Short Article

A Reliable and Secure Crowdfunding Platform Using Decentralized Blockchain

Hironori Tanise, Istiaque Ahmed, Quoc Duy Nam Nguyen, Thi Hong Tran, *Senior Member, IEEE*

Department of Informatics, Osaka Metropolitan University (OMU), Japan

Correspondence: Thi Hong Tran, hong@omu.ac.jp

Communication: received 02 February 2024, revised 10 June 2024, accepted 07 August 2024
Online publication: 25 September 2024, Digital Object Identifier: 10.21553/rev-jec.365

Abstract– **Crowdfunding is a significant avenue for raising funds over the Internet to bring ideas into reality without relying on traditional funding sources. However, conventional centralized crowdfunding systems suffer from issues such as trustworthiness and transparency. In other words, it is necessary to ensure the reliability of information regarding project details, progress, and money exchanges, and to store this information in a form that cannot be altered. To ensure that the quality of projects is not degraded due to these causes and resolve the existing limitations, we propose a decentralized crowdfunding system using blockchain technology with two major contributions: "Decentralized Voting", and the "Decentralized Evaluating" methods. The Decentralized Voting Method aims to solve a particular platform's biased review by voting on the project's prospects and credibility. The Decentralized Evaluating Method aims to ensure project quality by exploiting the transparency of the invested projects. In this proposed blockchain-based solution, we used React and TypeScript for the front end and Rust-empowered Substrate at the backend. By using these methods, we verify through simulation that the implemented system works as proposed. This study identifies problems in crowdfunding and their causes, and then proposes a system that uses the two methods described above. The proposed system is expected to be a reliable distributed crowdfunding system.**

Keywords– **Blockchain, smart contracts, decentralized, crowdfunding, substrate platform, cryptography, fundraising.**

1 Introduction

With the advancement of the information system-empowered society, the exchange of money on the Internet has increased dramatically. Crowdfunding is one way of exchanging money on the Internet. Crowdfunding solicits resources from various contributors to bring a new idea to realization [1]. In traditional systems, the required amount of money and the schedule for the progress of the project are presented, the funds are provided by people using the Internet, and in return, monetary or non-monetary funds are provided at the time and date presented [2]. One of the most common problems with crowdfunding is a prevalence of fraud, such as many projects delivering their products later than expected [3]. These problems are caused by the lack of credibility of the crowdfunding systems, which is a centralized fundraising method on the Internet controlled by the system manager, which means that there is no obligation to repay the project sponsors. This means that it is unclear whether or not the project is proceeding as planned, and the money is exchanged for the project. Therefore, to solve the current crowdfunding problem, it is necessary to ensure that the details of the project, its progress, and the money exchanged are credible and that the information about the money exchanged is stored in an unaltered form. Blockchain technology is a method by which information exchange can be transparent, immutable, and efficiently recorded.

Blockchain came into the spotlight to enable direct peer-to-peer (P2P) exchanges between parties without the need for a financial institution as a third party. In addition, recording transactions using blockchain can have many characteristics such as Reliable and Available, Transparent, Immutable, Irrevocable and Digital [4]. Md. Nazmus Saadat et al. have conducted research on blockchain-based crowdfunding using the Solidity programming language [5]. H. Baber has developed an Ethereum smart contract using the Solidity programming language, which solves the fraud problem in traditional crowdfunding [2]. The platform is designed to eliminate the time and effort required by traditional crowdfunding platforms to match funders with funders, thereby solving the problems of time and money. Vakilinia et al. have worked to mitigate cyber threats in crowdfunding, primarily using blockchain transparency as a solution. Many studies, such as these, focus on solving only a single problem, such as transaction transparency or cost reduction, by taking advantage of the blockchain feature of transaction flexibility [6]. However, a significant problem still needs to be solved, such as the credibility of many crowdfunded projects and the loss of trust in the project's progress caused by the moral hazard of the project's proponents. This loss of trust can significantly impact the quality of projects published on the crowdfunding platform and can discourage supporters from investing in the projects [7].

In order to ensure that the quality of projects is not degraded due to various causes, it is necessary to go beyond the conventional approach of making transactions transparent. This paper aims to address the

issue of quality collateral for the project. We propose two techniques: one is a voting system, and another is a credit score system to solve the problem of ensuring the quality of projects. This research represents the problems in crowdfunding, identifies the causes behind those, and proposes a solution method for solving the problems using blockchain. Section 2 describes blockchain and crowdfunding, presents related research on crowdfunding using blockchain technology, and proposes two methods to address crowdfunding issues. Section 3 describes the proposed crowdfunding system. In Section 4, we develop and demonstrate the proposed crowdfunding system and discuss the proposed system. Section 5 summarizes the research.

2 Background

2.1 Decentralized Blockchain Technology Concept

The virtual currency Bitcoin was born as a result of Satoshi Nakamoto's paper published in 2008 [8]. Bitcoin does not require a financial institution as a third party, and transactions can be made directly between parties on a P2P basis. To achieve this, transactions that represent the contents of the transaction are included in a single block, and a decentralized time server is realized by including the hash value of the previous block in the header of the block to define a single time series between blocks. Only some participants need to keep the transaction history, all others know the last hash value and can check if the data has changed, and the only way to tamper with the data while keeping the hash is to find data collisions, which is computationally infeasible [9]. The technology that uses these methods of retaining transaction data, hash functions, etc., is the blockchain technology.

