IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue, 6, March 2019 E-ISSN: 2347-2693

Blockchain in FinTech: Applications, and Limitations

Vempalli R Durgeswar[1*], C.C. Kalyan Srinivas[2]

[1,2]Dept. of Computer Science & Engineering, KMM Institute of Technology & Science, Tirupathi – 517 102, Andhra Pradesh, India

[*]*Corresponding Author: vrdurgeswar1987@gmail.com, Tel.: +91-8106110830*

DOI: https://doi.org/10.26438/ijcse/v7si6.1619 | Available online at: www.ijcseonline.org

***Abstract*—** The Internet and digitization have already turned many elements upside down. The financial sector is no exception. Today, a new epoch of financial service, called "FinTech," has emerged. Blockchain, an innovation by FinTech, has attracted considerable attention. Blockchain is a relatively new technology that has shown a lot of possibilities. It emerged in 2009 as a public ledger of all bitcoin transactions. It became more popular since it can be used as backbone for various applications in finance, media, smart property, smart healthcare, security, governmental services and many more. Motivated by the recent explosion of interest around Blockchains, we examined various blockchain's applications. This paper discusses about Blockchain characteristics and also presents its limitations. This work even explores the types of fraud and malicious activities that can be prevented by Blockchain technology and identifies attacks to which Blockchain remains vulnerable. Here we also discuss about using Blockchain to Avert Online Attacks.

***Keywords*—** FinTech, Digitalization, Blockchain, Fraud detection, Hacking prevention, Online attacks.

I. INTRODUCTION

Now-a-days, blockchain concept has been receiving significant attention in financial technology (FinTech). It blends several computer technologies, like distributed storage of data, point-to-point transmission, consensus mechanisms and encryption algorithms. It is believed that blockchain is similar to the Internet and it may transform exiting operating models of finance and economy, which may lead to new round of technological innovations and industrial transformations within the FinTech industry.

The United Nations, the IMF (International Monetary Fund) and several developed nations such as the US, the UK, and Japan have been monitoring the development of this technology and have been exploring its application in various fields. Many other countries, including India and China have also initiated research on this technology.

This paper looks at characteristics and applications of blockchain, discusses malicious online activities; studies and highlights important security issues and vulnerabilities and presents blockchain's limitations.

II. BLOCKCHAIN – CHARACTERISTICS

A blockchain can be considered as a digitalized public ledger of transactions or events recorded and stored in chronologically and linearly connected blocks, known as "completed transaction blocks", in the form of a data structure and store this in a distributed manner across a network. All the blocks maintain the hash of previous blocks. The blockchain is considered as a database, in which records are shared by all network nodes, updated by miners, monitored by everyone and owned and controlled by no one; where nodes are computers or mobile devices; and miners are nodes with large computational resources that can be used for transaction validation purpose. This process is depicted in figure 1.

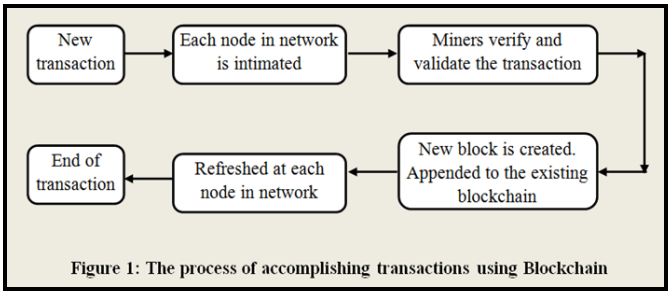

Figure 1: The process of accomplishing transactions using Blockchain

The major characteristics of blockchain are:

a. ***Decentralized*:** the blockchain stores transactions in a peer-to-peer network, where each node maintains an identical copy of the blockchain. During new transactions also, a new block is created and appended to the blockchain. Then, entire network is then refreshed with new blockchain.

b. ***Trust Free Transactions*:** In blockchain, each transaction is collectively verified and validated by miners, thus eliminates the intermediaries. Further, each transaction is unfolded before entire network, making deception is almost impossible.

c. ***Empowered Users*:** The blockchain assures high quality data, which is complete, consistent, widely available (decentralized), endured and accurate. Thus, the users can have complete idea about their transactions.

