iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.56064

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: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

Bitcoin in Blockchain Technology and Ethereum InSmart Contracts

Y. Mythili Maha Lakshmi[1], Y. Vamshi Vardhan Raj[2], Unnam Deepthi Chowdary[3], Oduri Gehini Naga Sai Ratna[4], Mosali Harini[5], Dr. Gayathri Edamadaka[6]
Department of Computer Science and Engineering, Konneru Lakshmaiah University, Hyderabad, India

Abstract: ***Blockchain is one of the most trending technologies which plays a major role in online transactions using cryptocurrencies. The blockchain is a chain of blocks that consists of all the transactions up to the size of 1MB. This blockchain has many properties such as decentralization, immutability, transparency, and audibility, making transactions more secure and tamper-proof. It is tamper-proof because there is no possibility to tampera block as every block in the blockchain has the hash of the previous block. And among cryptocurrencies, bitcoin is one ofthe most popular... In fact, blockchain was introduced to the world because of bitcoins. Apart from cryptocurrency, blockchain technology can be used in financial, NYC, and social services, risk management, food, healthcare facilities, and so on. Numerous studies have examined the potential that blockchain offers inmultiple application sectors, as well as the benefits and different kinds of blockchain. This paper presents a comparative studyof bitcoins in blockchain technology and the workflow of the bitcoin, compares bitcoin and Ethereum, and provides the use of smart contracts in this emerging technology. The methodology considered for this research is the Ethereum blockchain in smart contracts using a solidity programming language.***

Index Terms: Blockchain, Ethereum, Bitcoin, Smart contracts,Solidity

I. INTRODUCTION

Cryptocurrencies are attracting people from many fields these days. In recent years, researchers have shown great interest in blockchain cryptocurrencies. Blockchain technology developers have tried to improve this and make it more trustworthy for blockchain users. Blockchain was introduced to store transactions made by users using Bitcoin as Bitcoin was the first and most popular cryptocurrency introduced to the world. Billed as the first cryptocurrency, Bitcoin has beena huge success. Blockchain is the cornerstone of Bitcoin [5].A blockchain is considered a public ledger. All nodes in the public ledger have identical copies of the global data sheet. All data in the Global Data Sheet is identical and will be updated once trading is open. Initiated transactionsare stored on a chain of blocks, and once a transaction is initiated, new blocks are added to the blockchain as the mining process performed by miners completes. After solving theProof of Work and verifying the block, the miner inserts the block into the blockchain. Bitcoin does not support building complex decentralized applications. Blockchain has properties

Identify applicable funding agency here. If none, delete this. such as security, transparency, immutability, and decentraliza-tion. Blockchain can significantly reduce costs and improve efficiency. Blockchain can be applied to applications far beyond cryptocurrencies. Blockchain is used in many other ways in our daily lives. Block sizes are up to 1 MB and can accommodate 1 to 500 transactions. As the size of the block increases, so does the number of transactions the block can hold, which takes up more space and slows down the propagation to the network. The chain grows continuously as new blocksare added. Blockchains work in a decentralized environment (distributed ledger) made possible by combining several core technologies such as digital signatures, cryptographic hashes, and distributed consensus algorithms [3].Other blockchains such as Ethereum have been introduced as second-generation blockchains that enable the building of complex decentralized applications beyond cryptocurrencies. This Ethereum is rewarded to miners when new blocks are added to the blockchain after solving the most difficult puzzle called Proof of Work. Transaction fees charged by miners are also in the form of Ethereum. Ether transactions can be done between two people using the sender's wallet and public key for digital signature. The Ethereum blockchain is the most popular blockchain used to develop smart contacts. Ethereum is a permissionless blockchain embedded in a Turing machine using a Turing-complete language that allows the creation of smart contracts and decentralized applications [6].

There are two types of blockchains: public or permissionless blockchains and private or permissioned blockchains. A public blockchain is a blockchain that is accessible to anyone who accesses the blockchain. Users can write and transact using this blockchain,but they cannot edit the data until it is checked into the blockchain.

©IJRASET: All Rights are Reserved

The security of this blockchain is maintained using a consensus algorithm. will be Examples of these public or permissionless blockchains are Bitcoin and Ethereum. Private blockchains, on the other hand, only allow authorized users to access the blockchain. Only authorized users can write and trade on this blockchain. Examples of private or permissioned blockchains are Ripple and Eris.

II. BLOCKCHAIN ARCHITECTURE

Every transaction is initiated by the node in a decentralized blockchain network after using the private key cryptography or permission cryptosystem and verifying the digital signature.A transaction is considered a data structure. When a person initiates a transaction of asserts then first the digital signature is verified then a block or a node is created. And all these blocks are stored in an unconfirmed transaction pool and then they are propagated into the network using a specific protocol known as the Gossip protocol. Then the miners need to check,validate and verify these transactions based on certain criteria.For example, a node tries to verify and validate a transaction by checking whether the initiator has sufficient balance tomake the payment or tries to fool the system by using double- spending. Double spending refers to using the same input amount for more than one user at the same time which might cause confusion to the miners while verifying. This double spending problem can be solved by my multi-transitional pool. And once the transaction is verified and validated by the miners then the transaction is appended in a block. Peoplewho use their own computational powers to mine are called miners. There are two types of miners one is called solo minersand the others are called pool miners.

Miner nodes need to solve the proof of work and spenta sufficient amount of their computing resources in order to publish a book. The miner who solves the proof of work will get an opportunity to create a new block and he will also receive an award for solving the proof of work after validationwhich'll be done by other peer miners using the consensus mechanism. After that, the new block is added to the existing chain and ledger which is transparent because everyone can view it and it contains accurate details which are verified and validated by the minors.

Now when the transaction is confirmed, the next block will link itself to the newly created block which is been verified and validated by miners using a cryptographic hash pointer. Now the block will obtain the first confirmation whereas the transaction will obtain the second confirmation. In this way whenever a new block is appended to the chain, the transactionwill be reconfirmed. In general, a transaction will need six confirmations to be considered final [3].

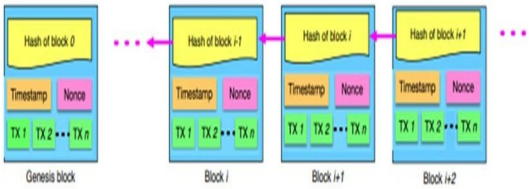


Fig. 1. Continuous sequence of the blocks in the blockchain [2]

A. *Transaction*

A blockchain can be defined as a small unit of tasks that is stored in records and these records are known as blocks [3]. All the blocks are executed, implemented, and stored in the blockchain for verification and validation done by the miners in the blockchain network. Each block in the blockchain can beverified but not updated. So, to initiate a transaction a person needs to own a wallet, a program linked to your blockchainto which only you have access and allows you to track the crypto that you own and helps you to commit a transaction to others. Each wallet is protected by a few cryptographic methods called public and private keys.

A public key is also identified as an address. This address basically consists of a set of numbers and alphabets whichhas to be shared with the other users in order to receive funds whereas the public key has to be kept as a secret. This private key is more like a bank key which helps in authorizes the spending of the funds which've been received by the associatedpublic key.

With the help of the wallet, the user can commit a transac- tion to another using his funds after authentication using the public and private keys. And the transaction will be committedin the blockchain.

So, after a transaction is initiated by a user then a blockfor that specific transaction is created. And once the blockis created then the block is broadcasted to all the P2P par- ticipation computers in the computer network. And these are called nodes. Now the miners add these block blocks in the mem pool or memory pool so that they will be mined by the miners. And then the miners start mining that block that is supposed to be mined. The miners will start mining the block by solving a hard puzzle called proof of work (POW).

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Thefirst miner to complete the mining of the block is considereda winner and will receive a reward in the form of Ethereum. And the other miners will validate that transaction with the help of some rules set by the blockchain. And after the transactions are validated by the miners they are stored in a block and are sealed with a lock called a hash. Every block has its own unique hash value.

After the block gets validated by the miners they add itto the blockchain. And every block consists of the hash ofthe previous block in this way the blocks can't be alteredor modified. Once the block is added to the blockchain thenit can't be edited or modified. And then the transaction willbe committed. Blockchain came into the picture because of Bitcoin, therefore blockchain is the underlying technology of blockchain.

When a person initiates a transaction, the miners validate and verify that specific transaction. And once the transaction is verified and validated it will be stored in a file called a block, which is the basis of the blockchain network. Thisblock basically consists of two parts the block header and the block body. When information is stored in a block it doesn't take up a large amount of space. Blocks might include magic number, block size, block header, transaction counter, andtransactions. And among all these elements the transaction element is the largest. It depends upon the storage size ofthe block header which includes the sub-elements such asversion, previous block hash, hash Merkle root, time, bits,and nonce.

1) *Magic Number:* A number with precise values that enables us to identify a piece of data as being a part of a given cryptocurrency's network.
2) *Block Size:* Block size basically sets the limit on the block so that we can write a certain amount of information in it.
3) *Block Header:* Block Header basically contains the information about the block.
4) *Transaction Counter:* This transaction counter repre- sents the number of transactions present in the block.
5) *Transactions:* Transactions are basically the list of trans-actions that are present in the block.
6) *Version:* Version basically indicates the cryptocurrency version that is being used in the block.
7) *Previous Block Hash:* Contains the hash of the previous block's header. This previous block hash helps us to know if any block has been changed or corrupted.
8) *Harsh Merkle Tree:* Root: Hash of the transactions of the Merkle tree of that specific block.
9) *Time Stamp:* Time Stamp helps us to know when the block was created and when it was accessed.
10) *Nonce:* The encrypted number should be solved bythe miner to verify and validate the block.

The number of blocks that a Blockchain can contain depends upon the block size as well as the size of the transactions. And blockchain basically uses an asymmetriccryptography mechanism to validate the authentication of the transaction.

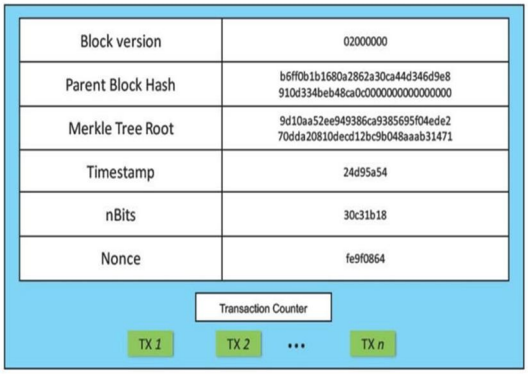


Fig. 2. The structure of the block [3]

B. P2P Network

A peer-to-peer network is basically a simple network of computers. In a peer-to-peer network, each computer acts asa node and each node acts as a server. As there is no centralso this peer-to-peer network allows us to share a huge amount of data. And while distributing the data in the peer-to-peer network all the tasks are equally divided amongst all the nodes. So, each node present in the network shares an equal workload. In order to stop the network from working, all the nodes in the network need to stop working individually, because allthe nodes in the network work independently. Unstructured P2P, Structured P2P, and Hybrid P2p networks are the three different types of P2P networks. A P2P network doesn't havea large number of nodes, it has less than 12 nodes. And each computer in the P2P network stores its own data which canbe accessed by the whole group of nodes.

As each and every node in the network acts as a client as well as a server thereis always a constant threat of an attack. Each computer in the network has an equal set of abilities and responsibilities. And also has the ability to share data with all the other computers in the network. And the P2P architecture actually composes0f 12 groups or more computers. Fie sharing, blockchain, collaboration, direct messaging, and file-sharing networks are a few of the applications of the P2P network.

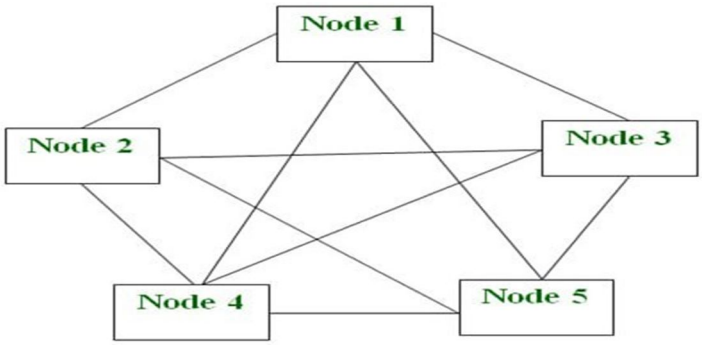


Fig. 3. Nodes in P2P network [4]

C. Consensus Algorithm

An agreement on one number among distributed networks can be carried out using the consensus algorithm. Blockchain is a digital database or distributed ledger and it is immutable and decentralized which produces security, privacy, and transparency. As blockchain is a decentralized ledger and does not have any central authority to control and verify transactions this consensus algorithm in blockchain acts asan agreement between all the nodes in the blockchain of the current data state in the ledger. In blockchain technology, the consensus algorithm provides reliability to trust known peers in the network. The consensus algorithm plays a core part in blockchain technology as it acts as an agreement between nodes and maintains the collaboration and corporation between the nodes. There are different types of consensusalgorithms they are:

1) *Proof-of-Work:* proof-of-work (Pow) is the first and oldest consensus algorithm of blockchain technology. It was initiated by Cynthia Dwork and Moni Naor in the year 1993 and it was re-established in 2008 by Satoshi Nakamoto who was also the founder of Bitcoin. Proof-of-work focuses on resolving complex mathematical problems and producing predictions as many as possible in the shortest time. proof-of- work is the most reliable and secure consensus algorithm butit lacks scalability. Proof-of-work is used by cryptocurrencies such as Ethereum, bitcoin, and other public blockchains. In this consensus algorithm, a group of people called minerscompete with each other and solve mathematical puzzles on the block before accepting it to the ledger to completethe transactions successfully within the network. This whole process is called mining when the miner creates a new block successfully, they are rewarded. this concept of proof-of-workis mainly used in Bitcoin. Using proof-of-work before every transaction helps to prevent double-spending if anyone is trying to do a duplicate transaction then it is identified and the transaction is canceled and not approved.
2) *Proof-of-Authority:* Proof-of-Authority (POA) was initiated in the year 2017 by Gavin Wood who was also the co-founder of Ethereum. The Proof-of-Authority consensusalgorithm is a permissioned blockchain in which the nodesare pre-selected and this proof-of-authority algorithm has high scalability and fault tolerance. In the Proof-of-Authority algorithm, the right to create a new block in the networkis given to the nodes whose identity or authority is verifiedor proven. it only allows authorized nodes to add a new block in the blockchain to complete the transaction. the proof-of-authority algorithm depends on the limited number of miners and provides high scalability and maintains privacy.proof-of-authority provides more security to companies and maintains their privacy an example of this is Microsoft Azure. Proof-of-Authority is not a decentralized system in this the validators are visible to anyone this algorithm is an attemptto make a centralized system more efficient.
3) *Proof-of-Stake:* The purpose of initiating proof-of-stake is the same as proof-of-work but it differs in process. proof-of-stake is a substitute for proof-of-work. As in proof-of-work, the miner has to resolve the mathematical puzzles to create a new block but here the miner who creates the block is selectedby the means in a deterministic manner also called a stake. in the proof-of-stake consensus algorithm, there is no reward to the miners as the miners are selected according to the stake, they invested in the transaction they only get their transaction fee there won't be rewards for the miners. In this proof-of- stake we have 3 types of stakes they are:

- Delegated Proof-of-Stake
- Leased Proof-Of-Stake
- Proof-Of-Importance

4) *Byzantine Fault Tolerance (BFT):* Byzantine fault tol- erance was initiated by Barbar Liskov and Miguel Castro in the 1990s and detailed by Leslie Lamport, Robert Shostak,and Marshall Pease in 1982. Byzantine fault tolerance presentsproblems and dilemmas the network must address as the next steps. Byzantine Fault Tolerance is a consensus algorithm on the blockchain that reaches a consensus on the same value evenif there are problems with the network. B. If the node does notrespond or does not respond correctly. The reason for starting the Byzantine Fault Tolerance algorithm is to solve problems in the network and continue normal transactions. Byzantine fault tolerance is possibly divided into two categories:

- Practical Byzantine Fault Tolerance
- Delegated Byzantine Fault Tolerance

5) *Proof-Of-Capacity:* Proof-Of-Capacity is a consensusalgorithm that allows the nodes to use the space to mine the crypto tokens and complete the transaction. Proof-of-Capacity was initiated because proof-of-work and Proof-Of-Stake are taking high energy consumption which can resolve that problem. Instead of frequently changing the hashing valueand the numbers in the block header proof-of-capacity stores the possible solutions of the mining activity in the mining device before the mining activity starts and there would be a high chance of winning the reward for the miners. The more storage the mining device has the many possible solutions for miners and there is no need for expensive components in this process the chance of participating in the network for the average miner is high.

6) *Proof-Of-Identity:* Proof-Of-Authority is a consensus algorithm for permissionless blockchain and it is similar to theproof-of-authority consensus algorithm. This proof-of-identityalgorithm replaces the proof-of-work and proof-of-stakealgorithms as in this algorithm each and every user gets the power to vote and receive the rewards. The proof-of-identity verifies the identity of the individual by the cryptographic method using the user's private key. Only identified and verified users can create a block and complete the transaction. the advantage of using proof of identity is it ensures integrity and authentication.

7) *Proof-Of-Activity:* The proof-Of-Activity consensus algorithm is a combination of proof-of-work and proof-of- stake algorithms in the blockchain. We use a proof-of-activity consensus algorithm for original transactions and agreements between the miners. In this proof-of-activity consensus algorithm, miners resolve the mathematical cryptographic problems with electrical energy and hardware. In this algorithm, the block is verified by the miners and before sending the block to the blockchain the block is checked many times so that the transaction is completed successfully without any problems.in this algorithm when the mining process is started it behaves like the proof-of-work and once the new block is created it behaves like the proof-of-stake algorithm. The cryptocurrency which mostly uses the proof-of-activity algorithm is Decreed (DCR).

8) *Proof-Of-Elapsed Time:* The Proof-Of-Elapsed Time algorithm is initiated to prevent high resource implementation and energy utilization and to be more efficient. this proof-of- elapsed time consensus algorithm generates a time and decides the rights applicable to the miners and block winners within the network of the blockchain. The proof-of-elapsed time algorithm ensures transparency. The Proof-Of-Elapsed Time was developed to determine who creates the next block in the blockchain network. this algorithm follows a lottery system sothat all the users get an equal chance of winning the rewards and creating the blocks. this algorithm works as it creates a random waiting time for each node so that when the waiting time is finished the node commits the transaction till thenthe node will be in the sleep position. The proof-of-elapsed time consumes more power than the proof-of-work algorithm as it allows each and every node to participate without any destruction in the transaction process and increases energy efficiency.

III. CRYPTOCURRENCIES

A well-known digital asset called a cryptocurrency is found on a decentralized network called the Blockchain. The word Cryptocurrency arrived from "crypto" which means cryptog- raphy and "currency" which means money. Cryptocurrency is basically used in Blockchain. The transaction details made using the cryptocurrency are stored in the blockchain which can't be edited or modified.

IV. BITCOIN A WELL-KNOWN CRYPTOCURRENCY

Bitcoin (BTC) is a cryptocurrency, or digital money, meant to function like money and a payment method independentof any one person, organization, or entity, hence eliminat-ing the requirement of third-party participation in monetary operations.

It is given to blockchain miners as a reward for their efforts in validating transactions and can be bought on numerous platforms. Blockchain came into the picture becauseof Bitcoin. All the transactions made using bitcoins are stored in the blockchain. Satoshi Nakamoto, an unidentified devel- oper or team of developers, presented Bitcoin to the worldin 2009. It soon rose to prominence as the most well-known cryptocurrency in the world. Because of its popularity, severalnew cryptocurrencies have been produced.
These competitionseither aim to supersede it as a means of transaction or are employed as utility or security tokens in other blockchainsand new financial systems.

V. BITCOIN'S BLOCKCHAIN TECHNOLOGY

A well-known digital asset called a cryptocurrency is found on a decentralized network called the Blockchain. Blockchain is a distributed record of transactions, a public ledger that stores data. Cryptography is used to protect data within the blockchain. The primary goal of the original Bitcoin whitepaper was to provide a decentralized electronic cash payment mechanism between diverse parties by removing central middlemen [6]. Blockchain came into the picture because of bitcoins which is one of the well-known and most used cryptocurrencies in the world. All the transactions made using bitcoins are stored in the blockchain. when a person wants to initiate a transaction, he needs to know the sender's public key which is also known as the bitcoins address. A Bitcoin transaction transfers ownership of a certain number of bitcoins to another Bitcoin wallet.
so, whenever someone initiates a transaction, a block willbe created for that specific transaction. once the block is created then it is broadcasted into the network to get validated and verified by the miners. After getting broadcasted into the network the miners will collect these blocks and add themto be mined queue. The miners collect the block and verifyand validate it by solving a hard puzzle called proof of work (POW).
Proof-of-work assures validity statistically as long as noone entity has enough computational power to add an illegal block to the chain. Each miner competes with the other minersfor the opportunity to add a block to the distributed ledger.The miner accomplishes this by performing computationally intensive tasks. Bitcoin mining requires the miner to discover astring that, when combined with the preceding block header's hash and then re-hashed, yields a certain text. Anybody attempting to "spoof" the chain (for example, by changingdata on past transactions) must calculate the proof of workfor all transactions in the block. To persuade the system to employ a fraudulent chain, blocks would have to be added to the chain at a rate quicker than a real chain would evolve.
Each miner that joins the blockchain network improvesdecentralization and enhances consensus processes. In contrastto traditional centralized, where consumers often lack trustand transparency in the provider, transactions on decentralizedblockchains are clear and visible to users. Miners that solvethe cryptographic challenge are rewarded, therefore miners arealways trying to build new blocks that may be added to the chain.

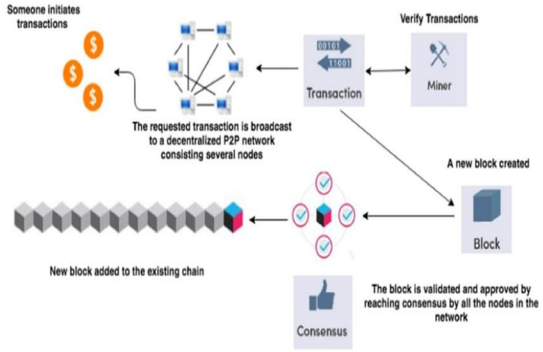


Fig. 4. Functional Pictorial Representation of a Blockchain network [3]

Users often allocate a transaction fee to miners upon suc- cessful block formation while submitting transactions. There will be no data in the header about the transaction charge. Users can charge a transaction fee by transferring less money to the receivers than the entire quantity of input. This unal- located transaction amount can be thought of as a transaction charge, as shown in Eq. 1.

$$Inputs - Outputs = Fees \quad (1)$$

Miners add their own Coin base transactions, as well as the transaction data they are attempting to check and validate whenmining a block. A coin base transaction is a sort of Bitcoin exchange that only a miner may produce. This transaction has just outputs, and one is generated for each new block mined onthe network.

This is the transaction in which a miner receives the block reward for their efforts. This transaction also includesany transaction fees earned by the miner. The network peers determine if the transaction is leveled out prior to choosing whether to record it in the distributed ledger.

The cryptocurrency transaction will deliver the block reward and the total transaction fees to the miner's specified address. This demonstrates that a miner must assign his reward when producing a block. But, as demonstrated in Eq. 2, every node on the network will verify whether the block meets the condition.

As a result, a miner can only use the block reward and transaction costs once the block has been validated [3].

$$Sum(BlockOutputs) <= sum(BlockInputs) + Rewards \quad (2)$$

Once the miners solve the proof of work, they will append it to the blockchain. Others miners will validate and verify this transaction. And each block in the blockchain will contain the hash of the previous block which will help us to maintainthe security of the blockchain. No one can edit or delete the blocks in the blockchains because every block has the hash of the previous block. And once the block is added to the blockchain the transaction will get committed. And all the transactions in the blockchain cannot be edited or altered and can be viewed by everyone as blockchain is a decentralized network.

VI. ETHEREUM

A decentralized blockchain with smart contract capabil- ities is Ethereum. The platform's native cryptocurrency is ether, abbreviated as ETH and represented by the symbol.The value of Ether on exchanges is only second to that of Bitcoin. The programmer is open-source. 2013 saw the development of Ethereum by programmer Vitalik Buterin. Gavin Wood, Charles Hoskinson, Anthony Di Iorio, and Joseph Lubin were other Ethereum founders. Fundraising for development work started in 2014, and on July 30, 2015,the network launched. Anyone may publish permanent and unchangeable decentralized apps on Ethereum, allowing users to share information with them. Financial instruments that do not directly rely on financial intermediaries like brokerages, exchanges, or banks are offered through decentralized finance (DeFi) apps. This makes it easier to borrow money using Bitcoin assets or to lend them out for interest. Customers of Ethereum may also generate and trade non-fungible tokens (NFTs), which are tokens linked to certain digital assets like photos. On top of the Ethereum blockchain, many more cryptocurrencies use the ERC-20 token standard, and theyhave made use of the Ethereum platform for ICOs. Ethereum underwent an upgrading procedure known as "the Merge" on September 15, 2022, switching from proof-of-work (PoW) to proof-of-stake (PoS). Ethereum now needs 99

A. Ethereum Account

In Ethereum, the state is made up of things called "ac-counts," each of which has a 20-byte address. Transfersof value and information between accounts constitute state transitions. Four fields are present in an Ethereum account:

- A counter called the nonce is used to guarantee that eachtransaction can only be completed once.
- The current ether balance in the account
- The contract code for the account if any
- The storage of the account (empty by default)

The primary internal cryptocurrency of Ethereum is called "Ether," and it is used to pay transaction fees. In general,there are two kinds of accounts: contract accounts, whichare managed by their contract code, and externally ownedaccounts, which are controlled by private keys. An externally owned account has no code, and sending messages from one requires creating and signing a transaction. In contrast, a contract account's code is activated each time it receives a message, enabling it to read and write to internal storage, send additional messages, or create new contracts. Note that Ethereum "contracts" are more akin to "autonomous agents" that live inside the Ethereum execution environment, always executing a specific piece of code when "poked" by a message or transaction, having direct involvement with their own ether balance, while simultaneously maintaining track of indeter- minate variables throughout their own trick/value store. They are not intended to be "fulfilled" or "complied with" in the traditional sense.

B. Transactions and Messages

Ethereum transactions and messages are the two main types of data that can be sent and stored on the Ethereum blockchain. A transaction on the Ethereum blockchain is a digital message that contains information about a transfer of Ethereum cryptocurrency from one account to another.

Smart contracts, which are self-executing agreements with theterms of the agreement between the buyer and seller being directly encoded in lines of code, can likewise be executedvia transactions. When a user initiates a transaction on the Ethereum network, they must specify the recipient address, the amount of Ethereum they want to send, and a gas fee, which is the amount of Ethereum they are willing to pay to havethe transaction processed. The gas fee is used to compensate miners who validate and process the transaction. Messages,on the other hand, are similar to transactions but are used to communicate with smart contracts on the Ethereum network. They can be used to send data or trigger specific functions within the smart contract. Unlike transactions, messages donot involve the transfer of cryptocurrency. Both transactions and messages are recorded on the Ethereum blockchain and can be viewed by anyone with access to the network.

This transparency and immutability is one of the key features ofthe Ethereum blockchain and makes it a popular platform for decentralized applications and smart contracts.

VII. ETHEREUM IN BLOCKCHAIN

The Bitcoin blockchain is comparable to the Ethereum blockchain. Ethereum blocks differ primarily in that they include the block number, difficulty, nonce, etc. Additionally, the most current state and the transaction list. The previous state is applied to each transaction in the transaction list to construct the new state.

The block header in the Ethereum blockchain consists of the Keccak 256-bit hash of the parent block's header, theaddress of the recipient of the mining fee, hashes of the roots of state, transaction, and receipt attempts, the difficulty, the block's current gas limit, a number indicating how much gas was used in all of the block's transactions, the timestamp, the nonce, and several additional hashes for verification.

With a focus on scenarios where rapid development time,security for small and infrequently used applications, and the ability for various applications to interact very efficiently are important, Ethereum aims to design a different protocol for decentralized application development. This protocol will offer a unique set of trade-offs that, inour view, will be extremely helpful for a broad category of decentralized applications. Ethereum achieves this by creating a blockchain with a built-in Turing-complete programming language that enables anyone to create smart contracts and decentralized applications with their own arbitrary rules for ownership, transaction formats, and state transition functions. In a sense, this is the most fundamental abstract layer. A blockchain that has a Turing-complete programming language built in that anybody can use to develop decentralized applications and smart contracts with their own custom ownership, transaction format, and statetransition rules. Name coin can be implemented in its most basic form in just two lines of code, and alternative protocols for currencies and reputation systems can be created in less than twenty. With the additional capabilities of Turing completeness, value awareness, blockchain awareness, and state, smart contracts—cryptographic "boxes" that store value and only unlock it if certain conditions are met—can alsobe built on top of the platform. These contracts have far more power than those offered by Bitcoin scripting. The network's vulnerability to ASIC mining is one of its main issues. Ethereum uses the memory-intensive and less efficient Ethash proof-of-work method.

appropriate for ASIC mining. The Dagger-Hashimoto algorithm has been modified, and this is represented as Ethash. Every node in the Ethereum network is controlled by the EVM and follows its commands. The nodes then carryout the smart contracts' execution after being converted into EVM code [31]. Solidity is one of the most widely used programming languages for creating smart contracts. The average block duration on the Ethereum network is 15 seconds, with occasional spikes of up to 30 seconds. As of January 29th, 2018, the Ethereum blockchain weighs47.43GB using the Geth blockchain client with fast sync. Despite worries regarding Ethereum's scalability, it has beendocumented that the network has been effectively managed. Around a million unique transactions every day, or about 11 per second on average the proof-of-stake mining paradigm, where the reward is given to the miners based on their coinholdings rather than their computations, is supposed to bemade possible by the "Serenity" prototype of the Ethereum platform, which is based on the Casper consensus algorithm and is intended for later implementation. Token systems, financial derivatives, identity and reputation systems, file storage, insurance, cloud computing, prediction markets, andother applications are listed as possible uses for Ethereum. Decentralized applications are Ethereum's most crucial use case (Dapps). Some of them include Civic (identification), Augur (prediction markets), and Golem (supercomputing).

VIII. APPLICATIONS OF BLOCKCHAIN

Blockchain is a decentralized ledger or database technology that is used by all nodes in a computer network to store data electronically in a digital medium. In the blockchain, the data is stored in a structured format so that we can easily traceand maintain the information.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

As Blockchain is becomingmore and more popular within the last decade and it might become the next big thing in the world of technology. So, this Blockchain technology can be used in different applications and in different sectors such as Healthcare, online identity verification, the energy industry, protection of copyrights, Cryptocurrency, the Internet of Things (IoT), and Logistics.

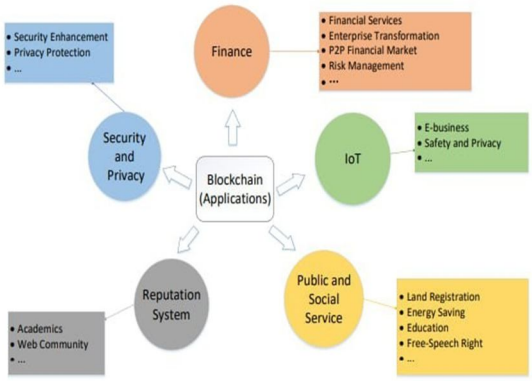


Fig. 5. Representative application domains in blockchain [2]

A. Healthcare

Blockchain is a distributed ledger technology it secures information so that only authorized people can access the data. By using blockchain in healthcare canter we can secure the patient's personal information and their reports so that without doctors' permission no one can view patients' reports. Blockchain maintains transparency so that we can trace and maintain the records easily.

B. Online Identity Verification

Identity verification and authorization of a person has been a difficult task nowadays in both the public and private sectors. With Current identification tools it is difficult to identify a particular person who they are and with these methods it very expensive and time taking process. As nowadays everyone is forgetting their usernames and passwords it is difficult to identify the particular person using their photos or with their government-issued ID and it is easy to spoof. Using blockchain technology we can identify, trace and verify the individual within seconds.

C. Energy industry

To maintain steady energy supplies and ensure the overall health and wellness of the nation the energy sector pro- tects electricity, oil, and natural gas resources and assets. Blockchain is a distributed ledger that stores digital transac- tions without using a central authority and it provides greater efficiency and security and gives updates on energy usage.

D. Protection of copyrights

Blockchain is a decentralized database in which all thetransactions are recorded. Once the transaction is validated theupdated data is reflected on all the nodes. Nowadays with the development of technology, there is more data transmission like photos, videos, documents, music, etc. with this thereis an increase in copyrights and ownership regulations there are many loopholes in present copyright protection techniques these are very time taking and less secure but using blockchain smart contract technique we can trace the data who are usingit and downloading it by this we can protect and control the data.

E. Cryptocurrency

Cryptocurrency is the finest implementation of blockchain. Cryptocurrency is a digital payment method for transactions that don't count on banks for any type of verification. Instead of carrying physical money and doing transactions by using cryptocurrency from anywhere to anyone we can send and receive payments easily without our time and energy. These cryptocurrencies are stored in the digital wallet and all the transactions made using the cryptocurrency are stored in the digital database where we have all transaction details of our cryptocurrency. A digital wallet is a tool in which we store our encryption keys which confirms the particular person's identityand allows access to their cryptocurrency. there is no third- party collaboration in this transaction and it is very secureand easily tracible.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

F. *Internet of things (IoT)*

The Internet of Things (IoT) is a method of a network device with which we interchange information and communicate with each other. But those technologies lack in security and efficiency of the network using blockchain (IoT) Internet of Things maintains security and efficiency as blockchain is immutable it traces the unauthorized users and modifications made by them as blockchain is a distributed shared ledger it stores the digital assets securely without any third-party involvement.

IX. SMART CONTRACTS

A smart contract, often referred to as a crypto contract, is a piece of software that, under particular circumstances, directly and independently controls how digital assets are transferred between the parties. Similar to a conventional contract, a smart contract operates with automatic contract enforcement. Smart contracts are computer programmers that run precisely as their authors have coded or programmed them to. Smart contracts are binding by code, just like a conventional contract is by law. By utilizing smart contracts to move value from one party to another party, the Bitcoin network was the first to employ them. Later, the Ethereum platform appeared, and it was regarded as being more potent because programmers and developers could create unique contracts using a Turing-complete language. These are some of the most common smart contract platforms such as Ethereum, Solana, Polka Dot, Hyperledger fabric, etc.

A few applications of smart contracts are:

A. *Real Estate*

Reduce the amount paid to the middleman and divide it among the participants. As an illustration, a smart contract to move apartment ownership once a specific number of resources have been transferred to the seller's account.

B. *Vehicle Ownership*

A blockchain can be used to implement a smart contract that records car ownership and maintenance. For instance, the smart contract could mandate vehicle maintenance every six months, failure to which would result in the suspension of a driver's license.

C. *Music Industry*

The music industry may use a blockchain to record the ownership of music. A blockchain-based smart contract can be used to automatically credit the owner's account with royalties when a piece of music is played for commercial purposes. Also, it can be useful in resolving ownership disputes.

D. *Government elections*

It would be very difficult to decrypt the voter address and amend the vote once the votes are stored in the blockchain, increasing the confidence against unethical acts.

E. *Healthcare*

Healthcare payment processes can be automated with smart contracts to reduce fraud. The ledger contains a record of every action, and the smart contract may finally determine the amount of all transactions. The hospital bill needs to be paid once the patient can leave the facility, therefore this clause may be written into the smart contract.

X. ETHEREUM IN SMART CONTRACTS

On the Ethereum blockchain, there are present self- executing programmers referred to as smart contracts. They allow for the creation of decentralized applications (DApps) that can perform complex operations without the need for a central authority or intermediary. In Ethereum, smart contracts are written in the Solidity programming language and are stored on the blockchain as bytecode. Once deployed, they can be executed by anyone with access to the Ethereum network. Smart contracts in Ethereum can be used for a wide range of applications, including:

A. *Decentralized finance (DeFi)*

Smart contracts are used extensively in DeFi applications, such as lending and borrowing platforms, decentralized ex- changes (DEXs), and prediction markets.

B. Gaming

Smart contracts can be used to create decentralized games that run on the Ethereum network, allowing for provably fair gameplay and the creation of unique in-game assets.

C. Supply Chain Management:

Smart contracts can be used to track the movement of goodsand ensure that they are delivered to the correct destination, creating a transparent and tamper-proof supply chain.

D. Identity Management

Smart contracts can be used to create decentralized identity systems, allowing individuals to control their own identity datawithout relying on third-party providers.

E. Voting And Governance

Smart contracts can be used to create decentralized voting systems and governance mechanisms, allowing for transparentand fair decision-making processes. Overall, smart contractsin Ethereum are a powerful tool for creating decentralized applications that are secure, transparent, and self-executing.

