A STUDY ON THREATS AND VULNERABILITIES OF BLOCKCHAIN TECHNOLOGY

Parul Mehra[1], Bhavna Galhotra[2*], Devesh Lowe[3]

Abstract:
Since its inception, Blockchain technology has revolutionized the way transactions work. It provides a safe and secure mode of transaction, which involves digital currencies which cannot be manipulated by anyone with malicious motives. It maintains all information of transaction in forms of blocks which store information. Blockchain technology is an embodiment of decentralized organized collection of data. It offers a public ledger system which combines a public key encryption for all transaction to resolve the double spending problem by storing block over a distributed network setup at multiple locations making it impossible to change and hence more secure. This paper expounds the core principles of Blockchain technology and its implementation in various domain areas to study the applicability and advantages it offers over conventional data management. Authors also observe the reasons for shift towards a decentralized crypto-ledge platform and rise of Bitcoin and other cryptocurrencies. Paper also discusses a detailed perspective of potential risks and drawbacks of this technology along with its security features, threats, and vulnerable areas.

Keyterms: Block Chain, Bit coin, Crypto currencies, Security constraints

[1]Student, Information Technology Department, Jagan Institute of Management Studies Sector 5 Rohini, Delhi, India.
[2*]Assistant Professor, IT Department, Jagan Institute of Management Studies Sector 5 Rohini, Delhi, India.
[3]Assistant Professor, IT Department, Jagan Institute of Management Studies Sector 5 Rohini, Delhi, India.

***Corresponding Author:** Bhavna Galhotra
*Assistant Professor, IT Department, Jagan Institute of Management Studies Sector 5 Rohini, Delhi, India.

DOI: - 10.31838/ecb/2023.12.si5.047

I.INTRODUCTION

Blockchain technology was initially introduced by Satoshi Nakamoto [1]. Blockchain technology is an embodiment of decentralized organized collated data. Bitcoin, blockchain has been known to be the public ledger for all transactions and resolved the double-spend problem by combining peer-to-peer technology with public-key cryptography [2] just like we saw the advancement of blockchain technology in the current times, it too started with people being apprehensive about something that they don't understand. As each block is connected to the others via a peer-to-peer connection. The Blockchain is a technology and a method that allows community users to validate, keep and synchronize the content of a transaction ledger which is replicated across multiple users. [3]

The blockchain, on an initial level, works on network security which assures users of the privacy of their data. Here public ledger is a decentralized, parallelly maintained ledger or a document that lists down all the transactions along with transaction details, which is shared amongst the participants by a methodology of public key cryptography whose changes are replicated amongst all the users.

Public key encryption is in which message data is encrypted with a recipient's public key. The Message can't be unscrambled by any individual who does not have the coordinating private key, who is dared to be the proprietor of that key, and the individual related to the general population key. [4] There are two types of keys, the public key, and the private key, just as the name suggests the private key is private to the participant of the blockchain and the public key is the key that is required to facilitate the private key.

II. BLOCKCHAIN AND CRYPTO-CURRENCY

Cryptocurrency is the booming technological sector, but the transition from carrying out transactions based purely on instinct to trusting the stock market and especially the currency that is not tangible was not very easy. When blockchain with cryptocurrency was introduced, naturally people and countries were apprehensive due to its complexity and functions which led to being a restricting factor in its growth, but the thing that gained attention was the underlying technology, which worked as an online ledger to store records, data, and information about that data in a ledger format and which is stored in form of blocks which are linked to each other. This format and arrangement of transaction records and details related to data increased the transparency of the data, which is a boon in disguise. If transparency is more then it gradually leaves a deliberate opening for anyone who wants to tamper with the data. [5]

Blockchain has been known to be the public ledger for all transactions and resolved the double-spend problem by combining peer-to-peer technology with public-key cryptography [2]. Blockchain technology has three versions stated as: blockchain1.0, blockchain 2.0, and blockchain 3.0 which are based on their applications in different scenarios. Blockchain technology was introduced via finance and digital currency but gradually it was widely used in every sector of society such as the health care sector, music sector, supply chain monitoring, agriculture industry, market monitoring, supply chain management, etc. Today's world is data-centric, and blockchain technology enables data to be stored in a systematic format, increases availability, and provides ease of tracking to the user. Blockchain technology's versions 2.0 and 3.0 flourished around 2015.

