Proceedings of the International Conference on Inventive Computation Technologies (ICICT-2018)
IEEE Xplore Part Number: CFP18F70-ART; ISBN:978-1-5386-4985-5

Blockchain Technology: A Novel Approach in Information Security Research

Sandeep Shiravale
School of Computer Engineering and Technology
MIT Academy of Engineering
Pune, India
scshiravale@it.maepune.ac.in

Dr.V.Shrikanth
Dean-Skill Development,
Professor, Department of CSE
KLEF, India
vsrikanth@kluniversity.in

***Abstract*—A blockchain technology originally block chain, is the recent development in the industry gaining great ground. It is the concept by which the digital information is distributed across the network but it is not duplicated. This growing list of records, called blocks, is associated with a hash function. The technology allows any node which is part of ant network to join or leave the chain process execution and the execution process is independent on the identification of each network. Every network can update their entries into a record of, and they can control how the stated records are further processed. This technology is introduced a decade ago considering a concept of unique currency but till date it is facing certain technical challenges like scalability, block size, network propagation, and security and so on. The paper discusses about the challenges, opportunities and recent advances in this area.**

Keywords—blockchain, architecture, challenges, future scope

I. INTRODUCTION

Blockchain is a next generation technology introduced a decade ago and still under development process. Blockchain can be stated as an entity open to everyone, in which all the network nodes participating in the chain process complete certain transactions and are stored in the form of a chain of blocks. This chain grows as the number of network nodes increases and their consistent transactions create new blocks which get appended. Blockchain can work in a decentralized environment and can be described as follows. A user in a network initiates a transaction which is broadcasted further in the associated networks. All the associated networks verify this transaction, the user details and the authenticity by using various cryptographic algorithms. After the verification process, the transactions are integrated with the other transactions made by different network nodes and a new block of data is updated in the records named ledger. This newly created block is added to the blockchain thus making it permanent and unalterable. The entire transaction gets completed. [1]

This technology is enabled by integrating different core technologies like cryptography, digital signatures and distributed databases. All transactions are completed in a decentralized fashion thus resulting in effective resource management and improving the efficiency.

Currency transactions between end users, different organizations or through third parties are generally centralized and can be controlled. To complete an online transaction like purchase or currency transfer, it is necessary to involve a financial organization such as a credit card company. This company can charge a transaction amount. The complete process can face certain security challenges as there are many parties involved. Blockchain technology has been developed to solve this issue. The major focus is to develop a system by which there is no necessity of a third party company.

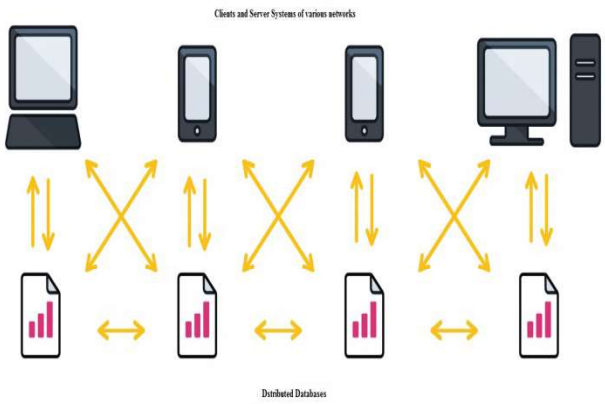

Fig. 1The blockchain Technology

The figure 1 describes the blockchain technology. The clients which are part of different networks can work with different databases. The blockchain database is thus spread across many locations, making the maintained records completely public and easily verifiable. There is no centralized version of this information giving rise to a secure environment.

The blockchains are built from three different technologies. A) Peer to Peer Network which helps in creating a chain of blocks, B) Asymmetric key cryptography where we can have two different keys viz. public and private and C) A program which implements blockchain protocol. Each completed transaction is updated and this information shared and available to all the network nodes. The system is thus more transparent and better equipped. [4]

Blockchain can best be described with the help of Google Docs. A specific document uploaded on Google Docs can be accessed by many individuals but the simultaneous editing

by the individual on the same record may not be possible. This is how the databases work today. Blockchain is one of the suitable and secure methods for completing transactions though it is facing certain challenges. [5]

II. ARCHITECTURE

A blockchain works like a mesh network were all the blocks are linked to each other. The nodes which are part of this network define and agree upon a shared state of data and follow certain constraints. Each block which is part of the shared state makes change to its current state. This technology can be categorized as Public and Private.

