Journal of Computer Science and Engineering Research (JCSER)
Volume 2, Issue 2, Date: 31 - December – 2025
ISSN: 2978-4328, DOI: 10.64820/AEPJCSER.22.8.15.122025

Decentralized and Adaptive Blockchain Based Offline Payment System Using Hardhat and Ethereum

Mrs. G. Sharmila [1, *], K. Neha [2], M. Kaviya [3], M. Juhe Sherin [4], Justin Ronaldo [5]
[1, 2, 3, 4,5] Department of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Puducherry, India.
Email: [1] sharmilacse@mvit.edu.in, [2] guruneha1221@gmail.com, [3] mkaviyacsebtech@gmail.com, [4] mjsherin19@gmail.com, [5] justinronaldo595@gmail.com
*Corresponding Author

***Abstract*—Blockchain technology is a cutting-edge advancement in information technology. Bitcoin, as one of its initial uses, has attracted considerable attention as a cryptocurrency. Alongside Ethereum, which emphasizes blockchain-driven smart contracts, these technologies lie at the heart of modern cryptocurrency innovation. Off-chain transactions offer a scalable solution for blockchain networks, reducing congestion, lowering transaction fees, and improving processing efficiency without compromising decentralization. However, existing off-chain solutions often face security and flexibility challenges, particularly in environments with high latency and unstable connectivity. The proposed system leverages the Hardhat blockchain framework with Ethereum to enable secure peer-to-peer transactions from user wallets, ensuring seamless fund transfers even in offline conditions. Additionally, it integrates blockchain-based email functionality, allowing encrypted messages to be sent securely over a decentralized network, thereby enhancing data privacy and security. To further strengthen data integrity, the system incorporates the Inter Planetary File System (IPFS) for decentralized file storage, reducing reliance on centralized servers and minimizing data loss risks. By combining off-chain transactions, blockchain-based email, and IPFS storage, the system enhances efficiency, security, and reliability, offering a robust decentralized solution for financial transactions and secure communication. The data is distributed across all cryptocurrency users within the network. This ensures that when a user initiates a transaction, data mining processes are conducted.**

Keywords—Off-chain Transactions; Blockchain Scalability; Hardhat Blockchain; Ethereum Cryptocurrency; Decentralized Network; IPFS Storage; Encrypted Messaging; Peer-to-Peer Transactions.

I. INTRODUCTION

Cryptocurrency is a blockchain-based technology commonly associated with Bitcoin. Unlike traditional money, Bitcoin does not have a physical form; instead, it exists as a block of data secured by a hash for validation. This [1] data is distributed across all cryptocurrency users within the network, enabling data mining processes whenever a transaction is made. While [3] cryptocurrencies offer several advantages, they also present challenges when used as a form of currency. Legally, there is still no regulation governing the circulation of cryptocurrencies. In Indonesia, cryptocurrency is a relatively new phenomenon. With the rapid technological advancements in the era of Industry 4.0, it is expected that digital money will soon replace physical currency, offering numerous conveniences.[2] Blockchain and cryptocurrencies like Bitcoin, Ethereum, and Litecoin are innovative financial technologies that are rapidly transforming the finance sector and reshaping the global economy.

Offline payments are essential for enabling transactions in environments with limited or no internet connectivity.[4]Off-chain transactions play a key role in improving scalability by reducing congestion on the main blockchain, allowing for faster and more efficient processing.[10]Payment channels, a widely used layer-2 solution, help address scalability concerns but come with limitations such as locked funds and the need for pre-established channels, which reduce flexibility and introduce potential security risks. To enhance blockchain adoption in offline-first applications, it is necessary to overcome these constraints and ensure robust security.

Our proposed solution introduces a comprehensive threat model to address security challenges in offline payment systems. By leveraging universal composability (UC) under synchronous conditions, we ensure resilience against adversarial attacks, making transactions more secure and scalable. This approach provides a more flexible and efficient framework for offline transactions without compromising security. Additionally, our methodology includes systematic provisioning and analysis of the source code to ensure integrity, reliability, and adherence to security principles.[5]The protocol's performance is evaluated based on key metrics such as transaction speed, scalability, and resilience under adverse network conditions. By balancing security, scalability, and flexibility, our solution facilitates the broader adoption of blockchain-based offline payments for real-world applications.

A. Hardhat

Hardhat is a powerful Ethereum development framework that streamlines smart contract creation, testing, and deployment. It features the Hardhat Network, a local blockchain for gas-free transaction simulation, enabling rapid prototyping.[6] A

Received: 22-8-2025
Revised: 31-12-2025
Published: 31-12-2025

key advantage is mainnet forking, allowing interaction with real-world blockchain data in a controlled environment. Hardhat integrates seamlessly with Ethers.js, Web3.js, and Solidity, supporting extensive plugin customization for enhanced workflow automation.

