International Journal For Technological Research In Engineering
Volume 9, Issue 10, June-2022 *ISSN (Online): 2347 - 4718*

RESEARCH PAPER ON BLOCKCHAIN

[1]NAMAN SHARMA, [2]RUPEN SHARMA, [3]TANISH SHARMA, [4]MS. GURPREET KAUR
[1,2,3]Students, [4]Assistant Professor
Department of Computer science Engineering
MVSIT, Sonipat, India

Abstract

In the modern world, online crowdfunding plays an important role where many investors can come together and fund projects presented by various creators. Our project aims to compare pros and cons between conventional crowdfunding and blockchain crowdfunding. In conventional crowdfunding, one faces a lot of issues such as transparency issues, fraudulent issues, investor abuse etc. However, to overcome these issues, blockchain crowdfunding comes into play. Blockchain crowdfunding helps to overcome the issues faced in conventional crowdfunding. To implement blockchain crowdfunding, we have proposed a model named "Block Funding", which is made using ethereum smart contracts. It consists of a web app made using React/Next.Js and ethereum smart contracts used in the backend. It primarily focuses on all the basic crowdfunding features as well as voting through blockchain. Moreover, the model is deployed on a rinkeby test network.

1 Introduction

Crowdfunding is a mechanism in which some amount of capital is required from a large number of individuals to invest in some business ventures. It can be used through social websites by bringing together a large number of entrepreneurs and investors together, with the potential to increase entrepreneurship and by expanding the pool of investors and venture capitalists[1]. Crowdfunding has created various opportunities for many entrepreneurs as they raised millions of dollars by deploying their projects to various crowdfunding websites such as Kickstarter and Indiegogo, these websites attract thousands of people to interact with the projects and invest in them so that in return they could also receive benefits through them. According to some surveys, crowdfunding is mostly synonymous with Kickstarter as it is the largest crowdfunding platform. Kickstarter is driven by two types of users -

1.Creator- Creators are the one who creates innovative projects and deploys them for funding.they can also create pages where they can list information and also add some videos, photos, etc. of their projects so that the backers can get proper details about the projects and they also set a goal for funding and the deadline, plus rewards where backers can achieve on some contribution to the project.

2. Backers-Backers are the one who funds the project by donating some amount to them so that project can reach its goal for funding and backers also in return are rewarded according to their contribution.[2]

According to some survey in 2010 over one and a half billion dollars has been transferred from Kickstarter backer to project creator and Kickstarter 5% cut with each dollar means the revenue collected was around 75 to 80 billion dollars which is a huge amount but the most important question arises is the transparency of kickstarter[3] and many fraud and failure cases are also reported such as a product CST-01(Central StandardTiming) 'the world's thinnest watch', which raised more than 1 million dollars but was not able to keep up to their promise. Thus the technology which is best and trending to solve the issue of transparency in crowdfunding is 'blockchain', blockchain is a distributed ledger and mainly known for its transparency and can be used as an even more legitimate way for funding a vast spectrum of projects and causes. Blockchain is essentially a digital ledger of transactions that is distributed among various networks on the blockchain[4], each block on blockchain contains the hash value of the previous block and its own hash value too thus like this a chain of blocks are combined together to form blockchain and if someone tries to tamper with them the hash values of each block changes. The key feature of blockchain is to provide transparency and trust, every transaction made on the blockchain can be viewed and can not be deleted. Thus we can say blockchain is the answer to the question raised earlier about the issues faced due to transparency and fraud in crowdfunding.

2 Blockchain

Blockchain is an immutable distributed ledger, makes the history of any digital asset unalterable and transparent using cryptographic algorithms and decentralization.[4].Blockchain is a simple way of passing any type of information from A to B or transaction etc.in a decentralized way and maintaining transparency.The term blockchain is only heard with cryptocurrency but apart from this, this technology has various other fields such as Banking system, Supply chain, Crowdfunding, Land Registry, Voting, Storing data such as passports, ID cards etc.

Given below is a diagram 1 which shows the working of blockchain.The first block of the blockchain is called a genesis block and contains a hash value of 0000, it can be also called block 0 of blockchain.Block 1 contains the previous hash value of genesis block.And as we can see that all the blocks are interconnected to each other according to their hash values, each block contains a hash value of previous block.

