AN OVERVIEW OF SECURITY ISSUES AND CHALLENGES RELATING TO BLOCKCHAINTECHNOLOGY

Himalaya Singh*

Dr. Shilpa Vardia **

ABSTRACT

Blockchain technology (BT) is one of the most popular problems in the recent years, it has already changed people's lifestyle in some specific area due to its hugeeffect on many organizations or institute, and What itcan do will still continue to cause impact in many places. Although the characterization of (BT) blockchain technologies can bring us more reliable andsuitable services, the security issues and challenges behind this modern technology are also an importanttopic that we need to worry about.

Keywords: Blockchain, Technology, Security issue, risks, Cryptocurrency, Ethereum, Smart contract.

Introduction

Bitcoin, Cryptocurrency, Ethereum, Smart contract is the initial application of blockchain, it's a types of digital currency based on (BT) blockchain technology, using for trade things on the internet like money as we do in the real world. Because the success of Bitcoin, Cryptocurrency, Ethereum, Smart contract citizens now can use blockchain technology in a lot of area and service, such as financial market,IT, supply chain, voting, medical treatment andstorage.

But as we use these tools or services in our dailylives, cyber criminals also have the opportunity to engage in cyber-crime. For example, 70-75% ofattacks are a classic security issue in Bitcoin, Cryptocurrency, Ethereum, Smart contract that hackers try to control the system's mechanisms using the same technology base.

In this paper, we will have a pilot study about 1, what is blockchain technology in Section 2, then we'lldiscuss different application in blockchain 3, and what service do they offer in Section 4, at the end, we shall talk about the security issues and those challenges we need to overcome in Section 5, The paper is concluded in Section.

*Research Scholar, Department of Accountancy and Business Statistics, University College of Commerce and Management Studies (Mohanlal Sukhadia University, Udaipur, Rajasthan), himalayasingh2377@gmail.com

**Assistant Professor, Department of Accountancy and Business Statistics, University College of Commerce and Management Studies(Mohanlal Sukhadia University, Udaipur, Rajasthan), shilpa.vardia@gmail.com

Concept of Blockchain

It is not presently only single individual technique, but contains Cryptography, mathematics, Algorithm and economic financial model, combine (P2P) peer- to-peer networks and using distributed consensus algorithm to solve traditional distributed database coordinate problem, it's an integrated multifield infrastructure construction.

The blockchain technology expressed of six key fundamentals.

Decentralized

The essential attribute of blockchain, means that blockchain doesn't have to rely on centralized node anymore, the data can be collection, classification, record, store.

Transparent

The data's record by blockchain system is transparent to each node, it also transparent on update the data, that is why blockchain can be trusted.

Open Source

Most blockchain system is open to every- one, record can be check publicly and people can also use blockchain technologies to create any application they want.

Autonomy

Because of the base of consensus, every node onthe blockchain system can transfer or update data safely, the idea is to trust form single person tothe whole system, and no one can intervene it.

Immutable

Any records will be reserved forever, and can'tbe changed unless someone can take control morethan 70% node in the same time.

Anonymity

Blockchain technologies solved the trust problem between node to node, so data transfer or even transaction can be anonymous, only need to knowthe person's blockchain address.

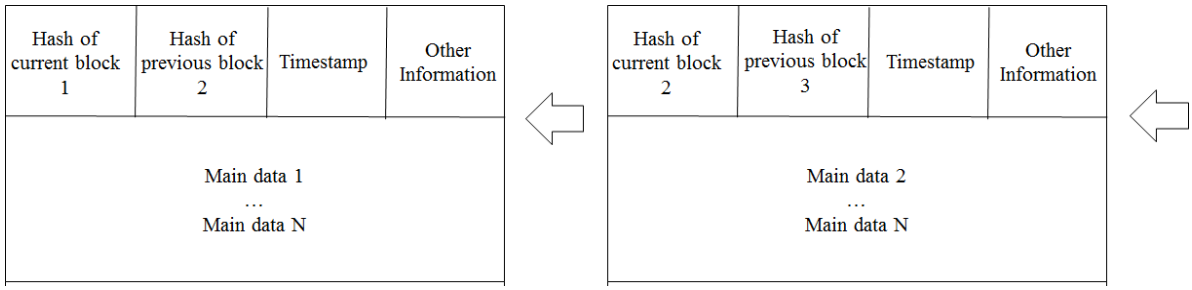

Figure No 1: The structure of block chain

How Blockchain Works?

