iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VI **Month of publication:** June 2020

DOI: http://doi.org/10.22214/ijraset.2020.6364

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

Overview of Blockchain

Akshay S. Gaikwad
MET Institute of computer science

Abstract: Blockchain is a distributed, decentralized, public ledger for securely exchanging digital currency and transaction information. Blockchain was invented in 2008 by satoshi Nakamoto as public ledger for cryptocurrency bitcoin. Blockchain allows the participants to verify the transactions independently. This paper explains the concept of blockchain, characteristics, how blockchain works, and its security mechanisms. It attempts to highlights role of Blockchain in various fields.
Key aspects: Improved accuracy by removing human involvement in verification. Cost reductions by eliminating third-party verification Decentralization makes it harder to tamper with. Transactions are secure, private and efficient. Transparent technology.

I. INTRODUCTION

Cryptocurrency is digital or virtual currency designed to work as a medium of exchange that uses cryptography to secure and conduct financial transactions. Cryptocurrencies use decentralized control to conduct the transfer of assets. For achieving functions like decentralization, transparency cryptocurrencies use Blockchain. Bitcoin is one of the most popular cryptocurrency examples of blockchain. Blockchain consist of several nodes. Node is a computer that is connected to the blockchain network. When a computer system connects to the Blockchain network, a copy of the Blockchain data gets downloaded into the system and the node comes in sync with the latest block of data on Blockchain.

There are three types of blockchain.

A. Public Blockchain

A public blockchain is known as a non-restrictive, permission-less distributed ledger system. Anyone who has access to the internet can sign in on a blockchain platform to become an authorized node and be a part of the blockchain network. A node that is a part of the public blockchain is authorized to access current and past records, verify transactions or do proof-of-work for an incoming block. These blockchains usually use Proof of Work or Proof of Stake for consensus mechanism. Another important advantage of a public blockchain is that no one individual or company is able to control the information which is contained on the blockchain. Bitcoin and Litecoin blockchains are the most common public blockchains.

B. Private Blockchain

A private blockchain is more restrictive or permission blockchain operative only in a closed network. Private blockchains are usually used within an organization's or enterprises where only selected members are participants of a blockchain network. The level of security, authorizations, permissions, accessibility is in the hands of the controlling organization. Private blockchain networks are deployed for voting, supply chain management, digital identity, asset ownership, etc. The transaction speed of a private blockchain is faster than public blockchain. If requires a company running a private blockchain can easily change the rules of a blockchain, revert transactions, modify balances, etc. The cost of transactions in private blockchains is generally not very expensive. Choosing a private blockchain can help banks and other organizations to protect their fundamental product from destruction.

C. Hybrid Blockchain

A hybrid blockchain is an integration of the private and public blockchain. Only a selected section of data from the blockchain can be allowed to go public, keeping the rest as confidential in the private network. A transaction in a private network of a hybrid blockchain is usually verified within that blockchain network, but sers can also release it in the public blockchain to get verified. Hybrid blockchain provides a blockchain solution that is most important to highly regulated enterprises as it enables them to have the flexibility and control over what data is kept private and which data should be shared on a public ledger. An example of a hybrid blockchain is Dragonchain.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

II. HOW IT WORKS

Blockchain is the chain of blocks, in which block is consists of digital information and the chain is the public database. Blocks stores the transaction information like the date, time, dollar amount, and who is participating in transactions. Blocks also store the information that distinguishes them from other blocks. Each block stores a unique code called a "hash" that makes block unique, apart from every other block. Hashes are cryptographic codes created by an algorithm that maps data of arbitrary size to a bit string of a fixed size (hashed value). Every block in the chain also stores the hash value of its previous block. The first block in the chain is known as genesis. As genesis does not have any previous block its previous hash value is 0.For adding block in the chain several things should be followed:

1) The transaction must occur .
2) Transaction information gets added to the block.
3) Once that information receives by the block then it again sends to the nodes in the network.
4) Once this request received by the nodes it then analyzed and approved by all the nodes.
5) After this the node which will add the block to the blockchain is selected. This selection is based on certain mechanism.
6) After approval of request that new block can now officially added to the chain.

It makes use of digital signature to send the transactions to the network.

A. Security in Blockchain

One of the core aspects of blockchain technology is Security. Blockchains depend heavily on cryptography to achieve their data security.

Blockchain makes use of cryptographic hash functions to calculate the hash value of a particular block. This value calculation is based on data inside the block and it is unique for each block. Transactions in blockchain are variable in lengths and run through a given hashing algorithm, the output generated from these algorithms always have a fixed length. This output does not depends on the length of the input transaction.

