A Comprehensive study on Blockchain with its Components, Taxonomy and Consensus

Dr. K.Sharmila[1], Dr.S.Kamalakkannan[2],Mrs. R.Devi[3], Mrs.C.Shanthi[4]
Assistant Professor[1,2,3,4],
Department of Computer Science,
VISTAS((Vels Institute of Science, Technology & Advanced Studies).
1.sharmila.scs@velsuniv.ac.in,2.kannan.scs@velsuniv.ac.in
3.devi.scs@velsuniv.ac.in,4.shanc08071978@gmail.com

Abstract

Block chain as a technology has shown rapid development and creates buzz in recent years behind the Bitcoin crypto-currency system. Blockchain-based applications are jumping up, covering various fields including monetary administrations, reputationsystemand Internet of Things (IoT), etc. Nonetheless, there are as yet numerous difficulties of Blockchain innovation, for example, versatility and security issues holding on to be survived.This paper shows an exhaustive review on Blockchain innovation.Here in this article an overview of Blockchain architectures firstly and some typical consensus algorithms used in different Blockchain. Furthermore, technical challenges and recent advances are briefly listed.

Keywords: Blockchain, Internet of Things (IoT)

1.Introduction:

Blockchain technology originally block chain, was first coined in 2009, by Satoshi Nakamoto, that enables the cryptographically validated transactions and data that are not under the control of any third party organization. Any transaction ever completed is recorded in an immutable ledger in a verifiable, secure, transparent and permanent way, with a timestamp and other details.

A blockchain is characterized by censorship resistance, immutability and global usability, and has a global network of validators called miners, who maintain it through block rewards, named cryptotokens (Jeremy Gartner, in Shulman, 2018).Vitalik Buterin (2017), the creator of Ethereum, states that decentralization assures fault tolerance, attack resistance and collusion resistance[1].

Blockchain (BC)technology, is consider to be necessary for forming the backbone for ensuring enhanced security and privacy for various applications in many other domains including the Internet of Things (IoT) eco-system. Many research is currently being conducted in both academia and industry applying Blockchain in varied domains[2].

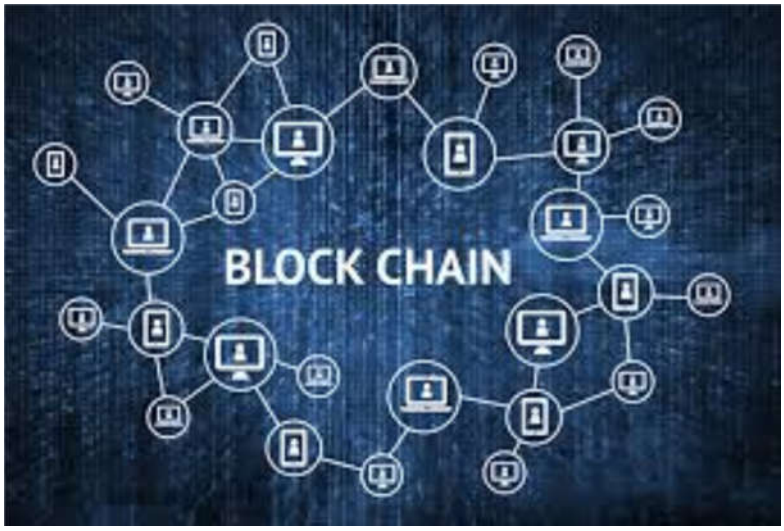

Figure 1: Blockchain technology

2.Taxonomy of Blockchain systems:

Current blockchain systems are categorized roughly into three types: public blockchain, private blockchain and consortium blockchain [3]. In public Blockchain, it enables all the users to read and write such as in Bitcoin, access to it. Differently, only a group of pre-selected nodes would participate in the consensus process of a consortium blockchain. As for private blockchain, only those nodes that come from one specific organization would be allowed to join the consensus process. Everyone in the world could join the consensus process of the public blockchain. The main difference among the three types of blockchains is that public blockchain is decentralized, consortium blockchain is partially centralized and private blockchain is fully centralized as it is controlled by a single group[7].

3.Components of Blockchain

A Blockchain comprises of two different components namely transactions and block which is defined as follows:

1. Transaction: A transaction, , represents the action triggered by the participant.

2. Block: A block, is a collection of data recording the transaction and other associated details such as the correct sequence, timestamp of creation, etc[4].

Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger [5]. The first block of a blockchain is called genesis block which has no parent block. A block consists of the block header and the block body as shown in Figure 1. In particular, the block header includes Block version, MarkleTree Root Hash,Time shamp, nBits, Nonce, Parent Bloch Hash. The block body is composed of a transaction counter and transactions.

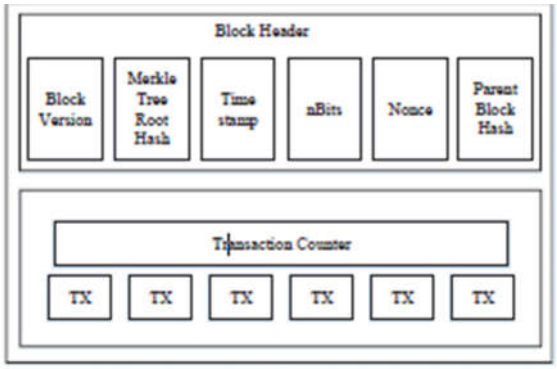

Figure 2: Blockchain-Block Structure

The major benefits of the Blockchain is that it and its implementation technology is public. Another major advantage of the it is that it is decentralized in the sense, there is no single device that stores the data, the transactions are not subject to approval of any single authority or have to abide by a set of specific rules etc. The overall advantage of Blockchain technology is security.

4.Consensus Algorithms

In blockchain, how to reach consensus among the untrustworthy nodes is a transformation of the Byzantine Generals (BG) Problem [8]. How to reach a consensus in distributed environment is a challenge. So it is one of the challenge faced by blockchain as the blockchain network is distributed. In blockchain, there is no central node that ensures ledgers on distributed nodes are all the same. The general approaches to consensus in blockchain is as follows

PoW (Proof of work) is a consensus strategy used in the Bitcoin network [9]. PoS (Proof of stake) is an energy-saving alternative to PoW. Proof-of-Authority (PoA) is a consensus algorithm which can be used for permissioned ledgers. PBFT (Practical byzantine fault tolerance) is a replication algorithm to tolerate byzantine faults [10]. DPOS (Delegated proof of stake). The major difference between PoS and DPOS is that PoS is direct democratic while DPOS is representative democratic. DPOS is the backbone of Bitshares [11]. Ripple [12] is a consensus algorithm that utilizes collectively-trusted subnetworks within the larger network. Tendermint [13] is a byzantine consensus algorithm. A new block is determined in a round.

5. Applications of Blockchain

Besides crypto currencies Blockchain has many other applications. In financial services, blockchain can be used for asset management, insurance, cross-border payments. Blockchain in cloud, can be used to facilitate distributed cloud storage. Blockchain has undeniable use cases in the Internet of Things (IoT); encrypting the smart appliances on blockchain protects individual ownership and enables transferability. Blockchain can provide a robust solution for supply chain sensors which can store, manages, protects, identify and transfers smart information for supply chain sensors. Healthcare can use blockchain smart contract to store and encrypt the personal health records with a private key which grant access only to specific individuals. Besides there, blockchain can be used for other general healthcare management, such as supervising drugs, testing results, managing healthcare supplies, and regulation compliance. Blockchain provides solutions to the critical problems of ownership rights, royalty distribution, and transparency in the music industry. Blockchain can be used for digital voting, digital identity such as passport, and other certificates and many others.

