IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ICRTTC '23
International Conference on Recent Trends and Technologies in Computing
Department of Computer Science and Engineering, Arasu Engineering College
Vol. 12, Special Issue 1, April 2023

TRANSAZIONE: Enabling Algorand Based Transaction

Mrs. M.C. Jayaprasanna[1], M. Bhagavathy Vignesh[2], N.Michael Danieal[3], A.Mohamed Salman Mydeen[4]

M.E, Assistant Professor, Anjalai Ammal Mahalingam Engineering College, Kovilvenni, India[1]

B.Tech/IT, Anjalai Ammal Mahalingam Engineering College, Kovilvenni, India[2]

B.Tech/IT, Anjalai Ammal Mahalingam Engineering College, Kovilvenni, India[3]

B.Tech/IT, Anjalai Ammal Mahalingam Engineering College, Kovilvenni, India[4]

Abstract: Algorand is a cutting-edge block chain protocol that enables fast, secure and cost-effective transactions. Our platform leverages the power of Algorand's technology to bring a new level of efficiency and trust to online transactions. Our user-friendly interface makes it easy for anyone to send and receive payments. Whether they're a business looking to streamline their payments or an individual looking for a more secure way to manage their finances, our platform has everyone covered. With Algorand, people can rest assured that their transactions are made fast, secure, and cost-effective. The platform can also guide new users to make their first account and help them make their first transaction using Algorand. The interface is a simple login and send interface which is simple, intuitive and easy to understand for the end user to use.

I. INTRODUCTION

Block chain is a distributed ledger technology that allows for secure and transparent peer-to-peer transactions without the need for intermediaries. It is based on a decentralized network of nodes that work together to validate and record transactions on the ledger. Each block in a block chain contains a cryptographic hash of the previous block, creating an immutable and tamper-proof chain of blocks. Algorand is a block chain platform designed for the next generation of financial applications. It was created by Silvio Micali, a Turing Award-winning computer scientist and professor at MIT. The Algorand block chain was launched in2019, and it has quickly gained popularity due to its unique features and capabilities. Algorand is built on a pure proof-of-stake (PPoS) consensus algorithm, which ensures security and decentralization while achieving high transaction throughput and low latency. Unlike traditional proof-of-work (PoW) block chains, where miners solve complex mathematical problems to validate transactions and earn rewards, in PPoS, the valuators are randomly selected based on their stake in the network. This eliminates the need for expensive mining equipment and reduces energy consumption, making the network more environmentally friendly.

Algorand is designed to be scalable and can process thousands of transactions per second with low transaction fees. This makes it ideal for use in financial applications, where speed and cost-effectiveness are critical. Algorand is built on a layer-1blockchain, meaning that it provides a complete block chain infrastructure that does not require additional layers or off-chain solutions to be usable. This ensures that the platform is secure, reliable, and efficient. Algorand offers smart contract functionality through the Algorand Standard Assets (ASA) protocol, which allows users to create and exchange custom digital assets on the Algorand block chain. The platform also supports atomic swaps, which allow for instant and trustless exchange of different digital assets without the need for an intermediary. Algorand has a strong focus on security and privacy, with features such as key rotation, multi-signature accounts, and private smart contracts. This ensures that users can transact on the platform with confidence, knowing that their assets are secure and their privacy is protected. Algorand is used in a variety of industries, including finance, healthcare, and real estate, and has partnerships with major companies such as Circle, World Chess, and the Marshall Islands government. The platform is also actively involved in research and development to continue improving its features and capabilities. The formatter will need to create these components, incorporating the applicable criteria that follow.