When a transaction takes place a new block is added to the blockchain it is first mined and verified by the miners, miners solve the given problem and the one who solves faster gets to add the block to the blockchain and also receives some awards like in ethereum miners receive 3 ether for mining a block.Each block contains a public and a private key, they are generated using cryptographic algorithms like ECC(Elliptic-Curve Cryptography) which is used in ethereum because it uses 256 bits as compared to RSA also which uses 3072 bits.Using shorter key can result in less computational power and fast and secure connection.A block contains three different values-

1 Data- Data can be any information sent from one user to another

2 Hash Value- Hash value is the current hash value of the block which is generated when the block is added, they are generated using hashing algorithms such as SHA-1 or Keccak-256 etc.

3 Previous Hash Value- Previous hash is the hash value of the previous block.

If someone tries to tamper with blockchain the hash value of the block changes and as we know all the blocks are connected, the hash values of all the blocks will change but their are some attacks such DDOS(distributed denial-of-service) attacks and the 51% attacks in which miners or group of miners control 50% of a network mining power, hash rate and computing power to mine new blocks. Attackers uses 51% attacks to reverse the transactions that have taken place which is also known as double spending problem.Thus there are some challenges to the technology such as 51% attacks and setting up the environment for blockchain, hiring developers etc. which is quite expensive right now but these challenges wont stay like this in upcoming future.

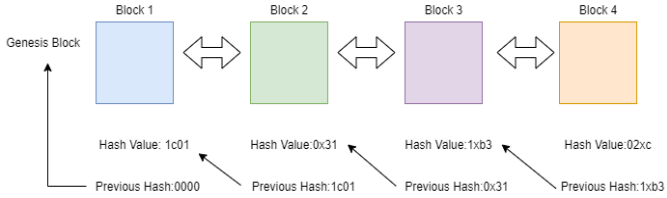


Diagram 1

3 Literature Survey

Zibin Zeng et.al[5] explains a survey blockchain in his paper where he is comparing different aspects of applications and challenges faced by the blockchain technology and mining management ways to increase throughput and decrease processing time. Cynthia Weiyi Cai et.al[6] explains and identifies gaps in economic and finance, and also researches how crowdfunding and blockchain can be used in the finance industry. Hasnan Baber et.al[7] explains about how crowdfunding is beneficial in current scenarios and also introduces a model 'WHIRL' which is a blockchain-based crowdfunding model that assures the members to get their project funded. Waheeda Dhokley et.al[8] explains about blockchain crowdfunding model and introduces a blockchain-based model system 'CROWDSF' which integrates both crowdfunding and blockchain to achieve security. Zhao Hongjiang et.al[9] explains the problems faced in crowdfunding like investor abuse,illegal transactions, frauds etc. and proposed a solution using blockchain to overcome these issues.

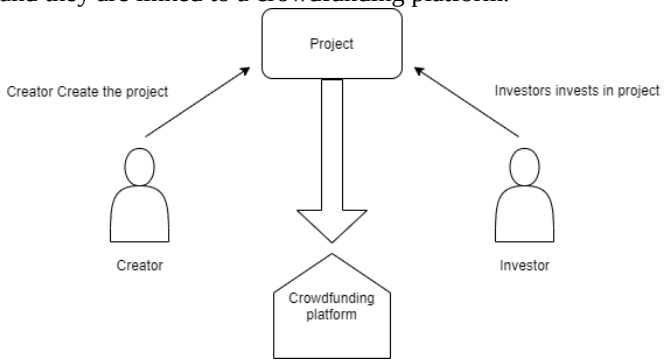
4 Conventional vs Blockchain Crowdfunding

4.1 Conventional Crowdfunding

In simple terms crowdfunding means that a large number of people come together to invest in small or large amounts to fund a project related to any business. Crowdfunding expands the scope of investing online via a variety of social media platforms. Online funding helps in the huge engagement of various investors and entrepreneurs across the world to invest in the projects. Even small amounts of funding from a lot of people help in generating a great amount to finally start working on the project. This modern crowdfunding model is generally based on three types of actors: the project initiator who proposes the idea or project to be funded, individuals or groups who support the idea, and a moderating organization (the "platform") that brings the parties together to launch the idea.[5] Crowdfunding has been used to finance huge varietal entrepreneurial outlines related to travel, medicine, airlines, transport, e-commerce, fashion and beauty, and many alike. Crowdfunding can be done on various online platforms but the most used platform is Kickstarter.

