IJCCN | INTERNATIONAL JOURNAL OF COMPUTING & COMMUNICATION NETWORKS

ISSN: 2664-9519 (Online); Vol. 1, Issue 1, August 2019

A Technical Review on Blockchain Technologies: Applications, Security Issues & Challenges

Bilal Bin Mahmood, Muhammad Muazzam, Nadia Mumtaz and Sajjad Hussain Shah

Department of Computer Science, Bahria University, Islamabad, Pakistan

* Corresponding Author: Bilal Bin Mahmood; bilalbmahmud@gmail.com

Received; Revised; Accepted; Published

Abstract: Blockchain technology is gaining more attraction with every passing day, as it has revolutionized the traditional trade due to its distributed ledger feature, every record in this ledger is secured by rules of cryptography which makes it more secure and tamper-free. As a result, blockchain has the potential to change the way we buy and sell, how we interact with government and verify the authenticity of everything from property titles to organic fresh vegetables. Blockchain is a distributed database of records where the transaction is verified by consensus of various participants in the system. This paper review the blockchain technology and some specific applications, risks, challenges for financial and non-financial domains. This paper help to new researchers in this area to explore and design new solutions to taking the existing demands and challenges into account.

Keywords: Blockchain, Applications, Decentralization, Security

1. Introduction

T new emerging technology is based on decentralized database record, containing public transitions records and keeping tracks which help to monitor the participants, digital events and public ledgers. In blockchain technology, every step performs with the mutual census of the parties and agreement [1]. Once the transaction is being made it cannot be removed from the information system. This is working perfectly in both the financial and non-financial domains. Giving tracks for all the events that have been performed are stored electronically online. This technology helps to improve the democratic and public ledgers. It also opens the doors for digital economical scalability in centralized architecture [2]. In traditional analogy, money transactions perform physically where the stealing probability is high because it's being observed by thousands of peoples, cameras and security staff. Blockchain is a way in which organizations perform transactions by multi distributed manners. To perform transitions and identify the information, the Multiple Distributed Ledgers (MDL) technology is used. This is one of the applications of blockchain technology, where without any central ownership, all the records are being maintained electronically and available globally and the records can be verified anytime. Further, the interference of the third party can be verified at any point and the tampered source [3].

The current digital economy is a reliance on authorities and an agreement between them. If we are talking about Facebook, a third party is telling us that our post and information is shared only with our friends and family. In the banking transactions, the third part is telling us that our transactions are successful and money is being transferred to the particular source. If we use E-marketing /Ecommerce or online authority tools which is notifying us on the order we have placed and the credit we have to pay. The fact is that we are living in an era, where we are relying on third parties to provide us security and privacy with the confidentiality for our assets. But the question is that these third party sources can also be hacked or manipulated. This is the point where blockchain technology became useful. It has the potential to revolutionize the way the records being stored, enabling them and to perform tasks with distributed consensus [1]. Each and every transaction along with the assets and privacy of the concerning parties can the verified with their records and present situation when both parties are involved [4]. Distributed census and confidentiality are the two major characteristics of blockchain technology. The advantage of using blockchain is that it incorporates the issue and technical challenges. Once blockchain implemented, it cannot be reversed or denied, because the agreement is pursued with the mutual consensus of all the participants [5]. Today in the digital world, a new trend is catching the mainstream which focuses on storing information safely and securely in a distributed environment so that it cannot be tempered or compromised. This new approach is much better than old conventional approaches in which all the information is stored in a central repository that is controlled by an authority.

The main hazard in the conventional approach is that information confidentiality and integrity can be compromised easily. Blockchain is defined as a distributed ledger/database that keeps records of all the transactions/information between all the entities in the network insecure manner by implementing basic rules of cryptography. All the transactions/information are chunked into blocks and linked in such a way that every block is connected with previous and next block. This technical review paper presents the blockchain risks, elements, architecture, working, types and applications.

