Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

Blockchain-Based Crowdfunding Platform

[1]vipul Gupta, [2]tushar Goel, [3]Ajay Pratap Singh, [4]MR. Vivek Kumar
[1,2,3,4]Dept. of CSE, MIET, Meerut

Abstract: Crowdfunding has revolutionized fundraising for startups and social organizations by shifting from traditional approaches involving banks and investors to online platforms hosted on social media or dedicated websites. However, the proliferation of fraudulent fundraisers and illicit investors has eroded trust among governments and social workers. The emergence of blockchain technology in recent years has introduced a promising solution, ensuring fraud-free transactions between investors and fundraisers. Numerous blockchain-based crowdfunding initiatives have successfully raised funds through cryptocurrencies. This study focuses on a crowdfunding platform that harnesses the power of blockchain technology to facilitate decentralized, fast, and secure transactions. By employing arbitrary nodes within a network pool, this platform aims to overcome the challenges posed by fraudulent activities and establish a trustworthy ecosystem for fundraising. This research explores the implications, benefits, and potential challenges of such a blockchain-based crowdfunding system in the context of modern fundraising dynamics.

Keywords: Blockchain; Crowdfunding; Decentralize; fundraising; Ethereum

1. Introduction

1.1 Overview

Crowdfunding (CF) is a widely used method for raising funds, often in small increments, from a broad audience, or "the crowd," to support various financial needs, including business ventures, social causes, loans, or often financial requirements, through dedicated online platforms [1]. Fundraising is a complex process that hinges on trust among multiple stakeholders, including donors, intermediaries, and organizations that act as custodians of donated funds. Trust is the cornerstone of fundraising, serving as the bedrock upon which investors place their faith and financial support in recipients. This research delves into the processes that empower investors in fundraising endeavors through the application of blockchain technology. The objective is to automate the fundraising process, mitigating concerns related to fraud or misallocation of frauds. This is achieved through the use of smart contract technologies, which have applications not only in fundraising but also in sectors such as communication and healthcare. The utilization of blockchain technology significantly bolsters investor confidence and trust while enabling fund recipients to validate the legitimacy of funding sources, ensuring compliance with legal requirements. The research methodology employed in this study is primarily library research, drawing from international and national periodicals and related works to provide a solid foundation for the investigation.

1.2 Background History

1.2.1 Blockchain

The first cryptocurrency, known as Bitcoin, was introduced in 2009 and served as a marker for the blockchain. After ten years, distributed ledger technology has become the most frequently used idea in the world. Currently, 46% of all cryptocurrencies in trade are made up of Bitcoin. But there is much more to learn about the core idea of Bitcoin. The word "Blockchain" refers to the idea of continuously expanding recorded ledgers arranged like a linked chain [2]. It combines features of data integrity, traceability, security, and peer-to-peer decentralization.[5] In a linear blockchain, a normal block has three parts:

1. The hash value of the current block
2. Data value

3. The hash value of the previous block

The Genesis block is the name given to the initial block in a blockchain. It is devoid of the prior block's hash value. A block's value that has the previous block's hash value in it aids in the linear connection of two blocks.

