




## Capitalizing on Blockchain Technology for Efficient Crowdfunding: An Exploration of Ethereum's Smart Contracts



Cynthia Jayapal<sup>1\*</sup>, Arputha Rathina Xavier<sup>2</sup>, Poonguzhali Arunachalam<sup>3</sup>

<sup>1</sup> Department of CSE, Kumaraguru College of Technology, Coimbatore 641049, India

<sup>2</sup> Department of CSE, B S Abdur Rahman Crescent Institute of Science and Technology, Chennai 600048, India

<sup>3</sup> Department of Electronics and Communication Engineering, Sri Sairam College of Engineering, Bangalore 562106, India

Corresponding Author Email: [cynthia.j.it@kct.ac.in](mailto:cynthia.j.it@kct.ac.in)

<https://doi.org/10.18280/ijssse.130415>

### ABSTRACT

**Received:** 27 March 2023

**Revised:** 9 July 2023

**Accepted:** 15 August 2023

**Available online:** 28 September 2023

#### Keywords:

*crowdfunding, blockchain, Ethereum, smart contracts, equity*

Blockchain technology, the bedrock of cryptocurrency, has evolved beyond its initial scope, paving the way for a plethora of decentralized, secure applications. The anticipation surrounding blockchain's potential to become the dominant technology orchestrating online transactions is growing, due to its ability to provide efficient and secure solutions for a diverse range of applications on a global scale. This study delves into the potential benefits of deploying blockchain technology in the realm of crowdfunding. In recent years, crowdfunding has emerged as an alternative route for start-ups to garner funds, presenting a less bureaucratic and simpler process. The conventional crowdfunding model entails a collective of individuals contributing minor sums to support a project or start-up, with the crowdfunding platform earning a commission to coordinate the needs of both funders and fundraisers. Nonetheless, blockchain technology could potentially enhance the crowdfunding process by introducing a decentralized, tamper-proof system comprised of interconnected nodes, thereby bolstering transparency, trust, efficiency, and convenience. To realize this potential, this paper proposes the application of Ethereum smart contracts to tackle prevalent issues in both Donation-Based and Equity-Based crowdfunding models. By adopting this approach, we hope to bring about greater transparency and efficiency to the crowdfunding process, thereby fostering an environment of trust that may catalyze further innovation in this space.

## 1. INTRODUCTION

Crowdfunding, characterized by the amalgamation of financial contributions from a vast cohort of individuals, empowers the public to support a variety of ventures, projects, and ideas by furnishing the necessary financial resources. This mechanism transcends the need to depend on traditional funding avenues such as banks, fostering a direct link between the fund providers and seekers. The evolution of this process has enabled the replacement of traditional financial institutions with large groups of individual investors, thereby reshaping the landscape of funding sources.

While the notion of a collective funding a project is age-old, the advent of the Internet has ushered in a novel iteration of this concept, thereby expediting and simplifying the fundraising process. Technological advancements have made it feasible to connect with a multitude of potential investors worldwide via a singular platform, thereby revolutionizing the fundraising paradigm. This disruption has obviated the reliance on traditional sources, enabling individuals to directly approach the public, who can then opt to support their idea or project financially. This process not only facilitates easier access to funds but also provides a valuable validation of their idea or concept through each transaction.

Blockchain-based crowdfunding offers an array of advantages over traditional methods, including increased speed, efficiency, automation, elimination of intermediaries,

flexibility, and immutability. However, the growth of crowdfunding in India has been impeded by several challenges, such as the hesitation of start-ups to utilize online platforms owing to concerns about the integrity, authentication, and commitment of global participants. Additionally, the lack of governmental support for online fundraising poses another hurdle. Central agents' commission fees, a significant drawback of traditional crowdfunding, can be mitigated by leveraging decentralized agents like blockchain technology. Despite these challenges, reward-based crowdfunding in India is experiencing an upswing. According to "Statista Market Insights", the annual growth rate of crowdfunding transaction values is projected to reach \$5.2 million by 2027. Blockchain, a decentralized distributed ledger, allows the storage of digital assets, such as cryptocurrency, in digital wallets. Facilitating secure and transparent transactions, smart contracts record all operations and make them accessible to any party without requiring a central agent. These contracts can incorporate real-world constraints and can be scripted in languages such as Solidity or Go (in the case of Hyperledger).

