Study on Blockchain Technology

M. Gayathri[1], M. Rashmika[2]

[1,2]Student, Dept. of Computer Science, Sri Krishna Adithya College of Arts and Science, Coimbatore, India

Abstract—**A blockchain, originally block chain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a timestamp and transaction data. By design, a blockchain is inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority. Blockchains are secure by design and are an example of a distributed computing system with high Byzantine fault tolerance.**

Index Terms— **transaction, block chain, ledger, digital**

I. INTRODUCTION

Blockchain is currently one of the hot topic specially in financial sector. A blockchain is a singly Linked List of block, with each block containing a number of transactions. It provides a decentralised, immutable data store that can be used across a network of users, create assets and act as a shared black book that records all transactions. Each transaction can be easily queried, affording greater transparency and trust to all parties involved. With the original creator, or creators, being anonymous the true motivations behind blockchain are arguably unknown. However it has proven to be a more than adequate solution to the many issues. The preface of cryptocurrencies, specifically Bitcoin, has brought the concept of blockchain technology into the mainstream. A blockchain is a continuously growing distributed database that protects against tampering and revision of data. The industry has already seen the power of a distributed system with Git Version control; blockchain builds on the same Merkle tree approach, but also adds consensus, which specifies rules on how data can be added and verified. Transactions are added in blocks and must follow the exact order in which they happened thus the name blockchain.

II. BLOCKCHAIN FUNDAMENTALS

Originally blockchain was segregated as block chain where blocks holds the list of digital records which are secured using encryption technology (Cryptography). Blockchain is a shared, distributed ledger which helps in processing any digital transaction over the business network and track the tangible or intangible assets involved that facilitates the process of recording transactions and tracking assets in a business network. Asset can be tangible a house, a car, cash, land or intangible like intellectual property, such as patents, copyrights, or branding. Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved. A blockchain by itself is just a data structure defining how the data is stored and logically put together. Every block in a chain can be considered as a pages in a book, where every page has text and also the meta-data which tells the title, chapter number, page no. Transaction data is permanently recorded in files called blocks. They can be thought of as the individual pages of a city recorder's record book or a stock transaction ledger. Blocks are organized into a linear sequence over time, also known as the block chain. New transaction are constantly being processes by miners into new blocks which are added to the end of the chain and can never be changed or removed once accepted by the network.

Fig. 1. Blockchain

III. BLOCKCHAIN TECHNOLOGY

A blockchain is a digitized, decentralized, public ledger of all crypto currency transactions. Constantly growing as completed blocks are recorded and added to it in chronological order, it allows market participants to keep track of digital currency transactions without central recordkeeping. Each node gets a copy of the blockchain, which is downloaded automatically. A blockchain is the structure of data that represents a financial ledger entry, or a record of a transaction is digitally signed to ensure its authenticity and that no one tampers with it, so the ledger itself and the existing transactions within it are assumed to be of high integrity.

International Journal of Research in Engineering, Science and Management
Volume-1, Issue-9, September-2018
www.ijresm.com | ISSN (Online): 2581-5782

175

IV. USECASE BLOCKCHAINS

In Bitcoin's blockchain, the blocks contain information about transactions in Bitcoin. The block states who sends which Bitcoins to whom. As the blockchain has been used to keep track of the movement of all Bitcoins since their inception, the ledger can be checked to know exactly who owns which Bitcoin at any time. The 'who owns what' at any time, is what we call the current 'state' of the blockchain. A transaction only occurs once it is included in a block and added to the chain. Hence, when a block is added to the chain, the state of the blockchain is updated. After all, Bitcoins have moved.
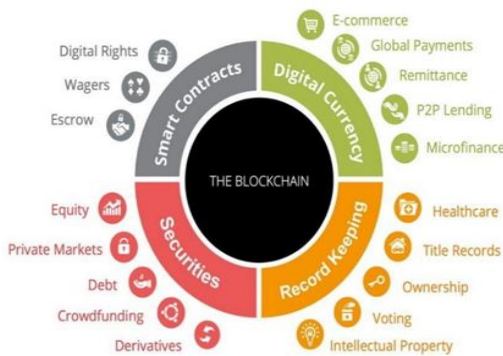

