Block Chain Technologies In Financial Sectors And Industries

Dinesh Kumar K, Komathy K, Manoj Kumar D S

Abstract :The Blockchain technology is growing exponentially into our daily lives. The Blockchain integration with IoT, big data, artificial intelligence and cloud computing have lot of benefits and challenges. The various industries and financial institutions started to implement the exploration of blockchain. The blockchain revolution will not take much time to spread all over the world. In order to identify the scope of blockchain in financial and industrial sector, this paper reviews the integration of IoT and smart contract would give lot of advantage in financial sectors and extreme automation in industry.

Index Terms: Bitcoin, Blockchain, Consensus Mechanism, Distributed ledger, Internet of Things, Merkle root, Nonce, Smart contract.

1 INTRODUCTION

Blockchain technology is a decentralized ledger system where transactions can be recorded and verified electronically over a network of computers without a central ledger that offers a high level of transparency, immutability, security, distributed, consensus and faster settlement. Blockchain essentially removes the need for intermediaries who were previously required to act as trusted third parties to verify record and coordinate transactions by facilitating the move from a centralized to a decentralized and distributed system. In the year 2008, Satoshi Nakamoto published a paper introduced crypto currencies formally called Bitoin, a first blockchain application [1]. Bitcoin is the crypto currency that provides a trust in a distributed and decentralized system. Bitcoin is a distributed decentralized time stamped peer-validated shared ledger that logs legal transactions. The shared ledger is publically verifiable by all network peer nodes [2]. Transactions are broadcasted to the blockchain network, and their transaction validities are audited by peer participants. The transactions are collected and recorded into blocks that are sealed cryptographically. The group of special nodes are called miner node (Special node) validate the transactions based on the existing block chain, and propagate the transaction to the miners, the miners include the transaction to the next block to be mined. The transaction life cycle of miners follows a. The miners collects all the transactions for the stipulated time duration b. Miners creates a new block and try to append it with the current blockchain, through a cryptographic hash computation c. Once the mining is completed and the hash is obtained, the block is appended in the existing blockchain and hence updated blockchain is disseminated in the distributed network [1]. There are two models of blockchain network – Permission less (an open environment) and Permission (a close environment)

2 BLOCKCHAIN PERMISSION LESS MODEL – FINANCIAL SECTOR

The Permission-less model works in an environment and over a large number of participants. The users do not need to know the identity of the peers, and hence the users do not need to reveal their identity to others. This model is very suitable for good for financial applications like banking using cryptocurrency [2]. The privacy and security of permission less system is tamper-proof – it is extremely hard to make a change in the blockchain as the chain grows. For Bitcoin, the transaction are pseudo-anonymous are sent to public key address, cryptographically generated addresses, computed by the wallet applications. The peers address in bitcoin is synonymous to an account in a bank. The wallet listens for transactions addressed to an account which encrypts the transactions by the public key of the target address the target node can decrypt the transaction and accept it. However, the actual transaction amount is open to all for validation. The applications of permission less model are many such as cryptocurrency, Ethereum, Bitcoin, zcash all together permissionless blockchain allow people to act anonymously that they do not know each other identity.

- *Dinesh Kumar K, Assistant Professor, Department of Information Technology, AMET Deemed to be University, Chennai, Tamil Nadu, India,dineshkumar01@gmail.com*
- *Komathy K, Professor, Department of Information Technology, AMET Deemed to be University, Chennai, Tamil Nadu, gomes1960@yahoo.com*
- *Manoj Kumar D S, Assistant Professor, B.S Abdur Rahman Crescent Institute of Science and Technology, Chennai,Tamil Nadu, India, manojkumards03@gmail.com*

