USE OF BLOCKCHAIN TECHNOLOGY FOR FUNDING USING SMART CONTRACT

Akash Kumar[1]
UG Scholar
Department of Computer Science & Engineering
Galgotias University, Greater Noida, Uttar Pradesh, India

Saket Kumar[2]
UG Scholar
Department of Computer Science & Engineering
Galgotias University, Greater Noida, Uttar Pradesh, India

Abstract – **Crowdfunding is a method of obtaining money online that was first used by creative people to finance their projects with small donations from the public. This project uses blockchain technology to offer smart contracts for crowdfunding. This makes it possible to provide crowdfunding in a secure, transparent, and safe environment. This project's objective is to establish interactive forms for campaign creation, financial contributions, campaign monitoring, request approval, and request finalization so that both campaign creators and contributors may easily start and support campaigns. The donor may be able to follow the progress of the funds they provided. All transactions will be recorded and stored as blocks on the blockchain. Smart contracts are an enticing aspect of blockchain technology. Without the assistance of a reliable third party, blockchain must facilitate, execute, and enforce an agreement between untrustworthy parties. It is necessary to create executable code that runs on top of the blockchain in order to do this. The code in execution is called smart contract.**

Keywords*: *Crowdfunding, BlockChain, Smart Contracts

I. INTRODUCTION

Every transaction is recorded in an immutable digital ledger called a blockchain. Since it is a distributed system, each node in the decentralized network contains a copy of every record. The Ethereum-enabled running programs in the blockchain are known as smart contracts. It enables the execution of all Smart contracts. A quick and simple way to raise money for creative project ideas would be through crowdfunding. The problem with the present crowdfunding groups is that they charge huge charges and occasionally perform tricks. Avoiding these kinds of problems will be made easier by implementing a crowdfunding process on blockchain. Shrewd agreement for crowdfunding avoids the traditional platform costs and transaction fees usually associated with other crowdfunding stages, like Kickstarter, by combining Peer to Peer lending. Our project's purpose is to create a strong application so that any ground-breaking idea can be implemented. A blockchain-based crowdfunding platform that we are planning is a website. We provide a UI that is much friendly so that anyone may get through and share their comments on this application. At that time, everyone has access to these thoughts. Everyone who wants to share their ideas is welcome to do so. Each of these cycles is carried out instinctively.

Since blockchain technology is still relatively new, there aren't many studies and researches online. Blockchain can be regarded as a distributed database that is shared among interested parties and contains records of every transaction that has ever been made. Decentralization of information, persistence, anonymity, and auditability are just some of the characteristics of blockchain. The blockchain system is made up of two main components: blocks and transactions. While the block is a collection of data that records the transaction and other associated details, such as the appropriate sequence, creation timestamp, and so on, the transaction refers to the activity that the member sets off. A blockchain's transaction records, or blocks, are linked together cryptographically to make them tamper-proof. This signifies that no embedded block may be altered or removed. Blockchain relies on consensus methods to be reliable.

An organized technique of literature review is employed in the study. A strong groundwork for research in information systems is provided by literature reviews, which also enhance the topic. The topic of blockchain within information frameworks is strengthened by a review of the literature on smart contract applications. Four steps are used to guide the survey. The audit of the examination's goal and protocol is stage 1 of the process. Step 2 entails reading the writing and determining whether it is viable. The quality assessment and information extraction are introduced in stage 3. Stage four is when we deconstruct the discoveries. This approach of doing a literature review was selected since it was created especially towards research on information systems. This is how the remaining portion is organized:

- **Planning Phase**

As part of our systematic literature review investigation, we develop a review methodology. It helps keep a thorough strategy as unbiased as possible. We explain why we're doing this review, sketch up a plan for doing so, zero in on the problem at hand, scour the literature for relevant articles, read and analyse those articles critically, and finally, present our findings.

- **Selection Phase**

In the second stage of the review, we search the Google Scholar database for research publications. We look for journal articles, conference papers, and particular white papers from 2013 to 2021 and the most well-known theories as smart contracts are a novel technology in information systems. Given that smart contracts are a relatively new information systems technology, the time span was selected. This window of time enables us to access the necessary search engine articles. . Articles were searched using the following keywords and Boolean operators: blockchain and business; blockchain and organization; smart contracts and business; smart contracts and organization; smart contracts and enterprise; and distributed autonomous organizations and businesses. These combinations were used independently in each search.