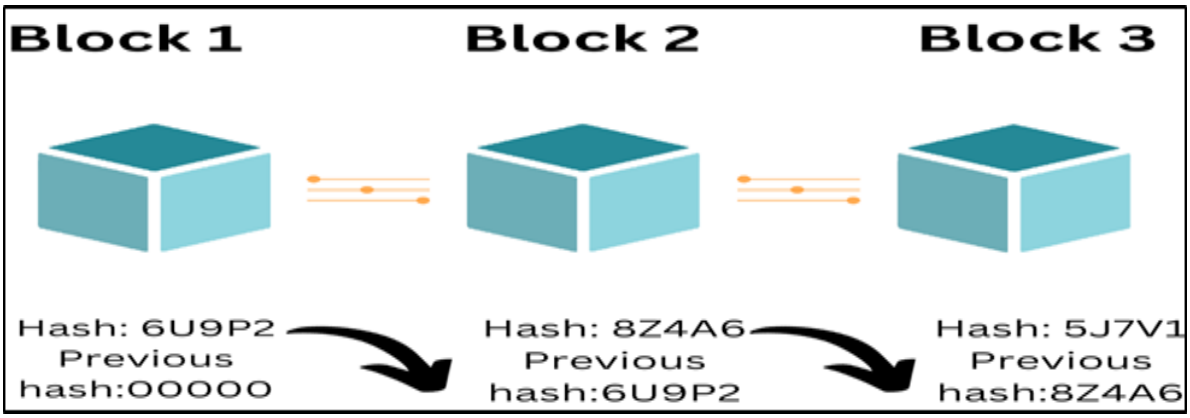

Fig. 1 A typical blockchain network is displayed

1.2.2 Cryptography

The study and application of methods for protecting data and communication from adversaries is known as cryptography. [11] It entails developing and evaluating systems, protocols, and algorithms that guarantee the privacy, accuracy, and legitimacy of data. A vital component of contemporary computers and information security is cryptography. In order to guarantee the secrecy, integrity, and validity of data, cryptography is essential to the security of information systems. It is used in many different domains, such as digital signatures, secure communication, authentication, and sensitive data security.

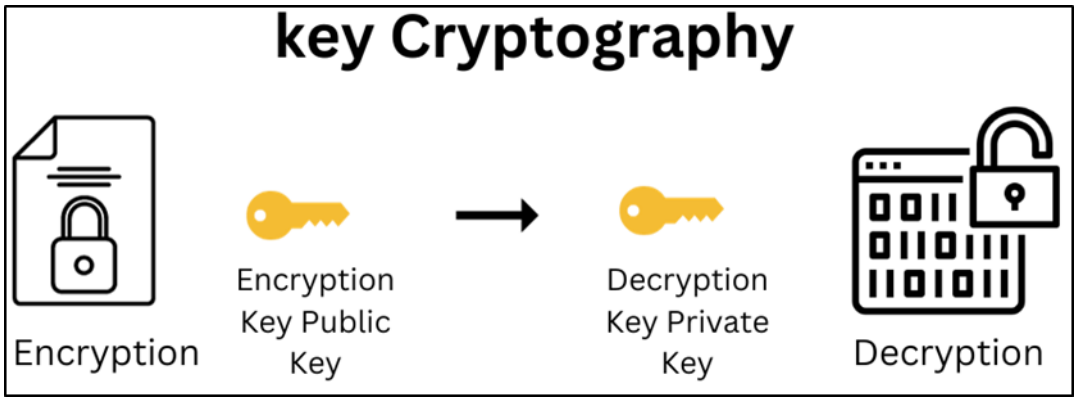

Fig. 2 The idea behind key cryptography

1.2.3 Smart Contract

A self-executing contract known as a "smart contract" has the conditions of the buyer-seller agreement encoded directly into the code. [13] It is powered by a blockchain, a distributed, decentralized ledger that keeps track of transactions over a computer network. Smart contracts eliminate the need for middlemen by enabling automated and trustless agreement implementation. Smart contracts are used in many different industries, including supply chain management, real estate, banking (particularly in decentralized finance, or DeFi), and more. By automating the execution of agreements in a safe and decentralized manner, they have the ability to optimize workflows, lower expenses, and boost the effectiveness of complex transactions.

1.3 Supported Technologies and Algorithms

Technology Used:

Python serves as the backbone of our application, providing a robust and flexible programming environment. Leveraging the capabilities of blockchain technology, your project ensures secure and transparent data storage and transactions. For the user interface, HTML lays the foundation of our web pages, while CSS and Bootstrap contribute to styling and responsiveness, delivering a visually appealing and user-friendly experience.

Consensus Algorithms:

Proof of Work (PoW): Used in blockchain networks like Bitcoin, where participants (miners) solve complex mathematical problems to validate transactions and create new blocks.

Proof of Stake (PoS): Participants create new blocks and validate transactions based on the number of coins they hold and are willing to "stake".

Cryptography for Security:

This technology is used for secure key generation, digital signatures, and encryption within blockchain networks. RSA facilitates secure key generation and digital signatures, ensuring the authenticity of transactions, while SHA-256 enhances data confidentiality through effective encryption methods. Together, these cryptographic techniques contribute to the overall integrity and security of blockchain-based systems.

