APPLICATION OF BLOCKCHAIN TECHNOLOGY OF FUNDING USING SMART CONTRACT

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

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

Rashmi Rathi[3]
Assistant Professor
Department of Computer Science & Engineering
Galgotias University,Greater Noida, Uttar Pradesh, India

***Abstract* – Crowdfunding is an online fundraising strategy that originated as a means for the public to donate small amounts of money to support innovative projects. This project aims to propose a smart contract solution for crowdfunding using blockchain technology, providing a secure and transparent method of fundraising. The objective of this project is to develop an interactive platform for campaign creation, contribution, viewing, request approval, and finalization, enabling both campaign creators and contributors to effortlessly create and finance campaigns. Contributors will be able to track their contributions, which will be recorded and stored on the blockchain as a block. A compelling feature of blockchain technology is the ability to facilitate, execute, and enforce agreements between untrusted parties without the involvement of a trusted third party through the use of smart contracts. To accomplish this, an executable code must be implemented on top of the blockchain, which is known as the smart contract**.

Keywords*: *Block Chain, Crowdfunding, Smart Contracts

I. INTRODUCTION

The blockchain is an incorruptible digital ledger that records every transaction. It is a distributed system thus all the records are stored in every node in the decentralized network. Smart Contracts are the running applications in the blockchain allowed by Ethereum. It allows running of all the Smart contracts. Crowdfunding provides an easy way to find cash for innovative project ideas. The issue with the current crowdfunding organizations charging high expenses and once in a while there were tricks occurred. Actualizing a crowdfunding procedure in blockchain will assist with staying away from these sorts of issues. By consolidating Peer to Peer shrewd agreement for crowdfunding eliminates the customary transaction charges and platform expenses typically connected with other crowdfunding stages, for example, Kickstarter. The target of our undertaking is to make a solid application with the goal that each groundbreaking thought gets life. We have planned a crowdfunding site which is a blockchain based website. We give a simple to utilize interface for everybody to make and post their thoughts on this application. These thoughts at that point become public to everybody. Any individual who wishes to help their thoughts can contribute. Every one of these cycles are done in an intuitive way.

Blockchain is fairly new technology, there are only few studies and researches available on the internet. Blockchain can be characterized as a distributed database of records of all transactions that have been executed and sharedamonginterest members. The attributes of blockchain incorporates decentralization of information, persistency, anonymity and auditability. There are two primary parts in blockchain framework, which are transaction and block. Transaction speaks to the activity set off by the member, while the block is a collection of information recording the transaction and other related subtleties, for example, the right sequence, timestamp of creation, and so on. The transaction records, or blocks, in a blockchain are connected together cryptographically, delivering them tamper proof. This implies each block that have been embedded can't be changed or erased. To achieve reliability, blockchain uses consensus algorithms.

The research uses a systematic literature review method. Literature review gives a good foundation for research in information systems and strengthens information system as a field. An audit of literature of smart contract application reinforces the field of blockchain inside information frameworks. We direct the survey in four stages. Stage 1 is the audit of the purpose and protocol of the examination. Stage 2, includes looking through the writing and viable screening. In stage 3, the quality examination and information extraction are introduced. In stage 4, we break down the discoveries. This literature review method is chosen because it is developed specifically for information systems research. The remaining part of the section is structured as follows:

- **Planning Phase**

We design a review method which is important in conducting a systematic literature review study. It minimizes biases in a detailed plan. We discuss the purpose of the review and design a protocol, identify the issue, search the literature, evaluate texts, critically reading and analysing texts and present the review results.[8]

- **Selection Phase**

In the second phase of the review, we look for the research articles using Google scholar database. Since smart contract is a new technology in information systems, we search for journal papers, conference papers, select white papers from 2013 – 2018 and most influential theories. The time frame

was chosen considering that smart contract is a new technology in the field of information systems. This time frame helps us to get the required articles from the search engine. In the search for articles, the keywords and Boolean operators used are as follows: smart contract + business, smart contract + organization, smart contract + enterprise, blockchain + business, blockchain + organization, blockchain + enterprise, distributed autonomous organization +business, decentralized autonomous organization + enterprise. [12] These pairs were used independently in every search. From the results of these searches, we conducted an efficient screening process. We excluded articles not relevant to the study, duplicates, and articles that we could not obtain the full text of. In addition to reading the articles, we carried out a practical screening.