d. ***Cryptographic*:** In blockchain, all transactions are encrypted using public-private key. At origin, the transaction message is encrypted using the private key. Then, miners use public key to verify the content. If it is original, and unaltered, then blockchain process continues. In case of hacked or intercepted (altered) messages, the transaction is rejected.

e. ***Openness*:** Blockchain can be used for many applications. It can be used to record, transfer or register tangible assets like houses, vehicles or intangible properties like music, or patents. With Smart Contract feature, a work can be accomplished automatically, when satisfied certain conditions, with computer programs.

f. ***Immutable*:** All transactions are stored in anonymous and irreversible manner. The transactions, which are registered and added to the blockchain cannot be modified or rolled back.

III. BLOCKCHAIN – APPLICATIONS

The blockchain technology has intrigues programmers, businesspersons, and investors all over the world. Take a look at the domains, where blockchain can be successfully applied.

Domain	Applications
The Banking and financial services	KYC compliance, Trade finance, Payments, Trade settlement
Government and Public sector	Digital Identity: Electronic Passports, E-Residency or Birth or Wedding Certificates, Personal Identification, Online Account Login
Smart contracts	Digital rights, escrow, Automate Transactions via IoT
Securities	Equity, crowd funding, debts, derivatives
Record keeping	Health records, ownership, IPR, Eliminating counterfeit drugs

IV. USING BLOCKCHAIN TO AVERT ONLINE ATTACKS

- Evil activities on the internet – like identity theft, intrusions, (like viruses, hacking or other malware) can be averted using blockchain. It can be used in two other specific types of online fraudulent activities like double-spending and record hacking. The blockchain solves the problem of double spending using mining. Only the blocks with correct answers to the problem (i.e. the proof-of-work) are added to the blockchain. Then, the one among multiple payments is accepted and registered on the blockchain, making it impossible to double spend the amount.
- The blockchain is continuously monitored by entire network of nodes, each of which maintains a copy of the blockchain. Thus, the intruders cannot insert fraudulent blocks into the public ledger. Thus, the integrity of records in the blockchain cannot be compromised. Further, if one or more ledgers are hacked, the other network copies provide reliable backup and overwrite hacked version.
- Blockchain can even put a stop to fraud in assets. This is achieved by registering and tracking all transactions of the asset and by recording its attributes. With which, it is difficult to replace the original with counterfeits.
- The smart contracts can even be used as escrow so that the parties involved comply with contracts. Because of this, defaults by buyers and poor service by providers can be reduced.

V. BLOCKCHAIN LIMITATIONS AND VULNERABILITIES

A copy of each transaction is kept at every node of the network. The very purpose of this is to remove intermediation. However, it leads to very costly redundancy. The figure 2, depicts the same.

