AN OVERVIEW OF BLOCKCHAIN TECHNOLOGY

Sivanesan.R[1], Ashwin.S[2], Vignesh.P[3], Manikandan.G[4]

[1]Assistant Professor, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Coimbatore, Tamilnadu, India.
[2,3,4] Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Coimbatore, Tamilnadu, India.

---***---

ABSTRACT – *Blockchain is a rising innovation for decentralized and value-based information sharing over a vast system with untrusted members all around the world .It empowers new types of circulated programming designs. In spite of the fact that the innovation was fundamentally embraced in computerized money in introductory days, yet it is a promising innovation for different zones as well. This paper gives a detailed view about blockchain in a rearranged way. The paper features the types of ledger in blockchain and a portion of the terms & difficulties also.*

Keywords: **Blockchain, Bitcoin, Crptocurrency Centralize ledger, Decentralized ledger.**

1. INTRODUCTION

Currency transactions between persons or companies are often centralized and controlled by a third party organization. Making a digital payment or currency transfer requires a bank or credit card provider as a middleman to complete the transaction. In addition, a transaction causes a fee from a bank or a credit card company. The same process applies also in several other domains, such as games, music, software etc. The transaction system is centralized, and all data and information are controlled by some third party organization, rather than the two main entities involved in the transaction process. Blockchain technology has been invented to overcome this issue. The aim of Blockchain technology is to create a decentralized platform where no third party can control of the transactions and data. Blockchain is a distributed database solution that maintains a rapid growing list of information & data records that are confirmed by the nodes participating in it. The data is recorded in a public ledger, including information of every transaction ever completed. Blockchain is a non-centralized solution which does not require any third party organization in the middle of any transaction. The information about every transaction is stored in Blockchain is shared and available to all nodes. This attribute makes the system more transparent more than centralized transactions involving a third party. In addition, the nodes in Blockchain are all confidential, which makes it more secure for other nodes to confirm the transactions. Bitcoin was the first application that introduced the technology called Blockchain. Bitcoin created a decentralized environment for cryptocurrency, where the participants can buy and exchange goods with digital money.

Even though Blockchain looks to be a promising solution for transactions by using cryptocurrencies, it also has some technical challenges and limitations that need to be studied and rectified. High integrity of transactions and security, as well as privacy of nodes are needed to prevent attacks and attempts to break a transactions in Blockchain. In fact, confirming transactions in the Blockchain requires a computational power.

1.1 SHORT HISTORY OF BITCOIN

In 2008, an individual or group writing under the name of "Satoshi Nakamoto" issued a paper "Bitcoin : A Peer-To-Peer Electronic Cash System". This paper describes a peer-to-peer version of the cryptocurrency that would allow online payments to be directly sent from one to another without passing through a financial institution. Bitcoin was the first realization of this concept. The word cryptocurrency is the label that is used to define all networks and mediums of exchange, uses cryptography to secure transactions; against those systems where the transactions are channeled through a centralized trusted organisation or entity. The author of the first paper wanted to remain incognito, therefore no one knows Satoshi Nakamoto to this day. After few months, an open source program implementing the new protocol was released that began with the block of 50 coins. Anyone in this world can install this open source program and become part of the bitcoin peer-to-peer network. It has grown towards popularity since then.

2. BLOCKCHAIN TECHNOLOGY

The concept of blockchain is by explained clearly how Bitcoin works, since it is linked to the Bitcoin. The blockchain technology is relevant to any digital money transaction exchanged online. Internet commercial is specially tied to the financial institutions, serving as the trusted third party, who process and mediate any e-transaction. The main purpose of trusted third party is to validate, safeguard and maintain transactions. A few number of percentage fraud is unavoidable in online transactions, so it must be prevented throughout financial transactions. Thus, resulted in high transaction costs. Bitcoin uses cryptographic proof instead believing the third party, so that the two willing parties can execute via online transaction over the Internet. Each transaction is guarded through a digital signature. Each transaction is sent through a "public key" of the receiver and digitally signed using a "private key" of the sender. In case to spend money, owner of the cryptocurrency needs to prove the ownership of the "private key". The entity receiving the digital currency will verify the digital signature thus the ownership of corresponding "private key" on the transaction using the "public key" of the sender. Every transaction is transmitted to every node in the

Bitcoin network and then recorded in a public ledger after verification. Every single transaction needed to be verified before validity then only it is recorded in the public ledger. Verifying nodes needs to ensure two things before recording anything transaction:

1. Spender owns the cryptocurrency: On the transaction digital signature needed to be verificated.

2. Spender's account should have sufficient cryptocurrency : checking every transaction against spender's account in the ledger to make sure that spender has sufficient balance in the account.