In this crowdfunding system, a smart contract is constructed to house the scripts executing various functions and is then stored on a decentralized blockchain. The individual seeking funding, hereafter referred to as the initiator, launches the project as either a donation-based or equity-based model. In the equity-based model, the initiator delineates the project's milestones and deadlines, after which donors can contribute

funds. Upon achieving the first milestone, which may include the hiring of employees and initiation of execution, the initiator can accept cryptocurrency or assets from the smart contract and update the next milestone, such as the completion of production. Should the project fail to meet the milestone, the funds are refunded to the donors. If the project proves successful, the initiator can reward the donors with a share of the profit, proportional to their contribution. In a donation-based model, even if the milestones are not met, the amassed funds are still allocated to the initiator.

## 2. LITERATURE

The novel and transformative technology of blockchain, characterized by its secure, transparent, and anonymous validation of transactions, poses a monumental shift in the realm of crowdfunding. This paradigm shift is largely facilitated by the aggregation of transactions in a decentralized digital ledger, eliminating the need for intermediaries, and thereby ensuring a degree of trust within the network [1]. A distinct feature of blockchain is the transparency of data stored on the ledger, allowing stakeholders to verify the authenticity of a project [2]. Blockchain technology, with its high operational efficiency and low cost, emerges as a potent alternative to traditional crowdfunding methods. The elimination of intermediaries in transactions, facilitated by decentralization, contributes to this efficiency. Data stored on the ledger is secure against unauthorized modification, ensuring accuracy and reliability, thereby instilling confidence in users [3]. The immutability of data, achieved through cryptographic links between transactions, makes it infeasible to alter any single transaction without modifying the entire chain. This feature underscores the integrity and security of data recorded on the blockchain, making it an ideal fit for applications requiring tamper-proof records [4].

Crowdfunding, a method of obtaining capital from a multitude of individuals primarily through online platforms, has witnessed a significant surge in popularity. This trend is largely attributed to the proliferation of the internet and social media, making it easier for people to connect and share information about their projects [5]. Changes in legislative frameworks over the past decade have facilitated a more conducive environment for crowdfunding activities, thereby contributing to their popularity [6]. Crowdfunding platforms offer several advantages, one being the connection with potential customers, thereby providing valuable feedback on the product or service offered [7]. According to recent studies, crowdfunding provides non-financial benefits as well, such as fostering better connections between inventors and funders globally, and allowing investors to access more information about the project in its early stages for informed decisions [8].

However, traditional crowdfunding platforms are not without their drawbacks. A significant concern is the risk of fraud, as contributors are exposed to such risks owing to the limitations of traditional legal and reputation security measures [9]. The use of blockchain technology in crowdfunding platforms has been explored to mitigate prevalent issues such as fraud, money laundering, and uneven information access [10].

Blockchain technology operates as a decentralized network characterized by the distributed storage of data across numerous computational units rather than a single central

entity [1]. The permanency of the data within a blockchain ensures an unalterable and auditable transaction history. Furthermore, anonymity is preserved for users as personal identification remains confidential within the network. These unique attributes lend blockchain to be a robust and reliable method for recording and verifying transactions. Each block within the chain encapsulates a collection of transactions, along with a distinct digital signature termed as a "hash." This hash not only provides a linkage to the preceding block in the chain but also safeguards the integrity of the data within the block. A blockchain system comprises two primary elements: transactions and blocks. Transactions, initiated by network participants, such as the transmission or receipt of digital assets, are documented and validated by the system. Blocks function as repositories for these transactions and incorporate additional pertinent information, such as the chronological order of transactions, the timestamp of block creation, and the hash of the prior block in the chain. Collectively, these components constitute a decentralized and secure digital ledger that facilitates the storage and transfer of information and assets, eliminating the requirement of intermediaries. Relying on cryptography and consensus algorithms, the blockchain system is engineered to resist tampering, thereby instilling a high degree of trust and transparency among all network participants [1]. In a blockchain system, the records of transactions, referred to as blocks, are cryptographically linked. This cryptographic connection renders the blocks impervious to alteration or deletion without triggering the notice of network participants [11]. The application of cryptography also guarantees that the information housed within the blocks is safeguarded against unauthorized access, thereby ensuring the privacy and security of network participants [12]. While the application of blockchain technologies offers numerous benefits, associated challenges cannot be overlooked. One salient concern emanates from the considerable power consumption and computational resources that the operation of these decentralized networks necessitates [13]. The expansive network of computers integral to the blockchain system demands a significant quantum of energy and computational power to validate and process transactions, thus rendering the technology resource-intensive [14].

