Block chain technology in different domains and challenges-A Review

Archana Chhabra,

Department of Computer Science and Egineering,

Lovely Professional University, Phagwara, Punjab, India

Abstract

In this era of distribute networking security and privacy of information is the main concern of an individual over a network. There are many ways to secure transmission of data over a network but each has its pros and cons. Now a days, security, privacy and trust is provided with the means of blockchain technology. Initially, blockchain has its root in cryptocurrency (bitcoin) but now it is used in different domains for assuring integrity, confidentiality and authenticity of the data being shared.

Keywords: Blockchain, Finance, Iot, Cyber security, Healthcare, Government, Business

1. Introduction

Initially the blockchain was come into the market for bitcoin and cryptocurrency but now it has found its use cases in several industries using finance, health care and Iot. A blockchain is a highly encrypted list (chain) of records (blocks) that serve as a public (distributed) digital ledger that records and validates online transactions and events between permitted people in a secure network[1]. A Blockchain is a type of diary or spreadsheet containing information about transactions. Each transaction generates a hash. If a transaction is approved by a majority of the nodes then it is written into a block. Each block refers to the previous block and together make the Blockchain. For Example, A Bitcoin Block contains information about the Sender, Receiver, number of bitcoins to be transferred. The first block in the chain is called the Genesis block. It offers a secure way to exchange any kind of good, service, or transaction.

Industrial growth increasingly depends on trusted partnerships; but increasing regulation, cybercrime and fraud are inhibiting expansion. Further Blockchain provides a lower cost of trade with a trusted contract monitored without intervention from third parties who may not add direct value.[2,3].

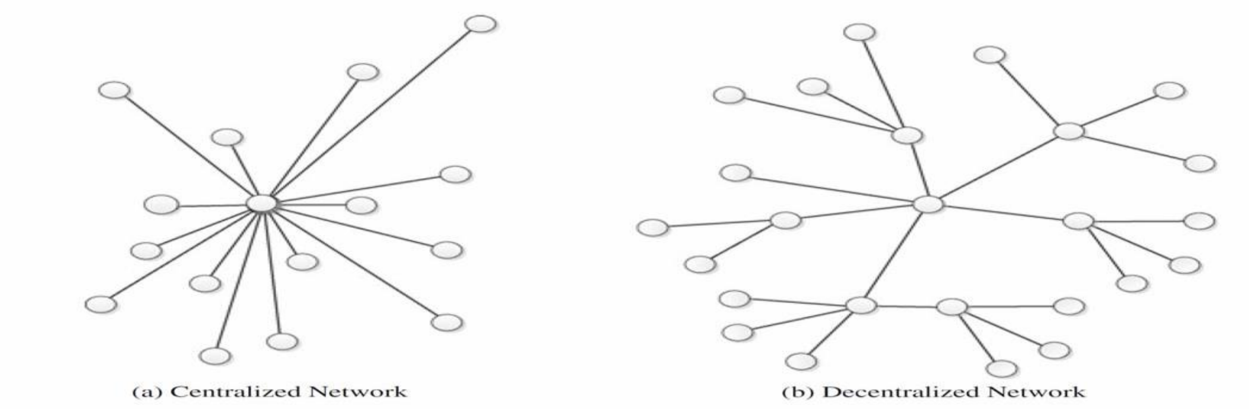

Fig 1: Centralized and Decentralized network [2]

