TEST Engineering & Management

Jan-Feb 2020
ISSN: 0193-4120 Page No. 17618 - 17625

Security Issues and Challenges in Blockchain Technology: A Review

Mr. Gajanan Badhe, Dr. Maithili Arjunwadkar
Progressive Education Society's Modern Institute of Computer Application, Pune, India.
Email: badhe.gm@gmail.com, maithili.arjunwadkar@gmail.com

Abstract

Along with increasing utilization of Internet enabled devices such as mobile phones, web based applications gaining more and more access in the modern digital life, therefore ensuring security and privacy, especially for the financial and e-commerce applications becoming critical day by day. Blockchain technology is one of such technologies, which is emerged on the basis of internet technology. The growth of various cryptocurrencies is the example of the rapid development of Blockchain technology recent years. Blockchains are immutable and distributed digital ledger systems without a central authority, storing the cryptographically signed transactions in the form of blocks and these blocks are connected to each other forms a Blockchain. This paper focuses on the security issues of Blockchain technology applications and presents the review of various security issues, security incidents and challenges discussed in to date research papers, white papers and technology articles.

Keywords- *Blockchain Technology, Cryptocurrency, Distributed Ledger, Security Issues and challenges.*

I. INTRODUCTION-

Blockchains are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify. New blocks are replicated across all copies of the ledger within the network, and any conflicts are resolved automatically using established rules.

There are mainly two types of block chain: Public Blockchain and Private Blockchain. Public Blockchains use computers connected to the public internet to validate transactions and bundle them into blocks to add to the ledger. Any computer connected to the internet can join the party. Private Blockchains, on the other hand, typically only permit known organizations to join. Together, they form private, members-only "business network." This difference has significant implications in terms of where the (potentially confidential) information moving through the

Jan-Feb 2020
ISSN: 0193-4120 Page No. 17618 - 17625

network is stored and who has access to it. Bitcoin is probably the most well-known example of a public blockchain and it achieves consensus through "mining." In Bitcoin mining, computers on the network (or 'miners') try to solve a complex cryptographic problem to create a proof of work.[8].

In the Blockchain network, the ledgers are public to the community of users in essence; each block has the cryptographically linked connection with its previous block after validation. The block chains are constantly growing, according to the transactions and, thereby, being appended the new blocks. Each block contains a hash value regarding the content of the previous block in the Blockchain network.[2] The Blockchain technology has successfully enabled e-commerce systems such as Ethereum, Bitcoin, Litecoin, and Ripple etc.

The Blockchain technology has been broadly used for a variety of applications. Three different types of Blockchains are available based on the availability of the data, managed data, and actions, including public-permissionless Blockchain, the public-permissioned Blockchain, and private blockchain. Blockchain technology has widely used in different emerging fields such as the Internet of Things (IoT), education, finance and auditing etc.[5] The Blockchain is an encrypted, distributed database that records data, or in other words it is a digital ledger of any transactions, contracts - that needs to be independently recorded. One of the key features of Blockchain is that this digital ledger is accessible across several hundreds and thousands of computers and is not bound to be kept in a single place.

Distributed ledger technologies or Block chains are immutable digital ledger systems implemented in a distributed fashion (i.e. without a central repository) and usually without a central authority. This technology became widely known in the beginning of 2008 when it was applied to enable the emergence of electronic currencies where digital transfers of money take place in distributed systems. Various digital currency systems such as Bitcoin, Ethereum, Ripple, and Litecoin are only an example of this technology. This technology is broadly useful and can be used for variety of applications. Due to this inherent nature and architecture of Blockchains it provides the inbuilt security mechanism upto certain extent. But after commercialization of cryptocurrencies like Bitcon, Bitcoin Gold, Litecoin, Etherium Blockchains etc. are available in the market, are prone to attack because of its valuation in international market corresponds to other currencies and attackers try to gain more and more hashing power for solving puzzles and validating the block.

Jan-Feb 2020
ISSN: 0193-4120 Page No. 17618 - 17625

Blockchain technology is a solution for the problem of centralization. It's a system for keeping records by everybody, without any need for a central authority – a decentralized way of maintaining a ledger that is practically impossible to falsify. Blockchain technology enables the creation of a decentralized environment, where the cryptographically validated transactions and data are not under the control of any third party organization. Any transaction ever completed is recorded in an immutable ledger in a verifiable, secure, transparent and permanent way, with a timestamp and other details.

