International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7 Issue-4, September 2018

Blockchain Technology - A Sturdy Protective Shield

L. Venkateswara Kiran, R. Bala Dinakar, P. Siva Prasad

Abstract: Blockchain Technology, very popular buzz word after the tremendous success of Bitcoin. An immutable ledger in Blockchain makesthe transactions in decentralized manner. Blockchainapplications cover different fields like financial services, reputation system and Internet of Things and many more. Even though there are so many challenges forBlockchain technology like scalability and security to be overcome. This paper briefs an overview on Blockchain technology. We are providing an overview of Blockchain architecture, security, and technical challenges are precisely listed. We are also brief the future trends for Blockchain.

Keywords: We are also brief the future trends for Blockchain.

I. INTRODUCTION

Now a days the word Crypto currency is very popular and we are listening frequently in Industry and Academia. Bitcoin is very famous and most successful cryptocurrency. In 2016 it reaches 10 billion dollars market. The transactions in Bitcoin never depends on the thirdparty because it have a specially designed storage structure. The technology which we use to develop cryptocurrency is Blockchain. Blockchain was first started in 2009.It is like a public ledger and all the transactions are stored in the form of blocks. In Block Chain new blocks are appended continuously and it increases in size. The peculiar characteristics of Blockchain are decentralization, persistency, anonymity and auditability. With these characteristics Blockchain reduces cost and improves the efficiency of the application. For the financial services like digits assets, remittance and online payments, Block chain can be used because the payments in this technology never use banks and third party. We can use Blockchain in other fields like IOT, reputation systems and security services.

Blockchain never destroy. We can't delete the transactions in Blockchain. With this reason it can be used in reliable businesses. It is distributed so, can avoid single point failure.

II. FEATURES

The features of Blockchain include

Collaboration among competitors
Flexibility
Resilience
Distributed Verification

a) Collaboration among competitors

Companies which are under competition with one another have a common platform in which without fear those can collaborate openly.

b) Flexibility

Blockchain doesn't concentrate on the participant and their identity and whether they remain the same over time. The positions of the participants continuously shifting.

c) Resilience

Diversity of participants participate in Blockchain. Each participant has full copy of data. This redundancy makes the system resilient to attacks.

d) Distributed Verification

Many parties can verify program and data stored in different locations independent of one another.

III. HOW BLOCKCHAIN ARCHITECTURE WORKS

Blockchain uses peer-to-peer network to validate the transactions. It permits users to create and check the transactions without central authority.

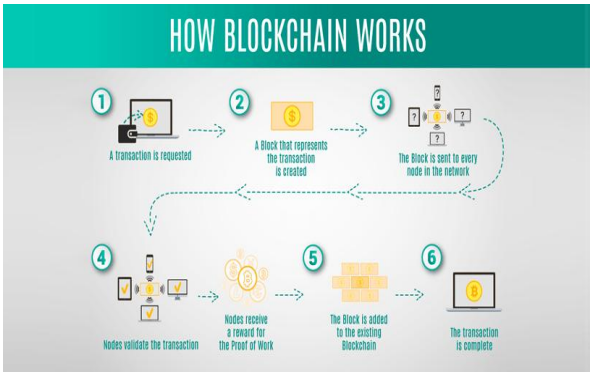

Fig. 1: Blockchain Architecture

Categorization of Blockchain Technology

a. Public Blockchain

Public Blockchain network is an open ended network and anybody can participate without getting permission. The participants execute consensus protocol and maintain the shared public ledger. It is more secure and maintains low privacy than private Blockchain.

Revised Manuscript Received on 30 September 2018.
***** Correspondence Author
L. Venkateswara Kiran, Assistant Professor, Department of CA, Godavari Institute of Engineering and Technology, Rajahmundry (A.P), India
R. Bala Dinakar, Assistant Professor, Department of CA, Godavari Institute of Engineering and Technology, Rajahmundry (A.P), India
P. Siva Prasad, Assistant Professor, Department of CA, Godavari Institute of Engineering and Technology, Rajahmundry (A.P), India

b. Private Blockchain

An invitation is required to participate in Private Blockchain. Private Blockchain put restrictions to the participants. Definitely it increases the privacy and less effort is required to execute consensus.Private Blockchain is less secure than Public Blockchain.

