IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BUILDING A SMART CONTRACT BASED ESCROW PLATFORM FOR CROWDFUNDING ON BLOCKCHAIN

Bhavika Mathur, Research Scholar, JECRC University, Jaipur (Raj.)

Abstract

This paper is aimed at the investigation and review of the social crowdfunding platforms. We study the prevalent high cases of corruption and fraud in the delivery of financial benefits to the intended recipients on the social crowdfunding platforms. We also study the current model of public and private tender funding structure and the causes of cost-overruns and contract-failure in these projects. We discuss a novel theoretical and practical model of giving the control of money to the original funders based on a conditional contract. We review and postulate a new blockchain based funding model to fund the causes on social crowd-funding platforms and also the Public/Private/PPP (Public Private Partnership) projects. We also discuss how adoption of a transparent mechanism of funding will make it easier to attract funding for genuine projects and inspire confidence of the general community.

Keywords: *Smart Contract, Blockchain, Solidity, Crowdfunding, Escrow, Fraud Prevention, Non-profit, Government Tenders, Distributed Ledger Technology.*

Introduction

Crowdfunding can be defined as a way of raising funds for a project or a campaign by the initiative of an individual or an organization via common accessible crowd- funding platforms. The data suggests that the crowdfunding initiatives that are non-profit are more likely to succeed and attract a greater corpus of donation amount than other forms of initiatives. Crowdfunding of projects via platforms like Kickstarter or Indiegogo gives Power to micro-investors — investors who can invest small amounts of Capital in projects thereby increasing the diversity of the cap-table of a project by orders of magnitude.

Crowdfunders also gain access to hitherto Inaccessible opportunities to invest in varied projects — from community driven initiatives to big start-ups who are building disruptive products. The patterns in crowd-funding change sharply and every wave of change decides how the funds are allocated to the causes and projects. In year 2020, $34 Billion have been raised through crowd-funding. An individual crowd-funding campaign raises an average of $568 (INR 40,000)1. Entrepreneurs, individuals, and non-profit organizations that initiate crowd-funding campaigns have the benefit of highlighting a cause or a project and gaining initial traction.

Blockchains have become the foundation of future crypto-assets class. But one of the most important uses of blockchain is also as a mode to make secure and energy- efficient online transactions. The most common problem with existing crowd-funding and tender platforms is that the there is no two-way binding parity between the goal and distribution of funding. Also, most of the crowd-funding platforms are not regulated, and thus a sizeable chunk of crowd-funding initiatives turn out to be frauds.

A multi-variate study2 (Glaeser and Shleifer, 2001) found out that non-profits find it easy to attract funds on crowd-funding platforms in relative comparison to others. The process of raising funds on crowdfunding platforms is standardized and is usually created according to the playbook of the platform.

There are multiple benefits of using a smart contract based crowdfunding platform including transparency, efficiency, security, and speed. Using a blockchain ensures that the crowdfunders community has the utmost control over the disbursement and the execution timeline of the project. The crowdfunders' community can also add their own votes which are subject to approval by the community.

Problem Statement

One of the main benefit of crowdfunding is that it is one of the most accessible way of raising funds in a short amount of time. It is also a very transparent way for investors to find projects that they are interested in and fund them. However, the biggest challenge for traditional crowd-funding platforms is the high rate of fraud cases. A long-term study3 (Gabison, et. al., 2015) studied the regulatory framework for the frauds committed on the crowd-funding platform. They outlined that due to the global nature of accessibility of crowd-funding platforms and the donors spanning multiple geographies, it is difficult to enforce traditional anti-fraud legal and security measures on such platforms.

Furthermore, there is also an issue of cost and time overruns on the crowd-funded projects. Most of the time, the fundraisers or the entrepreneurs do not deliver the goods or services or the results on the stipulated timeline. An exploratory study4 (Mollick et al, 2014). has shown that over 75% of the crowd-funding projects deliver products later than promised.

Theoretical Framework

In this section, we will explain the theoretical framework that proposes a blockchain based fraud-resilient crowdfunding platform with an intermediary escrow platform for fund disbursing. We also explain how such a model has an inherent smart-contract design that enforces project execution timeline, donation, and refund conditions.