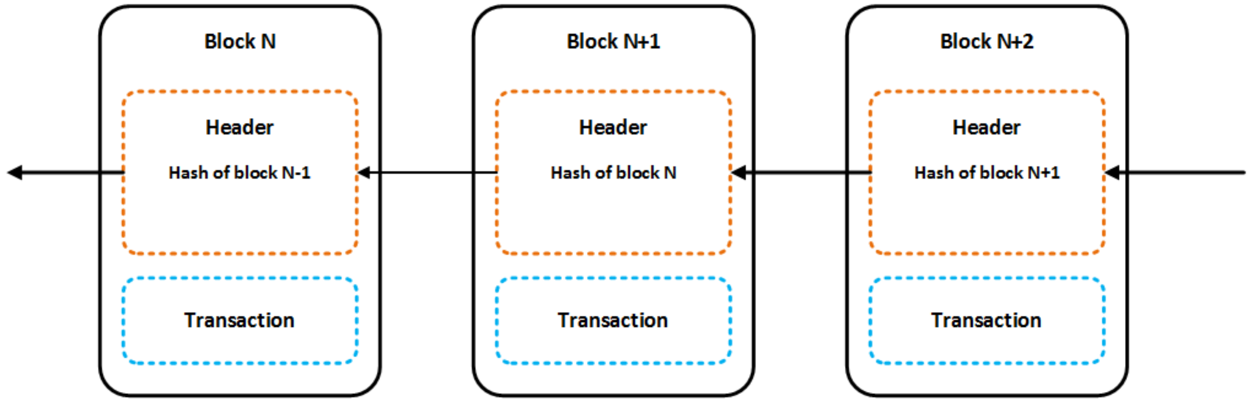

Fig 2: A chain of blocks- Blockchain network[3]

1.1 How blockchain works?

a) Assume that the transaction has to be made between user A and user B.
b) Each transaction between A and B is done in the form of a block over the network.
c) Than each block is broadcasted to every node in the network and these nodes are able to verify the data in the block.
d) The block which is verified, is then added to chain of blocks, which could be used by each node on the network.
e) Any change to this block is not possible rather all the users can only see it.
f) Finally, the transaction between A to B will be completed.

1.2 Comparison with conventional database[4]

a) Blokchain uses various encryption and decryption algorithms for maintain privacy od data where as in the conventional system it is done by the central server in the form of rows and columns.

b) In Blockchain technology all the nodes on the network are having same access rights to verify the data whereas traditionally it is done by central monitor.

c) Transactions are visible to all nodes in the same form and is changes made by one user are transparent to all others on the network in Blochain network but in conventional networks it is only visible to central server which manages all the transactions.

d) Blockchain systems are comparatively more secure than the conventional central systems as in Blockchain technology one can keep a check on previous block.

1.3 Characteristics of Blockchain technology

There are the following key characteristics of Blockchain Technology and are listed as below:

a) ***Decentralization:*** Previously conventional transaction systems are operated by a single central trusted entity, which is responsible for validating the integrity authenticity and confidentialy of the transaction made bewtween different users. But it increases the cost anf performance bottleneck at the central system. To overcome from this problem it is preferred that there is no trusted third party requirement for making transactions and one such featue is provided by Blockchain networks which uses different algorithms to maintain the authenticity of the data.

b) ***Persistency:*** It is easy to validate the transactions quickly and the source of invalid transaction if any, as invalid transaction can be easily find out and reported because rolling back or deleting the transaction is nearly impossible in Blockchain.

c) ***Anonymity:*** It helps in hiding the real identity of the user as each user can interact with the blockchain with a generated address. Moreover perfect privacy is not guaranteed by Blockchain due to the intrinsic constraint.

d) ***Auditability:*** Transactions can be easily verified and tracked because every current transcation refers some previous transaction over the chain of network and once the current transaction is recorded into Blockchain it will switch from uspent to the list of spent transactions [5].

2. Applications of Blockchain in different domains

There are many loop holes in different domains in terms of maintaining security, confidentiality and integrity of information or transaction taking place between two or more entities, so to overcome for this it is very difficult to work on any single platform especially when we talk about banks, legal issues, health care, Iot and many more.Today there is a need to change and adapt some new technology for providing these services to people in a better way and one such technology advancement is provided by means of integrating the concept of Blockchain technology to the existing central distributed system. Moreover, it will help in increasing the productivity and reduce conflicts among various departments. Further, Blockchain can also be used for land records,social welfare projects and so on. Some of the major application areas of blockchain are listed below:

2.1 Finance market

- Bitcoin
  Satoshi Nakamoto was the first person who introduced the concept of Bitcoin or digital currency in 2008 [6]. The transaction between different users is made possible with Bitcoin as it consist of Blockchain public ledger which make transactions across a peer to peer in the network. For examples, Bitbond, BitnPlay, BTC Jam, Codius and DeBuNe are the active Bitcoin in the market.

