WORKING OF BLOCKCHAIN TECHNOLOGY

[1]M. Satish Kumar, [2] Dr.V. Naga Lakshmi

Research scholar, Professor
Computer Science
GITAM UNIVERSITY, VISAKHAPATNAM, INDIA

Abstract: Blockchain is a chain of blocks where each block contains data of value without any central supervision. It is cryptographically secure and immutable. A Blockchain is a diary that is almost impossible to forge. Each block consists of Index, Timestamp, Data, Previous Hash, and Hash. Blockchain databases consist of several decentralized nodes. Each node participates in administration: all nodes verify new additions to the blockchain, and are capable of entering new data into the database. Blockchain-based applications are springing up, covering numerous Fields including financial services, reputation system and Internet of Things (IoT), and so on. However, there are still many challenges of blockchain technology such as scalability and security problems waiting to be overcome. This paper presents a comprehensive overview on blockchain technology. We provide an overview of blockchain architecture firstly and compare some typical consensus algorithms used in different blockchains.

Index Terms **-** Bitcoin, Hash, Genesis Block, SHA-256

I. INTRODUCTION

The first work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta, The first blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto in 2008, In August 2014, the bitcoin blockchain file size, containing records of all transactions that have occurred on the network, reached 20 GB (gigabytes).[12] In January 2015, the size had grown to almost 30 GB, and from January 2016 to January 2017, the bitcoin blockchain grew from 50 GB to 100 GB in size. Blockchain can play crucial role in Internet of Things (IoT) and development of smart systems since we can track the history of individual devices by tracking a ledger of data Exchanged. It can enable smart devices to act like an independent agent which can autonomously perform several transactions. Applications of blockchain is used in different areas .

II.WHAT IS BLOCK CHAIN?

This one spreadsheet is called a block .The whole family of blocks is the Blockchain. Every node has a copy of the Blockchain. Once a block reaches a certain number of approved transactions then a new block is formed. The Blockchain updates itself every ten minutes. It does so automatically. No master or central computer instructs the computers to do this. As soon as the spreadsheet or ledger or registry is updated, it can no longer be changed. Thus, it's impossible to forge it. You can only add new entries to it. The registry is updated on all computers on the network at the same time.

III. BLOCKCHAIN ARCHITECTURE

Working of blockchain:

A Blockchain is a type of diary or spreadsheet containing information about transactions. Each transaction generates a hash. A hash is a string of numbers and letters. Transactions are entered in the order in which they occurred. Order is very important. The hash depends not only on the transaction but the previous transaction's hash. Even a small change in a transaction creates a completely new hash. The nodes check to make sure a transaction has not been changed by inspecting the hash. If a transaction is approved by a majority of the nodes then it is written into a block. Each block refers to the previous block and together make the Blockchain. A Blockchain is effective as it is spread over many computers, each of which have a copy of the Blockchain. These computers are called nodes. The Blockchain updates itself every 10 minutes.

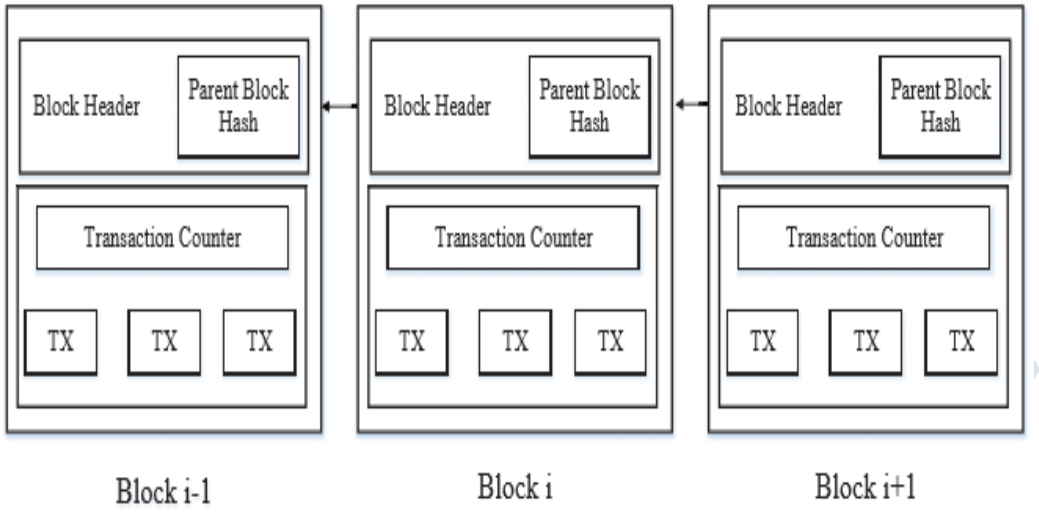

Fig. 1: An example of blockchain which consists of a continuous sequence of blocks