A blockchain is a decentralized and distributed digital ledger that is used to record transactions across a network of computers. There is no 'central authority' in a blockchain. A smart contract, according to Wikipedia, is "a computer program or a transaction protocol which is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement".

A transaction represents an action of the participants. Any action can be defined as a "transaction" by the programmer of the decentralized application. For private organizations, the crowd-funding model is preferable to traditional funding as long as the capital requirements for the initial product/project funding is below the initial financial momentum gained via the crowd-funding platform. By implementing a smart contract based escrow layer in the current crowd-funding structure, we can create a contract that will escrow the funders' money until the following conditions are met:

a) When the goal amount is reached
   i. Once the contributors vote for initial release of funds as per the underlying consensus algorithm, a Minimum Threshold Capital (MTC) from the escrow is released to the fundraisers to begin the work. The MTC is defined in the smart contract.
   ii. Any subsequent work is divided into milestones as per the contract and again the contributors can decide to release the next stage of amount from the escrow to the fundraisers. The fundraisers have to raise an expense request to get the next round of money released.
   iii. If there is fraud or time or cost overruns, the contributors can vote, as per the underlying consensus algorithm, to recover money from the escrow fund to the extent of their initial contribution and exit the project; or The contributors can exit the project and initiate a request blacklist the fundraisers and their address.

b) When the goal amount is not reach
   i. The contributors vote to either extend the timeline until the goal is reached as per the underlying consnsus algorithm; or
   ii. The contributors vote to release their respective contributions back to themselves and exit the project. Each transaction is recorded on the blockchain on the Ethereum Network and can serve as a proof of transaction.

In the proposed model, the individual or the organization raising the funds can also offer ICOs (Initial Coin Offerings) to the potential investors. ICOs help minimize the transaction cost and also disintermediates banks. ICOs are a unique way of capital formation for entrepreneurs and crowd-funding campaigners. They also help build trust in the crowdfunders' community at the early stage of project development. Ownership of tokens/coins offered via ICOs indicate ownership of financial stake in the product or the company.

Ethereum, is undoubtedly the uniform and most popular protocol for developing decentralized applications (dApps). Decentralized applications along with smart contract allow developers to build applications on the Ethereum ecosystem rather than writing their own blockchain technology.

The theoretical design of the model is charted in Figure 1 given below. The distributed application will necessarily have a frontend layer and a local node and the Ethereum network. A smart contract will enforce the control over the escrow funds and the conditions of the project execution and milestone releases.

Figure 2 outlines how a transaction is implemented via a smart contract on the crowdfunding platform. Figure 2 outlines a sample case between stakeholders and the role played by the smart contracts in the execution of the transactions between the stakeholders/ actors on the crowdfunding platform.

