Crowdfunding dApp: Blockchain-based fundraising protocol

Isha Purushotham[1], Jeevanjot Singh[2], K P Sajith[3], Kaarnik Jamwal[4], Sarthak Kumar[5], Y Mohamadi Begum[6]
[1,2,3,4,5]*Students, Department of Computer Science and Engineering, Presidency University, Bangalore*
[6]*Professor, Department of Computer Science and Engineering, Presidency University, Bangalore*

Abstract **- Using blockchain as the underlying technology, many things in the current financial systems can be improved. But it's not only related to financial stuff though, many other things can also be improved. One of them is no censorship crowdfund. As building any censorship resistance app is "LITERALLY IMPOSSIBLE", crypto networks will be used to get around it. Reimagining the following prospects of crowdfunding using block chain technology will come into the picture in making and validating a transaction which will make the app different and more secure than the other apps available in the market.**

This paper presents a possibility of implementing conventional crowdfunding by utilizing the transparency and immutable features of block chain technology which works on improving all the weird aspects of existing crowdfunding apps that a centralized application can have.

Index Terms **- Application Binary Interface, Decentralized Application, Distributed Ledger Technology, Proof of Work, Proof of Stake, Cryptocurrency, Merkle-Patricia Tree, Cryptography.**

1.INTRODUCTION

Blockchain technology is a decentralized ledger, a more efficient, safe, and tamper-proof system of nodes in connection which records every transaction made on it. It consists of a network in which every node is equal in authority and power. The idea of crowdfunding is to collectively raise funds for a project or a business venture to attain financial support at an early stage. Crowdfunding has disrupted the way of financing and allowed start-ups and people in need to raise funds without much hustle and bureaucracy. In the existing model, a pool of people contributes small amounts of money towards a project or cause and expect some financial or nonfinancial returns. A crowdfunding platform takes a commission and matches the needs and expectations of funders and fundraisers.

The introduction of blockchain in crowdfunding will make it more reliable, transparent, trusted, decentralized, cost-efficient and convenient. A crowdfunding platform that was acting as an intermediary before provides the technology which will act as a medium of transaction and exchange.

Additionally, in the current crowdfunding platforms, there are problems of centralization and control from a single entity. If a platform creator wants, they can ban users from raising more money especially if it is directly affecting the platform. Even governments can shut down some projects if they don't think it's credible. The current system of Crowdfunding has a Single Point of Failure, i.e., if it fails, it will stop the entire system from working. Single Point of Failures are undesirable in any system with a goal of high availability or reliability, be it a business practice, software application, or other industrial systems.

The major goal of the work is to build a decentralized fundraising web application so that it can overcome the shortcomings of the already existing applications.

The objectives that the project proposes to achieve are-

1. Censorship resistance Fundraising protocol.
2. No direct taxes to be paid to govt authority on donation.
3. Highly Decentralized. (No control of single authority)
4. No Account Blocking.
5. No Single Point of Failure.

Blockchain technology: It is a structure that stores transactional records, also known as the block, of the public in several databases, known as the "chain," in a network connected through peer-to-peer nodes. Typically, this storage is referred to as a 'digital

ledger.' In the bitcoin white paper written by Satoshi Nakamoto and released in year 2008, an electronic coin is defined as a chain of digital signatures *[1]*.
Every transaction in this ledger is authorized by the digital signature of the owner, which authenticates the transaction and safeguards it from tampering. Hence, the information the digital ledger contains is highly secure.
In simpler words, the digital ledger is like a Google spreadsheet shared among numerous computers in a network, in which, the transactional records are stored based on actual purchases. The fascinating angle is that anybody can see the data, but they can't corrupt it.