Its task automation system simplifies repetitive development processes, increasing efficiency.[11]Hardhat also offers comprehensive debugging tools, including detailed stack traces and error messages, making troubleshooting easier. The framework enhances security by enabling rigorous testing and vulnerability assessments, ensuring smart contracts are robust before deployment. With its automation, flexibility, and security features, Hardhat is an essential tool for building scalable and secure decentralized applications (DApps), making it a preferred choice for Ethereum developers.

B. The Interplanetary File System(IPFS)

The Inter Planetary File System(IPFS)is a decentralized, peer-to-peer protocol designed for secure, efficient file storage and sharing. Unlike traditional servers,[12]IPFS uses a content-addressable system, identifying files by cryptographic hash to ensure data integrity, immutability, and redundancy. It breaks files into chunks and distributes them across multiple nodes, enabling faster retrieval, reducing bandwidth costs, and enhancing resilience against data loss and censorship.

IPFS supports versioning, making it easy to track and update stored files. It integrates seamlessly with blockchain and Web3 ecosystems, powering NFT storage, smart contracts, decentralized applications (DApps), and distributed web hosting. By eliminating reliance on centralized cloud providers, IPFS enhances security, transparency, and efficiency, making it a cornerstone of the decentralized internet. Additionally, its interoperability with protocols like Filecoin enables incentivized, permanent storage solutions, ensuring long-term data availability.

II. LITERATURE SURVEY

For illustration, Mr. Prasanna Kumar M J, Poorvika D A [6] proposed real. This research addresses scalability and security challenges in off-chain blockchain transactions, particularly in unreliable network conditions. Our proposed offline payment protocol leverages loosely synchronized clocks and channels with known latency bounds to enable secure transactions between offline parties. By integrating on-chain smart contracts with offline wallet interactions, it ensures reliability despite intermittent connectivity. Additionally, Trusted Execution Environments (TEEs) enhance security and platform flexibility. Empirical evaluations using Intel SGX demonstrate high efficiency, advanced security, and resilience against real-world attacks. The protocol operates within a universally composable framework under synchronous conditions, ensuring robust protection. This approach significantly enhances blockchain-based offline payments, offering a secure and adaptable solution for decentralized transactions in environments with limited connectivity. For illustration, Nikolay Ivanov and Qiben Yan[7]proposed a real. This research addresses scalability and security challenges in off-chain blockchain transactions, particularly in unreliable network conditions. Our proposed offline payment protocol leverages loosely synchronized clocks and channels with known latency bounds to enable secure transactions between offline parties. By integrating on-chain smart contracts with offline wallet interactions, it ensures reliability despite intermittent connectivity. Additionally, Trusted Execution Environments(TEEs)enhance security and platform flexibility. Empirical evaluations using Intel SGX demonstrate high efficiency, advanced security, and resilience against real-world attacks. The protocol operates within a universally composable framework under synchronous conditions, ensuring robust protection. This approach significantly enhances blockchain-based offline payments, offering a secure and adaptable solution for decentralized transactions in environments with limited connectivity. For illustration, Raed Saeed Rasheed, Khalil Hamdi Ateyeh Al-Shqeerat, and Ahmed Salah Ghorab [8] proposed a real. This research addresses scalability and security challenges in off-chain blockchain transactions, particularly in unreliable network conditions. Our proposed offline payment protocol leverages loosely synchronized clocks and channels with known latency bounds to enable secure transactions between offline parties. By integrating on-chain smart contracts with offline wallet interactions, it ensures reliability despite intermittent connectivity. Additionally, Trusted Execution Environments (TEEs) enhance security and platform flexibility.

Empirical evaluations using Intel SGX demonstrate high efficiency, advanced security, and resilience against real-world attacks. The protocol operates within a universally composable framework under synchronous conditions, ensuring robust protection. This approach significantly enhances blockchain-based offline payments, offering a secure and adaptable solution for decentralized transactions in environments with limited connectivity. For illustration, Ikechi Saviour Igboanusi, Kevin Putra Dirgantoro, Jae-Min Lee[9]proposed a real-Pure Wallet(PW) is an innovative electronic payment system that enables offline blockchain transactions. It operates in three steps: first, cryptocurrency is converted into a token via a token manager while online. Next, offline transactions occur using Near Field Communication (NFC), allowing encrypted token exchange between mobile devices. Finally, once reconnected to the Internet, the receiver submits the token to the token manager to convert it back into cryptocurrency. By leveraging smart contracts, PW ensures secure and decentralized transactions, making financial exchanges possible in areas with poor connectivity. While the system successfully facilitates offline payments, challenges remain, such as optimizing token management, ensuring scalability, and securing offline communication channels. Further research is required to enhance efficiency, security, and real-world adaptability.PW demonstrates the feasibility of blockchain-based offline payments, providing a practical solution for financial transactions in network-limited environments. For illustration, Joshua Lind, Oded Naor, Ittay Eyal [10] proposed a real, Teechain is a next-generation layer-two payment network that enhances blockchain scalability by enabling asynchronous off-chain transactions. Traditional blockchains like Bitcoin and Ethereum suffer from inefficiencies due to global consensus requirements, slowing

