechanism during the transaction. There is no third party communication. Instead of this that will use a public ledger .All transaction should be automatically recorded in this ledger

2.3. Transparent

In blockchain stored data are transparent and also immutable. That is why blockchain are trusted.

3. PUBLIC AND PRIVATE BLOCKCHAIN

Blockchain is mainly divided in to three types. Public,Private and consortium blockchain.This paper focusing on the comparison between public and private blockchain based on some recent property. Public and private blockchain should have many similarities as well as differences in it's functionality[9].

Property	Public Blockchain	Private Blockchain
Read Permission	Public	Could be public or restricted
Immutability	Approximately beyond to tamper	Could be tampered
Efficiency	Low	High
Centralized	Yes	No

Table 1. Comparison table

4. CHALLENGES IN BLOCKCHAIN

Blockchain has faced some challenges in industry especially during bitcoin transaction. Those problems inherent to functions of the Bitcoin blockchain are compiled below.Summaries some typical challenges below[10].

4.1. Scalability

The amount of transactions are increasing day by day. Most of the companies were suggesting blockchain for their transaction process. All transaction have to be stored and it will be validated. The capacity of the block will very small. Some transaction must be delayed due to miner prefer high transaction fee to those transaction. So the large block size will lead to reduce the propagation speed. There fore scalability problem is quite though.

There some methods to avoid the scalability problem in blockchain

- Storage Optimization of blockchain
- Redesigning blockchain

4.2. Privacy Leakage

Users believed that blockchain gives better privacy when handling sensitive data. In blockchain users could only generate address instead of their identity. In 2013Meiklejohn and in 2016 Kosba shows that blockchain cannot guarantee the transnational privacy. Recent study shows that bitcoin transactions are linked together to an account address to reveal the identity of user. The problems were leak out the users identity

Elliptic Curve Diffie- Hellman- Merkle(ECDHM) can be used to overcome this problem. It will deals with public and private key. This will exchange shared secrets between two people.It will helps to secured message transaction0n over the internet. A secured platform like smart contract and ethereum is also developed to keep secured transaction

4.3. MITM Attack

MITM [11] means Man in The Middle Attack. This is known as third party interaction. Here a user came in the middle, who may have a forged public key. By using this key, he can easily decrypt the sensitive data. In blockchain public key is distributed across the participating nodes. Each block should be connected with a link to previous and following blocks. Because of this, the public key is immutable it should not attack by any forged keys.

4.4. DDoS Attack

Distributed Denial of Service attack (DDoS) is an attack [11] which is target to attack one particular system Such as c computer, website, server or other network resources. Therefore, the incoming messages or connection to the target system may slow down, or even crash or shut down. Especially in blockchain DDoS attack create some significant business risk. Practically it is impossible to prevent this type of attack.

Flow analytic device is one of the common solution for DDoS attack. This device will be watch and react against the attackers. This will be telling what action to take next. This device would help to clear the traffic. Because it will redirect the bad traffic.

5. SECURITY FEATURES OF BLOCKCHAIN

- Use ledger. Ledger should record each and every transaction in a blockchain. This ledger is immutable. Existing data cannot be edited or deleted. In blockchain technology these ledger is decentralized application. So, no one can access the transaction or even any sensitive data from this ledger [12]. People can only read the information from a ledger.
- Another type of security feature is the chain of block. In blockchain each block should contain a hash value. These blocks are connected by its previous hash. Suppose an attacker came to correct the data, then its hash will be changed. It will affect the overall chain. So, it will increase the protection of sensitive data or information.
- Blockchain technology is a decentralized application. Mainly it will support peer to peer communication. So, in a network node is considered as computers. These thousands of nodes should have the copy of distributed ledger. This should be authenticating the transaction. If any of the node does not agree a transaction, then it cannot be proceeding. So, it will be cancelled[12]. This will protect from a fraud transaction.

6. APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

6.1. Blockchain for health care industry

In today's life patient doesnt like to reveal there treatment details to outsider. In this case patient can use this technology to keep secure all information from others. This blockchain can be used as a website, or mobile app. Each and every user in a blockchain has two keys. Public key and private key. By using this only who can make a transaction. For example there two person Alice and Bob. Alice want to send some secure data to bob. So that Alice sign a digital signature by using here private key. That means private key is always act like as a password. Then shew will hash the data by using here public key and generate an address. Then bob validate the digital signature. If it is validated they will make a transaction. So by using these type of security methods, potions information can be protected from others.