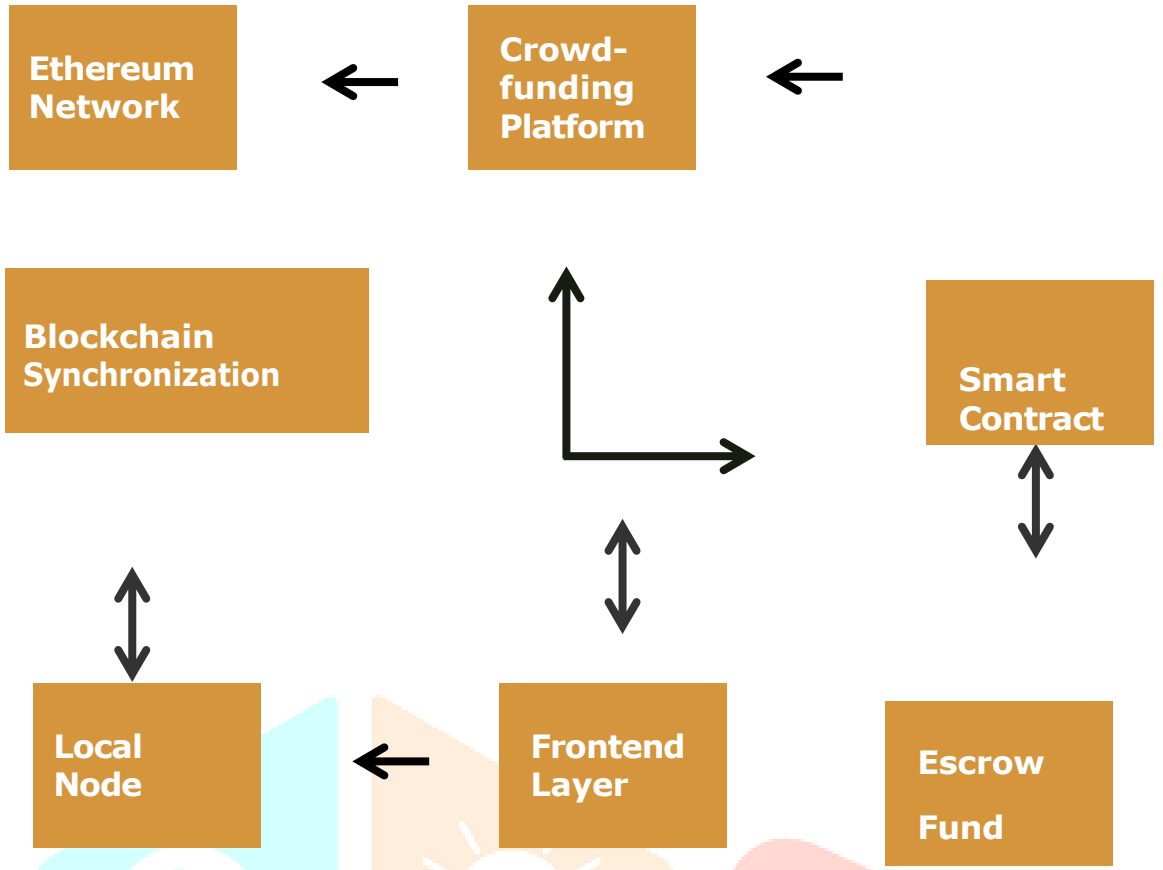

Figure 1. Standard structure of the proposed crowd-funding platform on the Ethereum network

Benefits and Applications

One of the major benefits of using a smart-contract based crowdfunding platform is that it provides a robust mechanism for building two-way binding trust between the stakeholders of the platform. Other benefits are described below:

Removal of intermediaries: The blockchain removes the necessity of financial intermediaries such as banks, loan agents, etc.

Validated transactions: All transactions on the blockchain are validated before they are done. This ensures transparency and no actor or a cluster of actors can "fake" a transaction. This builds trust in the crowdfunding community. Blockchain transactions have "true traceability".