The main working processes of blockchain are asfollows:

1 The sending node records new data and broadcasting on the network.

2 The receiving node checked the message from thedata it received, if the message was correct it would be stored in a block.

3 Execute the Proof of Work (PoW) or Proof of Share (PoS) algorithm for all received nodeblocks in the network.

4 After executing the consensus algorithm theblock will be stored in the series, each node in thenetwork accepts this block and will continuously expand the chain base on this block.

The Structure of Blockchain

Normally in the block, it contains main data, hash ofprevious block, hash of current block, timestamp and other information. Figure 1 shows the structure of block.

Main data. Depending on what service is this blockchain applicate, for example: transactionrecords, bank clearing records, contract records or IT data record.

Hash.

When a transaction was executed, it was hashed in a code and then transmitted to each node. Because it can contain thousands of transaction records in each node's block, the blockchain used the Merkle Tree function to generate the final hash value, which is also the Merkal Tree Root. This final hash value will be recorded in the block header (the hash of the current block), using the Merkle tree function, data transmission and computing resources canbe significantly reduced.

Time stamp. Time of generated block.

Other Information. The block defines signatures, Nonce values, or other data like that the user.

How to Get Consensus?

The consensus function is a mechanism that consentsall blockchain nodes in a single message, can ensure that the latest block is added correctly to the chain, guarantee that the message stored by the node was thesame and will not be a 'fork attack', even protecting against malicious attacks.

Proof of Work (PoW)

Proof of work is a piece of data that is difficult (expensive or time-consuming) to produce but easy to verify for others and that meets certain requirements. Preparing a proof of work can be a random process with little probability so that on average a lot of trialand error is required before valid proof of work can begenerated. Bitcoin uses hashcash proof of the work system.

When calculating a POW, it is called 'mining'. Eachblock has a random value called 'nones' in the blockheader, by changing this nons value, the POW mustgenerate a value that makes this block header hash value less than the 'difficulty target' that has alreadybeen set. The difficulty means how long it will take when the node calculates the hash value less than thetarget value. In order for network participants to accept a block, miners must complete a proof of work that covers all the data in the block. The difficulty ofthis work is adjusted so as to limit the rate at which anew block can be generated every 5 minutes by the network. Due to the very low probability of successfulgeneration, it makes it unpredictable which worker computer in the network will be able to generate thenext block.

Proof of Stake (PoS)

Because the proof method of work will waste a lot ofelectrical power and computing power, the proof of the stakes does not require expensive computing power. With proof of stake, the resource that is compared is the amount of bitcoin that a miner owns, someone holding 2% of bitcoin can mine 2% of the'proof of stake block'. Proof of the stake method canprovide increased protection from malicious attacks on the network. Additional security comes from two sources:

1. Carrying out an attack would be much moreexpensive.
2. Less incentive for attack. The attacker must ownalmost the majority of all bitcoins. Therefore, theattacker suffers severely from his own attack.