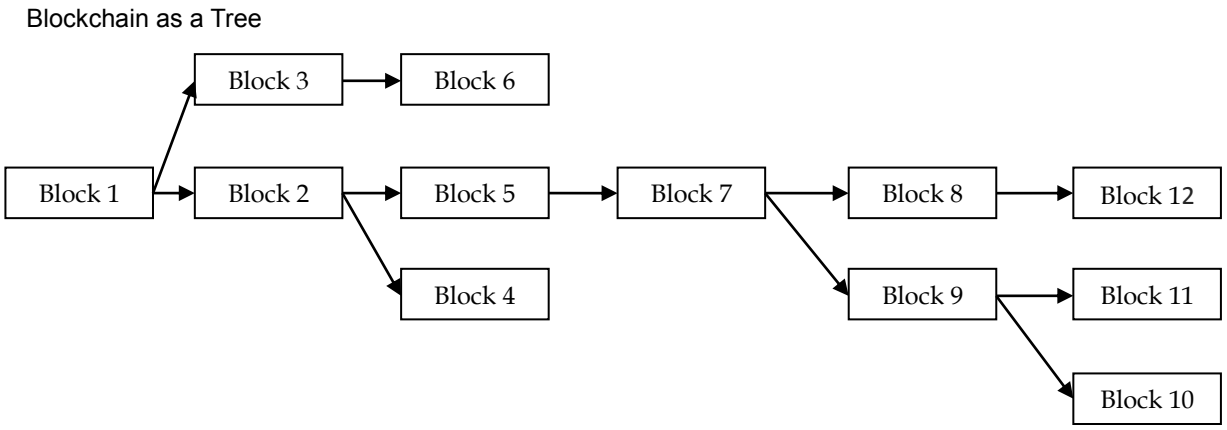

Figure 1. *The Longest chain in the blockchain is the accepted chain*

2.1 BLOCKCHAIN OPERATION

The block in a blockchain consists of block header and set of transactions. The block header contains set of block content such as version number, time stamp, previous block hash, 32 bit nonce value and merkle root hash. The hash function takes the block header and set of transaction as an input then generates fixed length of block hash which is also stored back in current block in block chain.

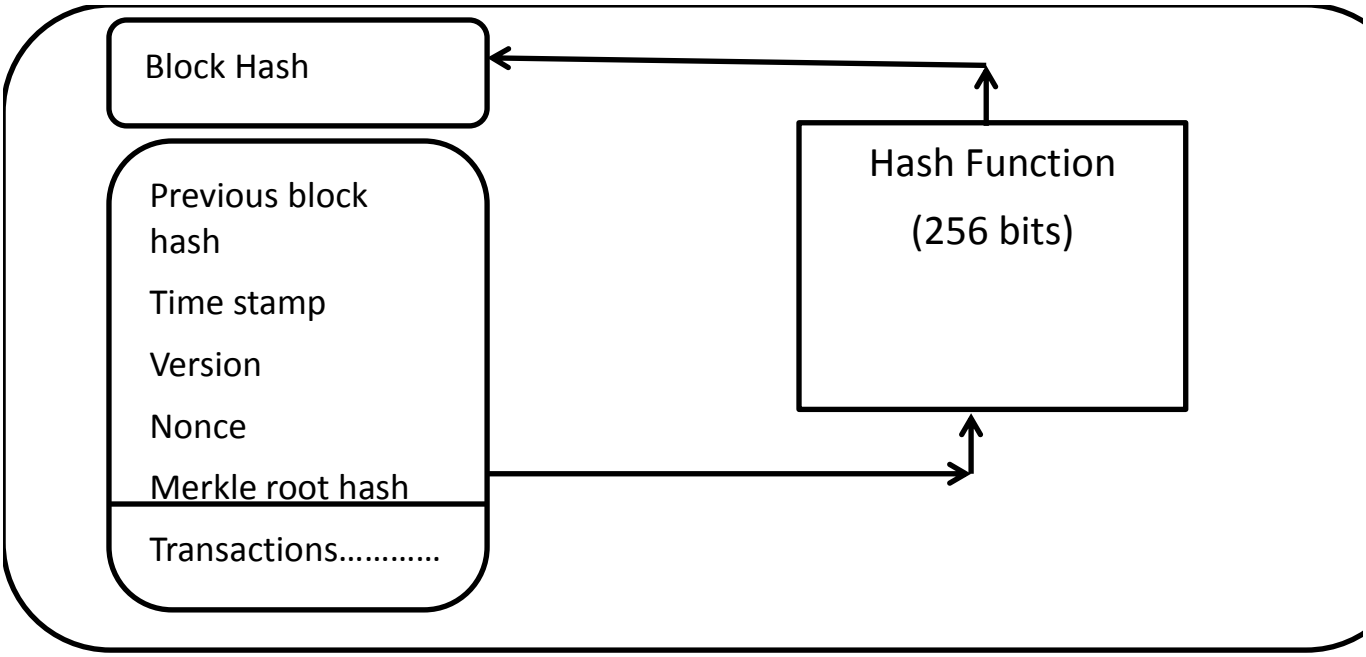

Figure 2.*The Blockchain operation generates a hash 256-bit number from the block content, the previous block hash, and other elements.*