- **Requirements for inclusion and exclusion**

No content that couldn't be downloaded or seen in its entirety was considered during the first article selection process. Articles that are irrelevant to the study, were not published between 2013 and 2021, and are unrelated to blockchain technology or smart contracts are included. Incorporating prestigious white papers, journal articles, conference papers that have undergone peer review, and publications on smart contract solutions into an organization was the second stage.

- **Execution Phase**

At the third stage of the review, we gather information from articles to be used as the basis for the analysis and extract data from those that are eligible according to the research issues driving this study. Using qualitative methodologies, we extract and aggregate key information in the review's fourth step. After data analysis comes the study report's literature evaluation.

Characteristics of crowdfunding

Others have made an effort to pinpoint the characteristics and restrictions of crowdfunding within the context of the few associated literature. By fusing the social networking website with entrepreneurial financing and serving as a tool for product or service evaluation, crowdfunding is believed to upend the conventional fundraising cycle. De Buysere et al. (2012) proposed many advantages project owners receive from crowdfunding:

• Capital raising.
• Getting insightful feedback before introducing the good or product to the general population.
• Determining the potential market for the suggested idea and obtaining a "Proof of concept."
• Establishing early relationships with customers.
• Assist with the product or service's marketing.

Funders also profit in a variety of ways at the same time:
• Social return as people see the initiative they funded becoming a success.
• Financial return if they made an investment in the project (CFI model) or a material return by receiving a reward (donation-based approach).

II. METHODOLOGY

The proposal is an online platform that essentially improves the current techniques for crowd fundraising. Blockchain is frequently seen as a democratic tool that enables individuals to interact and operate as they see fit by utilizing decentralized networks. By leveraging tax deductions as an incentive, adopting blockchain as a method for crowdsourcing may frequently increase the potential donor pool. This encourages donors to donate with fewer constraints and offers transparency throughout the giving process. In summary, blockchain crowdfunding may be viewed as a solution to reduce the need for centralized gatekeepers and large-scale facilitators while enabling more cash to be contributed in an unconventional fashion Depending on whatever procedure has to be automated and integrated into the blockchain ecosystem, a smart contract is a self-executing agreement between an investor and a fundraiser, a platform and a user, or between other parties. The money will be retained in the smart contract itself rather than being transferred to the campaign creator directly. The campaign creator must create an expenditure recommendation if they want to use this sum. Following that, the campaign creator's request should be approved by the approvers (contributors). Due to the usage of blockchain technology in its implementation, the voting mechanism is decentralized. This guarantees the voters' privacy while increasing the voting system's security and efficiency. If the necessary number of votes is attained, the campaign creator can complete the payment. Security is boosted during the process, and contributors' opinions are also solicited. The problem with the current system is that organizations charge both the client and the beneficiary heavily. There is no documentation of the money, honesty, or contact between both the donor and the customer during the project's development. Trust is the biggest problem with crowdfunding among the already operating companies. These groups do not have benefactor guarantee insurance.

- Excessive charges
- Lack of a donor guarantee policy
- Lack of transparency
- Lack of data

Under the suggested framework, the goal developers will put their task ideas in the project, and others who are interested will donate money to the task idea. The main way it differs from previous forms of crowdsourcing is that all of the money is presently provided in virtual currencies (digital money) like ether. The blockchain, an immutable ledger, will be used to store and trace all ether deposits. Subsidized money is within the hands of donors. The donor has complete control over the money they invested thanks to the Request endorsement module. Only in case the creators' solicitation needs to be approved by the majority of investors. Gaining control of investment funds builds trust.

- Financial control over money

- Trust
- Without fees
- Guarantee Policy
- Documentation of all transactions
- All transactions are secured

Overview

On the Internet, crowdfunding and crypto currency are both widely used, and they work well together. A solution that can deal with many of the problems that occur in crowdfunding is blockchain innovation. The terms of the agreement provide that all money will be deposited into the pool. All of the money will be sent to the recipient after the request satisfies the established requirements. Blockchain-based A public, online platform for payment systems is Ethereum. With the use of transaction-based state changes, it is a modified version of Bitcoin. The Ethereum platform creates and supports the cryptocurrency known as ether. The EVM (Ether Virtual Machine), which would be provided by Ethereum, is a decentralized computing platform that can run a program on open hubs.

