A Comprehensive Study on Blockchain Technology

D. Madavi

Assistant Professor, Dept. of CSE, DVR & Dr. HS MIC College of Technology, Andhra Pradesh, India

---***---

Abstract - *A Blockchain is an emerging Technology now-a-days mostly from last two years a more funding is also spent on research of the technologies used. This Technology is used almost in all the sectors of real world applications which use E-Tag or Electronic or Online. It can change the dimensions of the digital operations by performing distributed ledger transactions in daily human's life by averting the third parties. Blockchain Technology is situated under the cryptocurrencies such as Bitcoin, Ethereum, Facton, Bitshares, Namecoin and Truthcoin platform and implemented in a Distributed environment with decentralized database having strong consistency, reliability and security support. This paper will gives a demonstration about the future challenges, working and some of the applications of Blockchain Technology.*

Key Words: Bitcoin, Blockchain Technology, Blockchain3.0, Cryptocurrency, Distributed ledger transactions, Ethereum.

1. INTRODUCTION

A Blockchain is one of the biggest buzzword in the technology now-a-days. First major application of Blockchain Technology was Bitcoin, which was released in 2009. A bitcoin is a public ledger system of every transaction taken place through the internet in a secure and safe manner. The bitcoins Blockchain works in a decentralized way. While traditional digital currencies are issued by central banks whereas Bitcoin used in Blockchain has no central authority. Instead, this Bitcoin was maintained by a network, which solves the complex mathematical problems. The Difference between Blockchain and Bitcoin is shown in the table1.

Motivation behind this technology is in the year of 2009, the world is feel shocked with a disastrous collapse in the financial sector and a political leaders were examine about what could be done and what should be done, a bitcoin technology has been came into picture all around the world. This project has defined entirely new form of money; it has caused a state of confusion and accepts this change willingly and enthusiastically. In which both rules and its execution are provided by the software rather than the human beings. Bitcoin achieve two things: it makes the money to be transparent and replaces the need of private organizations for transferring money over the internet [1].

The success of Bitcoin project, a Blockchain Technology is very useful in almost all of the applications which use the internet. This technology was developed for efficient, reliable, cost effective and secure systems for developing financial transaction of a distributed ledger system. Failures of current transactional systems are:

- Business transactions are in-efficient, expensive and chances of attacks are high.
- Transactions time is too long for settlement of money.
- Limited transparency and inconsistent information.
- If a bank is centralized then cyberattacks and fraud will be more.
- The intermediator that is need of third parties validation adds inefficiencies.
- Transactions cash is in small amounts ad done only in local.

An increasing in transactions volumes, complexities, E-transactions, In-app purchases, mobility of people and devices, emergence of IOT (Internet of Things) needs a faster payments, transparency, reliability and security in a distributed public ledger environment [4].

Not only Bitcoin, there are some other companies which develops a Blockchian platform to help firms to build technology related processes. Ethereum, Ripple, Hyperledger, IBM, R3 are some decentralized technologies developed for Blockchain Platform. Interoperability is the one problem that there is no guarantee that each one is compatible with the other. Carlos Torres Vila, CEO, BBVA says that this technology brings the more efficient processing, cheaper, more traceable and Alicia Pertusa, Head of Digital Transformation at the investment banking division of BBVA, She said that the loan issue process is saving the 40 to 50 percent of time on Blockchain over the traditional loan process. This process is not just causing disruption to the process but it shows the impact on the running of current products [5]. Tokens are used in traditional process whereas block chains are used here and these blockchains are unstructured in nature. This BBVA Blockchain loan trail was between two parties initially but later this technology greatly helps to processes of syndicated loans for many parties. They wanted to build it step by step later add more parties to our system.