- Ripple
  The Ripple is a currency exchange, remittance and realtime gross settlement system (RTGS) [7] that uses ripple protocol across a peer-to-peer network, a decentralized exchange that focuses on the banking market. Other well known currency exchange and remittance systems are Coinbase, BitPesa, Billion, Stellar, Kraken and CryptoSigma.

2.2 Health care

Blockchain deals in an effective way to overcome the problems of interoperability in the current healthcare system [8]. It could be used by all the stakeholders such as healthcare bodies, medical researcher and many more to share electronic health record [EHR] in a secure way [9]. EHR helps to improve the quality of medical [10] and also recommend the list of best suited Doctor for the treatment [11]. It is not easy to manage the healthcare data such as analyzing, storing, and most importantly privacy concerns. Hiding Healthcare data from others should be ensured so that other entities cannot use it for making some fraud or other personal benefits.

2.3 Real Estate

In dealing with real estate conventionally, all the land records are authenticated between two parties by a central authority which clears each statement of the transaction. Now to do all this in a more secure way Blockchain network can be used. As the records and document are stored in the form of a block which are not possible to modify and moreover it is easily authenticated and verified by a trusted third party. Also it is already in use by many law firms to overcome the traditional long process of filing for real estate.

2.4 Smart Contracts

It is the another strong area where blockchain concept can be used efficiently for making contract and agreements among people. Many users are already using the application of smart contracts in their day to day life where rules are implemented by softwares. It is very easy to register, verify and implement contracts by using Blockchain technology. For example, banks are using escrow accounts as the test case to make dummy transactions for ensuring the privacy and security whicle transacting using the blockchain technology.

2.5 Other industrial domains

In addition to above mentioned applications , many useful applications are threr in other domains like construction and telecommunication industries. In the construction industry, blockchain can be used for construction management through enhancing the current processes of contract creation, registration, monitoring, control, and management. In addition, blockchain services can support better construction supply chain management, and construction equipment leasing [12]. In the telecommunication industry, blockchain can enhance telecommunication services management [13]. Blockchain can improve traceability, contract management, and governance processes in the telecommunication industry. Moreover it can also be utilized for logistics, agriculture and food industry by the way of RFID.

3. Issues and Challenges in Blockchain

The promise of blockchain benefits is appealing; however, many challenges face the adaptation and deployment of blockchain in industrial applications. Here we will highlight some key challenges in using blockchain in this context. These challenges are both technical and non-technical. The technical challenges are related to security, integration, and scalability, while the non-technical challenges relate to privacy, professional preparation, and government regulations.

3.1 Security

One of the main concerns of utilizing blockchain is security. As blockchain applications are connected and available over the Internet, they are vulnerable for various cyber-attacks including stealing, spy attempts, and Denial-of-Service (DoS) attacks, which can make blockchain services unavailable. One of the stealing attacks was against MtGox, a bitcoin exchange based in Tokyo, Japan, in 2014 that resulted in a loss of $600 million [14]. Another example was against Ether digital currency that values around $55 million.

