International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

Decentralized Crowdfunding Platform Using Ethereum Blockchain Technology

Siddhesh Jadye[1], Swarup Chattopadhyay[2], Yash Khodankar[3], Dr. Nita Patil[4]

[1-3]*Student, Computer Department, Datta Meghe College of Engineering, Navi Mumbai, Maharashtra, India*
[4]*Faculty, Dept. of Computer Engineering, Datta Meghe College of Engineering, Maharashtra, India*

Abstract - *In today's world, blockchain-based systems are in demand across various industries, because of its secure, trusted, and decentralised network as well as for being more efficient than the traditional methods.*

However, the traditional ways these days are facing a lot of issues and challenges because of the complex and less secure network. Blockchain network integration overcomes the problems faced by traditional methods across industries. The Blockchain integrated network provides benefits such as increased security, increased transparency, increased efficiency and decreased chances of fraud. Although the blockchain-based systems provide various benefits, due to lack of knowledge about this technology, the implementation rate is low. In this work, we have highlighted the distinction between the traditional crowdfunding platform as well as blockchain network-based crowdfunding platform and the benefits of implementing blockchain network in other sectors.

This work highlights the issues and challenges faced by the industries, as mentioned earlier, by using the traditional methods as well as the solutions to the problems provided by the blockchain network-based systems to those industries. This work helps the people to understand the benefits of blockchain network-based systems in their respective industries as well as execute it to improve the transparency, efficiency, and security of the system altogether.

Key Words: **Blockchain, Crowdfunding, e-Voting, Ethereum, Cryptocurrency**

1. INTRODUCTION

Crowdfunding could be a methodology of raising capital through the collective effort of friends, family, customers, and individual investors. This approach faucets into the collective efforts of an outsized pool of individuals—primarily on-line via social media and crowdfunding platforms—and leverages their networks for bigger reach and exposure.

Crowdfunding is actually the other of the thought approaches to business finance. historically, if you wish to lift capital to begin a business or launch a brand new product, you'd have to be compelled to clean up your business arrange, marketing research, and prototypes, so look your plan around to a restricted pool or moneyed people or establishments. These funding sources enclosed banks, angel investors, and working capital corporations, very limiting your choices to a number of key players. you'll think about this fundraising approach as a funnel, with you and your pitch at the wide finish and your audience of investors at the closed finish. Fail to purpose that funnel at the proper capitalist or firm at the proper time, and that's it slow and cash lost.

Crowdfunding platforms, on the opposite hand, flip that funnel on-end. By supplying you with, the bourgeois, one platform to create, showcase, and share your pitch resources, this approach dramatically streamlines the normal model. historically, you'd pay months separation through your personal network, vetting potential investors, and defray your own time and cash to induce before them. With crowdfunding, it's a lot easier for you to induce your chance before a lot of interested parties and provides them a lot of ways to assist grow your business, from finance thousands in exchange for equity to contributory $20 in exchange for a first-run product or alternative reward.

2. METHODOLOGY

2.1 Traditional Crowdfunding Concept

Most ancient business funding takes one in all 3 forms: self-funding, bank funding, or working capital. The problem is that for many folks, self-funding is implausibly restricted. Bank funding needs having AN existing business with sensible revenues and income. And venture fund capital nearly invariably needs a product or service that has mass attractiveness. This makes ancient funding terribly restricted and laborious to induce for newer businesses. It will inhibit growth even for products and services with immense potential.

Crowdfunding permits businesses with very nice product and repair ideas to lift funds from regular folks in tiny investment amounts. Once it works, it will very offer your business an enormous boost. firms like Kickstarter, Indiegogo, and Crowdfunder were among the earliest to create it well-liked.

One drawback is that even with crowdfunding, the model remains very inefficient. In step with Kickstarter, seventy eight of campaigns that raise 2 hundredth of their goal ultimately become absolutely funded, whereas Martinmas of comes end having ne'er received any funding the least bit. This brings United States of America to however blockchain is dynamical the crowdfunding landscape

2.2 Blockchain Based Crowdfunding

Blockchain

Blockchain, typically named as Distributed Ledger Technology (DLT), makes the history of any digital plus unalterable and clear through the utilization of decentralization and science hashing.