A smart contract, a self-enacting digital agreement integrated within a blockchain network, constitutes a computer code that autonomously operationalizes the contract's terms upon the fulfillment of preordained conditions. The implementation of smart contracts obviates the necessity for intermediaries and ensures the programmed agreement is automatically executed, thereby enhancing security, transparency, and efficiency. In the context of crowdfunding, a smart contract can serve as a secure platform regulating the fund distribution between the project owner and the contributors. The contributors' funds are automatically held by the smart contract until a predetermined objective or date is achieved. Upon attainment of the goal, the funds are released to the project owner; otherwise, they are safely returned to the contributors. The literature also provides a definition of how access control policies should be incorporated into a smart contract [15]. The work of Satish Babu and Babu [16] illustrates the construction of a DApp over a smart contract, leveraging the capabilities of web3.0 to build a secure web interface enabling user interaction with the blockchain framework.

### 3. PROPOSED METHOD

#### 3.1 Problem statement

In the traditional way of centralized crowdfunding, a third party is involved for money transactions. In decentralized crowdfunding, there will be no third party member and our transaction is made between peer to peer connectivity over the distributed system using blockchain. The application is built on the Ethereum framework which is highly secured and is built on consensus algorithm. The idea is to store all digital tokens in a smart contract that runs on the Ethereum framework. Once the contract is deployed on the internet. We make use of API calls to send and receive data. Most of the transactions are carried out by Ethereum. So all our transactions are secured and helps us to donate and accept tokens based on the smart contract.

#### 3.2 Components of crowdfunding using blockchain

Crowdfunding applications include three major components namely an initiator, investor and the crowd funding platform. These are considered as organizational entities which have common communication channels and ledger. Chain code represents scripts to implement a prescribed interface by managing the ledger states submitted by an application. An Ethereum blockchain contract has a name of contract, state variable that defines contract state and collection of functions to carry out the smart contract.

The chain code handles the business logic as mutually agreed upon between the investors and the initiators and hence is considered as a smart contract. The state of this chain code is secured and is accessible only to the members and not by other chain codes and hence makes the crowd funding platform secure and authenticated. Figure 1 illustrates various components of crowd funding such as initiator, investor and platform.

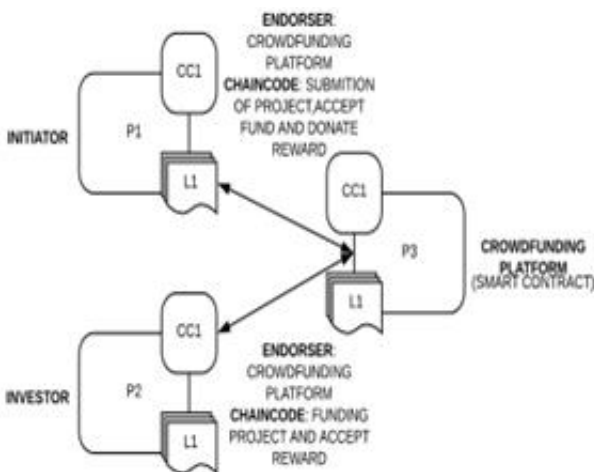


Figure 1. Components of crowdfunding

#### 3.3 Assets

The tangible asset of this application is the project. The project asset may include project title, project description, goal amount, type of project, milestone for the project, deadline for the project, list of investors for a project, investors contribution for a project and status of a project. Figure 2 depicts sample list of crowdfunding assets.

PROJECT
1.project title
2.project description
3.goal amount
4.type of project
5.milestone 1
6.deadline
7.list of investors
8.investor's contribution
9.status of project

Figure 2. Assets of crowdfunding

#### 3.4 Transactions

A smart contract is a self-executing computer program that automatically enforces and executes the terms of an agreement between parties in a decentralized manner, typically on a blockchain platform. The use of smart contracts in crowdfunding allows for transparent and secure management of funds and rewards. Transactions made using smart contracts are recorded on a distributed ledger, which is maintained and validated by a network of nodes. Each transaction is verified and settled across all nodes, and then stored in a block. The block is added to the blockchain after being validated and verified by a miner, who ensures the information contained within it is correct. Several types of transactions can be made using smart contracts in crowdfunding. These include createProject, fundProject, fundInitiator, contributeReward, acceptReward, updateMilestone, updateProgress, and refundInvestor.

