DECENTRALIZED CROWDFUNDING

[1]Lakshya Sangar1, [2]Kush Aggarwal, [3]Devesh Khandelwal, [4]Ms. Aashita Chhabra
[1,2,3]Students, [4]Assistant Professor,
Department of Information Technology
[1,2,3,4]Dr. Akhilesh Das Gupta Institute of Technology and Management

Abstract - Crowdfunding decentralized application (Dapp) accumulates integrated planning and execution of several processes. This involves flow of information and financial capital, management of goods and services, information regarding the storage and movement of raw materials, building products, and finally, full-fledged finished goods from one point to another . Proper implementation of funding in a business in its empirical stages can result in benefits like increased sales and revenues, decreased frauds and overhead costs, quality improvisation. As a result, this will lead to accelerated production and distribution in the business prospects, at a crucial phase of a project venture, the initial phase. Reimagining the following prospects of crowdfunding using block chain technology can make a monumental difference in the startup industry. This paper presents a possibility of implementing conventional crowdfunding by utilizing the transparency and immutable features of block chain technology.

Keywords: Application Binary Interface, Decentralized Autonomous Organization, Decentralized Application, Distributed Ledger Technology, Integrated Development Environment, Application Programming Interface

I. INTRODUCTION

A blockchain is a decentralized digital ledger that is incorruptible by nature, recording 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 early stage financial support. Such ideas can be easily realized by a shared economy currency and a peer-to-peer transaction system that also has the ability to reduce fees of the transaction. Ethereum is a blockchain implementation that aims to provide the same by giving its users the ability to create smart contracts: a self-executing set of rules devised to govern how information is exchanged in the Ethereum blockchain.

Conventional crowdfunding platforms have been able to provide funding services, by mediating between entrepreneurs and investors. However, they lack in terms of reducing fee charges, which are levied in two forms:

1) Platform fee (4-5%): for connecting both investors and project creators
2) Payment Processing Fee (3.5%) : for transferring the amount

Additionally, crowdfunding platforms also hold a risk of transfer and identity fraud over the internet, thereby letting the middlemen platforms take advantage by providing trust and receiving profits in exchange. Nevertheless, majority crowdfunding platforms have a dissuasive nature of inefficiencies and information asymmetry that requires correction.

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

II. BACKGROUND

A. BLOCKCHAIN

The introduction of blockchain was marked by the first crypto currency launched in 2009 by the name of Bit coin. 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 *[7]*. However, the underlying concept behind bitcoin deserves much more scrutiny. Blockchain technology is a concept of continuously growing recorded ledgers in the form of a connected chain, hence the name, Blockchain. It incorporates characteristics of peer-to-peer decentralization, data integrity, traceability and security. A typical block in a linear blockchain consists of 3 components:

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

[5] 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

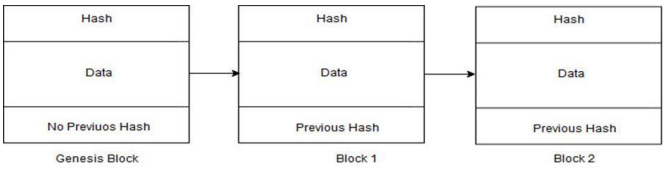
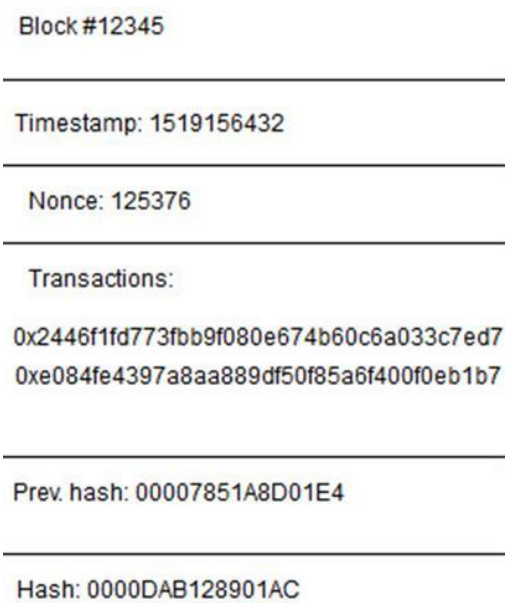


Fig. 1 ILLUSTRATION OF LINEAR BLOCKCHAIN



Figs 2 ILLUSTRATION OF SINGLE BLOCK ENTRY

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. *[5]* Written in solidity language, smart contracts are simple computer programs that verifies the terms and conditions of an agreement and gets executed automatically. 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. *[8]* Nick szabo first defined the concept of smart contract and smart property in the 1990s. *[6]* Glaser described the concept of blockchain by 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.

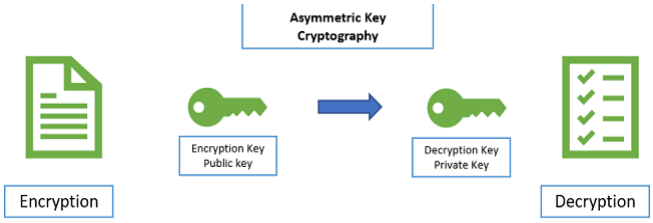


Fig. 3 CONCEPT OF ASYMMETRIC KEY CRYPTOGRAPHY

D. CONSENSUS MECHANISM

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.

Higher stakes in a network gives the strongest incentive to maintain security of the network.

E. MERKLE TREE

The design of a blockchain requires a colossal amount of data repositories that can hold infinite amounts of transaction history, since every transaction in a ledger is immutable and stored persistently. These storage requirements are increasing with the expanding network. This can be harmful to a network's security, since nodes with higher storage capability might dictate the network, making it less decentralized. Merkle trees are used to diminish these disk space requirements.