- **Exclusion and Inclusion criteria**

Articles that cannot be downloaded or accessed as a full paper have been excluded from the first step of article selection. These include articles that are irrelevant to the study, articles not published between 2013 and 2018, and articles that are not related to blockchain and smart contracts. Second step involved including high-quality white papers, journal articles, peer-reviewed conference papers,and articles on smart contract applications in an organization. [5]

- **Execution Phase**

In the third phase of the review, we extract data from eligible articles based on the research questions guiding this research and collect information from articles to serve as raw material for the analysis. In the fourth phase of the review, we extract and combine essential facts using qualitative techniques. [12]Data analysis is followed by the literature review study report.

Features of Crowdfunding:

Within the domain of little related literature there have been attempts by some to identify the features and limitations of Crowdfunding. Crowdfunding is said to disrupt traditional funding cycle by merging the social web with entrepreneurial finance, as well as being a validation tools for products or services. De Buysere et al. (2012) suggested a number of benefits that project owners gain with Crowdfunding:

- Raising capital.
- Gaining valuable feedback before releasing the product or service to the market.
- Understanding if the proposed idea has a mass appeal and getting a "Proof of concept".
- Building early connections with customers.
- Support Marketing for the product or service. [14]

In the same time, funders gain a number of benefits as well:

- Social return as they see the project, they have supported realized
- Material return by getting a reward (Donation-based model)
- Financial return if they invested in the project (CFI model

II. METHODOLOGY

The project is a web application which is basically an enhancement of the existing crowd funding systems. Blockchain is widely considered a democratic tool that uses decentralized systems to give people the freedom to collaborate and transact as they see fit. Using blockchain as a tool for crowdsourcing can in many cases expand the possible pool of donors by using tax deductions as an incentive — thereby promoting the ability to give with fewer restrictions and providing transparency through the giving process. In short, blockchain crowdfunding can be seen as a way to allow more capital to be donated in a nontraditional way while reducing the need for large-scale facilitators and centralized gatekeepers. [13] A smart contract is a self-executing agreement between investor and fundraiser, platform and user, or between other parties depending on which process needs to beautomated and put into the blockchain ecosystem. The amount will not be directly given to campaign creator rather it will be held in smart contract itself. If the campaign creator wants to use this amount, he/she has to create a spending request. Then the approvers (people who have contributed to the campaign) should approve the request created by the campaign creator. The voting system used is decentralized as blockchain technology is used in implementing it. [16] This makes the voting system more secure and also cost efficient while guaranteeingthe voters privacy. Campaign creator will be able to finalize thepayment once the required votes are obtained. In the process, security is increased and also the peoples/contributor's opinion is taken. In the existing framework, the issue is that organizations charge intensely to both the benefactor andthe client. There is no record of the cash, directness, or communication between the investor and the client in buildingup the project. [11] Among the existing organizations, trust is the foremost issue with crowdfunding. None of these organizations offer benefactor guarantee policies. [7]

- Not Transparent
- High Charges
- Donor guarantee policy not available
- No track of Records

1. In the proposed framework, the mission makers will post their task thoughts in the mission and the intrigued individuals will donate the fund to the undertaking thought. Where it differs from the old crowdfunding is that all the cash is currently digital currencies like ether. All ether deposits will be recorded and tracked in the blockchain, which is an immutable ledger. Donors have control over subsidized cash. With the Request endorsement module, the donor has full command over the cash they invested. Just in case a majority of the investorsneed to approve the solicitation made by the creators. By giving control over invested money, trust is gained. [15]

- Trust
- Control over money

- No charges
- Donor Guarantee Policy
- All transactions are recorded
- Money is Stored Securely.