III. FUNCTIONALITY OF BLOCKCHAIN TECHNOLOGY

Bitcoin, blockchain has been known to be the public ledger for all transactions and resolved the double-spend problem by combining peer-to-peer technology with public-key cryptography [2]. Double spending is a situation in which a user of a digital currency can spend several times the same amount of money before there has been a realization that the amount has already been spent/claimed [3]. Double spending is a probable risk that comes inevitably with the concept of cryptocurrency, double spending means reclaiming the currency that had been already spent beforehand, or in a simple manner using the same currency for more than one transaction. It can be done by tampering with pre-existing blockchain and adding a new node or a new block to the chain and by this method the person who inserted a new block of data can travel to the whole chain of data and has full access to tamper the data and commit a fraudulent activity by reclaiming the currency which does not even exist or has been already spent. So to prevent such activity bitcoin assigns every block an encrypted number which includes a timestamp which further includes the time of the creation of the block, information about the previous block, and the information present inside that current block is also encrypted using the SHA algorithm.

The main aim of blockchain is to operate a different collection of data present at different locations which are linked together via a chain to which access is given only to the people who are concerned with the data. Blockchain technology independently works on public key and private key methods, where a unique private key is provided to the user the data is concerned and a public key can be shared with other users also. For creating a new transaction record one has to go through a very strict verification procedure, which slows down the whole process majorly as for each record thousands of nodes are being computed and travelled to verify one transaction. That means once a record is made inside a block it can never be tampered with or altered again, existing research had been made to increase the security and efficiency of blockchain and to facilitate the ovation of new applications. But the increased verification limits the application of blockchain technology in the internet of things, a internet of things includes many devices that may or may not have the computational ability or may be working on very low power.

IV. THREATS AND CHALLENGES OF BLOCKCHAIN TECHNOLOGY

Blockchain technology includes many preventive measures to minimize cyber-attacks. However, blockchain has been identified to be vulnerable to many types of attacks. The 51% attack is unique to blockchain and it happens when a single node controls more than half (51%) of the processing power of the blockchain. [2] The people who have benefitted most from blockchain technology are those who adopted blockchain technology in the early stages of its introduction in the finance sector, but still, blockchain technology is prone to many cyberattacks as if the attacker gets to even a single node it gets access to the whole chain and 51% of attacks that happens on the blockchain are unique attacks. A single node can govern or dominate the whole chain, which in the wrong hands can turn the major part of the currency upside down. In the finance sector blockchain technology had proposed many innovative methods to organize data, and transactions, the creation of smart contracts, payment systems, and many more. In the non-finance sectors also, blockchain technology is gaining the spotlight, for example, trying to incorporate blockchain technology in voting systems, which would provide transparency to the masses, while every record is maintained inside the blockchain. [6] For making huge transactions via bitcoins or blockchain technology, trust was the integral aspect when it came to introducing the technology to the masses, investors must have trust that their information would not be sacrificed in any situation. The blockchain on an initial level works on network security, which assures users of the privacy of their data. With new trust mechanisms arising from Blockchain, people may be able to share their properties without the concern of losing privacy [2]. Being an un-tangible source of online transactions, the main hurdle for blockchain to overcome is to gain the trust of the users, since complete transparency is not provided by blockchain technology, the user is bound to feel insecure about his / her information that can be exploited by anyone. The hurdle of incomplete transparency is overcome via encrypting the data at every level. Blockchain requires a very strict verification process to create a new transaction record, which leads to a significant latency of confirmation time and a waste of computing resources. Currently, it takes about 10 min for a transaction to be confirmed [2]. All transactions have to be stored and they will be validated. The capacity of the block will very small. Some transactions must be delayed due to miners preferring high transaction fees for that transaction. The large block size will lead to reducing the propagation speed, therefore scalability becomes a big problem [7].

V. BLOCKCHAIN NETWORK SECURITY PROS AND CONS

Underlying blockchain technology, the organization of a business community can be decentralized, peer-to-peer, and coalition. [2] The technical parts of the underlying blockchain work mainly on trust-less computing, network security, and smart contract. Just as human civilization developed, and financial records have been made and maintained, the main question that arises is whether the data is safe. Many methods have been proposed to maintain transaction records efficiently and effectively, but is it full proof? Double-entry bookkeeping is a methodology applied for years to maintain the transaction logs but it is proven to not be efficient since it can also be easily tampered with [8].

