Enhancing Security Through Blockchain Technology –A Quick Review

R. Gowthamani, K.Sasi Kala Rani, E.Mohanraj, S.Sudhakar

Abstract: The concept of Blockchain technology is budding as a popular way to build the next generation of systems to tackle security challenges. Solving several troublesome problems of scalability and data integrity arising with traditional storage is achievable with Blockchain technology. Blockchain innovation is decentralized, conveyed record to trade advanced money safely. Compactly, giving security, secrecy, and information trustworthiness with no outsider association as far as controlling the exchange is named as a Blockchain innovation. It serves as an undeniable ledger that permits the transaction to takes place in a decentralized way and works on Bitcoin protocol, where Bitcoin is a consent-less network in which every user can connect with the network. This paper discusses the review of the Blockchain concept with a focus on the challenges and benefits.

Keywords: Blockchain, Decentralization, Bitcoin Integrity, Scalability.

I.INTRODUCTION

Blockchain is an advanced concept in the field of Computer Science and Security while thinking about research. It is a decentralized record, and it very well may be eluded as blocks in a chain in which each block has a pointer to the past one. After bolstering the subtleties of the exchanges or occasions into the Blockchain, it is challenging to alter those particulars which imparted to the individuals from the network. Blockchain clients in the networking system are mindful of the transactions occurring. In Blockchain, every one of the blocks is associated, and one block placed above the previous block. It utilizes the key for upcoming blocks with the last nonce with signature.[1]. Here submitted transaction forms a list when another block included; the chain develops. To guarantee consistency, appropriated distributed consensus algorithm alongside with asymmetric cryptography can be utilized. As of late, cryptocurrency has moved into a generally utilized word in the industry and among academia. The Bitcoin was developed by an obscure gathering or individual, as expressed in "Bitcoin: A peer-to-peer electronic cash system." [2] in the year 2008. CNN Money characterizes Bitcoin as "another cash that made in 2009 'Transactions made with no middlemen, no transaction fees and no need to give your real name. Wikipedia, on the other hand, describes Bitcoin as a world level cryptocurrency and digital payment system.

- *R.Gowthamani Assistant Professor, Dept. of CSE, Sri Krishna College of Engg. and Tech., Coimbatore, India, gowthamanir@skcet.ac.in*
- *K.Sasi Kala Rani, Professor, Dept. of CSE, Sri Krishna College of Engg. and Tech.,, Coimbatore, India*
- *E.Mohanraj, Associate Professor, Dept. of CSE, KSR College of Tech., Tiruchengode.*
- *S.Sudhakar, Anna University, Chennai, sudhasengan@gmail.com*

It is called a first decentralized digital currency, because of this system works without a central repository or single administrator." Bitcoin is a decentralized cryptocurrency and digitalizing payment system. Here there is no man in between transaction and no transaction expenses. And the minors will be getting the reward if they can demonstrate the exchange, also called Work Proof. Bitcoin be an exceptionally planned information storage structure. Every transaction in a system will happen without using the outside person. Blockchain considered as a free ledger, and every submitted transaction maintained as a list. This link proceeds as new blocks annexed towards the ending part of a block. An Asymmetric cryptographic and distributed consensus algorithm used to provide security and consistency. An innovative Blockchain framework has essential attributes decentralization, suitability, persistency, and obscurity. With the use of these characteristics, Blockchain will use low expense to improve the efficiency of the system. The remainder of this survey paper sorted as pursues. Segment II exhibits a presentation about Blockchain engineering.Part III comprises the utilization of Blockchain. Part IV incorporates critical qualities. Section V brings out the working head of Blockchain, and Section VI includes of characterization of Blockchain, Section VII incorporates the Challenges of Blockchain, and segment VIII finishes up this work.

2. BLOCKCHAIN ARCHITECTURE

Blockchain comprises of the succession of blocks, which embrace a full badly maintained of exchange records like traditional unwrap verification [3]. Figure 1 represented a holder of Blockchain Architecture. The block which starts is called the beginning block, and it will not have a parent block. The origin block is the first block of a Blockchain. The Block contains two parts, namely the header and the data, as shown in Figure 2. The data part holds all about transactions. The header of a block connects the transactions. Changes in any exchange will bring about a change at the block header. The headers of upcoming blocks are connected using a chain. The entire Blockchain needs to be updated if anywhere any change happens.