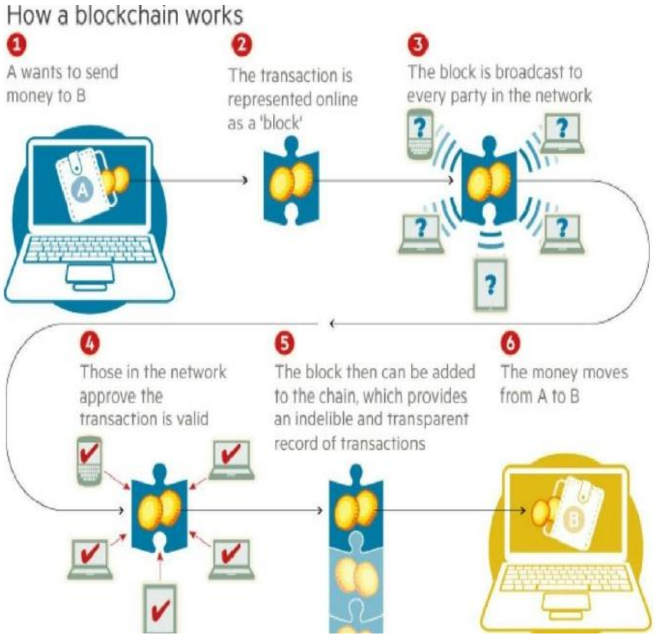
How a blockchain works
1
A wants to send money to B
A
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
?
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
B

Fig – 1: Process of Cryptocurrency in Block Chain

However, there is always a question, how the order of these transactions that are broadcast to every other node in the Bitcoin peer-to-peer network is maintained. The transactions does not come in order, they are generated and there is a need for a system to make sure that double spending of the cryptocurrency does not occur. In fact, the transactions are passed through node by node in Bitcoin network, there is no guarantee that in what orders they are received to a node.

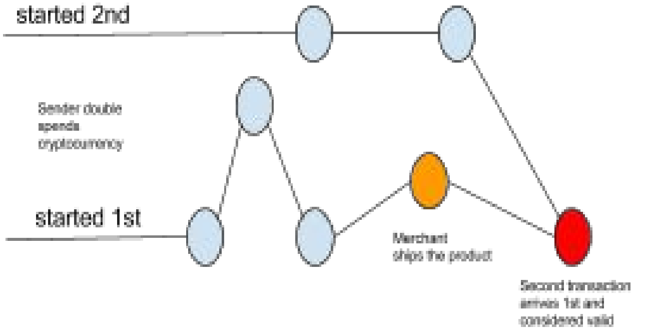
started 2nd
Sender double spends cryptocurrency
started 1st
Merchant ships the product
Second transaction arrives 1st and considered valid

Fig – 2: Bicoin Peer to Peer Network

Blockchain has two kinds, permissioned and un permissioned. Un permissioned - it is shared crosswise over different PC's in the system; so anybody can view & change or exchange what is recorded, the information put away is time stamped, that it can't be erased or refreshed further. The augmentations to the record or new records are followed and refreshed continuously for everybody with every entrance. Despite, of its circulating nature blockchain is hard to hack, as every one duplicates are situated at better places. Permissioned - this work the very same way, but it fit's for limiting who can approve the exchanges in the system. A blockchain promotes secured online transaction using cryptography by making cryptographic key combined with a wallet programming. In blockchain, to give verification and non-renouncement an advanced mark is used , that the key-controlling element can perform the exchanges from its related record.

2.1 Centralized ledger

When compared to other industries, accounting system and its digitalization has not yet attained maturity. The reasons might be due to very high involvement of regulators. The accounting details of any organisation should meet all regulatory requirements in order to retain the validity and integrity of all transactions. Organisation needs to be very precaution in developing new ledger systems to make sure that is high security and must prevent any fraudulent activities. To achieve this, manually processed and verified many transaction are still carried, which will affected the day to day operations. Most of these manual tasks are not automated and doesn't seems to be automated in the upcoming future, so it must be maintained with the integrity and validity of transactions.

