BLOCKCHAIN: THE FUTURE OF MONEY

[1]SamandeepKaur [2]Er. Navroz Kahlon[2]
Research Scholar(MTech),. Assistant Professor
CSE Dept
Punjabi University, Patiala.

***ABSTRACT*:** Blockchain is making the mark as the next generation financial technology because of the security that it provides in this modern information and internet age. It brings security via the authentication of the peers sharing virtual cash, along with that it also provides encryption and hashing. As per global financial industry, blockchain market will rise up to USD 20 billion by the year 2020. Also, blockchain related applications are expanding at a rapid pace. This paper includes the blockchain terms, architecture, centralized, distributed and decentralized ledger systems and various hot trends related with this technology in the current industry.Properties of public, private and consortium blockchain architecture are compared and discussed in the paper. Security related Issues in the bitcoin are discussed. As Blockchain is rising rapidly as cyber money, security challenges are also there like Blockchain Settlement, Transaction related security and Wallet Security etc., which is explained in detail in this paper. In addition, this paper also explains the different types of architecture of blockchain and the differences between them.

Index Terms: **Bitcoin, Blockchain, Cloud, Authentication, Encryption, Security, Blockchain, AWS**

I.INTRODUCTION:

Next Generation technologies have taken over almost all the industries and financial sector is no different. The use of electronic cash or virtual money is increasing at a fast pace. Blockchain is the current big thing in the financial sector as provides a secure usage of electronic cash by using peer-to-peer communication and there is no involvement of any third parties. It is also known as a public ledger system where hacking prevention is done during virtual money transfers. Because of a distributed database architecture that it has and which grows in the continuous manner, this technology is made to disable operator tampering. All the transaction related records are encrypted using a policy or method and is runs in the blockchain software. Bitcoin is one of the most popular electronic currency and it uses blockchain. As compared with the centralized[2] database against the distributed database, it is much secure to blockchain on the basis of data storage and management, where damage can be prevented. It also brings transparency because of its openness parameter and it can work great for the those applications and sectors which needs to have the disclosure of data. Because of that, it is expected to grow in large extent in financial and Internet of Things(IoT)[4-6] related applications. It finalizes the transaction[11] related record by using the work authentication process, in which person who loans the electronic cash creates a block by integrating the transactions over the network. The hash value is created by verifying it and then connects the previous block. Every block is updated periodically and they are then reflected on the electronic cash related transaction details which shares the current transaction details block. This process then brings security[1] for electronic cash transfers and adds the reliable[7] mechanism in it.

1.1 BLOCKCHAIN ARCHITECTURE

It is a chain of blocks containing particular databases integrated in a network in secure manner. It can also be described as multiple computers connected with each other and not with a centralized server making it a decentralized[12] server. The concept of blockchain can also be compared with the methodology used in applications like Google Docs or Github where multiple people work on the same documents simultaneously and can make necessary updates. Blockchain is not limited just for cryptocurrencies, but it is also used in record keeping, and digital notary systems. Fig. 1 shows the centralized, decentralized and distributed ledger illustrations using nodes:-

Centralized architecture is traditional and it used client-server model. In this model, server keeps all the information as it is easy to update. In this type of system, database is controlled by multiple administrators. In distributed blockchain architecture, every participant under the blockchain[15-17] network maintains, and update the new transactional entries. This type of architecture is not controlled by different individuals, but by every member of the blockchain based networks. In this system, every member of the blockchain network assures that records are maintained in proper order along with data security[3] and validity. Therefore, the parties which do not trust or have some trust[25] related issues reaches a common consensus.