3.2 Scalibilty

To agree on some transaction blockchain requires distributed ledger for including multiple entries in the trancasction which is then linked to the ledger transaction and added to the chain of blocks. This process is relatively complex, yet effective given a limited sized blockchain. Unfortunately, current applications requiring blockchain generate huge amounts of transactions to be processed and linked, which could easily degrade the overall performance. Second issue is when the blockchain is used to find, verify, or use earlier transactions. This includes various steps and the performance is inversely proportional to the size of the blockchain. Thus, the bigger the blockchain the slower the process gets. Scalability has become a major issue with the increase in the size and number of entities involved and transactions being performed.[15]

3.3 Integration

Blockchain technology cannot be effectively used alone as a solution for various applictions rather it is generally combined with many distributed system applications for giving better results. Blockchain could be used as a source to add new functions that are required to support future business models. Integrating blockchain solutions with existing applications including legacy applications can be challenging. This challenge is mainly due to interoperability and security issues. For example, legacy applications may not be ready to be smoothly and securely integrated with newer systems and applications including blockchain solutions.

3.4 Privacy

Blockchain are of three types public, consortium and private. Each of these three has different characteristics and privacy issues [15]. In public blockchain , all the participants have right to view so it is difficult to maintain privacy of any participating industry entity and conduct some transactions in such blockchain. Further in consortium blockchain, it is also not possible to maintain full privacy because it allows some selected participants to completely view the transaction. And in private blockchain it is relatively easy to maintain a better degree of privacy; but, as it is controlled by single entity so not considered a secure environment as it is only controlled by a single[16].

3.5 Current Regulations Problems

Central bodies somewhere feel ignored or insecured in using the blockchain technology because it weakens their rules and policies. For example, use of Bitcoin in financial market, had affected the ability of central bank to control the economic policy and the amount of money, that makes government be cautious of using blockchain technologies. Moreover authorities are currently working on this new issue, and new rules and policies are soon going to be formulated for the effective use of this new technology otherwise, it will be a great risk to the market.

4. Conclusion

There's no doubt that blockchain is a hot issue in recent years, although it has some topics we need to notice, some problems has already been improved along with new technique's developing on application side, getting more and more mature and stable. The government have to make corresponding laws for this technology, and enterprise should ready for embrace blockchain technologies, preventing it brings too much impact to current system.When we enjoy in the advantage of blockchain technologies bring to us, in the same time, we still have to stay cautious on its influence and security issues that it could be have.

References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *Www.Bitcoin.Org*, p. 9, 2008.

[2] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, “A brief survey of cryptocurrency systems,” in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2016, pp. 745–752.

[3] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2015.

[4] Blockchain-Understanding the potential – Barclays- Simon Taylor.

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

[6] Nakamoto, S., 2012. Bitcoin: A peer-to-peer electronic cash system, Oct,2008.

[7] Ripple, “RippleNet”, https://ripple.com

[8] M. Mettler, “Blockchain technology in healthcare: The revolution starts here,” in *e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on*. IEEE, 2016, pp. 1–3.

[9] L. A. Linn and M. B. Koo, “Blockchain for health data and its potential use in health IT and health care related research.”

[10] B. A. Tama, “Learning to prevent inactive student of Indonesia open university.” *Journal of Information Processing Systems*, vol. 11, no. 2, pp. 165–172, 2015.

[11] B. A. Tama and K.-H. Rhee, “Tree-based classifier ensembles for early detection method of diabetes: an exploratory study,” *Artificial Intelligence Review*, 2017.

[12] ——, “The IoT electric business model: Using block chain technology for the internet of things,” *Peer-to-Peer Networking and Applications*, pp. 1–12, 2016.

[13] F. Tian, “An agri-food supply chain traceability system for china based on RFID & blockchain technology,” in *Service Systems and Service Management (ICSSSM), 2016 13th International Conference on*. IEEE, 2016, pp. 1–6.

[14] S. Porru, A. Pinna, M. Marchesi, and R. Tonelli, ``Blockchain-oriented software engineering: Challenges and new directions," in *Proc. 39th Int. Conf. Softw. Eng. Companion*, 2017, pp. 169_171.

[15] G. Karame, ``On the security and scalability of bitcoin's blockchain," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2016, pp. 1861_1862.

[16] Z. Zheng, S. Xie, H. N. Dai, and H. Wang, *Blockchain Challenges and Opportunities: A Survey*. Tamil Nadu, India: PAP Calibration Works, 2016.