RESEARCH REVIEW JOURNALS
Volume-03
Issue-09
September-2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

A Review of Security Issues and Challenges of Blockchain

[1]Dr Anupam Bhatia & [2]Divya Jindal

[1]*Assistant Professor, CRS University, Jind, Haryana (India)*
[2]*M.Tech Scholar, CRS University, Jind, Haryana (India)*

ARTICLE DETAILS

Article History
Published Online: 07 September 2018

Keywords
Blockchain, Security, PoW, PoS

ABSTRACT

In this era of technology, use of Blockchain is increasing day by day and it has already changed the people's lifestyle due to its great influence on many areas of business. Although Blockchain features bring us more reliable and convenient services but still there are several threats to this technology. This paper will contented about what is blockchain, its security challenges and issues that we need to overcome.

1. Introduction

Till now we are using the centralized form of transactions between persons or companies and for making this digital payment, we need third party or we can say bank to complete the transaction and this transaction also leads to the fee from a bank or any other party.

For a system to be distributed it must have characteristics like consistency, availability and partition tolerance but blockchain based system only possess availability and partition tolerance.

The blockchain technology is composed of following key elements:-

- Decentralized: - The main feature of blockchain is its decentralized form. We can record, store and update data distributedly
- Transparent: - Blockchain is a trusted technology as there is transparency in data records and also during updating the data.
- Open source: - Blockchain is open to everyone as records can be checked publicly by people and they can create applications that they want.
- Autonomy: - As blockchain is consensus based so, data can be updated or transferred easily by every node.
- Trustless: - There is no need of third party to validate the transactions. Blockchain enables trust free transactions.
- Cryptographic:-In blockchain technology, transactions are encrypted using public- private key.

Blockchain is considered as a log because of batching of records into timestamped blocks and identification of each block is identified by cryptography hash.Every previous block is referenced by each block and this creates a link between the blocks and a chain is created which is called as blockchain.

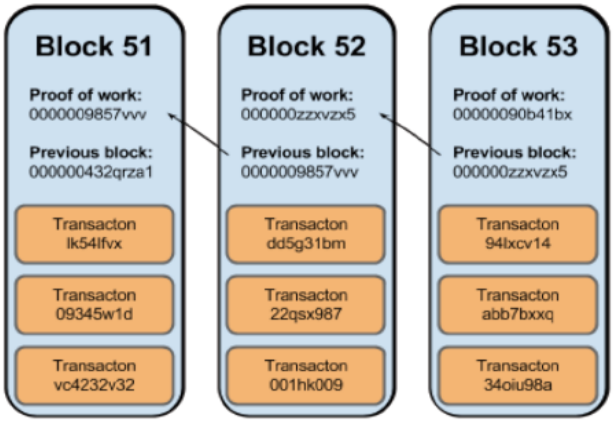

Figure 1 Example of Blockchain [2]

How it works:

- The nodes form a peer to peer network in which user interacts with blockchain via public/private keys.
- To sign into own transactions, users use their own private key and public key for addressing in network.
- Before further processing, the transaction is checked whether it is valid or invalid. Invalid transactions are discarded.
- All transactions validated by the network are ordered and packaged into a timestamped candidate block and this process is called as mining and it is confirmed by Proof-of-work.[3]
- After confirmation of all the transactions, a consensus exists between all the nodes.
- The new blocks are linked to previous blocks and aligned in continuous chain and this chain is called as public ledger.

The Structure of Blockchain

A block contains main data, hash of previous block, hash of current block, timestamp and other information.

Main Data- Main data depends upon service on which blockchain applicates.

Hash- After the execution of transaction, a code is used to generate the final hash value.

Timestamp- Time of block generated[1]
Other Information: - Like signature of the block, or other data that user define. [1]

How to get Consensus?

It is a mechanism in which all the nodes of blockchain agree on same message and current block have been added to the chain and also helps to protect from malicious attacks.

Proof of work (PoW)

ThePoW is the widest arranged consensus mechanism in the current blockchains. It was first introduced by Bitcoin and when we calculate the PoW, it is called Mining. Each block has a random value called 'nonce' in block header and by changing the nonce value;PoW has to generate a value smaller than the current target value which has already been set up. When such nonce is found, theminer creates the block and forwards it on network layer to its peers.