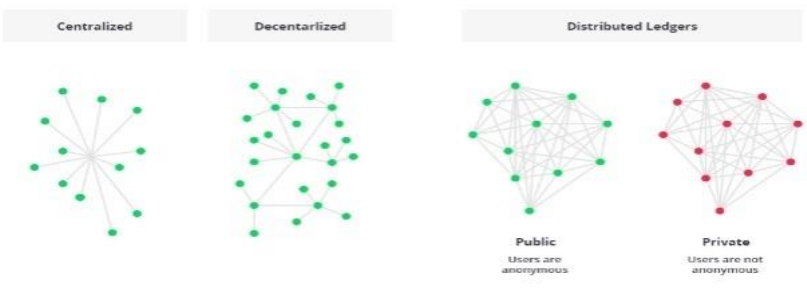

Fig. 1: BlockchainArchitecture[30]

Blockchain Architecture have three different categories explained below:-

Public Blockchain Architecture: In this type of architecture, data and system access is available to every user who wants to participate. Different examples of this type of architecture is Bitcoin[20], Etherium, etc whose blockchain systems are public.

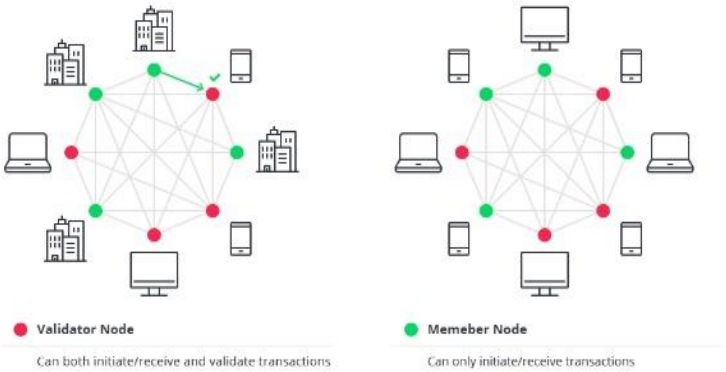

Fig. 2: Block Architecture Types[30]

1.2 PRIVATE BLOCKCHAIN ARCHITECTURE

This type of architecture is controlled by people from any particular company or organization or users who are authorized by having an invitation from the authority to participate.

Consortium Blockchain Architecture: This architecture integrates multiple organization. Functions and Policies are created in a consortium and they are controlled by the authorized users.

Property	Public	Consortium	Private
Read Permission	Public	Public or Restricted	Public or Restricted
Centralization	No	Partial	Yes
Immutability	Extremely Difficult to tamper	Can be tampered	Can be tampered
Consensus determination	Every Miner	Only nodes which are selected	Under a Single Organization
Efficiency	Low	High	High
Consensus Process	No need for permission	Needs permission	Needs Permission

Table 1: Comparing different Blockchain Architecture Categories.

Blockchain Architecture Components

Node – It can be a user or machine under the blockchain architecture.

Transaction – It is the smallest block of blockchain network consists of records etc. and serves like a purpose of the network. In case of bitcoin, it can also be said as an individual payment.

Block – It is a data structure which keeps a set of transactions distributed across all the nodes in the network.

Chain – It consists of a sequence of blocks in a particular order.

Miners – These are the particular nodes from where block validation process is performed before adding in the blockchain based architecture.

Consensus – It is the protocol which is followed to do blockchain operations.

II. LITERATURE REVIEW

Zhitao Wan, MinqiangCai, Jinqing Yang, XianghuaLin(2018) explained that blockchain based solutions are accepted worldwide. Blockchain-as-a-Service is used to fasten the deployment of blockchain. When comparing traditional blockchain service with cloud based blockchain, BaaS brings universal access and easy to implement approach. Existing BaaS erode the characteristics of decentralization and auditability. Author has proposed a total new paradigm to address different challenges in Blockchain. The proposed model provides deployable components as an integral part of Blockchain Service. The components can be implemented easily in cloud and in on-premises. Hyperledger fabric, composer based deployment clearly shows that the proposed paradigm is totally applicable for existing mainstream blockchain. Author's implementation has a prerequisite of docker clusters along with manual configuration.