Cryptocurrencies: a peer-to-peer electronic version of currency provides a mechanism that significantly reduces the reliability on crowdfunding platforms. Crypto currencies have been able to prove their efficiency and economic viability in the recent past. Ethereum, also referred to as blockchain 2.0, further explores the evolution of the idea of first-generation Distributed Ledger Technology such as Bitcoin. Its widespread application is based on the ability to host widespread applications based on smart contracts called Decentralized Applications (Dapps). Ethereum provides a common platform for Dapp creators and users, that can transact using its own cryptocurrency known as Ether.
In this paper, we propose a decentralized crowdfunding platform, which is designed on the Ethereum platform, written in solidity programming language. It aims to provide a peer-to-peer environment that brings project creators and investors on the same platform, and can exchange funds by using the cryptocurrency, Ether. The proposed platform should provide:

1) Trust
2) Low platform fee charges
3) Provenance tracking
4) Security

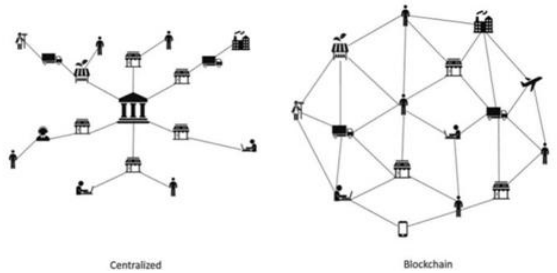


Fig1.

As in fig 1, differences between centralized and decentralized systems are shown. In general if the system is centralized, it can have single point of failure and will be vulnerable to attacks but the same can't be applied for decentralized systems which itself gives more robust security to decentralized systems.

2. BACKGROUND

A. BLOCKCHAIN

The introduction of blockchain was marked by the first crypto currency launched in 2009 by the name of Bit coin. Bitcoin was created by an anonymous person or a group of people going by the name Satoshi Nakamoto and released in the year 2009 as an open source software *[2]*.
Ten years later, it has become the world's most widely adopted concept of Distributed Ledger Technology. Bitcoin currently makes 46% of all cryptocurrencies in trade *[3]*. Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the "chain", in a network connected through peer-to-peer nodes
It incorporates characteristics of peer-to-peer decentralization, traceability, data integrity and security. A typical block in a blockchain consists of 3 components:

1. Hash value of current block
2. Data value
3. Hash value of previous block

[4] The first block in a blockchain is referred to as Genesis block. It does not contain any hash value of the previous block. The value of a block that contains the previous block hash value helps connect two blocks together in a linear fashion.

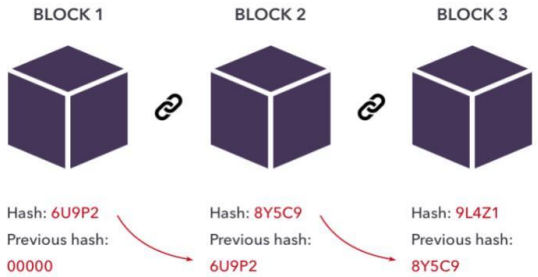


Fig2-a typical blockchain is shown where the new block is connected to another block and contains it's previous block hash. If somehow the previous block changes, the whole network after that will be

destroyed. This gives resilience to the blockchain system where you can't change previous block resulting in immutability and whole network history storage.

B. SMART CONTRACTS

Smart Contract is a set of predefined protocols that control the agreement between two or more parties involved in a transaction, without the need of an authorizing third party. Smart contracts are an integral part of Ethereum, the 2nd. generation blockchain. Using solidity developers can write dapps that implement self-enforcing business logic contained in smart contracts, leaving an undeniable and permanent record of transactions *[5]*.

Written in solidity language, smart contracts are simple computer programs that verifies the terms and conditions of an agreement and gets executed automatically*[4]*. The design of smart contracts reasserts the potential of blockchain systems to move from trust-based to trust-free interaction.

Due to the many iterative changes in ethereum's functionality, smart contracts and Dapps have amassed among the rising trend of blockchain.

There has been evidence of proposed systems that allow smart contracts to control ownership through intelligent assets. *[6]* Nick szabo first defined the concept of smart contract and smart property in the 1990s. *[7]* Glaser described the concept of blockchain using smart contract analysis, and Koulo, rikka proposed the idea of smart contracts resolving legal disputes.