Kickstarter is the number one and most used platform for crowdfunding. Kickstarter aims to bring the projects to life where interest groups, investors and entrepreneurs finance the various projects available on its platform, which are raised by various creators. Kickstarter has been a successful platform in funding a lot of projects. It is a great platform if one wants to bring their creative ideas to life on a budget because people adhere to such budget projects as they don't want to risk too much. Many projects on Kickstarter like EOS, Filecoin, Star Citizen, Tezos, et cetera were able to raise funds over $10 million. This is mere because these projects might be innovative and people had a certainty that they would ultimately benefit from it. Although, an out of the box idea with innovation and creativity is always eye-catching. However, there have been many frauds on Kickstarter as well. In the real world, the word of honor may not be maintained and ultimately lead to the destruction of dreamy promises made by fraudulent companies. One such example is "Beef jerky made from Kobe Beef" where this campaign raised more than $120,000 in funding, which was 50 times more than its actual funding goal. On investigation, it was found out that it was all fake including the tasters of the beef. Even Kickstarter had no information about the organization behind it. Such frauds generally leave the backers who fund these campaigns with disappointment and definitely with the empty pockets. Many other examples are also there where organizations are not able to fulfill the promises made by them to investors. Given below is a block diagram of conventional crowdfunding platforms. There are two types of parties which play a major role: one is a creator and the other is an investor. The creator

creates the project and investors invest in particular projects and they are linked to a crowdfunding platform.



4.2 Blockchain Crowdfunding

Blockchain is a peer to peer network, it is a distributed ledger which can be implemented in various scenarios such as crowdfunding. Crowdfunding is a process in which investors invest in products listed on crowdfunding platforms such as Kickstarter which is one of the biggest platforms for crowdfunding. According to some surveys, Kickstarter has gained a lot of importance in recent years but as we know there are flaws in everything like that Kickstarter has also faced issues regarding transparency. Thus to overcome the issue faced in recent scenarios of crowdfunding we can implement it with blockchain technology, blockchain can change the view of crowdfunding as compared to the current scenarios in ways such as-

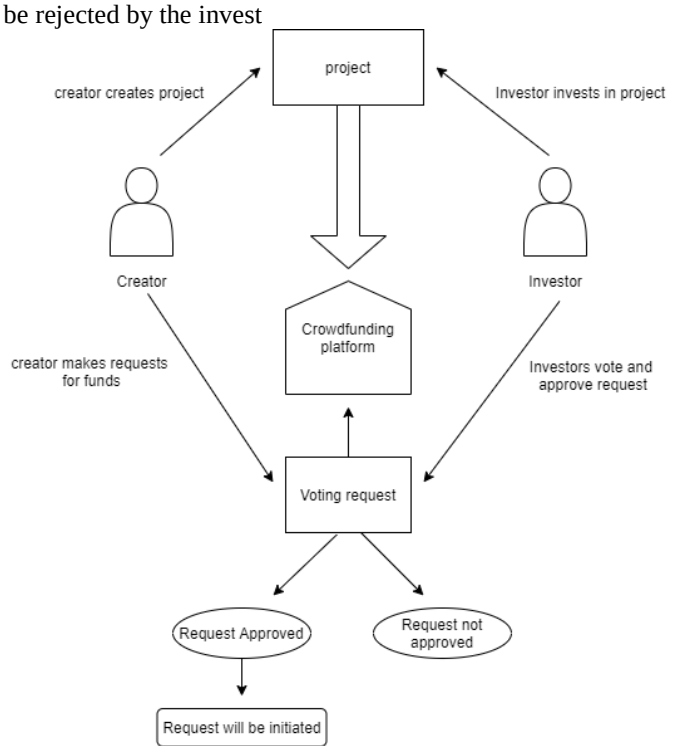
1 Transparency-One of the positive aspects of this technology is the transparency it provides, it provides a distributed and valid ledger of transactions. Blockchain is a transparent network where anyone can join the network and view information which also leads to building trust between creators and investors. In the case of crowdfunding, transparency is required to overcome the frauds so that people can trust each other in this process and also to cut off the role of third-party mediators.

2 Decentralization- Blockchain is a decentralized network that means that it will provide a decentralized network to both potential startups and funders, removing the influence of companies and eliminating large fees will also benefit in making crowdfunding less expensive for both investors and creators.[6]

3 Voting- We can implement voting through smart contracts, smart contracts are used for building business logic on the blockchain they are lines of codes that can be executed when terms and conditions are met[7]. We can use smart contracts to implement voting in the crowdfunding process which will benefit the investors so that they can vote for a request relating to investments made by the creator of the project and those votes can be recorded on the blockchain.