2. Traditional Crowdfunding Workflow

In the world of fundraising, each fundraising group often operates with its own unique set of guidelines and procedures. However, at its core, [9] the fundraising process is intricately connected to four primary entities: the donor, the fundraiser, the depository fund (typically a bank), and the fund receiver. Below is a high-level overview of how these entities interact within a fundraising organization:

1. **Donor:** Donors are individuals or entities willing to contribute funds to support a cause, project, or organization. They play a pivotal role in the fundraising process as the source of financial support.
2. **Fundraiser:** Fundraisers are individuals, organizations, or platforms responsible for initiating and managing fundraising campaigns. They create a compelling narrative to attract potential donors, promote the cause, and facilitate the collection of funds.
3. **Depository Fund (Bank):** The depository fund, often a bank or financial institution, serves as an intermediary in the traditional fundraising process. It is responsible for receiving and securely holding the funds donated by individuals or organizations. Funds are typically held in dedicated accounts to ensure transparency and accountability.
4. **Fund Receiver:** The fund receiver is the beneficiary of the fundraising campaign. This entity could be a non-profit organization, a business venture, a charitable cause, or an entity in need of financial support. They rely on the funds collection to achieve their goals and objectives.

3. Proposed Work Plan

Crowdfunding is made of three processes:

3.1 All-or-Nothing

All-or-nothing (AON) is a crowdfunding model where a fundraising campaign sets a specific funding target that must be reached within a predetermined time frame[6]. If the campaign does not reach this target by the specified deadline, then the project creators do not receive any of the funds pledged, and the money is returned to the backers or funders.

3.2 Keep-It-All (KIA)

The “Keep-It-All” (KIA) crowdfunding model is a system where project creators get to keep the funds they raise, regardless of whether they meet their funding target or goal. In other words, if a crowdfunding campaign is set up with a KIA model, project creators will retain all the funds pledged by backers, even if the campaign doesn’t reach the intended target[6,9].

3.3 Stretched Goals Scheme (SGS)

The “Stretched Goals Scheme (SGS)” is a crowdfunding model where the fundraising goal is designed to expand as the campaign progresses. The Key points to this scheme can be summarized as follows:

- Initial fundraising goal
- Predetermined additional values
- Fundraising goal expansion
- Action on goal achievement.

In other words, if the campaign meets its initial funding target and subsequent milestones, the project creators are obliged to incorporate the specified additional value into the project or deliver the promised enhancement.

These three are the three main processes of the crowdfunding fund generation mechanism.