The Ethereum network, which is one of the most popular blockchain platforms for smart contracts, uses ether as its native cryptocurrency. Ether is used to pay for transaction fees, also known as gas, when executing a smart contract on the Ethereum network. Each account on the network holds an amount of ether, which is used to initiate transactions and pay for gas fees. Using smart contracts in crowdfunding ensures that the terms of the agreement are automatically enforced, eliminating the need for intermediaries or third parties. This provides a more secure and transparent way of managing funds and rewards, reducing the risk of fraud or mismanagement. Figure 3 lists a few of the parameters that has to included in a transaction.

FROM	sender account : {0xFc2B791a08AbC9F51e71498e0369157B F05cb53A}
TO	receiver account : {0x4c6dF213Cf2e2c8d8Fe9D34984dFf67B9 48E6996}
VALUE	Amount in Weis (10 <sup>18</sup> weis = 1ether)
DATA	Bytecode + Arguments (if needed).
GAS LIMIT	Larger enough for an ether transaction.
GAS PRICE	To be determined by transaction Initiator.

Figure 3. Parameters for transaction

### 3.5 Transaction flow

An initiator submits the project with title, description, goal amount, milestone amount, deadline and type of project. After submitting the project, the project is recorded in the smart contract. Once it is in smart contract, N number of investors are able to fund the projects. All funds are stored in smart contracts and are not sent directly to the initiator. Once the agreed upon milestone is completed it is transferred to the project initiator. The initiator can now specify the next milestone of the project, once the goal amount is completed the project state changes to successful. If the project doesn't meet the goal amount then all the investors of the project can get their refund from the smart contract. Figure 4 illustrated the transaction flow in a crowd funding platform.

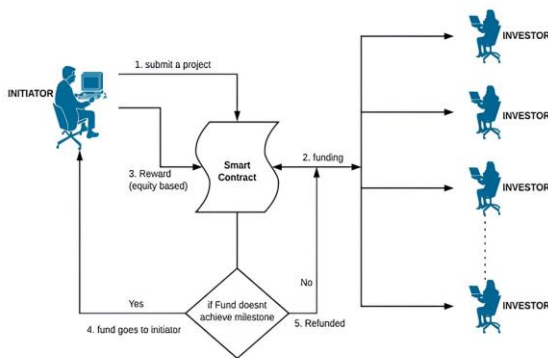


Figure 4. Transactional flow of crowdfunding

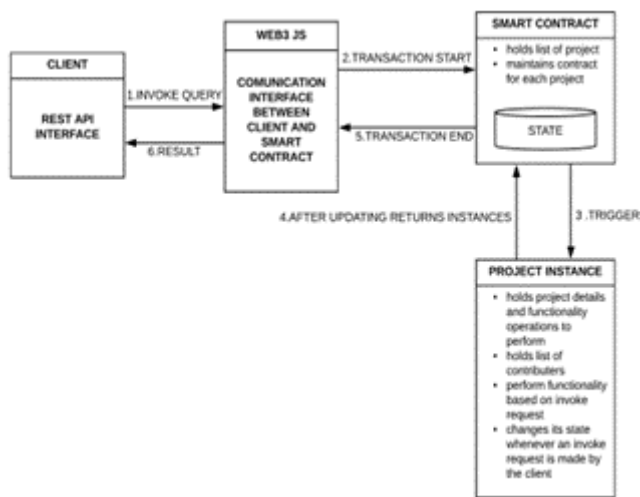


Figure 5. Process view of crowdfunding

### 3.6 Process view

When the client, an investor or an initiator. Invokes any request from the application side, then the web3 interface accepts the invoked request and maps the function call to the desired function in the smart contract. Whenever the request is made then the transaction is started in ethereum framework and the smart contracts holds all the credentials of the projects. The function call is performed and the state is changed in the smart contract. After performing the function call it returns the result to the web3 interface. The web3 interface instantiates the data on the client side and the client side is able to view the

result. Figure 5 shows the process involved in crowdfunding.

