University of Sindh Journal of Information and Communication Technology
(USJICT)
Volume 4, Issue 4, December 2020

ISSN-E: 2523-1235, ISSN-P: 2521-5582
Website: http://sujo.usindh.edu.pk/index.php/USJICT/

© Published by University of Sindh, Jamshoro

Blockchain Implementation Challenges and Limitations: A Critical Review

Kamran Dahri[1], Bisharat Rasool Memon[1], Muhammad Aquib[1], Zia Ahmed Shaikh[2]
[1]Institute of Informationa nd Communication Technology, University of Sindh, Jamshoro
[2]Directorate of Information Technology, Liaquat University of Medical & Health Sciences (LUMHS), Jamshoro, Pakistan
kamran.dahri@usindh.edu.pk, *bisharat.memon@usindh.edu.pk*, *aquib20034@gmail.com*, *zia.shaikh@lumhs.edu.pk*

Abstract*— Nowadays, Blockchain is one of the most growing technology that is basically used to store the data on top of distributed nodes via consensus algorithm and cryptographic mechanism which cannot be changed or deleted. This immutable nature of Blockchain makes it prominent among other data-structures to store ever growing and scatteredly originated data in a tamper-proof way along with transparency and trust between organizations. Hence this makes Blockchain ideal for storing transactional data such as land registration records, patients' records, financial transactions, vehicle registrations, and transfer records. Yet, various transformational issues and challenges make Blockchain's implementations a painstaking process. This paper highlights and illustrates such fundamental challenges and limitations to implement Blockchain in various domains.

***Keywords*— blockchain limitations, issues, transformational challenges, consesus algorithm, cryptography, hyperledger Fabric, smart contract, dependencies**

I. Introduction

Human beings are not capable of keeping vast amounts of data memorized for every moment therefore computer systems have been developed to store such data. These systems require some kind of data storage to hold the data. The data can be stored mainly in two ways: (i) centralized systems/ servers or (ii) distributed systems. In centralized storage systems, data is stored on a single entity and everyone has to fetch the data from that centralized storage. While in distributed systems, there are more than one node connected to each other without any central authority/ system. Fig 1. juxtaposes the difference between these two systems. A centralized system has certain limitations such as central storage, security, fault-tolerance and privacy, which remain unresolved. Contrarily, distributed systems addressing some of these issues of the centralized system come with their own limitations, such as interoperability, communication overhead, security, modification of the data and complete trails of the transactions are still challenging.

Recently, Blockchain has been pitched as the implementation of the distributed system which addresses the previously mentioned issues of both the centralized and distributed systems. The aim of the Blockchain technology defined by Nakamoto is a decentralized or peer to peer technology in which third parties are not required [5]. Blockchain is the combination or chain of the blocks having time-stamped which are tightly coupled as a linked list.

Bitcoin is the first deployed and succesful application of the blockchain. It is a digitial cryptographic currency used for the purpose of trading via Internet. After the hype of this application, Blockchain technology has been deployed in various domains, such as finance, land record, medical record, and IoT owing to its decentralized enviornment and non-deleteable ledger.

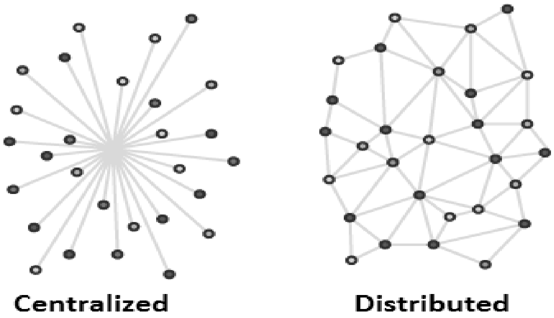

Figure 1: Difference between centralized and distributed

This paper illustrates the differnces between the centralized and distributed systems, explores the Blockchain technology with rspect to its limitations and its current applications.