A simple analogy for understanding blockchain technology could be a Google Doc. Once we produce a document and share it with a gaggle of individuals, the document is distributed rather than derived or transferred. This creates a decentralised distribution chain that provides everybody access to the document at identical times. nobody is fastened out awaiting changes from another party, whereas all modifications to the doc are being recorded in a period of time, creating changes fully clear. Of course, blockchain is additional difficult than a Google Doc, however the analogy is apt as a result of it illustrates 3 important ideas of the technology.

Blockchain is Associate in Nursing particularly promising and revolutionary technology as a result of it helps cut back risk, stamps out fraud and brings transparency during a climbable means for myriad uses.

Blockchain consists of 3 vital concepts: blocks, nodes and miners.

Blocks

Every chain consists of multiple blocks and every block has 3 basic elements:

A 32-bit integer known as a time being. The time being is randomly generated once a block is formed, that then generates a block header hash.

The hash may be a 256-bit range married to the time being. It should begin with an enormous range of zeroes (i.e., be extraordinarily small).

When the primary block of a series is formed, a time being generates the cryptanalytic hash. the information within the block is taken into account, signed and forever tied to the time being and hash unless it's well-mined. Grammar Check.

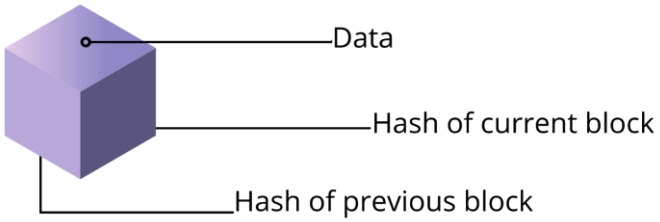

Fig -1: Contents of a single block in blockchain

Sample paragraph Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper.

Miners

Miners produce new blocks on the chain through a method referred to as mining.

In a blockchain each block has its own distinctive nowadays and hash, however conjointly references the hash of the previous block within the chain, thus mining a block is not simple, particularly on massive chains.

Miners use special code to resolve the improbably advanced mathematics downside of finding a nowadays that generates associate degree accepted hash. as a result of the nowadays is just thirty two bits and also the hash is 256, there are roughly four billion attainable nonce-hash combos that have to be deep-mined before the correct one is found. Once that happens miners are aforesaid to possess found the "golden nonce" and their block is supplementary to the chain.

Making an amendment to any block earlier within the chain needs re-mining not simply the block with the amendment, however all of the blocks that return when. This is often why it's very troublesome to govern blockchain technology. think about it as "safety in math" since finding golden nonces needs a massive quantity of your time and computing power.

When a block is with success deep-mined, the amendment is accepted by all of the nodes on the network and also the miner is rewarded financially.

Nodes

One of the foremost necessary ideas in blockchain technology is decentralization. nobody laptop or organization will own the chain. Instead, it's a distributed ledger via the nodes connected to the chain. Nodes is any quiet device that maintains copies of the blockchain and keeps the network functioning.

Every node has its own copy of the blockchain and therefore the network should algorithmically approve any recently deep-mined block for the chain to be updated, sure and verified. Since blockchains are unit clear, each action within the ledger is simply checked and viewed. Every participant is given a singular alphamerical number that shows their transactions.

Combining public data with a system of checks-and-balances helps the blockchain maintain integrity and creates trust among users. Basically, blockchains are thought of because of the measurability of trust via technology.

Smart Contract

A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible.

Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism.

While blockchain technology has come to be thought of primarily as the foundation for bitcoin, it has evolved far beyond underpinning the virtual currency

2. PROPOSED METHOD

Working of Smart Contract

A new technique for crowdfunding supported blockchain technology has been advised during this section. Ethereum is associate ASCII text file, public, blockchain-based distributed computing platform and OS that includes good contract (scripting) practicality. The good contract permits us to implement business logic and runs on blockchain network. Solidity is the most well-liked language for writing a wise contract good go for associate ethereum network permits America to exchange cash, share, or something of import in an exceedingly clear and conflict-free manner. This property of good contract enables America to use it in varied eventualities. Two good contracts are developed as delineated in the primary good contract deploys the second contract every time a replacement fundraising campaign is initiated. The second contract consists of all the logic that's needed for running the campaign. The primary contract has been noted as a generator and the second contract is noted as a campaign contract.