Miners must complete PoW so that blocks can accept the network participants.

Proof of stake (PoS)

There is lot of wastage of electric power and computing power while using PoW but proof of stake

consume less computing power.

Proof of stake is much secure than proof of work as executing attacks in proof of stake is much more expensive and the attacker might suffer from his own attack.

Blockchain Taxonomy

There are several ways in which we can categorize the blockchain network. The following ways are:-

a) Based on the access to the network:-

- Permissioned and Permissionless:
  Permissioned Blockchain network allows the network to appoint a group of network who are given the express authority to provide the validation of blocks of transactions or to participate in consensus mechanism.

  But in permissionless, we don't have to prove identity to the ledger.

b) Based on Transaction or Mining:-

- Public and Private:
  In public networks, all the participants may not be allowed to transact or mine but in private networks all the participants are identifiable.

  Based on Bitcoin Style Transactions or Smart Contract :-
  Bitcoin style transaction support the UTXo model and there is unique way for transfer and tracking of digital tokenized assets in blockchain which support UTXo model and account-based model helps to run arbitrary logic and establish verifiable multi-step processes.

2. Security Issues

Security is one of the major research aspects in the field of blockchain. Most of research was related to challenges and limitations in the blockchain security.

Some of the major attacks on blockchain are:-

51% attack:

This is one of the major threats that target the mining process. In this, more than 50% of computational power during mining process can be acquired by a user or a group of user and transactions can be altered, modified and self- reversed by the user or group and valid blocks are prevented to participate in mining process. Other attacks can also be implemented by attacker if this attack got executed. "Although this attack has not occurred since January, 2009 but the risk does exist, especially in the blockchain with small networks."[4]

Time Jacking Attacks:

This attack leads to creation of invalid timestamp during linking of transactions and it may happen that different blockchain can be accepted by deceived node.

Double Spending:

This attack leads to creation of multiple transactions using same coin by the hacker.

Although blockchain does not allow multiple transactions with same input but it may lead to not confirming of transactions of original receiver.

Selfish Mining:

Selfish attack means to get more and more power on network by making fool of genuine miners.
They are forced to take participation in such mining power which is stale and as a result they are going to waste their computational power and selfish mining group would be able to keep their mined blocks private.

Security Issues:

Although blockchain can prevent some attacks but there are some issues of security in blockchain. The issues are:-

Identity Theft:

The main issue in security can be to protect the digital identity of user i.e. its private key. Once it would be stolen by attacker, it can't be recovered by third party. So, it will lead to loss of identity of the person's assets owned by him/her and it would get difficult to identify the thief.

Illegal Activities:

Dishonest movement of funds can lead to become a place of illegality for blockchain technology and can create a channel for these activities.

System Hacking:

Although it is difficult for a hacker to alter the records but by altering the system and codes of programming, hacker can be able to implement its own technology MtGox, once the largest Tokyo-based Bitcoin exchange, was hacked in March 2014, and bitcoins worth $700 million were stolen. Poorly-maintained and outdated codes allowed criminals to double-spend. [4]

3. Challenges of blockchain

Data Flooding

One of the challenges in the blockchain is to control the data flooding. As per the growing of blockchain technology, data is also increasing day by day and it's getting difficult to synchronize the data in the same time as before and client is suffering from problem while running the system and is to protect the personal data and developing the system in which user can own and control their data.

Quick Transaction

Another Challenge with the blockchain system is the conformation of transaction in less time. As 2-3 days are taken by online credit card usually to confirm the transactions, so we need such network which can provide us as network to confirm transactions in less time.

Security

The main challenge in blockchain system is to maintain the security of these systems. Security has been the main and most important area of research from the last few years. There are so many attacks that can be occurred on the blockchain like 51% attack, DDos attacks, time jacking attacks, double mining attack etc. and there so many security issues on which research may be done.

Privacy

Another main challenge in blockchain system is to maintain privacy. It is a complicated issue. As we know a public key is issued to each participating device in blockchain and this is not mandatory for them to know everybody else's key, they just need to know the key of that transaction to which they are going to communicate but patterns can be identified easily and one can track the addresses between the transactions and hence lead to loss of privacy of devices.

