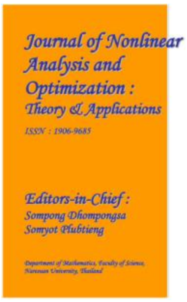
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.15 : 2024
ISSN : **1906-9685**



Journal of Nonlinear Analysis and Optimization : Theory & Applications
ISSN : 1906-9685
Editors-in-Chief :
Sompong Dhompongsa
Somyot Plubtieng
Department of Mathematics, Faculty of Science, Naresuan University, Thailand

Paper ID: ICRTEM24_149 **ICRTEM-2024 Conference Paper**

SMART LINK: CONNECTING CONTRACTS SEAMLESSLY ON THE BLOCKCHAIN

[#1]**M. JASHWANTH,** ***UG Student***
[#2] **T. ROHIT,** ***UG Student***
[#3]**T. SACHIT,** ***UG Student***
[#4]**P. SRAVANTHI,** ***Assistant Professor***
Department of CSE,
CMR COLLEGE OF ENGINEERING & TECHNOLOGY, HYDERABAD.

ABSTRACT- Security is paramount in banking systems, especially concerning sensitive user details. Breaches can lead to severe financial losses and breach of trust. Concerns arise from vulnerabilities in third-party systems, with centralized databases being susceptible to hacking and data manipulation. Block-chain offers a solution. Its decentralized, immutable ledger system cryptographically secures transactions, reducing the risk of unauthorized access and data tampering. Smart contracts automate processes, minimizing human error and malicious intervention. Block-chain encrypts and distributes sensitive information across a network, making it challenging for hackers to alter or steal data. Transparency allows users to track data flow, enhancing trust and accountability. Blockchain technology enhances banking security by mitigating third-party risks and ensuring confidentiality, integrity, and availability of user details. Its decentralized nature and cryptographic principles make it a valuable tool in the digital age.

Keywords: *Web3.0, Blockchain, Digital Currency, Ethereum wallet, Automated Transactions, Identity Management*t, *Digital Asset Management, Decentralized Network, Peer-to-Peer Transactions.*

I. INTRODUCTION

In today's interconnected world, security breaches pose significant risks across various industries, with the banking sector being particularly vulnerable. One of the critical areas of concern lies in the handling of user data by third-party entities, such as banks. When users engage in transactions through the banking system, their personal information is often shared with these intermediaries, creating opportunities for security breaches and compromising the confidentiality of user data. To address this issue, blockchain technology offers a promising solution. By leveraging blockchain, decentralized applications (DApps) can be developed, eliminating the need for centralized intermediaries. In such decentralized systems, users have direct control over their data, ensuring that sensitive information remains accessible only to authorized parties. In a blockchain-powered decentralized banking system, transactions occur directly between users without the involvement of third-party institutions. Smart contracts, which are self-executing contracts with predefined conditions, can facilitate these transactions securely and transparently. Each user retains ownership of their data, and transactions are verified and recorded on the blockchain, ensuring tamper-proof and immutable records.

II. RELATED WORK

In the pursuit of innovation and effectiveness, contemporary projects often lean on established solutions as foundational cornerstones for progress. This strategy not only acknowledges the expertise and strides made by predecessors but also fosters a collaborative environment where concepts can evolve and adapt to emerging challenges. In our project, we enthusiastically adopt this philosophy, thoughtfully integrating components from existing solutions to enhance our venture. These established solutions act as beacons, providing valuable insights and frameworks that steer the trajectory of our project.

A. **Peer-to-Peer Network:** Peer-to-peer (P2P) networks, which enable the transfer of blocks and transactions, are the foundation of blockchain systems and have a substantial impact on their security and efficiency. Considering this crucial function, a careful analysis of the P2P network topologies (Rashmi P. Sarode et al., 2021; Susilo et al., 2015; Skeen, D. 1982; Buterin, V. et al. 2014) used by popular blockchains such as Ethereum and Bitcoin is necessary. The fact that existing Ethereum blockchain explorers, like Etherscan, only offer information about transactions and block histories, without going into detail into the P2P network underneath, is noteworthy. This omission highlights a deficiency in our knowledge and oversight of blockchain infrastructure.