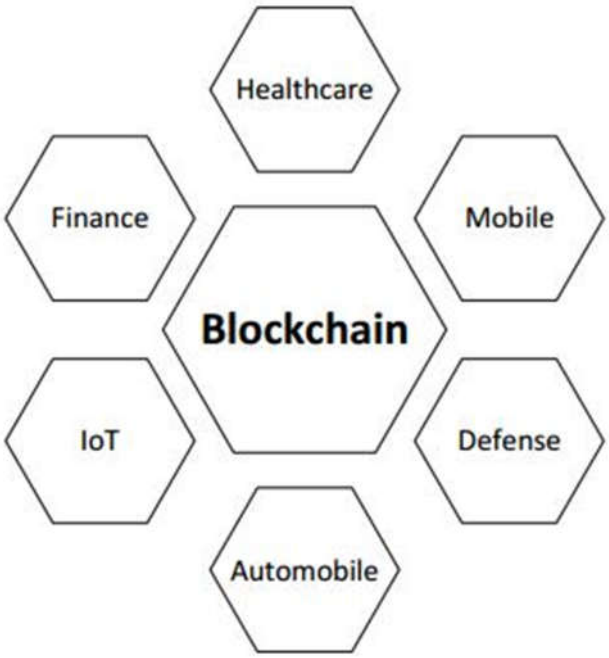

Figure 3: Blockchain Application Areas

6.Threats in Blockchain

A number of research has been conducted in this field such as Open Web Application Security Project (OWASP) enlisting common security attacks, Computer Emergency Response Teams (CERT) providing graphical representation of potential vulnerabilities, G-Cloud presenting a series of Cloud Computer Service Provider (CCSP) requirements [14], [15], [16]. Blockchain security risks do exists, and they must be recognized and mitigated if blockchain is keep its promise to transform how data is stored and acted upon. The following threat categories are identified 1. Endpoint Vulnerabilities, 2.Vendor risk. 3. Untested at Full Scale. 4. Lack of Standards and Regulation. 5. Untested code.

7.Scope For Improvement

Being an evolving technology, there will obviously a lot of scope for improvement. Firstly, the major challenge for Blockchain implementation is the lack of responsiveness and technology acquaintance. Secondly, transaction management requires database-level latency and speed to catch with industry expectations. Thirdly, security aspects which are not robust or rather not well tested and this is critical for the industry. Fourthly, involves stakeholders related to the asset management business where optimizations can be made. Fifthly, financial markets work under the lenses and directions of Regulators. Finally, the cost of transformation from the heritage systems to the new system would be very high and hence slow and gradual shift can take place, with each milestone giving more comfort and confidence to its stakeholders[6].

8.Conclusions

Blockchain is an emerging technology with software connector for decentralized and transactional data sharing across a large network. The Blockchain technology has been especially recognized to be suitable in developing nations where ensuring trust is of a major concern. In this article, a comprehensive overview on blockchain technologies including blockchain architecture and components of blockchain have been discussed. Furthermore, some applications and threats of blockchain

development and summarized some existing consensus approaches for solving the problems in blockchain are also anticipated. Nowadays blockchain based applications are springing up and in future it was planned to conduct in-depth investigations on anyone of the blockchain-based applications.

References:

1. Carmen Holotescu, " Under standing blockchain technology And How To Get Involved", The 14thInternational Scientific ConferenceeLearning and Software for EducationBucharest, April 19-20, 201810.12753/2066-026X-18-000.

2. Mahdi H. Miraz, Maaruf Ali, "Applications of Blockchain Technology beyond Cryptocurrency", Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 1, 2018.

3. V. Buterin, “On public and private blockchains,” 2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/ on-public-and-private-blockchains/.

4. Mahdi H. Miraz, Maaruf Ali, " Applications of Blockchain Technology beyond Cryptocurrency", Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 1, 2018.

5. D. Lee Kuo Chuen, Ed., Handbook of Digital Currency, 1st ed. Elsevier, 2015. [Online]. Available: http://EconPapers.repec.org/RePEc: ieee:monogr:9780128021170.

6. VIJAYA KITTU MANDA and S. S. PRASADA RAO, " Blockchain Technology for the Mutual Fund Industry", In National Seminar on Paradigm Shifts in Commerce and Management (pp. 12-17) 2018.

7. Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang , " An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", 2017 IEEE 6th International Congress on Big Data.

8. L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382–401, 1982.

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

10. C. Miguel and L. Barbara, “Practical byzantine fault tolerance,” in Proceedings of the Third Symposium on Operating Systems Design and Implementation, vol. 99, New Orleans, USA, 1999, pp. 173–186.

11. “Bitshares - your share in the decentralized exchange.” [Online]. Available: https://bitshares.org/.

12. D. Schwartz, N. Youngs, and A. Britto, “The ripple protocol consensus algorithm,” Ripple Labs Inc White Paper, vol. 5, 2014.

13. J. Kwon, “Tendermint: Consensus without mining,” URL http://tendermint. com/docs/tendermint { } v04. pdf, 2014.

14. OWASP Foundation, OWASP Top 10-2013: The the Most Critical Web Application Security Risks, 2013.

15. W. R. Claycomb and A. Nicoll, Insider Threats to Cloud Computing: Directions for New Research Challenges, in 36th Annual Computer Soft. and Appl. Conf., pp. 387–394, 2012.

16. HMGovernment, Government cloud strategy, pp. 1–24, 2011.