International Journal of Trend in Scientific Research and Development (IJTSRD)

International Open Access Journal

ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Blockchain : A Revolutionary Technology

Rajshree Srivastava[1], Shubham Kumar, Animesh Singh, Harshit Mohan Saraswat

[1]Assistant Professor
B.Tech IT, DIT University, Dehradun, Uttrakhand, India

ABSTRACT

A Blockchain is defined as a distributed database which consists of records, or public ledgers of all the transactions or digital events executed and shared among participating network. In this each transaction in the public ledger is verified by consensus of a majority of the participants in the network. As soon as the information is entered, it can never be erased. The Blockchain contains a verifiable record of every single transaction ever made. [9]It was developed firstly for Bitcoin as a peer-to-peer digital currency or popularly called as 'cryptocurrency'. The idea for Blockchain was coined in 2008. Since then the interest in Blockchain technology has been increasing. The reason for this increase in interest in Blockchain is its central attributes which provide security and data integrity without any third party organization in control of the transactions. Therefore it creates interesting and vast research areas, especially from the perspective of technical challenges, expectations and limitations. It was found wide range of applications in both financial and non-financial market.

In this paper, we have conducted a procedural and organized mapping study with the goal of collecting all relevant information about the evolution of Blockchain technology since 2008. Our objective here is to understand the enhancement, challenges and future expectations regarding Blockchain technology from the technical perspective. The focus is on working of Blockchain Technology including the revolutionary rise of Blockchain Technogy generation 1.0, 2.0, 3.0. This paper describes Blockchain technology and some of its compelling specific applications in both financial and non-financial sector. We then look at the challenges abroad and business opportunities in this fundamental technology that is all set to revolutionize our digital world.

I. INTRODUCTION

Currency transactions between companies or persons are often centralized due to a third party organization controlling it. Completing a digital payment or currency transfer always passes through a bank or credit card provider which serves as a middleman to complete the transaction. In addition, it also causes a fee from a bank or a credit card company for the transaction. The same process is applied in several other categories, including games, music, software etc. The transaction system is mostly centralized, and all the data and information are controlled and managed by a third party organization, rather than the two principal entities involved in the transaction. Blockchain technology is developed to solve the issue[5]. The goal of Blockchain technology is to create a decentralized environment where there is no third party is in control of any transactions and ledger. For the first time in history of humankind people anywhere can trust each other and transact with a large peer to peer network without any centralized management system. Trust is established with the help of protocols, cryptography and computer codes instead of any centralized organization. This strengthens our capacity for collaboration and co operation between individual and organization. Blockchain Technology is considered as a distributed database solution that maintains a continuously growing list of data records or public ledger that is confirmed by the nodes who participates in it. The data is stored as a record in a public ledger, including information of every transaction that ever been completed. The information about every transaction ever completed in Blockchain is shared and is made available to each nodes participating in it. This attribute makes the system more transparent than centralized a transaction which involves a third party. In addition, the nodes in Blockchain were all anonymous in order to make more secure for other nodes to confirm the transactions.

Bitcoin was the first ever application that introduced Blockchain technology. It created a decentralized environment for digital currency. Here the participant can buy or exchange goods with digital money popularly termed as 'Value For Money'. However, even though Blockchain seems to be a suitable solution for conducting transactions, it has some technical challenges and limitations which is supposed to be studied. High integrity of transactions, security and privacy of participating nodes are needed, to prevent attacks or attempts of disturbing transactions in Blockchain. In addition, confirming transactions in the Blockchain network requires a computational power. One of the key emerging use case of blockchain technology involves "smart contracts". Smart contracts are basically computer programs which can automatically execute the terms of a contract. Although cryptocurrencies or digital currencies business and management topic, we need to decide to narrow down the research topic to the technical perspective of Blockchain. Our objective was to find and map papers with technical viewpoints on Blockchain.

II. RELATED WORK

In 1991, a structure similar to Blockchain was mentioned in a research paper titled as "How to Time-Stamp a Digital Document" written by Haber and Stornetta. According to the paper, a person sends a document with a timestamp to a times tamping server and the server would sign the document with the current timestamp. Also, in addition the server has to link the document to the previous document. The pointers are pointed to specific data and not the location of the document. So if any change is made to the data, the pointer would become invalid. It ensures that no one could tamper the data that had once passed through the server.

