International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Research Paper Volume-9, Issue-4 ,2022 Regular Edition E-ISSN: 2349-7084

Fundraising through Blockchain

Vishakha Shelke[1*], Smit Khakhkhar[2], Yash Jani [3]

[1*] *Dept. Computer Engineering, Universal College of Engineering, Vasai, India*
[2] *Dept. Computer Engineering, Universal College of Engineering, Vasai, India*
[3] *Dept. Computer Engineering, Universal College of Engineering, Vasai, India*

e-mail: vishakha.shelke@universal.edu.in, smitkhakhkhar@yahoo.in, janikyash64@gmail.com

**Corresponding Author: janikyash64@gmail.com,*

Available online at: http://www.ijcert.org

Received: 13/04/2022, Revised: 17/042022, Accepted: 17/April/2022, Published: 18/04/2022

Abstract:- After China, India has the world's largest MSMEs (Micro, Small and Medium Enterprises) sector. MSMEs account for over 30% of GDP, a figure that has been stable in recent years. Unfortunately, 99.5 percent of MSMEs remain microenterprises, and have always found it difficult to grow for a variety of reasons. One major cause is the difficulty of raising funds or attracting investments. Approaching formal sources of money would benefit greatly if the economy became more formalized. They are currently confronted with significant obstacles that prevent them from approaching these sources. The most significant issue that businesses and individuals with brilliant ideas confront is that investors are hesitant to participate in their ideas due to concerns about the safety of their assets. Individual investors are wary of investing in startup ideas because of the countless online scams. There are a few drawbacks to online investment, like security, hacking, and exit scams. Money trials are not available to investors, and they have no understanding how their money is being spent. As a result, our suggested solution is a truly trustless decentralized system in which investors do not have to worry about their money being misappropriated. Investors own all of their funds outright, and every expense must be approved by the investors through a governance vote. Unlike traditional banks, all fund transfers and expenditures are accessible to everyone, resulting in a better money trail.

Keywords: Decentralized, Blockchain, Investments, Full Control, and Governance Vote.

---

1. Introduction

Raising funds for a business is a complex endeavor, and because of the countless online frauds, ordinary individuals are skeptical of investing in startup ideas. While there are a few drawbacks to online investment, such as

security, hacks, and exit scams, the major issue that companies/people with good ideas face is that investors are hesitant to engage in their idea due to concerns about the safety of their cash. As a result, the suggested system is a truly trustless decentralized system in which investors do not have to worry about their money being misappropriated.

Companies confront numerous challenges when using traditional fundraising methods to rise funding. As a result, we devised the concept of leveraging Blockchain Technology to raise funds. Because of its rapid advancement, Blockchain technology shows no indications of slowing down. Excessive transaction costs, double payments, internet fraud, lost data recovery, and other seemingly incredible things have proven wrong over the last few decades. However, thanks to blockchain technology, it may be possible to avoid all of this.

Blockchain is a distributed ledger (database) of immutable records called blocks that allows data to be securely stored globally. The data is kept in chronological sequence, and it cannot be modified once it has been recorded.

The following are some of the key advantages of incorporating Blockchain technology into your company: It's an immutable public digital ledger, which means transactions can't be changed once they've been recorded. Blockchain is always secure due to its encryption function. Because the ledger is updated automatically, the transactions are instantaneous and transparent, and because it is a decentralized system, no intermediary cost is required. A transaction's legitimacy is verified and validated. The banking industry is being disrupted by blockchain, which provides a peer-to-peer payment mechanism with the highest security and lowest fees. Blockchain technology enables quick and cross-border payments all around the world.

Due to the peer-to-peer connections, which cannot be tampered with, blockchain immediately identifies harmful assaults. Every piece of data saved on the blockchain network is validated and encrypted using a cryptographic method. Blockchain provides a transparent and secure manner of recording transactions by eliminating the need for a centralized system (without disclosing your private information to anyone).

2. Related Work

The system framework presented by Xuan Luo et al is made up of two layers: onchain and offchain. The on-chain layer is critical for the protection of users' assets. Both the HEX user and the HEX system must deposit a particular number of tokens into the smart contract in order to use the bi-directional payment channel. The creation of a new payment channel between the user and the HEX, or the addition of funds to an existing payment channel between the user and the HEX, is triggered by a user deposit. After that, the HEX user can use the HEX to sign off-chain trading transactions.When a user requests a withdrawal, both the user and the HEX agree to shut the payment channel and send the close transaction to the smart contract [1].