Huan Chen, Liang-Jie Zhang(2018) proposed the first blockchain based service model known as FBaaS and they have implemented that over the serverless architecture. They have proposed an abstraction method used in reduction of complexity of developing business logic over blockchain networks to better the performance. This model that author has proposed can be applied to consortium and public blockchain methods. There are some issues arised in public blockchain when the model is applied and it is related to the storage oversize which can be further improved by abstraction methods.

Jin Ho Park, Jong HyukPark(2017) explained the blockchain technology as a peer-to-peer model using P2P network technology to approve the transactions. It has a distributed structure and it consumes the peer network and their computing resources. Various technical measures like proof of work and stack are deployed in order to better the security of the blockchain. According to the author, blockchain security is enhanced in continuous manner, but still there are security issues related with the blockchain as

attackers always attempts the hack the personal key of the users smartphone or computer so that they can hack the user's bitcoin. Secure tockens can be used to secure the storage of personal key. Author discussed various trends related with the blockchain security. Different security related issues have arised in the blockchain like transactional security, wallet security and software related security, also various researches have been done to resolve or reduce these issues. Anonymity is important in case of user information and it has to be ensured when blockchain is used in the cloud based environments, so that user related information is deleted when service is removed. If it is not deleted, then it can be guessed from the remaining information. Author explained different security related issues and methods to reduce them.

Blockchain Security Challenges

Blockchain is rising or implemented at a fast pace as a cyber money and is also started as blockchain-as-a-service[27-29] model by various cloud service providers like Amazon, Microsoft, IBM etc, but there are lots of challenges[8-10] related with the security that it faces in blockchain agreement, transaction, wallet etc. All these issues are explained below:

Blockchain Settlement: There is only a single blockchain as there is a sequential connection related with the generated blocks, but a blockchain[23] can be divided into two because the two blocks which are acting as the latest can be generated on the temporarily basis in case two peers succeeded in mining the solution for generation of block simultaneously.During that operation, block, which is not selected as the latest block to continue mining becomes useless. Bitcoin always select the peer[21] which has 50 percent or more mining capability. So, if an attacker has 52 percent of mining or operating capability, then a "52 percent attack", where an attacker controls the blockchain[22] and he can damage or falsify the transactions creating a big problem[26]. In recent years, GHash, which is a popular mining pool, temporarily exceeded 50 percent threshold, which forces bitcoin community to make internal and external changes to cope up with the risk.

Transaction Security: As the script which is used for inputs and outputs is a programming language having flexibility, therefore different transaction forms can also be created using such. Bitcoin[18] Contact named function applies bitcoin for current authentication and financial related services. Contract is created using a multiple signature method known as multisig[13-14]. Complexity of the script increases automatically if transaction is not configured in proper manner. Therefore, a bitcoin which uses wrongly or misconfigured script is eliminated because there is no unlocking script which can be generated.

Wallet Security: The hash value of the public key which is encrypted[19] with a pair of public and personal keys is the address of the bitcoin. So the script which is used to lock the bitcoin transaction using the address as output can be unlocked using the unlocked script which must have a signed value with the public key of the address and the personal key. Bitcoin Wallet stores the personal key in order to generate the unlock script. Therefore, any loss of information in the wallet will leads to the loss of bitcoin as the information is the necessity for using bitcoin. So, the bitcoin wallet have become one of the popular subject of attacks in bitcoin. And to secure the bitcoin wallet, the multisig must be enabled for multiple signatures. Multisig allows transaction only in case, when multiple signatures are used, it does work with a single signature. For example, if there is an multisig method used with the online bitcoin and it needs the owner signature and as well as wallet signature for the transaction to be executed, it also helps as malicious bitcoin withdrawal can be prevented as the personal key of the owner is not stored, even if the online wallet application is taken over by the hackers. We can also use biometric authentication or two-factor authentication can also be used with the multisig.

Software Security: There can be bugs in the software in use with the bitcoin[24] which can be a big security flaw. All the software can have some or more bugs, bitcoin application is no different. One of the most famous bugs in bitcoin is CVE-2010-5139, which occurred in year 2010. This bug was caused by Integer Overflow and an invalid transaction, which was 0.5 bitcoin was issued as 184 trillion bitcoin and it was included in the normal block and this problem remain unresolved for 8 hours.

