

Empowering Entrepreneurs: The Potential of Blockchain-Based Crowdfunding

Aruna A¹, Reni Hena Helen R², Sanjay A³, Jeevanandham⁴, Saran A⁵

Computer Science Engineering, Dhanalakshmi College of Engineering, Chennai, India^{1,2,3,4,5}

Abstract: Crowdfunding using blockchain is a decentralized funding model that utilizes blockchain technology to increase transparency, security, and efficiency in the fundraising process. With blockchain's immutable ledger and smart contracts, crowdfunding platforms can enable secure and transparent fundraising without intermediaries. Blockchain-based crowdfunding offers several advantages over traditional models, such as reduced fees, faster processing times, and greater accessibility for both fundraisers and investors. By leveraging smart contracts, crowdfunding platforms can automatically enforce the terms of the fundraising campaign, such as the targeted contribution amount and deadline. If the targeted amount is reached, the smart contract can automatically end the campaign and distribute the funds to the intended recipients. In the event that the targeted amount is not reached within the deadline, the smart contract can automatically expire the campaign and return the donated amount to all contributors. This ensures that contributors are not left out of pocket if the project is not successful. Blockchain-based crowdfunding can also help democratize access to funding, enabling entrepreneurs and creators to reach a wider audience and raise capital for innovative projects. In addition, the use of blockchain technology can provide greater transparency and accountability, as all transactions are recorded on an immutable ledger. Overall, crowdfunding using blockchain has the potential to revolutionize the fundraising landscape, providing a more accessible, secure, and efficient alternative to traditional models. By leveraging the power of blockchain technology, crowdfunding platforms can provide a more democratic and transparent way for entrepreneurs and creators to fund their projects, while giving investors greater access to investment opportunities.

Keywords: Blockchain, Ethereum, Smart Contracts, Crowdfunding.

I. INTRODUCTION

Blockchain technology is most simply formed as a decentralized, distributed book that records provenance of a digital asset. By natural to design, the facts on a blockchain are unable to be made different, which makes it a within the law disruptor for industries like payments, cybersecurity, and state of health care. blockchain is an especially hoping and revolutionary technology because it helps reduce risk, stamps out fraud and brings transparency in a scalable way. Crowdfunding approach faucets into the collective efforts of an outsized group of individuals primarily online via social media and crowdfunding platforms and helps their networks for bigger reach and exposure. Crowdfunding is actually the other of the thought approaches to business finance. Historically, if you desire to lift money to begin a business or launch a brand-new product, you'd have to be compelled to clean up your business arrange, marketing research, and prototypes, so look your plan around to a restricted group or moneyed people or establishments.

In the process of raising funds, of undertow it is not easy, considering it requires trust between many parties, both the funders, intermediaries, or organizations as a place to store temporary funds to the recipient of funds. Trust is the main capital for fundraising organizations to vamp funders to donate their funds to recipients of funds. Trust is their challenge in attracting contributors to contribute their money to the organization. Not a few also a non-profit organization that uses technology to make it easy for contributors to contribute funds through them. In addition to trust which is the main factor to get as many funds as possible, technology also plays a big role in this as well. The blockchain is an incorruptible digital book that records every transaction. It is a distributed system in which all the records are stored in every node in the decentralized network. Crowdfunding provides an easy way to find funds for innovative project ideas.

The problem with the current crowdfunding companies is that they charge upper fees and sometimes there were scams happened. Implementing a crowdfunding strategy in blockchain will help to avoid these types of problems.

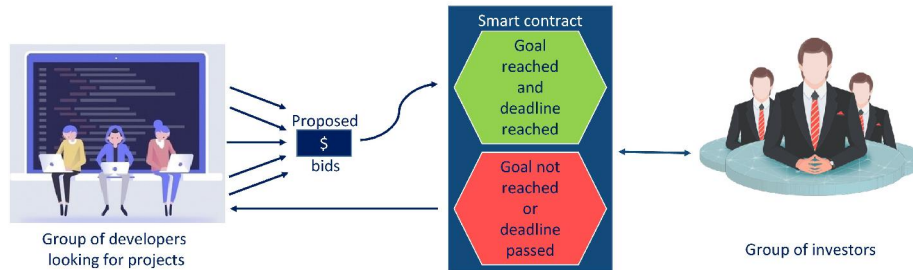


Figure 1 Blockchain, smart contracts and an iterative auctioning algorithm connects appropriate developers and investors cost-effectively and securely.

Bitcoin garnered enormous popularity in recent years and has become a household name. However, most of the people are not aware of the underlying technology blockchain that powers bitcoin. Bitcoin is a decentralized digital currency not regulated by any central bank or a single administration, it can be sent from a user-to-user on the peer-to-peer bitcoin network without the need for intermediaries. Transactions (movement of bitcoin from one account to another account) are verified by the nodes connected in the network through cryptography and recorded into a public distributed ledger called blockchain. Bitcoin was created by an anonymous person or a group of people going by the name Satoshi Nakamoto and released in the year 2009 as an open-source software. Bitcoins are rewarded to the nodes connected in the network when they perform a process called mining. Bitcoins are now accepted in various places for exchange of local currency, goods or services.