down transaction processing. Off-chain solutions reduce this burden by settling only final balances on-chain, but they still depend on periodic blockchain access,creating security risks.Malicious actors can exploit these delays to manipulate funds.Teechain addresses this issue by eliminating the need for synchronized blockchain access,making transactions faster and more secure.It achieves this through treasuries protected by Trusted Execution Environments(TEEs),which securely manage collateral funds.Additionally,committee chains with threshold secret sharing distribute trust,preventing reliance on a single TEE.This unique design allows Teechain to process over 1 million Bitcoin transactions per second in a 30-machine deployment,outperforming existing systems like the Lightning Network.It offers a scalable,secure,and decentralized solution for off-chain payments.

III. METHODOLOGY

The proposed system leverages the Hardhat blockchain framework with Ethereum to facilitate [13] secure peer-to-peer transactions directly from user wallets, ensuring seamless fund transfers even in offline conditions. By integrating off-chain transactions, it minimizes network congestion and transaction costs while maintaining security and decentralization. This approach allows users to conduct financial transactions efficiently without continuous Internet connectivity, making it ideal for environments with limited network access. Additionally, the system incorporates [14]blockchain-based email functionality, enabling encrypted message exchanges over a decentralized network. This ensures that communication remains private and tamper-proof, enhancing data security and preventing unauthorized access. To further strengthen data integrity, the proposed system integrates the [12] Inter Planetary File System(IPFS)for decentralized file storage, reducing reliance on centralized servers and mitigating risks of data loss or manipulation. IPFS ensures that stored data is distributed across multiple nodes, improving availability and resilience against failures. By combining off-chain transactions, blockchain-based email, and decentralized storage, the system enhances efficiency, security, and reliability. This holistic approach provides a robust decentralized solution for financial transactions and secure communication, catering to users who require privacy, integrity, and uninterrupted access to digital services in both online and offline scenarios.

A. User Wallet and Transaction Management

This module enables [13]secure peer-to-peer fund transfers using the Hardhat blockchain framework with Ethereum. Users can send and receive payments directly from their wallets, ensuring seamless offline transactions.[15] Cryptographic signing prevents unauthorized modifications, while key management and encryption protect private keys. Supporting multiple cryptocurrencies and smart contracts, it offers flexible financial interactions. Transactions are logged on-chain once online, ensuring transparency and traceability. Secure authentication mechanisms enhance fund security. With an intuitive interface, users can track balances, transaction history, and pending transfers. This decentralized system improves financial autonomy, security, and accessibility, especially in network-restricted environments.

B. Off-Chain Transaction Processing

This module reduces blockchain congestion and transaction fees by handling off-chain payments, enabling faster, scalable fund transfers.[13]Transactions are cryptographically signed for security and later recorded on-chain.It uses state channels or sidechains,maintaining decentralization while improving efficiency,especially for microtransactions.Off-chain transactions remain tamper-proof and verifiable,synchronizing with the blockchain ledger when online.This approach enhances scalability,lowers gas fees,and improves transaction speed,making decentralized finance more accessible and practical for real-world use,addressing delays and high costs while ensuring consistency and reliability.

C. Blockchain-Based Email System

This module enables encrypted messaging over a [16]decentralized blockchain network, ensuring privacy and security. Unlike traditional email systems, it eliminates reliance on centralized servers, preventing unauthorized access and data tampering. End-to-end encryption ensures only intended recipients can read messages, while smart contracts verify sender authenticity and block spam or phishing attempts. Blockchain immutability prevents message alteration, making it ideal for confidential industries like finance and healthcare. Removing [14] third-party email providers reduces risks of server failures and data breaches. This decentralized email system offers a secure, censorship-resistant, and privacy-focused communication network for users.