Scalability

Scalability is one of the main challenges in the field of blockchain system. It depends on the number of factors like latency, maximum throughput, cost per confirmed transaction and bootstrap time. As blockchain is a decentralized system which means there is no third party responsible for securing and managing the data and blockchain is growing so rapidly but its applications take 10 minutes to 14 minutes to transact the block so there is urgent need to find out the solution for better scalability because as the blockchain grows, the demand of better scalability also requires efficient storage, bandwidth and computational power.

Irreversibility

In intermediary networks, we can easily overcome the human and software errors by consulting the intermediates but it is infinitely more complicated in case of blockchain. We can only reverse any of the transactions by arranging 51% of processing power of network once a block is confirmed and new blocks are attached to it and thus it would lead to replicate the irreversibility of cash transactions.

Wasted Resources

To decrease the wasted resources with efficient mining is quite a difficult challenge to handle. Computational power also increases as the miners increase in the system and a steady creation speed is required to overcome this issue and hence results in reducing the mining rate.

Cost

It can be one of the main challenges of blockchain systems because people could never be agree to pay for a system which is not hidden. They would rather go for the centralized system where prices are more hidden.

Storage

Storage can be one of the main hurdles while developing applications under blockchain system. As because of Decentralized nature of blockchain, every node of the network must have to store more and more data and it would lead to huge cost to the system.

Lack of governance and standards

Another main challenge faced by blockchain is that there is lack of government laws and standards. Although blockchain offers us trustless, open and permissionless system but still there is need of an authority that could be responsible for maintaining standards and any other issue faced by the users. There is need to apply some regulations and law for using blockchain technology to secure the users privacy and data.

4. Literature Review

Several researches have been come in existence. Here in this section the existing relevant research have been discussed.

As per JohnPlansky, Tim O'Donnell, and Kimberly Richards [6], when Blockchain is used as a distributed ledger along with Bitcoin, it provides greater access to financial services and provides flexible reserves management.

As per Jeff Herbert, Alan Litchfield[2],the issue of protecting software copyright to minimize software piracy using Cryptocurrency blockchain technology can be solved by two methods i.e. Master Bitcoin Model and Bespoke Model. Both methods define their usability to make software more Protected and validated.

As per Arthur Gervais , Ghassan O. Karame , Karl Wust , VasilieiosGlykantzis , Hubert Ritzdorf , srdjanCapkun[5], Bitcoin's Blockchain offers more security than Etherum's Blockchain and existing Pow blockchains can achieve a throughput of 60 transactions per second without effecting blockchain security.

As per Chinmay A. Vyas and MunindraLunagaria, Bitcoin is one of the main Cryptocurrency emerged in the world but it lacks the security as respect to users.

As per Jennifer J. Xu[4] blockchain can prevent Double Spending attack and record hacking but still some attacks cause risk to the blockchain such as 51% attack, account takeover, digital identity theft, money laundering, and hacking and Future work can be made on solutions of the various attacks that cause risk to the blockchain technology and can help in improving the efficiency of Blockchain.

As per Vincent Gramoli [7],blockchain systems which make use of proof-of-work may be ill-suited for private chains if applications require the consensus to terminate and a theory of blockchain is to be precisely characterized that what type of their consensus algorithms offer and under what assumptions.

As per Marcella Atzori [8], blockchain is a disruptive technology and can prove itself in every field.

As perSunny King [9] , the Proof of stake designs are potentially more competitive form of peer to peer crypto-currency to proof-of-work designs due to the elimination of dependency on energy consumption and achieving lower inflation and lower transaction fees at similar network security levels.

As per Michele Ruta, FlorianoScioscia, SaverioIeva, Giovanna Capurso, Eugenio Di Sciascio [10], the logic-based clarification of discovery outcomes can be obtained through non-standard conclusion for matchmaking among request and resources.

As per Evan Duffield, HolgerSchinzel,Fernando Gutierrez [11] , theFast validation of payments via transaction locking and Master node consensus could be used to avoid having to wait for confirmation via a new block and reach speeds nearly as fast as credit cards and in most of cases a transaction should be validated by the network within a few seconds.

By using the Master node network as an authority and picking Master nodes via a deterministic algorithm powered based on the proof of work, we achieve a system that gives us comparable transaction time to a credit card transactions and transactions also being tamper resistant, backwards compatible and secure.