Figure1.1 Blocks in Blockchain

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ICRTTC '23
International Conference on Recent Trends and Technologies in Computing
Department of Computer Science and Engineering, Arasu Engineering College
Vol. 12, Special Issue 1, April 2023

II. LITERATURESURVEY

1. ALGORAND: A BETTER DISTRIBUTED LEDGER,

Prof. Raghavendra Prasad SG, Harshitha U Kumar.(2019)

Block chain is the most rapidly improving technology in distributed computing. It has come a long way from being a new paradigm which is gaining momentum in the ledger technology. Later came the applications of the proof-of-stake algorithms into the ledger technology. All of these performed well except that each did not provide a secure way of distributed computing. Thus, researchers brought in a new concept of the cryptographic ledgers which used the whole new Byzantine Agreement protocol and the technology got to be known as the Algorand. Advantages include the trivial computation, true decentralization, its finality for payments, scalability better compared to bit coin, security is very good supporting the crypto currencies. Disadvantages include Elaborates on basics without giving detailed analysis on potential use cases.

2. ALGORAND,

JingChen,SilvioMicali.(2019)

A public ledger is a tamperproof sequence of data that can be read and augmented by everyone. Public ledgers have innumerable and compelling uses. They can secure, in plain sight, all kinds of transactions — such as titles, sales, and payments—in the exact order in which they occur. Public ledgers not only curb corruption, but also enable very sophisticated applications — such as crypto currencies and smart contracts. They stand to revolutionize the way a democratic society operates. As currently implemented, however, they scale poorly and cannot achieve their potential. Advantages include Algor and works efficiently and securely even in a totally permission less environment, where arbitrarily many users are allowed to join the system at any time, without any vetting or permission of any kind. Of course, Algorand works even better in a permission environment. Disadvantages include Elaborates on basics without giving detailed analysis on potential use cases.

3. ALGORAND: ASECURE AND EFFICIENT DISTRIBUTED LEDGER,

JingChen,SilvioMicali.(2019)

Use In this paper we propose Algorand, an alternative, secure and efficient distributed ledger. Algorand is permission less and works in a highly asynchronous environment. Unlike prior implementations of distributed ledgers based on “proof of work,” Algorand dispenses with “miners” and requires only a negligible amount of computation. Moreover, its transaction history “forks” only with negligible probability: that is, Algorand guarantees the finality of a transaction the moment the transaction enters the ledger. Advantages include implementing the high-level structure of Algorand to achieve the desired properties of a block chain. Disadvantages include There is no code simplicity and redundancy.

III. PROPOSEDSYSTEM

The existing monetary system is controlled by banks and other major financial institutions, where banks are vulnerable to cyber-attacks and exploitation. Banks could get bankrupt which would not only affect the bank but also the users who are a part of the bank. People are unable to track their transactions which happen though these banks and require permission from a higher authority to track their transactions the proposed system uses Algorand which is a decentralized, permission less block chain platform designed to provide a secure, scalable and efficient platform for digital assets and applications. Some of the key aspects of Algorand are, User Experience- Ensure that the user experience of your dApp is simple, intuitive, and user-friendly.

Scalability- Consider the scalability of your dApp and ensure that it can handle a large number of users and transactions. Algorand is designed to be scalable and secure, making it a good choice for building large-scaled Apps. Security Ensure that dApp is secure and that sensitive user data is protected. Algorand's consensus algorithm is designed to be secure and prevent malicious actors from compromising the network. These are some of the key aspects to consider when building a system on the Algorand block chain. By carefully considering these factors and using Algorand's powerful toolset, you can build a secure, scalable, and efficient decentralized application that provides real value to users.

IV. SYSTEMARCHITECTURE

The existing monetary system is controlled by banks and other major financial institutions, where banks are vulnerable to cyber attacks and exploitation. Banks could get bankrupt which would not only affect the bank but also the users who are a part of the bank. People are unable to track their transactions which happen though these banks and require permission from a higher authority to track their transactions.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ICRTTC '23
International Conference on Recent Trends and Technologies in Computing
Department of Computer Science and Engineering, Arasu Engineering College
Vol. 12, Special Issue 1, April 2023

