International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

Blockchain Technology : Classification, Opportunities, and Challenges

Nadir Abdelrahman Ahmed Farah

Dept. of Information Systems, Arts and Science College, University of Bisha, Saudi Arabia

---

Abstract - *Blockchain is a new technology that has emerged with the appearance of the Bitcoin, which has added a new way of dealing financially. Based on the success of this technique with the idea of Bitcoin, the technique has been relied upon and applied gradually in various activities, whether governmental or private and received the confidence and satisfaction of customers. The paper highlights the challenges ahead and opportunities in this Modern technology that is all set to develop our digital world.*

Key Words: **Blockchain, Bitcoin, Block chain Structure, Classification**

1. INTRODUCTION

Blockchain technology is one of the approaches that has the possibility to enhance decentralization, transparency, equality, and responsibility on the internet[1].

Blockchain is a distributed database of records that can be either public ledger of digital issues or transactions that got achieved and have been shared among participating parties across a large network of untrusted participants. It stores data in blocks that can verify information which are very difficult to hack. It avoids the requirement of a third-party verification and thus deactivates any sector that leverages it traditionally. [2].

Using blockchain can provide higher security compared to storing all data in a central database. The use of these technologies in Bitcoin "mining" was ground-breaking in the data storage and management side, harm from attacks on a database can be prevented. Further, since the blockchain has an openness attribute, it can provide transparency in data when applied to an area requiring the disclosure of data[3].

2. THE STRUCTURE OF BLOCKCHAIN

In general, the block contains main data; the hash of the previous block, a hash of current one, timestamp and other information. Figure 1 shows the structure of block.

Main data: Depending on the kind of service in which this blockchain is applicable, for example, transaction records, bank clearing records, contract records or IOT data record.

Hash: When a transaction executed, it had been hash to a code and then transmitted to each node. Because it could contained thousands of transaction records in each node's block, blockchain used Merkle tree function to produce a final hash value, and also Merkle tree root.

Timestamp: Time of block produced.

Other Information: Like signature of the block, Nonce value, or other data that user defines [7].

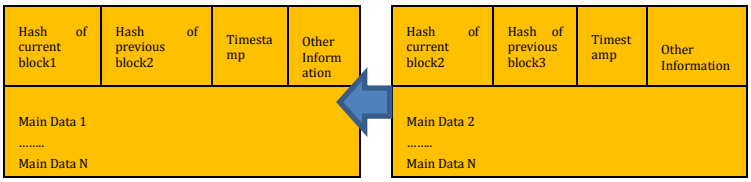

Fig -1: Structure of Blockchain

3. BLOCKCHAIN CLASIFICATION

Four types of blockchains can be defined as shown in Table 1.

Table -1: Blockchain Types

Based on access to Blockchain	Based on access to Blockchain Data
Permission-less: Any one can join	**Public:** All who access can modify
Permissioned: Approved users only	**Private:** Only specific users can write / modify

Public and Permission-less are used interchangeably and so are Private and Permissions. Depending on the use case, one needs to select an appropriate architecture from those defined in Table 1.

There are different blockchain based system configurations against multiple parameters such as performance, cost efficiency, and flexibility. Different dimensions of a blockchain system such as blockchain configuration, storage, computation, a degree of decentralization are considered in coming up with the classification [4]

3.1 Public / Permission-less blockchains

Public blockchains are open for all. Anyone can join them to post transactions and to participate in the mining and consensus process of adding a new block of a transaction to them. These blockchains usually use Proof of Work (protocol requires all nodes on the network to solve cryptographic puzzles by brute force) or Proof of Stake (protocol of block verification does not rely on excessive computations) for consensus mechanism. Having more number of participants working well for this model, as it further reduces the possibility of a 51% attack[4].

3.2 Private / Permissioned blockchain

Permission blockchains are usually built usually by organizations for their specific business need. Blockchains are likely to have interfaces with existing applications of the organization. Organizations may opt for consortium blockchains where limited trusted members mandatorily need to sign off a transaction. In fully private blockchains, the right permission over the blockchain is given to a central organization[4].

4. STANDARD & BLOCKCHAIN-BASE TRANSACTIONS

The table below shows the key differences between the standard transactional model (so far quasi-unique and certainly prevalent) and the decentralized approach that provides (the so-called blockchain transactional model)[5].

Table -2: Standard vs. blockchain-based transactions

Model	Standard	Blockchain
Paradigm	Trusted third party	Trusties System
Architecture	Centralized Server	Peer-to-Peer Network
Database	Single Copy	Multiple Copies
Security	Controlled Access	Cryptography
Price / Cost	Intermediation	Consensus
Access	Private	Public

5. BITCOIN

In a seminal white paper in 2008, at the height of the US sub-prime mortgage crisis, an anonymous author, or group of authors, using the pseudonym Satoshi Nakamto, described the implementation of a blockchain that supported the creation and use of a virtual currency. This virtual currency was dubbed bitcoin. Unlike money, bitcoin is not issued by a central bank but rather created as a reward for peers in a peer-to-peer network who take it upon themselves to add a block of verified transactions to the existing bitcoin blockchain.

The bitcoin network consists of a group of globally distributed computers all running open source software. When a transaction occurs, all the nodes in the system verify its authenticity. A set of the computers in the system, take it upon themselves to add blocks of verified transactions to the bitcoin blockchain in effect recording the transaction into a fixed distributed ledger [6].

6. USES OF BLOCKCHAIN

Blockchain can be used for many different applications other than digital currency. In addition, the introduction of smart contracts opened the door for many financial applications using blockchain. In this section, we will discuss some of the most prominent use-cases of the blockchain.

6.1Financial Contracts

Blockchain offers community verification that means that the terms of the contract is known to everyone and cannot be retreated on.

Thus, providing security to counterparties engaging in financial contracts. It is also, in theory at least, fixed, so providing a permanent and public record of all the contracts and what happened in them that can be used by regulatory organizations to understand the events in the market (in short, it has transparency built in) [6].

6.2 Asset Tracking

Another possible use-case for blockchain is as an asset tracking tool for ascertaining proof of ownership or source of a particular asset.

The presence of stolen goods in the international supply chain is a problem that needs addressing. It is required to have a system of publically viewable, fixed, verified records of ownership that can be examined at any time to determine the source of any particular item [6].

6.3 Payment System

It is possible to use blockchain to implement payment systems in currency. This is a natural extension of its ability to manage payments and transaction in cryptocurrencies[6].

6.4 Digital Identity

Just as blockchain can be used to track ownership and source of goods, it can also be used to store the identity of people. Imagine that your passport is stored on a blockchain and the visas you get and your entry and departure from countries are recorded as blockchain transactions. This means that they are fixed, society verified and decentralized. By adding smart contracts to the system, it may also be possible to encode rules for denying entry to certain people (sanctions against countries of origin, security reasons or any other reason) and have them automatically implemented on the blockchain. The rules would be visible to all and automated which would reduce the possibility of human error entering into the process [6].

7. OPPORTUNITIES OF BLOCKCHAIN

- Blockchain technology affected the transforming of the current Internet from “The Internet of Information Sharing” to “The Internet of Value Exchange".

- The possibility of blockchain to initiate significant change has been proved, including in changing banks’ business models as well as the business models of

their clients from a plurality of industries, and the financial services industry.

- Blockchain facilitates all operations within the banking industry. First, it automates the process of matching positions against accounts. That means that clearing and settlement become faster without approval at later stages. Second, this technology is more transparency and that feature allows blockchain fulfill all regulatory requirements more efficiently. Third, since the conditions for every transaction are transparent and fixed, blockchain technology minimize many risks, that is, they are not changing. Fourth, it avoids centralization data with decentralized register stores the full data connect to all transactions as well as the origins of traded assets. And fifth, blockchain technology isolate interim steps saving many.

- Blockchain reinforces market efficiency: On financial markets, trade is happening in a fraction of a second. But the actual exchange of goods may hover over days and include more banks and clearinghouses. This can lead to mistakes, delays, additional costs and unnecessary risks.

- Blockchain technology allows smart contracts: A smart contract is a computer code that demonstrates a step-by-step transaction. It can be linked to more various blockchains, track different goods so that it can exchange / transfer these goods when needed for a transaction. The broker buys shares on behalf of his/her client. The order is placed, which includes private keys and seller and buyer. That way performance of a smart contract is executed and linked to multiple blockers, which confirms the buying and selling power. [8].