The output is known as a hash. Every block in the chain also stores the hash value of its previous block except genesis. If anyone tries to change the data inside the block the generated hash value is different from the previous one. The next block in the chain will still contain the previous hash, and the person would need to update that block in order to cover their tracks. In order to change a single block, a person would need to change every single block after it on the blockchain. Recalculation of all those hashes would take an enormous amount of computing power. In other words, once a block is added to the blockchain it becomes very difficult to edit the data and impossible to delete.

B. Consensus

In blockchain network there are several nodes. Any node cannot add the block to the chain directly, it has to follow consensus. Consensus is the agreement process which decides who will add the block to the blockchain. To achieve this certain test needs to follow.

This is why when there could be contradictory results in a distributed system; use of consensus algorithms helps for better output. The tests, called "consensus models," require users to "prove" themselves before they can participate in adding a block to the blockchain network. Most common test employed by Blockchain are called proof of work and proof of stake, Delegated proof of stake etc.

C. Proof of Work

In the proof of work consensus mechanism, miners compete against each other to complete transaction on the blockchain network and get rewarded. The node must prove that they have done work by solving a complex computational math problem. If a node solves these problems, they become eligible to add a block to the blockchain. To solve complex math problems, nodes have to do lot of calculations which cost them significant amounts of power and energy. It is possible that two competing nodes generate next block simultaneously. In such case the chain which becomes longer thereafter is consider as authentic one. Consider two nodes created two blocks simultaneously A1 and B1.Miners keep mining their blocks until the longer branch is found. First miner creates chain A1A2 and second one is still working on generating B2 then second minor has to shift to A1A2.This test is implemented in Bitcoins Blockchain.

D. Proof of Stake

Proof of stake is another type of consensus algorithm by which a cryptocurrency blockchain network aims to achieve distributed consensus. Proof of stake is designed to overcome the proof of work's disadvantage of consuming significant amounts of power and energy. In Proof of Stake (PoS) The blockchain keeps track of a set of validators, and anyone who holds the blockchain's base cryptocurrency can become a validator by sending a transaction that locks their cryptocurrency into a deposit. Then, an algorithm chooses from the pool of candidates the node which will validate the new block. The selection algorithm is Randomized block selection or Coin age based selection. In the randomized block selection method of selection, a formula which looks for the validator with the combination of the lowest hash value and the size of their stake, is used to select the next validator who is eligible to add the new block to the blockchain. The coin age based system selects the validator based on the coin age of the stake which is calculated by multiplying the number of days the cryptocurrency coins have been held as stake by the number of coins being staked. The validator verifies all the transactions and publishes the block. His stake still remains locked and the reward is also not granted yet. Other nodes on the network verifies the block, if block is verified then the validator gets the stake back and the reward too.

E. Delegated Proof of Stake

Even though it has the name Proof of Stake associated with it, it is different from proof of stake algorithm.

In Delegated proof of stake, users of the network vote to select a group of users or delegates who are responsible for creating new blocks. Delegates are the only entities who can add new blocks to the blockchain. For every round a block from selected delegates chosen as leader. The leader is responsible for creating block and validating transactions. The block proposed by the leader is validated from other delegates. If validated transactions does not have any issue then leader receives the reward for creating new block. If transaction is faulty, it de-listed the leader or delegate from the list of delegates and other user is added to the list based on votes of other users. Delegated proof of stake is energy efficient and environmentally friendly because it does not require high computer power and generally approachable for users with poor equipment.

F. Practical Byzantine fault Tolerance

Practical Byzantine Fault Tolerance is a consensus algorithm introduced by Barbara Liskov and Miguel Castro. In Practical Byzantine Fault Tolerance, nodes are arranged in a sequential manner where one node is referred to as primary node or leader node and other nodes are referred to as a secondary node or backup nodes.In case of primary node failure, any secondary node can become primary node. A practical Byzantine Fault Tolerant system is the system that works on the condition that the maximum number of malicious nodes must not be greater than or equal to one-third of all the nodes in the network. In practical Byzantine Fault Tolerant system client sends a request to the primary node. Then in pre-prepare phase primary node broadcast the request to all the secondary nodes. In prepare phase secondary nodes process the request and sends it to client. The request is served successfully when the client receives ‘n+1’ replies from different nodes in the network with the same result, where n is the maximum number of faulty nodes allowed.

III. CHALLENGES FOR BLOCKCHAIN

A. Scalability

Over the past few years, cryptocurrencies (especially Bitcoin and Ethereum) have attracted a lot of interest.

The number of transactions in cryptocurrencies increases drastically. Due to this blockchain become huge in size. Though Blockchain networks are capable of processing thousands of transactions per second without any failure. Original restriction of block size and the time interval used to generate a new block creates a huge impact on processing millions of transactions, Due to this, the Bitcoin blockchain can only process around 7 transactions per second, which cannot fulfil the requirement of processing millions of transactions in a real-time process.