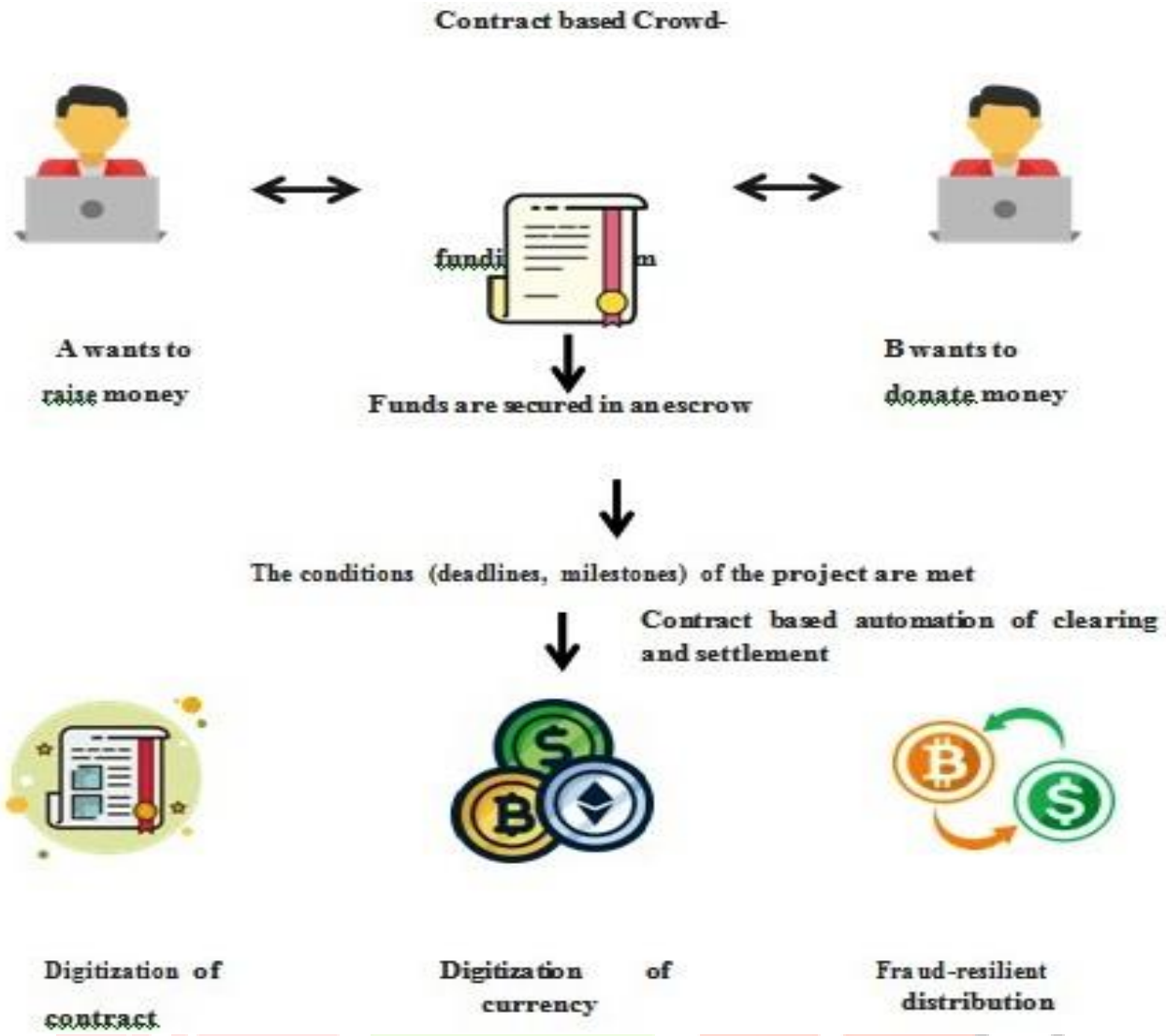

Figure 2. Using smart contracts to design a fraud-resilient distribution mechanism for crowd-funding platforms.

Reduced Costs: An end-to-end transaction on the blockchain only costs a fraction of what it costs via traditional modes of transaction. High speed of transactions: Transactions on blockchain are blazing fast. It takes only a few seconds for a transaction to be securely validated and committed on the Ethereum network across all nodes.

Scalability: One of the great benefits of blockchain technology is the scalability. The transaction speed on a blockchain is agnostic to the number of nodes connected on the network. This makes blockchain the best suited technology driver for building highly scalable applications

Literature Review and Related Work

The literature on novel crowd-funding models is scarce, much less for blockchain based crowd-funding models.

Our survey of projects on leading intermediary crowd-funding platforms found three major categories of crowdfunding projects:

1. Wherein a person or a representative, usually in personal capacity or in affiliation with a non-profit organization is raising funds for a cause. This model doesn't involve any exchange of goods or services.
2. Wherein a person or an organization is raising funds for a product or service that will be released in the near future. The crowdfunders will gain access to the product or service for their contribution.
3. Wherein a person or an organization is raising funds for a product or service that will be released in the near future. The crowdfunders will receive a share in the future profits of the product or service based on the corpus of their contribution.

A research5 (Messini Petruzzelli, 2019) divides the crowdfunding models into only two categories:

a) Reward based crowd-funding; and

b) donation based crowd-funding

A study6 (Agrawal, Catalani, and Goldfarb 2015) found out that geographic concentration of investors allows projects to gain wider traction and raise more funds in relatively less time.