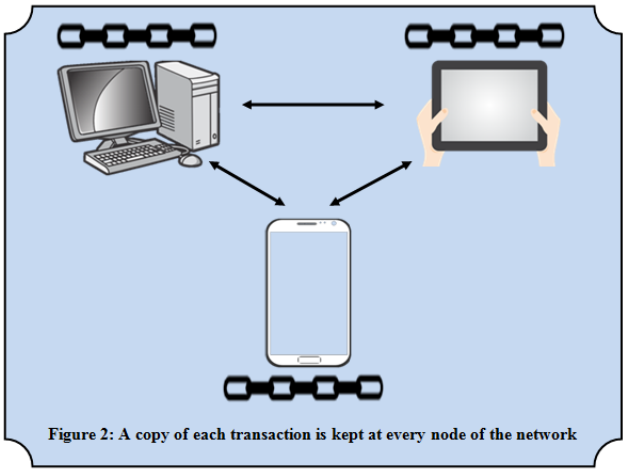

Figure 2: A copy of each transaction is kept at every node of the network

- The blockchain mechanism is always slower than traditional centralized databases, due to the very basic nature of blockchain.
- It is very well known that the blockchain averts many malicious attacks and reduces risks. However, it does not eliminate all attacks. Blockchain suffers from 51% attack, account takeover, digital identity theft etc.
- A miner having exceptionally more computational resources, than the rest of the network nodes, may dominate the verification and approval of transactions. Then the miner controls the content of a blockchain. With more than half (i.e. 51%) of the network's processing power, the dominant node ignores all other nodes, and manipulates the blockchain. Even fraudulent transactions, can be inserted or assets from others can be stolen.
- The record in the blockchain cannot be hacked. However, the programming codes or systems that implement the blockchain technology can easily be hacked. Then, hackers may gain the control of assets.
- The blockchains preserve anonymity and privacy with the help of key (private and public) - a form of digital identity. If the private key is lost, or stolen, no third party can recover it. Because of this, all the assets of the person, (owns in the blockchain) will be lost and it is nearly impossible to identify the robber.
- Further, using latest technologies like quantum computing, the cryptographic keys can be cracked easily – with which the foundation of blockchain technology itself vanishes.
- The dust transactions, which involve transferring very small amounts, but take huge blockchain space, may result in Denial of Service (DoS).
- Someone may change the unique ID of a transaction, before it is confirmed by the network nodes. In such a situation, the intruder may intercept and change the transaction details. However, all the addresses and public key details remain unchanged. Then, all network nodes will approve it, resulting in transaction malleability.
- Eclipse attacks may happen, in which the attacker may gain control of a fragment of network, which may cause the synchronization delays. This results in delay in the delivery of a block to a node.
- The anonymous sellers and buyers may do illegal business – since there is no presence of central controlling or monitoring authorities.

The anarchy may propagate with this kind of activities. The public and private agencies, academicians, lawmakers, and public representatives should understand these problems and develop the policies, regulations and laws to govern the use of blockchain technology. The widespread adoption is essential for successful prevention of fraud and other types of attacks. This may ensure the security and better functioning of the blockchain technology.

VI. CONCLUSION

This paper defines the blockchain technology, specifies its characteristics, presents the online attacks, indicates the attacks that can be averted by blockchain and even shows the attacks to which the blockchain is vulnerable (limitations).

REFERENCES

[1]. Dorri, A., Kanhere, S.S., Jurdak, R.: Blockchain in internet of things: challenges and solutions. arXiv preprint arXiv:1608.05187 (2016)
[2]. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the Internet of Things. IEEE Access 4, 2292–2303 (2016)
[3]. Lin, I.C., Liao, T.C.: A survey of Blockchain security issues and challenges. Int. J. Netw. Secur. 19(5), 653–659 (2017). https://doi.org/10.6633/ijns.201709.19(5).01
[4]. Zheng, Z, Xie, S., Dai, HN., Chen, X., Wang, H.: An overview of Blockchain technology: architecture, consensus, and future Trends. In: 978-1-5386-1996-4/17 6th International Congress on Big Data PP557-564 IEEE (2017).
[5]. Singh, S, Singh, N.: Blockchain: future of financial and cyber security. In: 978-1-5090-5256-1/16/PP463-467 IEEE (2016)
[6]. Porru, S., Pinna, A., Marchesi, M., Tonelli, R.: Blockchain-oriented software engineering: challenges and new directions. In: 39th IEEE International Conference on Software Engineering Companion PP169-179 IEEE/ACM (2017)
[7]. Hou, H.: The application of Blockchain technology in E-government in China. In: 978-1-5090-2991-4/17/IEEE (2017)

[8]. Li, Y, Huang, J., Qin, S., Wang, R.: Big data model of security sharing based on Blockchain. In: 3rd International Conference on Big Data Computing and Communications 978-1-5386-3349-6/17, pp. 117–121 IEEE (2017).
[9]. Zikratov, I., Kuzmin, A., Akimenko, V., Niculichev, V., Yalansky, L.: Ensuring data integrity using Blockchain technology. In: Proceeding of the 20th Conference of fruct Association ISSN 2305-7254 IEEE (2017)

Authors Profile

Mr. Vempalli R Durgeswar is pursing Master of Technology from Jawaharlal Nehru technological University Anantapur, AP, India. He has patespated in several national and international conferences and workshops. His interests include – Internet of Things, and Big Data Analytics and Health care.

Mr C.C. Kalyan Srinivas, working as Assistant Professor in the Dept. of Computer Science and Engineering, KMMITS, Tirupati. Affilatried to JNTU Anantapur, AP. He has published several journals in national and international publications. His area of interest is Artificial intelligence and computer networks.