4 Opportunities - Many opportunities can be given to both creator and investors as blockchain crowdfunding will provide a decentralized network where the role of small companies and third party mediators will reduce which will result in eliminating large fees and will make the process less expensive, equal opportunities can be given to both investors and creators by providing them public access and full control on the network.[8]

Given below is a block diagram of the Blockchain crowdfunding platform in which there is a creator who creates the project and deploys it on the platform and investors can donate to a particular project and can become the part of the project apart from all this blockchain voting is used in which creator can request for funding and investors can vote to whether approve the request or not, if the request is approved after voting then the request can be initiated further else it will be rejected by the invest



Given below is a table which highlights the key point differences between conventional crowdfunding and blockchain crowdfunding

Conventional Crowdfunding	Blockchain Crowdfunding
A large number of people come together to invest in small or large amounts to fund a project related to any business.	Blockchain is a peer to peer network, it is a distributed ledger which can be implemented in various scenarios such as crowdfunding.
There is no transparency as to how transactions are being made.	Blockchain is a transparent network and a distributed network.
It is not a secure method of crowdfunding as there is no transparency to the donors.	It is a secure method of crowdfunding as transparency of data flow is maintained
It does not provide voting opportunities to the donors.	It provides voting opportunities to donors. For example, the manager of the contract can make a request for funding and donors can vote on that particular request. If approved by all, then request will be processed further else it won't be.
Conventional crowdfunding is less efficient as many fraudulent cases are reported.	Blockchain Crowdfunding is more efficient.

Diagram 4

5 Research Work

In this section, the authors have proposed a model to change the current scenario process and to improve the ongoing difficulties in the field of crowdfunding. The primary purpose of the model is that we can use blockchain in crowdfunding and to make the process transparent.

5.1 Project Architecture

The project focuses on two major roles-

1 User/Donator - User is an entity who can view all the deployed campaigns on the web app. A user can access all the information regarding a particular campaign and if found potential users can also donate in the campaign and can become part of the donors for a particular campaign he or she donated. Users can donate in multiple campaigns and can access all the perks given to a donor for a particular campaign. Suppose a user donated 2 ether and in return, the campaign gives the user a 5% share in the company, just like these different perks can be given to a donor in return for donating. Another interesting feature given to the user is voting the donors for a particular vote on a request initiated by the creator of the campaign. Request made can be any type but primarily it is regarding the further investments like a creator can make a request to buy some hardware from a vendor, he will add the request and donors can approve or reject them., if approved creator can finalize the request and the amount will be deducted from the campaign contribution. The amount will be sent directly to the vendor, thus the issue of fraud will be resolved here as instead of giving the amount to the creator its been transferred directly to the vendor.

2 Creator - Creator can create a campaign by giving some minimum contribution which is in Wei (the smallest unit of ether 1 Ether = 1000000000000000000 Wei).The campaign gets added on the web page with its address, donors can view the campaign. The creator can make a request as per the requirement for building a product and the address of the vendor, donors can reject or approve the project after approving the creator can only finalize the request.

4.2 Modules

The authors have used different modules in the project. These modules are -

1 Minimum Contribution- Creators can contribute a minimum amount in Wei to deploy the campaign on the web-app. Without giving a minimum contribution creator can deploy its project

2 Single campaign - Donor or creator can view the single campaign information, this module shows the information regarding a particular campaign, information such as manager or creator address, requests, donors or approvers of the campaign amount. And it also gives the option to the donor to donate in the campaign and can view all the requests made or finalized.

3 Request module - Creator can make requests for a particular item regarding building a project as if the creator makes a request for buying a battery. Creator will fill a form with fields such as description, the amount required and the recipient address, the recipient is the vendor from which the battery will be purchased. The request will be added and the donors can view, approve, or reject the request. After voting if approved the creator will finalize the request and the amount will be deducted from the campaigns account and will be sent to the recipient directly.

5.3 Technology

The authors have used Ethereum for backend and React and Next.js for frontend

Given below is the system architecture of our project

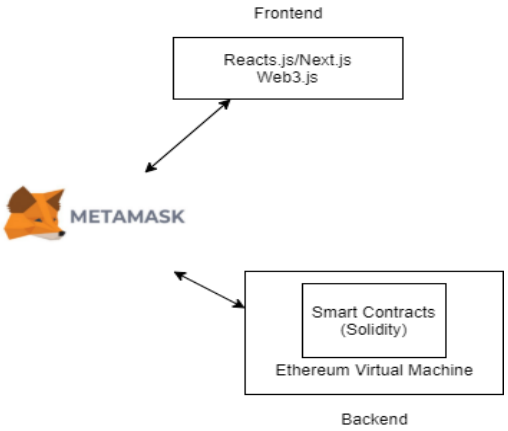


Diagram 5

1 Frontend - For the client side we have used React.js and Next.js, React.js is a library used for building frontend web apps, Next.js is a library on React.js which is used for server - side rendering and Web3.js is javascript library which is used for interacting with ethereum node using HTTP.