It is a decentralized ledger with transaction information and database, and the ledger is shared by all network nodes. In other words, blockchain allows all transactions to be recorded efficiently in a decentralized manner with immutability, traceability, and transparency [4].

- Immutability is a fundamental blockchain property that stems from the fact that once a transaction has been successfully verified and recorded in the blockchain, the transaction cannot be edited or deleted [10].
- Traceability indicates that all transaction information registered in the blockchain ledger can be referenced. It indicates that access is available to everything that remains part of the ledger, regardless of the size of the information [11].
- Transparency indicates that all blockchain network participants share the same blockchain ledger.

Another feature that is essential to create a flexible blockchain network is the smart contract. By addressing a transaction, a smart contract can be executed, and it is automatically executed independently and in a prescribed manner on all nodes in the network [12].

We describe the Substrate platform for building the blockchain. Substrate indicates that the role of each element is as follows [13]. The outer node is responsible for the part of the node that is not processed by Runtime. It communicates with other network participants using consensus, which allows them to agree on the state of the blockchain. Runtime manages transactions and handles changes to the blockchain state deviation function. Runtime also includes a number of modules and support libraries called FRAMEs that simplify Runtime development. These modules are called pallets, and by using FRAME's libraries and services, it is possible to build your own pallets. This feature allows the proposed system to use existing pallets as well as its own pallets to implement the proposed methodology for flexible blockchain development. By using the functionality of the pallets, the proposed system is implemented in a flexible method.

2.2 Concept of Crowdfunding

Crowdfunding is the process of receiving funding from an unspecified number of people on the Internet. In the traditional system, the project is funded by people on the Internet, and in return, they provide monetary or non-monetary support [2]. The crowdfunding system manager receives a fee from the users and matches the supply and demand of these fundraisers and investors. Because of this internet-based fundraising method, crowdfunding is an effective and efficient way to raise the funds needed in a hassle-free and efficient manner [5]. There are many different platforms for crowdfunding, but the process is similar for all of them. In order to design a crowdfunding system, it is necessary to define the type of crowdfunding as a point to keep in mind. There are several types of crowdfunding, depending on the entity that needs funds, the purpose of the crowdfunding, how the funds are provided, whether or not there is a "return", and whether or not profit is sought [14]. The process of crowdfunding does not vary greatly by type, but it may require additional steps such as legal regulations and contracts. This section describes the three main types of crowdfunding: donation, purchase, and loan.

- Donation-type crowdfunding is a mechanism for making donations to social contribution activities. Basically, there is no non-monetary return, but often a return in the form of a letter [14, 15].
- Purchase-based crowdfunding is a form of crowdfunding in which people support a proposed project and receive a non-monetary return in the form of goods or services in proportion to the amount of support they provide [14, 15].
- Loan-based crowdfunding is a system in which the crowdfunding system manager acts as an intermediary to match businesses with investors. Investors receive a financial return on their investment [14].

2.3 Related Works on Crowdfunding

2.3.1 Centralized Crowdfunding: Crowdfunding is attracting attention in the Fintech field as a new way to raise funds, and in 2017, Kickstarter, the dominant

crowdfunding platform overseas, launched its service for our country. As such a global scale platform, Kickstarter has attracted a lot of interest and a lot of research is underway. Molick presents the dynamics of crowdfunding as a problem, with over 75% of crowdfunded projects delivering their products later than expected [3]. Empirical analysis shows that project entrepreneurs need to be prepared for this and that careful planning is necessary to set appropriate goals that will allow them to deliver their products on time. Uchida and Hayashi conducted an empirical analysis using CAMPFIRE, a major crowdfunding platform in Japan, for comparison with Molick's Kickstart [16]. The analysis also found differences in the quality of the videos posted on the platform and the geographic region in which the platform is located. Zhao, T et al. describe four types of crowdfunding: P2P lending, investment crowdfunding, donation crowdfunding, and reward crowdfunding [17]. They believe that the lack of regulation in the UK and US for two of the most popular forms of crowdfunding has created three problems: first, a lack of industry standards makes it difficult for both crowdfunding entrepreneurs and investors to make informed decisions; second, the quality of projects can be different, making it difficult for investors to make informed decisions; and third, the ini lack of regulation in the UK and US can make it difficult for investors to make informed decisions. Quality of projects makes it difficult for investors to compare projects; and third, entrepreneurs have indicated that many projects have been given up because they cannot raise enough money to support their ventures. I. Ahmed et al. implemented decentralized charity using an electronic know-your-customer (eKYC) authentication approach and cryptographic HASH [18]. They proposed coin-toss function for data selection, and a random time delay between pieces of data are used to avoid attacks based on guesswork.

In order to improve the credibility of the crowdfunding system, it is necessary to analyze the causes of the decline in credibility of the traditional system. We believe that the two causes of the decline in credibility are "Biased screening by certain platforms" and "Quality assurance for projects".

