Deployment of Modern Web 3.0 Application using Ethereum Blockchain

Veena M Naik
Faculty ISE Department, Sri Krishna Institute of Technology, B'lore -560090, India
Manoj SE [1], Rajesh Dattathri Bobade [2], Sowndarya T [3]

Abstract:

Creating a Modern Web 3.0 application on the Ethereum 2.0 blockchain network to make trade and business between identified and anonymous participants easier, sometimes without the need for a middleman. The proof-of-stake technology used in this initiative speeds up transactions and lowers gas costs. Additionally, it offers a highly programmable smart contract that automates execution and makes it possible to create new digital assets and financial instruments. Additionally, it gives peer-to-peer transactions access to a very secure network. It also seeks to offer a variety of functionalities, such as DeFi transactions and the development of Web 3.0 games.

I. Introduction

A blockchain is a decentralized system made up of various records combined into blocks. All of these blocks are linked together to form a blockchain. The data structure of a linked list is widely used here. One of the well-known applications of blockchain technology is cryptocurrencies like Bitcoin, Ether, etc. The blockchain is not controlled by a single entity, but is controlled or managed by a group of people using this blockchain.

For example, if a person wants to transfer money to another person, then there is a need to trust a third party like banks or financial institutions. However, with the use of blockchain, a person can directly transfer money to another person without the need of a third party. The drawback with a centralized entity is that they are singular in number, and all it requires is one person with administrative privileges in an organization to manipulate the data, intentionally or unintentionally. A block comprises of data that is to be stored hash of the previous block and hash of the current block. A hash is generated by the combination of all the data in block by using some hashing techniques. The hash signifies the state of the block. It is similar to a digital fingerprint, making the block more secure and tampering with it is almost impossible. In addition to hashing, blockchain technology uses the asymmetric key mechanism Encryption from an asymmetric key, each Users have a pair of keys, public and private keys. Private key must be kept in a safeplace by the author. Public keys can be used to process transactions. When performing a transaction/action on the blockchain, the sender's account uses the recipient's account's public key to encrypt the data.

II. Background Study (Literature)

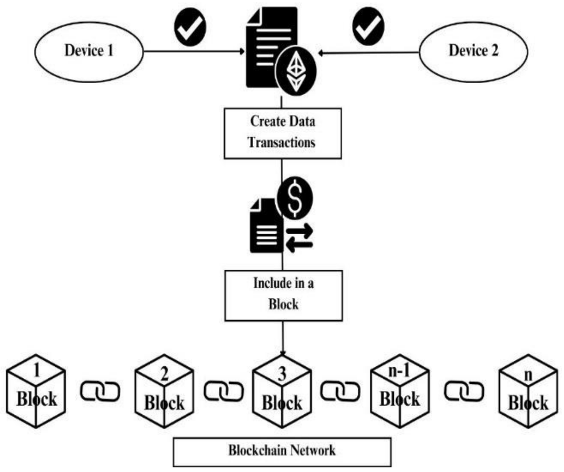
[1] Identifies block chain as a management innovation, astute contracts, plans of action, enterprising probabilities and obstacles, and as a block chain as an innovation that is universally beneficial.

[2] Discusses intelligent contracts, also known as smart contracts, which automate contractual clauses using triggers made in software. Intelligent contracts are a new technology that has arisen in the blockchain space. These previously established triggers can be customised, for instance, with certain dates or circumstances. [3] Provides the technical foundation for "Decentralised Finance (DeFi)"—a finance ecosystem that enables complex financial products and transactions in a trustless and borderless manner, such as lending/borrowing, derivatives (trading), and borderless stable assets. Smart contracts are defined as code-based agreements that are executed without human intervention. [4] The most popular blockchain platform nowadays is Ethereum. With developer limitations, Ethereum is Turing complete for smart contract coding. Researchers in this field have written numerous reviews with a variety of various points of view. 25 tools were covered, divided into two groups: formal verification for correctness and vulnerability detection for security assurance. [5] Focuses on a general review of blockchain technology's popularity as it becomes more and more significant. Nearly 1000 (33%) C-suite executives claim to be considering blockchain technology or to have already actively used it. The capabilities of the new technology are already known to researchers and developers.