University professor of Accounting and Economics at Carnegie Mellon, author of the book Momentum Accounting and Triple Entry Book-keeping Yuji Ijiri, has proposed a method, just as the name depicts “Triple Entry Book-keeping” in which not just the two financial intermediaries are keeping the track of financial backlog, the financial backlog is maintained globally at more than one place so our trust is not completely dependent on the above two intermediaries but rather the record is being dynamically saved. Triple entry bookkeeping has been successfully implemented in Bitcoin and the underlying technology, blockchain technology. Its main aim was to create multiple simultaneous copies of every transaction or any kind of data with the functionality of the system to authenticate what's written. A ledger that authorizes itself, cannot be destroyed, since multiple copies are present, even in the worst-case scenario if the parent copy of the data is sacrificed, it would not affect the other copies. Open transparent algorithm establishes trust less computing.

Since we know that, at an initial level blockchain technology works on public key and private key, where the public key is visible to the masses and can have any user, but the anonymity of the user is maintained throughout, on the contrary, private key authorize the user on some specific security criteria such as user name or password and then the access is provided to the user. Blockchain technology includes several preventive mechanisms (e.g., distributed consensus and cryptography) to reduce the risks of cyber-attacks. [2] Blockchain technology facilitates a tamper-proof mechanism as the data cannot be modified unless the associated participants are authorizing the access.

Whenever the code malfunctioning is diagnosed, the code in the public network becomes vulnerable to the world. Access to one node can easily compromise most of the chain. There had already been cases, where a small group of people successfully accessed the control of the network's mining hash rate and computing power allowing them to modify payments while they were online. Another such vulnerability consists of routing attacks, where data is updated simultaneously at multiple locations, which indicates the presence of a network and data transfer. All you have to do is to observe and intercept the data that is being transmitted during a transaction via ISP when the network is discovered it can easily tamper, most traffic exchange is trying to add parallel blockchain, and when change is made the whole chain is compromised and destroyed. The routing attacks are anonymous until the chain has suffered considerable harm.

Another potential threat area is that third-party applications are not always authorized, and sensitive data is compromised while establishing new connections with a previous connection. And third-party applications themselves don't have appropriate security applications. There can be transaction content leakage, which can reveal user identity, and time. When multiple transactions can be made at a single time, forcing a deadlock, which would lead to the wrong desired mapping of input transaction to output that transaction was meant to display. The primary objective of any kind of block chain attack comes under two broad categories namely ballot stuffing and bad-mouthing, since bad mouthing can easily be prevented the attack rate of this domain is less, but when it comes to ballot suffering the attacks are undetectable, and hence unpreventable, which in turn leads to the increased count of constant camouflage attacks. On the other hand, there are many advantages of block chain too. The transactions are transparent and publicly available for everyone to check and validate without needing to go through a central authority [3]. Transaction records are publicly available since the underlying technology is based on public and private key cryptography, which facilitates the easier display of insensitive data, and since block chain is not a centralized repository of data, there is no sovereign controller of the whole chain. The transparency of the information allows for faster processing of transactions and information exchanges due to the elimination of the middle layer between the parties [3]. Transactions happening needs to be processed before being replicated amongst various inter-connected nodes, and since the data or the transaction details are readily available for each user as well the as the operating system the speed is increased tremendously since no unnecessary checks are performed. There is no middle layer authentication taking place, which furthermore adds to the reduced time of computation and processing of the data. The information remains anonymous despite its public availability due to the existence of a set of public and private keys associated with an account [3]. The public key is available to all the participants of the block chain, whereas, just as the name suggests the private is only visible and confidential to the user. Which in turn makes the core data anonymous. Each user has a public key and a private key associated with the chain.