- **Overview**

Both Crowdfunding and Cryptocurrency are prevalent on the Internet and they coordinate impeccably. Blockchain innovation is a solution that can address many of the issues that arise in crowdfunding. The contract is written such that all cash will be added to the pool. [12] Once the solicitation meets the predetermined criteria, all the cash will be moved to the beneficiary. Blockchain-based Ethereum is an open-source, public platform for smart contracts. It is the modified form of Bitcoin via transaction-based state transitions. Ether is a Cryptocurrency which is created and supported by the Ethereum platform. Ethereum provides a decentralized computing system, the Ethereum Virtual Machine (EVM), which can run applications on public hubs. [7]

Blockchain

The blockchain is initially started from the Bitcoin, invented by obscure individuals.A simple analogy for how blockchain technology operates can be compared to how a Google Docs document works. When you create a Google Doc and share it with a group of people, the document is simply distributed instead of copied or transferred. This creates a decentralized distribution chain that gives everyone access to the base document at the same time. . Each Block is connected to one another and they were secured using cryptography.. Blockchains can be divided into three sorts: 1) public blockchain (Bitcoin and Ethereum); 2) consortium blockchain (Hyperledger and Ripple); 3) private blockchain and 4)hybrid bockchain. [8]

Peer to Peer

As a distributed ledger technology, blockchain records transactions as an immutable timestamped digital block that indicates senders and receivers. No centralized authority manages the blockchain networks and only the participants can validate transactions among each other. [7]

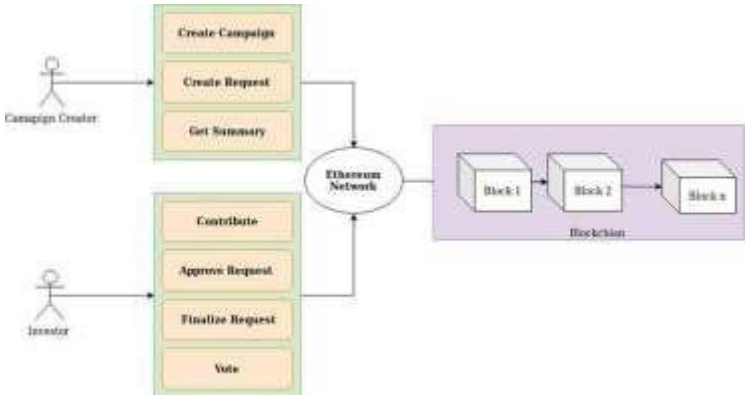
Consensus Protocol

Blockchain networks rely on consensus algorithms to reach agreement among various distributed nodes. A consensus mechanism such as proof of work (PoW) or proof of stake (PoS) secures the network and prevents unauthorized users from validating bad transactions. [7]

Various consenses algorithm:

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

Figure 1



- **Proposed Algorithm**

1. Create Metamask account.
   1.1. Then create an Ethereum account on Rinkeby Test Network.
2. Create Smart Contract.
   2.1. Create Campaign Contract.
   2.2. Create factory contract.
3. Deploy Campaign Factory contact. (It creates instances of Campaign Contract)
4. Deploy Campaigncontract.
5. Start the server by running the command “npm run dev” in terminal.
6. Open localhost:3000 in browser:
   Main page will be loaded which shows the list of all campaigns created so far.
7. Createa campaign (Byclicking Create Button) by entering minimum contribution in wei.
8. View a particular campaign detail:

   The view campaign page shows:
   •Address of Manager who created the campaign.
   •Minimum contribution.
   •Number of requests.
   •Number of approvers.
   •Campaign balance.

9. Contribute to the campaign to become approver.
10. Manager creates the spending request to spend the campaign money.
    The request is created by providing:
    •Description about the request.
    •Amount to be spent on that request.
    •Address of the recipient.

11. Request are approved by the approvers.

if(approvalCount > (approversCount/2)){
Then request is approved }
else{ Then request is not approved. }

12. Manager will finalize the request if it is been approved and the requested amount will be sent to the recipient.

III. MODELING AND ANALYSIS

Model In order to implement and run the project there are some software requirements that need to be installed and configured as mentioned below:

Metamask Wallet
Metamask allows to run Ethereum decentralized applications in the browser itself without running a full Ethereum node and it is a self-hosted wallet to store, send, and receive Ethereum or ERC20 tokens. It allows to create n number of accounts which are just like bank accounts. [7] Metamask wallet has to be installed from the chrome browser and network has to be set to Rinkeby test network which is available in options at top of the wallet. Then in order to test and run the project some fake Ethereum(currency) is transferred from Rinkeby faucet to the account being used in the project by giving it saddress. [11]

Infura key:
The Infura API Key is used to communicate with the Etthereum blockchain. This is the API Key that is required for running Butler.