C. CRYPTOGRAPHY

Blockchain technology, to enforce security of its network, makes use of Asymmetric key cryptography. A combination of public key and a private key is used in an asymmetric key cryptography. The use of asymmetric key cryptography helps ensure data integrity and privacy.

To authorise a transaction, the sender in a blockchain will cipher a transaction by the receiver's public key, which can be visible to everyone in the network. Next, the receiver obtains the cipher text which can be decrypted using the receiver's private key.

A private key, under no circumstance, can be disclosed by any participant of a network, since it ensures the security of data, and prevents any malicious attacks. Both public key and private key combinations can be generated for every transaction of a blockchain. This makes it possible to prevent brute force attacks until data is stored in a block. A public key, on the other hand, can act as an identification for a user without the need to reveal their real-world identity.

Hash function is a program that generates a standard size output of a variable size input. Data from blocks are connected using the network of hash functions that are made for every block generated in the blockchain.

Characteristics of hash function include:

1. Preimage Resistant: original input cannot be computed
2. Second preimage Resistant: no other input can be found that will generate similar output.
3. Collision Resistant: no two similar inputs will have the same hash value.

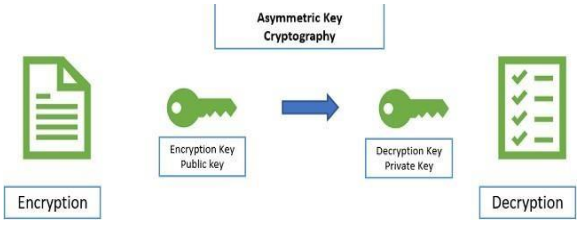


Fig. 3 CONCEPT OF ASYMMETRIC KEY CRYPTOGRAPHY

D. PROOF-OF-WORK VS PROOF-OF -STAKE

Blockchain systems require the majority of users to validate a transaction, which can then make an authorized block in a
blockchain. This method eliminates the requirement of a trusted third party and projects objectivity of the network for users. Majority consensus means a threshold number of nodes must validate new blocks in a blockchain.

There are two major types of consensus mechanisms:

1) Proof-of-Work (PoW): a probabilistically calculated energy-intensive cryptographic puzzle is created. Miners, also known as nodes compete, to solve this puzzle, higher the computational power of the miner's computer, higher the probability of solving the puzzle. The first miner to solve the puzzle is rewarded with cryptocurrency.

2) Proof-of-Stake (PoS): the chances of the node that publishes a block is determined by the miner's stake in the blockchain, instead of their mining power.

3. TOOLS/LANGUAGES USED

3.1 JavaScript

JavaScript is a text-based programming language used to create dynamic and interactive web content like applications and browsers.

3.2 CSS

CSS (Cascading Style Sheets) is used to style and layout web pages — for example, to alter the font, colour, size, and spacing of the content, split it into multiple columns, or add animations and other decorative features.

3.3 Solidity

Solidity is an object-oriented programming language created specifically by the Ethereum Network team for constructing and designing smart contracts on Blockchain platforms. Solidity, a smart contract language, chosen for this project due to the support available in developer community, object oriented features and syntax similar to JavaScript *[8]*.
It's used to create smart contracts that implement business logic and generate a chain of transaction records in the blockchain system.

Libraries and Frameworks Used

1. Next JS – JavaScript framework based on react.js and option of direct API building. It also supports server-side rendering which is important for SEO. Next works with file-based routing which is a good developer experience.
2. Ethers JS (web3) - A complete Ethereum wallet implementation and utilities in JavaScript (and TypeScript).
3. React Bootstrap - Designing and interface
4. Browser Image compressor - This module is used to compress jpeg and png images by reducing resolution or storage size before uploading to the application server to save bandwidth.
5. Truffle - Development environment, testing framework, and asset pipeline for block chains using the Ethereum Virtual Machine (EVM).
6. Ganache – It is used for setting up a personal Ethereum Blockchain for testing Solidity contracts.
7. MongoDB – Non-Relational Database. It uses JSON-like documents with optional schemas.