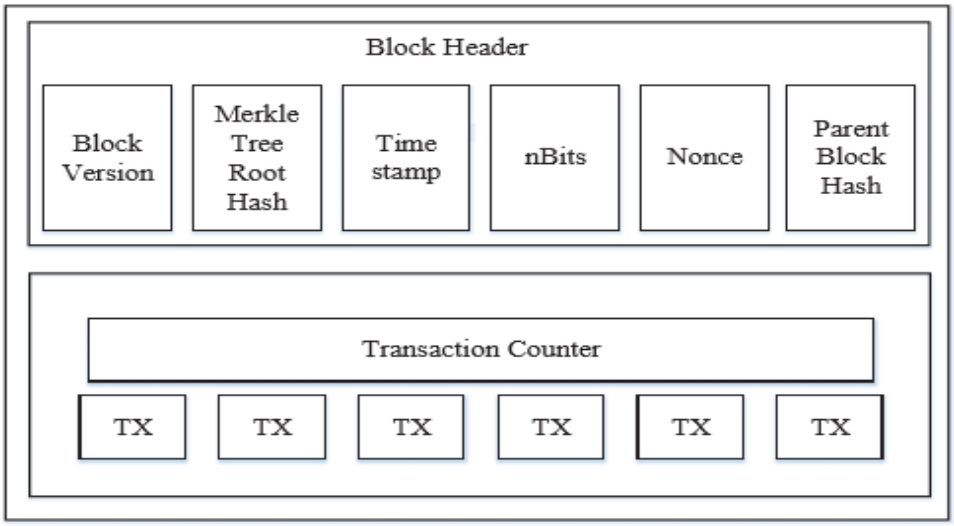

Fig. 2: Block structure

Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger [14]. Figure 1 illustrates an example of a blockchain. With a previous block hash contained in the block header, a block has only one parent block. It is worth noting that uncle blocks (children of the block's ancestors) hashes would also be stored in ethereum blockchain [15]. The first block of a blockchain is called genesis block which has no parent block. We then explain the internals of blockchain in details.

A. Block A block consists of the block header and the block body as shown in Figure 2. In particular, the block header includes: (i) Block version: indicates which set of block validation rules to follow.

(ii) Merkle tree root hash: the hash value of all the transactions in the block.

(iii) Timestamp: current time as seconds in universal time since January 1, 1970. (iv) nBits: target threshold of a valid block hash.

(v) Nonce: an 4-byte field, which usually starts with 0 and increases for every hash calculation (will be explained in details in Section III).

(vi) Parent block hash: a 256-bit hash value that points to the previous block. The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions . Digital signature based on asymmetric cryptography is used in an untrustworthy environment. We next briefly illustrate digital signature.

B. Digital Signature Each user owns a pair of private key and public key. The private key that shall be kept in confidentiality is used to sign the transactions. The digital signed transactions are broadcasted throughout the whole network. The typical digital signature is involved with two phases: signing phase and verification phase. For instance, an user Alice wants to send another user Bob a message.

(1) In the signing phase, Alice encrypts her data with her private key and sends Bob the encrypted result and original data.

(2) In the verification phase, Bob validates the value with Alice's public key. In that way, Bob could easily check if the data has been tampered or not. The typical digital signature algorithm used in blockchains is the elliptic curve digital signature algorithm (ECDSA)

C. Key Characteristics of Blockchain In summary, blockchain has following key characteristics.

• Decentralization. In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank), inevitably resulting to the cost and the performance bottlenecks at the central servers. Contrast to the centralized mode, third party is no longer needed in blockchain. Consensus algorithms in blockchain are used to maintain data consistency in distributed network.

• Persistency. Transactions can be validated quickly and invalid transactions would not be admitted by honest miners. It is nearly impossible to delete or rollback transactions once they are included in the blockchain. Blocks that contain invalid transactions could be discovered immediately.

• Anonymity. Each user can interact with the blockchain with a generated address, which does not reveal the real identity of the user. Note that blockchain cannot guarantee the perfect privacy preservation due to the intrinsic constraint

D. Taxonomy of blockchain systems Current blockchain systems are categorized roughly into three types: public blockchain, private blockchain and consortium blockchain . In public blockchain, all records are visible to the public and everyone could take part in the consensus process. Differently, only a group of pre-selected nodes would participate in the consensus process of a consortium blockchain. As for private blockchain, only those nodes that come from one specific organization would be allowed to join the consensus process.

IV. WHAT IS GENESIS BLOCK

The first block #0 created in 2009 is referred as Genesis block in Blockchain. It is common ancestral parent of all the new blocks created and if traversed backward in time we will reach genesis block in the end.