2.3.2 Problems with centralized crowdfunding systems: Consider the two issues of "biased screening by specific platforms" and "project quality assurance" as possible causes of the decline in the credibility of crowdfunding.

Issue 1: Biased screening by certain platforms: The first problem is the current screening process for crowdfunding projects. Since system managers manage the funds of borrowers and lenders themselves, they may create abusers, including misuse of funds and fund fraud [7]. In addition, mechanisms and personnel are needed to be able to properly review the vast number and variety of projects. However, many crowdfunding platforms use a centralized review process that is not transparent. The tasks essential for the operation of the system, such as project screening and fundraising in crowdfunding, are concentrated in the hands of the system manager. Jiang Jun points out that the concentration of all crowdfunding flows on the platform as a major disadvantage [7]. Specifically, the concentration of flows on the platform means that the system manager bears the credit risk as it manages the funds and services, which, prior to the establishment of legal regulations, could lead to misuse of funds, fund fraud, and other malfeasance, leading to a decline in the credibility of crowdfunding. Although current regulations have made these abuses impossible, system managers are merely intermediaries in crowdfunding and are not liable for any breach of contract by crowdfunded projects.

Today, crowdfunding system managers still need to conduct credible project scrutiny to ensure that investors are comfortable with their investments. We think that transparent project vetting procedures should be in place to avoid the occurrence of biased vetting, where the credibility of the project itself can change depending on who is vetting the project.

Issue 2: Quality assurance for projects: A second issue is the management of project credibility and quality, as Molick showed in an exploratory study that crowdfunding quality is very significantly associated with the success of crowdfunded projects, even among different groups acting as funders [3]. In contrast, Zhao Y et al. mentioned that only basic guidelines are provided to crowdfunding users, and no requirements are specified to ensure the credibility and quality of the projects [17]. For these reasons, supporters find it impossible to track and control the project process. In contrast to launching a crowdfunding project in the traditional way, a third-party organization, the management company, is essential to confirm trust in the project originator. Furthermore, it is difficult to completely eliminate concerns such as whether the invested funds are not being used as planned and are being misused [14].

Project credibility and quality assurance should be provided for project quality control. It is necessary to improve the progress of projects and the way funds are managed, and to take into account the design of systems that allow investors to invest safely.

2.3.3 Decentralized Crowdfunding: Zhu et al. focused on the application of blockchain technology to equity crowdfunding in China and showed that blockchain technology can enable efficient and low-cost share registration, share trading and transfers, and shareholder voting, and eliminate legal risks associated with fund management [19]. They attempted to implement blockchain technology in crowdfunding. Md. Nazmus Saadat et al. who have attempted to implement blockchain technology in crowdfunding, cited the problem of crowdfunding as being The problem with crowdfunding is that it is susceptible to fraud because traditional laws and security measures may not be working [5]. The company sought to solve this problem by implementing smart contracts, one of the features of blockchain technology, in the crowdfunding system. In addition, they actually built the system using the ReactJS language as the front end and the NodeJS language as the back end, and created a crowdfunding system using the Solidity language

for front-end development. H. Baber pointed out that the problem with the current centralized crowdfunding system is that the matching of donors and fundraisers is done by the crowdfunding platform, which is a trusted third party [2]. Focusing on the decentralized and transparent nature of blockchain technology as advantages of using blockchain technology for crowdfunding, we proposed a new crowdfunding system using blockchain technology.

Much of the research on crowdfunding using blockchain technology is often aimed at improving the efficiency of the system and operating at a lower cost. Some of them are addressing fraud prevention by using the transparency of transactions through the use of blockchain technology features, but they do not discuss the trustworthiness of the system or the project. Trustworthiness needs to be considered so that investors can invest safely.

2.3.4 Challenges in Decentralized Crowdfunding: The study on crowdfunding systems using blockchain technology currently conducted is listed and the issues are discussed. H. Baber showed the advantages of using blockchain technology in crowdfunding systems, such as reduced labor costs and transparency of transactions and contracts [2]. Md. Nazmus Saadat et al. showed that blockchain technology enables transparency of transactions, confidentiality of blockchain participants, and the ability to use smart contracts, a feature of blockchain technology, to automatically execute contracts [5]. However, using only blockchain features, they focused on solving only a single problem, such as transaction transparency and cost reduction. While these advantages could facilitate the progress of projects in crowdfunding, they do not directly relate to the problems of traditional crowdfunding, such as "Biased screening by certain platforms" and "Quality Assurance for Projects," and as a result, do not solve them. It is thought that this will not lead to a solution.

2.4 Preemptive Approaches

Based on the above, the concept of the proposed methodology is presented below to address two issues: "Biased screening by certain platforms" and "Quality Assurance for Projects".

Although there are multiple causes for the occurrence of problems 1 and 2, we can narrow them down to two causes: the project information is not transparent and the information is centrally managed as its genesis. This research believes that these problems can be solved by introducing blockchain technology, which is decentralized and characterized by transparency, and by making the system itself less susceptible to the morals of participants than conventional systems. Specifically, we believe that problem 1 can be solved by introducing a decentralized screening method in which the prospects and credibility of a project are voted on before the project enters the stage of accepting funding, and problem 2 can be solved by introducing a decentralized evaluation method with transparency for invested projects. In addition, the use of blockchain technology would alleviate one of the issues raised by many crowdfunding projects, namely high fees, since there is no need to manage the system, pay for credits, etc.