When a personal starts a replacement campaign the generator deploys an associate instance of the campaign contract on the ethereum network. The deployed contract stores and manages the money that is contributed to the campaign. The leader of the campaign is noted because the manager of the campaign. The manager, when having collected the specified quantity of cash (in the shape of ether) generates a payment request. This payment request must be approved by quite fifty % of its contributors. If the payment request has the specified number of approvers then the manager will end the request and transfer needed cash to the seller from the fund collected.

As delineated the manager when making a campaign has two functionalities. The in which the manager requests the payment from the contributors. The payment request is finalized when the campaign has gathered the required range of positive approvers.

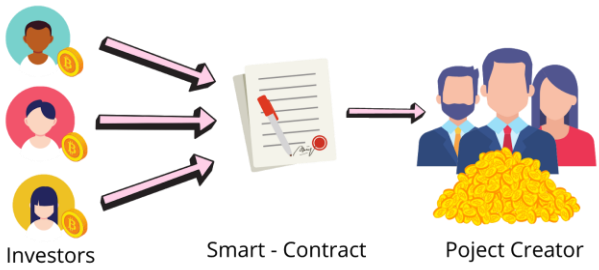

Fig -2: Smart Contract.

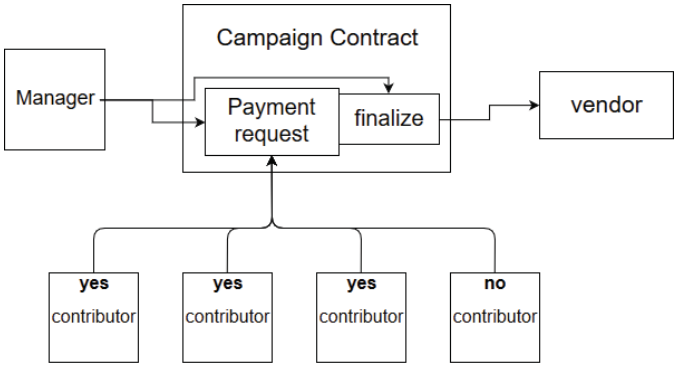

Fig. -3: The core functionality of a campaign contract.

Credits: Shivansh Pandey, Subodh Bansla

Ethereum isn't a traditional network thus varied tool and libraries were needed to attach our front-end internet application to that. Web3.js could be a JavaScript library. It allows us to move with remote ethereum nodes, victimization HyperText Transfer protocol or Inter-process communication affiliation. Ganache command line interface was conjointly needed by the application for connecting to the ethereum network. an associate instance of web3 was made and so its supplier was found out. This supplier helped web3 to move with varied ethereum networks. within the next section, the structure of the good contract that was deployed to the ethereum network is mentioned. The functionalities of the smart contract deployed area unit explained within the next section.

3. COMPARING PROPOSED METHOD WITH EXISTING METHODS

The conventional method used by crowdfunding websites has a major drawback. It does not allow a contributor to have any control over the money they have contributed. This results in frauds and scams. The proposed method addresses this problem and provides contributors with control over the money they have contributed.

Log of all the transactions happening in the network is called a ledger. Blockchain maintains a global ledger and each node in the network has a copy of this global ledger called the private ledger. Since every node has a copy of ledger so no node can perform malicious activity. Interaction of global and private ledger in Blockchain is depicted in fig-6. Ethereum is an implementation of blockchain and extends its functionality using smart contracts. Smart contracts can be used to implement logic in blockchain secured environments. Thus using blockchain and smart contracts, a new system has been designed to solve the problem faced by existing crowdfunding websites. It is a decentralized network whereas the traditional method uses a centralized approach. Decentralized approach eliminated the chances of a single point of failure. Thus the proposed system is robust. In the conventional method, funds are transferred online which a lot of times are subject to hacking resulting in loss of funds. The transfer of funds in the proposed system is in the form of ether. Ether is a cryptocurrency and thus very secure. Every time ether is sent, it is attached to ‡ur r ,rr…† ƒ`iyvp xr’ hq v† †vtrq v‡u sender's private key. The sender's signature on the message verifies that the message is authentic and transaction history is kept by everyone in the form of ledger so that no one can deny their transaction. Thus the use of digital signature in blockchain makes our system resistant to non-repudiation attacks. Working of digital signature is demonstrated in fig-7. In the digital signature, the sender signs the data file using its private key, and thus the data file gets a digital signature of the user. The signed data file can then be verified using the public key of the sender which is easily available and thus the authenticity of the data file is maintained. The digital signature ensures that the data is being sent by that particular person only and the person also cannot deny that.