The paper is divided into the separate section where more focus on to the point information related to blockchain and its applicability. Section 2 discusses the adaptation of blockchain. Section 3 elaborates the elements. Section 4 and 5 present the architecture and working process of blockchain. In last, the paper concludes with future direction.

2. Risks of Adaptation

Although blockchain is the best solution for the growing world and networks, it plays a vital digital role in the area of financial and non-financial structures. However, still blockchain has various risks related to its process and transaction, which are as follows:

- **Behavior change:** It is an old fact that behavior changes and the change is always constant. Blockchain has introduced as non-tangible trusted third party through which digital work is being done. By adopting this technology, the customers should be at peace that their work and assets are in safe hands. Some of the companies like banks for their products like visa and debit cards also thinking to adopt this technology and may also going to change their platforms and switch to the blockchain. This technology takes time to change the behavior of users and secure their systems more precisely [6].

- **Scaling:** Blockchain networks may take a long time to download or set up the networks. This complexity demotivated the new customers to adopt the blockchain and start their first transaction. The blockchain should be scalable to adjust in any type of traditional systems [7].

- **Bootstrapping:** Transferring the documents through blockchain from the initial stage may take time plus extra cost. Adopting and transferring the traditional systems into blockchain systems may take a long time for execution [8].

- **Fraudulent activities:** During blockchain transactions, the money can be hacked by intruders or attackers. Although the blockchain technology is more secure but still there is a need to protect the systems during transferring this technology.

- **Quantum computing:** Due to the lack of computing power, the whole system can be brought down to its knee if any third party interferes to hack it. The cryptographic keys are easy to crack down so they should be

powered enough that no one around can break it down in less of the time at least until we reach the error. The system should generate alert for the intrusion detection in case of any attack to enter in the system [9].

3. Elements of Block chain

The blockchain technologies composed of six key elements, which are as follows:

- **Decentralized:** The basic element of blockchain technology is that it is independent of all the other modules. It has got its storage, updating, and creation. Independent from others [10].
- **Transparent:** The data records in blockchain are transparent any one can claim or check the transaction at any point of time which makes it different from all other technologies. It also transparent to update the data that's why blockchain can be trusted.
- **Open Source:** Most blockchain system is open to everyone, record can be check publicly and people can also use blockchain technologies to create any application they want.
- **Autonomy:** Because of the base of consensus, every node on the blockchain system can transfer or update the data safely, the idea is to trust from single person to the whole system, and no one can intervene it.
- **Immutable:** Any records will be reserved forever, and can't be changed unless someone can take control more than 51% at the same time.
- **Anonymity:** Blockchain technologies solved the trust problem between nodes, so the data transfer or even transaction can be anonymous, only need to know the person's blockchain address.

4. Blockchain Architecture

The basic architectural structure of blockchain is the block containing details of all the transactions. The first most block is known as the Genesis Block and other blocks are known as Parent Block. Every block is linked to its parent block by a reference of hash value. Figure 1 represents a blockchain.

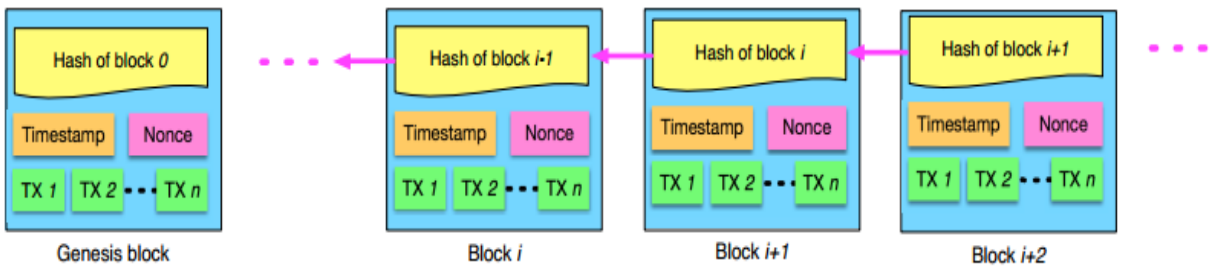

Figure 1. Blockchain Architecture

Block is divided into two parts *Header* and *Body* as shown in Figure 2. Header of the block contains:

i. Block Version
ii. Hashed value of previous block
iii. Hashed value of all the transactions in the block calculated by Merkle Tree function
iv. Timestamp
v. Other information like nonce, signature of the block or any user defined data

