Fundraising Portal using Smart Contracts in Blockchain using Group Signatures

M. V. Ranjith Kumar, Arpit Shukla, Saket Agarwal

Abstract: ***Generally, to make a campaign,startup, or any innovative idea successful requires some amount of donation. Fundraising or let us say Crowdfunding is an efficient way to raise money for your ideas, campaigns, startups etc. There are a lot of platforms available online and they provide space for setting up your own campaign so that you can gets funds for your campaign. people can go and contribute to any idea they like and get benefit from the pledge that you make. Certainly, there are lot of drawbacks to this model. There is no transparency and no assurance that your money is being put to the right use, there are charges to use the platform and many other issues. We try to over come these issues by making a fundraising platform using smart contract in solidity. This will be more secure as it uses Ethereum blockchain to make all the transactions and all the transactions are ethereum based. Not only this but the contributors have the right to vote for a transaction and only when a minimum consensus is achieved the requested transaction can be made.Contributors can have their own pool of contributors which can be achieved by multi-signature wallet.By creating a multi-signed wallet , there will be two factor authentication mechanism to access funds, which are related more to security concerns. This not only enables a transparent transaction but also develops trust in the users of the platform. This not only resolves major drawbacks faced in the current live non blockchain based platforms like Kickstarter but also brings in more efficient platform to serve the purpose***

Keywords: ***Fundraising,Crowdfunding, Blockchain, Ethereum, Kickstarter, Consensus, Smart contracts, startups, campaign, transactions, transparency, Group signatures.***

I. INTRODUCTION

Today's era is the era where count to people choosing self employment as an option is increasing day by day. People are getting more innovative and are being exposed to the current trends and new technological advancements. This has not only resulted in better and innovated products but has also increased the number of start-ups. As the number of start-ups have increased they require more amount of funds in order to have a kickstart to their idea. This is where the fund raising platforms come into play.

These platforms help start-ups, ideas, people who need donations or any other organization or personal who need funds to establish a campaign to raise funds for a cause. But these platforms are not completely secure and are not contributor centric. They aren't transparent and the funds are directly transferred to the campaign creator's account which can be used by him/her in any way they want without any track of how the money is spent the contributors are left out without any assurance."The present fundraising platforms have a lot of drawbacks they are not at all contributor friendly and help have been the abode of lot of scams where the campaign creator took all the money that they have raised and used it for their selfish motives and established the fact that these platforms need improvement and are a serious concern because some of the campaigns raise funds that are amounting to a large amount of money. The following are the drawbacks in the current model.

1. No Transparency
2. High Service charges by platform
3. No record of transactions
4. No Contributor guarantee Policy
5. Blockchain in an incorruptible ledger that keeps track of all the transactions.

All the records are stored in the node in a decentralized network where track of each and every transaction can be done. Ethereum allows running applications in blockchain using solidity. These smart contracts are coded using a high level programming language solidity." " The proposed system uses this concept of smart contracts to make a platform that over comes the issues that are there in the current live model for online crowdfunding or fundraising. All the transactions will be under a record and will be done using a crypto currency like ether and it's denominations . The contributor has full control over the investment that they make. This is done using the request approval module. The campaign manager will have to make request if he wants to make any transaction. This way the proposed system will be.

1. Trustful
2. Contibutors control money
3. Recorded transaction
4. Contributor Guarentee Policy
5. Secured storage of money

II. LITERATURE SURVEY

[1] Afiya Ayman & Amna Aziz & Amin Alipour & Aron Laszka in their paper on development on smart contract and development state. smart contract platforms are decentralized and trustworthy of general purpose computation that is smart contracts. These are applicable to a wide range of fields be it finance where money is involved or health or management.

Revised Manuscript Received on March 18, 2020.

M. V. Ranjith Kumar, Assistant Professor, Department of Computer Science and Engineering ,SRM institute of Science and Technology, Chennai

Arpit Shukla, Department of Computer Science and Engineering, SRM institute of Science and Technology, Chennai

Saket Agarwal, Department of Computer Science and Engineering, SRM institute of Science and Technology, Chennai

[2] Udokwu, Chibuzor & Kormiltsyn, Aleksandr & Thangalimodzi, Kondwani & Norta, Alex in their paper on The state of art for the blockchain enabled contracts talks about Consensus mechanism. They are basically groupped into two, voting basesd consensus and proof based consensus .