D. IPFS Integration for Decentralized Storage

This module integrates [12]Inter Planetary File System(IPFS)for decentralized file storage, ensuring data integrity, availability, and security without reliance on centralized servers. Unlike traditional storage, IPFS distributes data across nodes, making it resilient to failures, censorship ,and cyberattacks. Files receive unique cryptographic hashes, ensuring immutability and verification. Users access files via content-addressable storage, reducing URL dependency. Privacy is enhanced by eliminating centralized control, protecting sensitive documents and digital assets [13] IPFS optimizes bandwidth with peer-to-peer sharing, providing a scalable, cost-effective solution for financial records, encrypted messages, and long-term secure storage against unauthorized changes or deletions

E. Network Synchronization and Validation

This module ensures that offline transactions and blockchain-based emails remain synchronized and validated once users regain network access. When transactions occur offline,[18]cryptographically signed proofs are generated and stored locally on user devices. Upon reconnection, the system verifies these records against the blockchain using the Hardhat framework, ensuring data integrity and preventing double-spending. Hardhat provides a flexible testing environment that allows for thorough smart contract validation and execution before transactions are finalized on the Ethereum blockchain. The system also uses time-stamping and cryptographic hashes to detect any tampering or inconsistencies. Hardhat facilitates smart contract

automation and error handling, ensuring seamless synchronization. By leveraging[11]Hardhat's robust development and testing tools, this module enhances transaction security,automates verification,and ensures reliable offline-to-online transitions in decentralized applications.

F. User Interface and Access Control

This module offers a seamless interface for managing financial transactions,blockchain-based email,and decentralized file storage.Users can access wallets,transaction history,encrypted messages,and IPFS files securely.[19]Role-based access control(RBAC)prevents unauthorized actions,ensuring only verified users perform sensitive tasks.Designed for mobile and web,it supports multi-language and assistive technologies for accessibility.[20]Biometric authentication(fingerprint,facial recognition)enhances security,while real-time notifications update users on transactions and threats.Prioritizing usability,security,and accessibility,this module simplifies decentralized system navigation while ensuring strong data protection.

G. Architecture diagram

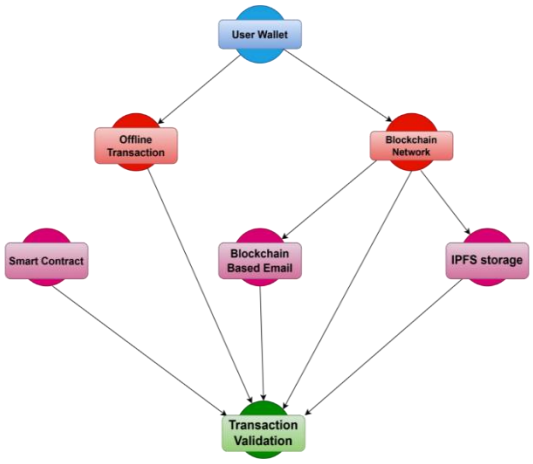


Fig 1:Architecture Diagram

The architecture of the proposed system, above figure (1) consists of three core components: [12]decentralized transactions, blockchain-based email, and IPFS-based file storage. Users initiate transactions and encrypted communications using their wallets, even in offline conditions. These offline transactions generate cryptographically signed proofs, which are stored locally until network connectivity is restored. Once reconnected, the system synchronizes these transactions with the blockchain, ensuring data integrity and preventing double-spending. The [14] blockchain-based email feature enables users to send encrypted messages over a decentralized network, ensuring secure communication without relying on centralized servers. Additionally, the system integrates the Inter Planetary File System (IPFS) for decentralized file storage, reducing the risk of data loss and ensuring high availability. Smart contracts automate validation and synchronization processes, enhancing security and efficiency. This architecture provides a seamless, secure, and decentralized approach to financial transactions and communication, making it highly reliable for users in both online and offline environments.

IV. PERFORMANCE ANALYSIS

Analysis of performance is essential for determining the efficiency of this analysis covers a number of important topics.Hardhat outperforms Proof of Work(PoW)in energy efficiency and transaction speed,as it eliminates mining and enables rapid smart contract execution.While [21]PoW offers stronger security through decentralized mining,Hardhat is optimized for testing rather than live deployment.In scalability,[11]Hardhat handles large-scale deployments efficiently,whereas PoW struggles with network congestion.Overall,Hardhat excels in efficiency and speed,while PoW remains superior in security.

A. Gas Calculation Formula

Gas calculation for offline payments in Ethereum involves pre-determining and reserving the required [22]gas to ensure seamless transaction execution once network connectivity is restored.In an offline payment system,the sender generates a signed transaction containing the recipient's address,amount,and a pre-estimated gas fee.This transaction remains stored locally on the device until it reconnects to the network. Once online, the transaction is broadcast to the Ethereum network, where miners validate it based on the Gas Used×Gas Price formula.

$$\text{Total Gas Cost} = \sum_{i=1}^{n} (\text{Gas Used}_i \times \text{Gas Price}) \quad (1)$$

Where,
Gas Used is the gas consumed by operation I,
Gas Price is the cost per unit of gas (Gwei).
The above equation (1) represents the sum of individual gas costs incurred at each step of the transaction execution. Here, Gas Used, Gas Used_2,..., Gas Used_n correspond to the amount of gas consumed by different computational operations within a smart contract or transaction, while Gas Price is the fee per unit of gas, typically denominated in Gwei.

