An Overview of the Revolutionary Technology: Blockchain

[1]Ashwni kumar, [2]Mariya Khatoon
[1]M.Tech student, [2]M.Tech student
[1]Department of Computer Science and Engineering,
[1]K.N.I.T, Sultanpur, U.P, India.

Abstract: The blockchain is one of the technologies that emerged in the last decade and is very promising. Extensive researches are underway to explore all the capabilities of blockchain. The range of blockchain application ranges from financial services, healthcare, automobile, risk management, Internet of Things (IoT) to public and social services. Several studies focus on using the blockchain data structure in various applications. In this paper we try to conduct a complete study of blockchain technology by discussing its structure to different consensus algorithms and reviewing blockchain applications. Furthermore, this paper also indicates the future directions of blockchain technology.

IndexTerms **- Blockchain, structures, Internet of Things (IoT), Application of Blockchain.**

I. INTRODUCTION

In recent years, the internet has seen the launch of many important applications, from the bottoms-up, that solve problems of adaption and distributed techniques. Some of these public and non profit systems have become well known and widespread. Cryptocurrency has recently attracted attentions of industry and academic world. Bitcoin, often called the first cryptocurrency, was a huge success with a capital market reached $10 billion in 2016. The blockchain is the central Bitcoin mechanism. The blockchain was first proposed in 2008 and implemented in 2009. Blockchain can be considering a public ledger in which all validated transactions are stored in a chain of blocks.

The Blockchain is a digitized, decentralized, and public register of all cryptocurrency transactions. These transactions are documented in a chronological order, helping participants to track of digital currency transactions without central record [1, 2, 3]. The distributed database is one of the main features of blockchain forming a peer- to- peer network, indicating that there is no single database or centralized sever [4]. Instead, there is a blockchain database across the decentralized network of computer exists. Each computer in the network is called a network node and every node on the network receives a copy of the duplicate blockchain that is automatically downloaded. Transactions are digitally signed with a public key cryptography that uses two keys, containing a public and a private key. These two keys are mathematically related to each other. Due to the complexity of mathematics used, it is almost impossible to guess these keys, which makes the transaction more difficult to decipher. The public key is used to sign and encrypt a message to be sent and the designated recipient can decrypt the message using his private key. To keep the blockchain database as a "global registry", the data for all new transactions is propagated to all nodes.

In this paper we discuss various areas of use of the blockchain, as well as the associated with security and privacy issues. We compare existing research and explore security and privacy issues in a systematic and detailed manner.

II. BLOCKCHAIN

2.1Definition

Blockchain is essentially a gigantic database that covers multiple networks, different institutions or geographic area and records ownership and values of transactions. Each time a transaction executed, the blockchain checks it first and records the transaction.

Blockchain can be used for any type of transaction such as value, data, cryptocurrency, asset, any type of contract or confidential data. Anyone with access to this database is authorized to view and participate in this database. It helps to create a data register in digital from, distributed by nature. A large distributed ledger means that each party participating in blockchain network has its own copy of ledger. If changes are made at any time, it will automatically be reflected in the copy of each part.

2.2Structure of Blockchain

In blockchain there is no centralized authority to control the data flow. The blockchain of network can be structurally different from the blockchain of another network. The blockchain consist of three elements [5].

2.2.1Block

Blockchain is database in a distributed ledger that keeps records of all the transactions. These records are called blocks. The dimension, the data in a block and the time of intervention are different for each block. Each blockchain records the movement of data (cryptocurrencies).

2.2.2Chain

A chain is created by linking all the blocks together. These chains are created using encryption, using hash functions. A hash is created from the data in the previous block.

2.2.3Network

The network consists of complete nodes. Computers running on the network and participating in the blockchain is called complete nodes. Bitcoin data is structured to records all record of all transactions. A complete node can be present in any geographical location on earth.

III. TYPES OF BLOCKCHAIN

The 3.1figure illustrates the three forms of blockchain, namely the public blockchain, the private blockchain, and the consortium blockchain [6, 7, 8].

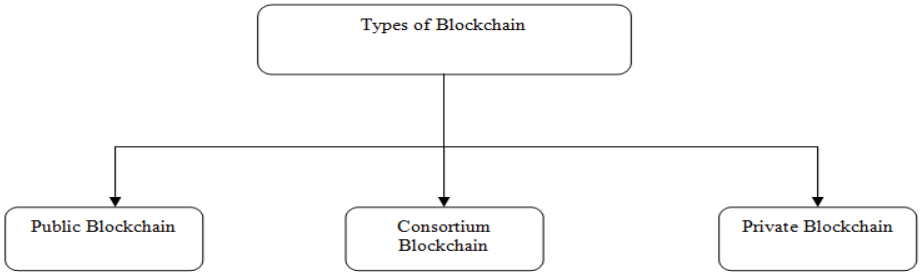

Figure 3.1: Types of Blockchain

These three forms are discussed in detail in this section.