Through the analysis of the above problem solving, this study develops two proposed methods. One is a decentralized screening method for projects, and the other is a decentralized evaluation method using scores. The decentralized screening method and the decentralized evaluation method are expected to solve Problem 1, biased screening by a particular platform, and Problem 2, quality assurance for projects, respectively.

3 Proposed System

3.1 Fundraising-Chain System Overview

Participants in Fundraising-Chain are divided into several roles: project owners, voters, and supporters. Project descriptions and transactions by individuals made by project owner are recorded in a blockchain ledger in Fundraising-Chain. Project owners are those who submit project ideas to Fundraising-Chain. Voters are those who vote on submitted project ideas. Supporters can invest in project ideas. We assume that there are multiple project owners, voters, and supporters in the Fundraising-Chain.

Figure 1 shows the general flow of using the proposed financing system The system typically consists of the following 7 steps. In Step 1, project owner submits a project, an idea, to the Fundraising-Chain after creating their accounts. In Step 2, each voter checks the various projects submitted. Votes are cast for those deemed suitable as crowdfunding projects. Step 3 was implemented using a decentralized votting methodology. The screening method is to determine if a submitted project is suitable as a project by the number of votes it receives. Projects that received more than a set number of votes as a condition were later made publicly available for investment by supporters. Voters' voting history and the success or failure of the project they voted for are stored in the blockchain ledger as a track record. Therefore, depending on the progress of the project, voting results may be overwritten in cases other than Step 3. In Step 4, supporters may invest in a project that has received a sufficient number of votes

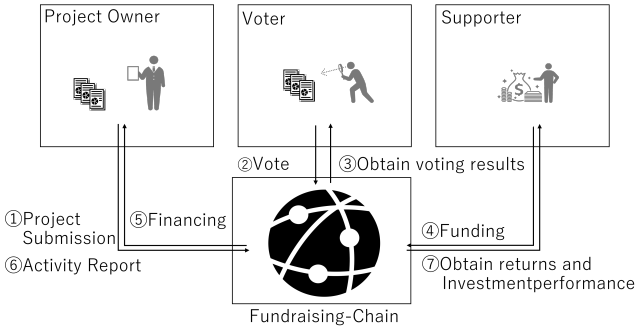

Figure 1. Fundraising-Chain Proposal.

to be published. In Step 5, the project owner can only obtain funds if the project reaches the target amount, as we propose an "All or Nothing" type of crowdfunding where the project owner can obtain funds by reaching the target amount within a predetermined time frame. If the target amount is not reached, the funds will be returned to the supporters and the project will fail. In Step 6, the project is promoted based on the investment by the supporters, and the activities are registered in the Fundraising-Chain's ledger. In Step 7, when the project is completed, the project owner makes a return to the supporters. The supporters will also receive a track record of having invested in and contributed to the project.

Table I
Step Details

Steps	Contents	Description Location
1	Project Submission	4.2
2	Vote	3.2, 4.2
3	Obtain voting results	3.2
4	Funding	4.2
5	Financing	4.2
6	Activity Report	4.2
7	Obtain returns and Investment Performance	3.2, 4.2

The system proposed in this paper differs from conventional ones in that there are two stages for judging projects: "Decentralized Voting Method" and "Decentralized Evaluation Method". The evaluation phase takes place after the project has been successfully completed and the project owner has thanked its supporters, where the project owner can give credit to the supporters and the supporters can give credit to the project owner at the same time. Crowdfunding participants will have a score at the time of account creation that indicates their creditworthiness. The score value changes with the timing of this rating, and the score can increase or decrease depending on how good or bad the rating is. The system then allows a voter to be authorized as a voter only if the score is above a certain number.

3.2 Decentralized Voting Method

This section describes the design of the Step 2 voting system in the fundraising system. The Decentralized Voting Method aims to solve the biased review by a particular platform by voting on the project's prospects and credibility.

The review method used by many crowdfunding platforms is a non-transparent review process, so when problems arise between project owner and supporters, many crowdfunding platforms do not hold those who have reviewed the projects accountable. Therefore, by using a third-party, multiple-voter, voting-style review method using blockchain technology, the process of project review will be transparent, and which voters cast which votes will be registered in the blockchain ledger as immutable and transparent data. Voters can therefore be expected to responsibly review projects. In this way, it would be possible to improve current screening methods. Figure 2 shows the proposed decentralized voting method.

Initially, the project owner registers the idea project in the Fundraising-Chain blockchain ledger. Then, voters cast their votes for projects in areas in which they are confident in their knowledge. Ideas that receive more than a certain number of votes during the voting period will be considered for support, while ideas with insufficient votes will be deemed inappropriate for crowdfunding and removed from the blockchain. By using a decentralized method of reviewing projects, the goal is to eliminate the traditional problem of opaque review through a centralized method. The system has a fixed voting period, and smart contracts are used when the voting period is exceeded. Projects that do not receive a certain number of votes through smart contracts are removed from the system. On the other hand, projects that receive enough votes are considered for investment. To prevent voter collusion and spam votes, the system requires account verification for all participants. In this proposed approach, the system administrator approves each role, such as system manager and voter. Administrators have the right to revoke malicious actions and fake accounts.