B. Solidity Compiler(solc)

Offline payment systems in blockchain enable secure transactions without requiring continuous internet connectivity. In such a system, [23] users can sign transactions locally using their private keys, generating cryptographic proofs that ensure authenticity. These signed transactions are temporarily stored on the user's device and are later synchronized with the blockchain once network access is restored. This prevents double-spending by ensuring that transactions are validated and recorded in the correct sequence upon reconnection.

Optimized Bytecode Size = Original Bytecode Size (2)

Optimization Factor

Where,
Optimization Factor is a compiler setting that reduces redundant instructions.
Here, the above equation (2) represents the Original Bytecode Size, which represents a contract's pre-optimization size, while the Optimization Factor measures compiler efficiency in reducing it. A higher optimization factor results in smaller bytecode, lowering deployment costs and improving execution efficiency. Since gas fees are based on storage and execution, minimizing bytecode size is essential. Solidity's solc compiler optimizes contracts by removing redundant code, inlining functions, and restructuring logic, reducing gas consumption. Optimized bytecode enhances performance, lowers fees, and improves scalability while maintaining security. For offline payments, digital signatures and cryptographic hashing prevent tampering, and smart contracts verify transactions upon reconnection.

C. Plugins:

$$Gas\ Efficinecy = \frac{Gas\ Used}{Total\ Operation} \quad (3)$$

Plugins in Hardhat extend its functionality by integrating additional tools and features for Ethereum smart contract development. They allow developers to customize workflows, automate tasks, and enhance debugging, testing, and deployment processes. Hardhat offers built-in plugins, such as hardhat-toolbox, which provides essential utilities for testing and contract interaction.

Total Operation
The above equation (3) represents Gas Efficiency in Smart Contracts Gas efficiency measures the effectiveness of [24]smart contract execution by evaluating gas consumption per operation. Lower gas usage indicates better efficiency, reducing transaction costs. Factors like contract complexity, executed operations, and Solidity function optimization impact gas efficiency. Techniques such as loop unrolling, minimizing storage reads/writes, and using efficient data structures enhance performance. Monitoring gas efficiency is crucial for cost-effective and scalable DApps, ensuring low user fees while maintaining high performance. For large-scale applications, optimizing gas usage leads to significant cost savings and improved blockchain efficiency.

D. Testing and Debugging

Testing and debugging an offline payment system in a blockchain environment requires ensuring that [14] transactions remain secure, verifiable, and correctly processed once network connectivity is restored. The process involves simulating various offline scenarios, such as delayed transactions, double-spending attempts, and cryptographic proof validation. Smart contracts must be rigorously tested using frameworks like Hardhat to verify that locally signed transactions are correctly stored and later validated on-chain.[25]Debugging involves checking for errors in cryptographic signatures, transaction validation logic, and data synchronization when transitioning from offline to online modes. Tools like Hardhat Network provide in-memory blockchain environments for simulating transactions without real network costs.

E. Transaction Verification

Equation (4) below represents the formula used to ensure the integrity and security of offline transactions. It generates a unique [5] cryptographic hash that acts as a digital fingerprint for each transaction. The sender and receiver addresses confirm the parties involved, while the amount ensures the correct value transfer.

The timestamp helps in maintaining transaction order, preventing replay attacks. The signature, created using the sender's private key, guarantees authenticity and prevents unauthorized modifications. When the offline transaction is later synchronized with the blockchain, the system verifies that the [12] hash remains unchanged, ensuring that the data was not altered or tampered with. This approach strengthens transaction security, prevents double-spending, and maintains trust in decentralized payment systems even in offline conditions.

F. Signature Verification(ECDSA)

Elliptic Curve Digital Signature Algorithm (ECDSA) [26] is used to verify the authenticity of a transaction by ensuring that it was signed by the rightful sender. The verification process involves checking that the sender's digital signature matches their public key. The formula for ECDSA verification is:

Where:
H(T)=Hash of the Transaction
(Sender Address+ReceiverAddress+Amount+TimeStamp +Signature) (4)
d_ A=Sender's private key
r, S=signature components generated during signing
n=Order of the elliptic curve
The above equation(5)ensures that only the sender with knowledge of the private key can generate a valid signature. The recipient or the network can later verify this signature using the sender's public key, confirming the transaction's authenticity and preventing forgery or tampering.

