Review on Blockchain Technology

Shankar Pawar
Ajeenkya D Y Patil University, Pune

Aditya Saraf
Ajeenkya D Y Patil University, Pune

Sanket Parade
Ajeenkya D Y Patil University, Pune

Shabnam Sharma
iNurture Education Solutions, Bangalore

ABSTRACT

The Blockchain technology is a recognized breakthrough of recent times. It has already changed people’s lifestyle in many areas due to its great influence on business and industry and is still believed to have continuous impact in many fields. Although blockchain may bring in reliable and convenient services, the security challenges and issues in newer innovation is one of the major areas of concern. The objective of this research work is to support the adoption of this innovation, by extensively explaining the concept of Blockchain, analyzing its advantages and disadvantages and judging its actual added value to a business.

Keywords

Blockchain, Ethereum

1. INTRODUCTION

Blockchain technology became widely popular after its applicability in the form of Bitcoins. Bitcoin is digital currency (just like money) which can be used to trade any item on the internet. It is often considered as a disruptive innovation as it compensates for the inefficiency and irregularities of the traditional banking system. But since everything as it's set of downsides, this also stands true for blockchain technology.

As we continuously use these tools in our everyday life, we as a society become vulnerable to malicious attacks from cyber criminals. A recent study shows almost 51% of attacks is a classic security in Bitcoin that hacker try to take control the system's mechanism, using the same technology base.

In this paper, quick look at the concept of blockchain, its applications in present times and services that they offer and finally mentioning the security issues and those challenges that need to overcome, are mentioned.

2. WORKING OF BLOCKCHAIN

Blockchain has 3 main elements in working process:

a. Data

b. Hash

c. Hash of the previous value

The steps for working process of blockchain are as follows:

1. Each block contains a piece of data and computed hash of block. Computed hash of one block will act as seed for immediate next block.

2. The data that is stored inside a block depends on the type of blockchain. For example, bitcoin stores the details about a transaction. The details include sender’s data, receiver’s and the amount of coins.

3. A block also consists of pre-computed hash value. This pre-computed hash value offers similar functionality as offered using fingerprint as authentication mechanism. It helps in identification of a block, will help in assessing all its contents, as it is always unique.

4. Once a block is created, its hash is being calculated. If data of block gets updated, it will also lead to the manipulation in hash value.

5. The third element inside each block is the hash of the previous block and this effectively creates a chain of the blocks, which makes blockchain a secure technology.

3. TYPES OF BLOCKCHAIN

There are mainly three types of blockchains that have emerged are as follows:

a) Public blockchain

b) Private blockchain

c) Consortium blockchain

3.1 Public Blockchain

A public blockchain is the type of blockchain which is used publicly i.e which is ‘**for the people, by the people and of the people’.** Here, no one is in- charge and anyone can participate in reading/writing/auditing the blockchain. These types of blockchain are open and transparent, hence anyone can review it at given point of time. In these types of blockchain, the decision making happens by various decentralized consensus mechanisms such as proof of work (POW) and proof of stake (POS) etc. Example: Bitcoin, Litecoin.

3.2 Private blockchain

Unlike public blockchain, there is an in-charge checks the process of read/write or a singular access right. Here, the consensus is achieved on the central in-charge who can manage access rights assigned to different groups of users. This functionality makes the private blockchain a ‘centralized’ one. It is also cryptographically secured from the company’s point of view and more cost-effective for them.

Example: Bankchain.

3.3 Consortium blockchain

This type of blockchain tries to remove the sole autonomy which gets vested in just one entity by using private blockchains. So here instead of one in- charge you have more than one in-charge. Basically, you have a group of companies or representative individuals coming together and making decision for the best benefit of the whole network. Such groups are also called consortiums.

Example: r3

4. NEED FOR BLOCKCHAIN

Having a system like the blockchain, there are many issues that get covered with its implementations such as privacy and control over data.

5. APPLICATION OF BLOCKCHAIN TECHNOLOGIES

5.1 Digital Currency: Bitcoin

Bitcoin's data structure and transaction system was built by blockchain technologies, makes Bitcoin became a digital currency and online payment system. By using encrypted technique, funds transfer can be achieved and doesn't need to rely on central bank. Bitcoin used public keys address sending and receiving bitcoin, recorded the transaction and the personal ID was anonymous.