B. **Distributed Ledgers (DL):** Distributed ledgers (DL) are on the verge of becoming a disruptive technology, capable of profoundly impacting a wide range of industries and established applications, such as cryptocurrency, which handles and shares transaction records across a network of users. The records can be verified by each user, and transactions are tied together using cryptography, so altering the records is nearly impossible. Blockchains promise the ability to maintain critical information in a trustworthy repository (ABEYRATNE, S.A et al., 2016; Ali Sunyaev 2020; Kakavand, Hossein et al., 2017) without any centralized management. Blockchains allow for transparency, efficiency, immutability of records, auditability, and security, which reduce problems of system component and database redundancy, fraud, misuse, and many cybersecurity challenges.

C. **Decentralized Databases (DD):** Decentralized databases, which are essential parts of blockchain technology, are transforming data management by dispersing data among a network of linked nodes instead of depending on a single authority. Because each member keeps a copy of the database, this technique guarantees resilience against single points of failure and improves transparency. An important characteristic is immutability, which offers a tamper-proof historical record by making data nearly impossible to change once it is stored on the blockchain. Permissionless access to decentralized databases frequently promotes diversity and creativity within the network. The necessity for a central arbiter is removed when consensus techniques, such as proof of work or proof of stake, enable network (Enis Karaarslan 2020; Jovan Kalajdjieski et al., 2022; Dekai Yan et al., 2021) participants to agree on the authenticity of transactions. Scalability is still an issue, though, especially as blockchain networks get bigger and process more transactions. Interoperability initiatives seek to facilitate smooth data transfer across various blockchain networks, and privacy concerns drive the creation of technologies that enhance privacy to safeguard confidential data.

III. METHODS AND EXPERIMENTAL DETAILS

A. No Third-Party Authorization:

The Third-party permission is an essential technique in centralized systems that helps to facilitate transactions and maintain parties' trust. This method usually entails depending on a central authority or middleman to handle user identities, validate and approve transactions, and ensure adherence to set rules and guidelines. Third-party authorization comes with a number of restrictions and hazards, in addition to the sense of security and legitimacy it might offer. These include the possibility of single points of failure, data breaches, and privacy and autonomy issues because users have to give up control over their assets and personal information to the central authority.

Decentralized systems use blockchain technology and cryptographic concepts to get around these problems by doing away with the requirement for third parties to grant permission. Decentralized networks disperse authority and decision-making over a dispersed network of nodes, each of which takes part in the validation and consensus process, as opposed to depending on a single authority.

Decentralized systems facilitate trustless transactions and interactions by utilizing consensus methods and smart contracts, which let parties communicate directly with one another without the need for middlemen. In addition to improving efficiency, security, and transparency, this strategy also encourages user autonomy and asset and data ownership.

B. Decentralized App with Blockchain:

The Through the use of Solidity, Smart Contracts, and cryptographic principles in the construction of our blockchain application, we set out to transform conventional systems through the utilization of decentralized technology. Our application is based on Solidity, a programming language created especially for creating Smart Contracts on blockchain systems like Ethereum. We can use Solidity to develop self-executing contracts that do not require middlemen or outside scrutiny by autonomously enforcing predetermined norms and conditions. Within our decentralized environment, these smart contracts ensure speed, security, and transparency by facilitating trustless transactions and interactions.

C. Gas Fee:

The transaction expenses incurred when carrying out activities on the Ethereum blockchain are referred to as gas fees. Gas fees are a crucial factor to take into account when developing blockchain apps with Solidity and Smart Contracts since they affect how affordable and useful decentralized applications (DApps) may be. Gas costs are required from users who engage with DApps through sending transactions or executing Smart Contracts in order to reimburse the network validators for the computational resources used.