III. Methodology

The Web App consists of the following methodology

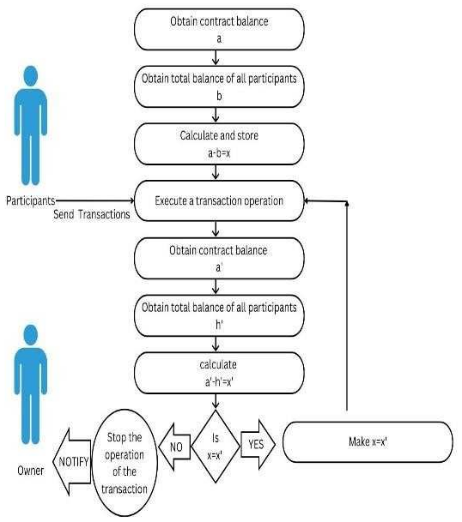
a) Architecture of the System



It shows the transaction steps involved. It involves two users interacting with a smart contract to meet the predetermined condition and get successfully executed. It involves steps from validating the device/user, to recording the transactions on the block chain network. Utilizing a Proof of Stake (PoS) consensus algorithm, the payment system with Ethereum 2.0 is decentralized and operates through a network of nodes that validate transactions. The facilitation of value transfers between parties is made possible by self-executing programs known as smart contracts. These smart contracts function through the Ethereum Virtual Machine (EVM), a computing platform residing on the Ethereum blockchain that enables the creation of decentralized applications (dApps).

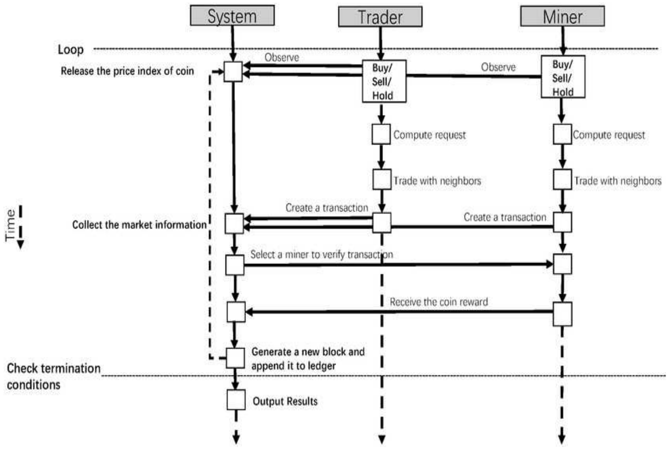
In Ethereum 2.0, payments occur in a block-and-validate style. The verifier nods increase the security and stop tampering. Sharding is also integrated to split the blockchain into bite-sized chunks so that it can easily grow and process. Ethereum 2.0's payment structure is efficient, secure, and scalable, making it an optimal choice. The Ethereum 2.0 payment system provides consumers with a number of advantages in addition to its technical capabilities, including faster transaction speeds, lower costs, and better security thanks to the use of cutting-edge cryptographic methods. Additionally, because the system is decentralised and no single entity has authority over it, it is immune to censorship and other types of intervention.

b) Data Flow of the System


Obtain contract balance a
Obtain total balance of all participants b
Calculate and store a-b=x
Participants
Send Transactions
Execute a transaction operation
Obtain contract balance a'
Obtain total balance of all participants h'
calculate a'-h'=x'
Owner
NOTIFY
Stop the operation of the transaction
NO
Is x=x'
YES
Make x=x'

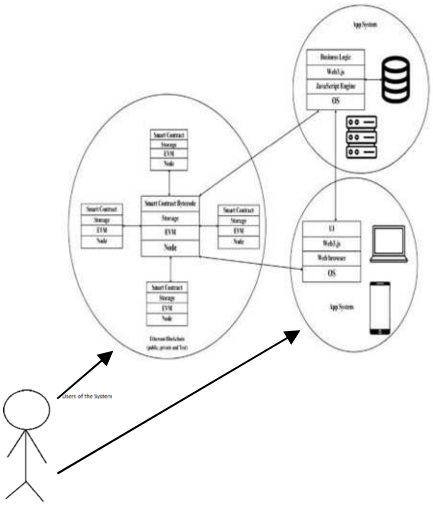
It shows the processing steps involved in the system. This includes the participants as well as the owners of the system and also the Smart Contract algorithm which runs in order to process the transaction. The distributed ledger technology that underpins the dataflow of the Ethereum 2.0 payment system makes use of a network of decentralised nodes to record and validate transactions. Data is first encrypted and broadcast to the network when a user starts a payment transaction, and numerous nodes then take in the data. Then, through a procedure called block creation, in which they combine the transaction data with other pending transactions into a block, the nodes compete to validate the transaction. The blockchain, a publicly available and unchangeable record of all transactions on the network, is where blocks are added after being created and verified by other network nodes. Through the introduction of sharding in Ethereum 2.0, this procedure is considerably more effective.

c) **Sequence Diagram of the System**



It represents the interactions between the system, Trader and the Miner. The interactions run in a loop and are timestamped interactions which run until a termination condition is met. The interactions and messages that takes place between the system components are shown in the sequence diagram of the Ethereum 2.0 payment system. The nodes, which interact with one another to maintain the blockchain and validate transactions, are the brains of the system. Data is encrypted and transferred to the network when a user starts a payment transaction, where it is received by several nodes. The nodes then interact with each other to validate the transaction using a Proof of Stake (PoS) based process. The blockchain, which is disseminated throughout the network, receives the transaction when it has been approved. The user and other network nodes are then broadcasted the transaction data for confirmation.