3.4 Data Flow Diagram of Proposed System

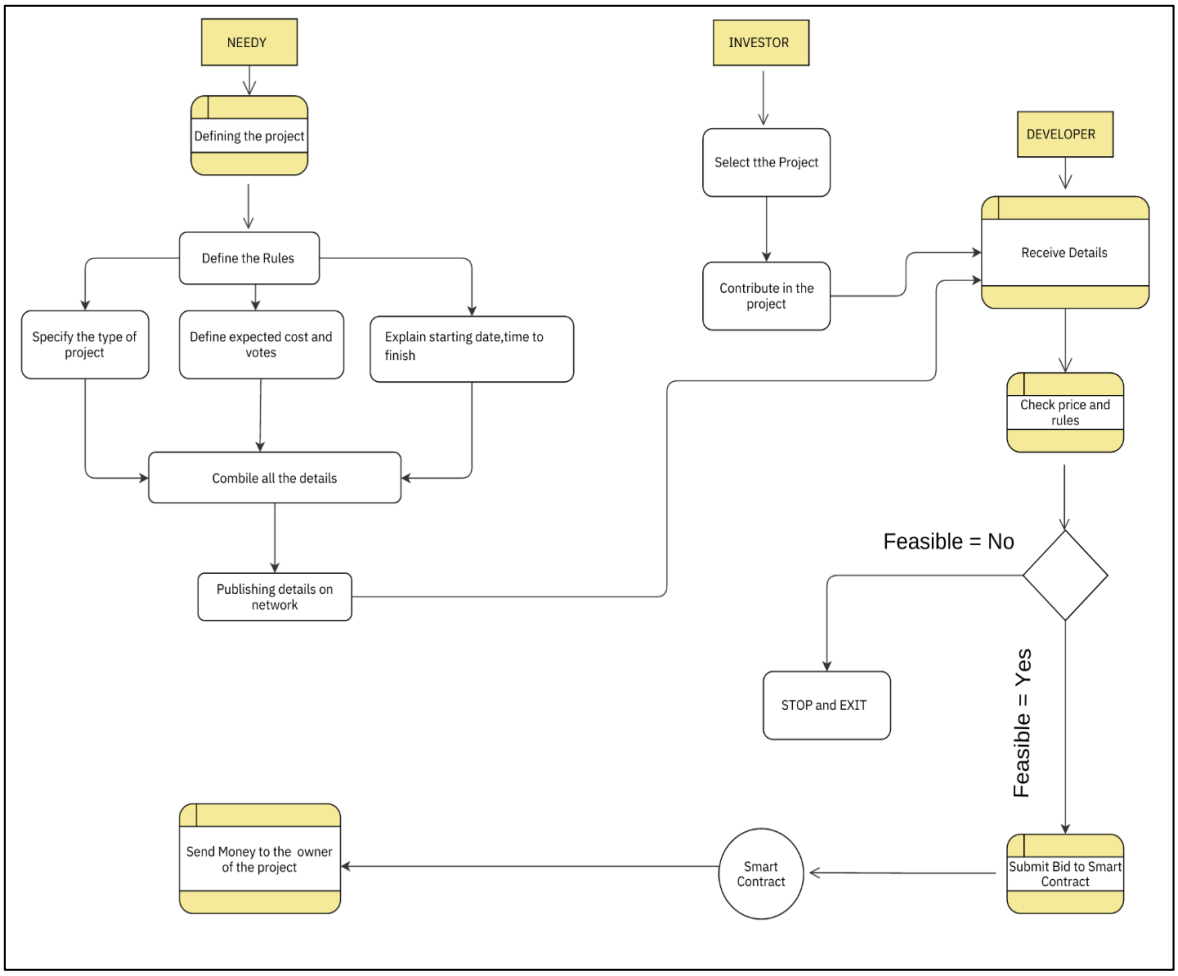

Fig. 3 DFD of the proposed system

4. Results

4.1 Wallet

The wallet is created to store the history of transactions done by the investor. So, it helps the investor to have a record of all the funding he/she did.