### 3.7 Crowd funding application and deployment

To make our smart contract work, it must be deployed in any of the platforms that supports a smart contract. Here Ethereum Framework is used to deploy the smart contract. Once the smart contract is deployed no more changes can be done to it. After deploying, the deployed address must be specified in our application. Once it is specified we can make use of functionalities in the smart contract with use of API calls. The web3 provider acts as the interface layer between the client and the Ethereum Virtual node. In an Ethereum Virtual node all the transactions are mined and attached to the block after performing operations specified in the smart contract. First, a smart contract solution is written in high-level language and is compiled as bytecode.

In a blockchain network, each smart contract is assigned a unique address that is used to identify it. This address is generated by hashing the address of the sender (i.e., the person or entity initiating the transaction) and the nonce. The nonce is a randomly generated number that is included in the transaction to ensure its uniqueness. To create and deploy a smart contract, a unique target account is assigned. The target account is a special type of account that can be used to deploy smart contracts. Initially, the target account's address is set to null, meaning it has not yet been assigned an address on the blockchain. To deploy a smart contract, a transaction is created with the target account as the recipient and the bytecode for the smart contract as the payload. The transaction is broadcast to the blockchain network and processed by the nodes on the network. Once the transaction is validated and executed successfully, the Ethereum Virtual Machine stores the bytecode for the smart contract permanently. The EVM is a virtual machine that operates on every node within the network. Once a smart contract is deployed, it can be interacted with by sending transactions to its unique address. The smart contract's functions can be invoked by sending a transaction that specifies the function to be called, along with any required parameters. The EVM ensures that the function is executed consistently across all nodes in the network, providing a secure and transparent way to manage digital assets and automate complex transactions.

To deploy a smart contract, a unique target account is assigned, which is a special type of account that can be used for this purpose. The target account's initial address is set to null, indicating it has not yet been assigned an address on the blockchain. To deploy the smart contract, a transaction is created with the target account as the recipient and the bytecode for the smart contract as the payload. Once the transaction is validated and executed, the bytecode is permanently stored in the Ethereum Virtual Machine (EVM) on each node in the network, allowing the smart contract to be interacted with by sending transactions to its unique address.

After a smart contract is deployed, it can be accessed by sending transactions to its unique address. Transactions can invoke specific functions of the smart contract by specifying the function and any necessary parameters. The EVM ensures consistent execution of these functions across all nodes in the network, which enables secure and transparent management of digital assets and automation of complex transactions. Figure 6 illustrates the blockchain deployment architecture.

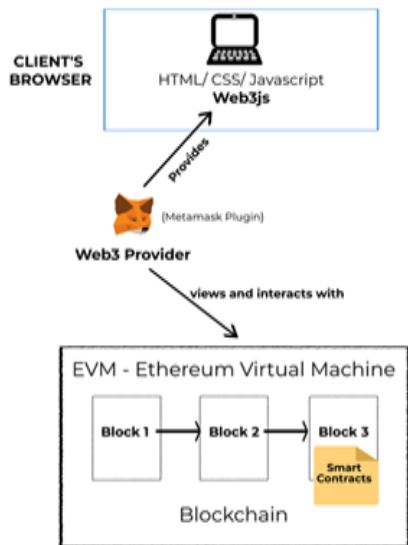


Figure 6. Architectural diagram of deployment

#### 4. STEPS FOR DEPLOYMENT

Figure 7 shows the steps involved in deployment of a blockchain platform.