d) *Use case of the System*

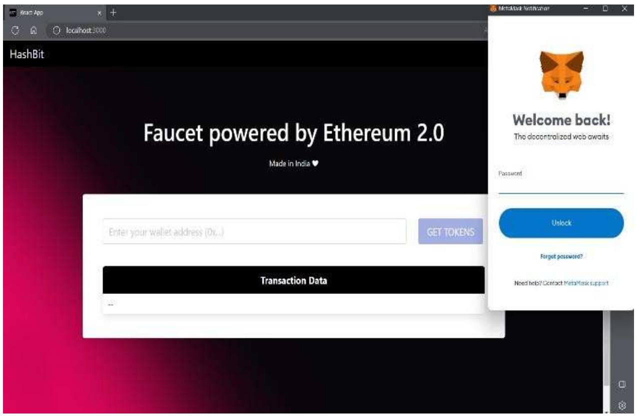


It describes what a user expects from a system. It represents a discrete task that involves external interaction with a system. It also tells us how the transactions run in conjunction with the Ethereum Blockchain, the servers and the app system.With p2p payments, users can send and receive money without the need of middlemen or conventional financial institutions. This technology is also ideally suited for facilitating transactions in decentralised exchanges (DEXs), where users can use different cryptocurrencies without the requirement of a central authority. The system also enables the development of new digital assets like security tokens and initial coin offers , through which corporations and individuals can raise money and issue their own unique tokens. Micropayments, remittances, and international transfers are the potential use cases.

IV Results & Discussion

The use of Ethereum 2.0's smart contracts for payments has shown promising results in terms of security, scalability, and cost-effectiveness. With its improved consensus algorithm and sharding technology, Ethereum 2.0 is capable of handling a larger number of transactions per second compared to its predecessor, making it a more viable option for mainstream adoption.

Furthermore, smart contracts have enabled the automation of payment processes, reducing the need for intermediaries and minimizing the risk of fraud and errors. This has resulted in faster and cheaper transactions, leading to cost savings for businesses and individuals alike.


React App

localhost:3000

HashBit

Faucet powered by Ethereum 2.0

Made in India ♥

Enter your wallet address (0x...)

GET TOKENS

Transaction Data

MetaMask Notification

Welcome back!

The decentralized web awaits

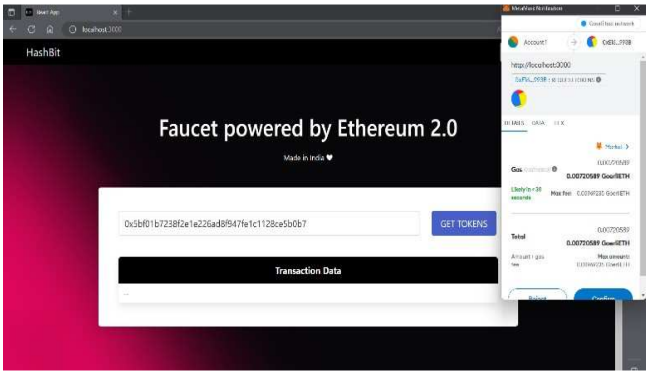
Password

Unlock

Forgot password?

Need help? Contact MetaMask support

Fig 1: The UI of the System and a metamask notification to greet the user.


React App

localhost:3000

HashBit

Faucet powered by Ethereum 2.0

Made in India ♥

0x5bf01b7238f2e1e226ad8f947fe1c1128ce5b0b7

GET TOKENS

Transaction Data

MetaMask Notification

Account1 → 0xE8...993B

http://localhost:3000

DETAILS DATA HEX

Gas 0.00720589 GoerliETH

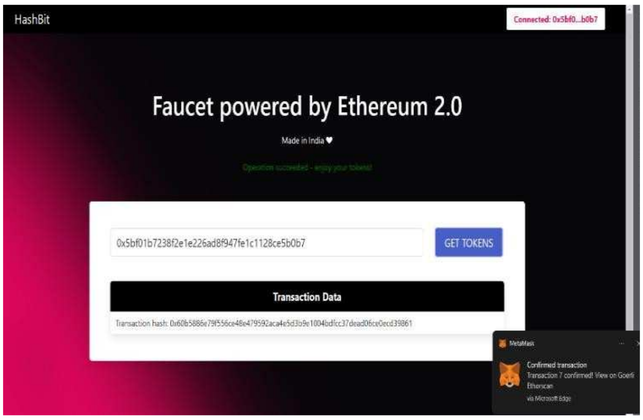
Likely in < 30 seconds Max fee: 0.00720589 GoerliETH

Total 0.00720589 GoerliETH

Amount + gas fee Max amount:

Reject Confirm

Fig 2: It shows the Address of the destination that is loaded in the system.