Genesis block is common ancestor of all the blocks and was created in 2009. It is encoded within bitcoin client software and can't be tampered. All the node always knows the hash and structure of genesis block which is secure root. The statically encoded genesis block can be seen inside the Bitcoin Core client in chainparams.cpp . We can look for exact block hash:

"000000000019d6689c085ae165831e934ff763ae46a2a6c1 72b3f1b60a8ce26f" in the block explorer websites to find details of Genesis block, latest transactions and all the newly created blocks with BlockHash, height, next block, size in bytes .

V. WHERE CAN BLOCKCHAIN BE USED?

In the following part of the article we will discuss some of the many various applications using Blockchain. We will frequently use the term smart contract. Let us define the term.The Blockchain is ideal for what are known as smart contracts.

What are smart contracts?

Smart contracts define the rules and penalties around a specific agreement in the same way as traditional contracts do. However, the big difference is that smart contracts automatically enforce those obligations. The contracts are coded so that they are discharged on the fulfillment of specific criteria.

A warranty claim

Usually settling warranty claims is expensive, time-consuming and often difficult for those making the claim. It is possible to implement smart contracts using Blockchain that will inevitably make the process a lot easier.

Derivatives

Derivatives are used in stock exchanges and are concerned with the values of assets. Smart contracts in the trading of stocks and shares could revolutionize current practices by streamlining, automating and reducing the costs of derivatives trading across the industry. Settlements could be completed in seconds rather than the three days that are needed at present. Using smart contracts, peer-to-peer trading will become a usual operation, resulting in a complete revolution in stock trading. Barclays and several

other companies has already trialed a way of trading derivatives using smart contracts, but they came to the conclusion that the technology won't work unless banks collaborate to implement it.

Insurance claims

With smart contracts, a certain set of criteria for specific insurance-related situations can be established. In theory, with the implementation of Blockchain technology, you could just submit your insurance claim online and receive an instant automatic payout. Providing, of course, that your claim meets all the required criteria. French insurance giant AXA is the first major insurance group to offer insurance using Blockchain technology. They've recently introduced a new flight-delay insurance product that will use smart contracts to store and process payouts. Other insurance companies will surely follow suit.

Identity verification

Too much time and effort is currently wasted on identity verification. Using the decentralization of Blockchains, the verification of online identity will be much quicker. Online identity data in a central location will vanish with the use of the Blockchain smart contracts. Computer hackers will no longer have centralized points of vulnerability to attack. Data storage is tamper-proof and incorruptible when backed by Blockchain. All over the world, the Blockchain is leading to big improvements in the verification of identity.

The Internet of Things (IoT)

The Internet of Things (IoT) is the network of physical devices, vehicles and other items embedded with software, actuators, sensors, software and network connectivity, connected to the Internet. All of those features enable such objects to collect and exchange data. Blockchain and its smart contracts are ideal for this.

Archiving and file storage

Google Drive, Dropbox, etc. have thoroughly developed the electronic archiving of documents with the use of centralized methods. Centralized sites are always tempting to hackers. Blockchain and its smart contracts offer ways of reducing this threat substantially.

There are many Blockchain projects which aim to do this. Bear in mind, however, that there is often not enough storage within Blockchains themselves, but there are decentralized cloud storage solutions available, such as Storj, Sia, Ethereum Swarm and so on. From the user's perspective they work just like any other cloud storage. The difference is that the content is hosted on various anonymous users' computers, instead of data centers.

The protection of intellectual property

Archiving enabled by Blockchain will offer much greater protection of intellectual property than before. An application called Ascribe, using Blockchain, already gives this protection.

Crime

Lawbreakers have to hide and camouflage the money gained from their exploits. Currently this is done with fake bank accounts, gambling, and offshore companies, among other stratagems. There are a lot of concerns regarding the transparency of cryptocurrency transactions. But, all of the necessary regulatory elements, such as identifying parties and information, records of transactions and even enforcement can exist in the cryptocurrency system.

As the technology gets more mainstream attention, Blockchain and its smart contracts have the potential to render most money laundering tactics ineffective and very traceable.

Social media

At present, social media organizations are able to freely use the personal data of their clients. This helps them make billions of dollars. Using Blockchain smart contracts, users of social media will be enabled to sell their personal data, if they so desire. Such ideas are being investigated at MIT. The aim of the OPENPDS/SA project is to provide the data-owner to tune the degree of privacy preservation using the Blockchain technology.

The use of smart contracts in elections and polls

Elections and polls could be greatly improved with smart contracts. There are various apps already in existence, such as Blockchain Voting Machine, Follow My Vote and TIVI. All of them are promising to eliminate fraud, while providing complete transparency to the results and keeping the votes anonymous. However, there is still a long road ahead before decentralized voting is implemented widely.

VI. LIMITATIONS OF BLOCK CHAIN

Complexity:

Blockchain technology involves an entirely new vocabulary.