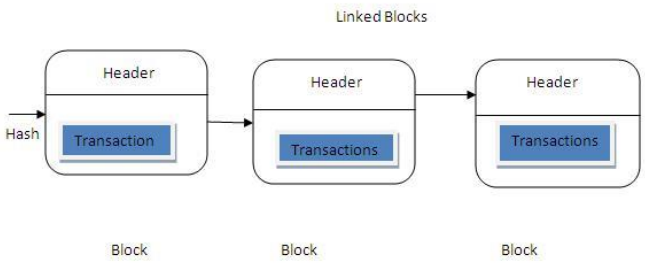

***Figure 1**. Blockchain Architecture*

The fields in block header are,

i. Version: each block follow specifies rules.
ii. Merkle Root: Number indicates transaction hash value in the block.
iii. Nonce: Four-byte field starts with zero and increments in the future for every calculation with hash.
iv. Parent Hash Block: This hash value 256-bit is used to point the before block.

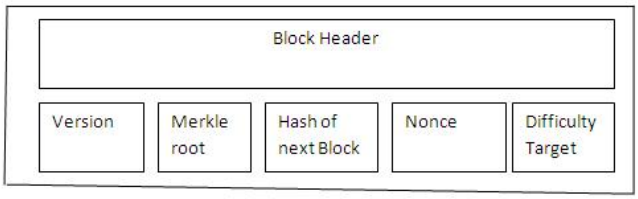

***Figure 2**. Model of BC Header*

The frame of each block made out of a counter of a transaction and remaining transactions. The quantity that a block of blockchain can have based on the size of the block and operation.

3. BLOCKCHAIN APPLICATIONS

Blockchain is a database stored using a decentralized system. It allows the transaction to completed without the use of a third party like a bank or any intermediary. Different financial administrations like excellent resources, settlement, and online installment [4], using Blockchain Technology. Further, it can likewise associated into the fields, as well as savvy contracts [5], open administrations [6], Internet of Things (IoT), notoriety frameworks, and security administrations [7] are utilizing Blockchain innovation in different ways.This field utilizes Blockchain in different ways. Because the Blockchain concept is a permanent one and also called immutable, stuffed replace can't changed once it pressed. Organizations that involve high unwavering quality and genuineness can make use of Blockchain to make consideration for clients. Likewise, Blockchain is isolated and can maintain a strategic distance from the single point of failure circumstance. With the end goal of savvy gets, the agreement can be executed with the use of miners naturally once the deal has finished on Blockchain.

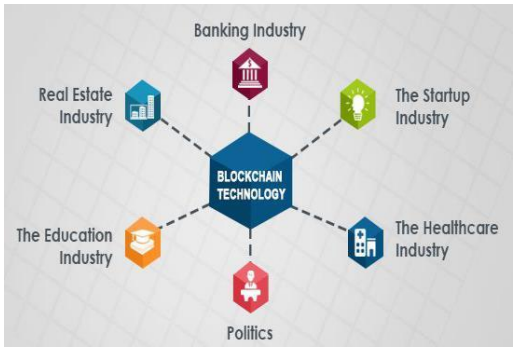

***Figure 3**. Applications of Blockchain*

Various applications of Blockchain in different areas shown in Fig 3.

4. KEY CHARACTERISTICS OF BLOCKCHAIN

The following points considered critical qualities of Blockchain.

4.1. Decentralization

Central trusted agencies would validate each transaction in a traditional transaction system. It increases costs and reduces performance. But with Blockchain, the outsider is never again required. To keep up consistency Consensus algorithms are used in a distributed network.

4.2. Persistency

Validation of transactions can be done quickly and will not permit invalid transactions with the use of miners, which are honest. Here there is no possibility to remove or may rollback connections after included in Blockchain. Blocks with void exchanges are recognized right away.

4.3. Obscurity

The entire user needs to interact with Blockchain using the formed address, which does not disturb the behavior of the user. Make a note that Blockchain not able to ensure perfect security safeguarding because of fundamental limitations.

4.4. Auditability

Blockchain of bitcoin incorporates data about equalization measure of system users dependent on Unspent Transaction Output (UTX-O) type, which advises as any exchange needs to point to some previous unspent transaction exchanges. When the present dialogue, included in the Blockchain, the status will be moved from unspent exchanges to spending transactions. Hence, every one of the exchanges could be adequately verified and followed.