The new blocks is mined by miner node and always find the longest chain as shown in the figure 1. The new block always includes it in the longest chain of blockchain. The blockchain transactions are replicated to the Bitcoin network, and their validity is verified independently by network participants. The valid transactions are verified by the miners locally, transactions are stored locally that becomes a cryptographically secure block. Bitcoin blockchain mining uses the hash algorithm protocol to generate 256-bit length as shown in the figure.3

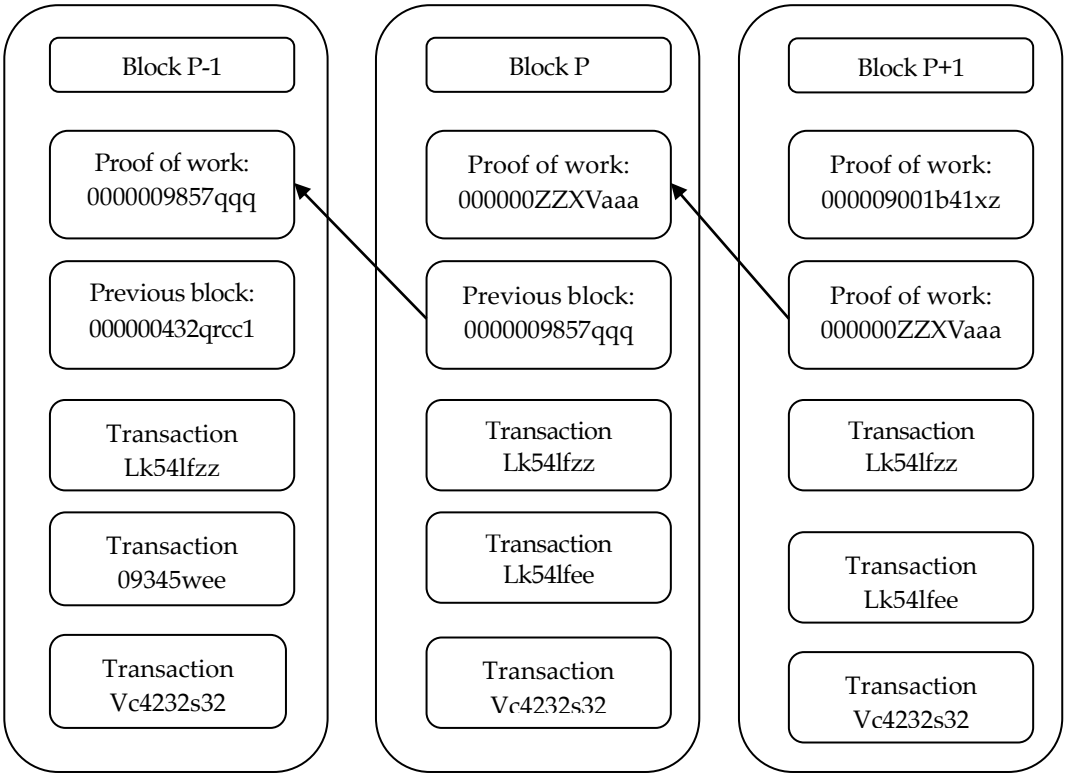

Figure 3. *The Block in a Blockchain - Securing transaction cryptographically*

An append-only shared ledger of digitally signed and encrypted transactions replicated across a network of peer nodes. A block may contain more than 500 transactions on average, the average size of a block is around 1 MB it may grow up to 8 MB or sometime higher as of 2009 [1]. Large block may help in processing large number of transaction in one go. Crytocurrency systems lacks in scalability as it takes long time for process transaction in terms of speed and bandwidth when compare to visa and other payment gateways [10].

2.2 PROOF OF WORK AND MINING

Hashing the transaction details is used for PoW, a consensus mechanism that interlink with computation power, making the consensus process expensive. The PoW is the initial basis for mining procedure which involves competition between users for verification of transactions. A valid user's has a change of winning is directly proportional to the computing power, According to Bitcoin mechanism "one CPU, one vote." The participants are compensated for contributing to block confirmation and construction. Each mined block contains a coinbase transaction, which is allocated to the winning participant. This mechanism is used to generate new Bitcoins in the blockchain. The winning participants who perform the PoW only for gaining profit. Recent days, mining is implemented in large mining unit located in region with electricity cost are affordable. The Blockchain miners in the mining process also share profits in proportion to hashing computation [1]. Bitcoin mining also required exclusive hardware power to compute and generate new Bitcoin. Similar to Bitcoin there are various cryptocurrency application available as shown in the table 3.