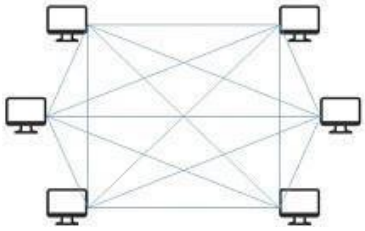

Figure No 2: Public blockchain

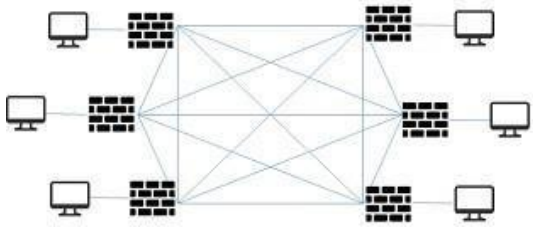

Figure No 4: Private blockchain

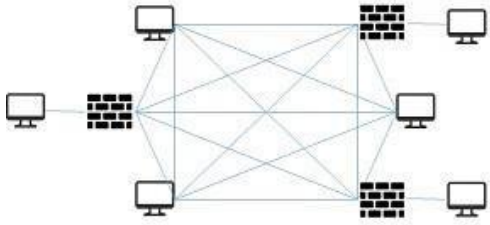

Figure No 3: Consortium blockchain

Type of Blockchain

Blockchain technologies can be roughly divided intothree types.

1. **Public blockchain**:Everyone can check and verify transactions, as well as participate in the process of achieving consensus. Eg: Both Bitcoinand Ethereum are public blockchains. Figure 2 shows a public blockchain

2. **Consortium blockchains:** This means that thenodes that have authority can be chosen in advance, usually there is a business-to-business- like partnership, data in the blockchain can be open or private, it can be seen as partially decentralized Is. Like Hyperledger and R3CEV are both consortium blockchains. Figure 3 shows the consortium blockchain.

3. **Private blockchain:** Node will be restricted, not every node can participate in this blockchain, there is strict authorization management on data access. Figure 4 shows a private blockchain.

Application of Blockchain Technology

Blockchain technologies can be used in many areas, not only in financial applications, but also in other industries.

Digital Currency: Bitcoin

Bitcoin's data structure and transaction system were created by blockchain technology, making bitcoin a digital currency and online payment system. By using encrypted technology, money transfers can be achieved and there is no need to depend on a central bank.

Bitcoin used public key addresses to send and receive bitcoins, record transactions, and personal IDs were anonymous. The process of verifying a transaction requires the computing power of other users to achieve consensus, and then record the transaction in the network.

Smart Contract: Ethereum

Smart contract is a digital contract that controls the digital assets of the user, formulates the rights and obligations of the participant, will be automatically executed by the computer system. It is not just a computer process, it can be seen as one of the contractparticipants, it will respond to receive messages and store data, and it can also send messages or valuesout.The smart contract is like a person that can be trusted, temporarily hold the asset and will follow the orderthat has already been programmed. Ethereum is an open source blockchain platform that combines smart contracts, offering a decentralized virtual machine to handle contracts, using its own digital currency called ETH, people can run many different services, applications or contracts on this platform.

Hyperledger

Hyperledger is an open source blockchain platform, focused on ledgers designed to support global business transactions, including major technology, financial and supply chain companies, with the goalof improving multiple aspects of performance and reliability. The project aims to bring together several independent efforts to develop open protocols and standards by providing a modular framework that supports different components for different uses. It will consist of different types of blockchains with their own consensus and storage models, and services for identity, access control, and contracts.

Other Applications

There are still many use cases for blockchain technologies, such as protection of intellectualproperty, traceability in supply chains, identity authentication, insurance, international payments, IOT, medical treatment or patient privacy in prediction markets.

Security Issues and Challenges

So far, blockchain has been paid a lot of attention in various fields, however, it also exists some problemsand challenges need to be addressed.

The Majority Attack (51% Attacks)

With Proof of Work, the probability of mining a blockdepends on what the miner does (e.g. CPU/GPU cycles spent checking hashes). If it holds 51% of thecomputing power, it will be able to take control of this blockchain. Obviously, this causes security issues. If someone has more than 51% computing power, he can find the nonce value faster than others, which means he has the right to decide which block isacceptable. What can it do?