The body of the block contains the data. The nature of data is depended upon the service provided by blockchain, for example the data of financial blockchain will contain transaction records. After execution of a transaction a hash value of all the transaction is calculated using a hash function. A time stamp is also appended to the transaction which helps in removing duplicity of the record.

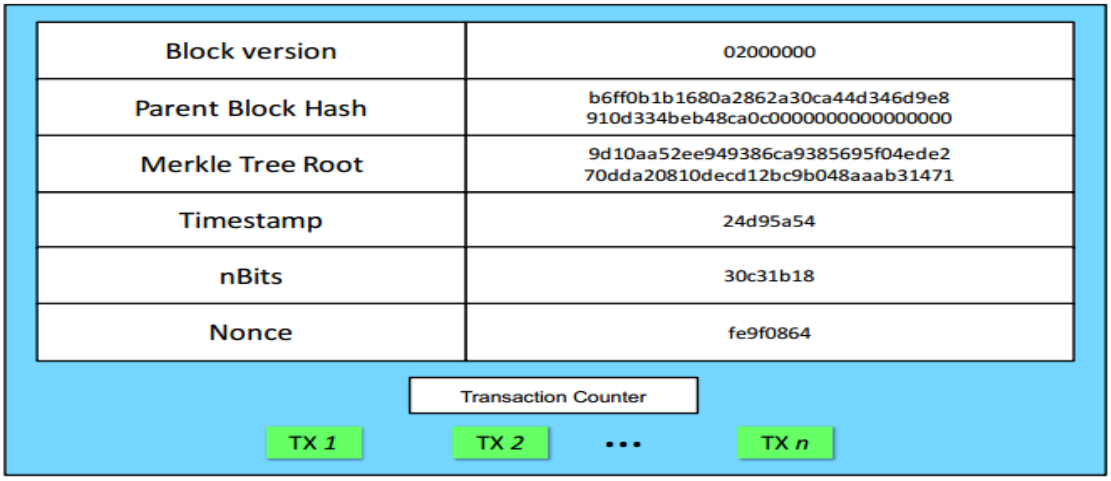

Figure 2. Two parts of Header and Body

5. Blockchain Working

To add new data to blockchain network the data is broadcasted over the network. The data is verified and then stored into a block. Before appending the block to the chain every node agrees on the message being valid consensus algorithms are used. Every node will process this new generated block by executing Proof of Work (PoW) or Proof of Stake (PoS) algorithm.

5.1 Consensus Algorithm

One of the major challenge in blockchain environment is maintaining trust between the nodes as it is a distributed ledger and there is no central node that ensures every node has same ledger. To overcome this trust challenge, some of implemented protocols are PoW and PoS.

5.2 Proof of Work (PoW)

PoW algorithm depends on resolving a mathematical problem that is hard to solve but can be verified easily. When a new block is created by the node it must resolve this mathematical problem. Once the problem is solved the block will be broadcasted over the network to achieve consensus on the new block.

Calculating PoW is known as ‘Mining’ and the node that calculates PoW is known as ‘Miner’. To generate PoW miner uses a random value Nonce form the block header and solves the mathematical problem which obtained value which should be less than the predefined value. PoW makes it unpredictable in the network that who will generate the next block.

5.3 Proof of Stake (PoS)

Proof of Stake (PoS) algorithm is an energy efficient algorithm as compared with PoW. PoS emphases the node to proof user ownership. It means that to add a new block, the user is charged. PoS provides a security from any malicious attack in the network.