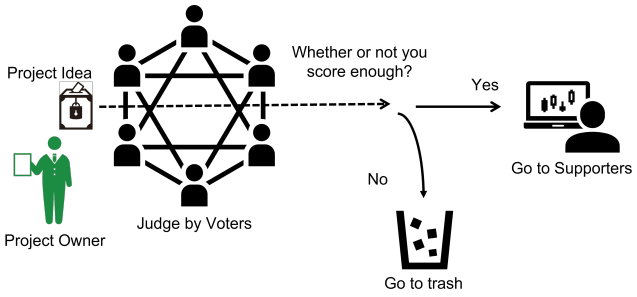

Figure 2. Proposal for a Decentralized Voting Method.

3.3 Decentralized Evaluation Method

This section describes the design of the Step 7 evaluation system in the financing system. The Decentralized Evaluation Methodology aims to ensure quality for projects by incorporating a method of transparency for the invested projects. Many crowdfunding platforms do not specify project submission requirements as a matters of project credibility and quality. This makes it impossible for many supporters to track and control projects. In response to this problem, we propose a decentralized and transparent individual evaluation method using blockchain technology, which will allow each person involved in the project progress to track and make decisions. Figure 3 shows the proposed decentralized evaluation method.

In the proposed Fundraising-Chain, an initial value is set for the credit score when an account is created. This score is held by each participant in the crowdfunding scheme, and it is possible to check another participant's score, and the Fundraising-Chain participant will be considered a supporter regardless of his/her score. In addition to supporters, there is a separate role as a

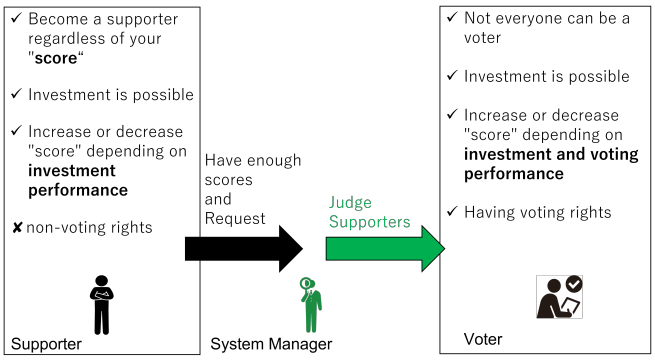

Figure 3. Proposal of a Decentralized Evaluation Method.

voter in that Fundraising-Chain. Voters, like supporters, can invest in publicly announced projects. Because of this involvement in the review of projects, the voters must be worthy of trust, as they will have a significant impact on the progress of the project. Therefore, two conditions must be met in order for a supporter to become a voter: first, the voter must have a certain number of credit scores in order to become a voter; second, the voter must be a person with a high enough trustworthiness score to be eligible to be a voter. The creditworthiness score is calculated based on several factors, including the voter's history of project evaluations, the success rate of projects they have supported, and their overall participation in the platform. Positive project evaluations contribute to a higher score, while backing unsuccessful projects or receiving a negative rating results in penalties. This multi-faceted approach ensures a comprehensive assessment of voter trustworthiness. The system can be expanded to include ongoing evaluation mechanisms, such as milestone-based reviews and periodic feedback. This approach allows for continuous assessment of project quality and progress, providing a more comprehensive view of the project's execution and enabling timely interventions if necessary. At this stage, we have implemented a feedback system, though it is not fully incorporated into the ongoing evaluation mechanisms.

Konomi and Kamiyama proposed a personal credit score provision system using blockchain technology [20]. Considering this study, the first condition is to implement a system in the blockchain platform, Substrate, that allows blockchain participants to perform rapid transactions in the process of updating the scores of the various participants. The second condition is that it must be determined by the system manager. To be judged by the system manager, the following three steps must be taken. In Step 1, the supporter who wants to be a voter must set the score above a certain number, which is a requirement to be a voter. In Step 2, they make an offer to the system manager on the Fundraising-Chain while keeping their score above the required number of conditions. In Step 3, the system manager receives the offer and checks the past performance of the supporter who made the offer. If the system manager determines that the track record is acceptable, then the system manager may authorize the supporter to be a voter. The reason for this second condition is that the collaboration between the project owner and the supporter allows the supporter to gain a track record of support and to intentionally increase the supporter's score with low risk.

4 System Implementation

4.1 System Overview

The overall diagram of the proposed system is shown in the Figure 4. The development system consists of three systems: front-end, back-end, and blockchain. Users will be able to use the web system by using their Polkadot account. The front-end part allows users to manipulate data in the back-end part, using the React and TypeScript languages to develop an intuitive interface, and the back-end part allows users to register all of the transaction data registered in the blockchain. All of the data can be registered, and the blockchain portion is being developed within the backend.

