# Crowdsourcing and Crowdfunding Platform using Blockchain and Collective Intelligence

**Er.Waheeda Dhokley[1] , Saurabh Gupta[2] , Ganesh Pawar[3] , Abrar Shaikh[4]**

[1 ,2 ,3,4] Department Of Computer Science,M.H.Saboo Siddik College of Engineering,Mumbai University,Mumbai,India

*Email: waheeda_aamir@yahoo.co.in , saurabhgupta14077041@gmail.com , pawarg124@gmail.com , abrar115052@gmail.com*

*Corresponding Author: saurabhgupta14077041@gmail.com*

***Abstract***- Most of the companies are introducing crowdsourcing and crowdfunding to enrich their engineering capabilities and seek solutions and funds to unsolved technical challenges and the need to adopt newest technologies.Small companies are newly born companies or entrepreneurial ventures which are predominantly based on brilliant idea, innovation and statistical study. One of the preeminent obstacle of Startup's is to seek capital and Human Intelligence to solve complex tasks of the product and in return bolster their project growth. As a result they need a platform which can quench their requirement. This can be achieved by 'Crowdfunding' and 'Crowdsourcing'.

In this paper, we conceptualize a blockchain-based system "CrowdSF" for crowdsourcing and crowdfunding. In which we will try to integrate both platform together where idea creator can recruit the worker to execute the project or seek masses for funding their project at one single platform. A Web-based prototype is implemented on a Ethereum test network along with collective intelligence which will be primarily used in recommendation system of our CrowdSF.

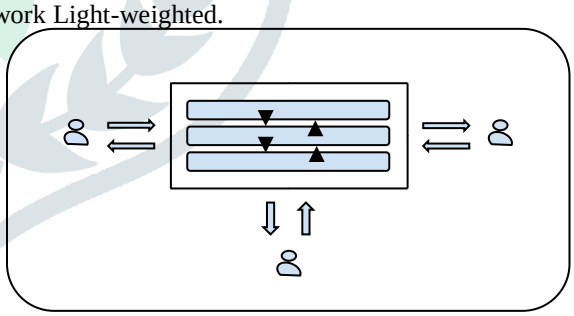
***Keywords***: Blockchain, Collective intelligence, Crowdfunding, Crowdsourcing, Startup.

## 1 INTRODUCTION

Crowdsourcing and Crowdfunding platform have emerged progressively in recent years.This platforms are predominantly based on Centralized System which brings their own inevitable drawbacks. Such systems are subject to weakness for their vulnerability to DDoS attack, remote hijacking and mischief attacks. Consequently a single point of failure will lead to fatal vandalism to the system.With Crowdsourcing platform such as OpenIDEO , INNOCENTIVE and Mechanical Turk has emerged lately.

Our CrowdSF aims at combining the success of those contemporary crowdsourcing platform suppliers with the advantages of current developments in blockchain technology. Our system will uses Ethereum-based smart contracts between Creator and Workers , the system will provide a transparent and straightforward display of the worker's qualifications and diligence for a natural distinction between high and low-quality workers on the basis of their Credit or Reputation score which they will acquire after every task they successfully execute. We will also introduce Backers in the system,which will back the idea of Creator and fund their project by providing them capital. Leading to crowdfunding.

Our application CrowdSF works on 3 main layers, the application layer, blockchain layer and storage layer. Workers with special skills could query and complete tasks which are posted by Creators in the application layer. The blockchain layer uses the task state changes as input to achieve consensus between workers and creators. Because of the limited data storage capacity in blockchain, We are using MongoDB database as a storage layer. System will encrypt the data and generate a hash key of the hash key data. Hash data will be stored in MongoDB while the hashkey will be stored in Blockchain. This will make the Blockchain network Light-weighted.



In this paper, we are proposing to create a platform including both domain ie. crowdsourcing and crowdfunding integrated together where idea creator can recruit the worker to execute the project or seek masses for funding their project with security. The remainder of the paper is organized as follows. In section 2, we present the Objective. Architecture of the system is given in section 3. In section 4, Working and results are explained. Later, we present a concrete analysis of the security properties in section 5. Finally Conclusion and References are included in this paper.