5. WORKING PRINCIPLE OF BLOCKCHAIN

This section introduces the working principle of the Blockchain mechanism. Bitcoin utilizes a little measure of evidence under the Cryptographic side as opposed to accepting the outsider. Thus, the thought "digital signature introduced." The sender who needs to begin an exchange sends information utilizing his private key, and the collector gets using his open key. The individual receives the information which intends to burn through cash, has to know the private key and the advanced mark. Singular hubs

present in the Bitcoin system is entirely mindful of the exchanges being occurring. The transactions must be "embraced" and "approved" to be accessible in an open ledger. To begin with, the sender demands an exchange. At that point, the validator must check the sender has enough cash in his record to make a "genuine" exchange. The shot of double spending in bitcoin evacuated by introducing Blockchain Technology. Here, linear ordering followed for ordering transactions and formed a link with one another. Every block of the blockchain contains the block hash value before that current block. Then the created block is sent to each peer node and validated. If it is valid, the block is added with the existing block as a chin using a hash function. Then transaction completes. A mechanism with asymmetric cryptography as the best mechanism for validating authentication in the blockchain. [8]. In the case of Digital Signature, every user of Figure 4. The working flow of the Blockchain system carries two keys named public and private keys. The confidential private key should be utilized to go into the transaction. Here, transactions with the digital sign to be broadcasted through the entire network system. The classic digital signature should concentrate on signing phases, and one more step called the verification phase. Let User A needs to be communicated with another User B with a message.

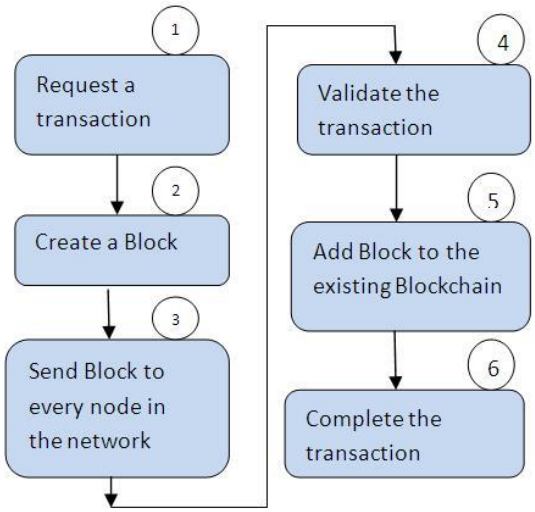

***Figure 4**. Working Principle of Blockchain*

5.1. In Signing

In the signing phase, User A scrambles information using the private key. Result sent to B with the encoded outcome and original data.

5.2. In Verification

In the authentication phase, User B certify the information with A's open key. User B verifies the originality of the message. To confirm if original information altered or not. Commonly used algorithm with blockchain is elliptic curve digital signature calculation (ECDSA) [9].

6. CLASSIFICATION OF BLOCKCHAIN

Categorizes in Blockchain frameworks are sorted into two kinds: open Blockchain and private Blockchain. In public Blockchain, every record evident to all people, and everybody could participate in the procedure of consensus. Here, expertly chosen nodes would take an interest in the method of agreement in consortium Blockchain. Concerning private Blockchain, nodes which coming from one specific region would be eligible to join the procedure of consensus.

6.1. Public Blockchain

The other name of the Public Blockchain network is also called permissionless Blockchain. Even sufficiently open-ended network. All people can join with the public network. A person who wants to participate with the network can join without asking permission — this point considered as the primary point and only comparison between public and private Blockchain networks. Anyone can join in the public Blockchain network, execute the consensus protocol, and can store shared ledger, which is open to all. The advantage of Public Blockchain is having high security when compared to the private network, whereas low privacy is the limitation. Also, substantial computational power and energy requirements and less eco-friendliness are limitations of the public blockchain.

6.2. Private Blockchain

A Permissioned Blockchain Network needs the challenge to take an interest in the networking system. The invitation must be approved either by the starter of the networking system or by the guidelines/conditions put by the initiator. A Private Blockchain system applies restrictions to some section members and permits just some kind of member that required in the networking system. [10] Disadvantages of Pubic Blockchain like low privacy and less eco-friendly rectified by Private Blockchain. While comparing public Blockchain, less security is a big problem in private Blockchain. A comparison of two kinds of public and private Blockchain shown in Table1.

***Table1.**Comparison of public and private Blockchain*

Property types	Read permission	Immutability	Efficiency	Centralized
Public	Public	Impossible to tamper	Low	No
Private	Restricted	Could be tampered	High	Yes

7. CHALLENGES IN BLOCKCHAIN TECHNOLOGY

Blockchain innovation has some specialized difficulties and confinements that have distinguished. Fig 5 shows specific test and restrictions for the version of Blockchain innovation in prospect generation networks.