- In the case of modified transaction data, adouble spending attack may occur.
- The block verifying transaction should bestopped.
- The goal is to stop the miner from mining anyavailable block.

A majority attack was more feasible in the past whenmost transactions were significantly higher than the block reward and when the network hash rate was verylow and prone to reorganization with the advent of new mining techniques.

Fork Problems

Another problem is the fork problem. The fork issue is related to the decentralized node version, compromised when software is upgraded. This is a very important issue as it covers a wide range of blockchains.

Types of Forks

When a new version of the blockchain software is published, the new agreement on the consensus rules is also changed in the nodes.

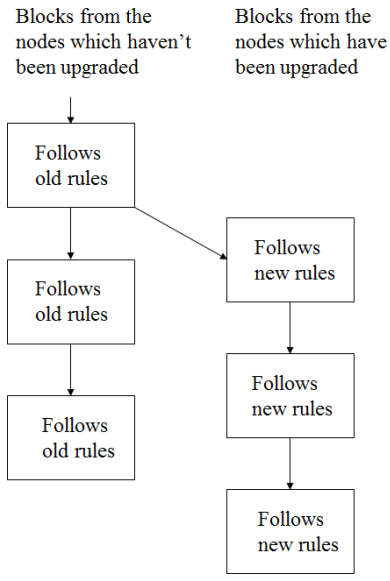

Figure No 5: Hard Fork

Therefore, nodes in the blockchain network can be divided into two types, new nodes and old nodes. so here comes the four situations.

3 New nodes agree to the transaction of theblock that is being sent by the old nodes.

4 New nodes do not agree to the transaction ofthe block that is sent by the old nodes.

5 Old nodes agree to the transaction of theblock that is sent by the new nodes.

6 The old nodes do not agree with the transaction of the block that is being sent bythe new nodes.

Due to these four different cases in achieving consensus, fork problems occur, and according tothese four cases, fork problems can be divided into two types, hard fork and soft fork. In addition to separating new nodes and old nodes,we have to compare the computing power of new nodes with old nodes, and assume that the computing power of new nodes is greater than 50

- **Hard Fork**

Hard fork means that when the system comes to anew version or new agreement, and it was not compatible with the previous version, the old nodes could not agree to the mining of the newnodes, so a series became two series. Althoughthe new nodes computing power was stronger than the old nodes, the old nodes would still continue to maintain the chain which though it was correct. Figure 5 shows the hard fork problem.

When there is a hard fork, we have to request allnodes in the network to upgrade the, agreement, nodes that have not been upgraded will not continue to work normally. If the moreold nodes were not upgraded, they would continue to work on other completely different series, meaning that the ordinary

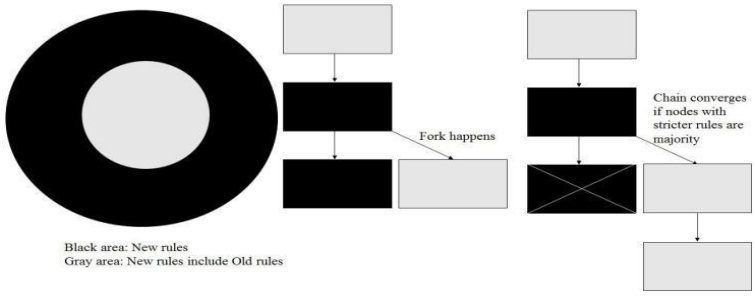

Figure No 6: Hard Fork happens because the old node verification requirement is much stricter than the new node