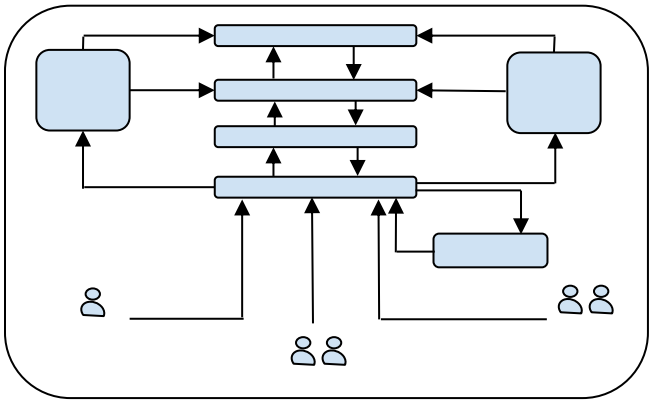
## 2 OBJECTIVE

- Build a single platform for Crowdsourcing and Crowdfunding domain.
- Solution should entrust on distributed blockchain framework which will safeguard against problems faced by centralized servers.
- Adopt such mechanism to address the quality of workers and counter the false-reporting and fraud committed by workers.
- To keep User-Interface of website as simple as possible.
- Data of the users should be Encrypted to assure the users privacy.
- Design a solution which is monitored by system to ensure the obliteration of fraud spendings in Crowdfunding.
- The System should require Creator's and worker's related Data from Crowd member and client.
- The System should have Creator related tabs on its profile that contains task description, task management, task submissions, task selections and inquiries.
- The System should not require a potential Backer or Crowd-member to open an account in order to see the information provided by it and the Creator.
- But, The System must require potential backer to open an account prior to being able to engage in that communication or make a commitment to pledge and must obtain consent for electronic delivery.
- The System shall provide an electronic notice of commitment to the backer which includes the amount pledged; the price of the security bought, if known; the name of the Creator; and the date and time at which the Backer will be free from any restrictions on the resale of the investment.
- The user interface of website to follow 8 golden rules of user interface design
- The user interfaces are kept as simple as possible so that they are completely user friendly.
- The website would be hosted on internet with co.in domain hence it is platform independent as well as browser independent.
- The website should also provide download option to the users to save the result in local/personal computer.
- Feedback of user is assumed to be trustworthy.
- The System shall contain crowd-member specific tabs on the crowd member profile, i.e., where the crowd member can view details of tasks, search for tasks, upload requirements specifications, and update account information and inquiries.
- Any change requested in processing through feedback would be judged on the basis of number of requests through feedback.
- The System shall ensure and maintain a high-level of integrity among users
- The System shall address any form of abuse or breach of legal conditions
- The System shall maintain high Quality of Service.
- The System shall be usable on all browser and operating system platforms.
- The System shall be efficient in error handling and prevent loss of data
- The System shall be readily available for usage.

## 3 CROWDSF ARCHITECTURE

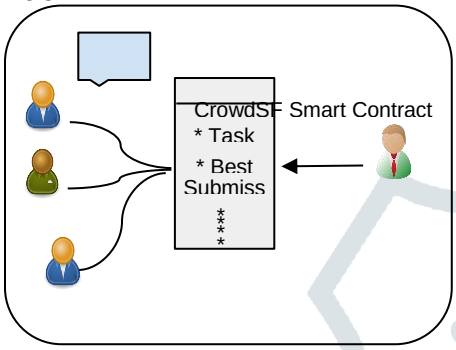
CrowdSF architecture is divided into three layers: Application Layer, Blockchain Layer and Storage Layer . A React based Webapp will be operating on Application Layer. All the data of Creator's idea or profile of Worker's can be viewed on this layer. Ethereum Based Blockchain will be used in blockchain layer . The blockchain layer uses the task state changes as input to achieve consensus among Workers and Creator and Backer.

As there exist lots of data collected from Creator and workers, because of the limited data storage capacity in blockchain. We will store all data in the MongoDB and its encrypted Hash key in Blockchain. We believe this separation can improve CrowdSF's data storage significantly and make blockchain network light-weighted.