The remainder of this paper is organized into five sections. Section II presents the background and the fundamentals of Blockchain technology, Section III provides related work, Section IV relates to the limitaions and challenges of Blockchain technology and Section V concludes this paper.

II. Background

This section provides a brief background to distributed systems and an overview of Blockchain technology.

As mentioned earlier, distributed systems are a collection of distributed services which are running on the distributed machine/host which does not require any central server or authority to perform the transactions. Distributed systems are also called peer to peer because of their decentralized architecture, which allows every node to communicate to another node. Blockchain is an instance of the distributed system that follows the rules and regulations of the distributed system with some modifications.

A. Blockchain

In the beginning, Blockchain technology was used for deployment of the Bitcoin digital currency, which is working in a decentralized peer to peer environment, offering the immutable ledger and provision of the complete trail of transactions. Anyone can become part of this Bitcoin network and can perform transaction cryptographically. Later, the concept of this technology was generalized to a distributed ledger broadcasted to every node which can store and validate the stored transactions without using tokens [5].

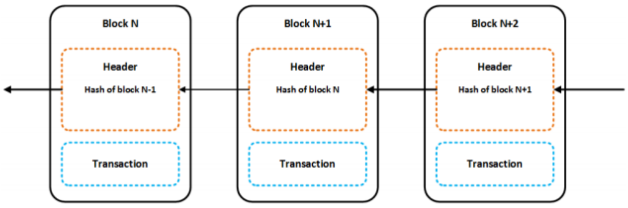

Figure 2: Creation of blocks

Figure 2 shows the formation of the blocks of the Blockchain. It is a chain of blocks, and blocks are replicated across all nodes. Blocks are basically created as the chain of the blocks crytographically. Each block in this chain has a hash of previous block, a nonce, and the data of this block. Every upcoming/ new block can only be appended at the end of the chain. Therefore, it creates an immutable ledger which cannot be deleted or changed. This makes it a more suitable technology than other mentioned technologies for record keeping of any domain where data tempering is strictly undesirable. Blockchain is basically classified into two main categories: public and private blockchain.

1. Public Blockchain

This type of Blockchain is also called permission-less Blockchain and is for everyone and anybody can become part of it. Participants of the network can join or leave the network at any time without a prior notice, Figure 3 depicts the public Blockchain structure.

Public Blockchain networks are suitable for the applications like cryptocurrencies or similar applications of the domains. Since the network is public, the participants of the network are unknown, yet they have equal rights to read and append the data to the ledger

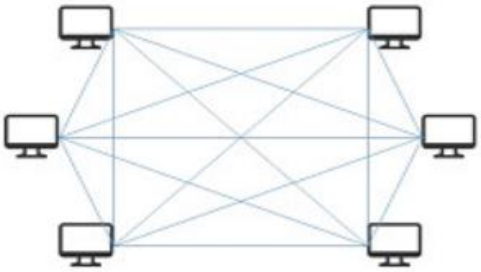

Figure 3: Public blockchain

2. Private Blockchain

Private Blockchain and permissioned Blockchain are interchangeable terms, suitable for closely related organizations for sharing of data. Since the network is private, only an authorized member can join the network and can access data. Contrary to a public Blockchain network, the operational cost of private Blockchain is less and response time is lower due to lesser number of peers on the network. Figure 4 shows the private Blockchain architecture.

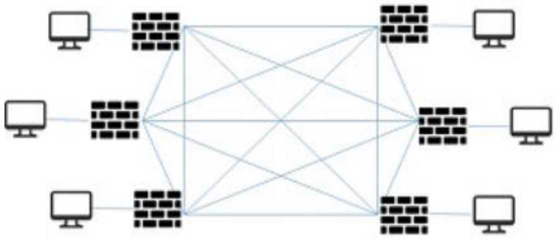

Figure 4: Private blockchain

III. Related Work

Literature suggests that there are few research efforts available which have highlighted the limitations and challenges of Blockchain technology. For example, [7] have pointed out some of the issues of Blockchain such as Majority Attack, issue of fork (hard and soft fork), scale of Blockchain, cost of integration of the Blockchain with the existing system and consumption of time to confirm the new transaction.