7.1. Throughput

The current throughput value of bitcoin is 7 TPS (Transaction Per Second). While comparing other transactions, this is at a low level, so the throughput is the main factor to be considered to improve.

7.2. Latency

The current latency value of bitcoin is roughly 10 minutes. More time needs to spent to achieve efficiency in the network on a block. There is a possibility of Double-Spending (DS) assaults. DS is the aftereffect of the effective expense of

cash more than once. Bitcoin secures beside DS. Thus, latency is a significant part of being considered in Blockchain Technology.

7.3. Size and bandwidth

Now, the size of the Blockchain in the Bitcoin system is more significant than 50,000 MB. The Bitcoin people group expects that the block with 1 MB size. Block created like clockwork in ten minutes duration. In this way, there is a restriction in the number of transactions that can be dealt with (by and significant 500 exchange in one block). At whatever point Blockchain requires controlling further operations, the size and transfer speed issues must be resolved.

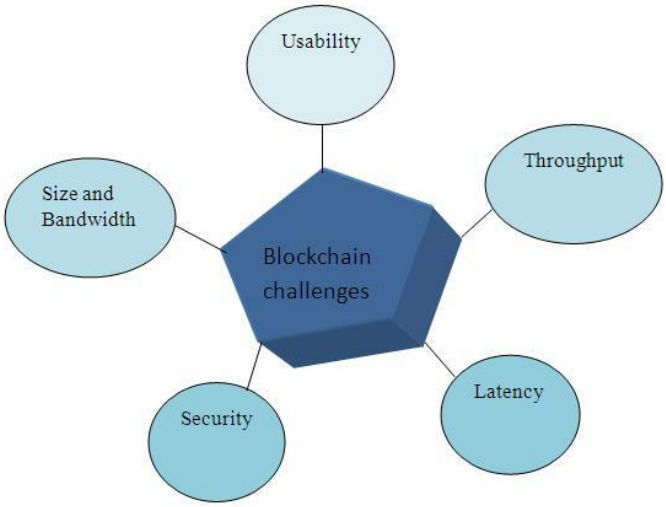

***Figure 5**. Technical Challenges*

7.4. Security

Currently, Blockchain has a probability of a 51% attack, and such an attack has complete control on the main part in hash-rate of mining in the networks. To defeat this issue in order to have the option to control Blockchain, further investigate on security is required.

7.5. Usability

The requirement for building up a added developer-friendly API for Blockchain usage is indispensable since the current Bitcoin API for developing services is complicated to apply. This usability challenge holds the technology back even though the potential of Blockchain is vast.

8. CONCLUSION

In this paper, the Blockchain technology with its key Characteristics and applications are discussed. Furthermore, we compared different types of Blockchain with its properties. Future challenges of Blockchain are identified as usability, latency, throughput, security, size, and bandwidth. Nowadays, safety is the primary concern everywhere.so as an extension of this work; an in-detail study on Blockchain supported applications with IoT for health care monitoring systems will be considered.

9 REFERENCES

[1] "State of Blockchain q1 2016: Blockchain funding overtakes bitcoin," 2016. [Online]. Available: http://www.coindesk.com/ state-of-Blockchain-q1-2016

[2] Hyperledger, " About Hyperledger ", https: // wwwhyperledger.org [online] -Available

[3] D. Lee Kuo Chuen, Ed., Handbook of Digital Currency,1st ed. Elsevier, 2015. [Online]. Available: http://EconPapers.repec.org/RePEc:.

[4] G . W. Peters, E. Panayi, and A. Chapelle, "Trends in crypto-currencies and Blockchain technologies: A monetary theory and regulation perspective," 2015. [Online]. Available: http://dx.doi.org/10.2139/ssrn. 26466188] G. Foroglou and A.-L. Tsilidou, "Further applications of the Blockchain," 2015.

[5] A. Kosiba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of cryptography and privacy-preserving smart contracts," in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.

[6] B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the bitcoin economy," 2013.

[7] C. Noyes, "Bitav: Fast anti-malware by distributed Blockchain consensus and feedforward scanning," arXiv preprint ar X iv: 1601.01405, 2016.

[8] NRI , "Survey on Blockchain technologies and related services," Tech. Rep., 2015.

[9] N. Zhang, S. Zhong, L. TianUsing blockchain to protect personal privacy in the scenario of Online taxi-hailing Int. J. Computer Communication Control, pp. 886-902, 2017.

[10] D . Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ecdsa),"International Journal of Information Security, vol. 1, no. 1, pp. 36–63, 2001.