### 3.1 Smart Contract

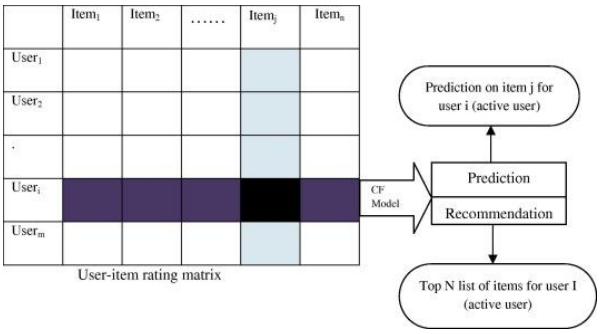
Traditional crowdsourcing systems focus on detecting cheating or malicious behaviors after workers have submitted results. In contrast, CrowdSF selects trustworthy workers based on reputation and reliability value in smart contract, which can effectively improve the quality of results. In order to achieve this goal,we combine expertise-aware with reputation to choose workers




A smart contract is a computer code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other. If the predefined rules are met successfully, the agreement is automatically enforced and accepted. The smart contract code then facilitates, verifies, and invoke the negotiation or performance of an agreement or transaction. It is the simplest form of decentralized automation.
It is a mechanism involving digital assets and two or more parties, where some or all of the parties deposit assets into the smart contract and the assets automatically get reorganize among those parties according to a algorithm based on certain data, which is not known at the time of contract invokes.

### 3.2 Recommendation System

Collaborative filtering is a domain-independent prediction technique for content that cannot easily and appropriately be described by metadata such as movies and music. This technique works by constructing a database (user-item matrix) of preferences for items by users. It then matches users with relevant interest and preferences by calculating similarities between their profiles to make recommendations. Such users build a group called neighborhood. An user gets recommendations to those items that he has not rated before but that were already positively rated by users in his neighborhood. Recommendations that are produced by Collaborative Filtering can be of either prediction or recommendation. Prediction is generally a numerical value, Rij, conveying the predicted score of item j for the user i, while Recommendation is a list of top N items that the user will prefer the most . This technique of CF can be divided into two categories: memory-based and model-based.




### 3.3 Prerequisites

Ganache - Provides personal Ethereum blockchain network.
Metamask - Brings Ethereum to your browser.
Truffle - A framework for Ethereum development.
Solidity - It is an object-oriented, high-level language for implementing smart contracts.
Web3js - web3.js is a collection of libraries which allow you to interact with a local or remote Ethereum node, using an HTTP, WebSocket or IPC connection.

## 4 WORKING AND RESULTS

In the context of the blockchain solutions, the introduction of smart contracts has made the technology far more ubiquitous than simply underwriting Bitcoin and the other cryptocurrencies. Bitcoin, after all, only facilitates cryptocurrency payments in a decentralized peer-to-peer (P2P) network. The network isn't built for other uses.

Nonetheless, when the Ethereum project popularized its smart contracts, they implemented a way to automatically execute legal-like functions in any blockchain based solution. For example, a smart contract can transfer cryptocurrency from one account to another automatically based on certain scenarios that are programmed in the contract.

This introduction of Ethereum smart contract on a blockchain has helped blockchain entrepreneurs and developers to create innovative DApps ie. Decentralized App. They have created new business models using decentralization and the security enhancements that blockchain technology offers. These have the potent to disrupt centralized providers.

We created 3 Sol Contracts :

- CAMPAIGN
- CAMPAIGN FACTORY

- MIGRATION

Code a simple smart contract and save it in a file after noting down the filename. The final node of your file name will need to ".sol". You now need to compile your code into an application binary interface (ABI) and bytecode (bin) for deploying onto the blockchain.
In general, an ABI is the interface between two program modules, one of which is often at the level of machine code. This interface is the de facto method for encoding or decoding data into or out of the machine code.

**4.1 Deploying Contract:**

**Install npm :** $ sudo apt-get update
$ sudo apt-get install nodejs
$ sudo apt-get install npm
**Install Truffle And Ganache-cli :**
$ sudo npm install -g ganache-cli truffle

Ganache CLI will automatically create 10 accounts associated with 10 private keys for testing purpose.As directly testing on main ethereum network will be too expensive. Each account has 100 ethers for testing purpose.

**4.2 Gas Limit**

The important thing to note are hash which is the hash value of the transaction number for this deployment. Block number is the block where the transaction or smart contract is written on.to deploy a contract we need gas price; in this case it is 1 ether. Gas price is the general cost of gas we were willing to pay for. The input field is the hash or signature value of the actual data content of the smart contract.

The maximum amount of units of gas you are willing to spend on a transaction is our gas limit. This avoids situations where there is an error somewhere in a contract, and you end up spending 1 ETH, then 10 ETH, and then 1000 ETH, going in circles but arriving nowhere. The unit of gas that we required for a transaction are already defined by how much code is executed on the blockchain. The amount of gas to be used should be ample enough to cover the computational resources you use or your transaction will fail due to an 'Out of Gas' error.