In 2008, an individual (or group) under the name of "Satoshi Nakamoto" published a paper titled "Bitcoin: A Peer-To-Peer Electronic Cash System". The paper described a peer-to-peer version of the e-cash that would allow online payments to be sent from one party to another directly, without going through a financial institution. Bitcoin was the first application for this concept. Now all networks and mediums of exchange that uses cryptography to secure transactions is labeled under "cryptocurrencies" The author of the first paper wanted to remain unknown and hence no one knows Satoshi Nakamoto to this day. An open source program implementing the new protocol was released, a few months later. The programme begin with the Genesis block of 50 coins. Anyone can install this open source program to become a part of the bitcoin peer-to-peer network.

Around 2014, attention shifted from Bitcoin to detailed study of Blockchain. The world realized that Blockchain can be separated from the digital currency and can be applied to other use-cases. Blockchains features like privacy, trust, reliability makes this technology suitable for every industry. You pick any industry; Blockchain is going to have a relevant conversation for them.

III. WORKING

Blockchain is a new class of information technology that combine cryptography with distributed computing in a model in which network of computers collaborate towards maintaining a shared and secured database. The blockchain is a continuosly growing list of the blocks of data linked and secured using cryptography. This makes it a trusted database. With this trust being maintained by open, secure, computer coded encryption instead of any single institution. Figure 1 shows the working. The working of blockchain can be explained in the following categories:

A. *Generation of block :*

The database consist of string of block , each one a record of data that is been encrypted and given a unique identifier called a hash. Blockchain considered as a series of blocks of data that are securely chained together.New block are formed as the participant make new transaction. These blocks are encrypted and given a hash value that represents a unique identifier of the data within that block. The hashing works over a standard algorithm that works over the data to compress it into the code. Each block contains a hash value that is dependent on the hash of previous block. So they are all linked together. If any of the block is altered then all the block linked to it is altered. This makes the data entered tamper proof.

Each block also contains a time stamp so that we know what happened and when.

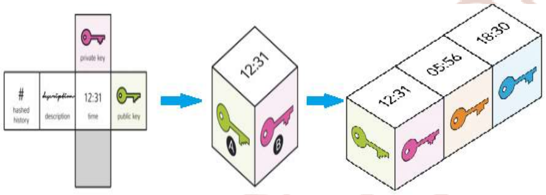

Fig 1 : Creation of a block

B. *Mining :*

Mining computers on a network validates transaction, add them to the block they are building, then broadcast the completed block to other nodes. So that they all have a copy of the database. Because there is no centralized component to verify the alterations of database, the block chain depends on a distributed consensus algorithm. Once completed a block goes into the Blockchain as a permanent record. The blockchains are designed so the transactions are immutable i.e. It cannot be deleted.

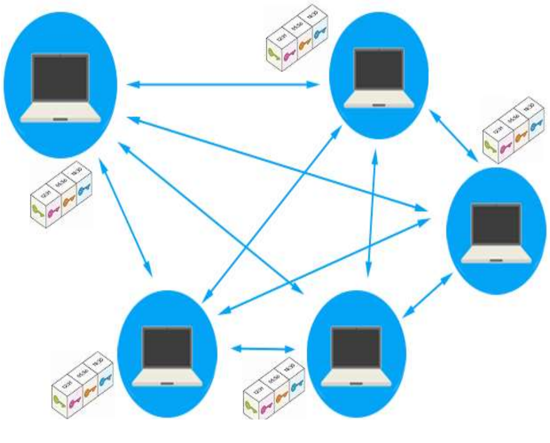

Fig 2: Peer-To-Peer distribution of a block in a Blockchain network

C. *Proof of work :*

In order to randomize the processing of blocks across the nodes blockchain uses various time stamping schemas. Proof of work is one of them. Proof of work describes a system that requires a non-insignificant but feasible amount of effort usually by requiring computer processing time. Miners compete to add the next block on the chain by racing to solve a very complex cryptographic puzzle. The first to solve the puzzle wins a lottery as a reward for his/her effort.

