3rd International Conference on New Frontiers of Engineering, Management, Social Science and Humanities
Osmania University Centre for International Program, Osmania University Campus, Hyderabad (India)
16th March 2019 www.conferenceworld.in
ISBN: 978-93-87793-77-4

Blockchain Technology: Security through Vulnerability

Harsha Patil

Research Scholar, MANIT, Bhopal

Ashoka Center For Business and Computer Studies, Nashik, India.

ABSTRACT

The objective of this research paper is to focuses on working framework of Blockchain Technology and enlightens the security of Blockchain technology through vulnerability. In current scenario, where Ecommerce, Netbanking and online applications' are continuously busy with updating its security aspects providing more and more security for data, Blockchain technology put the data open to all-available to all. Blockchain technology is stand with the strong block of concepts that "Open to all concept have several eyes to provide strong security then two eyes of security Guard". The Blockchain technology removed the concept of Security Guard i.e. during any transaction between two party there is no need of any third party services for transaction and its data security purposes.

Keywords: *Blockchain, Crypto-currency, Distributed Digital Ledger, POW.*

I. INTRODUCTION

"Blockchain" as the name suggest is the Chain of Blocks. The Chunk of digital information (Blocks) which are connected through the public databases (Chain). It is nothing but the newer version of the File organisation. Blocks stored digital information like actual record of any transaction, details of involve entities in the transaction, timestamps and other metadata of the transactions. Blocks also has unique id which is known as hash.

Blockchain technology is built using peer-to-peer networking. Anyone who is on network can access the blocks. There is no centralised community to control the Blockchain. It is operated by miners; the peoples who lend their computing power to the network to solve the complex computation algorithm problems. These blocks are stored in multiple computers. Due to its distributed and decentralisation, the validation process is broadcast in nature which provides it "the trusted approach". Block chain enables security and tamper proof capabilities for storing data and smart contracts. Any tampering of data attempted by a node or user in a block changes the hash of the block. The Block chain technology has the capability to face and provides the solution to fight with the problem of risk and security concern to be online.

ISBN: 978-93-87793-77-4

For example A sent B $100, the trusted third-party service would debit A's account and credit B's one, so they both have to faith this third-party is to going do the right thing. But with Blockchain technology if crypto currency bitcoin [1] is used there is no need has to trust in third parties, because anyone can directly verify the information written. Successfully completed transactions are bundled together and make a bunch of records known as block. Miners verify the genuine of transaction with in each block. For that purpose miners works with the algorithm known as proof-of-work (POW).

Blockchain technology has been going to be utilized in many applications like online payment transaction [3,4], smart contracts [5], many government and public oriented services[6], Internet of things applications[7] etc.

i) Data Structure

Blockchain is a restricted link list of Blocks. It is decentralised data structure which strongly support reliability of data. The basic structure of blockchain resist the modification of data and surfaces the alterations if any updations are done with block's data.

The hash of each block contains the hash of the previous block, which increases security and prevents any block violation.

ii) POW

POW is a mathematical puzzle solving algorithm which is used by miners to confirm transactions and add new blocks to the chain.

The complexity of puzzle is depends on the number of users, available computational power and the network load. POW deterring cyber-attacks, which unnecessarily eats the resources of the network. With POW, miners compete against each other to complete transactions on the network and get rewarded

II. CONCEPTS OF BLOCKCHAIN TECHNOLOGY

On the basis of scope, the Blockchain can be categorised as Public or Private. Public Blockchain are available to all miners or users for read or write permissions, However private

ISBN: 978-93-87793-77-4

Blockshain restricts the scope with limited number of authorised users only. Private Blockchain are created if users wants to keep the details secret. The blockchains are publically available to its users but data in blocks are encrypted by a private key and hence cannot be interpreted by everyone. The blockchain technology is implemented on the basis of Hash tree concepts. The Hash tree data structure (also known as Merkle tree) is very useful for maintain the integrity of data between sender and receiver. This concept not only functioned for Error control during transfer but also ensure correctness of data. Each block of chain has hash id. Any changes or alteration in records of Blocks updates the hash id.Thus the data remains unaltered, as any changes will be publicly verifiable. The public and distributed nature of blockchain make it more secure.