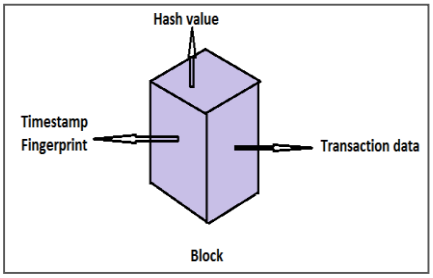

Figure 1. Components of 'Block'

The Blockchain term, originally block chain, was first coined in 2008, by (the still unknown) Satoshi Nakamoto, in the original source code for the virtual currency Bitcoin: "Nodes collect new transactions into a block (Figure 1), hash them into a hash tree"; "when they solve the proof-of-work, they broadcast the block to everyone and the block is added to the block chain".[1]

II. WORKING MECHANISM OF BLOCKCHAINS:

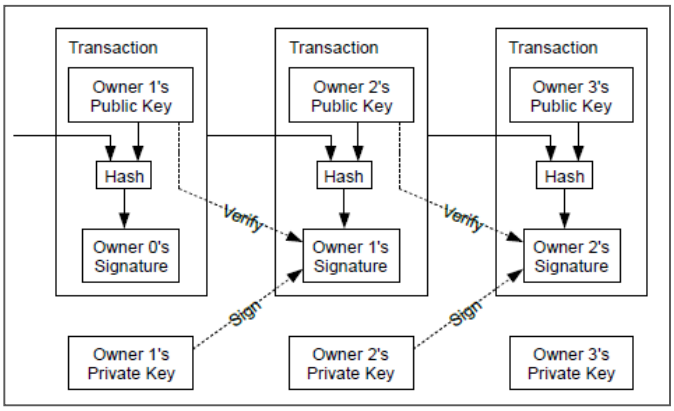

Figure 2. Concept of Blockchain

Blockchain are maintained through the consensus of set of computers (mining nodes) running Blockchain software. There is no central authority determining which node publishes the next block on the Blockchain (Figure 2). Each node maintains a copy of the blockchain and may propose a new block to the other mining nodes. Any node may propose new transactions, and

Jan-Feb 2020
ISSN: 0193-4120 Page No. 17618 - 17625

these proposed transactions are propagated between nodes until they are eventually added to a block. When mining nodes put together a new candidate block, they include a set of unspent transactions. They may take a combination of older transactions that have been waiting for some time and newer transactions that offer a higher payment (in the form of a transaction fee paid by the user who submitted the transaction). The mining node checks that each transaction is itself valid since the other nodes would reject the block if it included invalid transactions.[8]

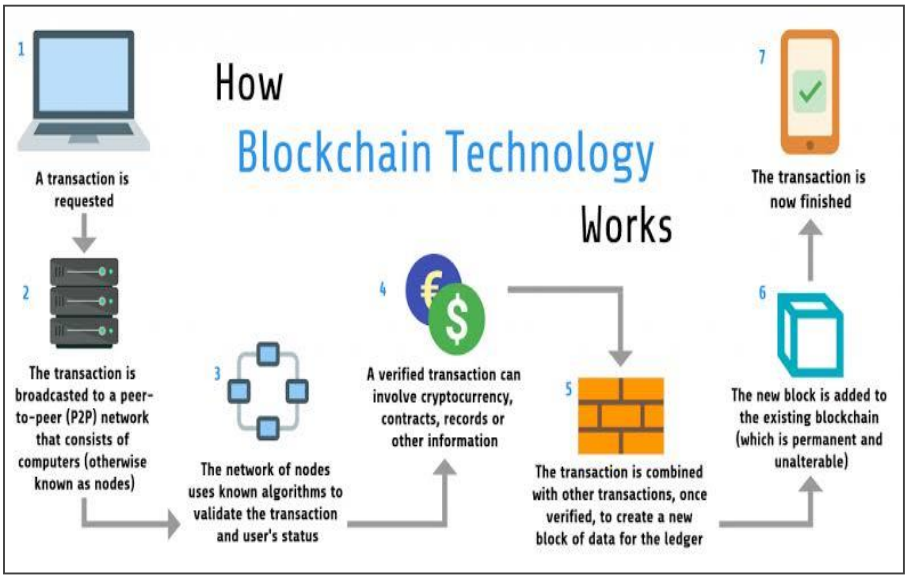

Figure 3. Working of Blockchain

III. ADVANTAGES OF BLOCKCHAIN TECHNOLOGY:

1. Improves the effectiveness with reduction in transaction time.
2. Reduces overheads and intermediary costs as it is direct transactions.
3. Highly secure due to use of cryptographic and decentralized Blockchain protocols.
4. Minimized the chances of cybercrimes, frauds and tampering of records.
5. Highly transparent processes with a proper record creation and tracking.