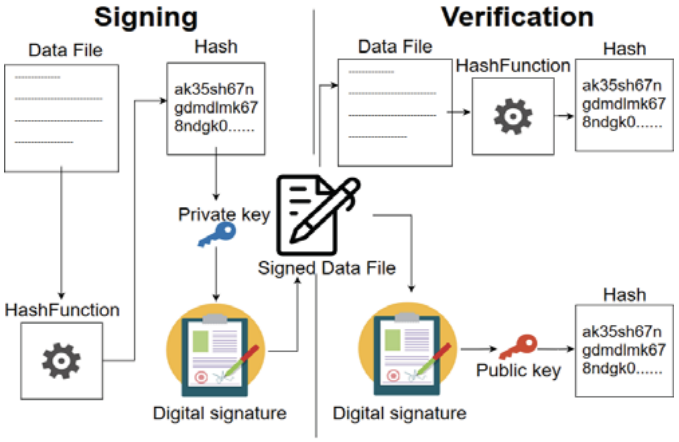

Fig. -4: Signing & Verification

Credits: Shivansh Pandey, Subodh Bansla

4. CONCLUSIONS

We can conclude that the implementation of blockchain can improve many drawbacks that area unit gift within the ancient crowdfunding platforms. This includes, increased security, increased potency, fraud protection.

In gist, we are able to say we've got achieved the subsequent things:

- Decentralization
- Fraud interference victimisation e-Voting
- Secure systems with Smart Contract
- increased potency
- Tokenization
- Having the ability to serve high demand
- Having the ability to retain all the positives of the standard Crowdfunding Platforms

REFERENCES

[1] Shivansh Pandey, 2018, “Crowdfunding Fraud Prevention using Blockchain”, JSS Academy of Technical Education,Noida, INDIA

[2] Hasnan Baber, 2019, “Blockchain-Based Crowdfunding: A ‘Pay-it-Forward’ Model of WHIRL,” International Journal of Recent Technology and Engineering (IJRTE).

[3] Ms. S. Benila, 2019, "Crowdfunding using Blockchain,"GRD Journals-Global Research and Development Journal For Engineering.

[4] Ferreira F. and Qr…rv…h G Tˆppr†s factors in a reward and equity based p…,□qsˆ□qv□t ph□ƒhvt□ v□ Proc.2018 IEEE International Conference on Engineering Technology and Innovation (ICE/ITMC), pp. 1-8, IEEE, 2018.

[6] "Value of funds raised through crowdfunding worldwide from 2014 to2016 (in million U.S. dollars),"Internet: https://www.statista.com/statistics /360512/funds-raised-via crowdfunding-globally/, [Oct.26, 2018].

[7] S. Nakamoto, 7v‡p,v□) 6 Qrr…-to-Peer Electronic Ch†u T'†‡r□ Internet: https://bitcoin.org/bitcoin.pdf, [Oct.26, 2018].

[8] Bencic F.M. and Zarko I.P . 9v†‡…viˆ‡rq Grqtr… Urpu□,y,t') 7y,pxpuhv□ 8,□ƒh…rq ‡, 9v…rp‡rq 6p'pyvp B…hfu v□"'‡u D□‡r…□h‡v,□hy Conference on Distributed Computing Systems, pp. 1569-1570, 2018.

[9] Kenton W. (2017, Dec 16), "Donation Based Crowdfunding."Internet:https://www.investopedia.com/terms/d/donationbased-crowd- funding.asp, [Oct.26, 2018].

[10]Solidity Documentation, Internet: http://solidity.readthedocs.org/en/latest/, [Oct. 27, 2018].

[11] Wood G. @‡ur…rˆ□) 6 Trpˆ…r 9rpr□‡…hyv†rq Genenralised U…h□†hp‡v,□ Grqtr… Internet: https://gavwood.com/paper.pdf, [Oct. 27, 2018].

[12] Kurian A.M. (2018), "Interacting with Ethereum Smart Contracts through Xri"w† D□‡r…□r‡: https://medium.com/coinmonks/ interacting-with-ethereum-smart-contracts-through-web3-js- e0efad17977, [Oct. 28, 2018].