Atom
Atom is a free and open-source text and source code editor developed by GitHub (Atom – A Hackable Text and Source Code Editor for Linux). Its developers call it a "hackable text editor for the 21st Century" (Atom 1.0). Atom enables users to install third-party packages and themes to customize the features and looks of the editor, so you can set it up according to your preferences and with ease (Atom). [11]

Ethereum: Ethereum is a blockchain-based platform best known for its cryptocurrency, ether (ETH).The blockchain technology that powers Ethereum enables secure digital ledgers to be publicly created and maintained. [11]

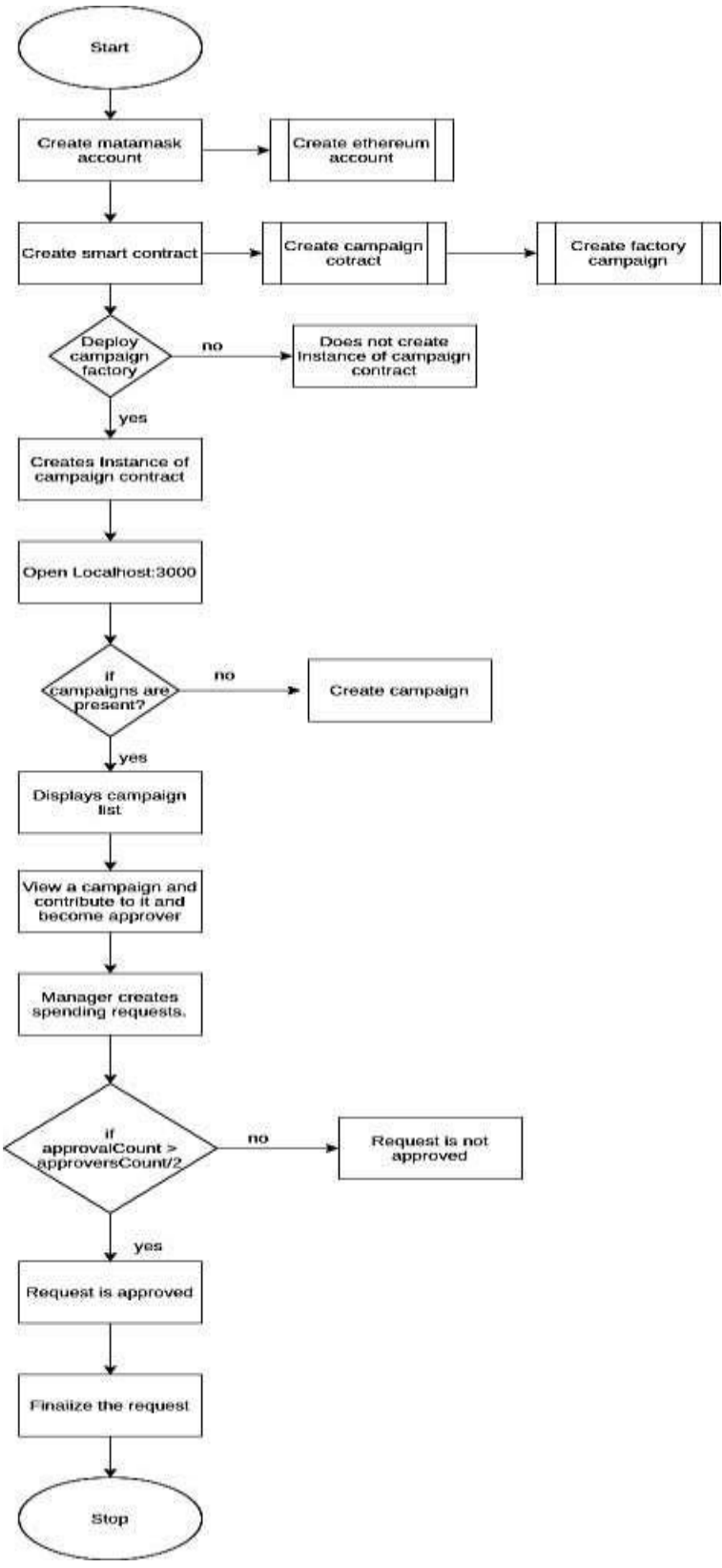
System flow:

