International Journal of Scientific Research and Engineering Development-– Volume 7 Issue 3, May-June 2024
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Crowdfunding Platform using Smart Contracts

Avisha Mulchandani[1] ,Parnavi Shrawgi[1] , Sai Shinde ,Aparna Mote[2]
[1]BE Students, Department of Computer Engineering, Zeal College of Engineering and Research, Pune, Maharashtra, India
[2]Professor, Department of Computer Engineering, Zeal College of Engineering and Research, Pune, Maharashtra, India

----------**********----------

Abstract:

In the ever changing field of investing and fundraising, our initiative presents a blockchain-powered crowdfunding platform. This platform combines the accessibility and flexibility of crowdfunding with the security, efficiency, and transparency provided by blockchain technology. It gives project creators the opportunity to reach a worldwide audience and gives contributors a safe and reliable environment in which to support the projects of their choice. Our platform guarantees a smooth and reliable crowdfunding experience with strong identity verification, integrated cryptocurrency wallets, and comprehensive reporting. Our initiative is a representation of the fundraising industry of the future; it seeks to transform the relationship between inventors and supporters, promoting creativity, trust, and cooperation worldwide.

Keywords **—Crowdfunding, Blockchain**

----------**********----------

I. INTRODUCTION

Since it requires a great deal of confidence between a multitude of parties, including funders, middlemen, and organizations that serve as a location to hold funds until the recipient needs it, raising money is a challenging procedure. Trust is the main tool fundraising organizations use to persuade people to give money to recipients of funding. Many charitable groups engage in fundraising activities. Building trust is proving to be a challenge in their efforts to raise funds for the group. Few charitable organizations use technology to streamline the process of receiving donations from the public. The key to generating as much money as possible is trust, but technology also has a huge part to play in this.Given this, the blockchain is connected to an impure digital ledger that records each transaction and is utilized in the nursing field. Every record is kept on every node in the localized network due to the distributed nature of the system. Ethereum supports Sensible Contracts, which are blockchain-based applications. All smart contracts function inside the Ethereum Virtual Machine. The problem with these crowdsourcing firms is that a lot of frauds are being found, and they want outrageous prices. These kinds of issues can be avoided by implementing a crowdfunding plan with blockchain technology. By utilizing blockchain technology, sensible contracts for crowdfunding do away with the usual transaction and platform costs connected to rival crowdfunding platforms.

II. ALGORITHM

1. Smart Contract : Smart contracts are lines of code that are stored on a blockchain and automatically execute when predetermined terms and conditions are met. At the most basic level, they are programs that run as they've been set up to run by the people who developed them for authentications.

A smart contract is an agreement between two modules in the form of computer code. They run on the blockchain, so they are stored on a public database and cannot be changed. The transactions that happen in a smart contract processed by the blockchain, which means they can be sent automatically without a third party.

2. SHA256 Hash Generation:

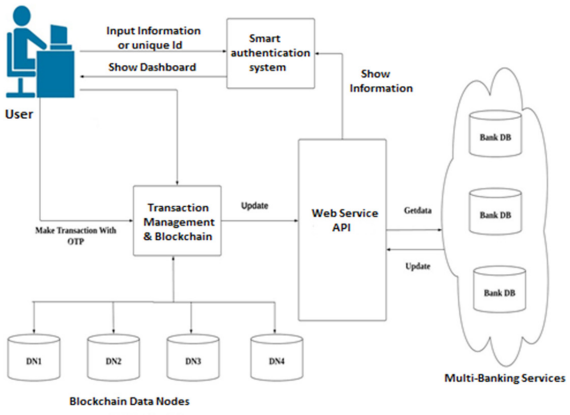
The SHA-256, also known as Secure Hash Algorithm 256-bit, is a cryptographic function that generates a 256-bit fixed-size hash. It belongs to the SHA-2 group, created by the US National Security Agency (NSA) in 2001. SHA-256 is employed in multiple security systems like TLS, SSL, PGP, SSH, IPsec, and the Bitcoin blockchain for generating digital signatures and authentication methods

3. Mining algorithm:A mining algorithm is a computerized procedure employed in blockchain technology, especially in cryptocurrencies like Bitcoin. Its purpose is to authenticate new transactions and incorporate them into the blockchain register. This process includes unraveling intricate cryptographic challenges to find a particular outcome known as a "hash" that fulfills specific requirements, like starting with a designated number of zero bits. The initial miner to solve the puzzle effectively incorporates the succeeding batch of transactions into the blockchain and receives a digital currency reward

4. Chain Consensus(Peer Verification):

In blockchain technology, chain consensus, or peer verification, is a key mechanism that ensures everyone in a decentralized network agrees on the current state of the shared ledger. This process is vital for upholding the integrity and security of the blockchain, preventing fraud like double-spending, and guaranteeing all versions of the ledger are the same throughout the network.