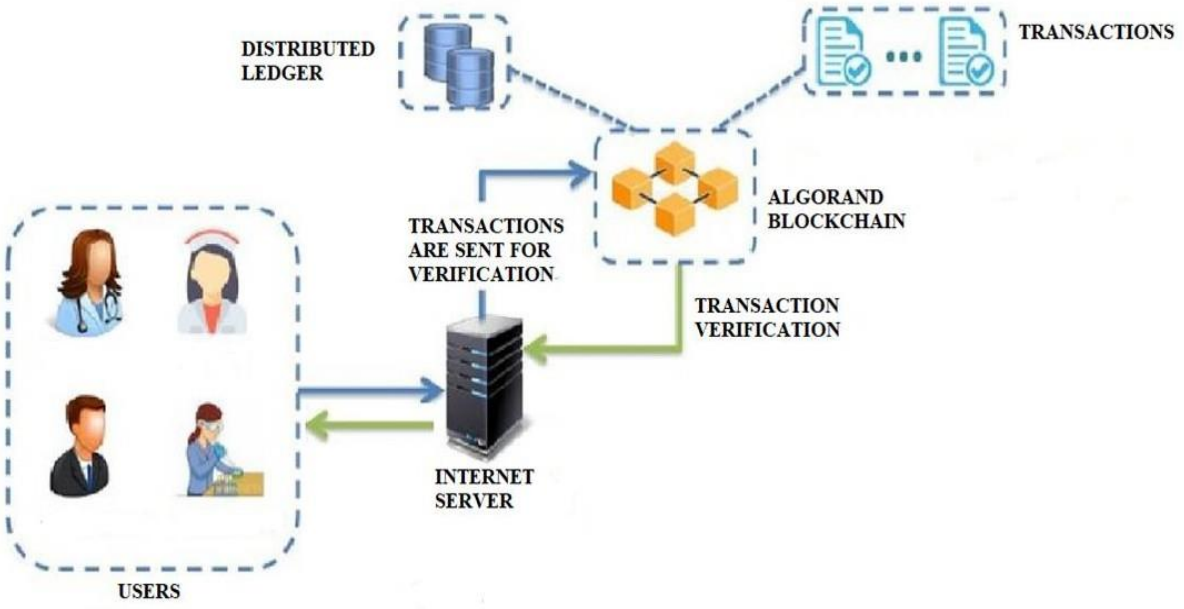

Figure4.1 System Architecture

V. ALGORITHM

The Decentralized Byzantine Agreement Protocol (DBAP) is a consensus algorithm used in block chain networks that enables nodes to agree on the state of the network despite the presence of Byzantine faults, where nodes can behave arbitrarily and maliciously. In traditional Byzantine Fault Tolerance (BFT) systems, a centralized authority is responsible for achieving consensus among nodes in the network. However, in decentralized systems like block chain, there is no central authority, and therefore a different approach is needed to achieve consensus. DBAP is designed to address this problem by allowing nodes in the network to communicate and reach consensus without relying on a central authority. The protocol works by using a random and verifiable mechanism to select nodes to propose blocks, and then requires all other nodes to vote on the proposed block. DBAP uses a threshold-based voting system where a certain percentage of votes must be received for the block to be accepted. In the case of Byzantine faults, where malicious nodes may try to sabotage the voting process, DBAP uses redundancy to ensure that a sufficient number of honest nodes participate in the voting process. One of the key advantages of DBAP is that it is highly resistant to attacks from malicious nodes, making it a secure and reliable consensus algorithm. Additionally, DBAP is highly scalable and can process a large number of transactions per second, making it suitable for use in high-performance block chain networks. In summary, the Decentralized Byzantine Agreement Protocol (DBAP) is a consensus algorithm used in block chain networks that allows nodes to communicate and reach consensus without relying on a central authority. It uses a threshold-based voting system and redundancy to ensure security and reliability in the face of Byzantine faults.

VI. MODULES

1. SIGNUP

This module allows you to create an account and access all the features of our website. To sign up, simply fill out the registration form with your basic information. Once you've completed the sign-up process, you'll receive a confirmation message indicating your successful sign-up to our site.

2. ALGORAND ACCOUNT CREATION

This module enables the user to easily create an Algorand account using the Algorand block chain at the touch of a button. The module will then generate a unique Algorand address and mnemonic that the user can use to access and interact with the Algorand network [7]. The account creation module is designed to be simple and user-friendly, so the user doesn't need any prior knowledge of block chain technology to get started.