2 Metamask - Metamask is a cryptocurrency wallet and is used as a chrome extension. It is used as an interface for interacting with ethereum blockchain. Meatmask is used for storing ethereum accounts, it is secure and efficient to use and we can also deploy to main ethereum networks using metamask. Our project is deployed to Rinkeby Test Network..

3 Ethereum - Ethereum is best known for cryptocurrency but it can also be used for business logic means we can use ethereum for building smart contracts. Smart contracts are the layer on the blockchain which are used for building business logic on the blockchain; they are programs that govern the behavior of accounts with ethereum state. We use Solidity language for building smart contracts, it is a high-level object-oriented language which is influenced by c++, python, and javascript to target ethereum virtual machines (EVM).

3.1 Why is Ethereum used?

Ethereum is best suited for building Dapps because-

1 Solidity- Ethereum has its own very high-level and object-oriented language that is solidity, it provides a human-readable format which can also be understood by machines and it is also a combination of Javascript, Python, and C++

2 Hashing technique - Hashing is a process of converting strings into random values using mathematical functions and it is one way to enable security during the transactions in the blockchain. Ethereum uses Keccak-256 which produces 256 bits hash. Keccak is a versatile cryptographic algorithm used for hashing and a winner of a multi-year contest held by NIST, it provides a sufficient hashing entropy for a proof-of-work system and it is best suited with Dapps. Keccak256() can also be used as a hashing function in solidity.

3 Public-key cryptography - The use of public-key cryptography in blockchain is to maintain security, public keys are widely used and private keys are kept hidden so while encoding a message we use public keys and while decoding it we use private keys. Ethereum uses ECDSA (Elliptic Curve Digital Signature Algorithm) for public key cryptography which uses public/private key pairs means for every public key there is a private key. We can share our public key with anyone because deriving a private key from a public key is next to impossible. Another type of cryptographic algorithm is RSA but it is not efficient as ECDSA, because RSA uses 3072 public keys for computational complexity and ECDSA uses only 256 public key for computational complexity and ECDSA has the same security as RSA but uses less bits thats why its more efficient than RSA.

ECDSA is based on equation, y^2 = (x^3 + a*x + b) mod p [9] this is based on the equation of a curve on a graph where 'y' is squared and for any X coordinate we have two values of y and the curve is symmetric to x axis. The modulo will have only prime numbers and are in range of 160 bits, the modulo 'p' means the possible values of y^2 are between 0 to p-1 which gives us 'p' possible values. However we are dealing with integers; it gives us 'N' possible points on the curve and N < p. Since 'x' is having 2 possible points which means N/2 possible 'x' valid coordinates on the curve.The graph given below shows the equation.

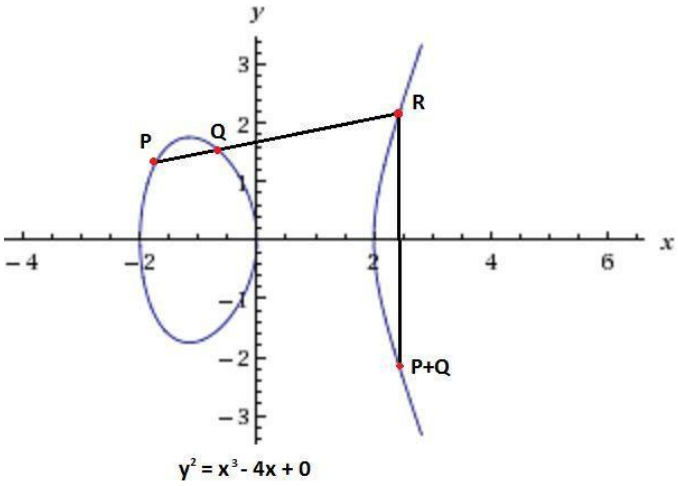


Diagram 6

The curve from on graph is based on equation y^2 = (x^3 + a * x + b)mod p where (a= -4, b=0) which is symmetric to x-axis and the points P,Q, and R means if we add point P to Q or draw a line from P to Q it will intersect point R and will lead to Point S where R is equal to negative S, (R = -S) to represent point R on x-axis [10]

ECDSA signature algorithm requires this equation for verifying and creating a signature, y^2 = (x^3 + a * x + b)mod p where a,b are parameters, p is prime modulo and N is number of points on the curve but now we add a point 'G' needed for ECDSA and it is known as a 'reference point'. For creating a private key we can use 160 bits and for public keys we use a point on curve generated via multiplication with G with a private key. Suppose we set 'dA' (some random no.) as private key and 'QA' (a point on curve) as public key so the formula will be QA = dA * G.