Proof-of-Work (PoW) in Blockchains (BC) is a commonly used consensus algorithm that suffers from high power consumption by miners and low transaction speeds, according to Sina Rafati Niya et al. This paper shows how to use Bazo, a Proof-of-Stake (PoS)-based BC that is specifically built and customized for IoT data streams. In comparison to PoW-based BC, Bazo performs better in terms of energy consumption and transaction processing [2].

Robert Norvill, Mathis Steichen, Wazen M. Shbair, and Radu State developed a method that allows for document sharing between banks to be automated and simplified. It was created with the goal of reducing the amount of duplicate and onerous labor that the KYC procedure necessitates. The demonstration demonstrates how the system works. It depicts how the system works from both the customers' and the banks' perspectives. The analysis of data leakage and duplication issues, for which several solutions have been explored, will be part of future work. [3].

Blockchain technology, according to Chaehyeon Lee of el, has the virtue of allowing a network to be maintained without the involvement of a third party while also enabling transparency because all players have distributed ledgers with the same data. Blockchain technology is being employed in a variety of areas because of these properties, yet the anonymity of blockchain can be exploited for criminal trading in the Darknet market. As a result, a mechanism to track transactions on the blockchain is required. This work presents a monitoring system as well as an explorer to display the system's results [4]

The system framework described by Sina Rafati Niya et al. gives us an idea of how we may use Supply Chain Tracking to monitor our various supply chains (SCT). It is seen as a significant challenge for parties involved in diversified production, processing, transportation, storage, and distribution systems. Many centralized SCT applications lack a design that can support or even enable major aspects of a dependable, transparent, and publically accessible SCT system for end users, according to studies on SCT solutions. This research shows how to create an SCT application that uses SC on the Ethereum network (BC)[5].

According to Santosh Pandey et al, blockchain technology includes dangers that need to be carefully examined and understood prior to design and development. Given the purely distributed nature of blockchain, where nodes can span continents, consideration of eventual consistency, system stability, and scalability when designing blockchain-based systems is a key aspect in planning and designing blockchain systems that is not readily incorporated in a modern architect's vernacular.[6]

Malicious behavior during blockchain consensus, threats to reputation systems, and excessive TX latency, according to Imran Makhdoom et al, are all major challenges for blockchain-based IoT systems. To address these issues, we offer "Pledge," a one-of-a-kind consensus technique based on Proof-of-Honesty. Pledge appears to be cost-effective in terms of computations, communications complexity, and transaction confirmation latency, according to preliminary testing [7].

Ryo Kawahara has developed a formal approach for confirming a blockchain protocol's customisable consensus rule. To accommodate a variety of blockchain applications, Hyperledger Fabric provides an application-specific, adjustable consensus rule called endorsement policy. However, this makes ensuring qualities like Byzantine fault tolerance problematic. [8].

We learn how to develop our Smart Contract and how to automate the procedure easily and carefully from the research work of Felix Franz et al. We discovered The blockchain technology is gaining traction because to its unique properties, which include security, immutability, transparency, and the elimination of middlemen. But it isn't just cryptocurrencies that are addressed. Smart contracts are regarded as a promising blockchain-based application.[9]

During our study, we discovered that the UN is developing an electronic "ePhyto" certificate system that will be controlled by the UN (UN). The national plant protection organization (NPPO) of the exporting country sends an ePhyto certificate to the NPPO of the importing country. The UN system establishes a secure channel of communication between pre-registered NPPOs. Industry participants who are not connected to the UN system, on the other hand, are unable to verify the authenticity of an ePhyto certificate or if it has been canceled or renewed.[10]

Because the act of interleaving blocks stored in multiple shards to build a unified master ledger generates overhead, the traditional method to scalability, namely sharding, does not simply fix the problem. Strong temporal coupling and weak temporal coupling are two strategies for interleaving the shards of permissioned blockchains discussed in this study. We use the EPaxos consensus protocol for transaction ordering to apply these strategies in a prototype system with a Bitcoin-like transaction structure.[11]