3. TRANSACTION

With this module, you can easily send and receive Algo tokens/Assets on the Algorand block chain network. To send Algorand tokens, simply enter the recipient's Algorand address, the number of tokens you want to send, and your mnemonic to authorize the transaction. The module will then process the transaction and update your account balance accordingly. To receive Algo tokens,

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ICRTTC '23
International Conference on Recent Trends and Technologies in Computing
Department of Computer Science and Engineering, Arasu Engineering College
Vol. 12, Special Issue 1, April 2023

simply share your Algorand address with the sender. Once they send the tokens, the transaction will be confirmed and the tokens will be added to your account balance.

4. TRANSACTIONVERIFICATION

With the transaction verification module, we can easily verify the status of our Algorand transactions on the Algorand block chain network. This module can retrieve the transaction details, including the transaction status and confirmation time. It enables the user to easily monitor the status of their Algorand transactions without any prior knowledge of block chain technology.

VII. SNAPSHOTS

Transazione enables the user to make Algorand transactions in an easier way.

1. LOGIN

Login helps you to safely log into your account without any hassle. Simply enter your UserID and password to login to Transazione.

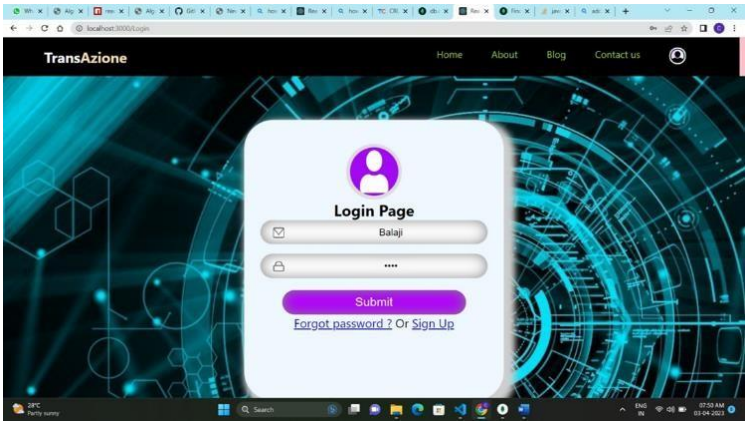

Fig.7.1 Login Creation

2. ACCOUNTCREATION

An Algorand account is essential to use the Algorand block chain and its features; this can be done at the touch of button

3. TRANSACTION

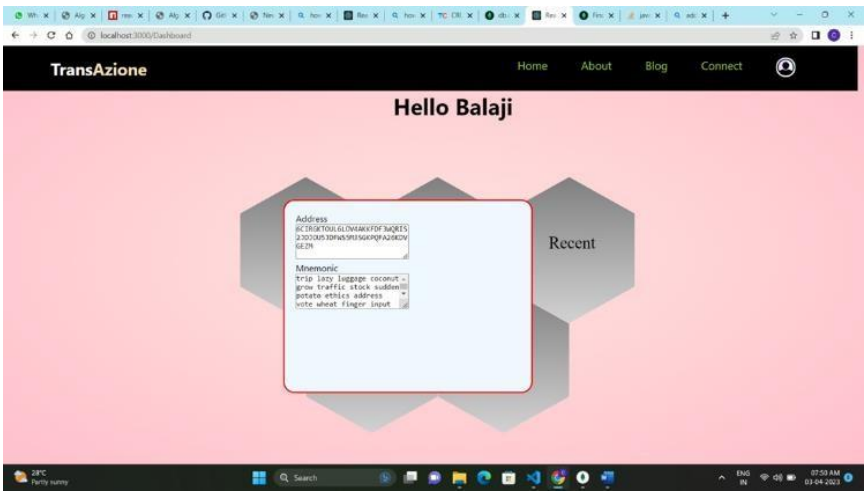

Fig.7.2 Algo Account creation

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ICRTTC '23
International Conference on Recent Trends and Technologies in Computing
Department of Computer Science and Engineering, Arasu Engineering College
Vol. 12, Special Issue 1, April 2023

This is the stage when the transaction takes place and all it requires is the receiver address and the amount to be transferred to the receiver.