S.No	Currency	Status	Release	Features
1.	Waves	Active	2016	An open Blockchain platform to develop applications for high volume transactions
2.	Ripple	Active	2013	Designed for P2P debit transfer
3.	Omni	Active	2013	Both a digital coin and a communication platform built on top of bitcoin blokchain
4.	Gridcoin	Active	2013	The first cryptocurrency linked to citizen science through Berkley Open Infrastructure for Networking Computing
5.	Emercoin	Active	2013	Trusted storage for any small data
6.	Bytecoin	Active	2012	Focused on user privacy through impassive and anonymous transactions
7.	Peercoin	Active	2012	Uses PoW and PoS functions
8.	Litecoin	Active	2011	Uses Scrypt as a hashing algorithm
9.	Bitcoin	Active	2009	The first decentralized ledger currency

Table 1. The Crypto currency application that uses Blockchain.

2.3 ETHEREUM

The Ethereum white paper [8], the need of ethereum is an alternative protocol for building decentralized applications will be useful for a large class of decentralized applications, ethereum is not like bitcoin cryptocurrency but distributed public ledger which comprises of untrusted participants. The main design of ethereum principles are 1. Protocol should be as simple as possible, even at the cost of storage or time inefficiency. 2. Ethereum provides scripting language, which a programmer can use to develop any smart contract. 3. The parts of the protocol could be designed to usable in other protocol as well. 4. The Ethereum virtual machine (EVM), will substantially improve scalability [8]. The Ethereum applications are three types such as financial application, semi financial applications and decentralized application used in industries.

3. BLOCKCHAIN PERMISSION MODEL – INDUSTRIAL SECTOR

The Blockchain can be applied beyond cryptocurrency. The underlying notions of consensus, security and distributed replicated ledgers can be applied to even closed or permissioned network settings. The enterprise blockchain comprises of few hundred known participants unlike Bitcoin blockchain has 13 million user as of now. In permissioned model every user can read transaction data. But only predefined user can validate transaction. The permission model is highly suitable for industrial sector and other sectors such as supply chain management like luxury goods, pharmaceuticals, cosmetics and electronics which does provenance tracking. The consensus algorithm used in private network, where the users are limited and white listed therefore costly consensus protocols such as PoW are not needed in permissioned model. The consensus protocols are used in private block are Practical byzantine fault tolerance algorithm and tendermint [3]. Hyperledger fabrics uses PBFT as it consensus algorithm that could handle Byzantine attack and can handle up to 1/3 replicas. The process of PBFT could be divided into three phase: pre-prepared, prepared and commit [4].

3.1 HYPER LEDGER

The Hyperledger is an open source distributed ledger blockchain technology and code base. It is an umbrella project of blockchain started in December 2015 by Linux foundation. Hyperledger project where multiple teams are collaborating to develop distributed ledger technology(DLT). The DLT framework is led by different organization such as Hyperledger Burrow is permissionable smart contract machine(EVM) led by monax, Hyper ledger Fabric is Permissioned with channel support led by IBM, Hyperledger Grid is Web Assembly-based project for building supply chain solutions led by Intel, Hyperledger Iroha is mobile application focus led by Soramitsu, Hyperledger Sawtooth is Permissioned & permissionless support EVM transaction family led by Intel [4], Simliarly some of the Hyperledger tools are shown in the table 2.

S.no	Hyperledger tools	Types
1.	Hyperledger Aries	Infrastructure for peer-to-peer interactions
2.	Hyperledger Caliper	Blockchain framework benchmark platform
3.	Hyperledger Cello	As-a-service deployment
4.	Hyperledger Composer	Model and build blockchain networks
5.	Hyperledger Explorer	View and explore data on the blockchain
6.	Hyperledger Quilt	Ledger interoperability
7.	Hyperledger Transact	Advanced transaction execution and state management
8.	Hyperledger URSA	Shared Crytographic Library

Table 2. Hyperledger Tools

The Hyperledger fabric was initiated by Digital Asset and IBM. Hyperledger fabric was designed to be a modular, scalable and offering solution for industries. Hyperledger Fabric implements specific types of permissioned model blockchain network on which members can track, exchange and interact with digital assets using transactions. The HLC separates the transaction processing workflow into three stages such as smart contracts, transaction ordering and transaction validation. The three distinct roles of participants are endorser, committer and consenter [9].