Public blockchains can complete transactions from any network. These transactions can be monitored and audited by any third party network and every node is equally important. Each transaction is validated and authorized by each of its constituent nodes via the chain's agreement procedure. This network is completely open and anyone can participate. This concept can be Though Public blokchain offer enhanced security, huge computational power is required for completing the transactions and there may not be privacy maintained.

Private blockchain is a closed network. It is just like a private network of any company where the company creates its own blockchain which is accessed by the company employees. They follow peer to peer architecture having transaction constraints. If there is any need for the data on a chain to be restricted, it can be done by changing the permission settings. Private blockchain maintains privacy, it needs less computational power but on the other hand, they are less secure. [6]
The architecture of a blockchain is described as below.

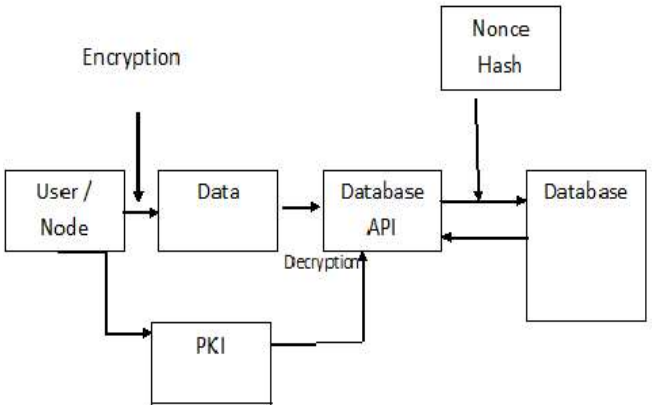

Fig.2 the Architecture

The figure 2 indicates the architecture of a blockchain technology. Blocks function like data structures which can integrate multiple transactions and distribute further to the other blocks. Each block contains a header which includes the following.

(i) Block version

(ii) Previous block header hash:

(iii) Merkle root hash

(iv) Time

(v) nBits

(vi) Nonce

The blocks are created by a process called mining. It is the process of adding transactions to the Ledger. Further, a common currency called bitcoin which do not require third party verification can develop peer to peer economy. The architecture can further be exemplified with the help of following example.

We can talk about direct money transfer without the need of a third party like a Bank. With the help of secure cryptographic algorithms, blockchain establishes decentralized database which can also be termed as a Digital Ledger. All nodes which are part of this network can view this ledger as well as all the transactions. The following steps are involved in one transaction.[7]

a) Person A wishes to transfer money using bitcoin. He needs to create a bitcoin wallet. The wallet informs the network about Person A, B and the amount.

b) The transaction is created with digital signature with the help of wallet of a person A. This transaction is now part of the chain.

c) This transaction is represented as a block. It is then advertised to all the nodes. Nodes will verify and after the verification process the node broadcast the block. The nodes accept the block and create the next one with the help of hash value of the previously accepted block. The miners complete the process and the stated block's ownership is transferred in the account of person B.

d) Person B receives the fund and the transaction is recorded. [8, 9]

III. TECHNICAL CHALLENGES

Blockchain technology is slowly gaining ground in the global business world but the security liabilities are also equally increasing. The leakage of information, public ledgers, mobile applications and operating system level security are all new challenges that have been identified. The following can be the risk factors or challenges while we integrate this technology in the global networks.

Efficiency:

Blockchains produce lots of data in the form of block information, transaction data, and hash values and so on. Some of the produced information may not be useful thus utilizing the network resources. The efficiency thus gets degraded affecting the performance of a particular chain. It is necessary to remove unwanted information so that the duplicate records should not utilize the storage thus

affecting the performance and can create a threat to the entire system.

Vulnerability:

Decentralization and ease of access has created some unexpected issues. As any node in the network can update the transactions, bitcoin transactions can lead to unwanted market trading. The entire operation is much energy consuming thus affecting many other factors like electricity making the entire environment vulnerable.

Private Key security:

The asymmetric key cryptography deals with two different keys. Public key which is known to everyone and the sender encrypts the data by using it. The other key is the private key which every individual maintains. The receiver decrypts the encrypted information with the help of the same. If the private key is hacked, the entire process can come to a halt thus blockchain cannot perform. Tracking and finding the right details becomes a challenge.

Complexity:

The technology includes chain of blocks which are created by nodes of different networks. If there is a small mistake in configuration, the entire transaction may not be successful thus creating complex situation. The best example is duplicate records which are utilizing the storage space as well as the network resources.

Latency:

To implement sufficient security for each transaction, it is necessary to maintain proper timeframe to complete one transaction. This technology implements a chain of blocks thus the records are consistently growing. This can give rise to latency as for an efficient secure transaction, more time is invested per transaction thus increasing the latency of the network.