The blockchain part is responsible for storing and managing the Fundraising-Chain database. Most of the system's proposals are implemented in the development of the blockchain portion. The following sections describe the development of the blockchain portion and how ideas such as decentralized vetting methods and decentralized valuation methods will be implemented.

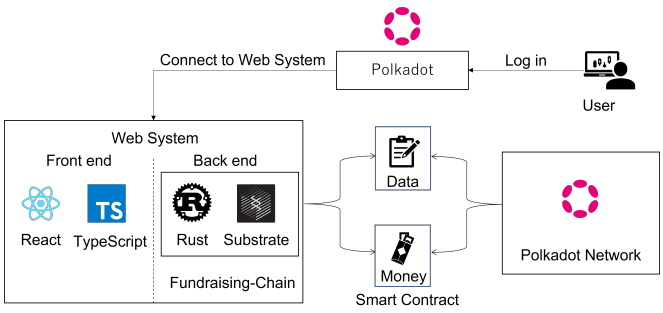

Figure 4. System Overview.

4.2 Blockchain and Smart Contract Concept

The blockchain used in the proposed system is Polkadot with the substrate framework, which is implemented using the Rust language. Which uses Nominated Proof-of-Stake (NPoS) as consensus and SHA-256 for tamper-proof data integrity. It also used, EdDSA/ECDSA for transaction authenticity. The Advanced Encryption Standard (AES) and Transport Layer Security (TLS) protocols safeguard data, guaranteeing confidentiality during transmission and storage. Polkadot also incorporates Zero-Knowledge Proofs (ZKPs) to protect transaction privacy. It is built with three pallets: the fundraising pallet, which handles the main flow of the crowdfunding system; the account pallet, which manages accounts; and the rating pallet, which manages scores that indicate creditworthiness.

Figure 5 shows an overall view of the proposed system and its functionality, which is composed of three pallets. The process flow in the proposed crowdfunding

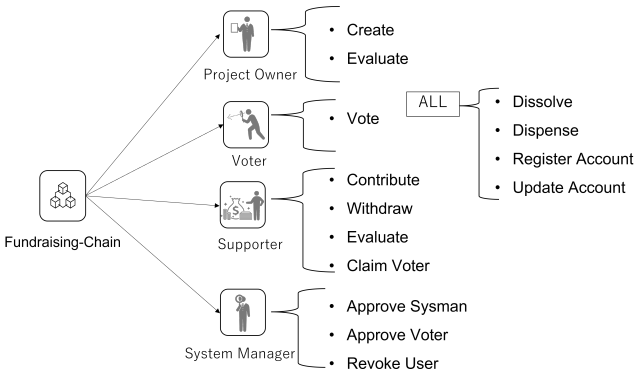

Figure 5. Main smart contracts of the proposed system.

system is as follows. The project owner can post a project by executing "Create" function by paying a certain deposit to register the project he/she wants to post in the Fundraising-Chain's blockchain ledger. The arguments are three pieces of information necessary for the project to proceed: the account in Polkadot that will receive the investment by the supporter if the project is successful, the target amount of the project, and the period during which the investment can be made.

The voter then executes "Vote" function to vote for projects registered in the blockchain ledger for project review, using as an argument the ID of the project for which he/she wishes to vote, as displayed on the front end. "Vote" function for voting has a certain voting period. The voting period is limited to a certain number of blocks from "Create" function, which is executed by the project owner to submit the project. After the Voteable Period, projects that receive more than a certain number of votes to pass the review process will be released to supporters, while projects that do not receive enough votes will be removed from the Fundraising-Chain.

After a project has been reviewed and published, supporters can invest in the published idea project by executing "Contribute" function. As with "Vote" function, "Contribute" function has an investment period. Unlike the fixed voting period in "Vote" function, the investable period depends on the investable period entered by the project owner as an argument when executing "Create" function. "Withdraw" function allows the project to withdraw all of its investment. "Dispense" function can be executed when the project's investable period has expired and the amount invested has reached the target amount.

"Dispense" function can be executed by any Fundraising-Chain participant, regardless of their role, and upon execution of the function, a portion of the project funds that have reached the target amount are decentralized to those who voted for the project, and all remaining funds are transferred to the project owner. After that, the project is assumed to be completed and the project is deleted from the Fundraising-Chain; the person who executes "Dispense" function gets the deposit that the project owner paid when he/she executed "Create" function.

The "Dispense" function and "Dissolve" function can be executed by any Fundraising-Chain participant. The calculation based on a certain of voting period, when "Create" function is executed, the investment period entered, and other factors are accelerated. The number of blocks, which is the time when the project is finally finished, is used. "Dissolve" function will refund any funds raised by the project to the supporters and dissolve the project. The person who executes the function gets the deposit they paid when they executed "Create" function. Since this function can only be executed after a certain amount of time in addition to the project end time, it is intended for projects that did not receive a sufficient number of votes during the review process, or for publicly announced projects that did not raise enough money to meet their fundraising goals, and therefore cannot proceed. The purpose of this function is to remove projects from the Fundraising-Chain.