Now for creating a signature, a signature of 40 bits is required where 20-20 bits each, the first one is called R and the other S, the pair of (R,S) constitutes a signature now to calculate two values we must generate random number k (20 bits) and use point multiplication to calculate point P = k*G, the point's x value is 'R' and for calculating S, we need a SHA1 hash of the message which gives a 20 byte value which will be represented by 'z'. We can calculate S using equation S = k^-1 (z + dA * R) mod p [11] where k^-1 represents inverse of 'k' and (k^-1 * k)mod p = 1. k is a random number used for generating R, z is hash of message and dA is private key, R is x coordinate of P = k*G.

As we have created the signature successfully so we can verify it using equation P = S^-1*z*G + S^-1*R*Qa, if x coordinate of point P is R means signature is valid else not. To verify this we will substitute. P = S^-1*z*G + S^-1*R*Qa, Therefore Qa = dA*G, So P = S^-1*z*G + S^-1*R*dA*G. Take S^-1& G common, P = S^-1*G(z + R*dA) x coordinate of P must match R and R is x coordinate of k*G.

So P = k*G, k*G = S^-1*G(z + R*dA). Cancelling out G both sides, K = S^-1*(z + R*dA)

By inverting k and S. We get S = k^-1(z + R*dA) this is the equation used for creating signature thus signature matches, Hence Proved.

5 Gas Fee - Gas fees are used for paying the energy and the computational powers to set and get the functions in the ethereum blockchain. Ethereum blockchain uses a concept of gas to measure the amount of energy used for a particular smart contract. Gas is measured in wei, which is the smallest unit of ether 1 ether = 10^18 wei.

5.4 Result

The Screenshots of our model are given below with features explained.

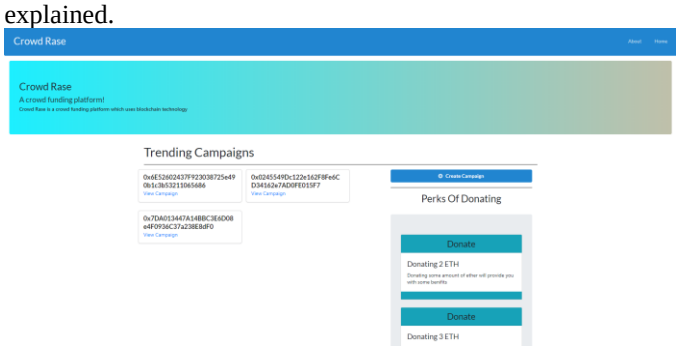


Diagram 7

This is the landing page of our project which shows the trending campaigns in the form of a card component with the address given of a particular campaign and we can also view the campaign details by clicking the view campaign link. In the top right, we have a button from where we can make or add a campaign, and some perks of donating are also given below.

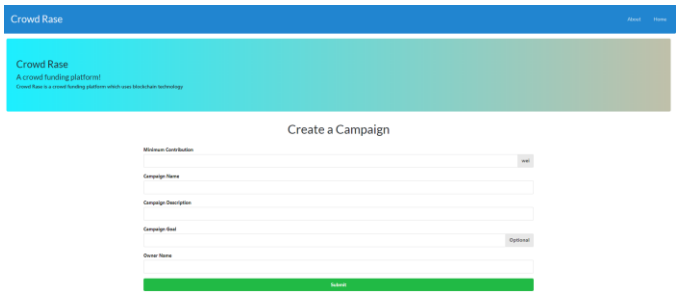


Diagram 8

With the use of this component, we can add a campaign by filling the particular details asked like Minimum contribution in Wei, campaign name, owner name, etc.