3.1Public Blockchain

In this type of blockchain, all network members can validate the transaction and participate in the process to reach a consensus. The blockchain was originally designed to safely remove the central authority in an asset exchange scenario. It ensures the decentralizing by established a block of peer to peer transactions. Each transaction is associated with the blockchain before being written to the system. Therefore, it can be confirmed and synchronized with every node of the network. Anyone with a computer and internet connection can register as a node can have the complete blockchain history. The redundancy of the public blockchain makes it extremely secure. However, it is very slow and inefficient. Bitcoin is good example of public blockchain. These are the blockchain that work between two parties on a large distributed database using cryptocurrencies.

3.2Private Blockchain

The private blockchain is the type of limited blockchain that allows the intermediary to return to a certain extent. The private blockchain has a strict management regarding the authority to access data in the network. None of the node in the network can participate in the verification and validation of transactions. Instead, a company or organization initiates, verifies and validates each transaction. This provides a higher level of efficiency in transaction verification and validation. The only big gap in the private blockchain is that it does not provide decentralized security like the one provided by the public blockchain.

3.3Consortium Blockchain

The consortium blockchain is a combination of public and private blockchain and can be perceived as partially decentralized. In this blockchain network, the details of the data or transaction can be open source or private and the node has the authority to choose in advance. It is essential to distinguish between a consortium blockchain and a totally private blockchain. However, the difference has not yet been deepened. In general, the consortium blockchain is a hybrid between the low trust of public blockchain and the single highly trustable entity model of private blockchain, whereas private blockchain can be precisely defined as traditional centralized system with cryptographic verification and validations attached.

IV. APPLICATION OF BLOCKCHAIN

Since the emergence of blockchain, a lot of research is being done to explore what we can do more with this extraordinary technology. The application of blockchain are still being discovered, a few of those will be discussed here.

The figure 4.1 describes the areas in which the blockchain is mainly used.

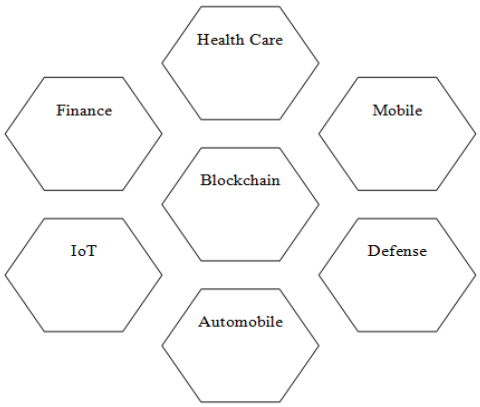

Figure 4.1: Area of Application of the Blockchain Technology

4.1Blockchain in Finance

Blockchain was originally developed as the backbone of bitcoin, which is a popular decentralized digital currency. The late blockchain is used in many digital currencies like Altercoin, Peercoin, Ethereum [9], Karma [10], Hashcash [11], and Binarycoin. Most digital currencies use the blockchain structure as the basis, although it uses a different consensus algorithm for checking verification and validation of blocks [12].

The figure 4.2 represents a generally financial transaction using smart contracts.

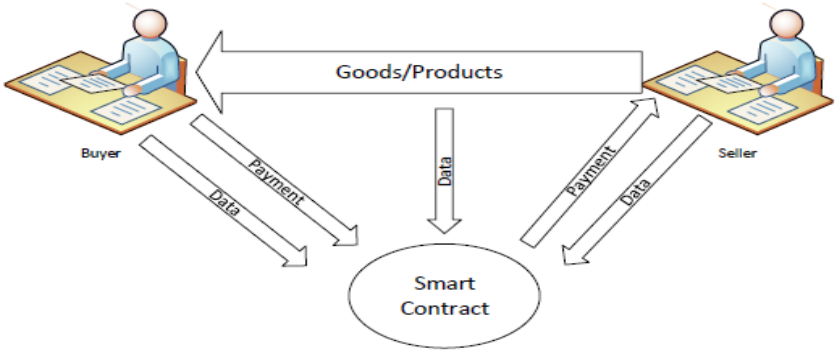

Figure 4.2: Blockchain in Financial Transaction

4.2Blockchain in Healthcare

The medical industry is very interested in blockchain technology to protect and keep track of medical data collected by the patient. Medical data is extremely important, and any error or modification can lead to extreme results. With blockchain data can be made public and used without the fear of change [13].

4.3Blockchain in Internet of Things (IoT)

Internet is now an integral part of everyone's life, sometimes we don't even know how everything is connected. All the devices like smart watches, smart fridges, cameras and your mobile phase etc. are connected to internet. Internet of Things (IoT) is basically a web of smart sensors and devices that is connected to the internet and is sharing information with each other to make our lives easier. There is no denying that IoT has made our environment smart for us, but it also makes us vulnerable [14].

The blockchain, as a decentralized and temperamentally resistance system, is very attractive for the internet of things (IoT) industry. The number of nodes in IoT is increasing day by day and so is the data that are being gathered. The security of data has always been an issues, blockchain can help secure and manage this data.