IV. CONCLUSION

Blockchain is the next generation technology of finance sector and is also considered one of the emerging technologies. It removes the centralization process and make transactions using the participants who jointly stores the transaction related records, and then they approve the transactions using a P2P technology. It utilizes the peer resources and works in distributed manner. Its architecture includes a chain of blocks that contains different databases integrated together. The blockchain architecture has three different types i.e. Public, Private and Consortium related blockchain architecture. Although it is said to be the secure method of transactions of virtual money, but still there are some issues related with security present in blockchain that further divided into blockchain settlement, transaction,wallet and software security. Multisig is a security related feature which must be used in order to secure the wallet and transaction related security, it can also comprise of two-factor authentication or biometric security feature. Blockchain is currently one of the prime research topic for technical and financial industry and more and more updations related to the betterment of this technology and for expansion is carried out.

V. FUTURE SCOPE

Blockchain is an emerging technology in finance sector and uses the power of computer science, algorithms and network resources to revolutionize financial services around the world. Mining usually consume large sets of GPU and network resources to generate virtual currency and is quite secure due to its distributed nature. There are some challenges related with the blockchain like security, inefficient technology design, Energy Consuming Consensus Mechanisms, privacy etc., but the research on blockchain is also is at large scale to counter these challenges. Blockchain can be seen as the future of money and more and more innovations and research only making it more powerful

.

REFERENCES

1. Il-Kwon, L.; Young-Hyuk, K.; Jae-Gwang, L.; Jae-Pil, L. The Analysis and Countermeasures onSecurity Breach of Bitcoin. In Proceedings of the International Conference on Computational Scienceand Its Applications, Guimarães, Portugal, 30 June–3 July 2014; Springer International Publishing:Cham, Switzerland, 2014.