6. Types of Blockchain

Blockchain technologies can be classified into three types, as follows:

1) Public Blockchain: This type provide an open access to general public, means that anyone can view the transactions and can become the part of the network by taking part in the consensus. Examples of public blockchain are Bitcoin and Ethereum. A public blockchain is shown in Figure 3.

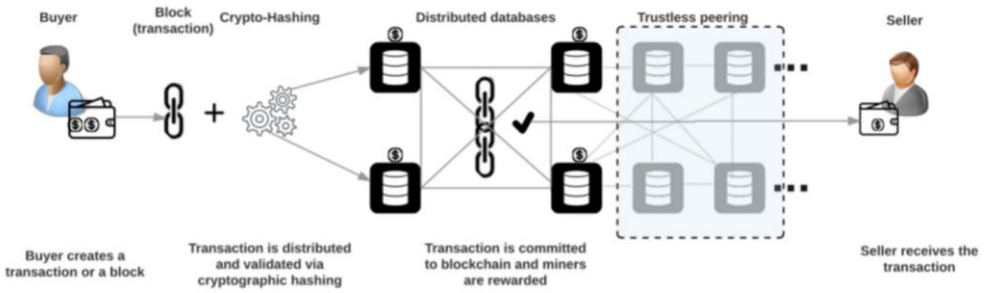

Figure 3. A Public Blockchain

2) Private Blockchain: This type allows those nodes that are privileged with rights to access the data. A private Blockchain is shown in Figure 4.

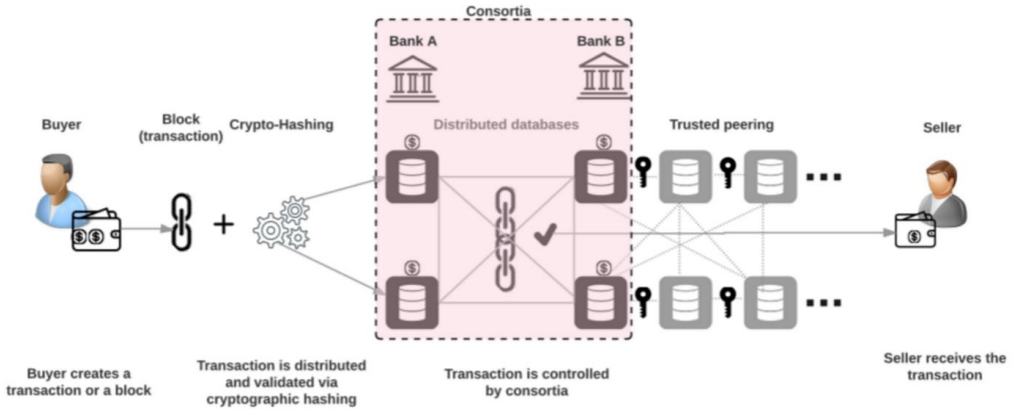

Figure 4. A Private Blockchain

3) Consortium Blockchain: Consortium Blockchain is hybrid combination of public and private blockchain where the data can be kept open or private. Hyper ledger and R3CEV are some examples of consortium blockchain. A consortium blockchain is shown in Figure 5.

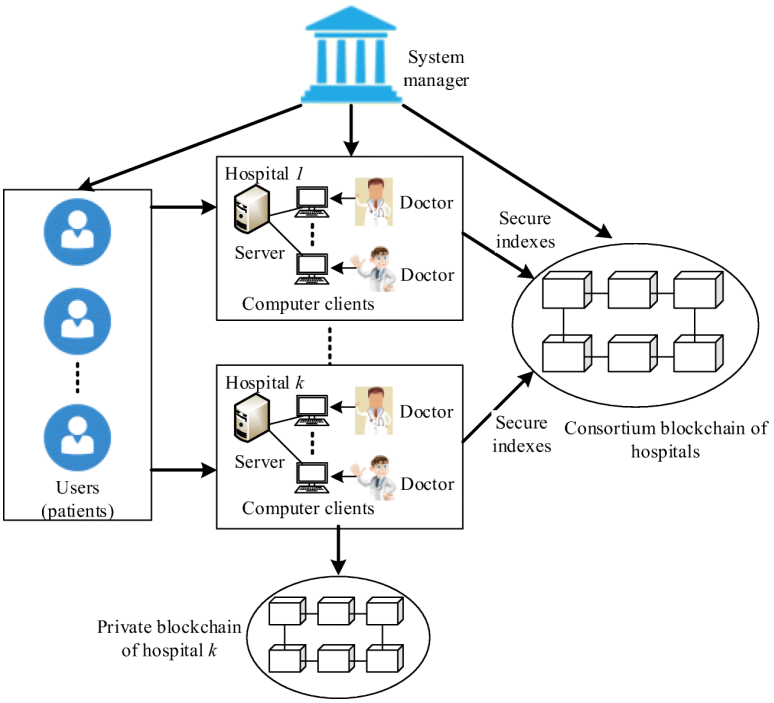

Figure 5: A Consortium Blockchain [11]

Table 1 shows the comparison of public, consortium and private blockchain.

Table 1: A general comparison of public, consortium and private blockchain

Property	Public Blockchain	Consortium Blockchain	Private Blockchain
Consensus determination	All miners	Selected set of nodes	One organization
Read permission	Public	Could be public or restricted	Could be tapered
Immutability	Nearly impossible to tamper	Cloud be tempered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

7. Applications of Blockchain Technologies

Blockchain Technologies are being deployed in many areas after reshaping financial world, it is also successfully deployed to meet challenges in industrial domain [12]. The major characteristics of blockchain from governance point of view are as follows.

A. Smart Contracts

Smart contracts is one of key advantage of using blockchain. Smart contracts is associated with blockchain, it automatically implements the policies and standard defined in contract and as per the agreed parties and the transaction is made according to the terms defined in the contract [13].

B. Smart Property

Smart property is another related idea with respect to controlling the responsibility of property or resource by means of blockchain utilizing smart contracts. The property can be physical for example, auto, house or cell phone, or on the

other hand it can be non-physical, for example, offers of an organization. It ought to be noted here that even Bitcoin isn't extremely money: Bitcoin is about controlling the responsibility of blockchain. Its innovation is finding the applications in extensive variety of territories; both monetary and non-budgetary. Monetary establishments and banks are no longer observe blockchain innovation as a danger to conventional business models. The world's greatest banks are in reality searching for circumstances here by doing research on imaginative blockchain applications. We can imagine putting evidence of presence of every single authoritative archive, wellbeing records, what's more, steadfastness installments in the music industry, public accountant, private securities also the marriage licenses in the blockchain. By putting away the unique mark of the computerized resource as opposed to putting away the computerized resource itself, the obscurity or security target can be accomplished.

C. Existing currency

Blockchain is being applied in both of the station that is financial and non-financial domains. These domains are relying upon the third parties for the safe and secure transactions. Another idea of smart contracts are also finding its way out but couldn't work until programmable payments started taking place in the networking zone. Blockchain and smart contracts are working together to enhance the cryptocurrency work at its ultimate best. Besides cryptocurrency, the blockchain is being widely used in other domains including the three basic:

- **Alternative blockchain**

  a technique of using block chain operations in a way that we achieve apportion consensus on the specific asset. In this the whole main network may share miners around to get the result. These chains have been distributed and are implemented SSL, DNS, Voting, file storage etc.

- **Colored coin**

  It is an open source of a protocol which allows many of the developers to produce digital assets by providing methods and functionalities to the bitcoin blockchain.

- **Side chains**

  These are the alternates of blockchain and are backed by the bitcoins just in a way gold is backed by dollars and pounds.

D. Financial applications

- **Private security:** It is very expensive compared to market or the company. For example people in the stock exchange cannot transact their money time to time so surely without any security given to them thus they take the hand of the blockchain and issue their shares through it.