The authors of [2] have identified issues and proposed the future direction in the field of record keeping via Blockchain technology. In this paper, identified issues include scalability of the Blockchain, consumption of execution power and unwanted time for confirmation of the transaction via every node in the network, growing storage of the data or immutable ledger, and lack of Blockchain professionals.

The authors of [3] have proposed three solutions and the application of the Blockchain technology for the record keeping in three different fields: land records, medical records, and financial records. The paper also describes the issues and its solutions to implement record keeping in various domain having immutable and authentic ledger.

The research work mentioned in [1, 15] have reviewed the fundamental challenges and issues of the Blockchain implementation such as throughtput, latency, privacy and security, scalablity and size of bandwidth, implementation cost, double-spending attacks and fork problem. It also provides the overview, background, requirements, and solutions of the blockchain implementation.

IV. EXISTING ISSUES

This section briefly discusses various existing issues in Blockchain implementations.

A. *51% Majority Attack:*

If network is compromised somehow and more than half (i.e., >=51%) of the peers of the network agree to tell a lie, then lie would become a truth, and remaining nodes in the network must accept the new false-truth. This issue was first pointed out by Satoshi Nakamoto and it is still known as a security flaw [5].

B. *Scalability:*

It is one of the most alarming issues in the Blockchain. The number of transactions are growing day by day on Blockchain networks, and as a result more computational power and storage devices are required to fulfill the data processing needs to remain part of the network [7].

For bitcoin network *Simplified payment verification* is a solution for scalability as it reduces the overhead information of the block and only stores header information for payment verification purposes.

C. *Storage of graphical data:*

So far, Blockchain is mostly used to store textual data inside blocks, while graphical data such as images can also be stored on it. However, storing images on the Etherum is extremely expensive. The cost of data storage is 640k gas per KB of data, and the current gas price is approximately 15 Gwei or 0.000000015 ETH. Where 1 ETH equals $200 presently. So, for uploading 1 Kb, we will be spending $2 [8, 14].

D. *Cost of installation & integration*

One of the fundamental issues of the Blockchain is the installation and integration of the Blockchain network with existing centralized or decentralized systems [9]. As these existing systems usually comprise of completely different architectures and technology while Blockchain frameworks follow their own architecture and algorithms.

E. *Overhead computation:*

Execution of smart contract code is required on every node with same given parameters to remain synchronized with the network. On the other hand, each miner in the network needs supercomputer or having similar computational power to compute and validate new blocks [10, 13].

F. *Shortage of professionals:*

Since it is a new technology having different architectures, algorithms, and dependencies therefore very few researchers and professionals are out there to fulfill industry needs. Even there is a shortage of documentation and literature related to this technology.

G. *Redundancy:*

Because of the decentralized nature and consensus validation, each node has to store every new block of data to make the network immutable. Whenever, any new block is created by any node, it is broadcasted across all nodes on the network and this broadcasting process continues until each new block is replicated on every full-node of the network [11]. This behavior makes the system totally redundant which causes storage and processing issues.

H. *Forks:*

Forks are classified as either accidental or intentional. Accidental fork happens when two or more miners find a block at nearly the same time. Subsequently the newly generated blocks are added to the chain of both the newly generated blocks and one of the chains becomes longer than the alternative(s). Finally, network discards the blocks that are not in the longest chain; hence they are called *orphaned blocks* [4, 12].

Intentional forks that modify the rules of a Blockchain can be classified as hard-fork or soft-fork. Figure 5 shows the fork in the block diagram.

Hence nodes are classified into two categories: updated nodes and old nodes. This sort of situation raises two issues:

i. The upgraded nodes may or may not accept the transaction block coming from the old nodes that are not upgraded yet.

ii. The old nodes may or may not accept the transaction block coming from the upgraded nodes that are upgraded.