Bitcoin is the forerunner to Ethereum, which is a blockchain that has more functionality than Bitcoin and is the backbone of this project. Not just Bitcoin and Ethereum every crypto currency is powered by Blockchain technology hence it is important for us to explore in detail how Blockchain works. First let's get an idea about the transaction system in Bitcoin which gives us a base for understanding the transaction system in Ethereum, followed by description of blockchain that is core to both Bitcoin and Ethereum.

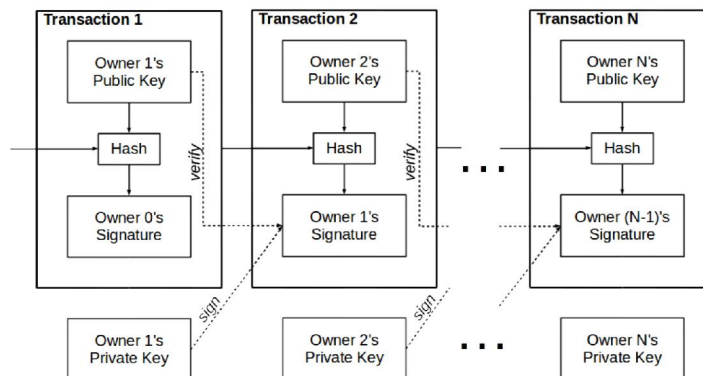


Figure 2 Bitcoin transaction chain of ownership

A “proof-of-work” algorithm run by “miners” in the blockchain peer-to-peer network makes decision regarding which transaction and order of transactions to be included in a block. Miners receive transactions from Bitcoin users and use those transactions to “mine” a block. Miner who successfully mines a block will be rewarded with bitcoin as an incentive for spending his resources such as computing power and time. To mine a block, a miner takes a part of previous block's hash, all the new transactions that are received in sequence and an integer called a nonce as shown in Figure 2 a simple blockchain structure.

If the value of the hash is below a certain threshold (that determines the difficulty of mining which results in average block time) then the block is successfully mined else the miner increases nonce and recomputes hash to see if it is below the threshold. The first miner who is able to compute the hash is rewarded, then he will broadcast the result to other miners in the network who will validate it and run the transactions in the block to get the current state of blockchain. This process repeats and new transactions that arrive are persisted in the blockchain. Although this algorithm is essentially just busy work at its core, it makes the system secure because the proof-of-work aspect means that an attacker cannot just spawn an army of virtual machines to take control of the blockchain. He must have to take control of more than half of the computational power present in the network to control the state of the blockchain. In addition to this, it serves to establish a digital crypto currency that does not require a third party to oversee the validation of the transaction by using the busy work to bring about a consensus on the system's state.

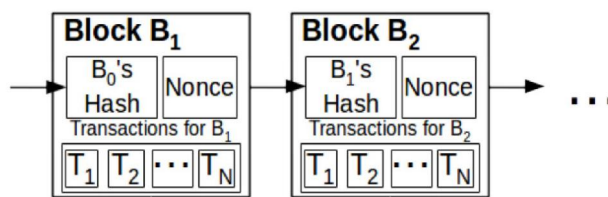


Figure 3 A simple blockchain structure

Ethereum is an open-source public distributed computing platform and operating system based on blockchain technology first used by Bitcoin. Ethereum extends the usefulness on Blockchain well beyond cryptocurrencies by making the blockchain programmable according to developer's needs. It was proposed by a cryptocurrency researcher VitalikButerin in his whitepaper published in the year 2013, where he states the intention of Ethereum is to provide, "a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that are used to encode arbitrary state transition functions".

These features make it the apt choice for building truly decentralized applications similar to this project and many other decentralized applications (dapps). Although Ethereum blockchain is much more advanced and intricate, it is still based on the same principles as Bitcoin's. Ethereum similar to Bitcoin also uses a proof-of-work algorithm run by a peer to peer distributed network to find consensus on the current state of the system, with the miners being rewarded in Ether(crypto currency used by Ethereum network). Network gets transactions from users distributed across the globe and the proof of work algorithm at regular intervals determines a sequence of those transactions to be included in the next block in the blockchain. Every new block added to the chain. determines the state of the system. The block creation time in case of Ethereum averages around 14 seconds while that of Bitcoin averages around 10 minutes, both operate on the same set of core principles of blockchain.

The major difference in Ethereum is the complexity of both, the state stored by the blockchain and how the transactions can alter the state of the blockchain. Ethereum's state mainly consists of objects called accounts located by 20-byte address . There are two types of accounts, externally owned accounts and contract accounts. Externally owned accounts or EOAs can be accessed by private keys similar to Bitcoin and have a field to store the current ether balance of that account. Contract accounts or CAs similar to EOAs have additional fields to store the contract code and storage. As CAs are a part of contracts, their interaction with other accounts and how they access or modify their storage are controlled by the owning contract. The contract storage is a key value store of data persistent among transactions. Unlike externally owned accounts, contract accounts cannot initiate transactions on their own.