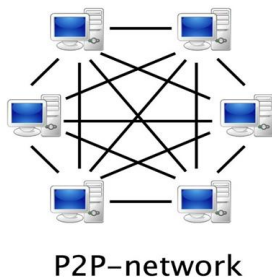Fig. 2. Use case blockchain

V. PEER-TO-PEER NETWORKS

Fig. 3. Peer-to-Peer network

To use a blockchain as a ledger for transactional data, I have to be able to check in the blockchain if someone actually made a transaction to my address or wallet. If the blockchain was only stored on one computer, and it happened to be turned off, this would be annoying to say the least. Therefore, the current state of the blockchain is downloaded, synchronized and made available by a large number of computers worldwide. These computers are called 'nodes', and they work together in a peer-to-peer network to ensure the blockchain is secure and up-to-date. Every one of these nodes stores the complete, updated version of the blockchain. Every time a new block is added, all the nodes update their blockchain.

VI. WORKING PROCESS

Every time a new transaction is initiated, a block is created with the transactions details and broadcast to all the nodes.

Every block carries a timestamp, and a reference to the previous block in the chain, to help establish a sequence of events. Once the authenticity of the transaction is established, that block is linked to the previous block, which is linked to the previous block, creating a chain called blockchain. This chain of blocks is replicated across the entire network, and all cryptographically secured which makes it not only challenging, but almost impossible to hack. When a new transaction or an edit to an existing transaction comes in to a blockchain, generally a majority of the nodes within a blockchain implementation must execute algorithms to evaluate and verify the history of the individual blockchain block that is proposed. If a majority of the nodes come to a consensus that the history and signature is valid, the new block of transactions is accepted into the ledger and a new block is added to the chain of transactions. If a majority does not concede to the addition or modification of the ledger entry, it is denied and not added to the chain. This distributed consensus model is what allows blockchain to run as a distributed ledger without the need for some central, unifying authority saying what transactions are valid and which ones are not.
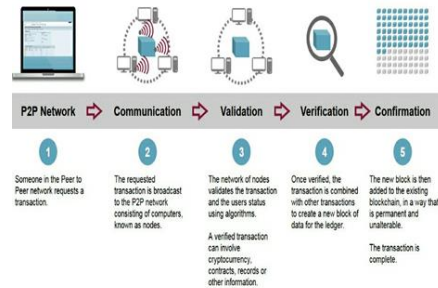

Fig. 4. Working process

VII. UTILITY OF BLOCKCHAIN

- It helps to maintain strong and secure Digital Identity
- Tokenisation : For the purposes of authenticating a unique physical item, the items are paired with a corresponding digital token
- Data Management for big organization
- Regulatory compliance is a big business opportunity by for many blockchain developers.
- For Audit Trail in any large financial institutions
- It can be a great technology for Contract Management between two parties involved.

Advantages:
- Empowered users
- High quality data
- Durability, reliability and longevity
- Process integrity
- Transparency and immutability
- Ecosystem simplification

- Faster transactions
- Lower transaction costs

Disadvantages:
- Performance
- Nascent technology
- Uncertain regulatory status
- Large energy consumption
- Control, security and privacy
- Integration concerns
- Cultural adoption
- Cost

VIII. CONCLUSION

Blockchain development is in its infancy. But already the technology is old enough that the community has bifurcated both culturally and technically. This should not be viewed as a bad thing. When the first blockchain was invented it sought to solve one very specific problem. Today, players in the space are stretching to reorganize every facet of the digital terrain. As the problems take on more definition, it becomes clear that there is not a single solution. At the same time, if the efficiencies gained by one successful blockchain project are to be shared across domains, then developers and industry managers will have to think about interoperability from the very beginning. Blockchain technology could be quite complementary in a possibility space for the future world that includes both centralized and decentralized models. Like any new technology, the blockchain is an idea that initially disrupts, and over time it could promote the development of a larger ecosystem that includes both the old way and the new innovation.

REFERENCES

[1] https://www.investopedia.com/terms/b/blockchain.asp
[2] https://en.m.wikipedia.org/wiki/Blockchain
[3] https://www.cio.com/article/3055847/security/-blockchain
[4] https://codeburst.io/blockchain/-technology.