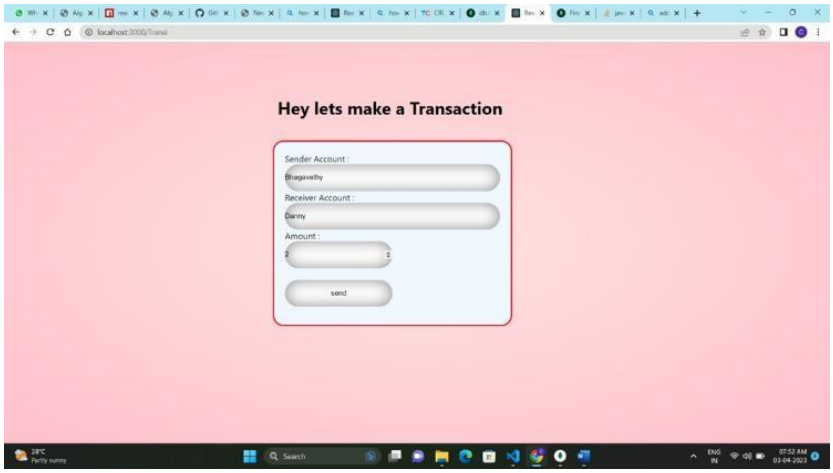

Fig.7.3 Transaction

4. TRANSACTION VERIFICATION

Finally the transaction can be verified with the help of Algo Explorer at the click of a button.

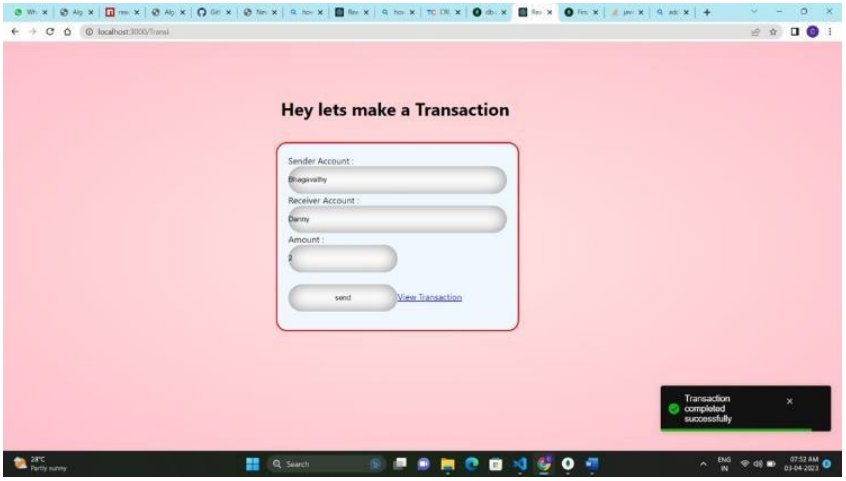

Fig.7.4 Verification by AlgoExplorer

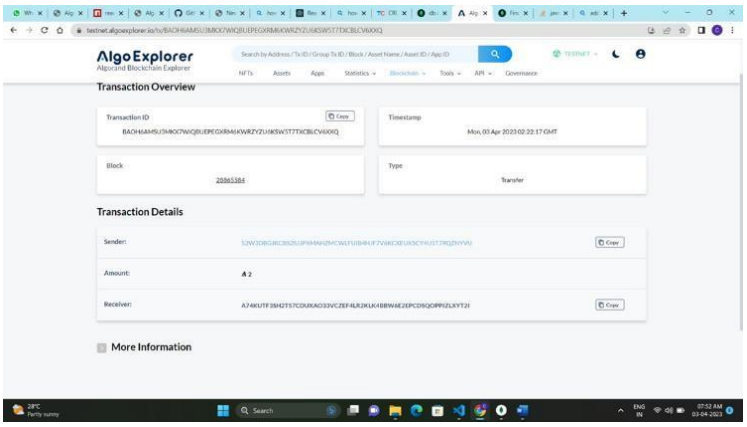

Fig.7.5 Transaction Overview

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ICRTTC '23
International Conference on Recent Trends and Technologies in Computing
Department of Computer Science and Engineering, Arasu Engineering College
Vol. 12, Special Issue 1, April 2023