G. Comparison of pow and the hardhat

Proof of Work (PoW) and Hardhat serve different purposes within the blockchain ecosystem. The Table (1), PoW [21], is a consensus mechanism used in networks like Bitcoin and Ethereum (before Ethereum 2.0) to validate transactions through computational mining. It ensures security and decentralization but requires significant energy consumption and has slower transaction speeds due to complex cryptographic puzzles. In contrast,[11]Hardhat is a blockchain development framework that provides an in-memory Ethereum node for testing and smart contract deployment. It enables rapid execution, debugging, and automation without the need for mining, making it energy-efficient and ideal for development environments. While PoW is designed for live blockchain security, Hardhat is tailored for smart contract testing and deployment, focusing

on efficiency rather than network-wide validation. In contrast,

Table 1. Comparison of PoW and Hardhat

Feature	Hardhat(Blockchain Development Framework)	Proof of Work(PoW)
Purpose	Used for smart contract development, testing, and deployment	Consensus mechanism for transaction validation
Energy Efficiency	High (simulation-based, no mining required)	Low(requires extensive computational power)
Transaction Speed	Instant (local execution)	Slower due to mining competition
Security	Security-focused for testing, but not a consensus mechanism	Highly secure but vulnerable to 51% attacks
Decentralization	Not applicable (development tool)	Fully decentralized but resource-intensive
Gas Fees	No gas fees in local testing	Requires gas fees for transactions
Mining Requirement	No mining involved	Requires miners to validate transactions
Scalability	High (limited to developed environments)	Limited due to high computational demand

Hardhat [13] is a blockchain development framework that provides an in-memory Ethereum node for testing and smart contract deployment. It enables rapid execution, debugging, and automation without the need for mining, making it energy-efficient and ideal for development environments. While PoW is designed for live blockchain security, Hardhat is tailored for smart contract testing and deployment, focusing on efficiency rather than network-wide validation.

H. Performance Metrics of Hardhat and Proof of Work(PoW)

The bar chart below from Figure 2 compares the performance ratings of Hardhat and Proof of Work (PoW) across four key metrics.

Energy Efficiency, Transaction Speed, Security, and Scalability. The blue bars represent Hardhat, while the red bars represent [21] Proof of Work (PoW). Hardhat significantly outperforms PoW in terms of Energy Efficiency and Transaction Speed, scoring close to 9 and 10, respectively, whereas PoW scores much lower in these areas. In terms of Security, PoW has a perfect score of 10, surpassing Hardhat, which has a moderate rating. For Scalability, Hardhat again outperforms PoW, indicating better adaptability to growing demands. This visualization highlights the trade-offs between the two systems, with Hardhat excelling in efficiency and speed, while PoW remains stronger in security.

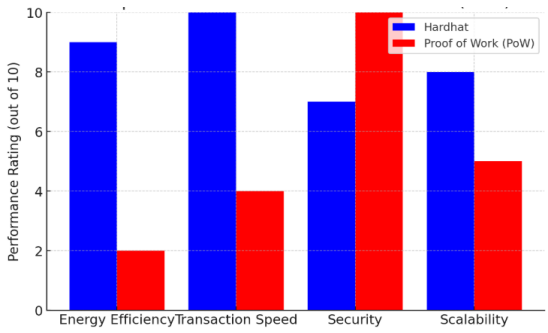
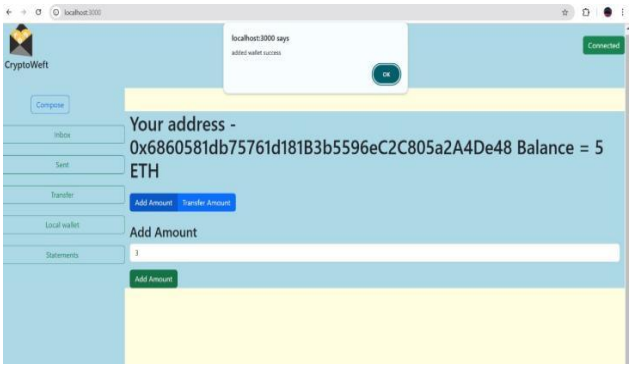