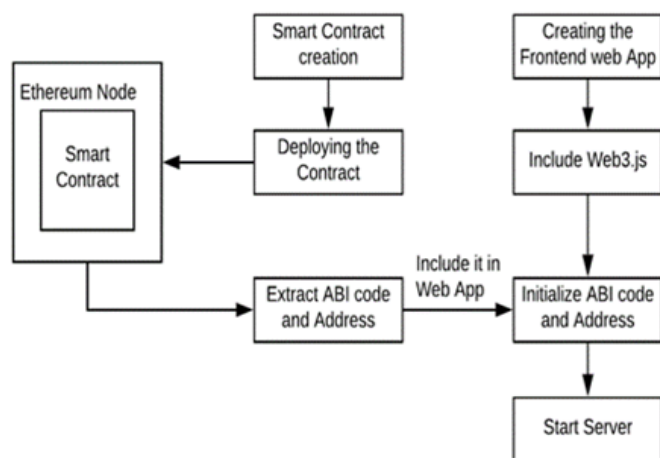


Figure 7. Flow diagram for deployment

1. A smart contract is a type of digital contract where the terms of the agreement between parties are written in code instead of traditional legal language. In the context of crowdfunding, these parties would be the investors and donors. Once written, the code is distributed across a decentralized blockchain network and is enforced by the network itself. Which details that when certain predefined conditions are met, smart contracts are automatically executed by the blockchain system. The Ethereum platform uses Solidity as its programming language for writing smart contracts. These contracts, when written in Solidity, are compiled into bytecode that can be executed by the Ethereum Virtual Machine (EVM) operating on each node within the network. This process ensures that the smart contract code is executed consistently and accurately across all nodes in the network. The code is transparent, secure, and tamper-proof, making it an ideal solution for managing complex financial transactions like crowdfunding. The smart contract must be first audited internally as it cannot be changed once deployed. In order to

verify a smart contract, click the contract tab in Etherscan and select Verify and Publish.

2. After the digital logic of a smart contract is implemented, it can be deployed on the Ethereum network, which is a decentralized public ledger. When a smart contract is deployed, it is stored in the Ethereum Virtual Machine (EVM) which is a virtual environment that runs on every node in the network. The EVM keeps track of all the transactions and contracts on the blockchain, and it ensures that each transaction is processed consistently across all nodes in the network. Each transaction is recorded in a block, and these blocks are linked together in a chain, hence the term "blockchain." To deploy a smart contract on the Ethereum network, developers can use different tools, such as Truffle and Remix IDE. Truffle is a development environment, testing framework, and asset pipeline for Ethereum, while Remix IDE is an online code editor for Solidity contracts that allows for easy testing, debugging and deployment of smart contracts.

3. To make it easier to interact with smart contracts, the Ethereum ecosystem has developed the Contract Application Binary Interface (ABI). An ABI is required in order to specify which part of the smart contract to invoke and returns the data in standard format. The ABI provides a standardized way for users and other contracts to interact with a deployed smart contract by defining the functions and data types that the smart contract exposes to the outside world. The ABI specifies the input and output types of each function in the smart contract, as well as how to encode and decode the data when making a function call. This makes it possible for developers to create user interfaces, web applications, and other contracts that can interact with the smart contract using a simple and consistent interface. Overall, the ABI is a crucial component of the Ethereum ecosystem, as it provides a way for developers to interact with smart contracts in a standardized and predictable way.

4. On the other hand, the frontend web application can be built in parallel. Web3.js is imported in this application, it acts as a communicator between our frontend and the smart contract deployed in the network.

5. Include the ABI code and deployed address in the application.

6. Finally start the server.

#### 5. RESULT AND ANALYSIS

The use of blockchain technology in crowdfunding platforms can increase the confidentiality of contributors since all transactions are recorded on the blockchain, making them transparent. This means that all donors and investors can view the records of each transaction on the blockchain explorer like Etherscan API. In Ethereum, transactions are carried out using ether cryptocurrency and require a small amount of gas to be spent for each transaction to proceed. In addition to the transparency and security features provided by the blockchain technology, smart contracts can also eliminate the need for trust among stakeholders. Smart contracts are self-executing and automatically execute the terms of the agreement once the conditions are met. The conditions for equity-based projects may differ from those of donation-based projects since the nature of these projects varies. However, in both cases, the use of smart contracts can increase transparency, security, and eliminate the need for intermediaries.

In Donation based projects, if the milestone is not reached



for a particular project, then the Initiator of that project would receive the funds raised till the deadline irrespective of milestone obtained. In Equity based projects, if the milestone is not reached then the fund raised for a particular project will be refunded to all Donors who have contributed. If the project obtains the milestone then that project Initiator could accept the fund from the smart contract and assign second milestone for that project. For each milestone the Initiator can assign new deadline. On each successful milestone completion the Initiator could accept the fund from the smart contract. Once the project is completed its funding the Initiator could give reward for the Donors. Total reward amount is donated to the smart contract. Once it is rewarded the Donors can get their reward amount from the smart contract. Each Donor will receive the amount based on their contributions. These functionalities are done in the smart contract. Unlike conventional crowdfunding platforms, the blockchain platforms remove involvement of any intermediary that has risk of any fraudulent activity or additional cost. The investor shall not lose his money if the initiator fails to complete a task and the initiator can be assured of funding as per agreement as the blockchain validates that the investor has the funding amount promised in his digital wallet. Figure 8 to Figure 10 illustrates the UI built for user interaction using Web 3.00 scripting.