5.2 Smart Contract: Ethereum

Smart Contract is a digital contract that controls user's digital assets, formulating the participant's right and obligation, will automatically execute by computer system. It can hold the assets temporarily and will follow the order which has already been program.

6. SECURITY ISSUES AND CHALLENGES

It focuses on two main issues: Hard fork and Soft fork. The description of both is given below:

6.1 Fork problems

Fork problem is related to the decentralized node version, agreement when the software upgrades. It is a very important issue as it involves a wide range in blockchain.

When a new version of blockchain software is published, new agreement in consensus rule also changed to the nodes. Therefore, the nodes in blockchain network can be divided into two types, the New Nodes and the Old Nodes. So here come four situations:

1. The new nodes agree with the transaction of block which is sending by the old nodes.
2. The new nodes don't agree with the transaction of block which is sending by the old nodes.
3. The old nodes agree with the transaction of block which is sending by the new nodes.
4. The old nodes don't agree with the transaction of block which is sending by the new nodes.

According these four issues, fork problems can be divided into 2 types- Hard Fork and Soft Fork.

6.1.1 Hard Fork

Hard Fork means when system comes to a new version or new agreement, and it is not compatible with previous version, the old nodes couldn't agree with the mining of new nodes, so one chain became two chains. Although new nodes computing power were stronger than old nodes, old nodes will still continue to maintain the chain which it though was right. When Hard Fork happens, we have to request all nodes in the network to upgrade the agreement, the nodes which haven't been upgraded will not continue to work as usual. If there are more old nodes that did not upgrade, then they work as a completely different chain, which implies that the original chain will now work as two fork chains.

6.1.2 Soft Fork

Soft Fork is the case when a system comes to a new version or new agreement, and it is not compatible with the previous version, the new nodes could not agree to the mining of the old nodes. Since the computing power of the new nodes are stronger than the old ones, the block which is mined by the old nodes will never be approved by the new nodes. But, the new nodes and the old nodes will still continue to work on the same chain. When Soft Fork happens, nodes in the network don't have to upgrade the new agreement at the same time. It allows the node to upgrade gradually. Unlike Hard Fork, Soft Fork works in only one chain and it won't affect the stability and effectiveness of system when nodes upgrade. However, Soft Fork makes the old nodes are unaware about the consensus rule is changed, contrary to the principle of every node can verify correctly to some extent.

7. SCALE OF BLOCKCHAIN

With the blockchain technology growing and the data increasing rapidly, the loading of store and computing will also become difficult. It takes huge amount of time to synchronize data, and at the same time data is increasing continuously which brings a big issue to the client while running the system.

7.1 Simplified Payment Verification (SPV)

It is a payment verification technology which, without maintaining full blockchain information, only uses the block header message. This technology can greatly reduce the user's storage in blockchain payment verification, lower the user's pressure when transaction is drastically increased in the future.

8. CONCLUSION

Blockchain innovation runs the Bitcoin digital money. It is a decentralized domain for exchanges, where every one of the exchanges are recorded to an open-record obvious to everybody. The blockchain additionally empowers the improvement of new frameworks with more popularity based or participatory basic leadership, and decentralized associations that can work over a system of PCs with no human interaction. These applications have motivated many to contrast the blockchain technology with the Internet, with going with expectations that this innovation will move the adjust of energy far from brought together experts in the field of correspondences, business. With the increase in the data and transactions worldwide, it is expected that more blockchain applications will develop soon leading to simplification of transactions and management.

9. ACKNOWLEDGEMENTS

Our thanks to the expert Prof. Shabnam Sharma for guiding us and helped us perform our research.

10. REFERENCES

[1] 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/ bitcoin.pdf. (2008).

[2] Nir Kshetri, "Can Blockchain Strengthen the Internet of Things?," IT Professional, vol. 19, no. 4, pp. 68 - 72, May 2017, Available: http://ieeexplore.ieee.org/document/8012302/

[3] Sarah Underwood, "Blockchain Beyond Bitcoin," Communications of the ACM, vol. 59, no. 11, pp. 15-17, November 2016, Available: https://doi.org/10.1145/2994581

[4] Waseem Akram, "Blockchain technology:Challenges and future prospects" Volume 8 , No 9 , November 2017, Avaliable:http://ijarcs.info/index.php/Ijarcs/article/view/ 4950/4387