IV. DISADVANTAGES OF BLOCKCHAIN TECHNOLOGY:

1. Blockchains uses excessive energy.
2. Mining does not provide network security.
3. Scalability issues increases over the increase in number transactions

V. SECURITY ISSUES AND CHALLENGES WITH BLOCKCHAIN TECHNOLOGY:

Jan-Feb 2020
ISSN: 0193-4120 Page No. 17618 - 17625

Blockchain technology has lot of attention in various fileds, however, also there exists some problems and challenges needs to face it, following are the issues.

Scale of Blockchain-

As Blockchain growing, data becomes bigger and bigger, the loading of store and computing will also getting harder and harder, it takes plenty of time to synchronize data, in the same time, data still continually increase, brings a big problem to client when running the system [14].

Fork Problems-

Another issue is fork problem. Fork problem is related to decentralized node version, agreement when the software upgrade. It is a very important issue because it involving a wide range in Blockchain. There are two types of forks Hard Fork and Soft Fork.

Hard Fork means when system comes to a new version or new agreement, and it didn't compatible with previous version, the old nodes couldn't agree with the mining of new nodes, so one chain became two chains. Although new nodes computing power were stronger than old nodes, old nodes will still continue to maintain the chain which it though was right.

Soft Fork means when system comes to a new version or new agreement, and it didn't compatible with previous version, the new nodes couldn't agree with the mining of old nodes. Because the computing power of new nodes are stronger than old nodes, the block which is mining by the old nodes will never be approve by the new nodes, but new nodes and old nodes will still continue to work on the same chain.[13]

Majority attack or Double Spend attack or 51% attack –

The attack is defined as the ability of someone controlling a majority of network hash rate to revise transaction history and prevent new transactions from confirming. In this attack a miner or a group of miners trying to control more than 50% of a network's mining power, computing power or hash rate. People in control of such mining power can block new transactions from taking place or being confirmed.[

Actual incidents of attacks on Blockchain applications:

Here, we present the some existing real-world security incidents that have affected adversely to Bitcoin Blockchains and its related technologies.

Jan-Feb 2020
ISSN: 0193-4120 Page No. 17618 - 17625

1. Bitcoin gold (January 2020) – 51 % attack on Bitcoin gold creates two deep Blockchain reorganizations resulted in double spends of 1,900 BTG and 5,267 BTG, respectively. The losses amount to around $87,500 at current prices.
2. Vertcoin (December 2018) 4 different attacks on the Vertcoin network concluded in the theft of around $100,000.
3. Bitcoin Gold (May 2018) More than $18 million were stolen through double spending in a Bitcoin Gold 51% attack conducted by an unknown malicious actor.
4. In August 2016, BitFinex, which a popular cryptocurrency exchange suffered a hack due to their wallet vulnerability, and as a result around 120000 bitcoins were stolen.[8]
5. Bitcoin (January 2014) – potential threat averted In January of 2014, a mining pool called Gash.io got so big that it neared 51% of the total mining power. This, of course, created some panic in the Bitcoin community but was fixed shortly after by miners who left the pool in order to balance things out. Additionally, the pool committed to a 40% limit for its future operations.
6. In 2013, the world's largest online anonymous market famous for its wide collection of illicit drugs and its use of Tor and Bitcoin to protect its user's privacy, reports that it is currently being subjected to what may be the most powerful distributed denial-of-service attack against the site to date. This attack is called Silk Road attack. [8]
7. Feathercoin (June 2013) 16,000 coins were double spent in an attack on a Litecoin clone known as Feathercoin. Back in the day, this coin ranked relatively high in the cryptocurrency charts.
8. One of the biggest attacks in the history of Bitcoin have targeted Mt. Gox, the largest Bitcoin exchange, in which a year's long hacking effort to get into Mt. Gox culminated in the loss of 744,408 bitcoins. However, the legitimacy of attack was not completely confirmed, but it was enough to make Mt. Gox to shut down and the value of bitcoins to slide to a three-month low.[8]

VI. Importance of Blockchain Security -

It is important to take a Blockchain security seriously, because the survival of any business depends on it. One security breach and a particular business organisation could lose the trust of your customers forever. A small mistake and the funds in company's crypto wallet are instantly cleaned out. This may possible because of the security issues and problems associated with the Blockchain technology presently. There are some

Jan-Feb 2020
ISSN: 0193-4120 Page No. 17618 - 17625

solutions to each of these problems are available for protecting the Blockchain, but it has limitations and only up to certain extent these can work to provide. Therefore Blockchain security related further research invites the researchers and technology persons for providing solutions to such problems.