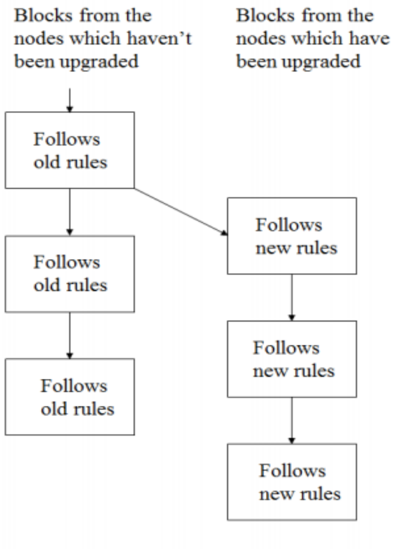

Figure 5: Issue of Fork

Due to the aforementioned issues, forks are categorized into hard fork and soft fork. When Blockchain nodes are upgraded, it causes the incompatibility between old and upgraded nodes. When upgraded nodes do not accept the transaction and agreement of the old nodes, it is called soft fork. When old nodes do not accept the upgraded version, it is referred to as the hard fork [12,15].

V. Conclusion

This article provides a brief background, related work, and highlights limitations of Blockchain technology. Its striking features like, immutable ledger, consensus algorithms and protocols, privacy and security, and interoperability make the Blockchain more feasible for record keeping. Blockchain is being implemented in various domains, such as finance, medical, land record, and IoTs. Nevertheless, there exist several issues in this technology, and are highlighted in this paper that need to be addressed. Despite these issues, Blockchain is growing and has become the hot topic for professionals and researchers to work on it.

References

[1] Bojana Koteska, E. K. (2017). Blockchain Implementation Quality Challenges: A Literature Review. *6th Workshop of Software Quality, Analysis, Monitoring, Improvement, and Applications,*, (p. 8).

[2] Hany F. Atlam, A. A. (2018). Blockchain with Internet of Things: Benefits,Challenges, and Future Directions. *I.J. Intelligent Systems and Applications*, 9.

[3] Lemieux, V. L. (2017). A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation. (p. 8). IEEE.

[4] Liao, I.-C. L.-C. (2017). A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, 7.

[5] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *URL: http://www.bitcoin.org/bitcoin.pdf*.

[6] *Storing Pictures On the Blockchain*. (n.d.). Retrieved from newsbtc: www.newsbtc.com

[7] Vukolić, M. (2015, October). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In International workshop on open problems in network security (pp. 112-125). Springer, Cham.

[8] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD) (pp. 25-30). IEEE.

[9] Bdiwi, R., De Runz, C., Faiz, S., & Cherif, A. A. (2017, July). Towards a new ubiquitous learning environment based on Blockchain technology. In 2017 IEEE 17th International Conference on Advanced Learning Technologies (ICALT) (pp. 101-102). IEEE.

[10] Lasla, N., Younis, M., Znaidi, W., & Arbia, D. B. (2018, February). Efficient distributed admission and revocation using blockchain for cooperative ITS. In 2018 9th IFIP international conference on new technologies, mobility and security (NTMS) (pp. 1-5). IEEE.

[11] Zhaoyang, D. O. N. G., Fengji, L. U. O., & Liang, G. (2018). Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems. Journal of Modern Power Systems and Clean Energy, 6(5), 958-967.

[12] Vukolić, M. (2015, October). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In International workshop on open problems in network security (pp. 112-125). Springer, Cham.

[13] Paul, R., Baidya, P., Sau, S., Maity, K., Maity, S., & Mandal, S. B. (2018, September). IoT based secure smart city architecture using blockchain. In 2018 2nd International Conference on Data Science and Business Analytics (ICDSBA) (pp. 215-220). IEEE.

[14] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare:“MedRec” prototype for electronic health records and medical research data. In Proceedings of IEEE open & big data conference (Vol. 13, p. 13).

[15] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.