All unused gas should always remain in wallet. So if you go to any MyEtherWallet, send for example 1 ETH to our donation address, and than use a gas limit of 400000, you will receive 400000 - 21000* = 379000 back. But if you were sending 1 ETH to any contract, and your transaction to the contract fails to accomplish (say, the Token Creation Period is already over), you will use the entire 400000 and receive nothing back.

*21000 is the current standard gas limit for simple transactions.

**4.3 Overview of Contracts**

Every User with an Idea will use this contract to upload it on the blockchain network. There are two Primary Contracts: Campaign Factory and Campaign.

**Campaign Factory** : This will store all the Campaign created by the Single Users.
**Campaign** : In this , new Campaign will be created by the User for new Ideas. The User will decide beforehand what he seeks from the Idea. whether it is Monetary Fund or workPower from the Crowd or workers. User will than add the following fields:

- Title of Campaign
- Description of Campaign
- Minimum Contribution
- Total Contribution
- Images for Campaign
- Videos/Assests for campaign

**4.4 Backing the Project**

- This campaigns crowdfunding is 'All or Nothing' i.e creator should get all his required funding within specific time interval of 1 month(max). If he fails then all the funding will be return backers. After successful funding creator can start working on his campaign.
- For avoiding fraud spending, Creator has to send a request to all backers for using the money funded to the campaign. All the backers then approve or reject the creator's request. To approve the request the half of backers should say 'yes'. If not then request will be rejected.
- The approve requested ethers or Rewards will then directly deposited to the workers accounts, to make system more transparent and trustworthy.
- The minimum amount a single backer can contribute will be mentioned in detail section.
- The address of the backer will be added in detail section and the count of backer will be updated.
- This detail of successful contributed backer will be used in future for prevention against fraud spending.

## 5 SECURITY ANALYSIS

As the saying goes,'The best defense is a good offense' and its nowhere more true than in enterprise security. Finding vulnerabilities and loopholes before hackers do can prevent devastating penetration, data loss, and prevent crippling hits to your operations and your reputation.The security of CrowdSF comprehends with the security of blockchain. In our System Creator ,Backer and workers all can take part in mining, we assume that the attacker (including malicious requesters, backer, workers and miners) cannot break the fundamental defense of blockchain,ie because the attacker will not have the majority of power or resource to supervise the blockchain network and the mostly the bulk of miners are honest. The network has less latency and messages are synchronous between reliable miners. For Security, the system will require 10 minutes for each block to be successfully uploaded to the network. Each Miner will compete among themselve to upload their block on the network and earn rewards in return.

Comparing with the traditional crowdsourcing system in which money is rewarded or exchange, here we use virtual coins in blockchain. Coins can be obtained either by mining or transferring it with others. We will assume that each particular user who has the secret key can securely acquire and transfer it with the client wallet. The data will be encrypted in order to prevent the users privacy from being exploited. The solution will be encrypted by leveraging a secure public key encryption algorithm. Workers will than use the corresponding requester's public key which will be available online to encrypt the solutions. Creator could decrypt the solutions successfully by the secret key. Specifically, the solutions are saved as cipher text in distributed database.

The potential malicious Creator and workers have specifically different goals to maximize their own profits. Security against malicious workers is straightforward, the only ways that malicious workers can cheat are: (i) submitting more than one answers in Answer Collection phase; (ii) sending the contract a fake instruction in the name of requester in Reward phase; (iii) altering the policy specified in the contract. The first threat is simply handled by the common-prefix-linkability and unforgeability of common prefix linkable anonymous authentication. The second there at can be approached by predicting others' answers, and it is prevented due to the semantical security of public key encryption.The third threat is simply handled by the security of digital signatures. The last issue is trivial, because the blockchain security ensures the announced policy is immutable.

Malicious Creator aims to collect useful solutions without losing the deposit, which is false-reporting attack in essential. To accomplish this goal, such creators misreport the evaluation solution as below par standard even if workers contribute high-quality of solution.Furthermore, they may even contradict that they have obtained the solutions. Besides, we require requesters make a deposit in our protocol, while they may benefit from not following or even breaking the protocol, which means that malicious requesters may attempt to generate a fork chain after they acquire the solutions initially.

In Crowdfunding, there can be a scenario where the people had funded and backed the project but the creator is unable to produce or execute his/her project or campaign. This may lead to a scam of fraud Spending of the fund alotted to them.For curbing such exploits, Creator has to submit or update their work detail on time to time basis. Backers which had funded to that particular campaign will get notification of the work. While spending the fund, Creator will have to take approval of spending from the backers. If more than certain default percentage of Backers responds with 'Yes' vote , than the creator will have the authority to use the fund alotted to them. This process will help in curbing the scam of Fraud spending.

## 6 CONCLUSION

Crowdfunding and Crowdsourcing in India are still in its infancy. However, it does face its share of challenges. Being an extremely new concept, the Indian population still has not widely accepted online crowdfunding or crowdsourcing. The initial hesitancy though, should be expected and would not prove to be a major obstacle given its due time.Despite the initial challenges, the future of crowdfunding and crowdsourcing in India is undoubtedly bright. Most of the skepticism regarding online crowdfunding would subside gradually. India's vast population means that India potentially has a huge donor base and workforce, the likes of which is unparalleled to other countries.

The primary requirements of any business are business capital and human resources.This is especially true in the cases of startup ventures and low level companies as these usually struggle with gathering resources. Hence our platform would be ideal for such companies our startup to accomplish their needs.

As centralization of system provides several benefits with respect to maintenance and updation of the system and its data, it eventually falters when it comes to the security issues. Hence use of blockchain in architecture will strengthen security aspect of the system. The scope of such platforms in India is bright but only if we actively participate.With the arrival of crowdfunding & online crowdsourcing, we finally have the chance to help budding companies flourish . We know that Minute drops of water over time, constitute an entire ocean. We may not have millions to spare, but if all of us pitch in, support whatever small amount we can, we would raise enough to make a difference.

## 8 REFERENCE


[1]Ming Li and Jian Weng and Anjia Yang and Wei Lu, "CrowdBC: A Blockchain-based Decentralized Framework for Crowdsourcing "https://allquantor.at/blockchainbib/pdf/li2017crowdbc.pdf

[2 ]Giones, F. & Oo, P., 2017. "How Crowdsourcing and Crowdfunding are redefining innovation management". In A. Brem & E. Viardot, eds. Revolution of Innovation Management. London:Palgrave Macmillan UK. http://link.springer.com/chapter/10.1057/978-1-137-57475-6_3

[3]Jackie Zimmermann , "Rewards-Based Crowdfunding: What It Is, When It Works" ,*Updated Dec. 6, 2017.* https://www.nerdwallet.com/blog/small-business/reward-crowdfunding/

[4]Ordanini, A.; Miceli, L.; Pizzetti, M.; Parasuraman, A. (2011). "Crowd-funding: Transforming customers into investors through innovative service platforms". *Journal of Service Management*. **22** (4): 443. doi:10.1108/09564231111155079. (also available as Scribd document)

[5]Ajay Agrawal,Christian Catalini, Avi Goldfarb , "Some simple economics of Crowdfunding",working paper 19133,June 2013 JEL No. D47,D82,G21,G24,L26,L86,R12,Z11 http://www.nber.org/papers/w19133.pdf

[6] Mary Thibodeau, Operations Manager at TruDex.io (2017-present) "How can blockchain be used in crowdsourcing?"https://www.quora.com/How-can-blockchain-be-used-in-crowdsourcing

[7]oon seok Lee, Mingxuan Sun, Guy Lebanon, "A Comparative Study of Collaborative Filtering Algorithms"https://arxiv.org/pdf/1205.3193.pdf , arXiv:1205.3193v1 [CS.IR} 14th may 2012

[8] S. Debnath, N. Ganguly, and P. Mitra. Feature weighting in content based recommendation system using social network analysis. In Proceedings of the 17th international conference on World Wide Web, pages 1041–1042, 2008.

[9] Schenk, Eric; Guittard, Claude (January 1, 2009). "Crowdsourcing What can be Outsourced to the Crowd and Why". Retrieved October 1, 2018.


## Authors Profile

Mrs.Waheeda Adam Dhokley. Works as an Assistant Professor at M.H. Saboo Siddik College of Engineering in Computer Engineering Department Qualifications:- B. E. (Comp.) M. E. (Comp.). Also, having a teaching experience of more than 12 years in this institute.

Mr. Saurabh Gupta Currently pursuing Computer Engineering from M.H. Saboo Siddik College of Engineering and belongs to Computer Engineering Department.

Mr. Ganesh Pawar Currently pursuing Computer Engineering from M.H. Saboo Siddik College of Engineering and belongs to Computer Engineering Department.

Mr. Abrar Shaikh Currently pursuing Computer Engineering from M.H. Saboo Siddik College of Engineering and belongs to Computer Engineering Department.