Blockchain

The blockchain was first launched from the mysterious people' invention of Bitcoin. Blockchain technology may be understood by thinking of it as a shared Google Doc. When you share a Google Doc with a group of people, the document is not copied or moved; it is simply distributed. As a result, a decentralized distribution chain is established, enabling simultaneous access by all parties to the source text. Each Block has a connection to the others, and cryptography was used to secure them. Following categories of blockchain exist:

i. Public (Bitcoin and Ethereum)
ii. Consortium (Hyperledger and Ripple)
iii. Private (private blockchain) and
iv. Hybrid (hybrid blockchain).

Peer to Peer

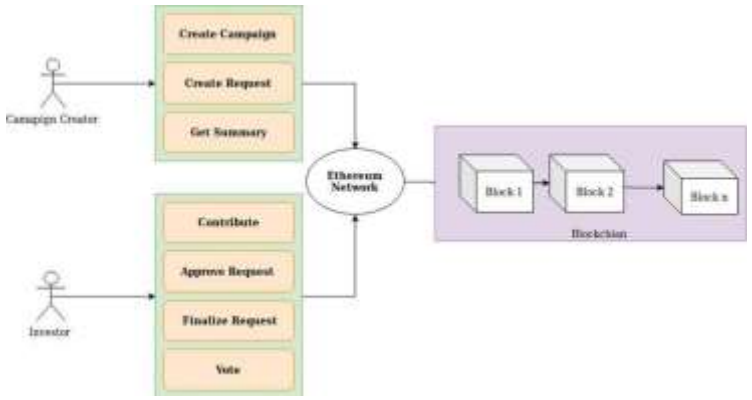
Blockchain is a distributed ledger system that stores transactions as immutable digital blocks with senders and recipients identified. The blockchain networks are run by decentralized organizations, and only the members may approve transactions amongst themselves.

Consensus Protocol

Blockchain networks employ consensus methods to reach an agreement amongst a wide variety of geographically separated nodes. Proof of stake (PoS) and proof of work (PoW) are two examples of consensus methods that may be used to increase network security by preventing fraudulent transaction confirmations by unauthorised users.

Various consensus algorithm:

- Proof of Work (PoW)
- Practical Byzantine Fault Tolerance(PBFT)
- Proof of Stake(PoS)
- Proof of Burn(PoB)
- Proof of Capacity
- Proof of Elapsed Time



- **Proposed Algorithm**

1. Open Metamask account.
   1.1. Then open Ethereum account.
2. Create Smart Contract.
   2.1. Create a Campaign.
   2.2. Create factory contract.
3. Then Deploy Campaign Factory contact to create instances of the Campaign.
4. Deploy Campaign contract.
5. Start the server on the terminal.
6. Open localhost:3000/3600 in chrome or any browser :- In the browser's page the list of all created campaign is available.
7. If Campaign is not available then create a campaign by entering minimum contribution required.
8. View a particular campaign detail:

   The view campaign page includes the following information about the campaign's originator:
   - The creator's address.
   - The bar for participation is set low.
   - Quantity of calls.
   - Number of supporters.
   - A well-rounded campaign.
9. Contribute to the campaign to become approver.
10. Manager creates the spending request to spend the campaign money by providing description of the request, amount required for the request and the address of the receiver.
11. Created requests are approved by the approvers. If approval Count is greater than half of the approvers Count then request is approved else the request is not approved.

.

12. If the request is accepted, the Creator will complete it and send the receiver the specified sum.

III. MODELING AND ANALYSIS

Model to implement and administer the project, the following software requirements must be downloaded and set up:

Metamask Wallet
Metamask is a self-hosted wallet that enables users to save, transmit, and accept Ethereum or ERC20 tokens directly from their web browser without the need to operate a complete Ethereum node. It enables the creation of an unlimited number of accounts that resemble bank accounts. Installing the Metamask wallet requires using the Chrome browser, and configuring the wallet's network parameters to use the Rinkeby test network. Afterwards, some fictitious Ethereum (money) is sent from the Rinkeby tap to the account that's being utilized by the project by providing its address in order to test and execute the project.