HashBit

Connected: 0x5bf0...b0b7

Faucet powered by Ethereum 2.0

Made in India ♥

Operation succeeded - enjoy your tokens!

0x5bf01b7238f2e1e226ad8f947fe1c1128ce5b0b7

GET TOKENS

Transaction Data

Transaction hash: 0x60b5886e79f556ce48e479592aca4e5d3b9e1004bdfcc37dead06ce0ecd39861

MetaMask

Confirmed transaction

Transaction 7 confirmed! View on Goerli Etherscan

via Microsoft Edge

Fig 3: Displays the completion of the transaction.

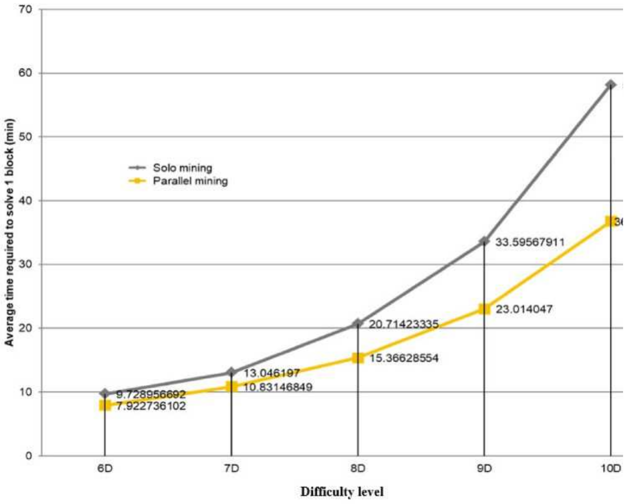


Fig: 4: Displays Average Time taken to solve one block

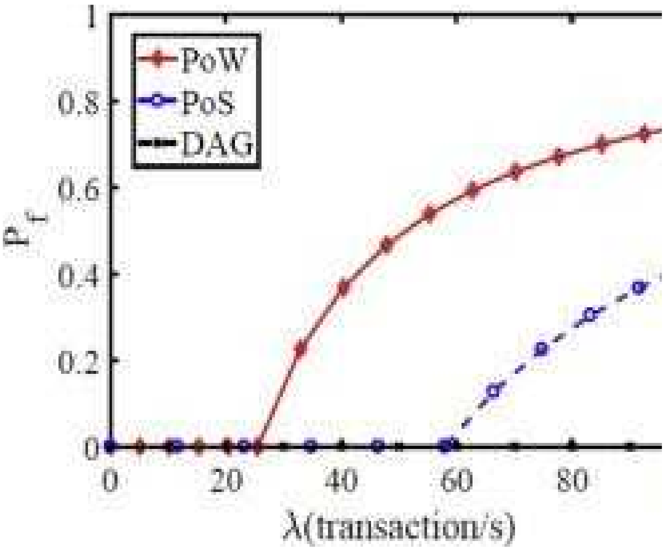


Fig 5: Comparison of performance between PoW and PoS

IV. Conclusion

In this paper, we discuss how the system supports a proof-of-stake blockchain network, which accelerates transaction speed and lowers gas costs. It also makes it easier to build a platform with robust encryption that ensures tamper resistance, immutability, and verifiability for a distributed and replicated ledger of events, transactions, and data produced by multiple IT processes. The system's ability to support perfect user transaction experiences without concern about hacks or transparency is also covered.

References

[1] Eva Andrea Meye et. al, “Decentralized Finance “A Systematic Literature Review and Decentralized Finance” Association for Information Systems AIS Electronic Library (AISeL) Year: 6-18-2022

[2] Satpal Singh Kushwaha et. al, “Ethereum Smart Contract Analysis Tools :A Systematic Review”. Volume10 IEEE 2022.

[3] David Nadler Prata et. al “A Literature Review about Smart Contracts Technology” Journal Home Page Available: https://ijaers.com/JournalDOI:10.22161/ijaers ISSN: 2349-6495(P) | 2456-1908(O) 2021.

[4] Siddharth Rajput et. al,“Blockchain Technology and Cryptocurrencies" IEEE (978-1- 5386-9346-9/19) 2021.

[5] Fran Casinoa et. al, “A systematic literature review of blockchain- based applications: Current status, classification and open issues. 22 November 2018.

[6] Jatinder Singh and Johan David Michels. “Blockchain as a Service (BAAS) : Providers and Trust. IEEE Symposium on Security and Primary Workshop: 2018

[7] Nikita Sanghi, Rupali Bhatnagar, Gaganjot Kaur and Vinay Jain. “Blockcloud with Cloud Computing.” International Conference on Advances in Computing Communication Control and Networking: 2018.