Public vs. Private Blockchain	
Different	**Same**
Permission model	Peer-to-peer architecture
Native cryptocurrency	Public key cryptography
The Blockchain	Transaction constraints

Fig.2: Public vs Private blockchain

High level view of Blockchain

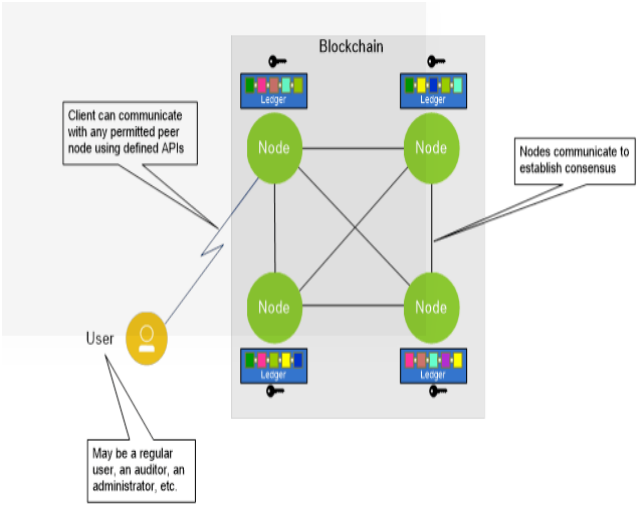

Fig.3: High level view of blockchain

Every node in Blockchain consists of a local copy of leger. In most of the systems these nodes belongs to different organizations. If these different nodes want to communicate each other they could gain the agreement on the contents of the ledger. For that no need of the central authority to validate the transctions.

There are different algorithms developed for gaining the agreement which is called consensus. To perform the operations provided by chain, users must send the transaction request. After completion of the transaction, the record of the transaction is added to one or more number of ledgers and those are not modified and destroy. This is the striking property of the Blockchain which is called immutability.

IV. SECURITY

A lot of data structures are available in market to provide security for data but, Blockchain is totally different. In Blockchain technology, there is no centralized database. For a transaction, the data will be decentralized in to different nodes available in the network. The information in all the nodes will formed as a block. The immediate transaction on the same data again formed as a block. These blocks are linked together. Nobody can delete the information available in the blocks. The users can access the information but not delete it. If anybody try to delete the information in one block, the same will be available in another block. Access rights are changed from customers to users.

In traditional approach, the data in terms of files, can be divided into blocks and apply one single formula to encrypt. But in Blockchain, different computers in the network do the above job. Two computers encrypt one block with an algorithm, the other two computers use different algorithm to encrypt the data. The data related to one file divided in to different blocks and encrypt individually and make a Blockchain. Even one block data get leaked, the other block data is safe.

For the above reasons most of the trading organizations, insurance companies, hospitals and many more shift their focus to Blockchain technology.

V.CONSENSUS ALGORITHMS

A consensus protocol has the following features depends on these features its efficiency can be determined.

- Security
- Real-time value
- Fault tolerance

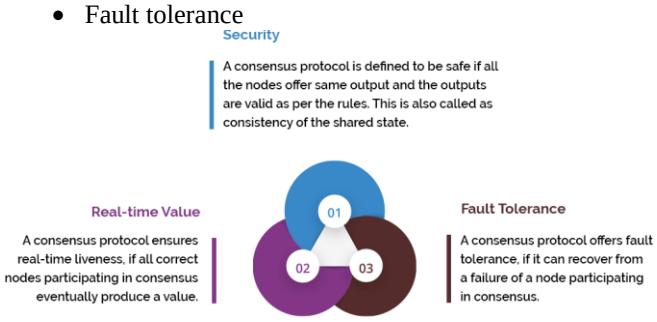

Fig.4: Consensus protocol features

The Blockchain network users develop the system which agreed the validity of the things that are added to the ledger. A consensus is needed to reach the maximum nodes in the Blockchain.

The main goal of the consensus protocol is to allow the node to offer a validated transaction which is added to the ledger. This prevents addition of blocks and incorrect transactions from the miners. There are many types of mechanisms to be used depends on the type of network. Let's discuss a few mechanisms.