Size and bandwidth:

The size and the use of network bandwidth is a big challenge. As the blocks are added in the chain, the size always grows thus consuming the bandwidth of the network. There is no predication on how many blocks will get added up thus this can be a big challenge.

Wasted resources:

The resources are heavily used as the chain grows. We even talks about the single currency thus giving rise to a concept called Proof-of-Work effort. With Proof-of-Work, the miners create group of transactions on a public ledger.

Politics:

The concept talks about using a common crypto currency. Each country is using own currency thus making this effort difficult to implement. [8],[9]

IV. PROPOSED WORK

There are many technical challenges while designing blockchain. One of the focused methods here is Storage optimization. The network protocol stack is described here.

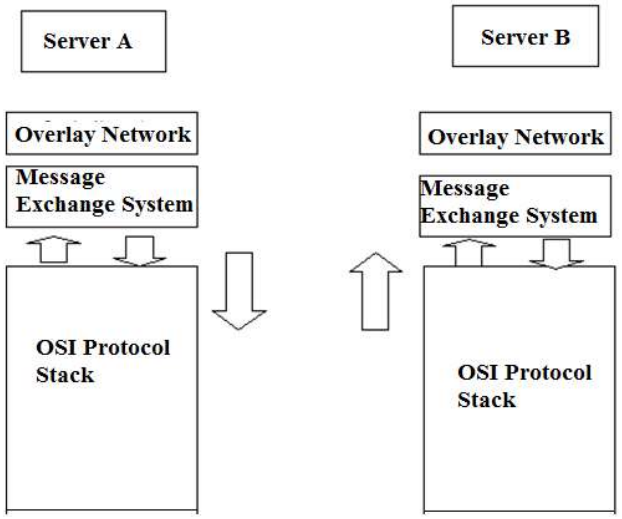

Fig. 3 Network Protocol Stack

The overlay network which works as a front end and the message exchange system. This network helps in communication and message exchanges. The message exchange system is directly associated with the OSI protocol stack. In the complete process, a novel cryptocurrency method can be defined. In this, older transaction records can be eliminated by the network nodes and a new database can be used to hold the non-empty addresses. The node doesn't need to maintain all the records to check whether a transaction is legitimate. The small networks having less computational power, limited resources can outsource their computations. The beneath network infrastructure will ensures that the computation results are correct.

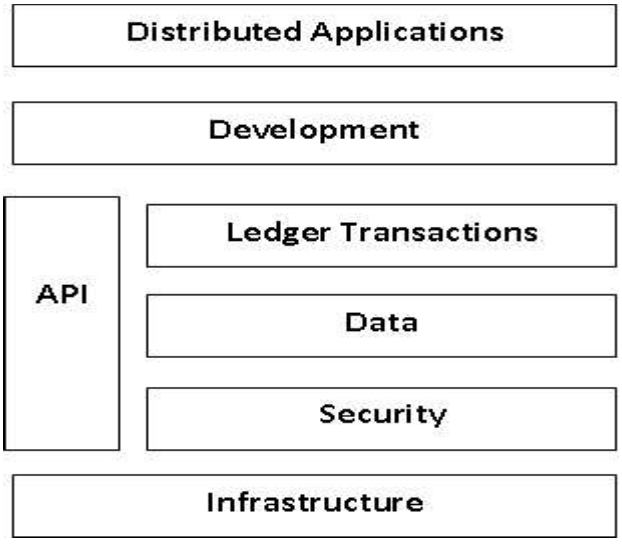

Fig. 4 Proposed Architecture

The Figure 4 talks about the proposed architecture that can eliminate the issue of network congestion. The network infrastructure is the base running the distributed ledger. The security module built above includes Identity management, Permissions and Encryption services. The security module is an important module which can describe the services that can be offered to the entire chain. Identity management manages all the incoming requests from the authorized nodes. The incoming requests are verified and then send for the permission request. After receiving the permissions from the network, the data is encrypted and further added to the chain in the form of a block. [10]

The data module talks about Secure Data Access Services, Intra-chain Services, and Off-chain Access Services. Those services securely store and retrieve available information, and ensure that only white listed nodes will exchange the information. Data module must work in synchronization with the security module as the chain of blocks is interconnected and loss of one single block can again create vulnerability. The Ledger Services validates block-based storage of transactions. Blocks are also validated for the inclusion in the chain. The development environment comprises of various development tools for writing, documenting, testing, deploying and monitoring various distributed applications. It also has development libraries as well as contract services. The Programming Interfaces enables integration of existing environment to ensure adoption of Blockchain-based solutions.