D. *Network consensus :*

The Blockchain is a distributed system, this means there is no centralized organization to maintain or verify the entries on the database. So, the database is maintained by a large number of computers. But these computer nodes in the network itself cannot be trusted. Thus it is required that the system provide a mechanism for creating consensus between scattered or the distributed parties. These do not need to trust each other but just need to trust the mechanism by which their consensus have arrived. Any computer that has been connected to the network and using a client can perform the task of validating transactions

Each of these miner computers gets a copy of the blockchain, which gets down noted automatically upon joining the network. When new entries into databases are made these changes are automatically updated across the network.

E. *Public key cryptography :*

Blockchain security methods include public key cryptography. A public key which is a long random looking string of characters (1MhQjwwFJdDiLMuYdDkoqJ9cQ1oD5ZdidP) is in address of blockchain. Value tokens sent in the network are recorded as belonging to the address. A private key is like a password that give the owner access to their digital access or data. A public key is associated with the private key so anyone make an encrypted transaction to the public key address. The encrypted message can only be deciphered with the private key that correspond to the public key. The public key can be openly distributed.

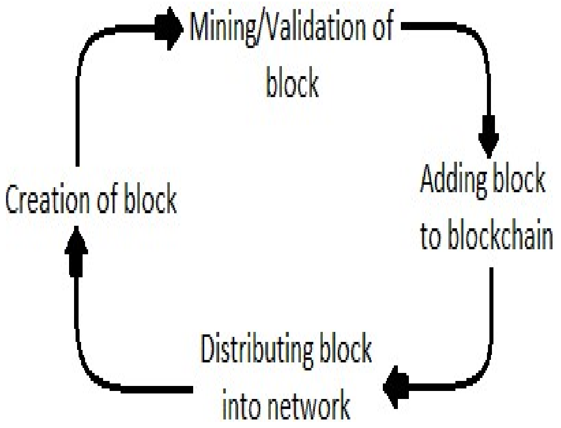
Mining/Validation of block
Adding block to blockchain
Distributing block into network
Creation of block

Fig 3: Working of blockchain

IV. EVOLUTION

Over the past few years Blockchain has been evolving rapidly from the original Bitcoin protocol to the 2nd generation Ethereum platform to today's process of building third generation of Blockchain. In this evolution we can see how the technology is evolving from simply being a distributed database to fully fledge globally distributed cloud computer.

A. Blockchain 1.0

The first block chain was conceptualized in 2008, by an unknown person or group named "SATOSHI NAKAMOTO" . The concept and technicality was scripted on a white paper termed ' Bitcoin : A Peer-To-Peer Electronic Cash System '. These ideas were first implemented in year 2009 as a core component which supported bitcoin where it served as a public ledger for all transactions. The invention of blockchain for bitcoin made it the first digital currency which solved the double spending problem without the need of any trusted authority or central server. It was a year later when we really seperated the concept of Blockchain from Bitcoin. It came to understand that the technology can have more general applications beyond digital currencies and functioning as a distributed ledger, tracking and recording any forms of values.

B. Blockchain 2.0

Within few years of Bitcoin 2nd generation of blockchain emerged. It was designed as a network on which developers can build any applications. This was possible with the development of Ethereum platform. Ethereum was initially described in a paper by detalic buteran in may'13 with a goal to build a distributed application. The system went live 1 year after and being very successful attracting a vast and dedicated community of developers. The important contribution of ethereum as 2nd generation blockchain is that it works to extend the capacity of technology from primarily being a database to more of becoming a general platform to run any decentralized applications and smart contracts.

C. Blockchain 3.0

In response to the limitations of 2nd , a 3rd generation of blockchain is currently under development. Many different organizations are currently working on the next generation blockchain infrastructure. Such projects include DFINITY, NEO, EOS, IOTA. Lightening network seeks to increase the capacity of existing block chains. The main idea is to not store the small transactions on the main blockchain. This is called an ' Offchain ' approach.It works by creating a small communities where small transaction takes place without each of those transactions registered on main block chain. This reduces the work load on main blockchain and makes it possible to run many small transactions within the sub network.

IOTA is trying to achieve high transactional rate using parallel transaction approach. The data structure here is more like a linear chain. Also, There are not specialized miners in this instead here every node that uses the network is a miner. In this network there is not any transaction fee for validation.