A transaction must have recipient address, a signature identifying the sending account and amount of Ether transferred from sender to recipient. This information is enough to move value from one account to another account either in case of CA or EOA. Even though contracts cannot create transactions they can send "messages" to other contracts. Messages are similar to transactions but it takes place between two contracts, by a CA triggering a function in its contract code, than EAO and CA.

Similar to transactions they do contain a message sender, a message recipient, amount of ether to transfer and an optional data field to call a function in the recipient's contract code. The actual state changes are done by the Ethereum virtual machine (EVM) upon receiving a transaction, by running the low-level contract bytecode. A fascinating concept called gas is used to by EVM to operate; it can be thought of as fuel purchased to execute a transaction. Bitcoin also allows scripting for complicated transactions but it is not turing-complete like Ethereum. Ethereum solved a major problem that Bitcoin had by finding a solution to transactions that involve loops. In case a transaction consisted of an infinite loop then calculating the state would be impossible, computational time would be massive, that can create problems for the blockchain.

Ethereum's fairly simple solution to overcome this problem was to have a cost for each transaction that it executed. For every transaction a user creates the amount of gas required for the transaction to be processed is purchased from the ether balance in the sender's account at an arbitrary price, typically the market price at that moment (the amount of gas sent directly affects the transaction processing time as the miner running the Ethereum blockchain get that gas amount is a incentive for mining so higher amount create higher incentive). Every bytecode operation done in the EVM costs a certain integer amount of gas, operations such as modify or add to contract storage are the most expensive because all those changes are persisted on the blockchain forever. The gas starts depleting when a transaction starts executing and stops if it completes or runs out of gas. If the transaction completes and some gas is left behind then it is refunded back to the transaction sender. However, if it terminates because of gas amount depleted to zero then no ether is returned and the transaction fails. High-level smart contract languages used to write smart contracts, that compile to bytecode executed by the EVM, and make writing a smart contract simple.

Solidity, a smart contract language, chosen for this project due to the support available in developer community, object oriented features and syntax similar to JavaScript. Writing a contract in solidity is similar to writing a class in other object oriented programming languages with functions, member variables and interacting with other contracts. The most important feature of a smart contract is their permanence and the immutability of the smart contract code. The access to a function in a contract can be restricted by using modifiers that make it impossible for a developer to call that function if his address does not have the privileges. Even if he adds code to permit his address to call the function, he will not be able to change the contract code once deployed. This might sound like a burden but there are certain important considerations why this was done. Smart contracts are digital version of written contracts, hence as written contracts cannot be modified after signed, Ethereum contract code is like a digital contract specifying, with the logical certainty of code, the exact behavior of the contract account, which can be seen as a kind of autonomous entity on the blockchain.

This is required for building applications that are based on completely trustless model where even the developer cannot manipulate once it is deployed, especially when the application involves money. An initial Ethereum dapp that took advantage of the complete trustless model was "The DAO" (decentralized autonomous organization). It was all built using smart contracts that users could invest in, make proposal, cast votes on the proposal based on the investments, get rewarded based on the weight of the investments when a proposal succeeds and lot more [9]. It was a wildly successful app raising \$150 million from user investments, but it was hacked in mid 2016 and lost \$50 million of the investments due to a flaw in the code So no matter how well intentioned a smart contract is, if it is badly coded then it is quite similar to poorly written hand contract and can be exploited by hackers. Ethereum was the perfect choice for this project "Crowdfunding dapp" that creates an environment for people to raise money for their dream project. With the smart contracts present, the application can store and manage user account data, store metadata and users can interact with the smart contracts using transactions created by project's client application. Ethereum makes the smart contracts always available, accessible anywhere and restrict control to people who are only authorized to use them. It can achieve this because of the underlying technology "blockchain" first used in Bitcoin.

II. LITERATURE REVIEW

Online crowdfunding enables people to raise funds for their project. People who are interested in a project can donate by making an online transaction. The donated money goes to the project manager, which he uses to complete the project or to make a product. This existing method of online crowdfunding has a major drawback. It does not allow

contributors to have control over the money they have contributed. Since in the existing method the project manager has all the control over the money contributed, he can very easily perform malicious activities.

Here we address this problem faced by the existing online crowdfunding platforms by using Ethereum network and smart contract.

The development of Blockchain technology has allowed businesses to build decentralized models. It has derived new methods to conduct transactions and make agreements. One of the technologies that propose an alternative to the traditional model is the smart contract. A smart contract is similar to a contract in the physical world, but it is digital and represented by a tiny computer program stored in a blockchain. These smart contracts can be used to implement logic. A method has been proposed here that uses smart contract to manage all the activities performed in a crowdfunding campaign. The proposed method has been implemented and its various features are tested by funding campaigns on hardhat test network.