The complex nature of the task at hand and the level of network congestion at the moment are taken into consideration when calculating gas fees. Gas fees are generally greater for more sophisticated procedures, such establishing Smart Contracts or carrying out intricate computations, than for simple transactions.

In our project, it's crucial to factor in gas fees when designing and implementing Smart Contracts and other functionalities we use gas optimization and gas price estimation to factor the gas fee.

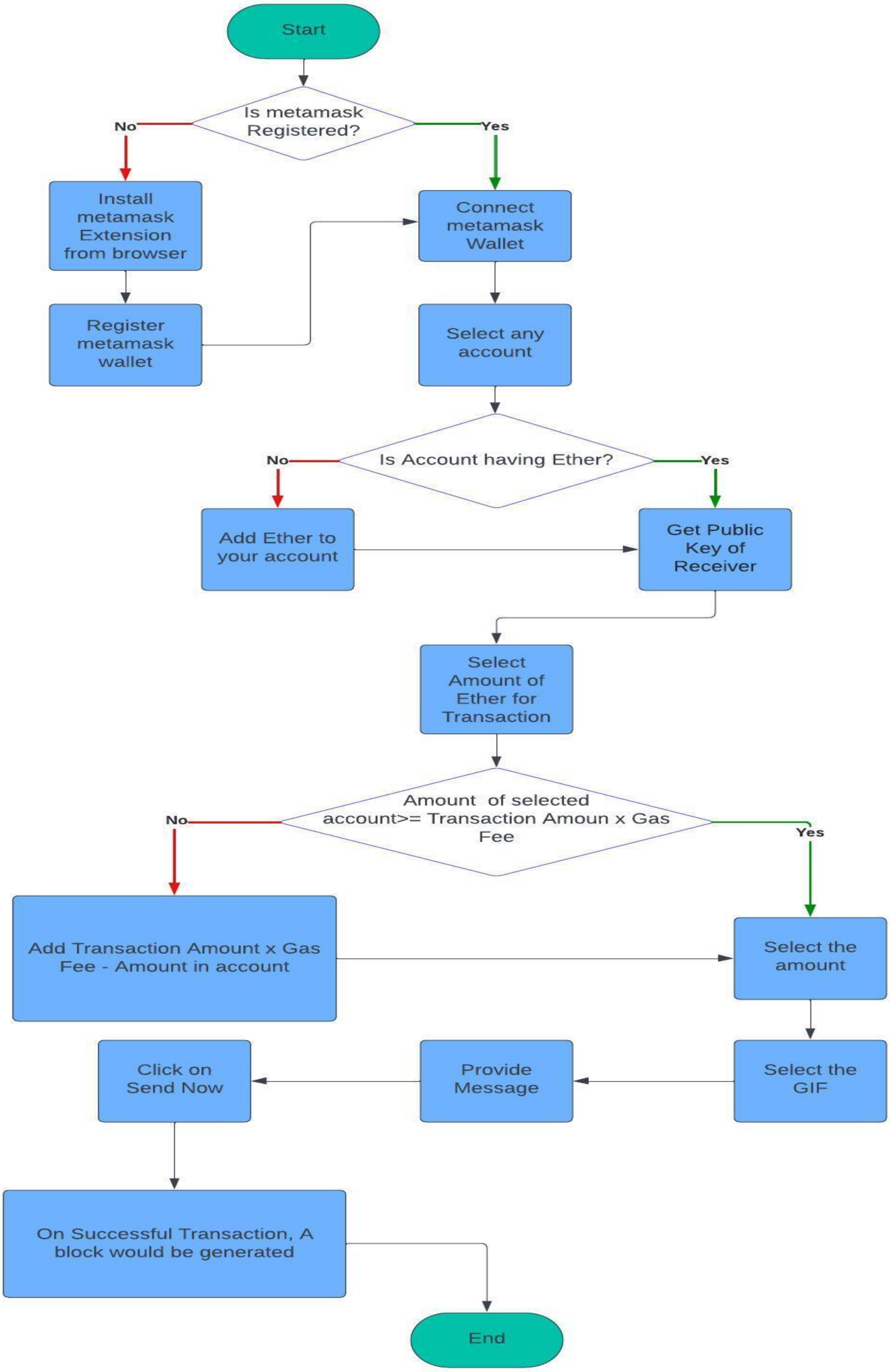

Start
Is metamask Registered?
No
Yes
Install metamask Extension from browser
Register metamask wallet
Connect metamask Wallet
Select any account
Is Account having Ether?
No
Yes
Add Ether to your account
Get Public Key of Receiver
Select Amount of Ether for Transaction
Amount of selected account>= Transaction Amoun x Gas Fee
No
Yes
Add Transaction Amount x Gas Fee - Amount in account
Select the amount
Select the GIF
Provide Message
Click on Send Now
On Successful Transaction, A block would be generated
End

Fig.Architecture of the model

IV. RESULTS AND DISCUSSIONS

Examining current solutions illuminates the range of strategies and techniques that can be used to improve blockchain model's performance in engineering settings. Every solution contributes to the overall objective of enhancing blockchain model performance for engineering activities.

No Third-Party Authorization (NTPA):

Approach: This solution emphasizes the significance of the tools, frameworks, and platforms utilized to make no third-party authorizations. To guarantee scalability and security, we utilized the Peer-to-Peer (P2P) network architectural plan to implement this authorization. We obtained no third-party authorization by employing a blockchain approach.