6.2. Electronic medical records.

Patients can handle electronic medical records by using the blockchain technology. Most of the health cares institution should not allow patient to access their medical data. Patients are becoming disappointed about the privacy of their medical records. This all can be avoided by blockchain.

In handling electronic medical records, blockchain should deal with different frame work for managing the authentication, confidentiality, and accountability. It is mainly used when handling the sensitive data. Online electronic records in blockchain will operated as decentralized application. In centralized environment all application should be done at one location. But in decentralized environment application should be done in different location.

Electronic medical records should affect some challenges and limitations. This system will face some important challenges during the implementation of personally controlled system. That is this personally controlled records would replace provider or hospital records. Some segment of the personally controlled records would be downloaded in to the institutional record to tribute the existing data

This challenges can be avoided by blockchain. Because blockchain leads a key exchange based transaction between two parties. Their personal identity does not revel to any others. Because

they are only providing their key identity. Each and every user in a blockchain should have one public key and one private key.

6.3. Blockchain to protect personal data

Today there is recent increase in reported incident of security problem in users personal data. Because of this there is a third party control over the data, who will collect all personal information. Blockchain can eliminate this third party and can transfer directly between two parties.

The amount of data recently increasing in our world. Facebook, is the largest online social-network, collected 300 petabytes of personal data. Personal data or sensitive data should not be secure in the hand of third parties. They are tried to attack and misuse. Blockchain helps users that not required to trust any third party. Blockchain recognizes the users as the owners of their personal data. Blockchain should have its own rules and regulation. It is known as smart contract. Before starting a transaction the gateway keeper should create some rules and will written as a contract. It will make a peer to peer communication. Bitcoin has demonstrated in financial space that is trusted and computing is possible in decentralized network. Blockchain is mainly proposed to handle the bitcoin, it is a digital currency.

6.4. Bitcoin

In 2008 bitcoin is invented as a new way to send value over the internet. Vitalik Buterin,is a programmer, introduced bitcoin in 2011. [2]

Bitcoin is a digital currency, created and held electronically. It is operated as a decentralized application. That directly control the transfer of digital currency. Value of bitcoin increasing in recent year. Bitcoin sets out to solve the distributed tracking and validation of transactions is one ot its main problem. It will keep the full history of transaction. Blockchain is mainly developed to transact this digital currency. If the user wants the recent history, then who can filtering it. Before making a transaction the rules and regulations of this will be written as a contract form known as smart contract. Transaction is only possible between two persons, before making it sender side should enter a digital sign. The transaction is validated by this digital sign. If this sign is validated transaction is proceed, that means botcoin should transacted.

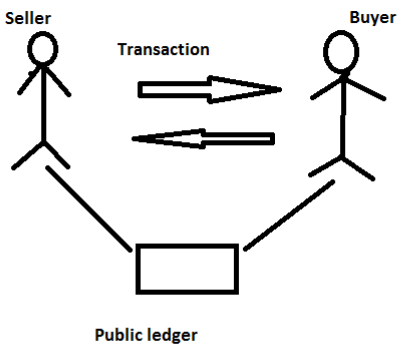

Figure 2. Ledger

6.4.1. SMART CONTRACT: Smart contract is also known as a crypto contract. Smart contract were first proposed by Nick Szabo in 1994. It is a computer program, it directly control the transfer of digital currency. These contracts are stored on blockchain technology. Smart contract is a decentralized system. It is existed in two parties[6].

There is no need to pay a middleman. It will saves time and conflict. Ledger is used in smart contract. It is a decentralized application.

6.4.2. LEDGER: Ledger is a decentralized application assigned to each user in a blockchain. After completing a transaction it will be recorded in the ledger automatically. For example there is two person A and B. The person A must give 100 rupees to person B. There is some other person is this blockchain. They also have a separate ledger. This data will be automatically updated in everyones ledger. Person A said that who should only give 10 rupees to B. Then there will be a voting mechanism. This voting mechanism can prove that the statement by person A is not validated. Therefore it will be rejected.

This Public ledger is best suited for all crypto currency transaction. There is no central administrator or centralized data storage.