2. Beikverdi, A.; JooSeok, S. Trend of centralization in Bitcoin's distributed network. In Proceedings of the 201516th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking andParallel/Distributed Computing (SNPD), Takamatsu, Japan, 1–3 June 2015.
3. Bonneau, J.; Miller, A.; Clark, J.; Narayanan, A.; Kroll, J.A.; Felten, E.W. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In Proceedings of the 2015 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 17–21 May 2015.
4. Christidis, K.; Michael, D. Blockchains and Smart Contracts for the Internet of Things. IEEE Access 2016, 4, 2292–2303.
5. Huang, H.; Chen, X.; Wu, Q.; Huang, X.; Shen, J. Bitcoin-based fair payments for outsourcing computations of fog devices. Future Generation. Computer. Syst. 2016.
6. Huh, S.; Sangrae, C.; Soohyung, K. Managing IoT devices using blockchain platform. In Proceedings of the2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, Korea,19–22 February 2017.
7. Armknecht, F.; Karame, G.; Mandal, A.; Youssef, F.; Zenner, E. Ripple: Overview and Outlook. In Trust andTrustworthy Computing; Conti, M., Schunter, M., Askoxylakis, I., Eds.; Springer International Publishing:Cham, Switzerland, 2015; pp. 163–180.
8. Vasek, M.; Moore, T. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits ofVirtual Currency Scams. In Proceedings of the International Conference on Financial Cryptography andData Security, San Juan, Puerto Rico, 26–30 January 2015; Springer: Berlin/Heidelberg, Germany, 2015.
9. Zhang, J.; Nian, X.; Xin, H. A Secure System For Pervasive Social Network-based Healthcare. IEEE Access2016, 4, 9239–9250.
10. Singh, S.; Jeong, Y.-S.; Park, J.H. A survey on cloud computing security: Issues, threats, and solutions.J. Network. Computer. Applications. 2016, 75, 200–222.
11. Kaskaloglu, K. Near zero Bitcoin transaction fees cannot last forever. In Proceedings of the InternationalConference on Digital Security and Forensics (DigitalSec2014), The Society of Digital Information andWireless Communication, Ostrava, Czech Republic, 24–26 June 2014.
12. Ziegeldorf, J.H.; Matzutt, R.; Henze, M.; Grossmann, F.;Wehrle, K. Secure and anonymous decentralizedBitcoin mixing. Future Generation. Computer. Syst. 2016.
13. Aitzhan, N.Z.; Davor, S. Security and Privacy in Decentralized Energy Trading through Multi-signatures,Blockchain and Anonymous Messaging Streams. IEEE Trans. Dependable Security. Computing. 2016, 99.
14. Heilman, E.; Foteini, B.; Sharon, G. Blindly signed contracts: Anonymous on-blockchain and off-blockchainbitcoin transactions. In Proceedings of the International Conference on Financial Cryptography and DataSecurity, Christ Church, Barbados, 22–26 February 2016; Springer: Berlin/Heidelberg, Germany, 2016.
15. Natoli, C.; Gramoli, V. The blockchain anomaly. In Proceedings of the 2016 IEEE 15th International Symposiumon Network Computing and Applications (NCA), Cambridge, MA, USA, 31 October–2 November 2016.
16. Shi, N. A new proof-of-work mechanism for bitcoin. Financ. Innov. **2016**, 2, 31.
17. Swan, M. Blockchain: Blueprint for a New Economy; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015.
18. Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies.IEEE Commun. Surv. Tutor. **2015**, 18, 2084–2123.
19. Wressnegger, C.; Freeman, K.; Yamaguchi, F.; Rieck, K. Automatically Inferring Malware Signatures forAnti-Virus Assisted Attacks. In Proceedings of the 2017 ACM on Asia Conference on Computer andCommunications Security, Abu Dhabi, UAE, 02–06 April 2017.
20. Decker, C.; Roger, W. Information propagation in the bitcoin network. In Proceedings of the 2013 IEEEThirteenth International Conference on Peer-to-Peer Computing (P2P), Trento, Italy, 9–11 September 2013.
21. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Available online: https://bitcoin.org/en/bitcoin-paper
22. Bozic, N.; Guy, P.; Stefano, S. A tutorial on blockchain and applications to secure network control-planes. SCNS IEEE **2016**.
23. Bradbury, D. The problem with Bitcoin. Compute. Fraud Secure. **2013**, 11, 5–8.
24. Paul, G.; Sarkar, P.; Mukherjee, S. Towards a more democratic mining in bitcoins. In Proceedings ofthe International Conference on Information Systems Security, Hyderabad, India, 16–20 December 2014;Springer International Publishing: Cham, Switzerland, 2014.
25. Bamert, T.; Decker, C.; Wattenhofer, R.; Welten, S. BlueWallet: The Secure BitcoinWallet. In Security andTrust Management; Mauw, S., Jensen, C., Eds.; Springer International Publishing: Cham, Switzerland, 2014;pp. 65–80.
26. Anceaume, E.; Lajoie-Mazenc, T.; Ludinard, R.; Sericola, B. Safety analysis of Bitcoin improvement proposals.In Proceedings of the 2016 IEEE 15th International Symposium on Network Computing and Applications(NCA), Cambridge, MA, USA, 31 October–2 November 2016.
27. Huan Chen, Liang-Jie Zhang, "FBaaS: Functional Blockchain as a Service", National Engineering Research Center for Supporting Software of Enterprise Internet Service, ICBC 2018, LNCS 10974, pp. 243–250, 2018.
28. Zhitao Wan, MinqiangCai, Jinqing Yang, Xianghua Lin, "A Novel Blockchain as a Service Paradigm", ICBC 2018, LNCS 10974, pp. 267–273, 2018.
29. Jin Ho Park, Jong Hyuk Park, "Blockchain Security in Cloud Computing: Use Cases, Challenges and Solutions", Symmetry 2017, 9, 164.
30. AnastasiiaLastovetska, "Blockchain Architecture" Available Online: https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture