International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 SJIF 2023: 8.176 ISSN: 2582-3930

Cryptocurrency, A New Way of payment implemented using Blockchain Technology

G. Akshit Sreenidhi Institute of Science and Technology, Telangana, Hyderabad akshit.17102001@gmail.com
G. Ramesh sreenidhi Institute of Science and Technology, Telangana, Hyderabad rameshguduri1618@gmail.com
N. Praveen Sreenidhi Institute of Science and Technology, Telangana, Hyderabad nenavathpraveen3@gmail.com

Dr. Ch. Niranjan Kumar, Dept. of computer science Engineering, Sreenidhi Institute of Science and Technology, Telangana, Hyderabad India niranjankumarch@sreenidhi.edu.in

---

Abstract - The usage of blockchain technology, a somewhat new approach from the field of computer science technology, has increased the use of cryptocurrencies as a decentralized and safe way of exchange. Bitcoin was one of the first uses of blockchain technology and has since garnered a lot of attention. Together with Ethereum, which concentrates on blockchain implementation with smart contracts, they constitute the basis for modern cryptocurrency development. This project was developed on the technologies like solidity, Ethereum, and ReactJS. With this Application the Cryptocurrency transactions processed Quickly , cheaply, and securely. Concerns remain about volatility, a lack of supervision, and potential criminal activities. In spite of these concerns, cryptocurrency continues to advance as new technologies are created

Key Words: smart contracts; Ethereum; Blockchain; Cryptocurrency;

1. INTRODUCTION

Cryptocurrencies, new payment methods implemented using blockchain technology, are beginning to revolutionize the world of computing and information technology. Satoshi Nakamoto's 2008 paper on Bitcoin and blockchain technology introduced a revolutionary concept that has since become viable. Nakamoto's identity is debated, but there is no doubt that the technology he introduced has the potential to solve a variety of social problems, not just investment and commerce. This paper aims to provide an introduction to blockchain and cryptocurrencies, starting with a review of pre-Bitcoin decentralized digital money and diving into its core features with Ethereum. These two of his cryptocurrencies account for the majority of the cryptocurrency market capitalization. However, like any new technology, it comes with some limitations and issues that are also described in this document. To develop the website, we used React as the front end, Solidity as the back end, MetaMask as the crypto wallet, and Sepolia as Ethereum. We also used smart contracts and other technologies to create a comprehensive and efficient platform for cryptocurrency trading.

1.1 The early concepts and proposals for decentralized digital currencies that operate without intermediaries.

The digital currency has been an idea for a while, but only recently has it been successfully implemented. There have been many approaches to making digital currency work. One idea was presented by Chaum who suggested using public key cryptography to make electronic mail untraceable and anonymous. Law et al. proposed using public key cryptography for electronic cash with banks as central trust authorities. Dwork and Naor suggested a system to fight junk mail by requiring users to compute a hard pricing function, providing proof of work as a way to exchange digital commodities. Other authors proposed using computational power as an asset similar to precious metals or minted coins.

These methods, however, have drawbacks, such as the need for a reliable third party or their inability to resolve the issue of duplicate spending. Banks could prevent the parallel issuance of two transactions in the centralized solution. In a decentralized system like cryptocurrency, double-spending is a major problem. Users must keep the peer-to-peer network's state constant in the absence of a central authority in order to stop attackers from compromising the system with fake data.

The implementation of quorum systems was one response to these issues. Voting is meant to outweigh false information and hostile network actors, which are presumed to be true in these systems. The network can be controlled if the vast majority of nodes agree on the information. This strategy is vulnerable to a Sybil attack, in which adversarial nodes can mislead numerous peers and introduce fake information.

2. What is Cryptocurrency

A cryptocurrency is a form of digital or virtual money that controls how money is created and verifies money transfers using cryptography technology. Since it is decentralized and runs independently from a central bank, neither a government nor a financial institution has any authority over it. A public ledger is known as a blockchain that uses sophisticated algorithms to maintain the system's integrity stores cryptocurrency transactions.
There are several different cryptocurrencies, including Ethereum, Litecoin, Ripple, and Bitcoin, which is the most well-known.
Cryptocurrencies are frequently praised for their potential to revolutionize how we think about money and financial transactions by enabling quick and safe transactions. But it also has its own set of security, volatility, and regulatory issues.

2.1 Challenges Faced by Cryptocurrencies

Rules: Cryptocurrencies operate in a largely unregulated environment, which can make them vulnerable to fraud, money laundering, and terrorist financing. Regulatory bodies around the world are still working on classifying and regulating cryptocurrencies.

Safety: The blockchain technology underlying cryptocurrencies is secure, but the wallets and exchanges used to buy, sell, and store them are not. Cybersecurity threats, such as hacking and phishing attacks, threaten cryptocurrencies and pose a significant risk to

Volatility: The value of cryptocurrencies can be very volatile, and prices can fluctuate by double digits in a single day. This could make it difficult for businesses and consumers to accept cryptocurrencies as a trustworthy payment of sum.

Predict: Despite the growth of digitalized money, adoption is limited. Many still view cryptocurrencies as speculative investments rather than viable payment methods. Additionally, businesses and consumers may be reluctant to adopt technologies that are still relatively new and unfamiliar.

Power consumption: The cryptocurrency mining process consumes a lot of resources and power, raising concerns about the damage done to the environment.

Interoperability: There are hundreds of cryptocurrencies with blockchain and technical specifications. This can make it harder for cryptocurrencies to work together and make it difficult for users to transfer funds between different cryptocurrencies.

3. BITCOIN, ETHEREUM, AND BLOCKCHAIN TECHNOLOGY

3.1 The Key Elements of Bitcoin

In his well-known work, Satoshi Nakamoto offered a solution to the difficulties in using and implementing digital currencies, particularly the issue of double spending. Though uncertainty surrounds Nakamoto's identity, it is known that he actively contributed to the Bitcoin project up until 2010, when he stepped down and turned the initiative up to the community.

Nakamoto suggested a brand-new system that keeps track of the sequence in which transactions take place using a network of computers unity is necessary for growth. This prevents him from using the digital money twice, thus preventing fraud.

In this system, digital money (known as "electronic coins") is represented as a series of digital signatures. Each time someone spends money, they add a new signature to the chain.

Public keys are stored in software, hardware, or online service “wallets”. This allows people to keep their electronic coins safe and use them for transactions.

To generate an electronic currency, you need to make a transaction that includes the public key of the next recipient of the money as well as the digital signature of the transaction that came before it in the chain. As indicated in Fig. 1, the private key is used to sign the transaction, and the public key is used to verify the transaction.

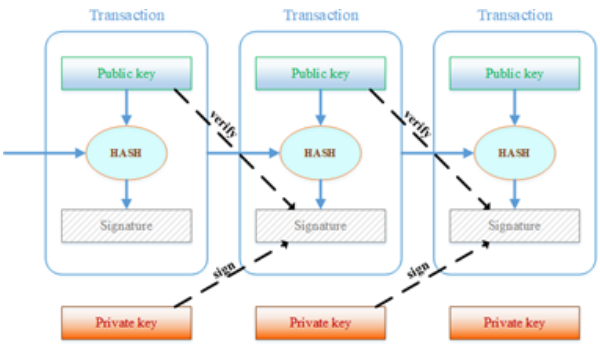

FIG-1: Blockchain-based transactional structure for Bitcoin and Ethereum

The Bitcoin ledger is a system that keeps track of who owns each Bitcoin. It's made up of two parts: the "state," which shows the current ownership status of all existing Bitcoins, and a "state transition function," which is a set of rules that describe how ownership of Bitcoins can change over time.

When someone wants to send bitcoins to someone else, they create a transaction describing the ownership transfer. This transaction is like a set of protocols directing how the Bitcoin network to include the transaction in the ledger. The state transition function then takes this transaction and applies it to the current state of the ledger to create a new state. The status will be changed to reflect the recipient's new ownership of the Bitcoins if the sender has sufficient Bitcoins to complete the transaction. The state transition function will provide an error and the transaction won't be performed if the sender does not have enough Bitcoins to complete the transaction.

In summary, a Bitcoin ledger is a system that uses a set of rules to track the ownership of each Bitcoin and ensures that only valid transactions following those rules change ownership.

3.2 The Bitcoin transactions

A hash value, as well as a list of inputs and outputs, are always recorded with each transaction in a blockchain network like the one used by Bitcoin. The results of an

To prevent double spending, 3 transactions can only be used as inputs once. An output is referred to as a spent transaction output (STXO) if it has already been used, and as an unspent transaction output (UTXO) if it hasn't. A transaction may have up to two outputs and several inputs. Smaller sums of coins can be transferred by combining multiple inputs, and the outputs can either be the amount sent to the recipient or the change returned to the sender. The distributed ledger that stores records of all network transactions and ownerships is kept up to date by the Bitcoin network. The ledger is kept on a copy by each peer-to-peer (P2P) node in the network. Users openly advertise their intention to send coins to another user, and the network then confirms the transaction's legitimacy. The double-spending problem occurs when a user tries to trick the network by sending the same coins in more than one transaction to various users. Additionally, a person can create many instances to carry out a Sybil assault and corroborate their initial intent. The network has defenses in place to stop these assaults and keep the blockchain's integrity.

3.3 Bitcoin Network: Proof-of-Work, Blockchain and Merkle Trees

In the Bitcoin network, to prevent fraudulent transactions, each node that verifies a transaction must provide proof of work by performing heavy computations. This ensures that the node is a valid member of the network. The system will stay consistent and legitimate transactions will be completed as long as the honest node has greater compute power than the attacker.
The hash of the preceding block, a nonce, and a series of transactions make up a block in the Bitcoin network. A timestamp server generates a hash of the block and publishes it, demonstrating that the information contained within was there at the time of hashing. The timestamp server additionally confirms that the block's timestamp is within two hours of the chain's prior block. As seen in Fig. 2, these blocks are then connected to form a chain, known as a blockchain, that can be traced back to any transaction in history. This characteristic of the blockchain makes it a safe and trustworthy means to record transactions.

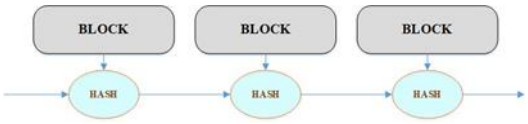

FIG- 2: The pattern of blockchain

The block's nonce is increased as part of the proof-of-work procedure until the block hash contains a value with the necessary number of leading zero bits. As soon as this is done, the computation is final, and any alteration of a block by a malicious attacker renders hashes for all upcoming blocks invalid. The network considers the longest chain to have the majority consensus to be the correct one. In a Merkle tree, transactions within a block are hashed. A leaf node's root is a hash of its offspring in a Merkle tree, which is a binary tree with numerous leaf nodes. Because discrepancies in the tree are reflected elsewhere in the chain, Merkle trees are crucial for long-term maintainability. To make room on the node for storing the blockchain, this is done. Simplified Payment Verification (SPV), which was first offered by Bitcoin, just needs a copy of the block headers from the longest chain and not the entire transaction record.

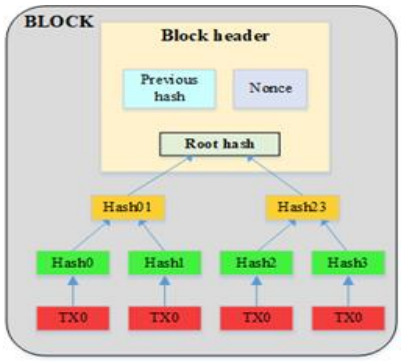

Fig -3: A Merkle tree is used to organize the hashed transactions in a Bitcoin block.

3.4 Bitcoin Network: proof-of-work, Blockchain, Mining and Consensus

The first transaction in a block, known as a Coinbase transaction in the Bitcoin network, creates a new coin that belongs to the block's author. As a result, nodes in the network can be compelled to approve transactions and distribute coins without the requirement for a centralised authority. This strategy encourages nodes to be honest because they have financial incentives to do so.

The goal of the Bitcoin network is to create blocks every 10 minutes or so. The complexity of creating new blocks gradually rises as the network's computer capacity grows over time in order to preserve a roughly constant block duration. This guarantees that the network functions effectively and efficiently and that new blocks are securely and promptly added to the blockchain.

New transactions on the Bitcoin network are immediately broadcast to all nodes. These transactions are gathered by each node, which then compiles them into blocks. The node then starts looking for the proof-of-work by locating a specified value, called a nonce, which, when hashed with the block data, yields a hash with a specific amount of leading zeros. It takes a lot of energy and computational resources to complete this operation because it is computationally demanding.

A node broadcasts the freshly formed block to the network once it has successfully found the nonce and produced the proof-of-work. The network's other nodes vouch that every transaction in the block is legitimate and has not yet been issued. The network recognises a block as valid if it passes this validation and adds it to the current blockchain by appending the previous block's hash to the header of the new block.
The way the decentralised and trustworthy Bitcoin network keeps track of all of its transactions is by routinely adding new blocks to the blockchain. The ledger's current status is acknowledged by all parties, preventing any one person or group from changing it to their own advantage.
The Bitcoin network encourages nodes to validate transactions in addition to rewarding block production. Mining is the process of approving transactions and adding new blocks to the blockchain. The amount of bitcoins that miners are given as payment for their work is fixed. This block reward was initially set at 50 Bitcoins per block but was to be gradually reduced to half that amount every 210,000 blocks. The initial 50 BTC were sent to the network using the "genesis block," the very first block on the blockchain. This reward-halving process continues until it is less than 1 Satoshi, the smallest Bitcoin unit equal to 10-8 BTC.
Multiple nodes may create and transmit the same block at nearly the same time in a distributed decentralized system like the Bitcoin network , but with distinct sets of transactions. This results in a condition known as a fork and an inconsistent network state. We currently have a number of chains coming from various blocks.
The network always starts with the longest chain in order to resolve this issue. The network gradually comes to an understanding of the blockchain's true course, and the forked chain is declared invalid. This consensus technique protects system integrity against hostile attackers and upholds network integrity.

3.5 Limitations of Bitcoin's Block Size on Transaction Throughput

Bitcoin has scalability issues due to its small block size of 1MB. Consequently, the maximum number of transactions that may be executed within a block is seven or fewer per second. In contrast, Visa's payment network can handle much higher transaction volumes, reaching 47,000 tps at peak times. Achieving this rate with Bitcoin would require massive amounts of data storage, leading to network centralization and going against the decentralized nature of blockchain technology. This highlights the need for a scalability solution to address Bitcoin's current block size limitations.

the notion of Bitcoin's soft and hard forks. The scalability issue with Bitcoin has remedies in the form of soft and hard forks. A change that is backward-compatible is a soft fork. Older software may accept newly produced blocks as genuine, which might lead to issues when network regulations change. In contrast, a hard fork is a software upgrade that introduces new rules into the network and prevents the previous version of the programme from being aware of the newly created blocks. Although they differ in terms of backward compatibility, both soft and hard forks strive to alter the network's protocol to address scalability difficulties

4. ETHEREUM

4.1 INTRODUCTION TO ETHEREUM AND ITS FEATURES

Vitalik Buterin developed the blockchain-based Ethereum platform in 2013. Buterin outlined a new blockchain in his article that fully supports Turing's entire programming language and fixes some of the drawbacks of Bitcoin's scripting language. This means that Ethereum is more adaptable and versatile than Bitcoin because it can allow loops and all other forms of calculations. Ethereum also offers transaction statuses. In other words, a blockchain can keep track of an application's or contract's present state. Contracts can be made by Smart He using this function. The terms and conditions between a buyer and a seller are directly written into lines of code that can execute themselves in a smart contract, which is a contract that is coded as software. Smart contracts make it possible to build decentralized applications on top of the Ethereum blockchain, enabling the creation of a wide range of applications beyond simple financial transactions.

Through the use of Ethereum, a blockchain platform, smart contracts may be made. In essence, a smart contract is a self-executing computer program that has the ability to automate specific actions or procedures. These smart contracts can be built using Ethereum's built-in programming language. It is Turing complete and can support any kind of computation that can be represented by an algorithm. This allows anyone to create their own custom rules for ownership, transaction formats, state transition functions, etc. The Ethereum Virtual Machine (EVM) is a decentralized Turing-complete virtual machine that runs on the Ethereum network, where smart contracts can be executed.. Smart contract execution is triggered by specific events and conditions defined in the contract and, once executed, is stored persistently on the Ethereum blockchain to ensure immutability and transparency.

The GHOST protocol (Greedy Heaviest Observed Subtree) is a modification of old traditional blockchain consensus protocol used by Ethereum. This mod aims to address the stale block problem in the network. Old blocks, also known as orphan blocks, are valid blocks that are not included in the longest chain because they were not discovered or propagated quickly enough.

If one mining pool has more overall processing power than another, then stale block issues can occur. This causes more blocks to be served from the initial pool, creating centralization issues within the network. The GHOST protocol addresses this issue by including these old blocks in the longest chain calculation. That is, rather than simply ignoring residual blocks, the GHOST protocol takes them into account when computing the heaviest observed subtree.

By including old blocks in the calculation, the GHOST protocol makes it more difficult for groups of miners to monopolize the network and increase mining rewards at the expense of others. Instead, the protocol encourages miners to cooperate and contribute to the network by rewarding older blocks with a share of the mining reward.

Ethereum addresses the centralization problem by rewarding miners for producing older blocks. H. Blocks not included in the main blockchain. These rewards are distributed so that the Legacy Block receives her 87.5% of the reward, and that Legacy Block's nephew (the block that references the Legacy Block) obtains her leftover 12.6% from the prize. This allows hashers to maintain an incentive to contribute to the network even if their blocks are not part of the main chain.

Uncles are a specific type of legacy block that Ethereum uses to maintain decentralization. These are blocks that are not part of the main chain but contribute to the security of the entire network. Modifications to Ethereum's GHOST protocol include up to 7 generations of these uncles. This means that a block can go back up to 7 blocks to its ancestors or uncles. This allows more miners to participate and receive rewards for their contributions, further promoting the decentralization of the network.

4.2 The Ethereum State and Accounts: Understanding the World State and the Components of an Ethereum Account

The accounts that make up the Ethereum state have related state transitions and are denoted by 20-byte addresses. In Ethereum, there are two different kinds of accounts: externally owned accounts, which are managed by private keys, and contract accounts, which are managed by their contract code. Four fields make up an Ethereum account: storage root, contract code hash, nonce, and ether balance. Addresses and account states are mapped by the global state. The number of transactions sent from a certain address or the number of contracts created by an account are both represented by the once field in an Ethereum account. In order to stop double-spending attacks, it guarantees that each transaction can only be completed once.

Another element in an Ethereum account, the ether balance, shows how much ether the address has. The cryptocurrency utilized

in the Ethereum network is called ether, and it is used to carry out smart contracts and pay transaction fees.

4.3 Transactions in Ethereum: Types and Components

A transaction in Ethereum is a single cryptographically signed command. A transaction might cause an account creation or a message call. A signed data packet transmitted from an external account qualifies as a transaction. The recipient of the message (another account or contract), the sender's signature, the amount of Ether to transmit, an optional data field, and two values (START GAS and GAS PRICE) are all included in each transaction. Certain elements of STARTGAS represents the maximum number of computational steps that can be performed during a transaction, and GASPRICE represents the cost of each computational step. Together, these values determine the total cost of executing a transaction, paid in Ether. Optional data fields can be used to add additional information or instructions to the transaction.

The process of creating, signing, sending, and including a transaction in the network and transaction pool. The next block to be mined is then chosen by miners from the pool of transactions. A transaction is regarded as final and cannot be modified once it has been added to a block and the blockchain.

A sender's willingness to pay in ether per unit of gas in order to include a transaction in a block is known as GASPRICE. As they receive greater rewards for processing transactions, miners give higher GASPRICE transactions priority. Therefore, if the sender wants the transaction to be executed swiftly, she should choose her GASPRICE value wisely.. However, there is also a minimum GASPRICE that miners will accept, and if the sender sets a lower value, the transaction will be rejected. This allows miners to get fair

rewards for their work and prevents the network from being spammed with low-value transactions.
Executing transactions and altering the states of senders and receivers are the responsibilities of Ethereum's state transition facility. By examining the legitimacy of signatures and nonces, the procedure starts by confirming the accuracy of the transaction. The function determines the transaction fee as STARTGAS * GASPRICE subtracts it from the sender's account balance, and then raises the sender's nonce if the transaction is legitimate. The desired amount will be sent to the recipient if the sender has enough Ether to do so, and if the recipient does not already have an account, one will be created. The contract's code is run if the receiver account is a contract. The state transition function will fail if the sender does not have enough ether or if all of the gas is used up by running code and reversing all state modifications minus the miner charge.
Ethereum allows a contract to send a message to another contract on the network. This message is similar to a transaction, but instead of being created by an external account, it's created by a contract. The data that a receiver contract requires to run its code, as well as the recipient contract's address and the amount of Ether she should send, are all included in messages sent between contracts.
Similar to transactions, the receiver contract runs its code when a contract sends a message. The receiver contract executes code and updates the status as directed by the message. This enables complex interactions between contracts on the Ethereum network, enabling the creation of decentralized applications (dApps) and other innovative use cases.

4.4 The Structure of an Ethereum Blockchain

In the Ethereum blockchain, a block contains information such as block number, difficulty, nonce, etc., as well as a list of transactions and their latest status, and each transaction in the list references its previous status to create a new Used to create status. Application. This means that each block on the Ethereum blockchain is a snapshot of the state of the whole network at a particular moment in time in addition to being a record of a transaction. By constructing smart contracts that can communicate with the Ethereum blockchain and alter the network's state, it enables programmers to create decentralized apps (dApps) on the blockchain.. The ability to run code on the blockchain is what distinguishes Ethereum from other blockchain platforms like Bitcoin.
On the Ethereum blockchain, a block header is a data structure that holds crucial details about the block. It includes the parent block header's Keccak 256-bit hash, which is used to connect blocks on the blockchain. It also includes the recipient's address for the mining fee. The recipient of mining awards will be sent to this address.
The block header also includes hashes for transactions, state roots, and confirmation tries. These data structures maintain the state of the Ethereum blockchain as well as a catalogue of transactions and their supporting documents.
The block's difficulty level, which defines how challenging it is to obtain a valid block hash, and the block's current amount, which establishes the maximum amount of gas that can be used for transactions within the block, are additional significant pieces of information in the block header. a gas cap. The block header also includes some extra hashes for verification, a date, a nonce, and the total amount of gas consumed in the block transaction.
Application Specific Integrated Circuit mining refers to the use of specialized hardware devices designed specifically for mining specific cryptocurrencies. Bitcoin's proof-of-work algorithm, SHA-256, is optimized for ASIC mining.
In contrast, Ethereum's Ethash algorithm is designed to consume more memory, making it less suitable for ASIC mining. This was done to facilitate a more decentralized network as it would be more difficult and expensive for an individual to develop and maintain his ASIC mining hardware dedicated to his Ethash.
Ethash is a modification of the Dagger-Hashimoto algorithm that combines a hash function with a memory-intensive problem to create a hard-to-solve but easy-to-verify proof-of-work puzzle. This approach aims to make the mining process fairer and more accessible to a wider range of participants.
Nodes that operate on the Ethereum Virtual Machine (EVM) and carry out their commands make up the Ethereum network. Solidity or another programming language is used to create smart contracts, which are then converted into EVM bytecode and executed by nodes. One of the most widely used programming languages for building smart contracts on the Ethereum network is Solidity. The time required for block generation and uploading it to the blockchain is referred to as Ethereum block time.. About 15 seconds, but can reach 30 seconds. This is much faster than the Bitcoin blockchain, which has a block time of around 10 minutes.
To join the Ethereum network, users can use blockchain clients such as Geth, which can synchronize with the Ethereum blockchain. Using the Geth blockchain client with fast sync, the Ethereum blockchain's size was 47.43 GB on January 29th, 2018.

5. TECHNOLOGIES USED TO DEVELOP ETHEREUM TRANSACTIONS FINANCE APPLICATION

5.1 METAMASK

MetaMask is a browser extension that allows users to interact with decentralized applications (dApps) on the Ethereum blockchain. It is a digital wallet allowing users to store, manage and transfer Ether and other Ethereum-based tokens. Users can also manipulate Smart Her contracts, participate in initial coin offerings (ICOs), and access decentralized exchanges (DEXs) directly from their browser. MetaMask is available as a browser extension for Chrome, Firefox, Opera, and Brave browsers and is used by millions of

people around the world to interact with his Ethereum ecosystem. It is an essential tool for developers and users of decentralized applications as it provides an easy and secure way to access and use the Ethereum network.

5.2 SOLIDITY

Solidity is a programming language used to create smart contracts on the Ethereum blockchain platform. It is a high-level language with JavaScript-like syntax designed to create safe, transparent, and self-executing smart contracts. Smart contracts written in Solidity can be used for a variety of purposes, including creating digital assets such as cryptocurrencies, setting rules for crowdfunding campaigns, and implementing governance structures for decentralized organizations. Solidity is a key tool in the Ethereum ecosystem, used by developers to build decentralized applications and services on top of the blockchain.

5.3 SMART CONTRACTS

A self-executing digital program called a smart contract runs on the blockchain network. They are software applications created to automatically examine, enforce, and enforce terms and conditions. Without the need for human interaction, smart contracts function on programming-encoded rules and automatically enforce those rules. They are available to everyone on the network and cannot be altered or updated once they are placed on the blockchain. Typically, trusted, decentralized agreements between two or more parties without the need for a middleman or centralized management are created using smart contracts. It has the ability to completely transform sectors like finance, real estate, and supply chain management by offering a transparent, safe, and effective means to do business and reach agreements.

6. LITERATURE SURVEY

6.1 EXISTING SYSTEM

Before the advent of blockchain technology, financial transactions were manually recorded in offline ledgers or centralized systems. The process lacked transparency and there was no easy way to access the recorded data or verify its accuracy. Because these records were not published on the Internet, they were susceptible to falsification and their integrity was not guaranteed. In addition, the risk of data loss and hacking was high as the system was controlled by a central authority. As a result, system security was not guaranteed. The lack of transparency and open records made it difficult to trace the flow of funds and often made it difficult to hold financial institutions accountable for their actions. Existing systems were inadequate to provide the security, transparency, and integrity required for modern financial transactions.

6.2 PROPOSED SYSTEM

The proposed system for Ethereum blockchain technology involves creating a decentralized network of nodes working together to process and verify transactions on the blockchain. Transactions on the Ethereum blockchain are processed through smart contracts. The terms and conditions between a buyer and a seller are written directly into lines of code in a smart contract, which is a self-executing contract. These smart contracts are transparent, and anyone on the network may check to see if they were actually executed and verified. The system increases transparency and security because transactions are recorded in an open, public ledger and cannot be changed once completed. Moreover, the system is decentralized. This means it is more resilient to hacks and data loss as it is not controlled by a central authority. The Ethereum blockchain also allows the creation of custom tokens to represent assets such as assets, stocks, and art. These tokens can be traded on decentralized exchanges, increasing liquidity and allowing access to previously illiquid assets. Overall, the proposed system of Ethereum blockchain technology offers a more secure, transparent and efficient way of processing financial transactions compared to traditional centralized systems.

7. FUTURE SCOPE

Future applications for Ethereum, cryptocurrency, and blockchain are numerous. Decentralized finance already uses the Ethereum blockchain. supply chain management, identity verification, smart cities, gaming, healthcare, and even governance are all examples of (DeFi) applications. This technology has a broad future use, is constantly developing, and has the capability to revolutionize many sectors and create safer, more transparent, and effective systems. It will be interesting to see how other economic sectors adapt and incorporate this technology as it continues to advance and expand.

8. CONCLUSIONS

In conclusion, blockchain technology or Distributed Ledger Technology has transformed how data is managed, shared, and stored.. This has led to decentralized networks like Bitcoin and Ethereum that provide a secure, transparent, and immutable system for recording transactions.
Is the first and most well-known cryptocurrency that operates independently of centralized authorities as a medium of trade and a store of value. Blockchain provides a secure and transparent record of all Bitcoin transactions, allowing users to trust the system without the need for an intermediary. By offering a more adaptable and versatile blockchain that enables the production of new types of transactions, we have expanded the capabilities of Bitcoin. Blockchain provides a platform for programmers to create and use their own a distributed application capable of running sophisticated business processes and logic by itself.

By offering fresh and original answers to age-old problems, the combination of Blockchain, Bitcoin, and Ethereum has the ability to bring about a revolution in a variety of industries. As this technology continues to develop and grow, it will be fascinating to observe how different sectors of the economy will adopt and incorporate it.

9. REFERENCES

[1] M. Yo Blockchain technology, bitcoin, and Ethereum: A brief overview March 2018 DOI: 10.1109/INFOTEH.2018.8345547Conference: 2018 17th International Symposium INFOTEH-JAHORINA (INFOTECH)

[2] Pagliery, Jose (2014). Bitcoin: And the Future of Money.
Triumph Books. ISBN 978-1629370361. Archived from the original on 21 January 2018.

[3] Matteo D'Agnolo. "All you need to know about Bitcoin"
. timesofindia-economictimes. Archived from the original on 26 October 2015.

[4] Johnson, Steven (2018-01-16). "Beyond the Bitcoin Bubble (Published 2018)"
. The New York Times. ISSN 0362-433

[5] Schroeder, Stan (2 September 2020). "Crypto wallet MetaMask finally launches on iOS and Android, and it supports Apple Pay"

[6] EST, Adam Piore On 11/19/18 at 5:09 PM (2018-11-19). "How blockchain technology could help us take back our data from Facebook, Google and Amazon"
. Newsweek. Retrieved 2020-11-11.

[7] Popper, Nathaniel (2016-03-28). "Ethereum, a Virtual Currency, Enables Transactions That Rival Bitcoin's (Published 2016)"
The New York Times. ISSN 0362-4331
Archived from the original on 2016-07-24. Retrieved 2020-12-08.

[8] Leising, Matthew (2 September 2020). "MetaMask's Blockchain Mobile App Opens Doors For Next-Level Web"
. Bloomberg News. Retrieved 3 December 2020.

[9] Jaffe, Justin (29 March 2018). "How to keep your cryptocurrency safe"
. Cnet Money. CNET. Retrieved 2020-11-12.

[10] Schroeder, Stan (2021-03-17). "Crypto wallet MetaMask now lets you swap tokens on your phone"
. Mashable. Retrieved 2021-06-26.

[11] Cimpanu, Catalin. "Exclusive: Google removes 49 Chrome extensions caught stealing crypto-wallet keys"
. ZDNet. Retrieved 2020-11-11.
Varshney, Neer (2018-06-12). "Google should learn from Apple's cryptocurrency guidelines"
. Hard Fork | The Next Web. Retrieved 2020-11-11.

[12] Thomas Dickerson, Paul Gazzillo, Maurice Herlihy, and Eric Koskinen. Adding concurrency to smart contracts. In Proceedings of the ACM Symposium on Principles of Distributed Computing, page 303–312, New York, NY, USA, 2017. Association for Computing