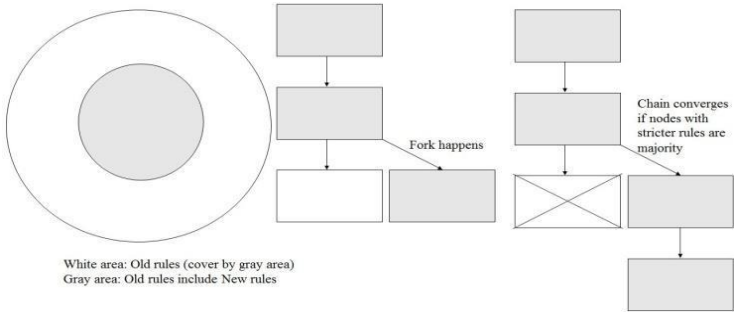

Figure No 8: Soft Fork happens because the new node verification requirement ismuch stricter than the old node

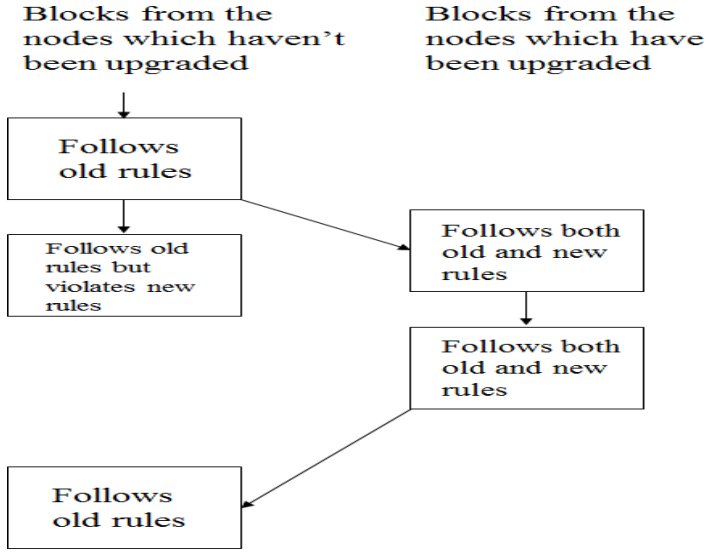

Figure No 7: Compatible hard fork

series would split into two series. Figure 6 shows the reason why there would be a hard fork.

Soft Fork

Soft fork means that when the system comes to a new version or new agreement, and it was not compatible with the previous version, the new nodes could not agree to the mining of the old nodes. Because the computing power of new nodes is stronger than that of old nodes, blocksmined by old nodes will never be approved by new nodes, but new nodes and older nodes willstill continue to operate on the same chain. Figure 7 shows the soft fork problem. When there is a soft fork, the nodes in the networkdo not need to upgrade to the new agreement at thesame time, it allows to upgrade gradually. Not likehard fork, soft fork will only have one chain, it willnot affect the stability and effectiveness of the system when nodes are upgraded. However, soft fork makes the old node unaware that the consensus rule has changed, contrary to the theory that everynode can verify somewhat correctly. Figure 8 showsthe reason why there would be a soft fork.

Scale of Blockchain

As the blockchain grows, the data becomes biggerand bigger, the loading of stores and computing will also become harder and harder, it takes a lot of time to synchronize the data, at the same time, the datastill grows, bringing a big problem to the customerwhen running the system

Simplified Payment Verification (SPV)

This is a payment verification technique, without maintaining complete blockchain information, onlythe block header message has to be used. This technology can greatly reduce user storage in blockchain payment verification, reducing user pressure if there is a huge increase in transactions inthe future.

Time Confirmation of Blockchain Data

Compared to traditional online credit cardtransactions, usually take 2 or 3 days to confirm thetransaction, only 1 hour has to be used to verify bitcoin transactions, it is much better than usual, but itis still not enough what we want. Lightning network is a solution to solve this problem. Lightning Network is a proposed implementation of hashed timelock contracts (HTLC) with bidirectional payment channels that allow payments to be safely routed across multiple peer-to-peer (P2P). payment channels. This allows the formation of a network where any coworker on the network can pay anothercoworker, even if they do not have a channel directlybetween each other.