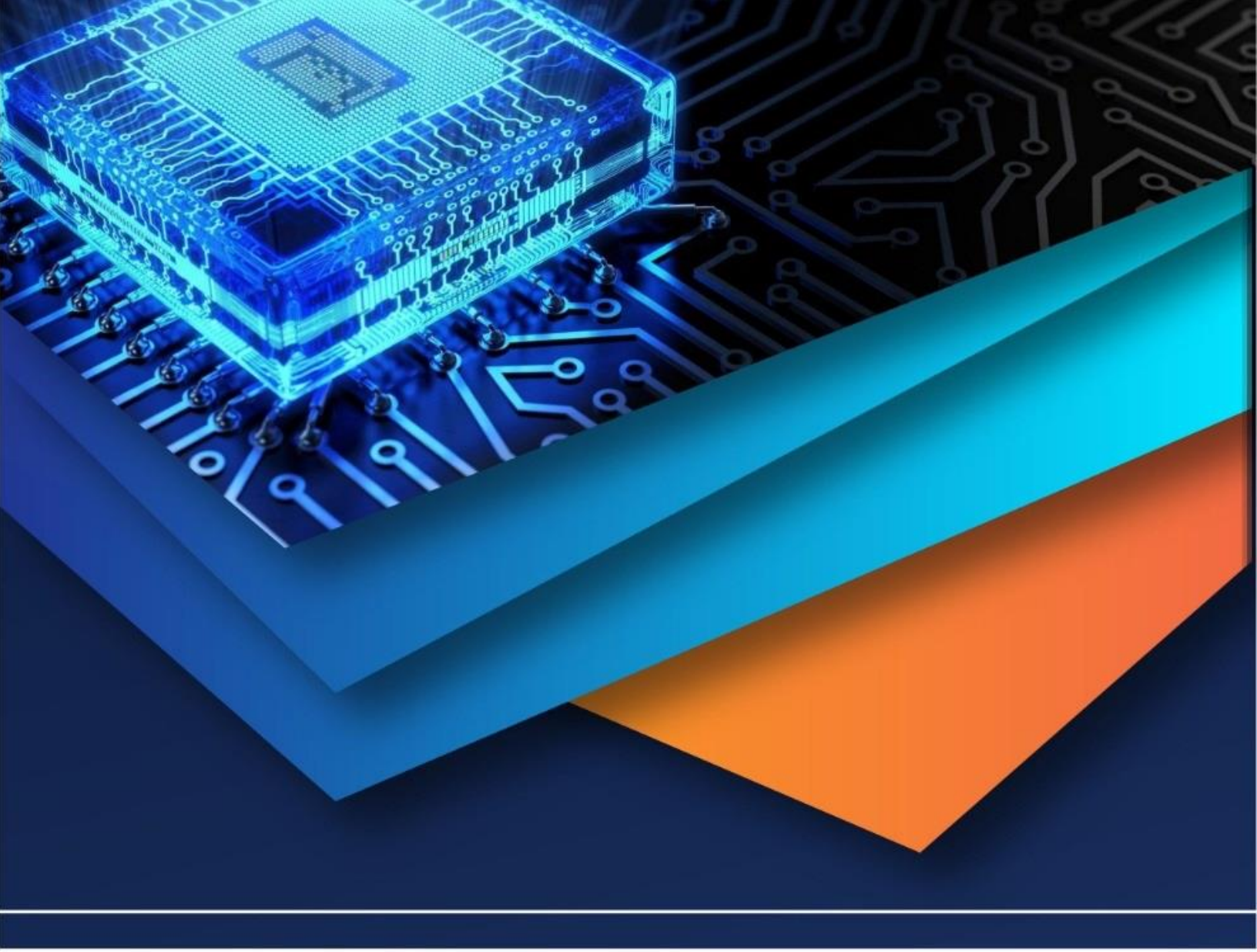
XI. CONCLUSION

The blockchain is lauded and approved for its peer-to-peer architecture and decentralized design. Yet, Bitcoin protects a lot of blockchain research. Blockchain, however, has several uses that go far beyond Bitcoin. The Bitcoin project is com- pletely non-governmental; it is a decentralized, autonomous initiative that is fundamentally unmanageable. An effective digital method of carrying out agreements between linked par- ties is through smart contracts. Using Solidity, a programming language with JavaScript-like syntax and semantics, these maybe created on the Ethereum Blockchain, which is a popular platform.

REFERENCES

[1] Zheng, Z., Xie, S.,Dai, H-N., Chen, X. and Wang, H. ”Blockchain challenges and opportunities: a survey”,Int. J. Web and Grid Services, Vol. 14, No. 4, pp.352–375, 2018.
[2] A. Afif Monrat , Olov Schele´n , Karl Andersson ,”A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities” , IEEE Access, Lulea. Uni. of Tech . Skelleftea . Sweden, Vol.7, pp.117134 - 117151, August 2019
[3] Roman Beck , ”Beyond Bitcoin: The Rise of Blockchain World” ,IEEE, IT.Uni.of.Copenhagen , Vol. 51, pp. 54 - 58, February 2018
[4] Joshua A. Kroll, Ian C. Davey, and Edward W. Felten, ”The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries” , Princeton University, New Jersey, pp21-21, June 11-12, 2013
[5] K. J. O’Dwyer and D. Malone, ”Bitcoin mining and its energy footprint”, Proc. 25th IET Irish Signals Syst. Conf., pp. 280-285, Jun. 2014.
[6] Y. Yuan and F.-Y. Wang, ”Blockchain and cryptocurrencies: Model techniques and applications”, IEEE Trans. Syst. Man Cybern. Syst., vol. 48, no. 9, pp. 1421-1428, Sep. 2018.
[7] Vujic˘ic´, D. Jagodic´ and S. Randic´, ”Blockchain technology bitcoin and Ethereum: A brief overview”, Proc. 17th Int. Symp. INFOTEH- JAHORINA (INFOTEH), pp. 1-6, Mar. 2018.
[8] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, et al., ”A survey on consensus mechanisms and mining strategy management in blockchain networks” in arXiv:1805.02707, 2018.
[9] M. Crosby, P. Pattanayak, S. Verma and V. Kalyanaraman, ”Blockchain technology: Beyond bitcoin”, Appl. Innov., vol. 2, no. 6, pp. 71, 2016.
[10] Tschorsch F, Scheuermann B. Bitcoin and beyond a technical survey on decentralized digital currencies. IEEE Communications Surveys Tutorials, 2016, 18(3): 2084–2123.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)