Proof-of-Work (PoW)

PoW is the frequently used and very strong consensus mechanism for blockchain technology. In PoWminer solve the complex puzzles on the new block before approving the block to the ledger. After the puzzle solved, the solution is forwarded to the remaining miners in the network and verified by them before accepted to their respective copies of the ledger. After verification approved transactions are finalized by the minors. If any user try to make a duplicate transaction, it will visible in the network and that transaction is never accepted.

Proof-of-Stake (PoS)

Proof of Stake is an alternate approach for PoW which requires a few CPU computations for mining. When compared to PoW, PoS process is quite different.

In PoS, new block creator is chosen in a deterministic way, depending on its wealth. That means there is no block reward in PoS.Therefore, the miners take the transaction fees. The implementation of PoS mechanism issomehow a complex task.

Delegated Proof-of-Stake (DPoS)

In DPoS token holders don't work on the validity of the blocks by themselves, but they choose delegates to do the validation. There are 21-100 selected delegates in DPoS system. The selected delegates are changed and assigned an order to deliver their blocks. If the delegates publish invalid transactions, the token holders replace them with other selected delegates. In DPoS, miners are collaboratingfor the development of blocks which is not happening in PoW and PoS.

Byzantine Fault Tolerance (BFT)

BFT is used to fix the issue of unreliable node. The Blockchain reliability breaks down when any member sends inconsistent information of the transactions to others.There is no central authority is available which can correct that inconsistency. To solve this problem, PoW offers BFT through its processing power. To identify the true transaction, nodes will vote regularly.PoS works with BFT is the best approach to approving Blockchain transactions..

Practical Byzantine Fault Tolerance (PBFT)

Each 'general' manages an internal state in PBFTmechanism. A general use the received message in connection with their internal state to start a computation process. This process enquire the each general about the opinion on the message.After getting a conclusion, the general shares the decision with others in the system. The consensus decision is build based on the total decisions submitted by all the generals.

SIEVE

HyperledgerFabric uses SIEVE consensus mechanism. This mechanism allows the network to remove non-deterministic requests. It achieves consensus on the output of the transactions.

Proof-of-Weight (PoW)

PoW algorithm works based on Algorand consensus model. The idea behind PoS is the percentage of tokens in the network represents the probability of discovering the next block. Proof of Reputation and Proof of Space are the some of its implementations.

VI. TECHNICAL CHALLENGES

Most of the companies and developers are trying to broaden the functionality of Blockchain technology. To make the Blockchain technology as outstand, important technical developments needed. In addition to that there is an uncertainty as how Blockchain technology is suitable for current regulatory schemes.

Security and Reliability

For all the public Blockchain applications, the coding and designing parts are available publicly. Even though, their updates and releases are not properly validated for security and reliability. Due to this, things like bugs, vulnerabilities and coding errors may cause and leads to huge loss to the users.

Scaling

Any Blockchain present now can't support huge amount of traffic. For example, Bitcoin can process seven transactions per second, and Ethereum can handle only 20 transactions per second. It is very difficult to implement Blockchain technology for the transaction networks like Visa and MasterCard, which requires thousands of card swipes per second. If any application propose Blockchain require high data storage capacity.Current state of the technology is not feasible for huge data storage capacity.

Accessibility

The users of Blockchain applications granted direct access to the information stored, rather than logging their account which was controlled by a third party. So, the responsibility of the users in Blockchain is maintaining the security of their cryptographic keys. An educational campaign is required for this new paradigm. But, unfortunately, the efforts are not sufficient. Input/outputcertificate of authenticity and compliance is one method for maintaining security practise.

Regulation

It is necessary to fill the communication gap between Blockchain developers and regulators. Both the regulators and Blockchain developers should aware about how technology works and what regulations pertain to its deployment.

VII. CURRENT TRENDS AND FUTURE DIRECTIONS

Over the last few years, the new technological development in the tech industry is Blockchain technology. It was developed to boom crypto currencies originally, but that doesn't sense that it is not suitable for other applications. Let's have a look a few trends that sets a shape in 2018 and beyond.