Fig 2. Performance Metrics of Hardhat and PoW

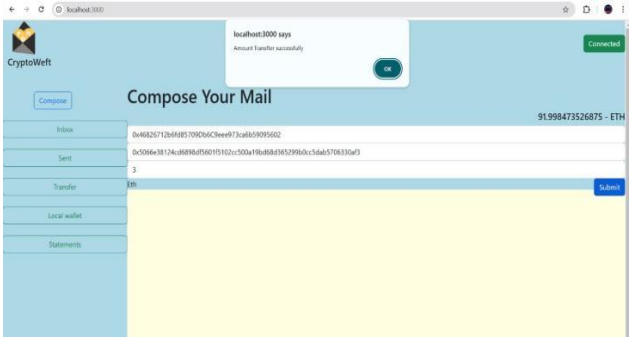
V. RESULTS AND DISCUSSION

The results of the proposed system demonstrate its effectiveness in enabling secure peer-to-peer transactions, blockchain-based email, and decentralized file storage, even in offline conditions. By leveraging the Hardhat blockchain framework with Ethereum, the system ensures seamless transaction synchronization once connectivity is restored, maintaining data integrity and preventing double-spending. The proposed system enhances security, scalability, and efficiency by integrating cryptographic signatures, smart contracts, and off-chain transactions. These features enhance efficiency by reducing blockchain congestion, lowering transaction fees, and preventing unauthorized modifications. Decentralized storage ensures reliability, minimizing data loss and reducing reliance on centralized servers. Using Hardhat with Ethereum, the system enables secure transactions, blockchain-based email, and offline file storage, ensuring seamless synchronization upon reconnection. Performance analysis highlights efficiency gains through off-chain processing, making it ideal for unstable networks. Hardhat Network streamlines smart contract development with instant execution, advanced debugging, automation, and plugins like Hardhat Deploy and Gas Reporter. Overall, it accelerates DApp development with a high-speed, flexible, and developer-friendly environment. We are used to building our application based on blockchain, which also enables us to link the pages within it.

A. Wallet Storage:

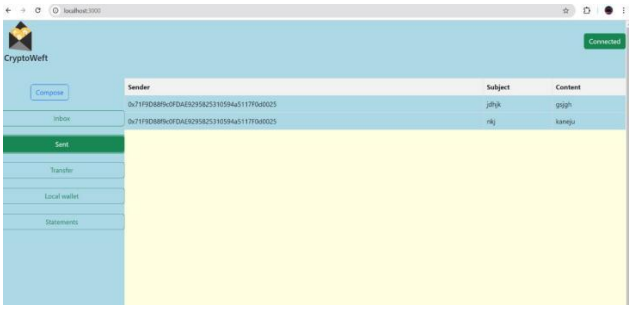


B. Mail Transaction:



C. Statement page:

D.Sender Transaction History page:



VI. CONCLUSION

In conclusion, Proposed system enhances blockchain scalability, security, and efficiency by integrating off-chain transactions, blockchain-based email, and decentralized storage. Utilizing Hardhat with Ethereum, it ensures secure peer-to-peer transactions, even offline, reducing network congestion, transaction costs, and processing delays while maintaining decentralization. Off-chain transactions improve financial accessibility in high-latency environments, while blockchain-based email and IPFS storage enhance data security and integrity. Encrypted messaging protects sensitive communication, and IPFS decentralization minimizes reliance on centralized servers. By combining these cutting-edge technologies, the system delivers a resilient and efficient decentralized framework, addressing blockchain limitations while ensuring secure transactions and communication.

REFERENCES

[1] Cryptocurrency Blockchain Technology in the Digital Revolution EraIntan Dwi Astuti, Suryazi Rajab, Desky Setiyouji, https://d oi.org/10.34306/att.v4i1.216

[2] East Sarajevo, Bosnia and Herzegovina , Blockchain technology , bitcoin and Ethereum, 2123 March 2018, doi:10.1109/ INFO TEH. 2018.8345547

[3] Accepting financial transactions using blockchain technology and cryptocurrency: A customer perspective approach Hayder Albayati a, Suk Kyoung Kim b ,Jae Jeung Rhob https://doi.org/10.1016/j.techsoc.2020.1013 20 12 December 2019; 24 June 2020;25June 2020

[4] Commit-Chains: Secure, Scalable Off- Chain Payments, *Rami Khalil, Alexei Zamyatin, Guillaume Felley, Pedro Moreno-Sanchez, and Arthur Gervais,* Paper 2018/642

[5] Offline Payments: Implications for Reliability and Resiliency in Digital Payment Systems, Laila Aboulaiz, Bunmi Akintade, Hamzah Daud, Monique Lansey, Megan Rodden, Lucas Sawyer, and Matthew Yip, August 16, 2024

[6] Jain S.M,(2023).Hardhat. In: A brief [8] Prasanna Kumar M J, Poovika D ,"A Secure and flexible blockchain based offline payment protocol ."International Journal of scientific research in engineering and , management , Volume 8, Issue 6, June 2024

[7] Nikolay Ivanov, Qiben Yan. "System- Wide Security for Offline Payment Terminals. "arXivpreprint arXiv:2107.08490, July 2021.

[8] Raed Saeed Rasheed, Khalil Hamdi Ateyeh Al-Shqeerat, Ahmed Salah Ghorab, Fuad Salama AbuOwaimer, Aiman Ahmed AbuSamra."Blockchain Mobile Wallet with Secure Offline Transactions. "Computers, Materials & Continua, Volume 75, Number 2, Pages 2905- 2919, March 2023.

[9] Ikechi Saviour Igboanusi, Kevin Putra Dirgantoro, Jae-Min Lee, Dong-Seong Kim. "Blockchain Side Implementation of Pure Wallet(PW): An Offline Transaction Architecture. "ICT Express, Volume 7, Number 3,Pages 327-334, September 2021.