Figure below (figure. 5) shows a list of continuously growing records called blocks. Each Block is linked to each other and they were secured using cryptography. Blockchain has the characteristics of integrity, decentralization, Immutability, Security, Anonymity. Consensus protocol is what which keeps the blocks on all the node to synchronize with each other.

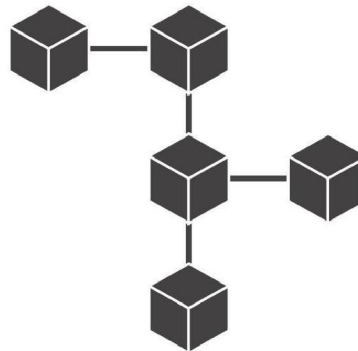


Figure 5

III. PROPOSED METHODOLOGY

The proposed system would allow entrepreneurs to create crowdfunding campaigns on a blockchain-based platform, such as Ethereum. The campaigns would be managed through the use of smart contracts, which would automate the process of accepting and distributing funds.

Donors would be able to contribute to campaigns using cryptocurrencies or other digital assets, with the smart contract automatically recording the contribution and updating the total amount raised. The smart contract would also specify the target amount to be raised, the deadline for reaching this target, and the rules for distributing funds.

If the target amount is not reached by the deadline, the smart contract would automatically return the funds to the donors. If the target amount is reached, the campaign would end, and the funds would be distributed according to the rules set out in the smart contract.

The use of blockchain technology would provide several benefits over the traditional crowdfunding model. Donors would have greater visibility into how their funds are being used and distributed, with the transparency and immutability of the blockchain ensuring that there is no room for fraud or misappropriation of funds.

The use of smart contracts would also reduce the need for intermediaries, reducing fees and increasing efficiency. The decentralized nature of the blockchain would ensure that there is no central point of control that could be hacked or compromised, providing greater security for donors and fundraisers alike.

Overall, the proposed system would offer a more transparent, efficient, and secure way for entrepreneurs to raise funds, and for donors to contribute to worthy causes.

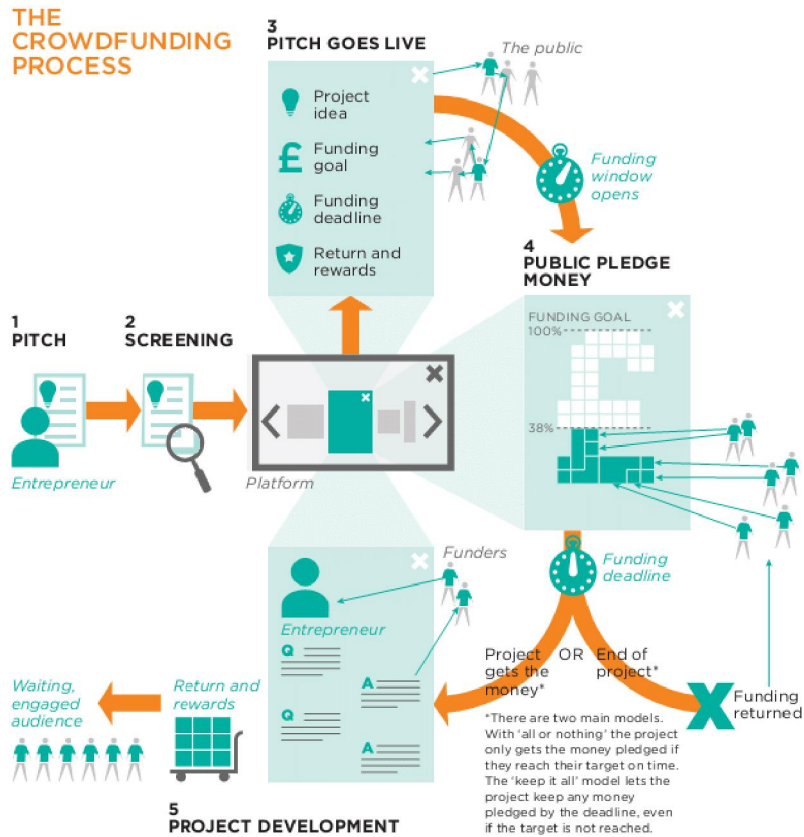


Figure 6: Crowdfunding campaign process

IV. IMPLEMENTATION

Crowdfunding dapp is divided into various activates a user can perform in the platform. Anyone who lands on the platform can browse through all the campaigns listed and explore more about each campaign. The application extensively uses Javascript libraries to build the user interface, handle user inputs and communicate with Ethereum network. The application is built on model view controller architecture so that there is clear distinction on each layer’s responsibilities. The landing page uses Campaign Registry contract to get all the campaigns registered on the platform. Once it gets the campaigns then it accrues campaign related data from IPFS and builds the user interface of the landing page. Next section gets into the details of Campaign Registry contract and user interface implementation.