Internet of Things

Internet of things connect devices ranging from wearable devices to any type of inter-connected device that you can imagine. All these inter connected devices need some sort of system that makes their data interoperable. That is the area where Blockchain comes in, but different manufacturers come together and agree the required Blockchain specifications.

Increased use of smart contracts

Using smart contracts we can bypass third parties and create airtight agreements. Industries like finance, real estate, academia and logistics are thinking to implement smart contracts in their applications. These contracts provide high level of transparency and security. Contracts will be verified and signed in a secure environment.

Content streaming

Using Blockchain technology in content streaming companies like Netflix and Amazon prime is useful because they requires secured data storage and provision of interoperability. But it requires large amounts of processing power.

We are now in the beginning days of Blockchain technology, and yet to see its impact over different applications we are using. At present, visualize the future of Blockchain is just like predict the future of the WWW in 1993.

VIII. CONCLUSION

In this paper, we present an overview on blockchain. We first give an overview of blockchain features and architecture. Later we discuss security and consensus algorithms used in blockchain. Furthermore, we listed major challenges in blockchain development. We proposed some possible future directions. Blockchain based applications are increases gradually and we are planning to do deep investigation on those applications.

REFERENCES

1. State of blockchain q1 2016: Blockchain fundingOvertakes bitcoin," 2016. [Online]. available:http://www.coindesk.com/state-of-blockchain-q1-2016/
2. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online].available: https://bitcoin.org/bitcoin.pdf
3. G. Foroglou and A.-L. Tsilidou, "Further applications of theblockchain," 2015.
4. A. Kosba, A. Miller, E. Shi, Z. Wen, and C Papamanthou,"Hawk: The blockchain model of cryptography and privacy- preserving smartcontracts," in Proceedings of IEEE Symposium on Security and Privacy (SP), SanJose, CA,USA, 2016, pp. 839–858.
5. M. Sharples and J. Domingue, "The blockchain and kudos:a distributed system for educational record, reputation and reward," inProceedings of 11th European Conference onTechnology Enhanced Learning (EC- TEL2015), Lyon,France, 2015, pp. 490–496.
6. C. Noyes, "Bitav: Fast anti-malware by Distributedblockchain consensus and feedforward scanning," arXiv preprint arXiv:1601.01405, 2016.
7. I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436–454.
8. F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications SurveysTutorials, vol. 18, no.3, pp. 2084–2123, 2016.
9. NRI, "Survey on blockchain technologies Andrelated services," Tech.Rep., 2015.
10. V. Buterin, "A next-generation smart ContractAnd decentralized application platform,"white paper, 2014.
11. V. Buterin, "On public and private blockchains," 2015.[Online]. Available: https:// blog. ethereum. org/2015/08/07/ on-public-and-private-blockchains/
12. S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proofof-stake," Self- Published Paper, August, vol. 19, 2012.
13. D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," Ripple Labs Inc White Paper, vol. 5, 2014.
14. J. Kwon, "Tendermint: Consensus without mining," URLhttp://tendermint . com/docs/tendermint { } v04. pdf, 2014.
15. S. King, "Primecoin: Cryptocurrency with prime numberproof-ofwork," July 7th, 2013.
16. G. Wood, "Ethereum: A secure decentralized generalised transaction ledger," Ethereum Project Yellow Paper, 2014.
17. D. Mazieres, "The stellar consensus protocol:a federated model for internet-level consensus," Stellar Development Foundation, 2015.
18. "Antshares digital assets for everyone," 2016. [Online]Available: https://www.antshares.org
19. C. Decker, J. Seidel, and R. Wattenhofer, "Bitcoin meets strong consistency," in Proceedings of the 17th International Conference on Distributed Computing and Networking (ICDCN). Singapore, Singapore: ACM, 2016.
20. D. Kraft, "Difficulty control for blockchain- basedconsensus systems," Peer-to-Peer Networking and Applications, vol. 9, no. 2, Pp.397–413, 2016.
21. A. Chepurnoy, M. Larangeira, and A Ojiganov, "Aprunableblockchain Consensusprotocol based on non-interactive proofs ofpast states retrievability," arXiv preprintarXiv:1603.07926, 2016.