The major protocol used in the transaction is Bitcoin NG (Next Generation). This protocol ensures that the transactions are done serially and follows the norms of a chain. Throughput and Latency are the two major areas of concern which can create blockage while completing any transaction. The protocol improves the situation by ensuring an election process that selects a leader. The protocol divides entire timeframe into small sections called as a period. It thus helps in properly managing the available bandwidth without affecting the performance of the network. [13]

V. DISCUSSION

Blockchain technology is gaining ground in the market. Multiple domains like Human Resources, Accounting, Retail and many more are slowly using this technology which is providing great returns. It is been supported by cyber security due to the recent outbreaks of many threats like ransomware. Very soon the industry will start using a common currency like bitcoin for their regular transactions thus eliminating the barricade of a third party. [13]

VI. CONCLUSION

Blockchain is the technology of the future which has the important features like decentralized infrastructure, persistency, anonymity, auditability and peer-to-peer nature. It talks about common currency and not limited to bitcoin. Blockchain will transform traditional transaction which includes a third party with the help of its key characteristics. Network Security is an interesting area where blockchain need to focus on. There are still certain challenges which this technology is facing and it is being addressed with high quality research.

VII. REFERENCES

[1] Bill Buchanan, Naseem Naqvi, "Building the Future of EU: Moving Forward with International Collaboration on Blockchain," The Journal of The British Blockchain Association, pp. 1-4, 27 April 2018.

[2] Jennifer Li, David Greenwood, Mohamad Kassem "Blockchain in the built environment: analysing current applications and developing an emergent framework" Creative Construction Conference 2018, CCC 2018, 30 June - 3 July 2018

[3] Benjamin Adams, Martin Tomko "A Critical Look at Cryptogovernance of the Real World: Challenges for Spatial Representation and Uncertainty on the Blockchain" 10th International Conference on Geographic Information Science (GIScience 2018). Article No. 18; pp. 18:1–18:6 2018

[4] Mandrita Banerjee, JungheeLee, Kim-Kwang Raymond Choo, "A blockchain future for internet of things security: a position paper" Digital Communications and Networks Volume 4, Issue 3, Pages 149-160 August 2018

[5] Ioannis Konstantinidis, Georgios Siaminos, Christos Timplalexis, Panagiotis Zervas, Vassilios Peristeras, Stefan Decker "Blockchain for Business Applications: A Systematic Literature Review" International Conference on Business Information Systems BIS 2018: Business Information Systems pp 384-399, 2018

[6] Ali Dorri, Salil S. Kanhere, Raja Jurdak "Towards an Optimized BlockChain for IoT" IoTDI 2017, April 2017, Pittsburgh, PA USA, 173-178, 2017

[7] Bin Liu, Xiao Liang Yu, Shiping Chen, Xiwei Xu, Liming Zhu "Blockchain based Data Integrity Service Framework for IoT data" IEEE 24th International Conference on Web Service 978-1-5386-0752-7/17 $31.00 © 2017 IEEE, 468-475, 2017

[8] Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park, Kyung-Hyune Rhee "A Critical Review of Blockchain and Its Current Applications" International Conference on Electrical Engineering and Computer Science (ICECOS) 2017, 109-113, 2017

[9] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, Huaimin Wang "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends" IEEE 6th International Congress on Big Data 978-1-5386-1996-4/17 $31.00, 557-564, 2017

[10] Yanqi Zhao, Yannan Li, Qilin Mu, Bo Yang, Yong Yu, "Secure Pub-Sub: Blockchain-Based Fair Payment With Reputation for Reliable Cyber Physical Systems" special section on research challenges and opportunities in security and privacy of blockchain technologies, Digital Object Identifier 10.1109/ACCESS.2018.2799205, 12295-12303, 2017

[11] Tianyu Yang, Qinglai Guo, Xue Tai "Applying Blockchain Technology to Decentrlized Operation in Future Energy internet" 978-1-5386-1427-3/17, pp 1-5, 2017

[12] Shehar Bano, Mustafa al-Bassam, and George Danezis, "The Road to Scalable Blockchain Designs" www.usenix.org, vol. 42, no. 4, 31-36, 2017

[13] Kevin O'Leary, "Exploring the Application of Blockchain Technology to Combat the Effects of Social Loafing in Cross Functional Group Projects" 2017

[14] https://www.vamsitalkstech.com/?p=1615

[15] https://www.pluralsight.com/guides/blockchain-architecture

[16] https://www.linkedin.com/pulse/proposed-blockchain-reference-architecture-mike-jacobs