Block Chain Technology and Development

Mrs. Dr. G. Vithya
Assistant Professor of CSE Dept,
PITS.

K. Nasrin Banu
Dept of. CSE
PITS.

Abstract:- **The block chain emerged as a novel distributed consensus scheme that allows transactions, and any other data, to be securely stored and verified without the need of any centralized authority. For some time, the notion of block chain was tightly coupled with a now well-known proof-of-work hash-based mechanism of Bitcoin. some are simple variants of Bitcoin, whereas others significantly differ in their design as well as provide different functional and security guarantees. This shows that the research community is in search of a simple, scalable, and deployable block chain technology. Various reports further point to an increased interest in the use of block chains across many applications and to a significant investment in the development of block chains by different industries. It is expected that the block chain will induce considerable change to a large number of systems and businesses.The paper highlights the challenges ahead and opportunities in this Modern technology that is all set to develop our digital world.**

Key Words- Block chain, Bitcoin, Block chain Structure, Classification

INTRODUCTION

Block chain technology is one of the approaches that has the possibility to enhance decentralization, transparency, equality, and responsibility on the internet.

Block chain 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.

Using block chain 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 block chain has an openness attribute, it can provide transparency in data when applied to an area requiring the disclosure of data.

STRUCTURE OF BLOCK CHAIN

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

Main data: Depending on the kind of service in which thisblock chain 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, block chain used Merkle tree function to produce a final hash value, and also Merkle tree root. A Collision is when two different blobs of data procedure the exact same hash. Afunction that creates a 256-bits hash (like SHA) will have fewer collision than one that produces a 128-bit hash(like MD5) because there are more possible hash values when you have more bits.

BLOCK CHAIN ALGORITHM

```
>>>import hashlib
>>> header_hex = ("01000000" +
...
"ae178934851bfa0e83ccb6a3fc4bfddff3641e104b6c4680c315
09074e699be2" +
...
"bd672d8d2199ef37a59678f92443083e3b85edef8b45c717593
71f823bab59a9" +
...   "7126614f" +
...   "44d5001d" +
...   "45920180")
>>>header_bin = header_hex.decode('hex')
>>>hash                                                    =
hashlib.sha256(hashlib.sha256(header_bin).digest()).digest()
>>>hash.encode('hex_codec')
'60ce4639bf63532b27e8f8b036b9846f5d2ae18556289f80e38
b85a5df4910e1'
>>>hash[::-1].encode('hex_codec')
'e11049dfa5858be3809f285685e12a5d6f84b936b0f8e8272b5
363bf3946ce60'
```

BLOCK CHAIN CLASSIFICATION

Four types of block chains can be defined as shown in Table .

Table :Block chain Types

Based on access to Block chain	Based on access to Block chain 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 .

There are different block chain based system configurations against multiple parameters such as performance, cost efficiency, and flexibility. Different dimensions of a block

chain system such as block chain configuration, storage, computation, a degree of decentralization are considered in coming up with the classification.

PUBLIC /PERMISSION –LESS BLOCK CHAIN

Permission block chains are usually built usually by organizations for their specific business need. Block chains are likely to have interfaces with existing applications of the organization. Organizations may opt for consortium block chains where limited trusted members mandatorily need to sign off a transaction. In fully private block chains, the right permission over the block chain is given to a central organization.well for this model, as it further reduces the possibility of a 51% attack.

PRIVATE / PERMISSIONED BLOCK CHAIN

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

STANDARD &BLOCK CHAIN-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 block chain transactional model).

Table: Standard vs. block chain-based transactions

Model	Standard	block chain
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

BITCOIN

In a seminal white paper in 2008, at the height of the US subprime mortgage crisis, an anonymous author, or group of authors, using the pseudonym Satoshi Nakamto, described the implementation of a block chain 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 block chain.

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 block chain in effect recording the transaction into a fixed distributed ledger.A block chain is typically managed by a peer-to-peer network collectively adhering to a protocol for internode communication and validating new blocks.

CENTRALIZATION VS DECENTRALIZATION

Centralization and Decentralization are the two types of structures, that can be found in the organization, government, management and even in purchasing. **Centralization** of authority means the power of planning and decision making are exclusively in the hands of top management.

Decentralization refers to the dissemination of powers by the top management to the middle or low-level management. It is the delegation of authority, at all the levels of management.

BASIS FOR COMPARISON	CENTRALIZATION	DECENTRALIZATION
Involves	Systematic and consistent reservation of authority.	Systematic dispersal of authority.
Decision Making	slow	Comparatively faster
Communication Flow	vertical	Open and free
Advantage	Proper coordination and Leadership	Sharing of burden and responsibility
Power of decision making	Lies with the top management.	Multiple persons have the power of decision making.
Implemented when	Inadequate control over the organization	Considerable control over the organization

USES OF BLOCK CHAIN

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

- Payment processing and money transfers
- Monitor supply chains
- Retail loyalty rewards programs
- Digital IDs
- Data sharing
- Copyright and royalty protection
- Digital voting ,etc…..

FINANCIAL CONTRACTS

Block chain 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.

SASSET TRACKING

Another possible use-case for block chain 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.

PAYMENT SYSTEM

It is possible to use block chain to implement payment systems in currency. This is a natural extension of its ability to manage payments and transaction in cryptocurrencies. Since all transactions can be seen publicly and cannot be altered once they are coded into the system, Block chain helps customers to spend their digital moneys much easier.

DIGITAL IDENTITY

Just as block chain 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 block chain and the visas you get and your entry and departure from countries are recorded as block chain 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 block chain. The rules would be visible to all and automated which would reduce the possibility of human error entering into the process.

OPPORTUNITIES OF BLOCK CHAIN

- Block chain technology affected the transforming of the current Internet from “The Internet of Information Sharing” to “The Internet of Value Exchange".
- The possibility of block chain to initiate significant change has been proved, including in changing banks’ business models as well as the business models oftheir clients from a plurality of industries, and the financial services industry.
- Block chain 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 block chain fulfill all regulatory requirements more efficiently. Third, since the conditions for every transaction are transparent and fixed, block chain 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, block chain technology isolate interim steps saving many.
- Block chain 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.
- Block chain 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 block chains, 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.
- Personal data protection: there is a low risk for the block chain 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. block chain processes are at risk only if the hackers can able to get access to the users' private keys.
- 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.
- Block chain data is complete, consistent, accurate, timely and more available.

BLOCK CHAIN 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 Block chain technology is the scalability issue due to the size of the public or permissionlessblock chain.
- Block chain 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 block chain.
- 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 block chain

transactions, thus there is a risk involved and partners must be chosen carefully.

- 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.

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

CONCLUSION

This paper has discussed the block chain 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 block chain helps removing the involvement of third parties in any transaction. It can be implemented in the different sectors to avoid fraudulent and forgery activities. Public ledger with no formal control or governance.

REFERENCE

[1] 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.
[2] 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/ijns2017-v19-n5- p653-659.pdf .
[3] Dusko K., 2018, "Impact of Blockchain Technology Platform in Changing the Financial Sector and Other Industries " , avaislable :http://repec.mnje.com/mje/2018/v14n01/mje_2018_v14-n01-a18.pdf.