Current Regulations Problems

For example, use the characteristics of a decentralizedsystem, will weaken the central bank's ability to control economic policy and the amount of money,which alerts the government to blockchain technologies, the authorities will have to research this new issue, accelerate the formulation of new policy,otherwise it will put the market at risk.

Integrated Cost Problem

Of course it will cost a lot, including time and money,to replace the existing system, especially when it is an infrastructure. We have to ensure that this innovative technology not only produces economic benefits, meets the requirements of supervision, but also bridges with the traditional organization, and it always faces difficulties from the internal organization that now exists.

Conclusions

There is no doubt that blockchain is a hot issue in recent years, although it has some topics that we need to pay attention to, with the development of new technology on the application side as well as some problems already improved, which is becoming more and more mature and stable.

The The government must make relevant laws for thistechnology, and the enterprise must be prepared to embrace blockchain technologies, preventing that it has too much impact on the current system.

While we enjoy the benefits of blockchain technologies, at the same time, we still have to be cautious on its impact and security issues that it mayhave.

References

A. Gervais, G. O. Karame, K. Wu¨st, V. Glykantzis, H. Ritzdorf, and S. Capkun, “On the security and performance of proof of work blockchains,” in Pro- ceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS’16), pp. 3–16, New York, NY, USA, 2016.

A. Gervais, G. O. Karame, V. Capkun, and S. Cap- kun, “Is bitcoin a decentralized currency?,” IEEE Security Privacy, vol. 12, pp. 54–60, May 2014.

A. Gervais, H. Ritzdorf, G. O. Karame, and S. Cap- kun, “Tampering with the delivery of blocks and transactions in bitcoin,” in Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Com- munications Security (CCS’15), pp. 692–705, New York, NY, USA, 2015.

A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Pa- pamanthou, “Hawk: The blockchain model of cryp- tography and privacy- preserving smart contracts,” in 2016 IEEE Symposium on Security and Privacy

(SP'16), pp. 839–858, May 2016.

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

G. Karame, "On the security and scalability of bit- coin's blockchain," in Proceedings of ACM SIGSAC Conference on Computer and Communications Secu- rity (CCS'16), pp. 1861– 1862, New York, NY, USA, 2016.

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

H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain ap- plied to smart contracts," in IEEE International Conference on Consumer Electronics (ICCE'16), pp. 467– 468, Jan. 2016.

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

I. Bentov, A. Gabizon, and A. Mizrahi, "Cryp- tocurrencies without proof of work," CoRR, vol. abs/1406.5694, 2014.

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

J. Garay, A. Kiayias, and N. Leonardos, The Bit- coin Backbone Protocol: Analysis and Applications, pp. 281–310, Springer Berlin Heidelberg, Berlin, Hei- delberg, 2015.

J. Singh, "Cyber-attacks in cloud computing: A case study," International Journal of Electronics and In- formation Engineering, vol. 1, no. 2, pp. 78–87, 2014.

L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding proto- col for open blockchains," in Proceedings of ACM SIGSAC Conference on Computer and Communica- tions Security (CCS'16), pp. 17– 30, New York, NY, USA, 2016.

M. Rosenfeld, "Analysis of hashrate-based double spending," CoRR, vol. abs/1402.2009, 2014.

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

S. King and S. Nadal, Ppcoin: Peer-to-peer Crypto-Currency with Proof-of-Stake, 2012. (https://archive.org/stream/PPCoinPaper/ ppcoin-paper_djvu.txt)

S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Feb. 24, 2013. (http://bitcoin.org/ bitcoin.pdf) security, exploits, and vulnerabilities," International Journal of Electronics and Information Engineering, vol. 3, no. 1, pp. 10–18,2015.

W. T. Tsai, R. Blower, Y. Zhu, and L. Yu, "A system view of financial blockchains," in IEEE Symposium on Service-Oriented System Engineering (SOSE'16), pp. 450–457, Mar. 2016.

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