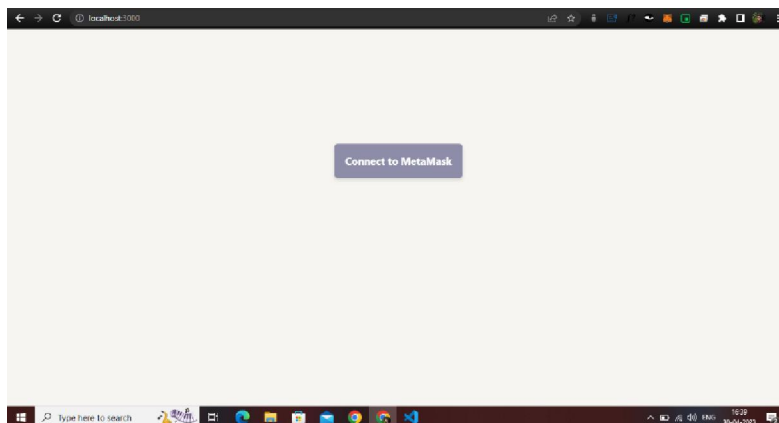


Fig 7. Home page

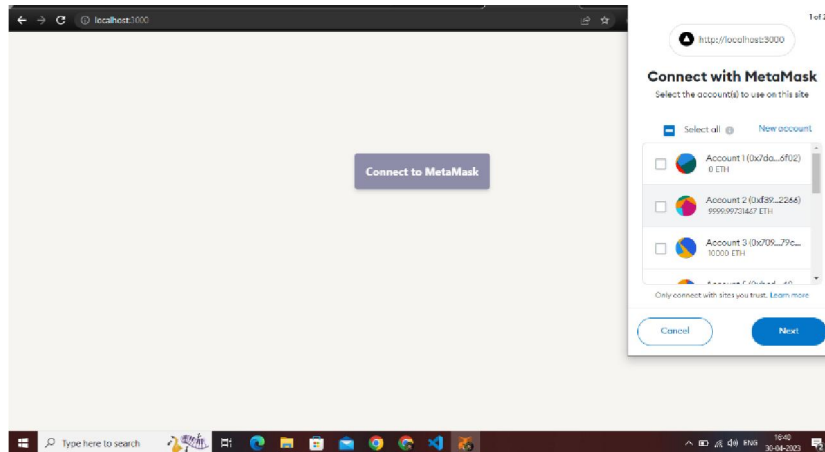


Fig 8. Connect with MetaMask

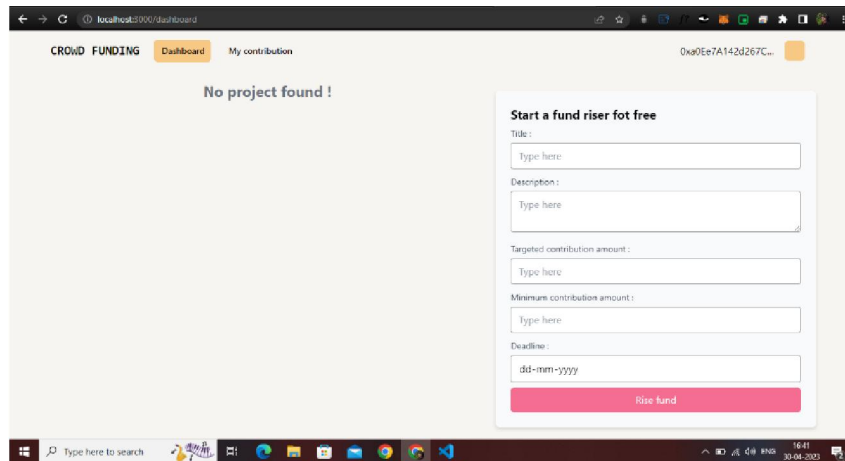


Fig 9. Campaign Creation

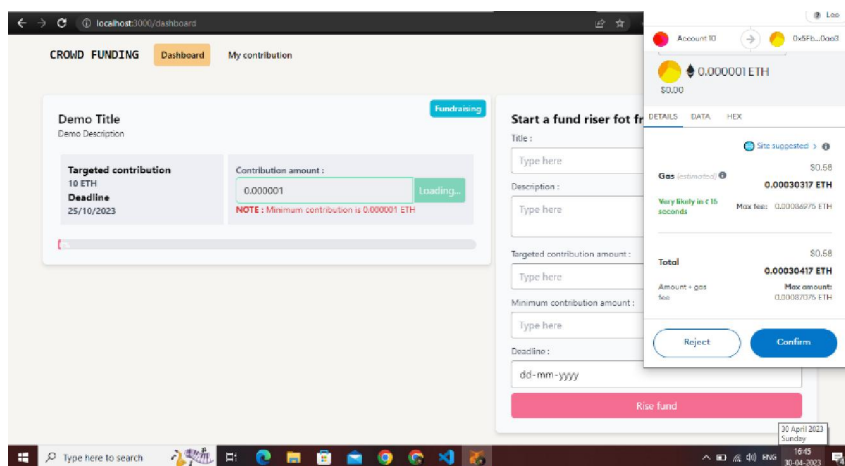


Fig 10. Money Contribution

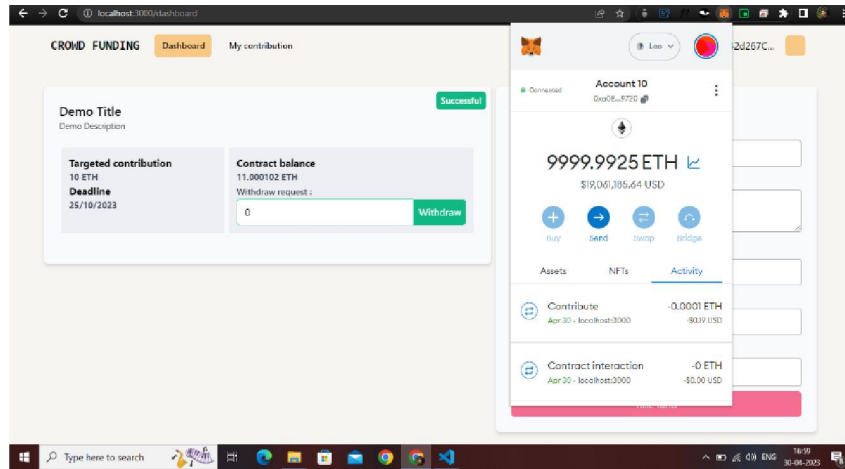


Fig 11. Withdraw Request

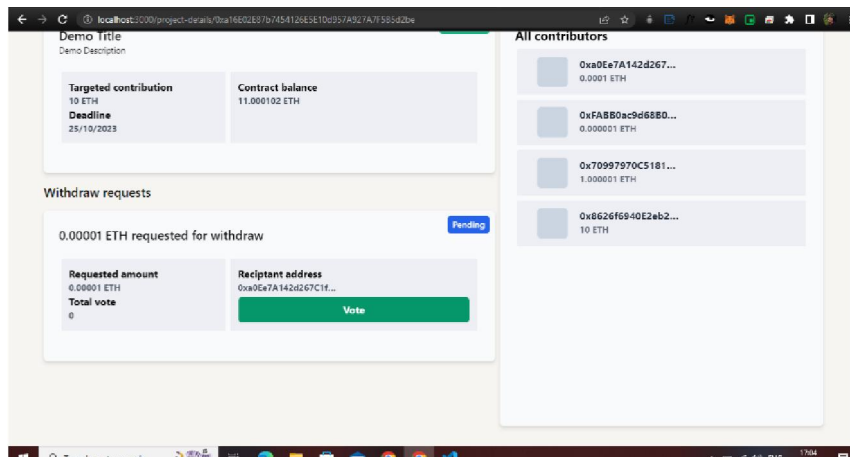


Fig 12. Voting for Withdraw Request

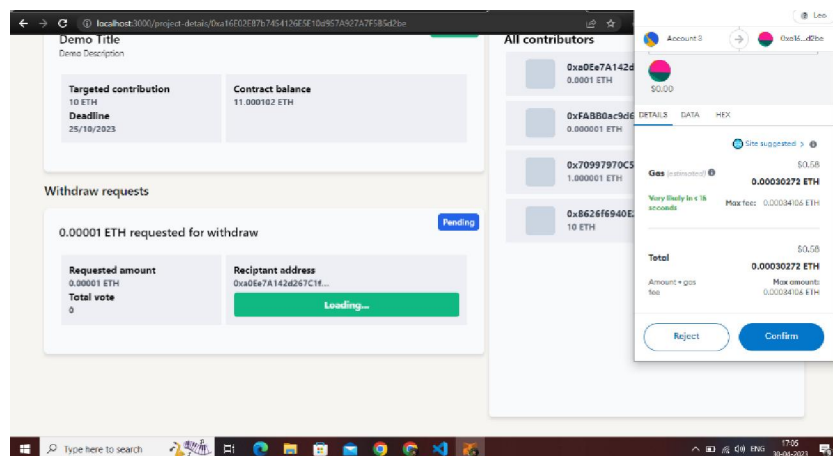


Fig 13. Accept / Reject the Withdraw Request

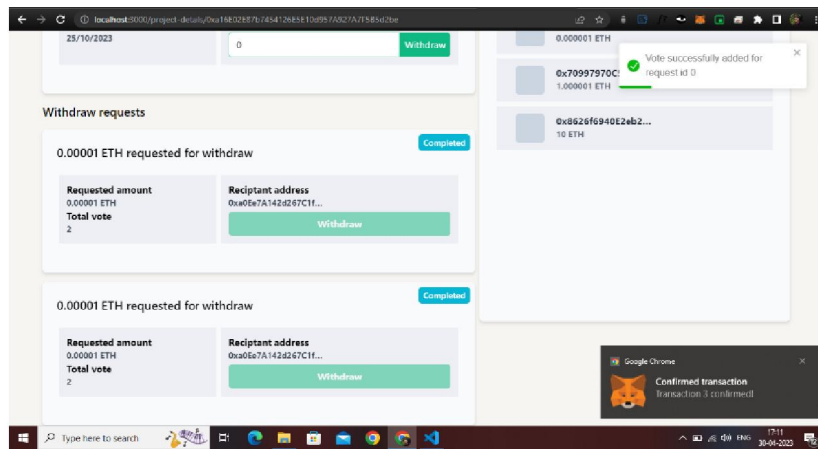


Fig 14. Withdraw Request Completed

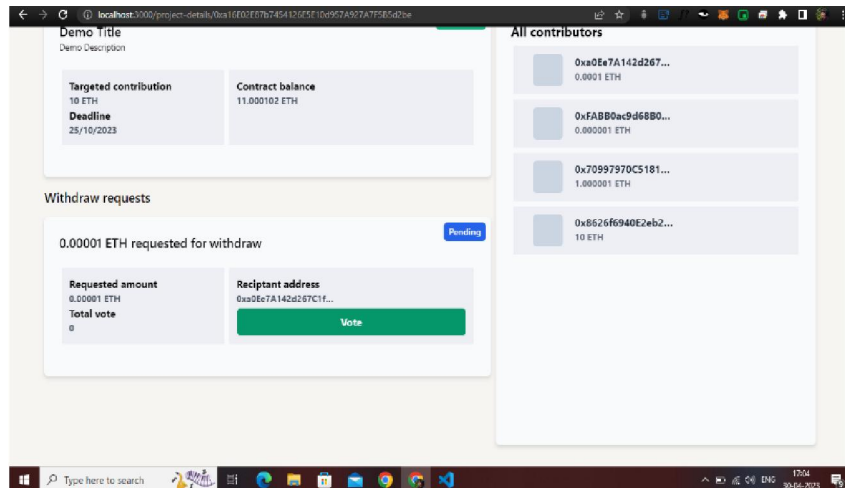


Fig 15. Contributors

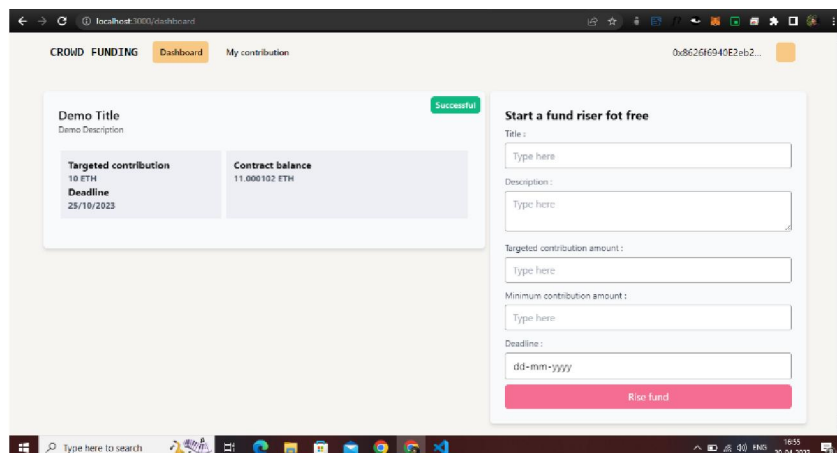


Fig 16. Campaign Completion

V. CONCLUSION

As the world is moving towards Web 3.0 and decentralized systems to solve their daily problems, it is important to test and build new alternative architectures that show us the ideology to provide innovative solutions. With the existing solutions in the crowdfunding world created and handled by intermediary corporations that have a say on various parameters of a campaign, the alternative solution based on peer-to-peer network handling the campaign transactions seems ripe. This project explores ways to remove intermediaries in a crowdfunding business use case. This was done with the help of smart contracts, written for the crowdfunding dapp application deployed in Ethereum blockchain, that guide the execution of a transaction. This interaction allows users to create and invest ether into campaigns that interest them.

Without much efforts campaign creators and campaign investors can perform their intended activities using the crowdfunding platform. There are new emerging blockchain platforms such as EOS, Stellar, Cardano and NEO [17] that provide more language choices and platform configuration choices compared to Ethereum but these platforms haven't proved themselves yet. EOS looks like a promising platform and in future this project can be moved to EOS if it proves to be a better choice than Ethereum.