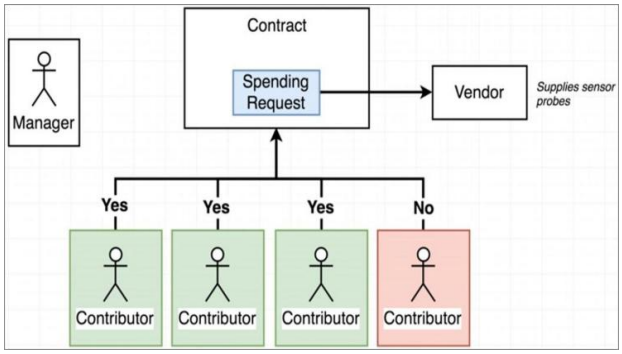
[3] Maher Alharby and Aad van Moorsel in their paper titled a systematic mapping study on current research topics on smart contracts. the transactions in current systems invlove a third party that executes and verifies the transactions(eg: banks). This is what results in security issues as it is a single point of failure and have high service fee. Block chain tackles all these issues as it unable non trusted authorities to interact with it each other in a distributed manner with the involvement of a third party.

[4] Alexandra Moritz & Joern H. Block in their paper on Crowdfunding. current platforms aren't fully secure and lot of scams and frauds have been done using these platforms. The major issue is that the contributor does not have the access to the money they contribute and have maximum disadvantage that way. Smart contracts have an involvement in finance as they involve crypto currencies and that can be used as an alternate source of money and can be made to use transactions.

[5] Maximilian Wohrer and Uwe Zdun in their paper on Design Patterns for Smart Contracts in the Ethereum Ecosystem explain various methodologies that can be implemented and how to improve their functionality it discusses various ownership pattern.

III. PROPOSED WORK

We discuss how blockchain technology can effectively and securely handle the relationship between fundraisers, platforms and the investors.The propose system is better than the previous Crowdfunding platforms because it provides various additional benefit to track the money that an investor spends in the campaign.This type of approach by using a Ethereum smart contract where contributors have an idea of where their money is being sent to, and they have the ability to review these spending requests before the money gets spent. The control lies in the congress of investors who collectively decide whether to pass or to not to pass a payment to the vendor collectively.It gets passed only when more than 51% of the investors agrees to it. This is done using consensus protocol.



IV. IMPLEMENTATION

We made a smartcontract in solidity which is a ethereum based smart contract development language.Solidity is a statically-tiped programming language designed for developing smart contracts that runs on the JVM.

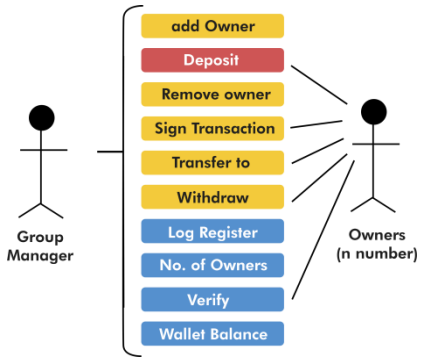
We made a contract named contract campaign, in the contract campaign we made an function named CreateRequest in which the request is created and description ,value and the approval count is stored.We made another function in contract campaign named function contributer in which if the contributer contributes more than the minimum amount given by campaing manager then the contributer count gets increased and approves the contributer to contribute.We made another function named approvedContract in which the votes of each contributor gets stored and if the voting percentage is more than 51% it will return true else it will reject the request.We made one more function named FinalizeRequest where the manager will finalize the request if the voting percentage is more than 51% and the request is approved.

We used web3 to compile our contract in the blockchain as web3 is a collection of libraries which allows us to interact with ethereum node. Using web3 we can retrieve user account, send transactions and interact with smart contracts.

The compile script in java script after compilation produces ABI and bytecode , these are stored in a separate file and then used in the deploy script using various web3 and node commands to deploy the contract into the ethereum blockchain , after the deployment is completed , we get the address at which the contract is deployed.

We have made it even made [6] Multi-Signature Wallets. These allow us to have a collection of money in the wallet with multiple owners and further it helps in implementing group signatures in them. This further increases the security and helps in making the system a tractable and more efficient as there is a group manager who keeps the track of all the transactions and any malpractice within the group can be easily identified with it.

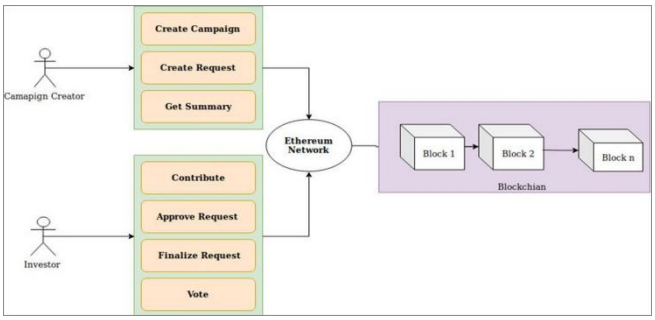
This MultiSig wallet contract constitutes of the following modules.