The next generation of blockchain will take us a step further in the journey. What we call the blockchains today is very limited and very efficient we still have many difficult problem to solve. The distributed cloud is under consideration to decrease the limitations and improve efficiency.

Table 1 list some of the specification and limitation of the evolution introduced so far.

Table 1 specification and limitation of evolution introduced so far

Evolution & Version	Specification	Limitation
Block-chain 1.0	1. Distributed database was introduced. 2. Transaction without third party. 3. Introduction to digital currency.	1. Programming and scripting limitations. 2. Limited to currencies only
Block-chain 2.0	1. Brought a programming language to blockchain. 2. Customizable transaction. 3. Introduction to Smart Contract. 4. Introduces DAPPs(Decentralized apps).	1.Scalablity 2.Mining consumes excess energy 3.Transactions per second
Block-chain 3.0	1. Scalable using Offchain approach 2. High transaction rate. 3. Distributed cloud	Limited to currency only

V. APPLICATIONS

The qualities including Distributed, Public, Time stamped makes the application fields for Blockchain technology so vast and wide. The rise of the technology has made most field of application fall for it. Some of the most Highlighted application fields are:

A. ***Digital Identity**:* Blockchain technology can be a solution to many digital identity issues, where identity can be uniquely authenticated in an immutable, and secure manner[6]. Current methods includes the use of problematic password-based systems of shared secrets exchanged and stored on an insecure systems. Blockchain technology can be applied to identity applications in these areas:

- Digital Identities
- Passports
- E-Residency
- Birth Ceritificates
- Wedding Certificates
- Online Account Login

B. ***Smart contracts*:** What if you could cut your mortgage rate, make it easier to update your will? The world of smart contracts is fast approaching. These are legally binding programmable and digitized contracts entered on the blockchain. They are smart as they are automated and can self-execute. What developers have to do is to implement legal contracts as variables and statements that can release of funds using the network as a '3rd party executor', rather trusting any single central authority.

C. ***Distributed cloud storage:*** Cloud storage using a Blockchain-powered network improves its security and decreases its dependency.

D. ***Digital voting**:* The greatest barrier in having electoral processes online is its security. Using blockchain, a voter could check that her or his vote was successfully transmitted while being anonymous.

Even this technology is recent and under study many companies in their fields have started using the technology. Some of them are:

CONCLUSIONS

Blockchain technology was the base for the evolving of Bitcoin. The distributed ledger coupled with the security of BlockChain makes it an attractive technology in solving the current financial as well as non-financial industry problems. The public, distributed and secure are key factors which makes it to be influenced to different fields and sectors. According to many this technology can have an impact similar to the introduction of Internet.

What we seeing, is BlockChain technology is going through slow adoption due to the risks associated with it. Many of the startups may fail or will fail with few winners. Having said this, we should be seeing significant adoption of the technology in a decade or two.

REFERENCES

1. J.bonneau, A.Miller, J.Clark, A.Narayana, J.Kroll, W.Felten, "SoK : Research Perspectives and Challenges for Bitcoin and Cryptocurrencies", IEEE Symposium on Security and Privacy. 2015
2. Michael Crosby , Nachiappan , Pradan Pattanayak, Sanjeev verma, and Vignesh Kalyanaraman ," .BlockChain Technology: Beyond Bitcoin ", Applied Innovation Review,Berkeley, Issue No. 2, June 2016
3. Jesse Yli-Huumo, Deokyoon Ko Where Is Current Research on Blockchain Technology?—A Systematic Review
4. A. Dyhrberg,"Bitcoin, gold and dollar-A GARCH volatility analysis", Elseiver, 2015
5. F.Velde, "Bitcoin: A primer", IDEAS2013
6. G. Andresen. Blocksize Economics. bitcoinfoundation.org, October 2014.
7. J. A. Kroll, I. C. Davey, and E. W. Felten. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In WEIS, 2013.
8. C. Percival and S. Josefsson. The scrypt Password-Based Key Derivation Function, 2012.
9. S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. http: //bitcoin.org/bitcoin.pdf, 2008.
10. I. Miers, C. Garman, M. Green, and A. D. Rubin. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In IEEE Symposium on Security and Privacy, 2013