2017 International Conference on Computational Intelligence and Networks

# An Overview of the Emerging Technology: Blockchain

Rishav Chatterjee
School of Computer Engineering
KIIT University
Bhubaneswar, India
rishavpiku@gmail.com

Rajdeep Chatterjee
School of Computer Engineering
KIIT University
Bhubaneswar, India
cse.rajdeep@gmail.com

***Abstract*—A Blockchain is basically a decentralized, distributed ledger of all the transactions or events which takes place only after involving multiple parties. It ensures high level of security as the transactions which takes place are entirely anonymous. Each transactions or digital events taking place in a Blockchain network is verified, only if it is agreed upon by the consensus of the majority party of the users participating in this process. Blockchain is one of the emerging technologies in today's world and a lot of revolution and research has just began regarding this distributed technology. Bitcoin has been the most popular cryptographic currency since it was invented and it is the best example that uses the Blockchain technology. In this paper, we will discuss about the research being done on this new domain of Computer Science. We will outline the underlining concepts about this new technology. We will try to peek a bit into its applications in the financial and non financial sector. It is not only the most popular topic to discuss about, but is the most technological breakthrough, that is all set to revolutionize the entire world.**

***Index Terms*—decentralized; distributed; ledger; consensus;**

## I. Introduction

Blockchain is a decentralized ledger or data structure. It can be referred as blocks in a chain where the corresponding blocks refer to the blocks, prior to them. Once the details of the transactions or events are fed into the Blockchain, it is impossible to tamper the details are shared with the members of the network.Users of the Blockchain network is completely aware of the transactions taking place. We will draw an analogy to justify the concept. We consider it to be a book based data structure where each page of the book refer to its previous page by a page. Here, book refers to the Blockchain, page refers to the book and an entry in any page refers to the blockchain transaction. It is easy to detect whether a page or a block has been tampered or not. Pages can be arranged in any manner so pages aren't important in a distributed ledger. Now, In Blockchain, each block is built on top of the previous block and it uses the latter's nonce and signature as a key for going into the next block. Miners of the network does the job of building a block and adding it to the chain. It is easy for the miners to guess a random string or nonce in order to tamper the block just by knowing the signature in a Public Blockchain. It is not easy to add blocks in the Blockchain and there is a reward of 12.5 bitcoins for that. In a Private Blockchain, the miners are given a contract and as a result, they can add on blocks to the chain. So, it can also be defined as a consensus oriented secured distributed public/private ledger which stored data over a peer to peer network.

### A. Advantages of Blockchain

The Blockchain protocols has several features. We have listed out few of them.

*1) Immutable:* It means that it is really difficult to tamper or alter a block.

*2) Irreversible:* This feature prevents double spending.

*3) Distributed system:* It means that a copy of the ledger is present with all its members.

*4) No Centralized Authority:* It doesn't depend on a central server to dominate and hence, a peer to peer system.

*5) Resilient:* This feature shows that it is not prone to any sort of major attacks.

## II. History and Evolution of Blockchain

The history of the Blockchain can be showed by considering the example of one of its counterparts. We are talking about the Bitcoin Blockchain. Satoshi Nakamoto invented Bitcoin and since then, it is the most popular and used Cryptocurrency. He developed the concept of Bitcoin as a currency, as resilient and trustworthy. But it had few anomalies.

*1) One kind of asset:* It was primarily built as a currency. It isn't applicable for other modes or assets.

*2) Time taking:* Satoshi Nakamoto's aim was to achieve the maximum possible consensus in order to pass a transaction. It doesn't give attention to the time taken to validate the same.Hence, the process is getting slow. The developers of Blockchain are working on different kind of technologies. We have cited few examples here.

### A. Colored Coins

The protocols which allows the digital assets other than Bitcoin to be transferred in the Bitcoin Blockchain using the Bitcoins as "tokens". Bitcoins can be used as a transfer element for the Bitcoin transaction where it can be regarded a meta data for representation of shares, property and other instances.

978-1-5386-2529-3/17 $31.00 © 2017 IEEE
DOI 10.1109/CINE.2017.33

### B. Alternative Blokchains

This is also termed as “Sidechains”. In the Alternative Blockchain feature, we can shift the bitcoins of the Bitcoin Blockchain to a new Blockchain. We can transfer using Bitcoins having said that, we have to adapt to the new rules as well. We might have lesser time for Validation, more easily programmable and most importantly, a separate consensus mechanism. It ensures user scalability.