VIII. CONCLUSION

Transazione utilizing Algorand's cutting-edge block chain protocol offers a fast, secure, and cost-effective way for users to transact and trade assets. The user-friendly interface makes it easy for new users to create an account and make their first transaction, while security measures protect user funds and prevent any unauthorized access to the platform. Moving forward, Transazione can continue to evolve and grow by adding new modules and features to enable more efficient and diverse transactions, and ensure the continued success of the site. Overall, Transazione has the potential to revolutionize the way we transact and trade assets, and it is an exciting development in the ever-evolving block chain industry.

REFERENCES

JOURNALREFERENCES:

[1] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timon, and P. Wuille, "Enabling block chain innovations´with pegged side chains." https://www.blockstream.com/sidechains.pdf,2014.
[2] M.Ben-or, Another advantage of free choice: completely asynchronous agreement protocols,in: 2nd Symposium on Principles of Distributed Computing, PODC, 1983,pp.27–30.
[3] B. Biais, C. Bisiere, M. Bouvard, and C. Casamatta, "The block chain folk theorem," The Review of Financial Studies, vol. 32,no. 5,pp.1662–1715, 2019.
[4] M. Borge, E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, and B. Ford, "Proof-of-personhood: Redemocratizing permission less crypto currencies," in IEEE European Symposium on Security and Privacy Workshops (EuroSPW),pp.23–26,April2017.
[5] J.Chen,S.Micali,Algorand,Technicalreport,https://arxiv.org/abs/1607.01341v9,2017.
[6] B. Chor, C. Dwork, Randomization inByzantine agreement, in:S. Micali (Ed.), Advances in Computing Research5: Randomness and Computation, JAI Press, 1989, pp. 443–497I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange an isotropy," in Magnetism, vol.III, G. T.Rado and H.Suhl, Eds. NewYork:Academic,1963,pp. 271–350.
[7] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. Gun Sirer, D. Song, and R.Wattenhofer,"˜"On scaling decentralized block chains," in Financial Cryptography and Data Security(J.70Clark,S.Meikle john, P.Y.Ryan, D.Wallach, M. Brenner, and K.Rohloff,eds.),2016.
[8] B.David,P.Gaži,A.Kiayias,A.Russell,Ouroborospraos: an adaptively-secure, semi-synchronous proof-of-stake block chain, in:EUROCRYPT,2018, pp. 66–98,inpress.
[9] D.Dolev, The Byzantine generals strike again, J.Algorithms3 (1)(1982)14–30.
[10] S.Micali, Algorand: the efficient public ledger,https://arxiv.org/abs/1607.01341,July2016.
[11] S.Nakamoto et al.,"Bitcoin: A peer-to-peer electronic cash system,"2008.
[12] D. Pike, P. Nosker, D. Boehm, D. Grisham, S. Woods, and J. Marston, "Proof of Stake Time: A time-accepted periodic pro of factor in a nonlinear distributed consensus." https://www.vericoin.info/downloads/ VeriCoin PoST White Paper 10 May 2015.pdf,2015.
[13] R. Saha,L.Luu, I. Parameshwaran, P. Saxena, and A. Hobor, "On power splitting games in distributed computation: The case of bit coin pooled mining," in IEEE 28th Computer Security Foundations Symposium, pp.397–411,2015.
[14] Y. Tselekounis, A. Kiayias, E. Koutsoupias and M. Kyropoulou, "Block chain mining games," in Proceedings of the ACM Conference on Economics and Computation, pp.365–382, 2016.
[15] E. Vasserman, Y. Kwon, D. Kim, Y. Son, and Y. Kim, "Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bit coin," in Proceedings of the ACMSIGSAC Conference on Computer and Communications Security, pp.195–209, 2017.

WEB REFERENCES:

[1] BitShares,https://bitshares.org/