1.1 Origins and underpinnings

The Innovation Foundations of Blockchain Technology includes the multidisciplinary fields such as software engineering, cryptographic science, Distributed computing, and economic game theory are as shown in the below

Figure1. Blockchain will operate at the intersection of these fields and provides the scalable and base for the software infrastructure. This structure supports global decentralized peers with economic incentives and security of digital assets. In the year of 1991, the Merkle tree was used to create a "Secure chain of blocks", which is a series of data records each one connected the one before it. The new record or data block in this chain would be the history of the entire chain and thus a Blockchain was created. Later Satoshi Nakamoto, who is a Japanee posted an innovative paper to cryptographic forum in the year of 2008 of October 31st. In this paper he specifies a way to overcome the problem of Double-Spend layout, which is a problem of creating a trouble with previous cryptocurrencies. Instead of specifying directly the Blockchain Technology, he specifies it as a chain of hashed timestamps. Here each timestamp includes a timestamp of previous in its hash one behind another [6]. Later this is refined for bitcoin. Each block of chain was cryptographically linked to the previous using hash digest. Blockchain is little more than a sequence of records; each hashed and linked to the previous one as shown in the figure2. In computer engineering terms, Blockchain is a cryptographically hashed data structure (linked list) with a structured collection of blocks.

Blockchain Technology

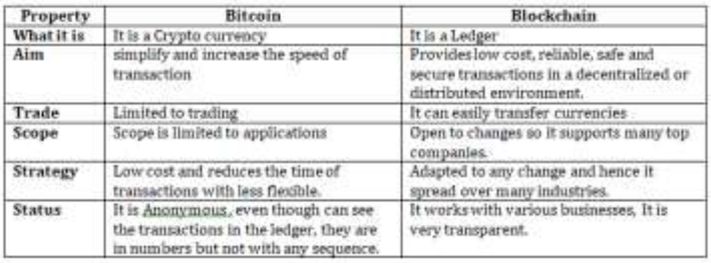
Fig -1: Foundations of Blockchain Technology

1.2 Bitcoin

The Bitcoin users do not reveal who they are. They maintain a digital wallet and by the use of special software, for trading the currency to exchange traditional currency or goods and services. Several thousands of businesses worldwide accept bitcoins currently in payment systems even for small online transactions at anytime and anywhere between any users worldwide. Users can take the advantage of bitcoin for verifying earlier transactions, to purchase from other users. Basic process is: if a person wishing to make a payment, then issues a payment instruction spread across the network of their persons. Standard cryptographic techniques are useful for both the persons to check that the transaction is valid. If block of transactions are verified successfully then receive then allocation of newly created currency is done. The process of transactions step-by-step is mentioned in the working model of this paper. The initial funding of bitcoins is an empty block with no transactions done other than the allocation of new bitcoins as a reward for solving the puzzle. The first block created 50 new bitcoins per block and this protocol divides into two equal parts and calls every 210000 blocks roughly every four years. The Bank of England, UK they offer 25 bitcoins per block and is likely to be reduced to 12.5 bitcoins per block in 2017. Therefore a total of planned bitcoins is 21 million, mostly reached to 2040. Currently there are little over 13 million bitcoins in usage, over an approximately one or two million users worldwide distributed.

The price of bitcoins had increased in the market over financial transactions since bitcoins scheme is introduced. This usage is rising roughly 5000% over the past two years said by UK Bank [10].

Table -1: Difference between Bitcoin and Blockchain



Property	Bitcoin	Blockchain
What it is	It is a Crypto currency	It is a Ledger
Aim	simplify and increase the speed of transaction	Provides low cost, reliable, safe and secure transactions in a decentralized or distributed environment.
Trade	Limited to trading	It can easily transfer currencies
Scope	Scope is limited to applications	Open to changes so it supports many top companies.
Strategy	Low cost and reduces the time of transactions with less flexible.	Adapted to any change and hence it spread over many industries.
Status	It is Anonymous., even though can see the transactions in the ledger, they are in numbers but not with any sequence.	It works with various businesses, It is very transparent.