Challenges: There are considerable challenges for adoption of Blockchain. In following section main roadblocks are discussed.

i) **Cost:** Validation of Transaction gets through huge amounts of computational power. Not only computation power but miners needs to be pay or otherwise incentivized to validate transactions.

ii) **Inefficiency:** During the appending of new block proof of Work algorithm takes vast time for validation process. Bitcoin [2] is a perfect example for the possible inefficiencies of blockchain. Bitcoin's POW system takes near about ten minutes to append a new block to the blockchain.

iii) **Privacy** : While secrecy on the blockchain network protects users from hacks and preserves privacy, at the same time technology has fear of illegal trading and activity on the blockchain network from dark Web.

iv) **Susceptibility:** Blockchain networks are susceptible to attacks due to its open availability, however still networks are safe due to enormous computation power required for such executions.

ISBN: 978-93-87793-77-4

III. BLOCKCHAIN OPERATION

After successfully completion of any transaction, the verification and validation process has started [10]. Validated transactions are grouped together in a block, which finally append in a relevant blockchain with unique hash id.

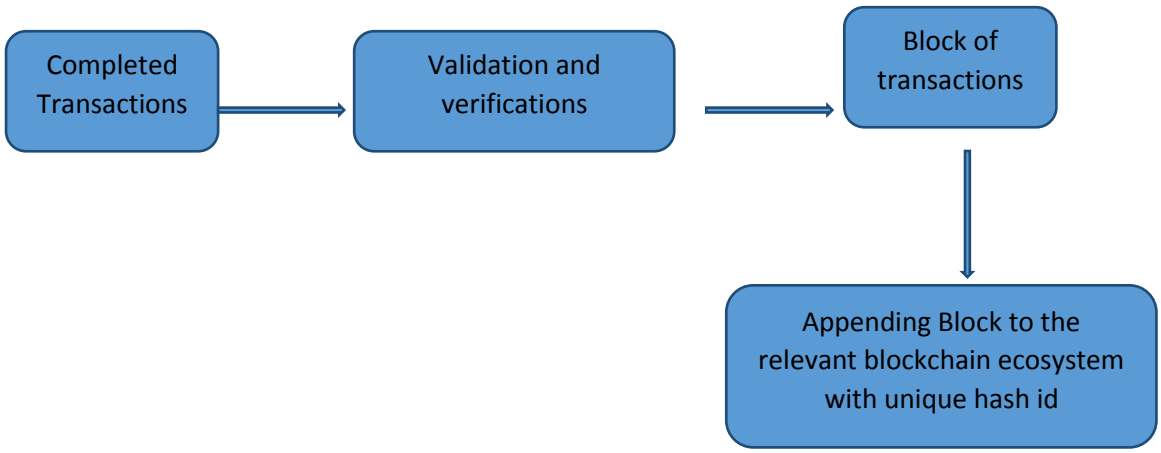

Figure 1: Operations of Blockchain

IV. CONCLUSION

Blockchain technology has many applications, the characteristics of security, tractability privacy of its make it more reliable for use. The invention of the Blockchain provides additional component to the Internet, which complement the lacking of security and trust in online applications. Its nature of decentralized across the global Internet is also very tempting in terms of ensuring data redundancy and hence survivability. BC technology is emerging with lots of scope for researchers and developers and extension required to reach its maturity.

REFERENCES

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

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.[Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] 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.2646618

ISBN: 978-93-87793-77-4

[4] G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain,"2015.

[5] Kosba, 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] W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world:Income tax onsiderations of the bitcoin economy," 2013. [Online].
Available: https://ssrn.com/abstract=2394738

[7] Y. Zhang and J. Wen, "An iot electric business model based on the protocol of bitcoin," in *Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN)*, Paris, France, 2015, pp. 184–191.

[8] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in *Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015)*, Lyon, France, 2015, pp. 490–496.

[9] C. Noyes, "Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning," *arXiv preprint arXiv:1601.01405*, 2016.

[10] Mahdi H. Miraz, "Blockchain: Technology Fundamentals of the Trust Machine," Machine Lawyering, Chinese University of Hong Kong, 23rd December 2017, Available: http://dx.doi.org//10.13140/RG.2.2.22541.64480/2