### C. Ethereum Blockchain

It is the newly developed Blockchain and it operates using digital contracts known as “Smart Contracts”. The protocol for Ethereum is different from Bitcoin Blockchain. Smart Contracts are basically small computer programs that accounts for a deal between a client and an end user. Blockchain has a wide range of financial and non financial applications. It has been used largely by Multinational companies like IBM, Amazon etc. and will be used further in the coming years. Many banks have collaborated in order to implement Blockchain technologies in their system.

### D. Hyperledger Blockchain

Hyperledger is an umbrella project of Open Source Blockchain and related tools [1], started in 2015 by Linux Foundation [2] to support the collaborative development of Blockchain based Distributed ledgers [3]. It has four platforms like Iroha, Fabric, Sawtooth and Burrow. IBM owns the Hyperledger Fabric and Intel owns the Sawtooth project of Hyperledger.

## III. Working of Blockchains

We will illustrate the working of Bitcoin transactions primarily in order to elucidate the working of Blockchain mechanism. Bitcoin uses some sort of proof under Cryptographic primitives rather than entirely trusting on the third party. Hence, the concept of “digital signature was introduced”. The sender sends using his private key and the receiver receives using his public key and the person needs to know the private key and the digital signature, if he wishes to spend the money. The peer nodes present in the Bitcoin network is completely aware of the transactions being taking place. The transactions must be “endorsed” and “validated” in order to be reflected in a public ledger. Firstly, the validator must know that the sender has the right to spend it. Secondly, the validators must be aware that the sender has enough money in his account to make a “legit” transaction. The transactions in a Bitcoin network are not ordered. So, there is a chance of double spending and it could be removed by the introduction of Blockchain Technology. In Blockchain, the transactions are ordered in form of blocks in a linear chain, which are linked to each other. Every block contains the hash of the block prior to it. We have introduced a concept called “Proof of Work”. In this, the task of the node is to find the random string or nonce. This random string has to be hashed with the transactions and the hashes of the previous blocks and then, it produces a hash with certain number of leading zeroes.

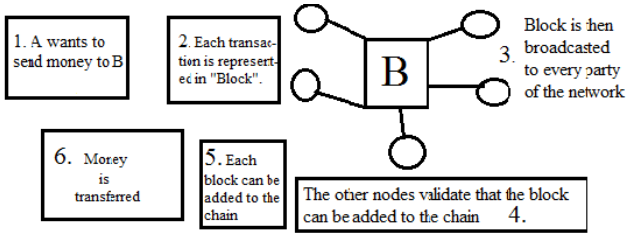


Fig. 1. Workflow of the Blockchain Mechanism

## IV. Blockchain Research in the Modern World

Blockchain is the newest topic in the domain of Computer Science and Security, as far as research is concerned. Many pioneer work has been done to improve the effiecieny of Blockchain [4]. According to the research done by Zhao et al. (2016), we have found that there has been an large scale increase in the number of research papers on Blockchains. Blockchains has been considered as vulnerable to many of the attacks. Most of them have been unique and it could resist till now. chain.com is a startup backed by NASDAQ, which built a platform for equity markets on top of Blockchain. This is one of remarkable examples to show its excellence.

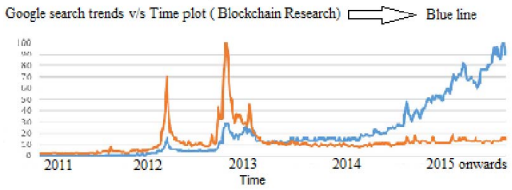


Fig. 2. Increase in the research of Blockchains

## V. Conclusion

Blockchain is still prevailing at its early stage of its research and development. Pioneer researchers in the domain of security and Cryptography have come forward to take it further to newer highs. It is going to a great help for the Financial and Non Financial sectors. It will pay heed to the issues of reliability, security and shared knowledge at the same time. It has been one of the most attractive technologies since its inception. This paper could conclude that there are numerous opportunities of research in this area and there is an urgent need to explore and seek for betterment just by minimizing the flaws and by enhancing its efficiency.

## References

[1] Ehsani and Farzam, “Blockchain in Finance: From Buzzword to Watchword,” CoinDesk (News), 22 December, 2016.
[2] Linux Foundation unites the Industry leaders to advance Blockchain Technology, 2016.
[3] Open Source Blockchain Effort for the Enterprise Elects Leadership Positions and Gains New Investments, 2016.
[4] Zhao et al., “Financial Innovation,” 2-28, 2016.