VII. CHALLENGES IN BLOCKCHAIN TECHNOLOGY -

Initial cost and integrations with existing system- Replacement of existing system with the Blockchain technology need high initial cost as we need to change the whole from centralized to distributed trusted model of Blockchain technology.

Identity security and privacy- Anonymity and security vary across application and ecosystem. Smart contract application may require contracts and transaction linked to known identities. Cryptocurrencies are tied to wallet rather than individuals.

Cultural Adaption issue – The Blockchain is a disruptive technology as it can replaces the existing technologies. Moving from centralized authority to a distributed system as the adoption of Blockchain technology impact on business process, organisation structure and governance therefore it creates some resistance from users of the system.

Uncertain regulatory and compliance status – Biggest concern for Bitcoin, need to work with existing regulatory framework, breach and accountability, compliance moves from reporting to consensus model.

Standardization – There are many solutions are available in Blockchain technology but which is applicable for standardization is difficult to decide. A common approach required for use case, block data format and structure, security and privacy of datasets, consensus algorithm, governance of smart contracts, regulatory and compliance.

VIII. CONCLUSION

Blockchain technology applications are already used in the financial and e-commerce sector such as cryptocurrencies like Bitcoin, Litecoin, Zcash etc.; also it has potential to impact on several other sectors wherever there is some transaction between two or more parties keeping records with security. In this paper we present a review of securities and challenges with Blockchain technology applications. Presently the cryptocurrencies with Blockchain technology gaining the market attention but along with that it attracts different types of security issues and challenges such as major or 51 % attack, minor or 34% attack on Blockchain

Jan-Feb 2020
ISSN: 0193-4120 Page No. 17618 - 17625

network, issue of legal support to cryptocurrencies in most of the countries in the world, non availability of government policy regarding adoption of cryptocurrencies, not availability of legal laws pertaining to Blockchain cryptocurrencies.

REFERENCES

[1] Satoshi Nakamoto (2008), Bitcoin: A Peer-to-Peer Electronic Cash System, satoshin@gmx.com, www.bitcoin.org

[2] Carter, Lemuria & Ubacht, Jolien. (2018). Blockchain applications in government. 1-2. 10.1145/3209281.3209329.

[3] R. Beck et al.: Blockchain Technology in Business and Information Systems Research, Bus Inf Syst Eng 59(6):381–384 (2017)

[4] Carmen Holotescu (2018), Understanding Blockchain Opportunities and Challenges, The 14th International Scientific Conference eLearning and Software for Education Bucharest, April 19-20, 2018

[5] Thais (2019), Blockchain in Education – Possible Applications of this Technology, Technologies & Tools on April 2, 2019

[6] https://99bitcoins.com/what-is-blockchain/

[7] Jin Ho Park 1 and Jong Hyuk Park (2017), Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions.

[8] A Study paper on 'Security aspects of Blockchain', Telecommunication Engineering Centre, Government of India.

[9] Raj Kumar (2017), 'Security Aspects of Blockchain Technology', https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/CybersecurityASPCOE/cybersecurity/5.%20Security%20Aspects%20of%20Blockchain.pdf

[10] https://www.zaptox.com/tag/working-of-blockchain-technology/

[11] P.J. Taylor et al., A systematic literature review of blockchain cyber security, Digital Communications and Networks, https://doi.org/10.1016/j.dcan.2019.01.005

[12] Archana Prashanth Joshi, Meng Han_ and Yan Wang (2018), A survey on security and privacy issues of blockchain technology, Mathematical Foundations of Computing @American Institute of Mathematical Sciences, Volume 1, Number 2, May 2018

[13] Iuon-Chang Lin and Tzu-Chun Liao (2017), A Survey of Blockchain Security Issues and Challenges, International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017 (DOI: 10.6633/IJNS.201709.19(5).01)

[14] G. Karame, \On the security and scalability of bitcoin's blockchain," in Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS'16), pp. 1861{1862, New York, NY, USA, 2016.