4. BLOCKCHAIN AND SMART CONTRACT

The term smart contract was coined by Szabo in the year 1996. He defined the smart contract as “A computer based transaction protocol that automates and executes the conditions, terms of a contract”. The main key features of a smart contract are it can self execute once the conditions are met [5]. Blockchain has turned out to be the emerging technology to support smart contracts or chaincodes. In addition to that, smart contracts have contributed to the development of blockchain, moreover this coupling has led to a second generation of blockchains, commonly known as Blockchain version 2.0. The combination of automatically

executed contracts in a private environment without centralized control promises to change the way current business is done. Essentially, the smart contract code or chain code is put away on the blockchain, and each contract is recognized by a special address and for clients to function with it, they fair send a transaction to this address. The right execution of the contract is implemented by the blockchain consensus protocol. Contracts present a set of points of interest such as taken a toll lessening, speed, exactness, effectiveness, and straightforwardness that have cultivated the appearance of numerous unused applications in a wide assortment of ranges. In spite of the fact that Bitcoin offers a essential scripting dialect, it has turned out to be deficient, which has driven to the development of modern blockchain stages with coordinates smart contract usefulness. The Blockchain also involves in cargo shipping to connect different logistics activity such as finance, supply chain management, IoT, and insurance using a five layer framework. The Architecture was designed to help users of smart-connected merchant ships

view transactions from anywhere and reduce real-time delays [11].

5. BLOCKCHAIN AND IOT

The Blockchain and the Internet of things (IoT) are rising innovations that will have a extraordinary affect in the next 4 years for industries. These technology will improve efficiency, give new trade openings and make strides straightforwardness and perceivability. Blockchain and IoT permits empower information captured from the Internet of things using shared record that's accessible to members within the industry network.Some of the applications of blockchain and IoT such as supply chain management, Autonomous vehicle solutions, manufacturing plant asset management, energy distribution etc [6]. In energy distribution the role of IoT and blockchain is most effective and productive. The Blockchain with IoT allows for a peer-peer business where computers can buy and sell energy automatically using smart contracts [7]. Blockchain and IoT could give solution for supply chain management in merchant shipping where very high cost involved for transportation. The Blockchain technology that drives supply chain management in profitable way by integrating IoT would capture key shipment data emitted from IoT sensor attached to consignments as the shipment moves from source to destination. The IoT system would call a transaction for the blockchain that contains the shipment container location and timestamp. The Blockchain could receive the bill of lading and proof of delivery for container shipments. This could minimize the delay and transportation time for materials flowing could be more accurately predicated [7].

6. CONCLUSION

The Blockchain technology in the financial and industrial sector has enormous potential. Using smart contract in Blockchain application could avoid the role of intermediaries and could increase the productivity as well. Blockchain is truely decentralized distributed peer-to-peer systems Financial institution could use Blockchain technology like Etherum is also a permission less public ledger based distributed computing platform which also featuring smart contract. The integration of the IoT and blockchain will increase the application of blockchain in industrial sector and development of government infrastructure would speed up the interaction between citizen, governments and industry.

REFERENCES

[1] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008; bitcoin.org/bitcoin.pdf.

[2] A.M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Crypocurrencies,O'Reilly Media, 2014.

[3] C. Miguel and L. Barbara, "Practical byzantine fault tolerance" in proceedings of the third symposium on operating systems design and implementation, vol. 99, USA, 1999, pp. 173-186.

[4] Hyperledger project, [online] Available: https://www.hyperledger.org/[Accessed on 5.7.2019]

[5] Szabo.N. The idea of smart contracts http://szabo.best.vwh.net/smart_contracts_idea.html (1997), accessed: 017-01-25

[6] Dennis Miller, IBM, Blockchain and the Internet of Things in the Industrail Sector, IT professional, 2018.

[7] TransActive Grid, Available:http://transactivegrid.net/ [Accessed on 5.07.2019]

[8] Viktor Trón, Felix Lange. Ethereum Specification [Internet]. 2015. https://github.com/ethereum/go-ethereum/wiki/Ethereum-specification

[9] IBM Blockchain based on Hyperledger Fabric from the Linux Foundation. Available from https://www.ibm.com/blockchain/hyperledger.html

[10] Visa Inc. Reports, available:https://www.usa.visa.com [Accessed on 5.07.2019]

[11] Karuppanan Komathy. (2018). Verifiable and Authentic Distributed Blockchain Shipping Framework for Smart Connected Ships. Journal of Computational and Theoretical Nanoscience. 15. 3275-3281. 10.1166/jctn.2018.7610.