Centralised ledger system are used by most of the organisations to record all day to day transactions. A centralised ledger system is a compilation of all transactions which is controlled by a single entity i.e. it has a single point of control. In centralized ledger system the reconciliation of internal and external data is required to ensure the integrity of transactions. No restrictions is provided in the centralized system on the operations which can be performed in the ledger. For example: Any user can modify a transaction and back date them. This can lead is misstatement of fraudulent activities and financial transactions.

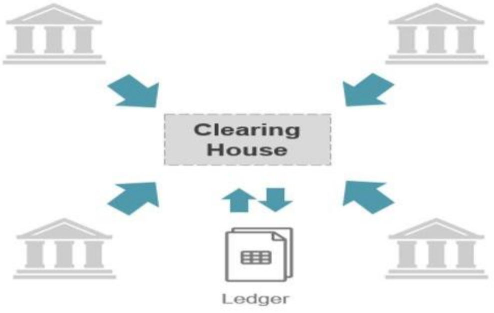

Fig – 3: Centralized Ledger

2.2 Distributed Ledger

A distributed ledger which is also known as a shared ledger or decentralized ledger is a list of synchronized and shared data which are geographically spread across multiple sites. To maintain data integrity, availability and resiliency the data is exactly replicated and synchronized across all locations. Unlike the centralized system, there is no single point of control or central administrator . If a location fails or stop functioning, the remaining location has the data and has the capacity to maintain the ledger or all transaction details and data in the absence of the failed location. Thus provides a real-time information and reduced error or fail rates of transactions. This also reduces the costs of infrastructure . In distributed ledger,a peer-to-peer network is used to communicate with nodes which are spread around the globe. Distributed ledger technology gives the opportunity for scale the economy by allowing the transaction to serve simultaneously as agreement, settlement, and regulatory reporting. Rather than building numerous duplicative and redundant services, one master prime record can serve as the source, eliminating the need for the reconciliation and increased post-trade processing speed .

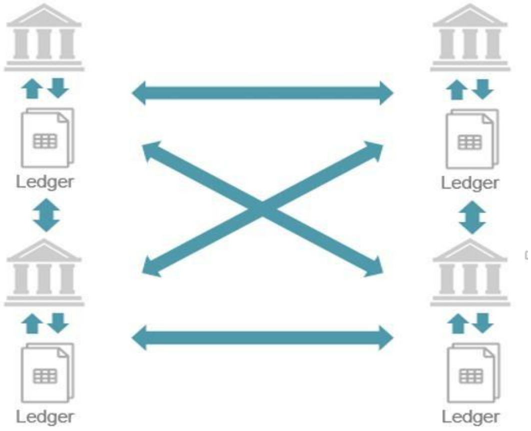

Fig – 4: Distributed Ledger

3. EVALUATING BLOCKCHAIN SOLUTION

Even though it is a latest new technology, blockchain is rapidly advancing and growing fastly. There are a number of main issues which organizations need to check and rectify the technology from both a technical and a general business point of view.

3.1 Regulatory and compliance implications

In 2008, the financial crisis which gets started, Measures are taken by governments in the majority of the countries , in order to check the activity of financial institutions and to ensure safety for transactions and to prevent future trouble. Also governments are very much responsive to every innovation or modification in this industry. Probably new innovations in the financial and banking sector will be thoroughly checked and needs to cope up with tough regulations.

3.2 Data privacy

Blockchain has many levels of security and one of the security is immutability of data. No changes can be done to the data after it is validated and included in this block. Hence , the data will remain there as long as the system is valid. Since the blocks are sent across the network and are open for all the participants to check, it's important to take some consideration aspects like concerns regarding privacy of the data which is included there. Some of the clients may wish to know if personal identification can be revealed or if data is encrypted.

3.3 Operational concerns

Similarly, to a production system a solution is offered by blockchain must have an operational side to it. This solution needs to be integrated and this depends also on the respective institution's applications. Hence, there might be business and technological issues, and maybe the staff will necessitate training. Also, such problems as capacity planning, business continuity may arise and will need to be addressed.

3.4 Data standards

As mentioned, different types of data's are included in this blockchain. Solutions are rapidly expanding and blockchain technology will be useful for other areas. At present, these kinds of solutions are utilized within open networks, for example, Bitcoin. On the other hand, there are private networks, where each participant can be known by another one. There are specific regulations in both of these cases which the participants need to respect. These must refer to structure, formatting, and taxonomy of the stored information. These regulations are called standards and they are defined, clearly communicated and then enforced to be followed within the entire network structure.