2. PRINCIPLES, CHARACTERSTICS AND TYPES

2.1 Characteristics

The Six characteristics of Blockchain Technology are:

- **Consensus Driven** (Trust Verification): for a transaction to be valid all other parties must agree up on its validity.
- **Immutability** (permanent and Tamper-proof): No participant can tamper with the transaction after it has been recorded. Once block is added, into chain then it cannot be altered. This creates trust in the transaction record.
- **Decentralized** (Networked copies): a blockchain is stored in a file that can be accessed and copied by any node on the network with reliability and consistency
- **Transparent** (Full transaction history): Due to the property of open, a Blockchain file can be accessed and audited by any party. This creates provenance under which asset lifetime can be calculated. Participants knows that where the asset came from and its ownership has changed over time.
- **Finality**: A single shared ledger provides one place to go the completion of a transaction.
- **Chaincode** (Business Contracts): Encapsulates the terms of contract agreement according to the business participants. Chaincode is stored on the validating peer nodes in the distributed network system.

2.2 Taxonomy

There are three different types of Blockchains are[12][13]:

Public orPermissionless Blockchains are accessible to anyone in the world. These Public Blockchain Protocols using Proof-of-work (PoW) consensus protocols are open source. In a public Blockchain any one can be able to download code and start running a public node on their local device to validate the transactions in the network, thus participating in the consensus processes. Consensus process is a process for determine what blocks are added to the chain and what the current state is. Anyone can make transactions in a network and add them as blocks on a chain if they are valid. Anyone can read and write permissions on the centralized database. Users who want to use this public Blockchain Technology can download the correct software tools and join in the distributed peer-to-peer network. Examples are Bitcoin, Ethereum, Monero Dash, Dodgecoin etc.

Private Blockchains have strict permissions for read and write operations. Accessing rules of the Blocks are changed if necessary whenever a trusted node wants to access, and controls the transactions are being to Blockchain by a single authority. Sometimes read permissions are also restricted if the data is not necessary as public always therefore providing great privacy. Although this approach puts it closer to the centralized database, it can add certain degree of cryptographic auditability.

Permissioned Blockchain provides a hybrid between public and private Blockchains.

3. WORKING MODEL

Internet changed the way we transfer the information as Blockchain changing the way we transfer a value. While talking about the working of this technology people need o know about different things and are confusing sometimes. Blockchain is generally referred to as a decentralized ledger of all transactions across a peer-to-peer network. Blockchain technology is not as same as bitcoin, instead Blockchain technology is underlying on the bitcoin and different other cryptocurrencies. Using these technologies different participants such as buyers, sellers can interact directly over the internet without using a third party in a distributed environment. Basically, Blockchain is essentially a database of collection transactions happening in the network. The database is public then not owned by a single party and all transactions are constantly synchronized to keep transactions up to date and secured by the art of cryptography hacker proof. Blockchain technology works as a network of computers all of which must approve a transaction that has been taken place before it has been recorded in a chain of computer.

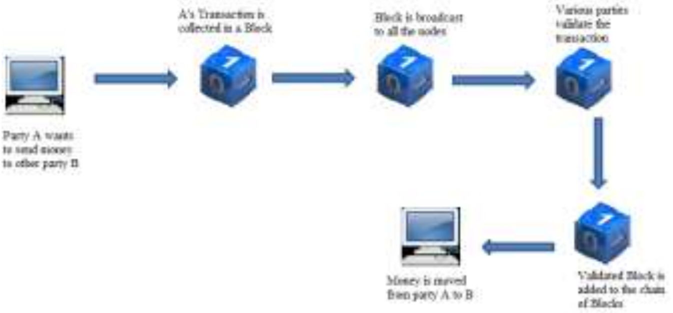

A's Transaction is collected in a Block
Block is broadcast to all the nodes
Various parties validate the transaction
Party A wants to send money to other party B
Money is moved from party A to B
Validated Block is added to the chain of Blocks

Fig -2: Blockchain and Bitcoin Example

Code of bitcoin makes the transactions secure and sharing in the network after the transaction is validated. This can be recorded on a network to access any public ledger. But on a Blockchain the information is transparently held in a shared Database without any intermediaries, which increases the trust among the parties.