Figures 8-10 are the screenshots of the crowdfunding project.

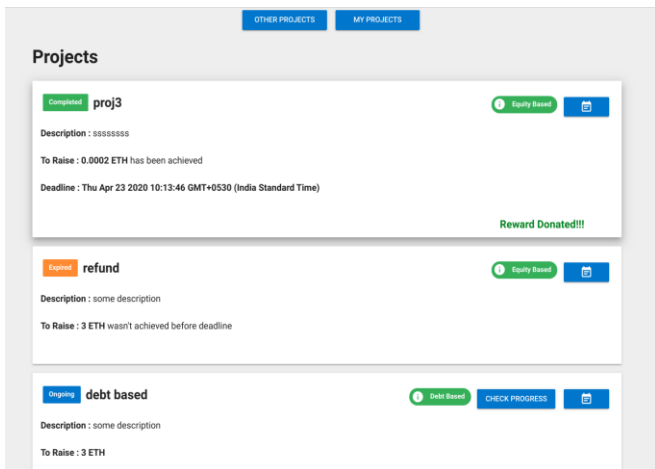


Figure 8. List of debt based and equity based projects

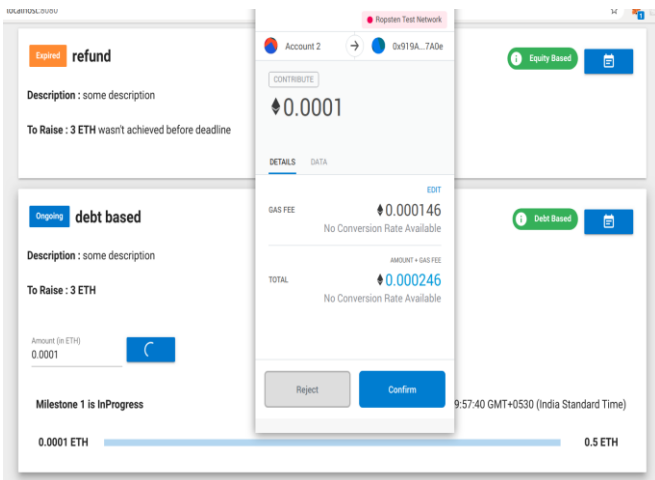


Figure 9. Undergoing funding process

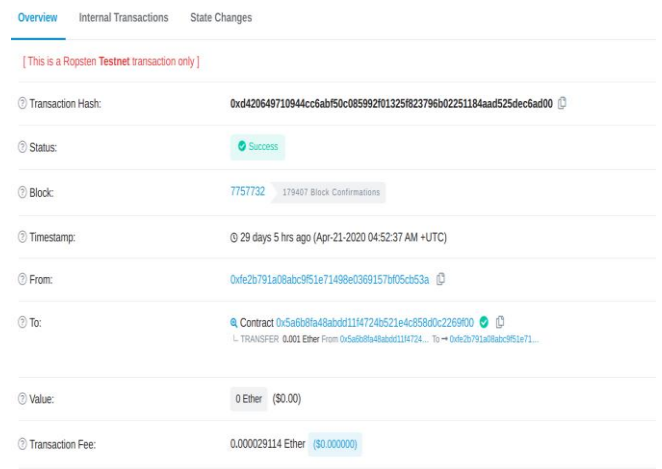


Figure 10. Information about the transaction

## 6. CONCLUSION

Blockchain technology has the potential to offer a low-cost and efficient solution for equity registration, transfer, and transactions in the crowdfunding industry. This technology can also help eliminate the legal risks associated with fund management and aid regulators in understanding and supervising the crowdfunding market. However, the current application of blockchain in equity management is still in its exploratory stage and requires addressing several legal and technical issues. The risk involved in equity based crowdfunding is that an investor might lose all his investment if the funded company goes bankrupt and the investor also might not be able to stick on to his financial obligation as promised. To successfully implement blockchain applications, cooperation is required between blockchain enterprises and market managers. They need to deepen their understanding of the technology, its opportunities, and risks to actively promote its adoption in the crowdfunding and digital asset management markets. Technical innovation and application can achieve economic efficiency and social benefits. It is recommended that the crowdfunding stakeholders try to involve technical experts to build their private blockchain and record their agreement terms as part of blockchain smart contract.