Merkle tree is a data structure that groups hash codes of transactions to produce a single hash code. This process is undergone using a tree structure in which leaf nodes contain transactions and are collectively computed to produce a root node that represents all leaf nodes. An altered leaf node would result in change of root node in a merkle tree.

Any participating node can verify transactions by linking to the header of a blockchain header (root node), without going through the entire succeeding chain of transactions. This protocol of minimizing storage for verification is known as Simplified Payment Verification, and is crucial for a blockchain's scalability.

III. CONCEPT OF CONVENTIONAL CROWDFUNDING

The idea of raising funds by approaching a multitude of investors for a project or a business venture is called crowdfunding. This has been deemed instrumental in many cases, to raise funds at an early stage of a startup. A typical crowdfunding platform has 3 actors :

1) Project creator
2) Financial intermediary (two-sided market intermediaries)
3) Investor

These actors are brought together on the same platform, crowdfunding platform.

A crowdfunding can generate revenue in 3 ways :

1) Interest : the amount of money gained using interest on funds that are temporarily held by a crowdfunding platform that originally belong to investors. This amount is generally held for a period of 30 days, after which, if the project is approved, the funds will be allocated to the business or a project.
2) Transaction Fees : commonly paid by fundraisers after the project receives successful funding.
3) Additional charges : payment gateway fees, automated tools, analysis algorithms etc.

Crowdfunding platforms can also function differently based on the commodity exchange in return of investment :

1) Equity and Royalty Based :
   The most widely accepted type of crowdfunding functionality. Equity and Royalty model includes capital-seekers sharing an equity share or a royalty share of the business project with capital-givers. Common examples of this model are Wefunder, Angelist and Seedrs.

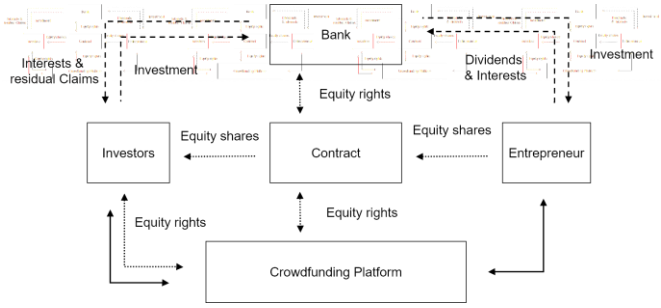


Fig. 4 EQUITY BASED CROWDFUNDING

2) Reward Based **:**
   Capital-seekers offer rewards on investment in the form of gifts or business products, given that investors pledge a certain amount to the project. Kickstarter is a famous example of rewards based crowdfunding, along with Indiegogo.
3) Debt based **:**
   Similar to loan based funding, a crowdfunding platform will grant a loan to a capital-seeker, using a capital-giver's investment. Capital-givers can then expect a return on investment as the interest levied on the capital-seeker. LendingHub, Crowdo and Moolahsense are some common examples.

IV. PROPOSED SYSTEM OF DECENTRALIZED CROWDFUNDING

To overcome the shortcomings of crowdfunding platforms in the past, the proposed crowdfunding platform eliminates a trusted third party to authorize transactions and guarantee the integrity of the platform.

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) Project creator or business entrepreneur registers on the Dapp by giving information about the business idea, amount to be raised etc, and is assigned a unique ID.
2) The creator then publishes his/her business idea on the blockchain using their private key, and a timestamp of the business ID is recorded, along with the required amount to be raised.
3) Similar to the creator, and investor also registers on the Dapp and is assigned a unique ID.
4) The potential backer can assess several available business ideas to choose suitable projects, and pledges and amount to the project. This information

gets stored on the network with respect to the backers unique ID.

5) After multiple backers fund a project, and funds raised are equal or more than the desired amount to be raised, and the fundraising time is less than 30 days, collected funds are transferred from escrow to the creator in the form of Ether
6) If any of the above conditions are not matched, the creator's application is considered void and is stated inactive.
7) A miner can validate the transaction of creator and escrow, to prevent double spending, and is rewarded in cryptocurrency Ether.

V. CONCLUSION

Blockchain, despite being a relatively new concept to the community, holds immense potential to bring many benefits to society. The notion of decentralized crowdfunding can propagate opportunity growth among businesses, collective economy and stimulating capital flourishment of society. By lowering the transactional cost and interest fees, it can engage numerous new investors, making it more adoptable.

Nevertheless, the implementation of this concept contains a plethora of loopholes that require correction. However, due to the constant evolution of blockchains, its achievability does not seem distant.

This paper gives evidence to the scope of reducing the number of intermediaries consisting in a blockchain. Integrity can be implemented by realizing the concepts of asymmetric cryptography. Using such elements makes crowdfunding robust and trust-free, in lieu of trustless.

REFERENCES

[1] Starkenmann Oliver Implementation of Crowdfunding Decentralized application on Ethereum Master Thesis, ResearchGate 2017
[2] S.Benilia et al, Crowdfunding using Blockchain, Global Research and Development Journal for Engineering, Vol 4, Issue 4, March 2019
[3] Swati Kumari and Keyur Parmar, Secure and Decentralized Crowdfunding Mechanism using Blockchain Technology, chapter 7, Proceedings of the International Conference on Paradigms of Computing, Springer, 2020
[4] https://cheapsslsecurity.com/blog/what-is-asymmetric-encryption-understand-with-simple-examples/
[5] Buterin, Vitalik et al. 2014. “A next-generation smart contract and decentralized application platform”
[6] 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.
[7] https://www.coingecko.com/en/coins/bitcoin
[8] Szabo, Nick. 1997. “Formalizing and securing relationships on public networks”