VI. IMPLEMENTATION OF BLOCK CHAIN IN DIFFERENT SECTORS

A. *Banking sector*

Till now each transaction is authorized by a third party, for example, a bank, if an individual wants to make a transaction, he'd send the amount via his/her bank account, but the bank account has their share of the transfer charges that they apply on every transaction. But blockchain technology facilitates the transfer of money "free of cost" since the whole system is a peer-to-peer system, which is secure and doesn't cost as much as normal transactions via bank. And all the money is digitally maintained in a decentralized triple entry manner, maintaining records at multiple places simultaneously, ensuring no centralized data. Bitcoin or another virtual currency supported by blockchain technology can help businesses to solve funding-related problems. [1]

B. Supply chain Management

If a problem occurs at one stage of the process, the blockchain mechanism can easily detect the whole chain and find the error node, since there is an interconnection which is between the nodes and an intra-connection which is between the chains. Blockchain provides transparency. It is a step-by-step authentication and verification [9].

C. Healthcare Industry

The Healthcare industry is in great turmoil due to delays in searching for appropriate records of hundreds and thousands of patients simultaneously, solved by blockchain technology. The Healthcare industry also finds the issue of distinguishing counterfeit medicines from original medicines, which is solved by blockchain by linking the checking mechanism to supply chain management. In the healthcare industry blockchain technology can reduce administrative overheads, to large extent.

D. Insurance

Counterfeit Insurance claims can be distinguished from original Insurance claims by using blockchain technology.

E. Transportation

Block chain technology facilitates easy tracking of packages. Which is a great factor for product-based companies.

F. Cloud Storage

Cloud storage is used by blockchain, eliminating the need for the main server, the data is securely maintained and easily updated on a cloud platform, which in return also decreases the overhead companies have to pay for their data's memory and cloud data is available at high speed and low cost.

G. Traditional Voting Process

Online voting platforms are discouraged due to lack of security and ambiguity, which can be solved by blockchain, as the user identity can be authorized, and then it can be given permission to make a change, i.e. to vote once, thus eliminating the possibility of ambiguity.

H. Music Industry

In the music industry, blockchain technology can play a crucial role in maintaining copyright details and implementing copyright claims on plagiaristic work.

I.Internet of things

Most researchers today associate Blockchain applications with the IoT. This is maybe due to the fact the IoT paradigm is integrative in nature and not only encompasses all advantages of the highly networked digital world but also its bias and challenges. [3]. The Internet of things is the major application of blockchain. The applications of blockchain in the internet of things include firmware editing that is usually embedded in interlinked devices. Smart contracts are a great aid to e-commerce-based businesses since the chance of human error is reduced to null. And there are many strategic and operational advantages of blockchain. [10]

VII. CONCLUSION

In the present study we evaluated the working of Blockchain and digital currencies in the present business scenarios. Authors observed that, though this technology provides a more reliable and secure platform for transaction processing, it still leaves traces of potential threat areas and vulnerable points where a continuous improvised and enhanced model is required. Authors acknowledge the growth of Blockchain in the business domains and financial transaction management and see a larger growth in the non-conventional transaction system in future.

References

1. X. C. a. G. k. Min Xu, "A systematic review of blockchain," Springer, China, 2019.
2. S. F. a. J. Y. J. Leon Zhao, "Overview of business innovations and research opportunities in blockchain and introduction to special issue," Springer, Hong Kong , China, 2016.
3. J. A. J. a. R. G. Saade, "Blockchain applications - Usage in different domains," IEEE, Canada, 2019.
4. D. N. G. ,. D. P. G. ,. D. D. G. ,. D. M. G. Dr. Sandeep Tayal, "A Review paper on Network Security and," Research India Publications, Rohtak (H.R), India, 2017.
5. S. X.-N. D. C. Zibin Zheng, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," Blockchain technologies and applications, no. 10.1109/BigDataCongress.2017.85, 2017.
6. A. M. R. M. u. H. H. N. Purwono, "Blockchain Technology," Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI), vol. 8, no. 2, pp. 199-205, 2022.
7. R. S. a. A. Alex, "A review on blockchain security," in International Conference on Recent Advancements and Effectual Researches in Engineering Science and Technology

(RAEREST) 20-21 April 2018, Kerala, India, 2018.

8. V. C. D. Danda B Rawat, "Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems," MDPI, 2020.
9. D. S. K. Chetna Laroiya, "Applications of Blockchain Technology," in Handbook of Research on Blockchain Technology, Elsevier, 2020.
10. D. S. L. C. Komalavalli, "Overview of Blockchain Technology Concepts," in Handbook of Research on Blockchain Technology, Elsevier, 2020.