Applicability to Engineering: This approach is important since engineering exercises require a high level of accuracy and precision. The use of blockchain models to interpret engineering instructions can significantly increase the effectiveness of computational query processing.
Privileges: The resulting model gives us better building adaptability and security and eliminates third-party authorization to provide more precise and accurate responses in the blockchain domain.

Distributed Ledgers (DL):

Approach: In implementing distributed ledgers, our approach emphasizes the utilization of blockchain technology to create a decentralized system. The solution focuses on designing a network of nodes that collectively maintain a shared, tamper-proof ledger, ensuring transparency and integrity. Through the use of consensus mechanisms and cryptographic techniques, we establish trust among network participant.
Applicability to Engineering: Engineering processes benefit from increased transparency, as all transactions are recorded and visible to authorized parties, facilitating traceability and accountability. The cryptographic security inherent in distributed ledgers ensures the integrity and confidentiality of sensitive data, safeguarding against unauthorized access and tampering.
Privileges: The implementation of distributed ledgers in blockchain offers improved transparency, security, and efficiency in various applications and industries.

Decentralized Databases (DD):

Approach: Decentralized databases focuses on leveraging distributed ledger technology to create a system where data is stored and managed across a network of nodes rather than a single central database. Smart contract functionality further enhances the automation and governance of data transactions, minimizing the need for manual intervention.