B. Energy Consumption

Bitcoin is the first and one of the most popular applications of the blockchain. Bitcoin’s blockchain uses proof-of-work (PoW) at first consensus mechanism for validating transactions and eliminating the need for centralization .Proof-of-work requires solving complicated mathematical puzzles for adding block in the blockchain, which requires highly specialized computer hardware to run the complicated algorithm. These specialized machines consume large amounts of power to run that increase costs, which is the serious issue. For overcoming this issue blockchain can use other consensus mechanisms like proof of stake, delegated proof of stake , delegated Byzantine Fault Tolerance etc. because they required less energy.

C. Interoperability

Interoperability in blockchain is the ability to share information across different block chain networks, without the need for intermediaries. The first blockchain was launched in 2009. Since then, many other blockchains have been created with their own rules and ecosystems. Different blockchain networks differ in parameters such as consensus models, transaction schemes, and smart contract functionality. To make mass adoption possible and let the industry evolve further interoperability maters .Interoperability can be achieved through methods like cross-chains, swaps which acts as a bridge between two different blockchains.

D. Selfish Mining

In proof of work consensus mechanism mining relies on miners who solve cryptographically complex puzzles to generate coins. Selfish mining is a strategy for mining blocks in which groups of miners withholds the block to increase their revenue. In this process the miner keeps with him the mined block with no broadcasting on network and will create a private branch which will be broadcasted after meeting certain requirements. Due to this, legitimate miners will waste time and resources on finding the block and private chain will be mined by selfish miners.

IV. CHARACTERISTICS OF BLOCKCHAIN

A. Immutability

The block created in blockchain can never be changed or altered. The blockchain calculates hash value based on data inside the block. This hash value is unique for every block. If one tries to change the data the hashed value generated is different from previous one. In order to change a single block, then, a person would need to change every single block after it on the blockchain.

B. Anonymity

Anonymity is one of the important aspect of security in blockchain. The actual identity of the user who is doing transaction is not known. User will be linked to a public address, but no one will get to know the actual name or address.

C. Decentralization

In decentralization blockchain allow transactions to be made directly from person to person without help of any third party. This improves financial efficiency and allow people to be less reliant on banks or other financial institution.

D. Transparency

One of the important benefits of blockchain technology is its transparency. The decentralization of the distributed ledger means that those transaction records are identically recorded in multiple locations. Having the same records spread across a large network for all to see is the base of blockchain transparency.

E. Persistence

Blockchain will not create or persist invalid transactions as determined by consensus. It is nearly impossible to delete or change transactions once they are included in the blockchain. Cryptographically, the blocks created are sealed in the chain and it is impossible to delete, edit or copy already created blocks and put them on the network. This leads to the creation of digital assets and ensures a high level of robustness and trust.

F. Auditability

Blockchain can serve as a distributed ledger that can record transactions between two parties in a verifiable way. Blockchains are resistant to make changes in any of stored data. For auditing any transaction instead of asking clients for bank statements or sending requests to third parties, auditors can easily verify the transactions on publically available blockchain ledgers.

V. APPLICATIONS OF BLOCKCHAIN

A. Blockchain Internet-of-Things (IoT)

Internet of Things refers to the millions of physical devices around the world that are now connected to the internet, all collecting and sharing data. Blockchain can be used in tracking billions of connected devices, enable transaction processing and coordination between devices. Blockchains decentralized approach would eliminate single points of failure, creating a more resilient and secure network for devices to run on. The cryptographic algorithms used by blockchain would make consumer data more secure.

B. Smart Contracts

A smart contracts is a computer code that can be built into the blockchain to facilitate, verify, or negotiate a contract agreement. Blockchain-based smart contracts are proposed contracts that can be partially or fully executed without human interaction. Normal process in which a third party receives and disburses money or property for the primary transacting parties, most generally, used with terms that conduct the rightful actions that follow. The disbursement is dependent on conditions agreed to by both the transacting parties. A smart contract avoids the involvement of third parties, it perform all the third party work in automated way without involvement of humans. Smart contract code in ethereum is written in solidity language. This eliminates resources like time and money that typically accompany using a third-party mediator.