- Personal data protection: there is a low risk for the blockchain processes users in case of a retailer or a partner in a transaction is subject to a cyber attack and loses traditional financial or personal data of the customers or its own. blockchain processes are at risk only if the hackers can able to get access to the users' private keys [10].

- The problem of redundancy is isolated. All the processes are stored on a distributed network, so it helps to protect integrity and authenticity.

- Highly sophisticated protocols and algorithms are used to protect the data.

- Blockchain data is complete, consistent, accurate, timely and more available[11].

8. BLOCKCHAIN CHALLENGES

- Regulation is the biggest challenge for non-fiat currency. The rate of technical innovation is surpassing the rate at which regulations catch up. The currency evolution has seen a transformation in the order from fiat currency to e-money to virtual currency to cryptocurrency.

- One key limitation of Blockchain technology is the scalability issue due to the size of the public or permissionless blockchain[4].

- Blockchain capacity: In order to have a dense network, we need a big number of tracks. The problem is that each of these tracks must be rooted in the blockchain.

- Locked-in funds: Funds are locked in each and every track. Choosing a partner to collaborate within a track is a commitment to that party. Closing the track and moving the funds into a new track with a different partner needs expensive blockchain transactions, thus there is a risk involved and partners must be chosen carefully [9].

- Lack of solid anonymity: A survey performed by Fabian et al. revealed that seven out of ten people consider that Bitcoin has a reasonable level of anonymity (medium to high), while the associated risks are medium or low[10].

- Block Shen uses encryption permanently, which requires a mining system that consumes considerable energy [11].

9. CONCLUSION

This paper has discussed the blockchain technology along with some of its important advantages. The technology is still improving with a lot of fields for different areas and industries and is set to change the world's manner. But it is not free from challenges, some of them have been highlighted too.

From the study above, it could be concluded that blockchain helps removing the involvement of third parties in any transaction. It can be implemented in the different sectors to avoid fraudulent and forgery activities.

REFERENCES

[1] Walid A., Nicolas S., 2017, " Blockchain technology for social impact: opportunities and challenges ahead " , available : https://doi.org/10.1080/23738871.2017.1400084

[2] Arijit C., Ashesh K., 2017, " Blockchain and its Scope in Retail"available: https://irjet.net/archives/V4/i7/IRJET-V4I7616.pdf

[3] Ketki R., Sheetal Y., 2018, " Blockchain Technology in Cloud Computing : A Systematic Review " , available : https://www.irjet.net/archives/V5/i4/IRJET-V5I4428.pdf

[4] Supriya T., Vrushali K., 2017, " Blockchain and Its Applications – A Detailed Survey " , available : https://www.ijcaonline.org/archives/volume180/number3/aras-2017- ijca-915994.pdf

[5] Ian P., Emre E., 2017, " Perspectives of Blockchain Technology, its Relation to the Cloud and its Potential Role in Computer Science Education" , available ; http://www.etasr.com/index.php/ETASR/article/view/1629/pdf

[6] Sherif F., 2018, " Blockchain and its uses " available : www.sheriffadelfahmy.org/wp-ontent/uploads/2018/01/doc-1.pdf

[7] Iuon-Chang L., Tzu-Chun L., 2017, " A Survey of Blockchain Security Issues and Challenges " , available : http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5- p653-659.pdf

[8] Dusko K., 2018, " Impact of Blockchain Technology Platform in Changing the Financial Sector and Other Industries " , available :http://repec.mnje.com/mje/2018/v14-n01/mje_2018_v14-n01-a18.pdf

[9] Roger W., Christian D., Conrad B., 2017, " Scalable Funding of Blockchain Micropayment Channel Networks " , available : http://drops.dagstuhl.de/opus/volltexte/2017/7363/pdf/dagrep_v007_i003_p099_s17132.pdf

[10] George C ., 2017, " Bitcoin – A Brief Analysis of the Advantages and Disadvantages ", available : http://www.globeco.ro/wp-content/uploads/vol/split/vol_5_no_2/geo_2017_vol5_no2_art_008.pdf

[11] Atul K., Arpit G., 2017, " BLOCKCHAIN: An analysis on next-generation internet ", available : http://dx.doi.org/10.26483/ijarcs.v8i8.4769