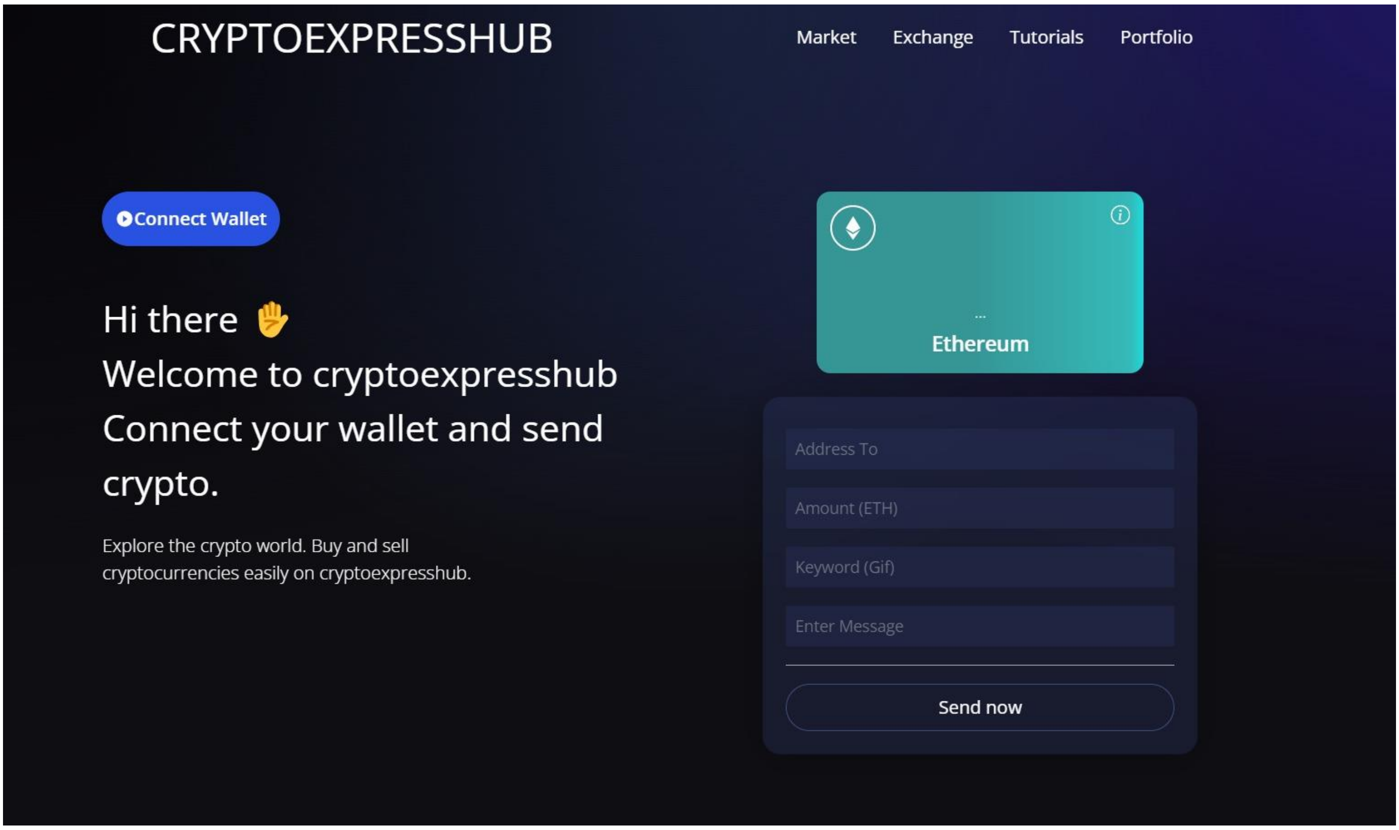
Applicability to Engineering: Decentralized databases offer significant applicability to engineering across various domains. From supply chain management to infrastructure monitoring and beyond, engineering processes benefit from the transparency, security, and efficiency provided by decentralized databases.
Privileges: DD enhances data integrity and trustworthiness by eliminating single points of failure and providing a tamper-resistant record of transactions. Overall decentralized databases offer an improved transparency, security, and efficiency.

Comparison:

Each solution brings its own merits to the table. While the first solution (NTPA) fosters direct peer-to-peer transactions, providing security and efficiency by eliminating intermediaries, the second (DL) transparent and tamper-proof transaction records across decentralized networks, promoting trust and resilience, the third (DD) further implement this by distributing data storage. Combining aspects of all these solutions presents an ideal approach empowering users towards a decentralized future.