3. Methodology

3.1 Proof of Stake (POS)

Proof Of Stake (PoS) blockchain ranks stakers in descending order of the amount of tokens staked, Every state change on the blockchain is done using a transaction. Be it the fun-raiser or investor, a transaction has to be signed with a private key and broadcasted to the network, along with signature data, namely, V, R, S values. The transactions are then propagated to all the nodes within a matter of seconds, the node which has staked the most number of tokens packs all the transactions in a block and verifies it's signature data V,R,S and then broadcasts the block, which is then added to the local blockchain. In case the the node acts malicious and packs a fraudulent transaction, all other nodes could chose to reject the block, leading to hard fork of the network triggering a re-org, the new blockchain will then be free of any malicious blocks The transaction can be safely assumed to be confirmed, once the blockchain height is +15 than the block in which the transaction was confirmed.

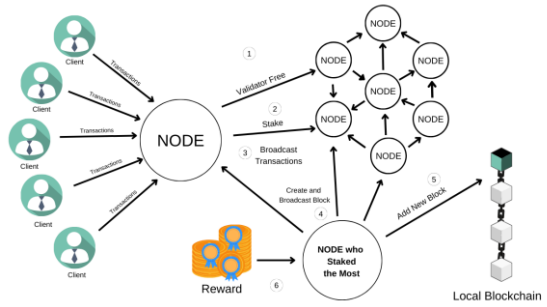

Figure 1 - Transaction confirmation methodology

3.2 Proposed System

Polygon's POS chain is one of the most active EVM chains, having processed over 1082.95 million transactions in less than a year, averaging close to 50.1 Transactions Per Second (TPS). Users who want to raise money for their ideas can go to the website and connect their Metamask wallet to start a project. The fundraiser must describe his idea, how the funds will be used, if there will be a working prototype, how long the project will take to complete, Budget and Burn sheets, and the amount of money that will be raised.

3.2.1 The proposed system is made up of six parts.

- Fund Raise Proposal
- User investments
- Funds locked into Vault
- Expense request by Fund Raiser
- Consensys voting by investors to approve the request
- Outcome of vote.

1. Fund Raise Proposal

Since it is a decentralized system, anyone can submit a fundraising proposal without waiting for approval.

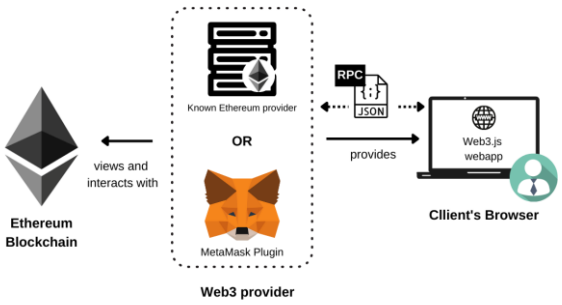

Figure 2 - Metamask Connection

Figure 2 shows how the user must connect their Metamask wallet to the website and provide information about the project, including the amount to raise, the Burn sheet, the project timeline, the Funds utilization sheet, and images about the project.

2. User investments

Figure 3 shows how the Investors need to connect their Metamask wallet with the website with funds, Investors can invest in any project listed on the website, without approval, without any minimum fund or minimum commitment, however, investors can invest more than 50% of the total fundraise so as to keep the system decentralized.

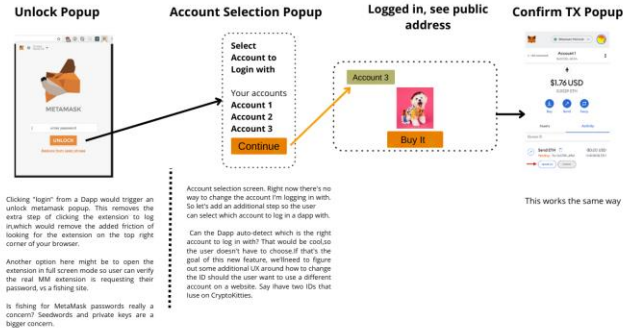

Figure 3 - Metamask transaction confirmation

3. Funds locked into Vault

After the fundraise deadline is reached all the funds are transferred to a safekeeping vault for future use.

4. Expense request by Fund Raiser

Whenever a fundraiser wants to spend the funds, they raise an expense request, stating the reason for expenditure, amount and payment address, which can then be approved by the investors, in case it isn't approved, the request is rejected and the funds aren't spent, hence making the system truly decentralized.