Infura key:
The Ethereum blockchain may be contacted using the Infura API Key. This serves as the API Key needed to operate Butler.

Atom
According to its official description, "Atom - A Hackable Text and Code Editor for Linux," Atom is a free and open-source text and source code editor developed by GitHub. It was dubbed by its developers to be a "hackable text editor for the 21st century" (Atom 1.0). It is easy and convenient for users to customize Atom to their preferences because to the availability of third-party packages and themes.

Ethereum: It is a blockchain-based platform. The cryptocurrency ether (ETH) is the platform's claim to fame. Blockchain technology developed by Ethereum allows for the creation and upkeep of transparent and trustworthy digital ledgers.

System flow:

Modules
When an online application is opened, it will first display the campaign page. Existing campaigns are displayed here, and selecting create campaign will lead us to a new page where we may complete the necessary financial transaction to launch a new campaign.

The campaign's details, such as the manager's address, the minimum donation, the number of applications the leader issued, the number of approvers, and the campaign's total balance, may be viewed here after clicking the see campaigns button on the first page. Donors have a voice in campaign decisions.

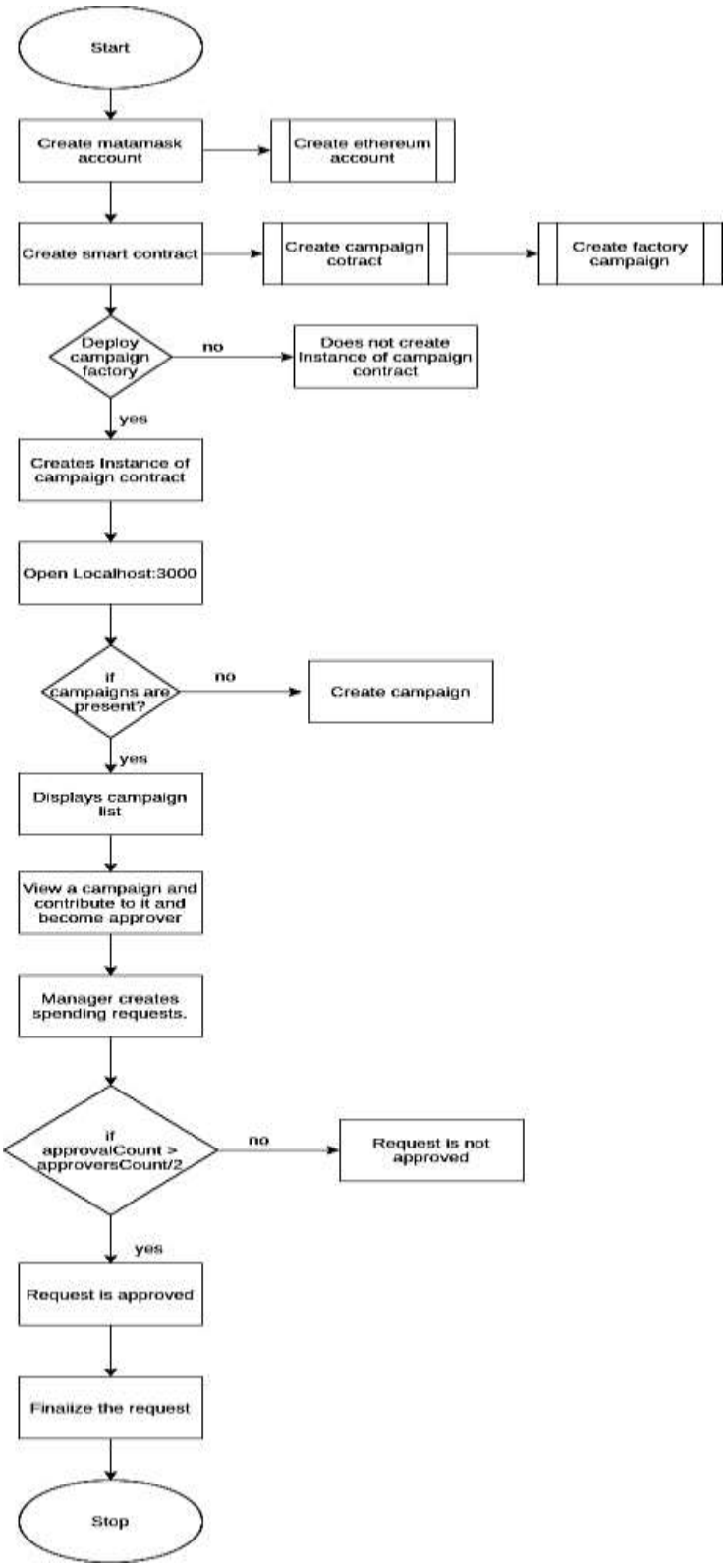


Fig. **Flowchart of the project**

When contribute button is pressed after entering the contribution in ether you become an approver to the campaign.

```
struct Request{
    string description;
    uint value;
    address recipient;
    bool complete;
    uint approvalCount;//keeps track of
    mapping(address=>bool)approvals;
}//every instance of request struct wil
```

Fig. Request function to check request's description

If you want to see what people have asked for, click the View Requests link. Here are the manager's specific needs. It also has a finalization and approval button. When a payment request has received the necessary number of votes, the manager will click the "Finalize button" to process the payment.

```
Request[] public requests;
address public manager;/* people could fi
uint public minimumContribution;
//address[] public approvers;
mapping(address=>bool)public approvers;
uint public approversCount;//keeps count
```

Fig. Checking number of approvers with this function.

When a creator clicks the add request button, they are sent to the create request web page, where they may enter the details of the purchase, including the reason for the purchase, the amount of ether the management wishes to pay, and the vendor's address.

```
function createRequest(string description,uint value,address recipient) public restricted
{
    Request memory newRequest=Request({
        description:description,
        value:value,
        recipient:recipient,