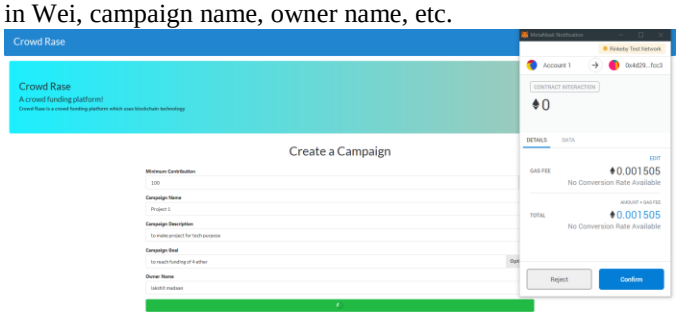


Diagram 9

On submitting we get a pop of our Metamask account which shows the gas details used for calling this function and the total ethers used. After confirming it takes around 20 seconds and we get redirected to the home page where our campaign gets added.

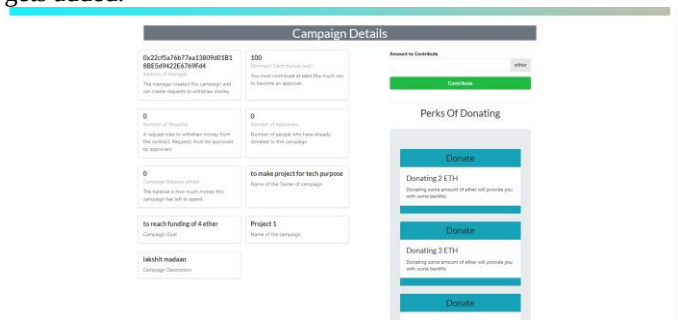


Diagram 10

We can click on the "view campaign" link and get redirected to the campaign detail page. Here we can look for the campaign details like owner name, manager address, number of approvers and requests made to the campaign, etc

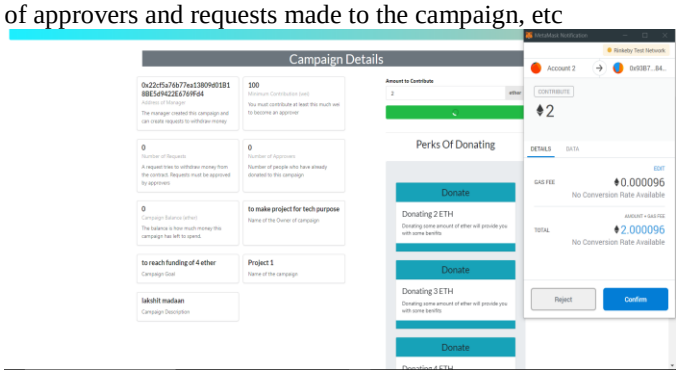


Diagram 11

If any user likes a particular campaign they can contribute to it and can be a part of the approver's list. After becoming an approver he or she can participate in voting the request and can also take advantage of perks of donation. On submitting we get a pop up from Metamask account for the transaction as we can see the user is donating 2 ether plus the gas fees.

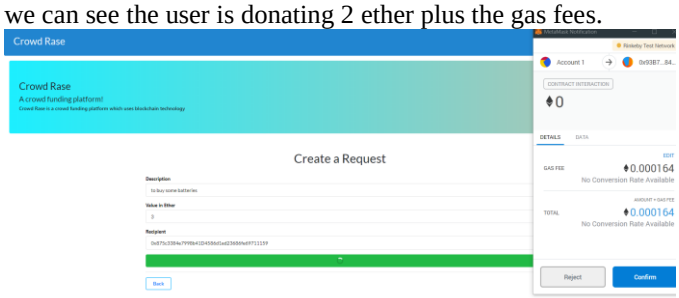


Diagram 12

The owner or the manager of the particular campaign can make a request for funding by filling the amount, description of the funding, and the recipient to whom we have to send the money. The manager has to pay a certain amount of gas fees to call the function and make a request.

Diagram 13

After when the request is added it can be viewed inside a table with Id, description, amount, etc. Approvers can now vote by clicking the approve button if approved by all then the bar will turn green and request will be ready to finalize

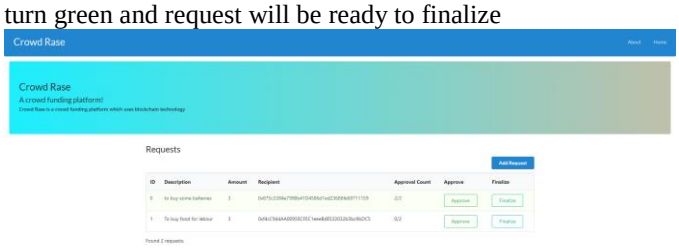


Diagram 14

As we can see the bar turns green means the request is approved by all and is ready to finalize by the manager. The manager can only finalize the request from its account else the transaction will fail