Integration:

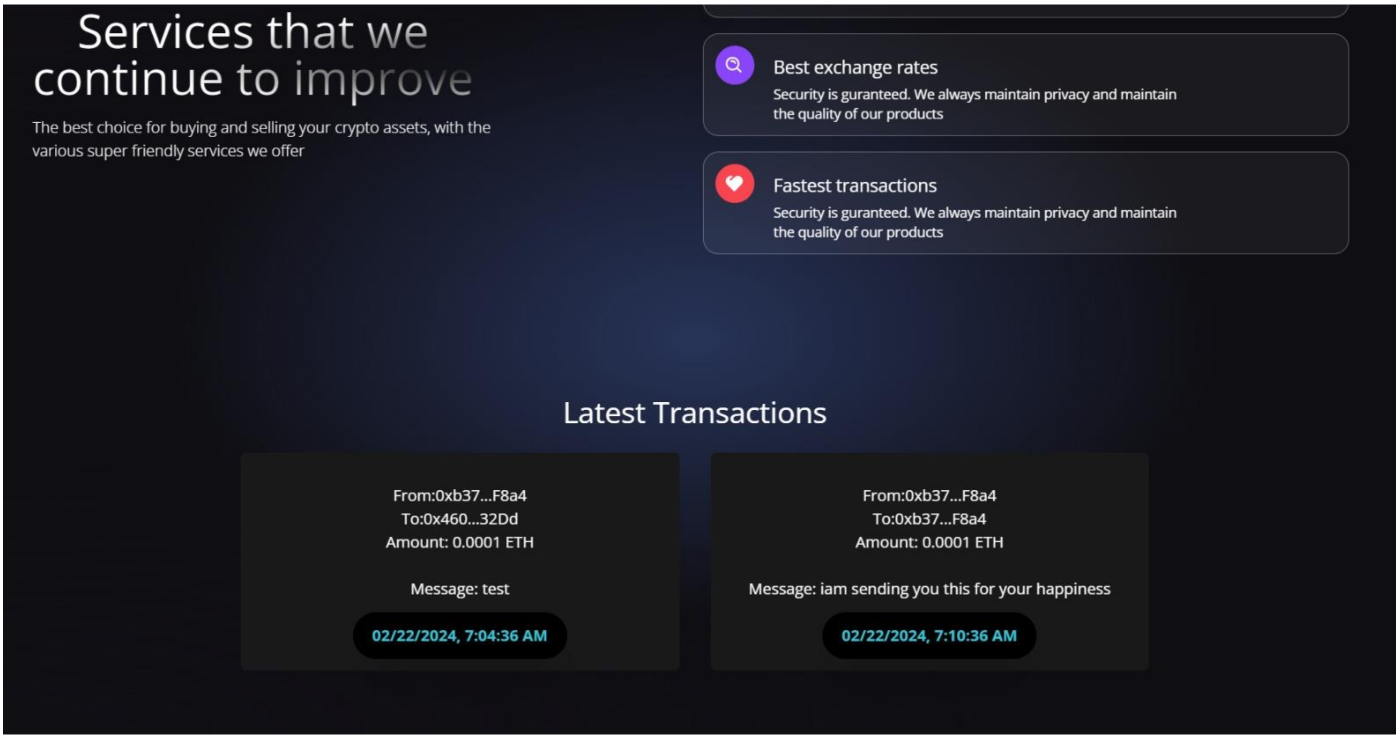
The integration of (NTPA), (DL), and (DD) implies results in a change in the digital domain that is significant. Transactions become direct and secure when middlemen are removed, supported by transparent, immutable records kept throughout decentralized networks. This structure is further improved by decentralized databases, which distribute data management and storage while encouraging openness and cooperation. When combined, these advancements create a foundation for a decentralized future where users will have efficiency, autonomy, and trust in their interactions and transactions.



Hi there ✋
Welcome to cryptoexpresshub
Connect your wallet and send crypto.

Explore the crypto world. Buy and sell cryptocurrencies easily on cryptoexpresshub.