        complete:false,
        approvalCount:0
    });//we we create new instance of struct we only have to initialize value types not re


    requests.push(newRequest);
}
```

Fig. Request function to make request in campaign

If the request receives a majority vote of approval, it will turn green and be ready for the manager to finalize. There's a "add request" button on the request that only the creator may click to make spending requests.

```
function approveRequest(uint index) public
{
    Request storage request=requests[index];/
    //1. first check that person must be a co
    require(approvers[msg.sender]);
    //2. the person must not have already vote
    require(!request.approvals[msg.sender]);

    request.approvals[msg.sender]=true;//we re
    //and then increse approvals count for thi
    request.approvalCount++;
}
```

Fig. Approve Request Function

```
function finalizeRequest(uint index) public restricted//only ma
{
    Request storage request=requests[index];
    //whenever a request is finalized we make complete as true
    require(request.approvalCount>(approversCount/2));//atleast
    require(!request.complete);

    request.recipient.transfer(request.value);//sending all the
    request.complete=true;
}
```

Fig. Function to finalize a request

The request will become grey after it has been fulfilled and the required amount has been transferred to the seller. The request has been closed, as shown by this status. To guarantee a smooth transaction, the wallet's funds are verified both before and after the request is complete.

IV. RESULTS & DISCUSSION

The first step in raising capital with blockchain-based crowdsourcing is to begin a campaign. Investors may use the unique 64-character public key provided to the campaign as an address to send funds. Investors may utilize Ether as a payment option. Instead of going to the individual who launched the campaign, the money will remain in the smart contract. The author of a campaign who wants to spend money on the campaign must first submit a spending request detailing the amount of ether needed and the address or public key of the vendor to whom the ether should be transferred. Donors are responsible for authorizing any use of the ether they provide before it is released from the smart contract. If more than half of those voting choose to give the money to the seller, they may do so right now. This method of crowd fundraising is far more efficient and safe than the present process. Because of the current system, the campaign creator has access to the funded money and can continue without the amount, the distribution of the money raised is slow, and a fee will be deducted from the donation because a third party, such as Kickstarter, is involved in generating the necessary funds. Therefore, Blockchain Crowd Funding is a novel and more efficient method for startups to get capital.

.