- **Insurance:** This is used to verify the ownership of the asset which can be physical or digital and can be identified by other identifiers easily. History is kept safe in the digital world.

E. Non - financial applications

- **Notary public:** It verifying authenticity of the document which can be done by blockchain as well. Documents are the proof that certain asset is authorized by this specific person and the proof can be given easily to the third parties but increasing its value blockchain takes it to the next level. Blockchain can help to verify the validity of the certificate as well as secures the privacy of the document by notarization.

- **Internet applications:** Name coin is the alternate of the blockchain with minor changes. As we know that DNS is controlled by the government and other higher co operations so that they have the authority to

sensor, hijack and take in control of person personal history. But with this, blockchain can has our own centralized private book on our computers [14].

- **PKI and KSI:** For the digital certificate distribution, PKI (Public Key Infrastructure) is widely used. Every working device should have the root core called CA (Certification Authority) to verify the digital process. The characteristics of the blockchain is locating the draw backs of PKI and gives us KSI which is key less security infrastructure. KSI uses hash functions which are cryptographic and allow verifications [15].

8. Centralized Architecture & Scalability Issue

The centralized architecture like the state and politics are formed for the purpose of consensus and reacting to the changes and responses. This architecture facilitates distinct users to maintain mutual interaction between different groups [16].

8.1 State as a single point of Failure (SPOF):

Even though they had been built in reaction to unique historical needs, businesses with top-down centralized coordination and hierarchical systems tend to be inherently inefficient. These technologies are totally based on coercion and they may lack flexibility and capacity to evolve, imparting inadequate responsiveness to demanding situations and to the growing societal demands [17].

9. Conclusion

The decentralized nature of blockchain technology is making it more attractive to resolve common problems in financial and non-financial domains. Bitcoin is based upon the blockchain technology. In this paper, we presented a comprehensive overview of blockchain technology, by first defining the technology and its features, architecture and how it works, some applications and in the last we have discussed some of the risk factors that are involved in deploying blockchain technology.

References

[1] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, pp. 352-375, 2018.

[2] M. Swan, *Blockchain: Blueprint for a new economy*: " O'Reilly Media, Inc.", 2015.

[3] G. Zyskind and O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*, 2015, pp. 180-184.

[4] M. Anwar, A. H. Abdullah, R. A. Butt, M. W. Ashraf, K. N. Qureshi, and F. Ullah, "Securing data communication in wireless body area networks using digital signatures," *Technical Journal*, vol. 23, pp. 50-55, 2018.

[5] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, pp. 183-187, 2017.

[6] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in *IEEE EUROCON 2017-17th International Conference on Smart Technologies*, 2017, pp. 763-768.

[7] P. Tasatanattakool and C. Techapanupreeda, "Blockchain: Challenges and applications," in *2018 International Conference on Information Networking (ICOIN)*, 2018, pp. 473-475.

[8] I.-C. Lin and T.-C. Liao, "A Survey of Blockchain Security Issues and Challenges," *IJ Network Security*, vol. 19, pp. 653-659, 2017.

[9] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395-411, 2018.

[10] H. Halaburda, "Blockchain revolution without the blockchain," *Bank of Canada Staff Analytical Note*, vol. 5, 2018.

[11] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *Journal of medical systems*, vol. 42, p. 140, 2018.
[12] M. Pilkington, "11 Blockchain technology: principles and applications," *Research handbook on digital transformations*, vol. 225, 2016.
[13] G. R. White, "Future applications of blockchain in business and management: A Delphi study," *Strategic Change*, vol. 26, pp. 439-451, 2017.
[14] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, 2017.
[15] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and L. Njilla, "Security implications of blockchain cloud with analysis of block withholding attack," in *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, 2017, pp. 458-467.
[16] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 2, p. 71, 2016.
[17] A. Wright and P. De Filippi, "Decentralized blockchain technology and the rise of lex cryptographia," *Available at SSRN 2580664*, 2015.