5. Consensys voting by investors to approve the request

Investors have to vote for the expense request before the deadline, after which their voting right for the expenses request ceases.

6. Outcome of the vote

After the deadline, the votes are calculated by the smart contracts, if the votes in favor are greater than 51%, the expense request is approved and the funds are sent to the provided address, in case the request fails, the funds stay as it is.

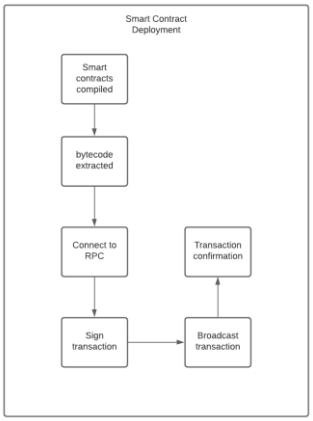

Figure 4 - Deployment Diagram

Figure 4 shows the deployment process which involves compilation of smart contracts with maximum optimization, we then extract the bytecode and connect to a reliable RPC, transaction is signed and broadcasted to the RPC, once the transaction is confirmed and included into a block, the smart contract can be used on the frontend.

4. Results and Discussion

4.1 Proposed System Result

The developed Proposed system will help common as well as institutional investors invest funds in a decentralized manner without the need to worry about the funds or seeking theft insurance, there isn't any entry barrier compared to the traditional system, unlike traditional banks where you are required to meet a set criteria, Decentralized Finance is a truly revolutionary system in that sense.

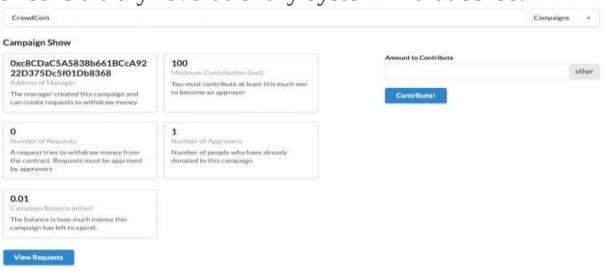

Figure 5 - Webapp

Figure 5 shows the frontend of the webapp where all the open fund requests are visible, along with total funds raised and backers.

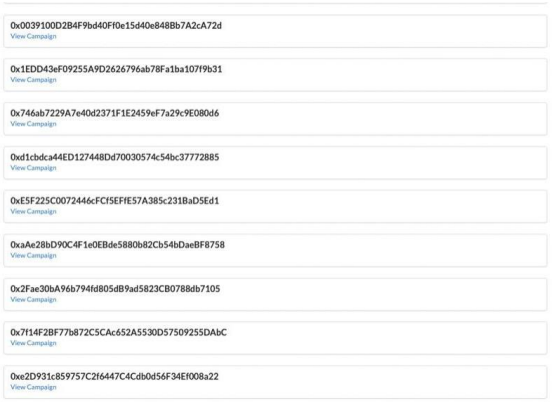

Figure 6 - Proposed system fundraiser page

Figure 6 depicts the GUI showing details about the fund proposal, including images, comments, number of investors and funds raised.

4.2 Qualitative analysis of proposed system versus existing system

Table 1 - Comparison of existing system and proposed system.

Parameter	**Existing System**	**Proposed System**
Trust factor	Low - due to centralizing nature	high - due to decentralized nature
Funds	Transferred to fundraiser	Locked in a smart contract
Provision for expenses	No provision	Every expense has to be approved
Traceability	The funds are managed by traditional banks so no direct access to transactions	All transactions occur on the blockchain so every fund transfer is visible
Fraud Chances	High	Zero
Cyber security concerns	Prone to cyber threats as the code is hosted on a centralized server	No Cyber threat as the code is immutable and stored on the blockchain
Emergency close	No provision	Investors can call an emergency vote to nullify a fundraise and receive their funds back

5. Conclusion

Blockchain is one of the hottest new technologies on the market right now, attracting a lot of attention from corporations, start-ups, and the media. Blockchain is best recognised as the backbone technology behind Bitcoin. Blockchain technology has the potential to transform a variety of industries and processes by making them more democratic, secure, transparent, and efficient. Even though the technology is still in its infancy, financial players are among the first to take advantage of it.