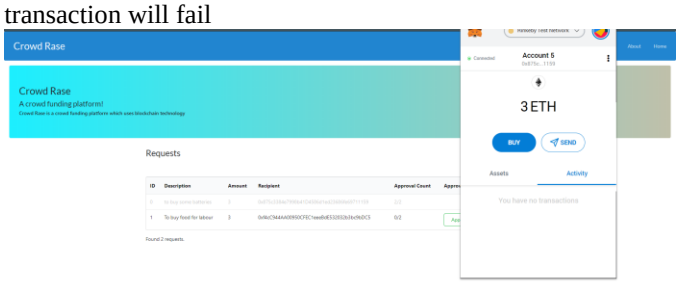


Diagram 15

After finalizing the request from the manager's account the amount will be deducted from the campaign balance and will be sent to the recipient. As we can see in the Metamask pop up that the recipient has received the amount and the request will fade automatically after success.

5.5 Future Scope

Blockchain crowdfunding has prominent scope. The capacity of the project can be expanded to different aspects. One of the future scope is that we can add file and image uploading systems using IPFS. IPFS (InterPlanetary File System) is a protocol for peer to peer network and to share data in a distributed file system. We can store the hash of a particular image or a file and we can store it on the distributed network. Moreover, the projects that are more utilitarian can be updated accordingly on the trending list based on the number of people investing in that particular project. We can also take this project on the next level by creating an authentication system for particular individuals like creators and investors, so that they can manage their profiles and can donate in various campaigns.

6 Conclusion

Crowdfunding with Blockchain has a substantial future. The development of such technology can do economical wonders in various financial fields. Our paper aims to highlight the key features and differences between conventional crowdfunding and blockchain crowdfunding. We have proposed a model in our paper that focuses on how we can use blockchain in crowdfunding. The model overcomes all the drawbacks found in conventional crowdfunding such as transparency and security. Blockchain is best known for its decentralized structure and transparency, the transactions made using blockchain are pellucid and reliable. Thus, we can see all the transactions on the distributed ledger which makes blockchain crowdfunding overcome fraudulent and transparency issues. There are many challenges faced by blockchain technology like setting up this technology is quite expensive; however, apart from these challenges this technology has many positive aspects, which we have covered in our model and that makes it unique.

References

1 https://www.investopedia.com/terms/c/crowdfunding.asp
2 https://www.lifewire.com/what-is-kickstarter-3486258
3 https://hackaday.com/2015/08/25/the-problem-with-kickstarter-a-lack-of-transparency/
4 https://builtin.com/blockchain
5https://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends
6 https://onlinelibrary.wiley.com/doi/full/10.1111/acfi.12405
7 https://www.ijrte.org/wp-content/uploads/papers/v8i3/C5398098319.pdf
8 https://www.ijcseonline.org/pub_paper/113-IJCSE-05801.pdf
9 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3133176
10 https://en.wikipedia.org/wiki/Crowdfunding#cite_note-unibocconi-5
11 https://www.howtotoken.com/explained/decentralized-crowdfunding-create-safer-type-of-investment/
12 https://www.ibm.com/blogs/blockchain/2018/07/what-are-smart-contracts-on-blockchain
13 https://www.howtotoken.com/explained/decentralized-crowdfunding-create-safer-type-of-investment/
14https://www.instructables.com/id/Understanding-how-ECDSA-protects-your-data/#:~:text=ECDSA%20stands%20for%20%E2%80%9CElliptic%20Curve,authenticity%20without%20compromising%20its%20security.&text=You%20shouldn't%20confuse%20ECDSA,is%20to%20encrypt%20the%20data.
15https://www.instructables.com/id/Understanding-how-ECDSA-protects-your-data/#:~:text=ECDSA%20stands%20for%20%E2%80%9CElliptic%20Curve,authenticity%20without%20compromising%20its%20security.&text=You%20shouldn't%20confuse%20ECDSA,is%20to%20encrypt%20the%20data.
16https://www.instructables.com/id/Understanding-how-ECDSA-protects-your-data/#:~:text=ECDSA%20stands%20for%20%E2%80%9CElliptic%20Curve,authenticity%20without%20compromising%20its%20security.&text=You%20shouldn't%20confuse%20ECDSA,is%20to%20encrypt%20the%20data.