It has made cryptography more mainstream, but the **highly specialized industry** is no place for a beginner… Thankfully there are blockchain and cryptocurrency courses and indexes being created for newcomers, but overall this is a very complicated industry that will not be soaked in and applied overnight.

Network Size:

Blockchains **require a large network of users**. If a blockchain does not hold a robust network with a widely distributed grid of nodes, it becomes more difficult to reap the full benefit. There is some discussion and debate about whether this a fatal flaw or not for many blockchain projects.

Transaction Costs, Network Speed:

Bitcoin currently being a prime example. The first few years of it's existence, it was noted that transactions we're "**nearly free**" Now, as the network continues to grow, we can clearly see that at this rate using Bitcoin will NOT be the most cost effective option of transferring money due to **rising transaction costs in the network**.

There's also the "politically charged" aspect of using the bitcoin blockchain, not for transactions, but as a store of information. This is the question of ''bloating" and is often frowned upon because it forces miners to perpetually reprocess and rerecord the information.

Human Error:
If a blockchain is used as a database, the information going into the database needs to be of high quality. The data stored on a blockchain is not inherently trustworthy, so events need to be recorded accurately in the first place.
The phrase **'garbage in, garbage out'** holds true in a blockchain system of record, just as with a centralized database.
Unavoidable Security Flaw:
There is one notable security flaw in Bitcoin and other blockchains: If more than half of the computers working as nodes to service the network tell a lie, the lie will become the truth. This is called a '51% attack' and was highlighted by Satoshi Nakamoto when he launched bitcoin. For this reason, bitcoin mining pools are monitored closely by the community, ensuring no one unknowingly gains such network influence.
Politics:
Blockchain protocols disrupt many of the systems in which our banks and governments have created over the period a very long time… In result to blockchain's increasing adoption, many politicians have felt obligated to take a stand to fuel or smother the new technology within their jurisdictions. Many, in my opinion, are very reactionary in their behavior… but only time will tell as to how beneficial or detrimental the technology can be within different societies. Just know that their opinions do matter and play a major role in the progress of applications running on a blockchain.

VII. HOW THE BLOCK IS CREATED

we need some software to develop blocks like c++ and some of the algorithms like SHA-256,SHA-512 are used to link the blocks ,Before we continue. You need to understand certain terms that we are going to use in our program:

- **This:** The "this" keyword is invoked inside a function and enables you to access the values inside a specific object that calls that particular function.
- **Constructor**: A constructor is a special function which can help create and initialize an object within a class. Each class is restricted to only one constructor.

Now that that's done, let's start making our block.
Creating the Block:

```
const SHA256 = require("crypto-js/sha256");
class Block
{
constructor(index, timestamp, data, previousHash = '')
{
this.index = index;
this.previousHash = previousHash;
this.timestamp = timestamp;
this.data = data;
this.hash = this.calculateHash();
}
calculateHash()
{
return SHA256(this.index + this.previousHash + this.timestamp + JSON.stringify(this.data)).toString();
}
}
```

in this way u have to create number of blocks and those are added based on their hash functions using different types of algorithms .

VIII. FUTURE OF BLOCKCHAIN

In future blockchain is used in different purposes like financial sector, hospitals, data security ect..There is lot of scope to change all the softwares into blockchain based software because of the security issues .present world face a lot of problem with security, it is achieved with the help of blockchain technology ,that's why it is an emerging technology in the world.

IX. CONCLUSION

In this paper I am discussed about blockchain technology basics, like what is block, advantages, disadvantages and how blocks are created. with the help of blockchain we will provide more security , And there are some limitations of the blockchain also discussed in this paper; those drawbacks are overcome with the help of some new techniques and some algorithms. With the help of some cryptography methods we will provide some more security to blockhain. We will found some problem in block chain this will be over come to add some new rules to blocks creation.

References:

- An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 2017 IEEE 6th International Congress on Big Data
- Blockchain: Future of Financial and Cyber Security, 978-1-5090-5256-1/16/$31.00 c 2016 IEEE
- Security and Privacy in Decentralized Energy Trading through Multi-Signatures, Blockchain and Anonymous Messaging Streams, Nurzhan Zhumabekuly Aitzhan and Davor Svetinovic, Member, IEEE,
- http://www.supplychain247.com/article/why_blockchain_is_a_game_changer_for_the_supply_chain
- https://www2.deloitte.com/us/en/pages/operations/articles/blockchain-supply-chain-innovation.html
- https://hackernoon.com/blockchain-technology-for-supply-chain-management-3d12121df57b
- https://www.commerce.gov/news/press-releases/2018/02/secretary-ross-releases-steel-and-aluminum-232-reports-coordination
- https://cerasis.com/using-blockchain-in-supply-chain-logistics