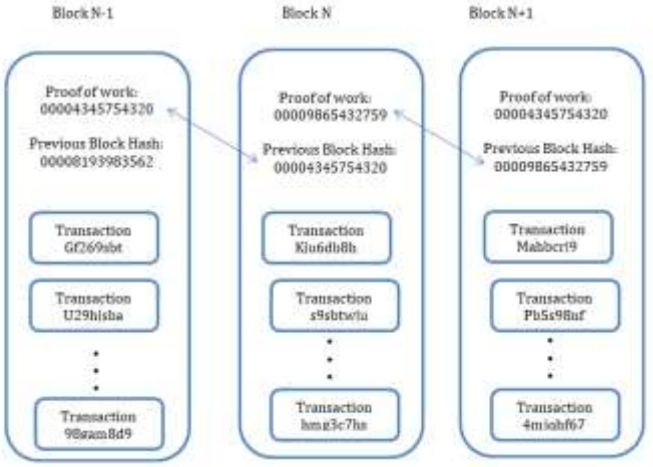


Fig -3: A Blockchain

There are various top most cryptocurrencies are Bitcoin(BTC),Ethereum (ETH), Ripple (XRP), Bitcoin Cash (BCH), Stellar Lumens (XLM), LiteCoin (LTC), Cardano (ADA), Tether (UDST) ,VeChain (VET), Maker (MKR) and many more[9]. The Blockchain technology is operated on above the network layer and below the applications. It provides abstractions for record of transactions, consensus rules and peer-to-peer network [16]. Figure 4 represents the stack of Ethereum for Blockchain Technology. Due to Blockchain layer and decoupling of smart contracts with blockchain layer, it creates the flexible environment than Bitcoin Blockchain. Smart Contracts are the piece of code implemented with specific rules and placed on top of Blockchain network, where digital assets are controlled by these smart contracts. These smart contracts are used for simple transaction like sending money from A to B. The smart contract code is auto executed if and only if all the parties are full fil the arbitrary rules. Furthermore these smart contracts can be used for more complex transactions like governing a group of people who shares the same interests and goals.

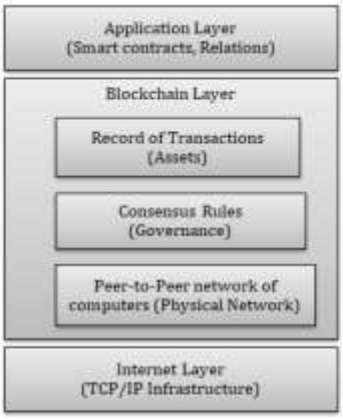


Fig -4: Blockchain Technology Stack of Ethereum

This shows the easy understanding of Blockchain technology, with an example of how a transaction has to be happened using Bitcoin. Anyone can download a simple piece of software and install on their computer to use bitcoin. Here are not able to register and giving personal details, to use this decentralized shared peer-to-peer system. After having a wallet, it creates a unique identity by generating addresses for a node on the network. Suppose if two parties wants to make a transaction as party A send money to party B. Here money is in the form of bitcoins and this transaction will eventually changes the bitcoin balances for both party A and party B. This transaction is collected in a block. A block records bitcoin transactions that have not entered at any of the previous block. The initial block is called as a genesis block. The new block is then broadcast to all the parties or nodes in a network. All other nodes in the network valid through a process called mining. With the bitcoin miners use special software to solve mathematical problems linked to blocks, named as proof-of-work, which is the basis for approving the transaction as shown in the figure 3. Miners are issued a certain number of bitcoins in exchange for performing the transaction. Once approved the new block is added to the Blockchain. Once block is added to the ledger balances are updated to reflect the new balances for all parties. This process goes on and a new block is formed for every ten minutes with a new set of transactions. The implementation way of block chain code is in the reference[17].