C. Supply Chain

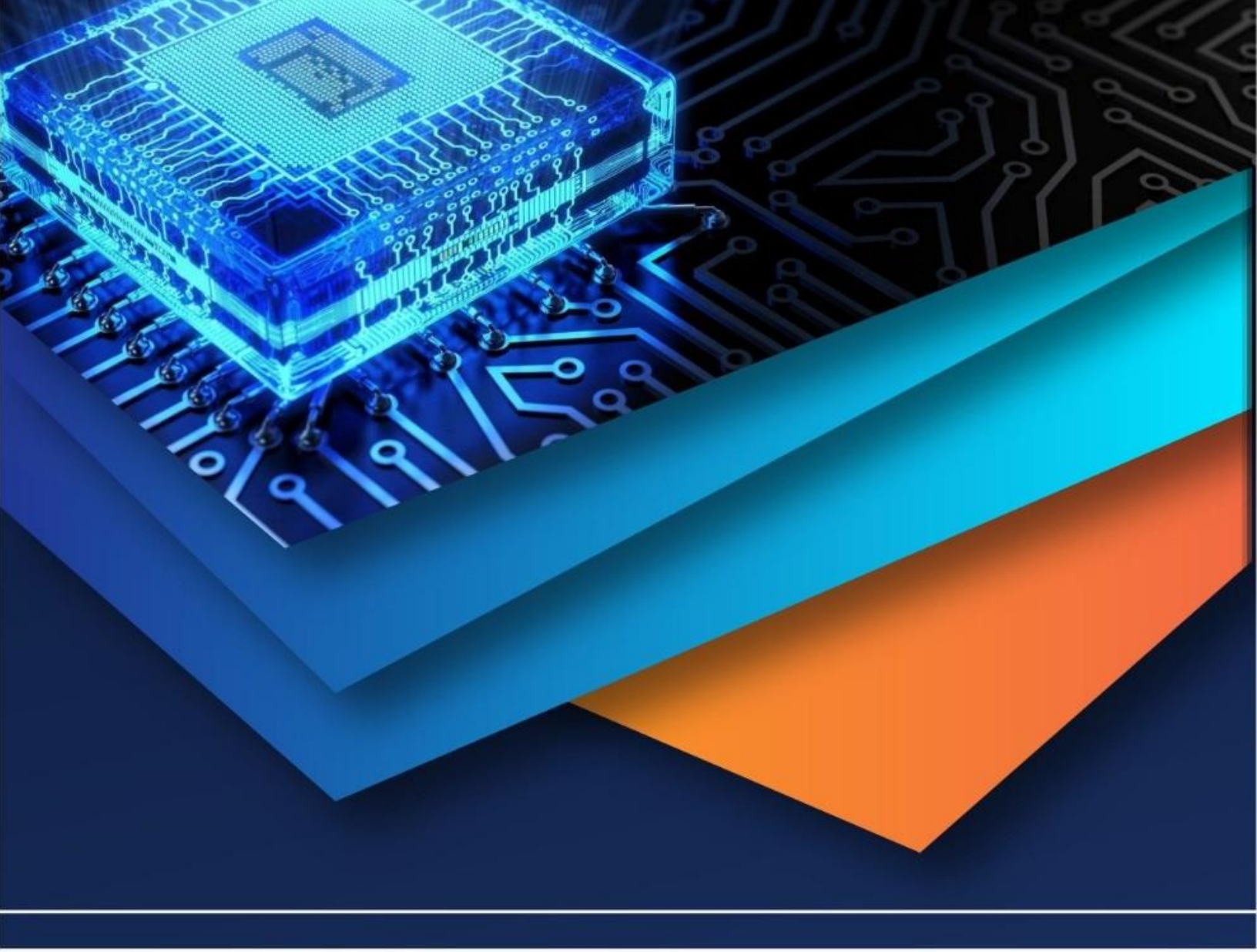
Companies can use blockchain to record product status at each stage of production. Blockchain makes it possible to trace each product to its source. Blockchain allows the company see where each piece of product comes from, each processing and storage step in the supply chain, and the products sell-by date. In case of a product recall, the company can also see which batches are affected and who bought them.

D. Finance

Using a distributed ledger feature of blockchain, banks can trade faster and cheaper and become more efficient. One of the main features of blockchain is that it removes the need of an intermediary and makes peer-to-peer transactions possible. Blockchain is used in the financial services, it could discard the fee-charging intermediaries such as those that transfer money between different banks. When the finance industry make use of smart contracts, it will improve contractual term performance as smart contracts execute without human interaction once certain pre-set conditions have been met.

REFERENCES

[1] An Overview of Blockchain Technology: Architecture, Consensus, and Future TrendsZibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3.
[2] Blockchain: Current Challenges and Future Prospects/Applications Spyros Makridakis * and Klitos Christodoulou Institute for the Future (IFF), University of Nicosia, Nicosia
[3] Blockchain: Current Challenges and Future Prospects/Applications Spyros Makridakis * and Klitos Christodoulou Institute for the Future (IFF), University of Nicosia, Nicosia
[4] Issues and Challenges with Blockchain: A Survey by Divyakant Meva Faculty of Computer Applications, Marwadi University, Rajkot, India



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY