Secure Fund Raiser Using Smart Contracts

Aceson Sunny, Mohammed Muhsin, Muhammed Yaseen

UG (Final Year), Department of CSE, Mar Athanasius College of Engineering, Kothamangalam, Kerala, India

---***---

Abstract - *Crowd funding is an online cash raising technique that started as a path for the people to contribute limited quantity of money to enable innovative individuals to fund the venture. Using crowdfunding, people can put resources into pioneering businesses through a middle medium or platform. The issue with the current crowd funding technique is that, third party medium don't give the assurance of the money investor contributed for the project and investor don't have control over the cash they contributed. This paper proposes the blockchain based crowd funding by using which the platform can give a private, secure and decentralized path for crowdfunding. The main objective of this paper is to let investors contribute to any project effectively by creating smart contracts through which the contributors can have a control over the invested money and also both the project creators and investors can effectively make and reserve funding for the project.*

Key Words: Ethereum, Smart Contracts, Fund Raising, Solidity

1. INTRODUCTION

Crowdfunding is a way to raise money from a large number of individual investors or companies. In this, investors can contribute to any project they are interested in and can gain the profit if that project gets successful [1]. Nowadays, many crowdfunding platforms already exist and they take huge chunk of money from investors and contributes and leave them with empty promises. Crowdfunding using blockchain changes the traditional way to deal with business funding. Generally, when people need to raise a cash to begin a business, they have to design strategy, statistical surveying, and models, and afterward present the thoughts around to attract people or organizations. These subsidizing sources included banks, angel investors, venture capital firms. The present day crowdfunding model depends on three kinds of on-screen characters: the task initiator who proposes the thought or venture to be funded, people or investors who invests in the thought, and a platform which puts these two characters together to make the venture successful. It is used to finance a wide scope of start-ups, pioneering ideas, for example, innovative activities, medical advances, travel and social business enterprise ventures.

1.1 Types of crowdfunding

Donation-Based Crowd funding: In this type of crowdfunding there is no financial return to contributor and financial investors [2]. This includes charities, NGOs, disaster reliefs and medical helps.

Rewards-Based Crowd funding: In this type, individuals contribute to the projects in exchange of rewards which can be either profit or some product. Many platforms available now a day which uses this kind of crowdfunding.

Equity-Based Crowd funding: Unlike the above two, this type of crowdfunding allows to be a part of the company by buying shares. So in this, investors get a return of the profit earned by the company.

1.2 Present day Crowdfunding

All the crowd funding transactions today is dependent on several different crowdfunding platforms which takes lots of money from both investors and contributors to process their request which might sometimes not even be up to the mark. Many platforms serve as gatekeepers and they have strict rules and regulations which makes both investors and contributors hard to have a freedom in making the project successful. Having a great idea on a crowd funding platforms is not a guarantee that there will be a success. User will need a tactics to make their crowd funding page more visible on search engine and attract new customers to that project which requires huge investments in advertisement alone. Many of the crowd funding platforms do not ensure that the promise will be met in regards to contributors and it might be sometimes unfair to the contributors which makes them hesitate to invest in the venture due to which project managers face problems. Sometimes project managers have seen their whole business collapse before they even got a way to start their production because when idea gets very popular in the crowdfunding websites, many different business people get inspired and try to make similar products like that which increases more competition.

1.3 Blockchain

A blockchain is a growing sequence of blocks, that are connected together using cryptography. Each block calculates the hash using some cryptographic method, a hash of previous block, a period stamp of when it is made, and value-based information which is generally represented as merkle tree [9]. Blockchain doesn't permit any alteration of the information in the block. When the information is recorded, some random block can't be changed without approval of more than half of the nodes inblockchain, that is 51 percent. It is a mutual and unchangeable record and the data in it is open for anybody and everybody to see making it decentralized.

Thus, blockchain solves the problem of spending more as there is no need of any central server or trusted authority. Blockchain is secured using two techniques that is Proof of Work and Proof of Stake. In proof of work, a piece of data is produced usually called as nonce which is very time-consuming and takes lots of electricity and processing. But it is very easy for others to verify that nonce and blocks which satisfies certain requirements [3]. In proof of work, miners compete against each other to complete transactions on the network and get rewarded. In proof of stake, miners keep something at stake and when they mine effectively then only they can earn the reward, else they will lose the money kept at stake.

There are generally two types of blockchain, a public and a private blockchain. A public blockchain is a network which is open to public and anyone can download the rules. And then they can read, write or participate in the network which makes it distributed and decentralized. A private blockchain allows organizations to employ distributed ledger technology without making their data public. Ethereum is a public blockchain which is decentralized framework, and is completely independent and is not constrained by anybody by any means [10]. Then it can be incorporated in the ethereum blockchain which cannot be altered by any individual. A smart contract is a computer protocol that allows us to facilitate and verify the performance of a contract. These transactions are trackable and irreversible. Smart contracts define the rules and penalties of an agreement in the same way as a traditional contract does. This smart contracts are written using solidity programming language.

1.4 Crowdfunding using blockchain

Blockchain in crowdfunding allows decentralization which means that no individual platform or group of platforms control the smart contracts which makes it transparent to everyone in the blockchain [4]. It's a peer to peer network which collectively follows to a protocol for inter-node communication and validate new block, so no one can alter any block without approval of more than 50 percent nodes in the blockchain which makes it secure and safe. Anyone can create the project in the website with blockchain and anyone who has internet connectivity can donate to the project. Contributors do not have to worry about the empty promises like the traditional crowdfunding. The smart contracts will handle all the transactions so all the money will be stored in smart contracts rather than sending to the third party. Blockchain gives more freedom to project managers and the contributors so that contributors can have fractional contribution to the project.

2. RELATED WORK

Alexander Backmann [5] has pointed out the differences and similarities between the old fund raising techniques and the peer to peer lending market. Both fund raising techniques have a lot differences in the raised amount, the process of screening and the knowledge gained for risk management. These sort of researches may explain whether results from the new peer to peer lending technique is applicable to the traditional fund raising technique or vice versa. This also focuses on the traditional fund raising where the return on investment was very less and the venture used to get collapsed frequently.

In a study on crowd funding and its implications in India [2], it is shown that crowdfunding accompanies numerous advantages compared with existing ways accessible to new companies and SMEs. As crowdfunding is not available to open public, its very hard to get the investors attracted to the new ventures but the new generation have more knowledge about crowd funding which is a good starting point for this crowd funding platform to grow. This will likewise empower the new ventures to reach out to a more extensive segment of investors and financial specialist for raising capital.

Huasheng Zhu and Zach Zhizhong Zhou [6] has analyzed that blockchain is still emerging technology which is in exploratory stage and there are many technical and legal issues which needs to be considered before making it available to the public. There is still a room for improvement for blockchain business and market influencers to work together and change the business, deploy blockchain technology in market, and introduce innovative ideas. They have to develop their understanding of blockchain innovation, its worth, its chances, and its dangers. They ought to effectively advance blockchain applications in the Chinese crowdfunding market. Monetary proficiency and social advantages can be accomplished through specialized advancement and applications of blockchain.

Michael Gebert [7] has explained the applications and importance of blockchain technology in crowdfunding is particularly for small scale businesses as the startups havea constant threat of employment crisis and insecurity. It is thus necessary for governments to facilitate access to funds by small enterprises. With non-favorable environment of European government, crowdfunding has not been successful in the European region. It is very necessary for the small scale businesses to raise funds to operate therefore, the growth of crowdfunding platform is important.

In the paper crowdsourcing and crowdfunding platform using blockchain and collective intelligence [8], it is analyzed that crowdfunding and crowd sourcing in India are still in its early stages. Being an extremely new idea, the Indian population despite everything has not broadly acknowledged on the internet crowdfunding. In spite of the underlying challenges, the eventual fate of crowdfunding and publicly supporting in India is going to be brilliant. The essential necessities of any business will be business capital and human resources. This is particularly evident in the instances of startups and low level organizations as these generally struggle with combining resources. Thus utilization of blockchain in engineering will help in security part of the framework. The extent of such stages in India is splendid however the public should participate in this to make it successful.

3. PROPOSED WORK

As crowd funding contains a lot of transactions, there is a need to handle and document the actions legally. Therefore, a smart contract is used which is a transaction protocol which automatically execute, control and document actions of the transactions according to the agreement on behalf of project creators and investors. This paper proposes a method which includes two contracts one which stores all the projects and other one which handle the transactions for each project. In any crowdfunding platform, the main entities are project manager, contributors, vendors, smart contract, spending request and voting system. There are three stages included in the crowdfunding:

3.1 Project creation

In the first stage a project manager creates new project by mentioning the name of the project, the description of the project and the minimum contribution to that project. And the contributors then can view the all the open projects in crowd funding platform and can choose any project for which they want to contribute. To mark themselves as contributors, they have to invest minimum contribution for that project which project manager has mentioned while creating the project. And this money is added to the wallet which can be used by the project managers as shown in Fig. 1.

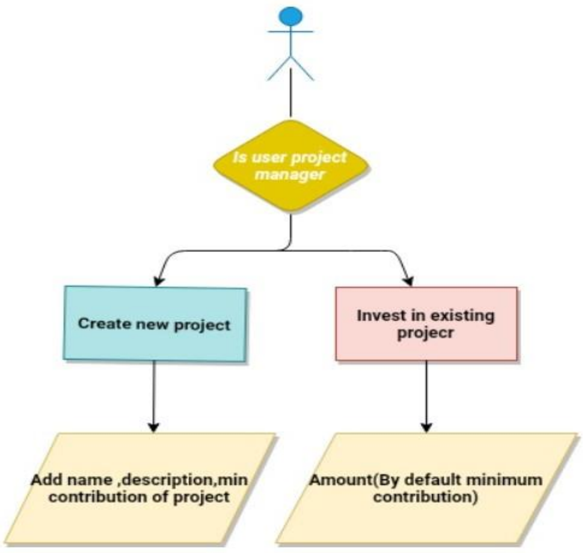

Is user project manager
Create new project
Invest in existing projecr
Add name ,description,min contribution of project
Amount(By default minimum contribution)

Fig -1: Creating or contributing to project

3.2 Spending request

In this stage, if a project manager wants to spend the money contributed by investors, then they have to create the spending request by giving the description about where they are going to spend the money, the total amountthey are going to spend and the address of the vendor who will supply the things required by the project manager as shown in Fig. 2.

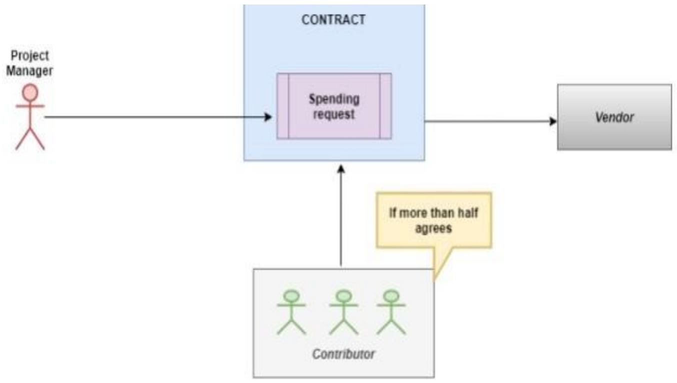


Fig -2: Voting system ensures money spent is in control of contributors

3.3 Voting system

The voting system is designed which ensures that the contributors who have invested in that specific project, only they can accept or reject the spending request sent byproject managers. And the voting system also ensures that the contributor once voted cannot vote again for that spending request. So if more than half of the contributors for that project agree for the spending request, then the money is sent to the vendor so that user can supply the utilities asked by project manager.

4. IMPLEMENTATION AND RESULT ANALYSIS

To implement the crowdfunding platform, a smart contract is needed which has to be written in solidity language. Then this is compiled and deployed in the ethereum blockchain using solidity compiler. Metamask which is a chrome browser extension is used to make all the transactions. Procedure for building a crowd funding platform:

Step 1: Creation of smart contract.

Step 2: Compilation of the smart contract to obtain the bytecode and application binary interface(ABI).

Step 3: Deployment of bytecode to the ethereum blockchain.

4.1 Creation of smart contract

It is a program which is written in solidity language to handle all the transactions automatically. As shown in Fig. 3, the project manager has to first create the project by mentioning the name, description and the minimum contribution for that project. Then user can create the spending request for spending the money contributed by the investors. For this project creators have to mention the description about where they are going to spend the money, the amount of money they are going to spend and the address of the vendor who will provide some service.

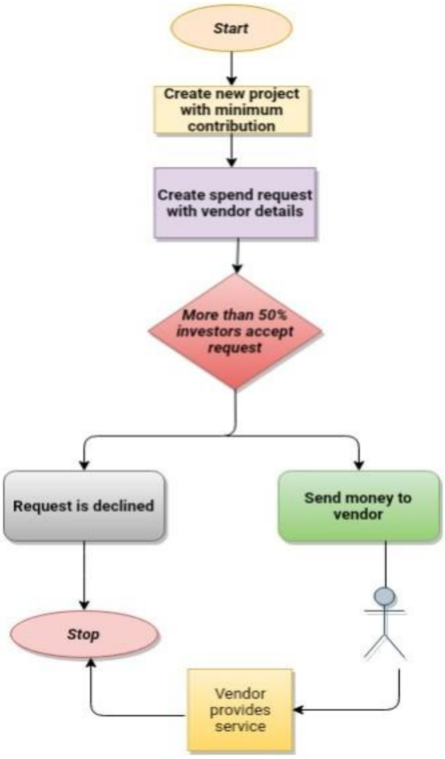

Start
Create new project with minimum contribution
Create spend request with vendor details
More than 50% investors accept request
Request is declined
Send money to vendor
Stop
Vendor provides service

Fig -3: Flow chart of project manager

In Fig. 4, it is shown that if the investor is interested in any project mentioned in crowd funding platform, then they can join the project by investing minimum contribution which project manager has set while creating the project. Then this money is added to the wallet assigned for the specific project. After that the contributor can either accept the spending request sent by the project manager or decline.

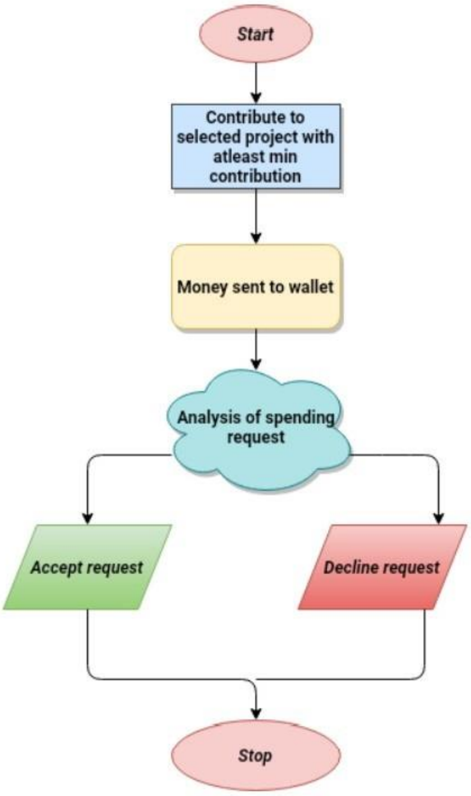

Start
Contribute to selected project with atleast min contribution
Money sent to wallet
Analysis of spending request
Accept request
Decline request
Stop

Fig -4: Flow chart of investor

4.2 Compilation and Deployment

The smart contract is compiled using the solidity compiler. This gives bytecode and application binary interface as output. Bytecode is then deployed to ethereum blockchain and application binary interface is used to interact with smart contract. Bytecode is hexadecimal representation of the compiled contract which can only be understood by Ethereum Virtual Machine(EVM).

The bytecode obtained from the compilation can be deployed to either rinkeby test network, ropsten test network or ethereum live network.

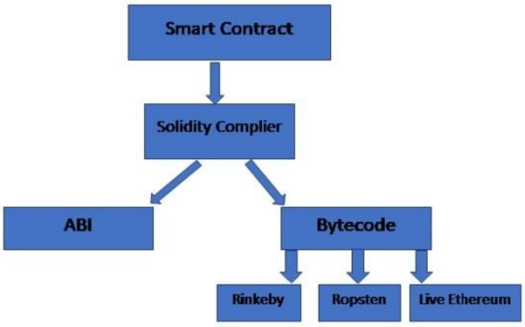
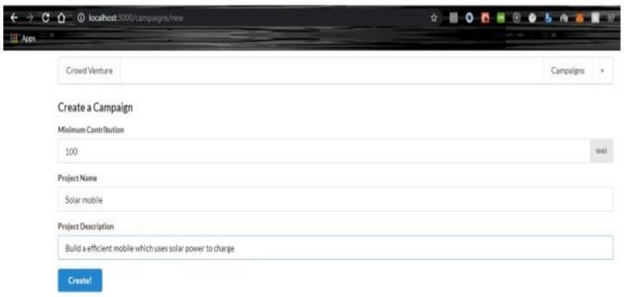


Fig -5: Compilation and deployment of smart contract

4.3 Result Analysis

When a user wants to create a new project then user can do it by pressing this button. It consists of name of the project, description of the project and the minimum contribution to the project as shown in Fig. 6.



Create a Campaign

Minimum Contribution

100 wei

Project Name

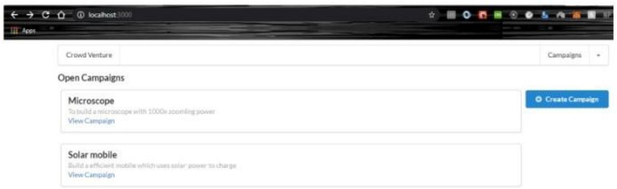
Solar mobile

Project Description

Build a efficient mobile which uses solar power to charge

Fig -6: Creation of venture

Here the list of all current projects are shown with their name, description and the address of project manager as shown in Fig. 7.



Open Campaigns

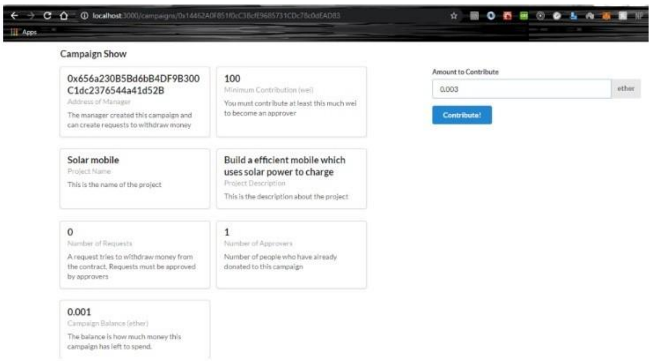
Microscope
To build a microscope with 1000x zooming power
View Campaign

Solar mobile
Build a efficient mobile which uses solar power to charge
View Campaign

Fig -7: List of all the projects

Contribute form contains the form to contribute to a particular project with minimum contribution. If user gives minimum contribution, user is added as a contribute to that project and renders back to home page as shown in Fig. 8.

Request form is created by the project manager to request money to spend. It consists of the description of request, value in ether and address of vendor as shown in Fig. 9.


localhost:3000/campaigns/0x14462A0F851f0cC38cfE9685731CDc78c0dEAD83
Apps
Contribute!

Campaign Show

0x656a230B5Bd6bB4DF9B300C1dc2376544a41d52B
Address of Manager
The manager created this campaign and can create requests to withdraw money

100
Minimum Contribution (wei)
You must contribute at least this much wei to become an approver

Solar mobile
Project Name
This is the name of the project

Build a efficient mobile which uses solar power to charge
Project Description
This is the description about the project

0
Number of Requests
A request tries to withdraw money from the contract. Requests must be approved by approvers

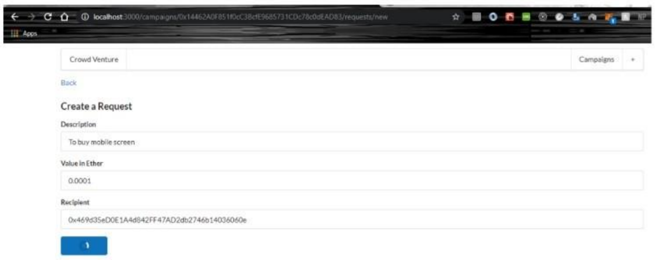
1
Number of Approvers
Number of people who have already donated to this campaign

0.001
Campaign Balance (ether)
The balance is how much money this campaign has left to spend.

Amount to Contribute

0.003 ether

Fig -8 Contribute to the project


localhost:3000/campaigns/0x14462A0F851f0cC38cfE9685731CDc78c0dEAD83/requests/new
Apps
Crowd Venture
Campaigns
+
Back

Create a Request

Description

To buy mobile screen

Value in Ether

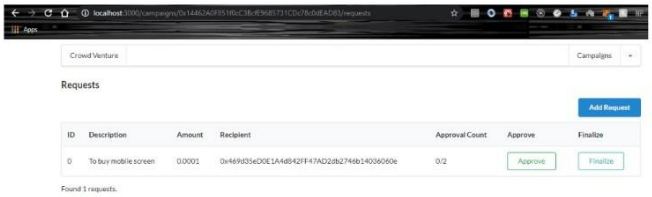
0.0001

Recipient

0x469d35eD0E1A4d842FF47AD2db2746b14036060e

Fig -9 Creating request

This is the list of requests made by the project manager which contains accept button which will increase the number of count as shown in Fig. 10.


localhost:3000/campaigns/0x14462A0F851f0cC38cfE9685731CDc78c0dEAD83/requests
Apps
Crowd Venture
Campaigns
+
Add Request

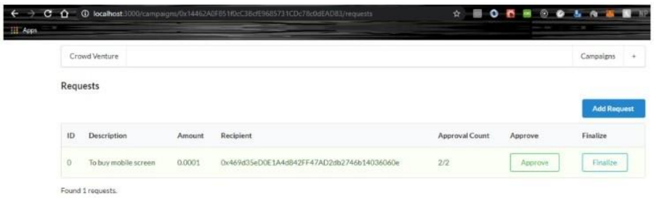
Requests

ID	Description	Amount	Recipient	Approval Count	Approve	Finalize
0	To buy mobile screen	0.0001	0x469d35eD0E1A4d842FF47AD2db2746b14036060e	0/2	Approve	Finalize

Found 1 requests.

Fig -10 List of request and voting system

When the request accepted is more than half, then the request will turn green indicating that the request is accepted by majority of contributors as shown in Fig. 11.


localhost:3000/campaigns/0x14462A0F851f0cC38cfE9685731CDc78c0dEAD83/requests
Apps
Crowd Venture
Campaigns
+
Add Request

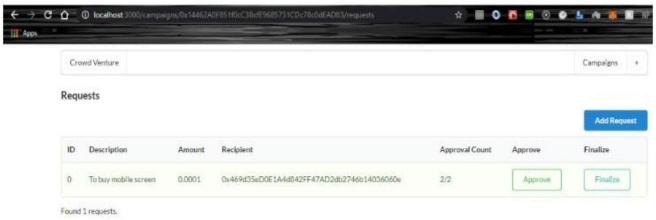
Requests

ID	Description	Amount	Recipient	Approval Count	Approve	Finalize
0	To buy mobile screen	0.0001	0x469d35eD0E1A4d842FF47AD2db2746b14036060e	2/2	Approve	Finalize

Found 1 requests.

Fig -11 Acceptance of request

After accepting by majority of contributors, money can be sent to vendor as shown in Fig. 12.


localhost:3000/campaigns/0x14462A0F851f0cC3BcfE9685731CDc78c0dEAD83/requests
Apps
Crowd Venture
Campaigns
+
Add Request
Approve
Finalize

Requests

ID	Description	Amount	Recipient	Approval Count	Approve	Finalize
0	To buy mobile screen	0.0001	0x469d35eD0E1A4d842FF47AD2db2746b14036060e	2/2	Approve	Finalize

Found 1 requests.

Fig -12 Sending money to vendor

5. CONCLUSION

Finally, it is concluded that the crowdfundingusing blockchain is a relatively new concept to the ICT community. Till now, the solidity code is successfully written for the campaign contract and compiled by using solidity compiler. The output of solidity compiler was bytecode and the interface is deployed into ethereum blockchain by using metamask. After deploying theproject, a decentralized web app is created with a frontend for creating a new project, contributing to a project,creating a new request, approving a request and finalizing a request. At present, the blockchain application in crowdfunding is still in the exploratory stage, where numerous lawful and specialized issues need to be settled.

With the evolution of blockchain, our proposed work has a bright future and a large scope for improvement and evolution. In the future, the proposed research work can progress further in an easier and safer way for all ideas that are achieved through the proposed crowdfunding application.

REFERENCES

[1] https://www.investopedia.com/terms/c/crowdfunding.asp

[2] Prinsha K, "A Study on Crowd Funding and its Implications in India Paripex," Indian Journal Of Research, Vol: 5, 1 January 2016.

[3] Arthur Gervais, Ghassan O. Karame, Karl Wust, Vasileios Glykantzis, ¨ Hubert Ritzdorf, and Srdjan Capkun, "A Study on Crowd Funding and its Implications in India Paripex," In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Association for Computing Machinery, New York, NY, USA, 2016.

[4] https://due.com/blog/a-new-era-of-crowdfunding- blockchain

[5] Bachmann, Alexander Becker, Alexander Buerckner, Daniel Hilker, Michel Kock, Frank Lehmann, Mark Tiburtius, Phillip Funk, Burkhardt, "Online Peer-to-Peer Lending–A Literature," Online Peer-toPeer Lending–A Literature. Journal of Internet Banking and Commerce, 2011.

[6] Zhu, H., Zhou, Z.Z. "Analysis and outlook of applications of blockchain technology to equity crowdfunding in China," Financ Innov, 2016.

[7] Gebert, Michael, "Application of blockchain technology in crowdfunding," New European.

[8] Dhokley, Er Gupta, Saurabh Pawar, Ganesh Shaikh, Abrar, "Crowdsourcing and Crowdfunding Platform using Blockchain and Collective Intelligence," International Journal of Computer Sciences and Engineering, 2016.

[9] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, 2017, pp. 557-564, 2017.

[10] D. Vujiciˇ c, D. Jagodi ´ c and S. Rani ´ c, "Blockchain technology, bit- ´ coin, and Ethereum: A brief overview," 17th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, 2018, pp. 1-6, 2018.