We can execute transactions faster for better customer service, ensure cost effectiveness in operations, and ensure transparency to customers and regulators using Block chain. With massive volumes of data being generated every day as a result of record digitization, it is critical for all enterprises to efficiently manage security threats and gain significant cost savings.

Because of its rapid advancement, Blockchain technology shows no indications of slowing down. Excessive transaction costs, double spending, internet fraud, recuperating misplaced data, and different apparently incredible matters have been proved to be fake withinside the previous couple of decades. All of this, however, may also probably be prevented by Blockchain Technology.

Acknowledgement

We would like to thank our Campus Director Dr.J.B.Patil, our HOD Dr. Jitendra Saturwar and our project guide Mrs.Vishakha Shelke for guiding us throughout the project and to bring the best out of us.

References

[1] Xuan Luo, Wei Cai, Zehua Wang, Xiuhua Li, and Victor C. M. Leung, "A Payment Channel Based Hybrid Decentralized Ethereum Token Exchange,"presented at the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea (South), 14-17 May 2019, pp. 49-50.

[2] Sina Rafati Niya, Eryk Schiller, Ile Cepilov, Fabio Maddaloni, K¨ursat Aydinli, Timo Surbeck, Thomas Bocek,

Burkhard Stiller , "Adaptation of Proof-of-Stake-based Blockchains for IoT Data Streams ,"presented at the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea (South), 14-17 May 2019, pp. 15-16.

[3] Robert Norvill, Mathis Steichen, Wazen M. Shbair, Radu State, "Demo: Blockchain for the Simplification and Automation of KYC Result Sharing," presented at the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea (South), 14-17 May 2019, pp. 9-10.

[4] Chaehyeon Lee, Heegon Kim, Sajan Maharjan, Kyungchan Ko and James Won-Ki Hong, "Blockchain Explorer based on RPC-based Monitoring System ", presented at the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea (South), 14-17 May 2019, pp. 117-119.

[5] Sina Rafati Niya, Danijel Dordevic, Atif Ghulam Nabi, Tanbir Mann, Burkhard Stiller, "A Platform-independent, Generic-purpose, and Blockchain-based Supply Chain Tracking", presented at the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea (South), 14-17 May 2019, pp. 11-12.

[6] Santosh Pandey, Gopal Ojha, Bikesh Shrestha, Rohit Kumar, "BlockSIM: A practical simulation tool for optimal network design, stability and planning", presented at the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea (South), 14-17 May 2019, pp. 11-12.

[7] Imran Makhdoom, Farzad Tofigh, Ian Zhou, Mehran Abolhasan, Justin Lipman., "A Proof-of-Honesty based Consensus Protocol for Blockchain-based IoT Systems", presented at the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2-6 May 2020.

[8] Ryo Kawahara, (2017), "Verification of customizable blockchain consensus rule using a formal method", presented at the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2-6 May 2020.

[9] Felix Franz, Tobias Fertig, Andreas E. Schutz, "Democratization of Smart Contracts: A Prototype for Automated Contract Generation", presented at the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2-6 May 2020.

[10] Qinghua Lu, Mark Staples, Hugo O'Connor, Shiping Chen, Adnene Guabtni, "Software Architecture for Blockchain-based Trade Certificate Systems", presented at the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2-6 May 2020.

[11] Chunyu Mao, Anh-Duong Nguyen, Wojciech Golab, "Performance and Fault Tolerance Trade-offs in Sharded Permissioned Blockchains", presented at the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2-6 May 2020.

Authors Profile

Mrs. Vishakha Shelke Currently working as an Assistant Professor and Head of Data Engineering department at Universal College of Engineering, Mumbai. She is pursuing a PhD in computer engineering at RAIT, DY Patil University in Navi Mumbai, after graduating with an M.E. in computer engineering from Savitribai Phule Pune University. She has 12 years of experience as a teacher. Social network analysis, Big data analytics, Machine Learning, and Artificial Intelligence are some of her areas of interest.

Mr. Smit Khakhkhar is a B.E. Computer Engineering student at Universal College of Engineering, which is affiliated with the University of Mumbai. Blockchain technology, Artificial Intelligence are some of his areas of interest.

Mr. Yash Jani is a B.E. Computer Engineering student at Universal College of Engineering, which is affiliated with the University of Mumbai. Web development, Blockchain technology, CryptoCurrency, Machine Learning, and Artificial Intelligence are some of his areas of interest.