The next section, Managing Participant Roles in the Fundraising-Chain, contains several functions that are executed by the four roles of the fundraiser, voter, supporter, and Fundraising-Chain system manager. To use Fundraising-Chain, one currently needs an account at Polkadot, but must register using their Polkadot account. Therefore, everyone who wants to participate in Fundraising-Chain must first execute "Register Account" function; "Update Account" function overwrites the data entered when executing "Register Account" function; and "Claim Voter" function is a function that allows the user to determine the creditworthiness of the applicant. "Claim Voter" function is a function that can be executed only when the credit score is above a certain number, and can be used to offer the role of Voter to the system manager.

There are three functions that can only be executed by the system manager. The first is the "Approve Sysman" function, which allows the manager "Sysman" to register participants as system managers. The second is the "Approve Voter" function, which allows the system manager to register participants as voters. The third is the "Revoke User" function, which suspends the account of any participant in the Fundraising-Chain system, rendering them unable to execute any function. These functions are relevant to the proposed new system, which involves "Decentralized Review Method" and "Decentralized Evaluation Method".

4.3 Implementation of Decentralized Voting and Decentralized Evaluation Methods

We describe a decentralized voting method and a decentralized evaluation method implemented in the blockchain part of the proposed system. The key aspects of both methods are the score representing the creditworthiness and the determination of roles based on the value of the score. In the current proposed system, after a successful project, the credit score is increased or decreased only by using "Evaluate" function of the fundraising pallet, which can be executed between the project owner and the supporters who invested in the project.

A weighted evaluation method is used in Fundraising-Chain, where the impact of score changes

is dependent on the user's score at the time of update. The score value is set to 100 when the account is created in Fundraising-Chain, with a maximum score value of 1000. When the score value reaches 500 or above, the user can execute the "Claim Voter" function to apply to become a voter, which will be reviewed by the system manager through the decentralized, transparent, and immutable nature of blockchain data. By using this score update method, a decentralized evaluation process can be implemented, and the trustworthy participation and score of participants can be confirmed through a decentralized evaluation method, thus allowing for a reliable decentralized approval process.

However, there is one thing that must be considered in the decentralized evaluation method. The purpose of the decentralized evaluation method was to recognize and confirm the appropriate voter for the person who sent the offer, and the reason for not letting the score value alone determine the voter as a voter was to prevent cases from occurring where the system could be used to intentionally advance a project and increase the score accordingly. Therefore, in addition to the value of the score, the proposed decentralized evaluation method provides an artificial solution in which the system manager takes action by checking the past performance of the blockchain participant who sent the offer. However, even though it is presented as a decentralized evaluation method by introducing the system manager as part of the decentralized evaluation method, the system manager has taken on some of the responsibility of making the final decision. This is a problem because the system manager is partially responsible for making the final decision, even though it is a decentralized evaluation method.

Therefore, it is necessary to introduce a proposal for a decentralized system that allows human review of performance without using a centralized system of system manager decisions as an improvement. This means using decentralized methods for determining who should be allowed to decide as a voter. For example, a decentralized voting method could be used to determine the voter instead of the system manager's decision in a decentralized evaluation method. This section only presents some suggestions for improvement when developing a crowdfunding system using blockchain technology in the future. To eliminate the need for a central system manager, the system can use a multi-step voting process or a staked-token system in the future. In the multi-step process, existing high-creditworthiness voters approve new voters. In the staked-token system, potential voters must stake tokens, which serve as collateral against malicious actions. To ensure transparency, the system manager's decisions on voter approval will be recorded on the blockchain. Each decision will include a rationale and be auditable by any participant, ensuring accountability and maintaining trust in the system manager's actions. Using the existing feedback and response system, rectifying the decisions based on participant concerns is possible.

5 Conclusion

In this study, we develop a decentralized crowdfunding system with a high degree of trustworthiness. To ensure mutual trust between project owners and supporters, we contribute two new methods: Decentralized Voting Method and Decentralized Evaluation Method. The voting method, a project's prospects and credibility by voting, avoids unreliable screening by certain crowdfunding platforms. The evaluation method ensures project quality by incorporating a method of transparency for invested projects. The open-source Substrate platform implements and evaluates crowdfunding systems, including these systems. Through simulations, we verify that the implemented systems work as proposed. However, the proposed system does not have a fully decentralized system compared to traditional crowdfunding systems, although it does have less responsibility for platform managers. Therefore, we are considering continues research to improve these aspects of the system.

Acknowledgment

This work was supported by JST the Japan Science and Technology Agency (JST) under a Strategic Basic Research Programs Precursory Research for Embryonic Science and Technology (PRESTO) under grant number JPMJPR20M6.

References

[1] R. Wash, "The value of completing crowdfunding projects," in *Proceedings of the International AAAI Conference on Web and Social Media*, vol. 7, no. 1, 2013, pp. 631–639.

[2] H. Baber, "Blockchain-based crowdfunding," *Blockchain Technology for Industry 4.0: Secure, Decentralized, Distributed and Trusted Industry Environment*, pp. 117–130, 2020.

[3] E. Mollick, "The dynamics of crowdfunding: An exploratory study," *Journal of Business Venturing*, vol. 29, no. 1, pp. 1–16, 2014.