6.4.3. Ethereum: Ethereum is a decentralized platform that runs the blockchain. That enables developers to build and deploy decentralized applications. Ethereum is similar to Bitcoin. Because it is a distributed public blockchain network. But there are some technical difference between these two. For each ethereum application the network needs to keep the current state information. Including all users balance ,smart contract code and where its all stored.[3]

Ether is a crypto currency, its blockchain platform is developed by Ethereum

7. OTHER APPLICATIONS

Blockchain have lot of applications in industry.Some of them are given below(fig:3). Today banking professionals were tried to adapt blockchain to make secure transaction. Finance is one of the most evident application of blockchain.

8. ANALYSIS

This paper tells about security of blockchain technology. From this review paper we can analyses that blockchain technology has facing some security issues. These security issues should affect the transactions also. There is a chance for different types of attacks in this technology, and also give some solutions to these issues. There are mainly three types of blockchain networks. Public, private and consortium. This review paper only concentrating on both public and private blockchain. Gives a short study between these by a comparison table.

Blockchain technology is an increased trending technology. Many applications are developed based on this technology. This review paper gives some solution for recent issues of blockchain.

9. CONCLUSION

Blockchain is an amazing topic in recent year, it will support different applications. Blockchain will give Better security during transaction of any value. This technology is mainly proposed to handling bitcoin transaction.Smart contract, Ethereum and distributed ledger are some applications of blockchain, This will also give more security.

Best suited and mostly used application of blockchain bitcoin. Blockchain gives faster and cheaper transaction than any other application. It will provide a better security especially to sensitive data. Blockchain applications often see additional benefits in its transparency and immutability.

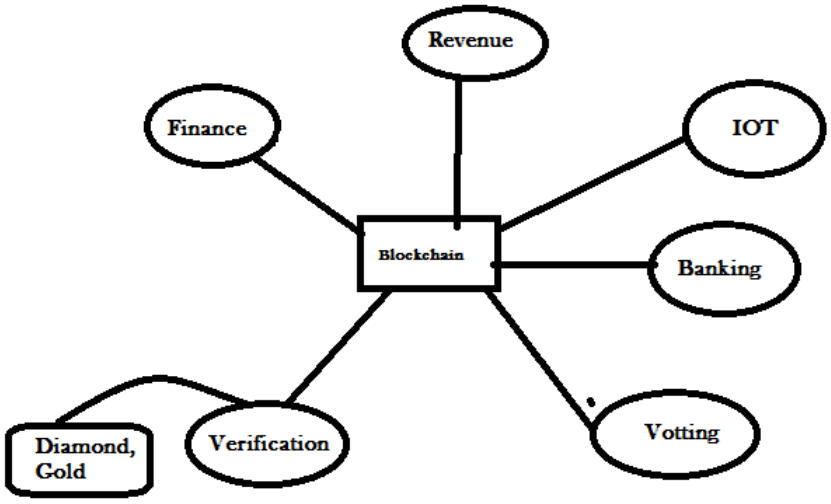

Figure 3. Applications

10. REFERENCES

[1] http://www.blockchain4innovation.it/wp-content/uploads/sites/4/2017/05/Blockchain-
[2] https://www.coindesk.com/information/who-created-ethereum
[3] https://www.coindesk.com/information/how-ethereum-works
[4] A Survey of blockchain security issue and challenges(Iuon-Chang Lin1,2 and Tzu-Chun Liao2)[jan-12- 2017]
[5] Public standares and patients controll:how to keep electronic medical records accessible but private(Kenneth D Mandl,Peter Szolovits,Issac S Kohane)[3 february 2001]]
[6] https://blockgeeks.com/guides/smart-contracts/
[7] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, Medrec: Using blockchain for medical data access and permission management, in 2016 2nd International Conference on Open and Big Data (OBD), Aug 2016, pp. 2530.
[8] G. Zyskind, O. Nathan, and A. . Pentland, Decentralizing privacy:Using blockchain to protect personal data, in Security and Privacy Workshops (SPW), 2015 IEEE, May 2015
[9] https://www.researchgate.net/publication/319058582 Blockchain Challenges and Opportunities A Survey
[10] http://www.meti.go.jp/english/press/2016/pdf/0531 01f.pdf
[11] https://www.dotmagazine.online/issues/innovation-in-digital-commerce/what-can-blockchain-do/security-and-privacy-in-blockchain-environments
[12] https://www.business2community.com/tech-gadgets/issues-blockchain-security-02003488