3.5 Network governance

As mentioned, Blockchain represents a business type of decentralized solution having no authority. There may emerge for a governing structure, mainly for those types of blockchain solutions which are used by financial institutions. This would need to be implemented for maintaining a certain set of rules regarding the onboarding, participation, problems which may arise, and others. Each participant must need to obey the network regulations, how they are maintained, established and then enforced.

3.6 Scalability

Bitcoin and Ethereum are one of the most popular organizations that implemented blockchain solutions, relying on various validation speeds. For example, a block is verified by Bitcoin in 10 minutes and recorded data will be confirmed after a number of 6 validations. Then, in as much as 60 minutes there will be cryptographic proof that attest the funds were transferred in a securely manner. The same operation takes place only in 17 seconds in Ethereum. So, there is a bit of a difference in speed. There are cases, such as payments between banks and high-volume operations, when this speed might not be satisfactory. Hence , organizations will use various blockchain solutions, depending on their specific needs.

3.7 Security

It certainly is very important to have the digital values secured, if you take into consideration the possibility of using blockchain technology and other cryptocurrency, such as Bitcoin. These digital funds have a public key and this private key is kept in a kind of digital wallets which have protection, called passphrase. It might be correct to say that a digital wallet is similar to an account. There are many various forms for all kinds of available devices.

4. CHALLENGES

Blockchain innovation is as yet rising and is in the evidence of idea phase of advancement and very few blockchain based frameworks got sent at modern scale, so genuine dangers with blockchain may not be evident for next couple of years till it progresses toward becoming standard more. This innovation should be painstakingly investigated before being embraced and its reception ought not be hurried. A disappointment in execution may prompt real results, and even fundamental dangers. Being a common record frameworks, blockchain should have delicate information also. Consequently, it must guarantee that its cryptography and digital insurances are strong and in accordance with the business best practices. Information assurance and isolation ought to be dealt with for cloud based retail arrangements too.

5. CONCLUSION

Blockchain technology runs the Bitcoin cryptocurrency. It is a decentralized environment for transactions, where all the transactions are recorded to a public ledger, which will be visible to everyone. The goal of Blockchain is to provide anonymity, security, privacy, and transparency to all its users. Despite, these attributes set up a lot of technical challenges and limitations that need to be addressed.

To understand where the current research on Blockchain technology positions itself, we decided to map all relevant research by using the systematic mapping study process . The goal of this systematic mapping study was to examine the current status and research topics of Blockchain technology. We excluded the economic, law, business, and regulation perspectives, and included only the technical perspective.

To conclude, we envision BlockChain to go through slow adoption due to the risks associated. Most of the Startups will fail with few winners. We should be seeing significant adoption in a decade.

6. REFERENCES

[1]N.Anderson, “Blockchain Technology A game-changer in accounting?,”.

[2]https://symbiont.io/uncategorized/distributed-ledgers-vs- centralized-databases/

[3]Distributed Ledgers, Internet: http://www.investopedia.com/terms/d/distributed-ledgers.asp

[4] “Know More About Blockchain: Overview, Technology, Application Areas and Use Cases,” Lets Talk Payments, http://letstalkpayments.com/an-overview-of-blockchain-technology/.

[5] “Financial Institutions: Blockchain ActivityAnalysis,”http://letstalkpayments.com/financial-institutions- blockchain-activity-analysis/.

[6] “What is Blockchain Technology? A Step-by-Step Guide For Beginners,” http://blockgeeks.com/guides/what-is-blockchain- technology/.

[7] S.Iyer,(2016 , July) ,” The Benefits of Blockchain Across Industries.”
:http://www.oracle.com/us/corporate/profit/big-ideas/041316-siyer-2982371.html.

[8] T.Virdi,” The benefits of Blockchain for financial services.”, https://betanews.com/2015/12/28/the-benefits-of- blockchain-for-financial-services/.

[9] Kishigami J, Fujimura S, Watanabe H, Nakadaira A, Akutsu A. The Blockchain-Based Digital Content Distribution System. In: Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conference on; 2015.

BIOGRAPHIES

Sivanesan Rajangam, Assistant Professor, Department of Computer Applications. Have Five Years of Teaching Experience in Esteemed Institutions and Corporate Experience as well.
Research Areas: Data Mining, Image Processing and Compiler Design.

Ashwin Surendran, Student of Computer Application Sri Krishna Arts and Science College, Coim batore.
Area of Interest: Image Processing, Networking.