Fig. User Interface - 1



Services that we continue to improve

The best choice for buying and selling your crypto assets, with the various super friendly services we offer

Best exchange rates
Security is guranteed. We always maintain privacy and maintain the quality of our products

Fastest transactions
Security is guranteed. We always maintain privacy and maintain the quality of our products

Latest Transactions

From:0xb37...F8a4
To:0x460...32Dd
Amount: 0.0001 ETH

Message: test

02/22/2024, 7:04:36 AM

From:0xb37...F8a4
To:0xb37...F8a4
Amount: 0.0001 ETH

Message: iam sending you this for your happiness

02/22/2024, 7:10:36 AM

Fig. User Interface - 2

V. CONCLUSION

In conclusion, the research and discoveries we have explored provide insightful information about possible approaches to completing the project's output. By using these strategies, we can improve the development of a crypto blockchain model that provides efficiency, security, transparency, and trust.

No Third-Party Authorization (NTPA):
In conclusion, the removal of the need for third-party authorization represents a major development in digital transactions. This method improves transaction security, transparency, and efficiency by enabling direct peer-to-peer interactions. Users are less dependent on centralised authorities as they have control over their assets and data thanks to smart contracts and encryption technology. Both individuals and companies can deal without the need for third-party authorization, ensuring that their transactions are safe, clear, and devoid of middlemen.

Distributed Ledgers (DL):
In conclusion, distributed ledgers are an innovative development in transaction processing and data management. These decentralised networks securely store and verify data across several nodes, utilising blockchain technology to provide transparency, integrity, and confidence in transactions. Distributed ledgers are ideal for a wide range of applications across industries because they remove the need for central authorities and promote flexibility and integrity.

Decentralized Databases (DD):
To sum up, decentralized databases enable a new approach in handling and storing information that promotes cooperation, security, and transparency. These databases protect the confidentiality and integrity of data while increasing stakeholder collaboration and openness by dispersing data administration and storage throughout a network of nodes. Decentralized databases offer a reliable and scalable solution for safe and effective data management through consensus procedures and cryptographic security measures.

In briefly, combining decentralized databases, distributed ledgers, and no third-party authorization changes digital interactions. By avoiding middlemen and depending instead on transparent records across decentralized networks, transactions become straightforward and secure. User autonomy over their resources and information promotes effectiveness and trust. While decentralized databases safely share data management, blockchain technology guarantees transaction integrity and transparency.

When combined, these developments move us closer to a decentralized digital world where efficiency, transparency, and trust are key characteristics of digital interactions.

REFERENCES

[1] S. Saroiu, K. Gummadi, R. Dunn, S. Gribble, and H. Levy, "An analysis of internet content delivery systems," in Proc. of the Fifth Symposium on Operating Systems Design and Implementation (OSDI), 2002.

[2] Saroiu, Stefan, Krishna P. Gummadi, Richard J. Dunn, Steven D. Gribble, and Henry M. Levy. "An analysis of internet content delivery systems." ACM SIGOPS Operating Systems Review 36, no. SI (2002): 315-327.

[3]Kazman, Rick, Len Bass, Gregory Abowd, and Mike Webb. "SAAM: A method for analyzing the properties of software architectures." In Proceedings of 16th International Conference on Software Engineering, pp. 81-90. IEEE, 1994.

[4] Chowdhury, Mohammad Jabed Morshed, MD Sadek Ferdous, Kamanashis Biswas, Niaz Chowdhury, A. S. M. Kayes, Mamoun Alazab, and Paul Watters. "A comparative analysis of distributed ledger technology platforms." IEEE Access 7 (2019): 167930-167943.

[5] Deshpande, A., Stewart, K., Lepetit, L., & Gunashekar, S. (2017). Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards. Overview report The British Standards Institution (BSI), 40, 40.

[6] Tmeizeh, Muhammed, Carlos Rodríguez-Domínguez, and María Visitación Hurtado-Torres. "A Survey of Decentralized Storage and Decentralized Database in Blockchain-Based Proposed Systems: Potentials and Limitations." International Congress on Blockchain and Applications. Cham: Springer Nature Switzerland, 2023.

[7] Bonifati, Angela, Panos K. Chrysanthis, Aris M. Ouksel, and Kai-Uwe Sattler. "Distributed databases and peer-to-peer databases: past and present." ACM SIGMOD Record 37, no. 1 (2008): 5-11.