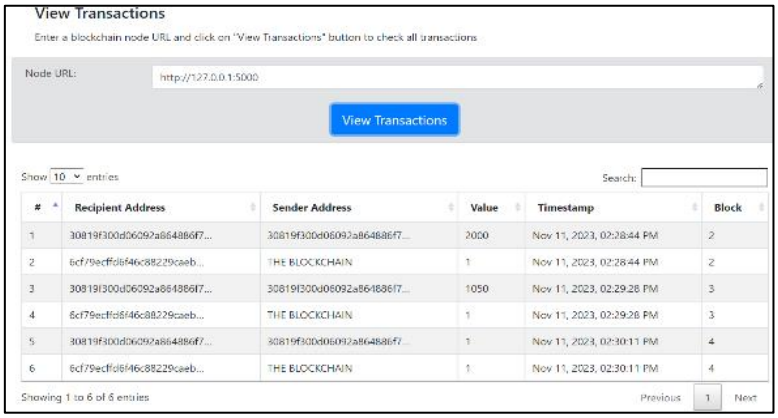

Fig. 4.1 Showing stored transactions in the wallet

4.2 Implementation:

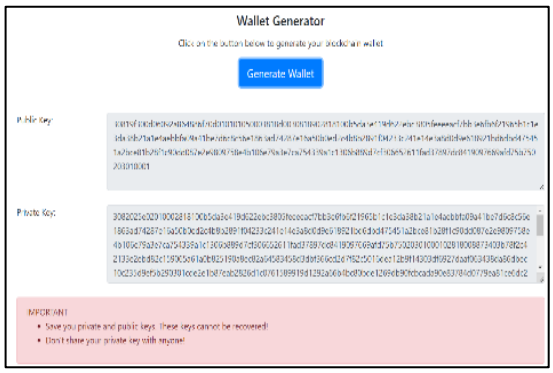

Fig. 4.2a Generated public and private key

Fig 4.2 b Details Page

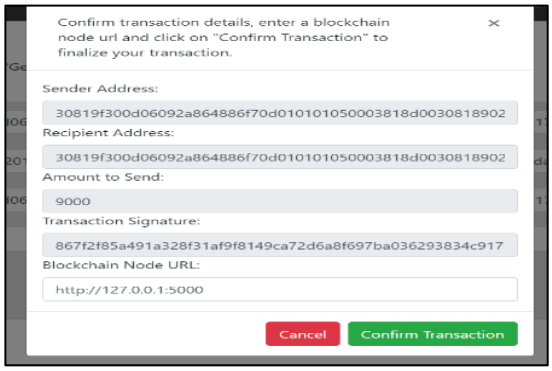

Fig. 4.2 c Confirmation Page

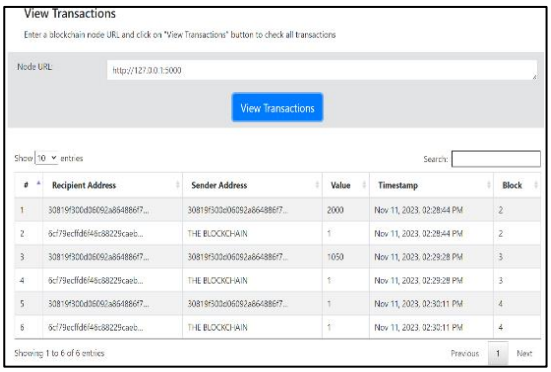

Fig. 4.2 d Transactions History

A wallet is generated which stores and shows the transaction data of the user done in a crowdfunding platform. So, it helps the user to keep track of all his transaction data history.

5. Conclusion

In summary, blockchain technology offers several advantages for fast and secure fund transfer within a fund generation platform, benefitting society in various ways. Ultimately, it is determined that blockchain-based crowdfunding is a relatively new idea within the ICT world. Up till now, the solidity compiler has been used to successfully write and compile the solidity code for the campaign contract. Bytecode was the Solidity compiler's output, and the interface was implemented into the blockchain. A decentralized web application with a UI for starting new projects, adding to existing ones, submitting new requests, approving requests, and completing requests is made once the project is deployed. The blockchain's application to crowdfunding is currently in its exploratory phase, requiring the resolution of certain legal and technical obstacles. Our suggested work has a bright future and plenty of room for development given the advancement of blockchain. In the future, any ideas realized through the suggested crowdfunding application will be able to advance the research project in a more straightforward and secure manner.

References

[1] Koch, Jascha, Siering, Michael "THE CHARACTERISTICS OF SUCCESSFULLY FUNDED PROJECTS ON CROWDFUNDING PLATFORMS"
[2] Anjee Gorkhali (2020) "BLOCKCHAIN: a literature review"
[3] Wackerow, "Ethereum Documentation: Introduction to DAPPS"
[4] Zhao, H., & Coffee, C.P. (2018). The application of blockchain technology in Crowdfunding Contracts.
[5] Isha Purushottam, Jeevanjot Singh, K P Sajith, Kaarnik Jamwal, Sarthak Kumar (2022) "Crowdfunding dApp: Blockchain-based fundraising protocol"
[6] Starkenmann Oliver implementation of crowdfunding Decentralization application of Ethereum Master Thesis, ResearchGate.
[7] Dianovics, Z. & Majd, N.E. (2021, March 3). Coin Crowder: An accountable blockchain decentralized application (DAPP).
[8] Jenik, I., Lyman, T., & Nava, A. (2017). Crowdfunding and financial inclusion. CGAP (Consultative Group to Assist the Poor) Working Paper.
[9] Keyes, C. F., & Daniel, E. V. (Eds.). (1983). Karma: An anthropological inquiry. Univ of California Press.
[10] Kirby, E., and S. Worner. (2014). Crowd-Funding: An Infant Industry Growing Fast. Madrid: IOSCO, Retrieved in December 2018.
[11] Gurdeep Singh, Prateek Kumar, Nishant Taneja (2019) "A Research paper on Cryptography"
[12] Buterin, Vitalik et al. 2014. "A next-generation smart contract and decentralized application platform"
[13] P.B. Kumbharkar, Rushikesh Palaskar, Satyam Yenegure, Geetank Asati, Aditya Valekar "Fund Crypt: Blockchain based Crowdfunding Platform using SHA-256 & POS Algorithm", 2023 2nd International Conference on Edge Computing and Applications (ICECAA), 2023
[14] Lijing Zhou, Licheng Wang, Yiru Sun, Pin Lv. "BeeKeeper: A Blockchain-based IoT System with Secure Storage and Homomorphic Computation", IEEE Access, 2018
[15] Siddhesh Bajad, Sonali Patil, Kartikesh Ambavade, Rohini Pise. "Voting Based CrowdFunding Using Ethereum Blockchain", 2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), 2023
[16] Rajiv Kumar, Manisha Saini, Ajeet Kumar Vishwakarm, Ruby Faizan, Divya Rawat, Deepak Negi. "Navigating the Blockchain Landscape: Role, Challenges, Risks, and Issues in the Banking and Finance Sector", 2023 IEEE 5th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA), 2023
[17] Hamed Taherdoost "Smart Contracts in Blockchain Technology: A Critical Review"