Modules:
When the web application is started the first page that is seen is campaign page where existing campaigns are displayed and a new campaign can also be created When create campaign is clicked it will redirect us to the page where a transaction needs to be performed in order to create a new campaign. [6]

When view campaigns button is pressed which is present in first web page it will be redirected to this page which consists of campaigns details like address of person who created the campaign (Manager), minimum contribution, number of requests created by manager, number of approvers and campaign balance as. Investors can contribute to the campaign and become an approver. [6]

Flowchart of the project

Figure 2



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

Pressing the view requests button will redirect you to the view requests page. The manager's requests are listed here. Additionally, it has a button for approving and finalizing. Approve buttons used by approvers to vote and Finalize button is used by manager to finalize the payment once the request gets enough number of votes.

When add request button is pressed it will be redirected to crea te request web page as shown in where a request can be created by specifying description of spending request, value in ether that you want to spend and address of recipient to whom manager wants to send mone y (vendor address).

In the event the request gets enough approvals/majority votes, it turns green and can be finalized by the manager. The request also contains an add request button, which is used to create spending requests, which can only be done by the manager (person who created the campaign).

Upon completing the request, the amount will be sent to the vendor address that was specified, and the whole request will turn grey after completion. Indicating that the request has been closed. The mo ney/currency in the wallet is checked before and after finalizing the request in order to ensur e that the transaction executed successfully.

IV. RESULTS & DISCUSSION

In Crowd Funding using blockchain to raise money for a startu p first a campaign has to be created and a unique 64- character public key is assigned to that particular campaign to which investors can use as an address to donate. Investors can contribute the money in the form of ether. The contributed money will remain in the smart contract itself and will not be sent to the campaign creator. Whenever a campaign creator wants to spend money on the campaign, he or she has to create a spending request which will include the amount of ether needed as well as the address or public key of the vendor to whom the ether should be sent, so that campaign creator would have the required material. This ensures that the contributed ether is always kept inside the smart contract and contributors must vote on the spending request. In the event that the percentage of votes is at least 51 percent, the amount will be automatically transferred to the vendor. This method of Crowd Funding is considerably faster and more secure than the existing system.Due to the current system, funded money is in the hands of the creator of the campaign, which means they can run off with the money, transfer of the money raised is slow and there will be a fee cut from the contribution because a third party, like Kickstarter, is involved in raising the required capital. As a result, Blockchain Crowd Funding is a more efficient and revolutionary method for raising capital for startups. [17]

Tabl :

Below are some projects has been solved in different method

Projects	Method	Keywords
Startups and Sources of Funding	Distal marketing	Startups, Funding, Growth, and Decision making
Financing the Startup Economy - A Critical Study	Investor Web application / Smart India website	Startup, Financing, India
Indian startup ecosystem: analysing investment concentration and performance of government programmes	Startups —India/ Smart India website	Startups —India, Investment in startups, Concentration among startups, Startups — Indian government programmes

V. CONCLUSION

Blockchain technology can enhance the transparency of crowdfunding transactions. As a result, users can feel more confident when they want to donate to a campaign. The application of smart contract on spending request also can help contributors to know how their money are being spent.

Smart contracts enable a secure way to raise money by assuring that money donated by investors is protected, as well as ensuring that each decision made with the help of donated funds involves the opinion of the investors i.e. whenever the creator of the campaign wants to spend money, they have to make a spending request indicating the purpose for using the funds, who the money is being sent to (vendor), and how much is needed. Smart contracts benefit from the fact that the blockchain is resilient against many threats.. The software also offers many benefits, such as improved reliability, faster, and more efficient operation. "Test cases" were taken in order to validate the web application. The application is user-friendly, has the required options, and can be used by users to perform the desired action. The goals achieved by the website are:

- creating a campaign
- Contributing to campaign
- Creating a spending request
- Approving the spending request
- Finalizing the request

VI. REFRENCES.

[1] N. Szabo, The idea of smart contracts, Nick Szabo's Papers andConcise 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).

[18] M. Bartoletti, L. Pompianu, An empirical analysis of smart contracts: platforms, applications, and design patterns, in: International Conference on Financial Cryptography and Data Security, Springer, 2017, pp. 494–509 (2017)