4.4Blockchain in mobile Application

A mobile application can be describe as a software application developed specifically for mobile devices such as Smartphone and tablets. The blockchain support peer to peer data service in a mobile application, as discussed in [15] and [16] for the transfer of peer to peer data file and direct payment [17]. Mobile users run mobile blockchain application using peripheral computer nodes for miners deployed with peripheral computing services providers. This service provides mobile user with computing resources at prices set by the service provider. The figure illustrates the use of the blockchain in mobile application.

4.5Blockchain in Defense

The blockchain can be used in defence application performing operational or support roles, as follows:-

4.5.1Cyber Defense

This is a low-cost, high pay off application of blockchain. First of all, the blockchain guarantees the perception of all digital events by transmitting them to all other nodes of the network, therefore it uses different consensus algorithms for validation and verification. Once secured data is tagged and archived, it can no longer be manipulated [18].

4.5.2Supply Chain Management

The growing concern about defence supply chain management in defence is driving the need of technology to establish the origin and traceability owner. Blockchain provides a solution to these problems, as discussed in [19].

4.5.3Blockchain in Automobile Industry

Modern vehicles are increasingly connecting to online or network- based applications and is therefore an excellent basis for using blockchain technology. As mentioned in [20], automotive security architectures must meet certain requirements to meet the future needs of intelligent vehicles.

V. CONCLUSION

Blockchain technology is extremely recognized and appreciated for its decentralized infrastructure and peer to peer nature. In this paper, we propose a comprehensive survey by initially discussing the structure of blockchain and its major components and characteristics. Finally, the applications, opportunities, and challenges of blockchain technology are summarized.

Blockchain technology transform every traditional industry to a new one either it is financial or non financial. Blockchain technology will explode in coming years. Early adopters will get truly benefit in future.

REFERENCES

[1]C. Ai, M. Han, J. Wang and M. Yan, "An efficient social event invitation framework based on historical data of smart devices", in 2016 IEEE International Conferences on Social Computing and Networking (Social Com), IEEE, 2016, 229-236.

[2]M. Han, M. Yan, J. Li, S. Ji and Y. Li, "Generating uncertain networks based on historical network snapshots", in International Computing and Combinatorics Conference, Springer, Berlin, Heidelberg, 2013, 747-758.

[3]S. Ji, Z. Cai, M. Han and R. Beyah, "Whitespace measurement and virtual backbone construction for cognitive radio networks: From the social perspective", in Sensing, Communication, and Networking (SECON), 2015 12th Annual IEEE International Conference on, IEEE, 2015, 435-443.

[4]M. Han, M. Yan, J. Li, S. Ji and Y. Li, Neighborhood-based uncertainty generation in social networks, Journal of Combinatorial Optimization, 28 (2014), 561-576.

[5] T. Laurence, "Blockchain For Dummies", John Wiley& Sons, 2019.

[6] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges", IJ Network Security, 19 (2017), 653-659.

[7] X. Xu, I.Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso and P. Rimba, "A taxonomy of blockchain-based systems for architecture design", in Software Architecture (ICSA), 2017 IEEE International Conference on, IEEE, 2017, 243-252.

[8]Z. Zheng, S. Xie, H.-N. Dai and H. Wang, "Blockchain challenges and opportunities: A survey", Work Pap.

[9]G. Wood, Ethereum, "A secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper, 151 (2014), 1-32.

[10]V. Vishumurthy, S. Chandrakumar and E. G. Sirer, Karma, " A secure economic framework for peer-to-peer resource sharing", in Proceedings of the 2003 Workshop on Economics of Peer-to-Peer Systems, Berkeley CA, 2003.

[11]A. Back et al., Hashcash-a denial of service counter-measure.

[12] F. Tschorsch and B. Scheuermann, Bitcoin and beyond, "A technical survey on decentralized digital currencies", IEEE Communications Surveys & Tutorials, 18 (2016), 2084-2123.

[13]L. A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health it and health care related research", in ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST, 2016.

[14]N. Barnas, Blockchains in national defense, " Trustworthy systems in a trustless world, Blue Horizons Fellowship", Air University, Maxwell Air Force Base, Alabama.

[15]F. Gierschner, Bitcoin and beyond.

[16]K. Suankaewmanee, D. T. Hoang, D. Niyato, S. Sawadsitang, P. Wang and Z. Han, "Performance analysis and application of mobile blockchain", arXiv preprint, arXiv:1712.03659.

[17] Z. Xiong, S. Feng, D. Niyato, P. Wang and Z. Han, "Edge computing resource management and pricing for mobile blockchain", arXiv preprint, arXiv:1710.01567.

[18]W. Tirenin and D. Faatz, " A concept for strategic cyber defense, in Military Communications Conference Proceedings", 1999. MILCOM 1999. IEEE, vol. 1, IEEE, 1999, 458-463.

[19]K. Korpela, J. Hallikas and T. Dahlberg, "Digital supply chain transformation toward blockchain integration", in Proceedings of the 50th Hawaii International Conference on System Sciences, 2017, 10pp.

[20] M. Steger, C. Boano, M. Karner, J. Hillebrand, W. Rom and K. R omer, Secup, " Secure and efficient wireless software updates for vehicles", in Digital System Design (DSD), 2016 Euromicro Conference on, IEEE, 2016, 628-636.