In the pioneering white paper (1) the anonymous author writing under a pseudonym of Satoshi Nakamoto discussed a novel system of decentralized application (dApp). Satoshi mentioned development of "a new electronic cash system that's fully peer-to- peer, with no trusted third party". The Bitcoin white paper was the first document to outline the principles of a cryptographically secured (elliptic curve cryptography), peer-to-peer electronic payment system that was designed to be transparent and fraud- resilient. It had put the power of distribution and control in the hands of the people. In yet another milestone white paper (2), now called as the Ethereum Whitepaper written by the creator of Ethereum, Vitalik Buterin, a Russian computer scientist, in 2013 introduced the concept of Ethereum protocol. Ethereum is the second largest blockchain protocol in the world, behind only Bitcoin.

Ethereum was created to provide a framework to run all decentralized applications or dApps as they are popularly called. It extended the concept of decentralized applications introduced by Blockchains and built a framework for developers to build their own applications based on the decentralized Ethereum protocol.

Buterin also wrote about the scope of a Turing-complete programming language for developers to write smart-contracts that can be enforced on the Ethereum platform. It explained how new transactions work on the Ethereum blockchain:

a) A new transaction is initiated

b) The details of the new transactions are sent to the nodes within the network.

c) New blocks are created on the blockchain with the meta information of the transactions and the timestamps.

d) The node performs computation and broadcasts the Proof-of-work if it is able to do so, to the rest of the network.

e) Other nodes in the network validate and accept the solution.

f) The process follows step a-e iteratively for the next block.

This paper (3) discusses the risks factors associated with the Initial Coin Offerings (ICOs). It explains how ICOs have disruptive effects over the traditional methods of financing projects and causes. The capital formation via ICOs help disrupt the traditional gatekept hierarchy. It outlines the distinction between the traditional modes of fundraising (VCs, intermediary banks, loan-sharks, etcetera). The risks and rewards of the ICOs differ vastly from that of traditional modes such as IPOs (Initial Public Offerings). The organization or the project owner issues tokens or coins through and indelible distributed ledger which are uniquely stamped with the organization's information and built on protocols such as Ethereum, Openledger, or Counterparty.

The paper outlines the best strategies for the pricing of the pre-offering crypto-asset and the post-offering crypto-asset. Usually, a cryptocurrencies' pre-offering price is arbitrarily decided or matches the price of cryptocurrencies offered by similar projects at the pre-offering stage. However, the post-offering prices of the crypto-asset is decided by the supply and the demand. The paper discusses that while there are benefits, there are also risks involved. The ICO model allows crypt-assets to be created and distributed without any initial conditions, escrow requirements from the fundraisers, or security measures to protect investors.

Crypto-assets are intangible products and do not reflect any real value unless there is a demand for it. Our novel approach solves this with the intermediation of an escrow fund. It ensures legal certainty of disbursal of funds only on the conditions of the smart contract.

This paper (4) discusses framework of funding of community projects with the help of smart contracts. It discusses the prospect of civic crowdfunding. It discusses a novel approach to solve the 'free-rider' problem by implementing a game theoretic mechanism which can be enforced via a smart-contract. It proposes development of a dApp that can be accessed via a web-browser. This dApp is based on a smart contract which has two conditions:

a) If the project deadline is reached, and total funds raised are greater or equal to target amount, 25% can be allowed for the fundraiser to withdraw.

b) If the project deadline is reached, and total funds raised have not reached the target amount, the contributors are allowed to withdraw their respective contributions.

This is similar to the approach that we propose wherein the withdrawal of funds depend on the current status of the crowd-funded project.

This paper (5) discusses the application of blockchain for the purpose of equity crowd-funding. The authors trifurcate the token standards into UTXO-based, layer based, and smart contract-based tokens. UTXO or Unspent Transaction Output based tokens use a native Blockchain asset. It serves as a categoric container to which more value can be added. Layer based tokens use transaction graphs to issue tokens. In this approach, new tokens are created and tracked. The base layer is Blockchain layer and

the second layer adds consensus algorithm, transaction types, and requirements. Smart contract based tokens allow for the contracts, built as a code, to track states and represent token ownership. These contracts map tokens to owner addresses i.e. the contract acts as an intermediary mapping layer between the transferee and the owner. These contracts are based on a now popular new standard — ERC777.