As per Deepak K. Tosh, SachinShetty, Xueping Liang, Charles A. Kamhoua, Kevin A. Kwiat, Laurent Njilla [12],pay per last *N* shares (PPLNS) scheme could be useful in keeping the attacker's impact lesser than proportional reward scheme

As per Maria Borge, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, and Bryan [13], there is a new Cryptocurrency PoPCoin, whose consensus mechanism influences PoP to eliminate the disadvantages of PoW and PoS and also ensure security.

Pop Coin leads to a continuously fair and democratic wealth creation process.

As per, JuhoLindman,MattiRossi,VirpiKristiinaTuunainen [14], Future work can be made on new application areas for blockchain technology, design decisions made in different systems relying on blockchain technology, features which can enhance and/or decrease the trust of users towards the economic or regulatory systems that they implement.

As per RajithaYasaweerasinghelage [15], Mark Staples, and Ingo Weber ,an approach was made to evaluate for predicting the latency of blockchain-based systems using architectural performance modeling and simulation which would provide a basis for future research into optimal system configuration, cost, and other non-functional properties.

5. Conclusion

We know that blockchain has been a current issue in recent years. There are many topics related to blockchain which we need to notice, although some problems has already been upgraded along with new technique's and getting more mature and established but still government have to make suitable laws for this technology.

Although Blockchain is a robust, distributed, peer to peer system with many advantages of blockchain technologies but still we must be aware about its security issues and attacks.

References

1. Lin, I. Chang, and T. C. Liao. "A Survey of Blockchain Security Issues and Challenges" IJ Network Security 19, no. 5 (2017): 653-659.
2. J. Herbert and A. Litchfield. "A Novel Method for Decentralized Peer-to-Peer Software License Validation Using Cryptocurrency Blockchain Technology." In Proceedings of the 38th Australasian Computer Science Conference (ACSC 2015), vol. 27, p. 30. 2015.
3. K.ChristidisandM.Devetsikiotis. "Blockchains and Smart Contracts for the Internet of Things." IEEE Access 4 (2016): 2292-2303.
4. J.J.,Xu, "Are Blockchains Immune to All Malicious Attacks?." Financial Innovation 2, no. 1 (2016)
5. Gervis, G.O. Karame, K.Wust,V.Glykantzis, H. Ritzdorf, and S. Capkun,"On the Security and Performance of Proof of Work Blockchains," Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security-CCS16, 2016
6. J. Plansky, T. O'Donnell, and K. Richards on "A Strategist's Guide to Blockchain".2016
7. V. Gramoli, "On the Danger of Private Blockchains." In Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL'16). 2016.
8. M. Atzori, "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?." (2015).
9. S. King,"Ppcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake." self-published paper, August 19 (2012).
10. M. Ruta,F.Scioscia, S.Ieva, G.Capurso, and E.D.Sciascio "Semantic Blockchain to Improve Scalability in the Internet of

Things." Open Journal of Internet Of Things (OJIOT) 3, no. 1 (2017): 46-61.

11. E. Duffield, H. Schinzel, and F.Gutierrez. "Transaction Locking and Master node Consensus: A Mechanism for Mitigating Double Spending Attacks." (2014).
12. D.K.Tosh, S.Shetty, X.Liang, C.A. Kamhoua, K.A.Kwiat and L.Njilla. "Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack." In Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 458-467. IEEE Press, 2017.
13. M. Borge, E. K. Kogias, P. Jovanovic, L. Gasser, N. Gailly, and B.Ford. "Proof-of-Personhood:Redemocratizing Permissionless Cryptocurrencies." In Security and Privacy Workshops (EuroS&PW),2017 IEEE European Symposium on, pp. 23-26. IEEE, 2017.
14. J. Lindman, V. K.Tuunainen, and M. Rossi. "Opportunities and Risks of Blockchain Technologies–a Research Agenda." (2017).
15. R. Yasaweerasinghelage, M. Staples, and I. Weber. "Predicting Latency of Blockchain-based Systems Using Architectural Modelling and simulation." In Software Architecture (ICSA), 2017 IEEE International Conference on, pp. 253-256. IEEE, 2017.