Blockchain is a data structure of a structured collection of shared ledger of transactions. The figure 3 shows the data structure used in the Bitcoin Blockchain. The Blockchain contains any number of blocks. For example, the bitcoins Blockchain consisting of more than 210000 of blocks as of January 2018 [7] [8] [11]. A blockchain is a double linked list of blocks, having a pointer to the next block as well as to the previous block. Each block is having the three different fields:

1. Data corresponding to the number of Transactions
2. Hash of the previous block
3. proof-of-work.

Each hash value of above is called a proof-of-work [14] for that block. Proof-of-work is obtained by solving a cryptographic puzzle. New block is added to the chain by using a process called mining. Once updated Blockchain becomes available at all the nodes.

4. EVOLUTION AND APPLICATIONS

4.1 Evolution

Blockchain Technology was perceived in 2008 to record Bitcoin Transactions in an immutable and publicly verifiable way. Three different evolutions of this technology is: Blockchain1.0, Blockchain2.0, Blockchain3.0 [3][4]. Blockchain1.0 related to bitcoin (http://bitcoin.org) and cryptocurrencies. More than 600 cryptocurrencies can be created from the birth of Bitcoin. The most popular ones are Ethereum is to create Blockchain applications easily (www.ethereum.org), Monero is for guarantee intractability of transactions (http://getmonero.org), and Ripple which enables instant payments for banks (http://ripple.com). Blockchain1.0 is for money, Blockchain2.0 is for registering, transferring contracts and conformation of those and Blockchain3.0 is for applications such as government, science, healthcare, education, Industries, home, financial services and more.

4.2 Applications

The first application of Blockchain technology is money. The applications of this technology are enormous and heterogeneous. Companies such as IBM, Amazon, Samsung, Verizon wireless, Overstock are in order to take a look at the Blockchain technology and uses for their own applications. Some of the Biggest US banks joined with the New York based financial Technology firm named as R3 for creating a framework for Blockchain technology. It is the first time of application of Blockchain into banking sector, the banks Royal bank of Scotland, Credit Suisse, UBS, BBVA, JPMorgan, State Street, common wealth bank of Australia have joined and create an application for Banks named as Blockchain technology [15].

General applications of this technology are bonded contracts, Banking Transactions, third-party arbitration, Multi party signature transactions. Financial related transactions such as charity donations, stocks, private or public equities, crowd funds, mutual funds, microfinance, air miles, currencies, bonds, insurance policies [2]. Public sector applications includes Voting ID's, passport registrations, identity cards, driver's licenses, Marriage certificates, birth certificates, death certificates, notary, vehicle registration, land or property certificates, quotations, health and safety inspections, building permissions, gun permissions, criminal records, court records, government records, student degree certifications, grades, learning outcomes, genome data, medical records, human resources records. Used in the private records like loans, contracts, bets, trusts, wills, attestations such as notarized documents, proof of insurance or ownership.

Distributed Blockchain technology is applied in the fields online identities, copyrights, trademarks, reservations, patents, digital rights, proof of authenticity. Not only in government sector, educations, finances and many more, but also this technology is used in other sectors such as cultural activities like, sports scores, cultural events, historical events, documentaries, weather data, traffic, music industry, temperature data.

4.3 Advantages

- It implements the shared data in peer-to-peer networks, without loss of data while storing and accessing.
- It ensures trust between the parties due to digital signature and validation
- Storing blocks of information on nodes, without loss of data even when an unexpected events are done.
- Transparency is allowed, to read different states of Blockchain not only the final transaction.
- Decentralization
- Automation with smart contracts between the parties.
- Once data is entered, cannot be changed or erased.
- Increasing the resilience
- Reducing the complexities and costs.
- No single point of failure due to distributed in nature.
- Used to coordinate and automate the interactions with external parties as well as own processes.

4.4 Disadvantages

- It needs high power consumption due to bitcoin transaction.
- More memory space is required for replication of data.
- Addition of new block to chain is slow.
- Transparency and immutability may provide some problems to user's reputation and privacy, because every network node can be able to access and store copy of the Blockchain.
- Smart contracts may be buggy.
- Mining requires expensive hardware and majority of computer power is wasted. To reduce the computing power of mining we can use proof-of-stake instead of proof-of-work.