Main Fucntionality of the contract is to have a group manager who has the access to a log book. This keeps track of all the transactions and can only be accessed by the manager. Manager can add members as owner to the wallet. These people can add money to the wallet and withdraw the amount from the wallet provided it is less than what they have deposited. This whole system provides an ability to trace the on goings in the pool of the owners

[7] We used Infura which helps in running our application without setting up our ethereum wallet. It also helps in the transaction signing as well as connection to the ethereum network.

As displayed in figure 1,the flow diagram of our fundraising portal is shown.



V. CONCLUSION

In this paper, we proposed a fresh linkable group signature based on the Consortium Blockchain to achieve the goal which tracing the real-world identity in anonymous cryptocurrencies.These solidity based contracts that run on an ethereum blockchain enable us to make more secure, transparent and trusted platform for fundraising. This platform not only is free to use because it does not have a third party involvement but it also keeps the track of all the transaction that takes place. More over it gives the contributors to know exactly where their money is and how they want it to be used by using a voting based consensus mechanism this enables the platform to be trusted and secured. Smart contracts are developing technologies that can be implemented in various performing platforms for making the system more secure and trusted.

RESULT

We proposed a fresh link able group signature based on the Consortium Block chain to achieve the goal which tracingthereal-world identity in anony mouscryptocurrencies.

REFERENCES

1. Afiya Ayman & Amna Aziz & Amin Alipour & Aron Laszka Smart "Contract Development in Practice: Trends,Issues,and Discussions on StackOverflow" arXiv:1905.08833v1 [cs.CY] 15 May 2019.
2. Udokwu, Chibuzor & Kormiltsyn, Aleksandr & Thangalimodzi, Kondwani & Norta, Alex. (2018). The "State of the Art for Blockchain-Enabled Smart- Contract Applications in the Organization." Tallinn University of Technology, Tallinn, Estonia
3. Alharby, Maher & van Moorsel, Aad. (2017). "A Systematic Mapping Study on Current Research Topics in Smart Contracts." International Journal of Computer Science and Information Technology. 9. 151-164. 10.5121/ijcsit.2017.9511.Y.
4. Alexandra Moritz & Joern H. "BlockCrowdfunding: A Literature Review and Research" Trier University, Trier, Germany Erasmus University Rotterdam, Rotterdam, Netherlands.
5. Maximilian Wohrer and Uwe Zdun Wahringerstraße "Design Patterns for Smart Contracts in the Ethereum Ecosystem" 29, 1090 Vienna, Austria
6. J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In S. Goldwasser, editor, *Advances in Cryptology — CRYPTO' 88*, volume 403 of *Lecture Notes in Computer Science*, pages 27–35. Springer-Verlag, 1990.
7. C. Boyd. Digital multisignatures. In H. J. Beker and F. Piper, editors, *Cryptography and Coding*, pages 241–246. The Institute of Mathematics and its Applications Conference Series, Oxford Science Publications, 1989.
8. D. Chaum and T. Pedersen. Wallet databases with observers. In E. F. Brickell, editor, *Advances in Cryptology — CRYPTO' 92*, volume 740 of *Lecture Notes in Computer Science*, pages 89–105. Springer-Verlag, 2018.
9. L. Chen and T. P. Pedersen. New group signature schemes. In A. D. Santis, editor, *Advances in Cryptology — EUROCRYPT' 94*, volume 950 of *Lecture Notes in Computer Science*, pages 171–181. Springer-Verlag,.
10. Ateniese, G., Camenisch, J., Hohenberger, S., de Medeiros, B.: Practical group signatures without random oracles. Cryptology ePrint Archive, Report 2005/385 (2005),

AUTHOR PROFILE

M. V. Ranjith Kumar is currently a Ph.D. research scholar in the Department of Information Technology in SSN College of Engineering, Anna University, India. He received his M.S. degree in Advance Computing: In Internet Technology with security from University of Bristol (UoB) United Kingdom. He completed his M.E. in Computer Science and Engi- neering, M.B.A. in General Management and B.E. in Electronic andCommunication
Engineering from Anna University, India. His research interests include cryptography and information security to apply deep theo- retical work in the mathematics of cryptography to real-world prob- lems. He is an active member in Professional Bodies such as IET, ISCA, CSI, IAENG.

Arpit Shukla is currently a Final year B.tech student in the field of computer science and engineeringfrom SRM institute of science and technology and is having keen interest in the field of Blockchain and solidity development. He is very keen in `in learning new advancements in the filed of blockchain and cryptography. He is and active member in the IET and a dedicated researcher.

Saket Agarwal is currently a B.tech pursuing student in the field of computer scinece and engineering who is in fourth year and has keen interest in javascript development and research in back end server side scripting. He is dedicated and very honest in his work and is keen to learn more day by day. He is an active member of IET.