REFERENCES

- [1] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *Ieee Access*, vol. 4, pp. 2292–2303, 2016.
- [2] Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, "A blockchain based truthful incentive mechanism for distributed p2p applications," *IEEE Access*, vol. 6, pp. 27 324–27 335, 2018.
- [3] V. Hassija, V. Chamola, S. Garg, N. G. K. Dara, G. Kaddoum, and D. N. K. Jayakody, "A blockchainbased framework for lightweight data sharing and energy trading in v2g network," *IEEE Transactions on Vehicular Technology*, 2020.
- [4] Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna, G. Jourjon, and A. Seneviratne, "A delay-tolerant payment scheme based on the Ethereum blockchain," *IEEE Access*, vol. 7, pp. 33 159–33 172, 2019.
- [5] D. Puthal, N. Malik, S. P. Mohanty, E. Kougiannos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18–21, 2018.
- [6] V. Hassija, G. Bansal, V. Chamola, V. Saxena, and B. Sikdar, "Blockcom: A blockchain based commerce model for smart communities using auction mechanism," in 2019 IEEE International Conference on Communications Workshops (ICC Workshops), May 2019, pp. 1–6.
- [7] A. C. Chapman and G. Verbič, "An iterative on-line auction mechanism for aggregated demand-side participation," *IEEE Transactions on Smart Grid*, vol. 8, no. 1, pp. 158–168, 2017.
- [8] F. You, J. Li, J. Lu, and F. Shu, "On the auction-based resource trading for a small-cell caching system," *IEEE Communications Letters*, vol. 21, no. 7, pp. 1473–1476, 2017.
- [9] Y. Yuan and F.-Y. Wang, "Blockchain and cryptocurrencies: Model, techniques, and applications," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1421–1428, 2018.
- [10] W. Chen, Z. Zheng, E. Ngai, P. Zheng, and Y. Zhou, "Exploiting blockchain data to detect smart ponzi schemes on ethereum," *IEEE Access*, 2019.
- [11] Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna, G. Jourjon, and A. Seneviratne, "A delay-tolerant payment scheme based on the Ethereum blockchain," *IEEE Access*, vol. 7, pp. 33 159–33 172, 2019.
- [12] K. R. Ozyilmaz and A. Yurdakul, "Designing a blockchain-based IoT with ethereum, swarm, and lora: The software solution to create high availability with minimal security risks," *IEEE Consumer Electronics Magazine*, vol. 8, no. 2, pp. 28–34, 2019.
- [13] J. Liu, W. Li, G. O. Karame, and N. Asokan, "Toward fairness of cryptocurrency payments," *IEEE Security & Privacy*, vol. 16, no. 3, pp. 81–89, 2018.
- [14] World Bank, "Crowdfunding's Potential for the Developing World," <https://www.infodev.org/infodev-files/wb-crowdfunding-report-v12.pdf>, online; accessed 29 January 2019.
- [15] U.S. Small Business Administration, "Research on the Current State of Crowdfunding," <https://www.sba.gov/advocacy/research-current-state-crowdfunding>, online; Accessed 01 May 2019.

- [16] Statista, “Transaction value in the Crowdfunding segment,” <https://www.statista.com/outlook/335/109/crowdfunding/united-states>, online; accessed 11 March 2019.
- [17] V. Hassija, V. Chamola, G. Han, J. Rodrigues, and M. Guizani, “Dagiov: A framework for vehicle-to-vehicle communication using directed acyclic graph and game theory,” *IEEE Transactions on Vehicular Technology*, 2020.
- [18] V. Hassija, V. Chamola, D. Nanda Gopala Krishna, and M. Guizani, “A distributed framework for energy trading between uavs and charging stations for critical applications,” *IEEE Transactions on Vehicular Technology*, 2020.
- [19] S. Car`e, A. Trotta, R. Car`e, and A. Rizzello, “Crowdfunding for the development of smart cities,” *Business Horizons*, vol. 61, no. 4, pp. 501–509, 2018.
- [20] E. Lins, K. J. Fietkiewicz, and E. Lutz, “How to convince the crowd: An impression management approach,” in *2016 49th Hawaii International Conference on System Sciences (HICSS)*. IEEE, 2016, pp. 3505–3514.
- [21] W. Wang, K. Zhu, H. Wang, and Y.-C. J. Wu, “The impact of sentiment orientations on successful crowdfunding campaigns through text analytics,” *IET Software*, vol. 11, no. 5, pp. 229–238, 2017.
- [22] M. Li, J. Weng, A. Yang, W. Lu, Y. Zhang, L. Hou, J.-N. Liu, Y. Xiang, and R. Deng, “Crowdbc: A blockchainbased decentralized framework for crowdsourcing,” *IEEE Transactions on Parallel and Distributed Systems*, 2018.
- [23] Pledgencamp, “Pledgencamp the next generation of crowdfunding,” <https://pledgencamp.com/>, online; accessed 11 March 2019.
- [24] C. Laurell, C. Sandstr`om, and Y. Suseno, “Assessing the interplay between crowdfunding and sustainability in social media,” *Technological Forecasting and Social Change*, vol. 141, pp. 117–127, 2019.
- [25] A. Motylska-Kuzma, “Crowdfunding and sustainable development,” *Sustainability*, vol. 10, no. 12, p. 4650, 2018.