III. SYSTEM ARCHITECTURE



IV. PROPOSED SYSTEM

The proposed system conducts secure banking transactions based on a blockchain architecture using distributed system authentication. Once the system validates the authenticity of the current request, it will display the dashboard where all user account information is accessible. Users can select a specific account and log in with their credentials. The system then sends an OTP and implements two-step verification. Once the OTP is validated by the system, it will show the homepage where users can conduct various transactions, such as checking balances and making withdrawals. When any transaction is completed, the system stores all the information in the blockchain. During the storage of transaction information in the blockchain, the system executes various algorithms, such as SHA for hash generation, mining to generate a valid hash, smart contracts for system policy, and consensus to validate the current blockchain on all Peer-to-Peer nodes. A blockchain is a digital, immutable, distributed ledger that chronologically records transactions in near real-time. The prerequisite for each subsequent transaction to be added to the ledger is the consensus of the network participants (called nodes), thereby creating a continuous mechanism of control against manipulation, errors, and issues of data quality.

COMPONENTS OF PROPOSED SYSTEM

Blockchain: Blockchain is an online ledger that provides decentralized and transparent data sharing. With distributed recordings, all transaction data (stored in nodes) are compressed and added to different blocks. The data stored in each block can be verified simultaneously and become inalterable once entered.

Multi-factor Authentication: Our proposed MFA provides a convenient and high-secure multi-stage identity verification process using random strings.

Strong privacy preservation of user credentials: In our proposed authentication scheme, user credentials are not stored in cloud servers but allow the servers to perform authentication on hashed credentials.

Smart Contract: Smart contracts are lines of code that are stored on a blockchain and automatically

execute when predetermined terms and conditions are met. At the most basic level, they are programs

USE CASE DIAGRAM

V. CONCLUSION

By using a decentralized approach, the suggested Blockchain donation mechanism for crowdfunding aims to increase transparency. Better authenticity and security are two requirements that this technology will meet. Moreover, it will increase transparency throughout the entire process. This will assist in eliminating intermediaries between creators and donors.

REFERENCES

[1] Yadav, Nikhil & .V, Sarasvathi. (2020). Venturing Crowdfunding using Smart Contracts in Blockchain.J

[2] Hannan MA, Shahriar MA, Ferdous MS, Chowdhury MJM, Rahman MS. A systematic literature review of blockchain-based e-KYC systems. Computing. 2023 Apr 13:1–30. doi: 10.1007/s00607- 023-01176-8. Epub ahead of print. PMCID: PMC10100622

[3] Huang, Yuxin & Wang, Ben & Wang, Yinggui. (2021). Research and Application of Smart Contract Based on Ethereum Blockchain. Journal of Physics: Conference Series. 1748. 042016. 10.1088/1742-6596/1748/4/042016.

[4] Phan Mai, Van & Vũ, Lã & Sơn, Đỗ & Khải, Nguyễn & Lâm, Lê. (2023). A Blockchain-based User Authentication Model Using MetaMask.

[5] Guggenberger, T., Schellinger, B., von Wachter, V. et al. Kickstarting blockchain: designing blockchain-based tokens for equity crowdfunding. Electron Commer Res (2023). https://doi.org/10.1007/s10660-022-09634-9

[6] Chandraprabha, K.. (2023). Smart Contracts-Based Trusted Crowdfunding Platform. 10.1007/978-981-19-1844-5_37.

[7] Khan, S.N., Loukil, F., Ghedira-Guegan, C. et al. Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-Peer Netw. Appl. 14, 2901–2925 (2021). https://doi.org/10.1007/s12083-021-01127-0

[8] Sadiku, Matthew & Eze, Kelechi & Musa, Sarhan. (2018). Smart Contracts: A Primer.