## REFERENCES

- [1] Miraz, M.H., Ali, M. (2018). Applications of blockchain technology beyond cryptocurrency. arXiv Preprint arXiv: 1801.03528. <https://doi.org/10.48550/arXiv.1801.03528>
- [2] Piscini, E., Guastella, J., Rozman, A., Nassim, T. (2016). Blockchain: democratized trust: distributed ledgers and the future of value. Deloitte Insights.
- [3] Jayapal, C., Sudhakar, C. (2023). Distributed technologies and consensus algorithms for blockchain. Novel Research and Development Approaches in Heterogeneous Systems and Algorithms, IGI Global, 100-122. <https://doi.org/10.4018/978-1-6684-7524-9.ch006>
- [4] Disruption, E. (2016). Tapping the potential of distributed ledgers to improve the post trade landscape. DTCC White Paper.
- [5] Vakulinia, I., Badsha, S., Sengupta, S. (2018). Crowdfunding the insurance of a cyber-product using

- blockchain. In 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), IEEE, pp. 964-970. <https://doi.org/10.1109/UEMCON.2018.8796515>
- [6] Cai, C.W. (2018). Disruption of financial intermediation by FinTech: A review on crowdfunding and blockchain. *Accounting & Finance*, 58(4): 965-992. <https://doi.org/10.1111/acfi.12405>
- [7] Schlueter, M. (2015). Underlying benefits and drawbacks of crowdfunding from the perspective of entrepreneurs in Germany. Bachelor's Thesis, University of Twente.
- [8] Schwienbacher, A., Larralde, B. (2010). Crowdfunding of small entrepreneurial ventures. *Handbook of Entrepreneurial Finance*, Oxford University Press, 1-23. <https://doi.org/10.2139/ssrn.1699183>
- [9] Zheng, Z.B., Xie, S.A., Dai, H.N., Chen, X.P., Wang, H.M. (2017). An overview of blockchain technology: architecture, consensus, and future trends. In 2017 IEEE International Congress on Big Data (BigData Congress), IEEE, pp. 557-564. <https://doi.org/10.1109/BigDataCongress.2017.85>
- [10] Muhammad, T., bin Ngah, B. (2020). Modeling debt and equity crowdfunding based on murabahah, musharakah and mudarabah: trust and awareness. *Ikonomika: Jurnal Ekonomi dan Bisnis Islam*, 5(2): 271-296.
- [11] Tsankov, P., Dan, A., Drachsler-Cohen, D., Gervais, A., Buenzli, F., Vechev, M. (2018). Securify: Practical security analysis of smart contracts. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 67-82. <https://doi.org/10.1145/3243734.3243780>
- [12] Chen, G., Xu, B., Lu, M.L., Chen, N.S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*, 5(1): 1-10. <https://doi.org/10.1186/s40561-017-0050-x>
- [13] Alharby, M., Van Moorsel, A. (2017). Blockchain-based smart contracts: A systematic mapping study. *arXiv Preprint arXiv: 1710.06372*. <https://doi.org/10.48550/arXiv.1710.06372>
- [14] Delmolino, K., Arnett, M., Kosba, A., Miller, A., Shi, E. (2016). Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In *International Conference on Financial Cryptography and Data Security*, Springer Berlin Heidelberg, pp. 79-94. [https://doi.org/10.1007/978-3-662-53357-4\\_6](https://doi.org/10.1007/978-3-662-53357-4_6)
- [15] Renu, S.A., Banik, B.G. (2021). Implementation of a secure ridesharing DApp using smart contracts on Ethereum blockchain. *International Journal of Safety and Security Engineering*, 11(2): 167-173. <https://doi.org/10.18280/ijss.110205>
- [16] Satish Babu, B.V., Babu, K.S. (2021). The purview of blockchain appositeness in computing paradigms: A survey. *Ingénierie des Systèmes d'Information*, 26(1): 33-46. <https://doi.org/10.18280/isi.260104>