[10] Joshua Lind , Oded Naor , Ittay Eyal. "Teechain : A Next - Generation Layer - two payment Network ."Proceedings of the 27th ACM Symposium on Operating Systems Principles (SOSP), pages 63-79, Oct 2019

[11] Nomic Foundation. (n.d.). Hardhat: Ethereum development environment for professionals. Hardhat. Retrieved April 2, 2025, from https://hardhat.org

[12] Gingu, I.-V., & Hursan, D. (2022). IPFS: Decentralized storage in a centralized world. IEEE Blockchain Technical Briefs. Retrieved April 2, 2025, from https://blockchain.ieee.org/images/files/pdf/techbriefs-2022-q4/ipfs-decentralized- storage- in-a-centralized-world.pdf

[13] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system, "Decentralized Bus. Rev., 2008, Art. no.21260.

[14] Al-Karaki, J. N., & Gawanmeh, A. (2023). Blockchain for email security: A perspective on existing and emerging solutions. Zayed University Scholars' Work. Retrieved April 2, 2025, from https://zuscholars.zu.ac.ae/works/6258/

[15] A. Mizrahi and A. Zohar, "Congestion attacks in payment channel networks, "in Financial Cryptography and Data Security, N. Borisov and C. Diaz, Eds., Berlin, Heidelberg: Springer BerlinHeidelberg, 2021, pp.170–188.

[16] V. Buterin et al., "A next-generation smart contract and decentralized application platform, "White Paper, vol.3, no.37, pp.2–1,2014.

[17] B. Srimanand S. G. Kumar, "Decentralized finance(DEFI):

The future of finance and defi application for Ethereum blockchain-based finance market, ”in Proc. Int. Conf. Adv. Comput., Commun. Ap pl. Informat. (ACCAI),2022, pp.1–9.

[18] “Biggest cryptocurrency in the world- Both coins and tokens-Based on market capitalizationonNovember11,2022. ”Staista. Accessed: Nov. 2022. [Online]. Available: https://www.statista.com/statistics/126901 3/biggest-crypto-per-category-worldwide/

[19] Role-Based Access Control Using Smart Contract, IEEE Access (Volume: 6),12240 - 12251,07 M a r c h 2 0 1 8 DOI: 10.1109/ACCESS.2018.28128 44, IEEE

[20] Biometric identification, Anil Jain, Lin Hong, Sharath Pankanti, Communications of the ACM Volume 43, Number 2(2000), Pages 90-98

[21] Performance analysis and comparison of PoW, PoS and DAG based blockchains, overlaypanelBin Cao a b, Zhe nghui Zhang c, Daquan Feng d, Shengli Zhang e, Lei Zhang f, Mugen Peng a, Y un Li c, Volume 6, Issue 4, November 2020, Pages 480-485

[22] Developing Cost-Effective Blockchain- Powered Applications: A Case Study of the Gas Usage of Smart Contract Transactions in the Ethereum Blockchain Platform ,ACM Transactions on Software Engineering and Methodology (TOSEM), Volume 30, Issue 3, Article No.:28,Pages138https://doi.org/10.1145/3431726,09 March 2021

[23] Secured Ethereum Transactions using Smart Contracts & SolidityVOLUME21 ISSUE 5 (May) - 2022, Aarush Kumar

[24] Implementation of smart contracts for blockchain-based IoT applications, 2018 9th International Conference on the Network of the Future (NOF),19-21 November 2018, IEEE *Xplore*: 03 January 2019, DOI: 10.1109/NOF.2018.8597718

[25] Automated Unit Testing of Solidity Smart Contracts in an Educational Context, Munich, 15.11.2023 Batuhan Erden

[26] Elliptic Curve Digital Signatures and Their Application in the Bitcoin Crypto-currency Transactions Benjamin K. Kikwai 16 October 2017International Journal of Scientific and Research Publications, Volume 7, Issue 11, November 2017 135 ISSN 2250-3153

[27] N. Ying and T.W. Wu, “xlumi: Payment channel protocol and off-chain payment in blockchain contract systems,”2021,arXiv:2101.10621.

[28] J. Poon and T. Dryja, “The bitcoin lightning network: Scalable off-chain instant payments,”2016

[29] V. Buterin. “Ethereum. On sharding blockchains.” GitHub. Accessed: Nov. 19, 2019. [Online]. Available: https://github.com/ethereum/wiki/

[30] J. S. Bellagarda, “The potential effect off-chain instant payments will have on cryptocurrency scalability issues-the lightning network,” in Proc. Int. Conf. Inf. Resour. Manage. (CONFIRM), 2019, vol. 2, pp. 1–14.