Various Modules and their Integration

Navbar - This is the essential part of the website, option to navigate to a different page is directly appended here. Child component to the Navbar includes Links, a Button in the top right to connect to a Blockchain network and a wrapper to show whether the connected network is correct or not. This module will always be shown in the top of the website in all the pages.

Campaign List - As the name suggests, the module is responsible for showing campaigns in the main and profile section. Every list of campaign consists of several components including cover image, title, description, status and percentage raised capital. Clicking on this module will take user to the specific campaign page where user can see details, donate to the campaign and get refund.

Raise Funds (Form Component) - This module is used to create the campaign in a three-step form process. It consists of few input components for title, description, date and amount. In the second step the module includes drag and drop image component. Upon confirming user should be able to start a new campaign.

Tab Module - The module is used in profile section where two components are used, showing all of the current user's raised campaigns and all donated based on selection.

Carousel Module - It's used to show all the images and videos uploaded by the user in a specific campaign.

Main Donation Module - It is always shown next to carousel module making it easy for users to either donate or get refund.

4. PROPOSED SYSTEM OF DECENTRALIZED CROWDFUNDING

To overcome the shortcomings of the existing centralized crowdfunding platforms, the proposed crowdfunding platform eliminates a trusted third party/central authority to authorize transactions and guarantee the integrity of the platform.
The proposed method offloads and decentralizes all the donation control codes to Blockchain Networks

(Polygon Testnet in the dApp). Test network (Testnet) is a copy of Ethereum blockchain identical in every way to main network except the fact that their Ether is worthless *[9]*

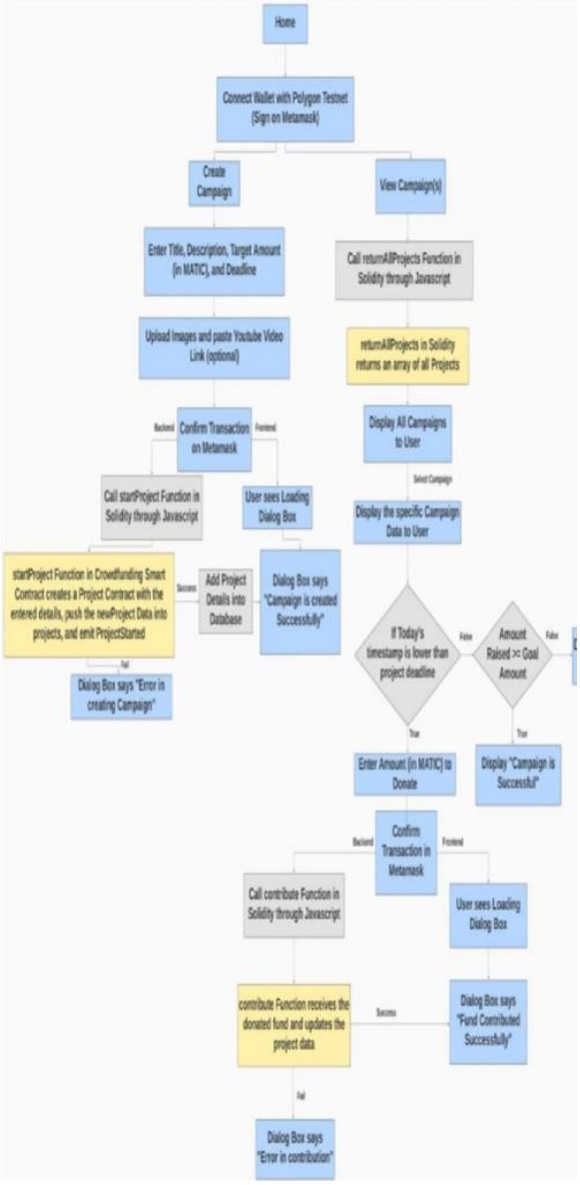
The basic difference in the proposed method will come in the method of transactions. In the case of platforms like gofundme and IndieGoGo, people have to use their credit and debit cards for payments. Blockchain's distributed ledger helps in getting rid of the centralized intermediaries such as Kickstarter and Indiegogo that take huge amounts of money from a campaign as a maintenance fee. Blockchain crowdfunding is a purer form of crowdfunding as it removes any intermediaries between the backers and the start-up *[10]*.