[4] D. Schatsky and C. Muraskin, "Beyond bitcoin," *Blockchain is Coming to Disrupt Your Industry*, 2015.

[5] M. N. Saadat, S. A. H. S. A. Rahman, R. M. Nassr, and M. F. Zuhiri, "Blockchain based crowdfunding systems in malaysian perspective," in *Proceedings of the 2019 11th International Conference on Computer and Automation Engineering*, 2019, pp. 57–61.

[6] I. Vakilinia, S. Badsha, and S. Sengupta, "Crowdfunding the insurance of a cyber-product using blockchain," in *Proceedings of the 2018 9th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, 2018, pp. 964–970.

[7] J. Jun, "Factors behind the growth of chinese crowdfunding," *Journal of the Doctorate Studies in Social Sciences*, vol. 17, pp. 43–61, 2020.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized business review*, p. 21260, 2008.

[9] M. Di Pierro, "What is the blockchain?" *Computing in Science and Engineering*, vol. 19, no. 5, pp. 92–95, 2017.

[10] E. Politou, F. Casino, E. Alepis, and C. Patsakis, "Blockchain mutability: Challenges and proposed solutions," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 4, pp. 1972–1986, 2021.

[11] J. Sunny, N. Undralla, and V. Madhusudanan Pillai, "Supply chain transparency through blockchain-based traceability: An overview with demonstration," *Computers and Industrial Engineering*, vol. 150, p. 106895, 2020.
[12] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[13] substrate, "Architecture," 2023, https://docs.substrate.io/fundamentals/architecture/, (accessd on 2024.9.1).
[14] T. Inoue, "Issues concerning crowdfunding: Prospects," *Yokohama business review*, vol. 38, no. 2, pp. 35–47, 09 2017. [Online]. Available: https://cir.nii.ac.jp/crid/1390853649528004736
[15] D. Mitra, "The role of crowdfunding in entrepreneurial finance," *Delhi Business Review*, vol. 13, no. 2, pp. 67–72, 2012.
[16] Y. Uchida and T. Hayashi, "Success factors in crowdfunding," *Akamon Management Review*, vol. 17, no. 6, pp. 209–222, 2018.
[17] Y. Zhao, P. Harris, and W. Lam, "Crowdfunding industry - history, development, policies, and potential issues," *Journal of Public Affairs*, vol. 19, no. 1, p. e1921, 2019.
[18] I. Ahmed, K. Fumimoto, T. Nakano, and T. H. Tran, "Blockchain-empowered decentralized philanthropic charity for social good," *Sustainability*, vol. 16, no. 1, 2024. [Online]. Available: https://www.mdpi.com/2071-1050/16/1/210
[19] H. Zhu and Z. Z. Zhou, "Analysis and outlook of applications of blockchain technology to equity crowdfunding in china," *Financial innovation*, vol. 2, no. 1, pp. 1–11, 2016.
[20] K. Konomi and N. Kamiyama, "Providing personal credit rating system using blockchain," *IEICE Technical Report*, vol. 119, no. 460, pp. 165–168, 2020.

Hironori Tanise is currently Master course student of Osaka Metropolitan University (OMU), Japan. His research interests include Blockchain, Dapp, data security, and privacy protection.

Istiaque Ahmed is currently pursuing a Ph.D. at Osaka Metropolitan University, Japan. He holds a Master's degree in Computer Science and Engineering (2015) and a Bachelor's degree in the same field (2013), from the University of Rajshahi, Bangladesh. His research interests include Blockchain, Security and Privacy, AI, and Machine Learning. He worked as a Research Scientist at the Blockchain Economy Research Center, GIST, Korea, and has experience as a Sr. Software Eng. and Blockchain Solution Consultant. He was also a lecturer in Computer Science and Engineering at multiple Universities in Bangladesh.

Quoc Duy Nam Nguyen is currently pursuing a PhD at the Blockchain Lab, Osaka Metropolitan University, Japan. He earned his Master's degree from National Cheng Kung University in Taiwan (2021) and his Bachelor's degree from Ho Chi Minh City University of Technology in Vietnam (2019). His research spans blockchain, secure communication, artificial intelligence, and machine learning, with a particular focus on signal and image processing, deep learning, and quantitative analysis.

Thi Hong Tran (Senior Member, IEEE) received the bachelor's degree in physics and the master's degree in microelectronics from Vietnam National University Ho Chi Minh City (VNU-HCM)—University of Science, Vietnam, in 2008 and 2012, respectively, and the Ph.D. degree in information science from the Kyushu Institute of Technology, Japan, in 2014. From January 2015 to September 2021, she was with the Nara Institute of Science and Technology (NAIST), Japan, as a full-time Assistant Professor. Since October 2021, she has been with Osaka Metropolitan University (OMU), Japan, as a full-time Lecturer, and with NAIST as a Visiting Associate Professor. Her research interests include digital hardware circuit design and Dapp development related to wireless communication, communication security, blockchain technology, SHA-2, SHA-3, and cryptography. She is a Regular Member of IEEE, IEICE, REV-JEC, and others.