V. CONCLUSION

Blockchain technology can increase the transactions' transparency. Users may feel more certain when they wish to contribute to a cause as a consequence. Contributors can learn more about how their money is being used by using smart contracts on expenditure requests.
Every time the campaign's creator wants to spend money, they must submit a spending request stating the reason for doing so, who the money is being sent to (vendor), and how much is required. This ensures that the money donated by investors is protected as well as that each judgement taken with the assistance of donated funds involves the opinion of the investors. The resilience of the blockchain to various attacks is advantageous for smart contracts. Other advantages of the programme is to include increased dependability and quicker, more effective operating. The web application was validated using "test cases". Users may use the application to carry out the requested operation because it is user-friendly, offers the necessary options, and is accessible. The following objectives were met by the website:

- Starting a campaign
- Contributing to a campaign
- Drafting a funding request
- Approving the funding request
- Submitting the request

These are all steps in the process.

In this paper, we identified a few research gaps in the field of smart contracts in this paper that call for more study. The areas that still need to be filled in include research on scaling and performance issues, the use of smart contracts on blockchains other than Ethereum, the sparse number of applications utilizing intelligent system contracts, the paucity of high-quality research on smart contracts and the dearth of studies on criminal conduct in smart contracts. Future academic works may devote attention to filling these voids.

VI. REFRENCES.

[1] N. Szabo, The idea of smart contracts, Nick Szabo's Papers and Concise Tutorials (1997). URL http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart contracts 2.html

[2] H.-N. Dai, Z. Zheng, Y. Zhang, Blockchain for internet of things: A survey, IEEE Internet of Things Journal (2019). URL https://doi.org/10.1109/JIOT.2019.2920987

[3] A. Bogner, M. Chanson, A. Meeuw, A decentralised sharing app running a smart contract on the ethereum blockchain, in: Proceedings of the 6th International Conference on the Internet of Things, 2016, pp. 177–178 (2016).

[4] Y. Zhang, J. Wen, An IoT electric business model based on the protocol of bitcoin, in: Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), 2015, pp. 184–191 (2015).

[5] P. McCorry, S. F. Shahandashti, F. Hao, A smart contract for boardroom voting with maximum voter privacy, IACR Cryptology ePrint Archive 2017 (2017) 110 (2017).

[6] L. Luu, Y. Velner, J. Teutsch, P. Saxena, SMART POOL: Practical Decentralized Pooled Mining, in: 26th USENIX Security Symposium (USENIX Security), 2017, pp. 1409–1426 (2017).

[7] E. Hillbom, T. Tillstrom, Applications of smart contracts and smart ¨ property utilizing blockchains, Msc thesis in computer science, Chalmers University of Technology and University of Gothenburg, Sweden (2016).

[8] A. Yasin, L. Liu, An online identity and smart contract management system, in: Proceedings of 40th Annual Computer Software and Applications Conference (COMPSAC), Vol. 2, 2016, pp. 192–198 (2016).

[9] V. Scoca, R. B. Uriarte, R. De Nicola, Smart contract negotiation in cloud computing, in: Cloud Computing (CLOUD), 2017 IEEE 10th International Conference on, IEEE, 2017, pp. 592–599 (2017).

[10] J. Wan, J. Li, M. Imran, D. Li, et al., A blockchain-based solution for enhancing security and privacy in smart factory, IEEE Transactions on Industrial Informatics (2019).

[11] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, M. Imran, Securing iots in distributed blockchain: Analysis, requirements and open issues, Future Generation Computer Systems (2019).

[12] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in: 2017 IEEE International Congress on Big Data (BigData Congress), IEEE, 2017, pp. 557–564 (2017).

[13] S. Omohundro, Cryptocurrencies, smart contracts, and artificial intelligence, AI matters 1 (2) (2014) 19–21 (2014).

[14] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Generation Computer Systems (2017).

[15] N. Atzei, M. Bartoletti, T. Cimoli, A Survey of Attacks on Ethereum Smart Contracts (SoK), in: Proceddings of International Conference on Principles of Security and Trust, 2017, pp. 164–186 (2017).

[16] K. Delmolino, M. Arnett, A. Kosba, A. Miller, E. Shi, Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab, in: Proceedings of International Conference on Financial Cryptography and Data Security, 2016, pp. 79–94 (2016).

[17] D. Harz, W. Knottenbelt, Towards safer smart contracts: A survey of languages and verification methods, arXiv preprint arXiv:1809.09805 (2018).