However, in the proposed method, people will simply send transactions through a direct metamask RPC connection to blockchain networks (basically calling a function of solidity from JavaScript using ABI).

The contract logic is entirely written in Solidity language, tested on Ganache local network, connected to the internet using Web3 API and developed on the Truffle IDE. The front end is designed using ReactJS, which interacts with the ABI in JSON format.

The mechanism of decentralized crowdfunding platform can be explained as:

1. Users can start and raise campaigns for their needs from the application. They will have to enter the Title, Description, Target Amount (in-network default token)**,** and Deadline for their needs on the first page. Then they will have to upload a maximum of 5 images (minimum of 1) for the project. Users can also embed a YouTube link, recommended for the validity of the project but not required.
2. Then on the next page after validating the transaction the Target Amount, Deadline, unique ID, and user's current blockchain address will be saved on the smart contract. After that, all this data including Images, Title, Description, and YouTube Link will be stored on a server (for images, Cloudinary API is being used). If everything works as expected then the user can see their raised campaign on the Campaigns page.
3. To donate to the campaign a different user with a different address should just select the campaign he/she is interested in and input the amount. Then after pressing the donate button, the user should validate the transaction on metamask. In the end, funds will be donated from the donor's wallet to the smart contract. Once the campaign reaches its target, the amount will be sent to the campaign raiser's wallet.
4. If the project is successful or failed, smart contract will deny any token being sent to it.
5. The front end will show either successful or running or failed.
6. For failed projects (not able to raise the target amount in the given deadline) the users who donated will be able to claim their refund directly from the website. Any refund claim where the user has not donated will be reverted back or cancelled by the blockchain.
7. The project starter should be able to see all their campaigns started by them in the profile section including all projects hey donated so far.



5. CONCLUSION

Blockchain, despite being a relatively new concept to the community, holds immense potential in bringing benefits to society. Crowdfunding has been playing a significant role in our society and economy, driving innovation, and creating new jobs and employment. Many people actually use this platform to raise money for different purposes. Even with this growing trend, there are still a couple of drawbacks with the current methods of crowdfunding: Centralization and Single Point-of-Failure - which can be solved by Integrating Crowdfunding and Blockchain.

Nevertheless, the implementation of this concept contains a plethora of loopholes that requires correction for example the Safety of Fund Utilization by a Campaign, Verification of a Particular Campaign or the Community Interest can be solved by Integrating a DAO (Decentralized Autonomous Organization) with this dApp where the user votes whether a particular Campaign should be approved for listing or not.

This paper gives evidence to the scope of reducing the possibility of single point of failure. Integrity can be implemented by realizing the concepts of Layer 2 Blockchain (such as Polygon. Using such elements makes crowdfunding robust and De-centralized.

REFERENCE

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 18 Oct 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] L.S., "Who is Satoshi Nakamoto?," 2 November 2015. [Online]. Available: https://www.economist.com/the-economist-explains/2015/11/02/who-is-satoshinakamoto

[3] https://www.coingecko.com/en/coins/bitcoin

[4] Buterin, Vitalik et al. 2014. “A next-generation smart contract and decentralized application platform”

[5] "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Solidity.

[6] Szabo, Nick. 1997. “Formalizing and securing relationships on public networks”

[7] Glaser, Florian. 2017. “Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis”. Proceedings of the 50th Hawaii International Conference on System Sciences.

[8] Solidity. [Online]. Available: https://solidity.readthedocs.io/en/develop/

[9] G. Hayes, "The Beginners Guide to Using an Ethereum Test Network," 16 February 2018. [Online]. Available: https://medium.com/compound-finance/the-beginnersguide-to-using-an-ethereum-test-network-95bbbc85fc1d

[10] A. Rosic, “Blockgeeks,”. Available: https://blockgeeks.com/blockchaincrowdfunding/.