5. CONCLUSION

Blockchain technology should not be considered as a way-out technology but it is an enthusiastic and used with various specific future research fields such as Artificial Intelligence (AI), Internet of Things (IOT), Data Mining concepts and in other fields. On the road to the future, the rapport of Blockchain with these research fields will provide unlimited innovations and revolutions to our society. There is a strong necessity of knowing about the details of how it is working, characteristics, uses of the Blockchain Technology. This study of paper have gotten a taste of concepts of Blockchain and will help to the peoples such as professionals and researchers who want to perform their work with Blockchain Technology and make decisions easy with this study.

REFERENCES

[1] Morgen Peck, Freelance Technology Writer, A White Paper on "Reinforcing the links of Blockchain " in IEEE Spectrum Magazine special edition "Blockchain World", November 2017.

[2] Valentina Gatteschi, Fabrizio Lamberti, Claudio Demartini, Chiara Pranteda, Victor Santamaria, "To Blockchain or Not to Blockchain: That is the Question?" in IEEE Computer Society,1520-9202 ©March/April 2018.

[3] Melanie Swan,"Blockchain: Blueprint for a New Economy" vol. 3, no.3, O'Reilly Media, pp.38-72, February 2015.

[4] Manav Gupta, "IBM Blockchain for Dummies" 2nd Edition, a Wiley brand.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[5] Arjun Kharpal ,"Blockchain Revolution: Everything you need to know about the Blockchain" ,CNBC, June 2018, in press.

[6] Karim Sulthan, Umar Ruhi and Rubina Lakhani, "Conceptualizing Blockchains: Characterstics and applications", IADIS International Conference Information Systems 2018.

[7] Shivika Narang, Praphul Chandra, Shweta Jain and Y.Narahari, "Foundations of Blockchain Technology for Industrial and Societal Applications", ACCS Publications.

[8] Satoshi Nakamoto, "Bitcoin: A peer-to-peer Electronic Cash System", Bitcoin Organization.

[9] Jacob Bushmaker, "The Top 50 Cryptocurrencies", in Invest in Blockchain © 2017-2018. https://www.investinblockchain.com/top-cryptocurrencies/ https://www.investinblockchain.com/periodic-table-cryptocurrencies/

[10] Robleh Ali, Roger Clews and James Southgate, "Innovations in Payement Technologies and the emergence of digital currencies", Emergence of Digital currencies topical articles, Bank of England, 2014.

[11] Tomaso Aste, Paolo Tasca and Tiziana Di Matteo "The Blockchain Technology: The foreseeable Impact on Society and Industry", published by the IEEE computer society, September 2017.

[12] Michail Sidorov, Ming Tze Ong, Ravivarma Vikneswaran, Junya Nakamura, Ren Ohmura and Jing Huey Khor, "Ultralightweight Mutual Authentication RFID Protocol for Blockchain Enabled Supply Chains", IEEE Access, DOI: 10.1109/ACCESS.2018.2890389.

[13] Shermin Voshmgir, Valentin Kalinov, "Blockchain: A Beginners Guide", BlockchainHub , September 2017.

[14] Chantelle Lafaille, "What is Blockchain Technology? A Beginner's Guide", article in the -Invest in Blockchain, February 2018. https://www.investinblockchain.com/what-is-blockchain-technology/

[15] Michael Crosby, Nachiappan, Pradhan Pattanayk, Sanjeev Verma, Vignesh Kalyanaraman, "Blockchain Technology Beyond Bitcoin", Berkeley University of California, Sutardja Center for Entrepreneurship & Technology Report, October 16, 2015.

[16] https://blockchainhub.net/blockchain-intro/

[17] https://github.com/IBM/BlockchainNetwork-CompositeJourney/blob/master/README.md