In the paper (6) the authors design a general framework for a blockchain based crowd- funding platform. It outlines the four major types of crowd-funding practices:

a) Donation based crowdfunding

b) Reward based crowdfunding

c) Equity based crowdfunding or Crowdinvesting

d) Crowdlending

The paper further discusses the application of blockchain technology in the crowdfunding space. In this paper (7), the authors have implemented a Proof-of-Concept (PoC) for a simple smart contract in the crowdfunding process. It discusses a step-by-step protocol for implementation of a smart contract in a crowdfunding platform. This involves:

a) Verification of project and the fundraisers of a project on the blockchain to ensure that only trusted parties are able to create projects.

b) Eliminating dependency on third parties or intermediaries such as banks, legal companies, among others.

c) Enforcement of requirements of each project via smart contract at each stage to decide on the next execution and fund disbursement cycle.

Conclusion

Crowd-funding platforms help unlock hitherto unavailable opportunities for micro and medium scale investors who otherwise could not invest in highly innovative ventures.

This paper examined characteristics of current crowd-funding platforms,

modes and modalities of different funding models, their lacunae and we also proposed a new blockchain based fraud-resilient model of crowd-funding based on the extensive review of current models and the new challenges.

We studied that how crowd-funding is a vital tool for artists, entrepreneurs, and non- profit Samaritans or organizations to validate their ideas and raise funds from the people with the least friction. We also studied the comparative factors that decide the success of a crowd-funding campaign.

We reviewed current models and systems that have been developed or proposed that aim to fight the problems in this space. We postulated a theoretical framework that allows the crowd-funder community to retain more control over the project.

We proposed an intermediary escrow platform that is enforced via a smart-contract on the blockchain.

Implementation of a smart-contract based transparent social escrow platform as the intermediate layer will increase the contributor's confidentiality and confidence when contributing to the campaign. All blockchain transactions are transparently recorded and are public records. This model will also build a binding two-way trust between the stakeholders.

Citations

1. Crowdcrux (2020): “Crowdfunding Statistics in 2020”.
2. Available at https://www.crowdcrux.com/crowdfunding-statistics-in-2020/
3. Glaeser, Edward L, and Andrei Shleifer. 2001. “Not-for-Profit Entrepreneurs.”
4. Journal of Public Economics 81 (1): 99-115.
5. Gabison et al, “Understanding Crowdfunding and its Regulation”, 2015.
6. Mollick et al., “The Dynamics of Crowdfunding: An Exploratory Study (June 26, 2013)”, Journal of Business Venturing, Volume 29, Issue 1, January 2014, P1–16.
7. Antonio Messeni P., Angelo N., Umberto P., Paolo R., “Understanding the
8. crowdfunding phenomenon and its implications for sustainability”, Technological Forecasting and Social Change. Volume 141, 2019, P138-148.

9. Agrawal A., Catalini C., Goldfarb A., “Crowdfunding: Geography, Social Networks, and the Timing of Investment Decisions” Journal of Economics & Management Strategy, Volume 24, 2015, P253-274.

References

1. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Available at https://bitcoin.org/bitcoin.pdf.
2. Buterin, V. (2014). A next-generation smart contract and decentralized application
3. platform. Available at https://github.com/ethereum/wiki/wiki/White-Paper.
4. Kaal, Wulf & Dell'Erba, Marco. (2017). “Initial Coin Offerings: Emerging Practices, Risk Factors, and Red Flags.” SSRN Electronic Journal.
5. Chandra P., Ranjat A., Sawale J., Rajsekhar L., Gaurang S., Wadki H., “Funding Community Projects with Smart Contracts on Blockchain”, 2018, IITB-Journal.
6. Roth, Jakob and Schär, Fabian and Schöpfer, Aljoscha, “The Tokenization of Assets: Using Blockchains for Equity Crowdfunding” (August 27, 2019). Available at SSRN: https://ssrn.com/abstract=3443382
7. Babar H., “Blockchain based crowdfunding”, Blockchain Technology for Industry, 2020 (P117-130).
8. Ashari, Firmansyah, et al. "Smart contract and blockchain for crowdfunding platform." International Journal of Advanced Trends in Computer Science and Engineering (2020).