



Implementation of Crowdfunding for Smart Contract Application Using Blockchain Technology

Kangana W.M.¹, Namita Chougule², Sejal Patil³, Soumya Kadadi⁴, Vrunda Kadam⁵

Assistant Professor, Dept. of Computer Science Engineering, S.G Balekundri Institute of Technology Belagavi,
Karnataka, India¹

Students, Dept. of Computer Science Engineering, S.G Balekundri Institute of Technology Belagavi,
Karnataka, India²³⁴⁵

ABSTRACT: Crowdfunding is an online money-raising strategy that began as a way for the public to donate small amounts of money to help innovative people finance their projects. This project is to propose smart contract for crowdfunding using blockchain technology. Through this, we can provide a safe, secure and transparent way for crowdfunding. The work of this project is to provide interactive forms for campaign creation, contribution of money, viewing of campaigns, request approval and finalizing requests through which both campaign creators and contributors can easily create and fund the campaigns. The contributor can be able to track the money that they sent. The Blockchain will record all the transaction and store as a block. An appealing feature of blockchain technology is smart contracts. A smart contract is executable code that runs on top of the blockchain to facilitate, execute and enforce an agreement between untrusted parties without the involvement of a trusted third party.

KEYWORDS: Blockchain, Crowdfunding, Smart Contracts

I. INTRODUCTION

The blockchain is an incorruptible digital ledger that records every transaction. It is a distributed system thus all the records are stored in every node in the decentralized network. Ethereum allows running applications in the blockchain called Smart Contracts. All the Smart contracts are run on the Ethereum Virtual Machine. Crowdfunding provides an easy way to find cash for innovative project ideas. The problem with the current crowdfunding companies charging high fees and sometimes there were scams happened. Implementing a crowdfunding strategy in blockchain will help to avoid these types of problems. By incorporating Peer to Peer smart contract for crowdfunding remove the traditional transaction fees and platforms fees normally associated with other crowdfunding platforms, such as Kickstarter. The objective of our project is to create a reliable application so that every new idea gets life. We have designed a crowdfunding site which is a blockchain based website. We provide an easy to use interface for everyone to create and post their ideas on this application. These ideas then become public to everyone. Anyone who wishes to support their ideas can contribute. All these processes are done in an interactive manner.

II. RELATED WORK

Blockchain is fairly new technology, there are only few studies and researches available on the internet. Blockchain can be defined as a distributed database of records of all transactions that have been executed and shared among participated parties. The characteristics of blockchain includes decentralization of data, persistency, anonymity and auditability. There are two main components in blockchain system, which are transaction and block. Transaction represents the action triggered by the participant, while the block is a collection of data recording the transaction and other associated details such as the correct sequence, timestamp of creation, etc. The transaction records, or blocks, in a blockchain are linked together cryptographically, rendering them tamper proof. This means that each block that have been inserted cannot be modified or deleted. To achieve reliability, blockchain uses consensus algorithms.

The research uses a systematic literature review method. Literature review gives a good foundation for research in information systems and strengthens information system as a field. A review of literature of smart contract applications strengthens the field of blockchain within information systems. We conduct the review in four phases. Phase 1 is the review of the purpose and protocol of the study. Phase 2, involves searching the literature and practical screening. In phase 3, the quality appraisal and data extraction are presented. In phase 4, we analyze the findings. This literature



review method is chosen because it is developed specifically for information systems research. The remaining part of this section is structured as follows:

- Planning Phase

In the first phase, we design a review protocol as this is an essential element in conducting a systematic literature review study. Review protocol minimizes biases in a detailed plan. We discuss the purpose of the review and design a protocol, a searching plan, selection criteria, data extraction method, data analyses and present the review results.

- Selection Phase

In the second phase of the review, we search for academic articles using Google scholar database. Since smart contract is a new technology in information systems, we search for journal papers, conference papers and select white papers from 2013 – 2018. The time frame was chosen considering that smart contract is a new technology in the field of information systems. This time frame helps us to get the required articles from the search engine. In the search for articles, the keywords and Boolean operators used are as follows: smart contract + business, smart contract + organization, smart contract + enterprise, blockchain + business, blockchain + organization, blockchain + enterprise, distributed autonomous organization + business, decentralized autonomous organization + enterprise. These pairs were used independently in every search. From the results of these searches, we conducted an efficient screening process, discarding articles not relevant to the study, duplicates, and articles that we could not obtain the full text. Further screening was done practically that involved reading the articles

- Exclusion and Inclusion criteria

In the first step of article selection, the exclusion criteria include the following: Articles that are not relevant to the study, articles that a full paper couldn't be downloaded or accessed, articles not published between 2013 and 2018 and articles not related to blockchain technology or smart contracts. In the second step, the inclusion criteria included high-quality white papers, journal papers, peer-reviewed conference papers, articles on smart contract applications in an organization.

- Execution phase

In the third phase of the review, we extract data from eligible articles based on the research questions guiding this research and collect information from articles to serve as raw material for the analysis. In the fourth phase of the review, we extract and combine essential facts using qualitative techniques. Data analysis is followed by the literature review study report.

Features of Crowdfunding

Within the domain of little related literature there have been attempts by some to identify the features and limitations of Crowdfunding. Crowdfunding is said to disrupt traditional funding cycle by merging the social web with entrepreneurial finance, as well as being a validation tools for products or services. De Buysere et al. (2012) suggested a number of benefits that project owners gain with Crowdfunding:

- Raising capital.
- Gaining valuable feedback before releasing the product or service to the market.
- Understanding if the proposed idea has a mass appeal and getting a "Proof of concept".
- Building early connections with customers.
- Support Marketing for the product or service.

In the same time, funders gain a number of benefits as well:

- Social return as they see the project, they have supported realized
- Material return by getting a reward (Donation-based model)
- Financial return if they invested in the project (CFI model)

III. METHODOLOGY

The project is a web application which is basically an enhancement of the existing crowd funding systems. In normal Crowdfunding's there is no security ensured for contribution amount. So, smart contract of Ethereum platform which is an application of blockchain can be used in order to solve this issue. Blockchain is a decentralized distributed ledger system that accesses, verifies, and transmits network data through distributed nodes. An Ethereum based smart contract is a cryptographic box which stores information, processes inputs, writes outputs and is only accessible to the outside if certain predefined conditions are met and the contracts in Ethereum are written in special language called solidity. In practice, Ethereum allows for an easy implementation of such smart contracts and in addition Ethereum offers developers online compilers of solidity code. Smart contract is written in such a way that the entire amount funded by the contributors will safely be kept in smart contracts so that no one can modify it or steal it. The amount will not be directly given to campaign creator rather it will be held in smart contract itself. If the campaign creator wants to use this amount, he/she has to create a spending request. Then the approvers (people who have contributed to the campaign) should approve the request created by the campaign creator. If the request gets majority no of approvals/votes as shown in then the amount can be sent to the vendor specified by the campaign creator. The voting system used is decentralized



as blockchain technology is used in implementing it. This makes the voting system more secure and also cost efficient while guaranteeing the voters privacy. Campaign creator will be able to finalize the payment once the required votes are obtained. In this the security is increased and also the peoples/contributor’s opinion is taken.

In the existing system, the problem is that the companies charge heavily to both the donor and the user. There is no track of the records of the money, transparency, communication between the investor and the user is developing the project. The trust is the main problem when it comes to the crowdfunding with the existing companies. None of these companies provide the donor guarantee policy.

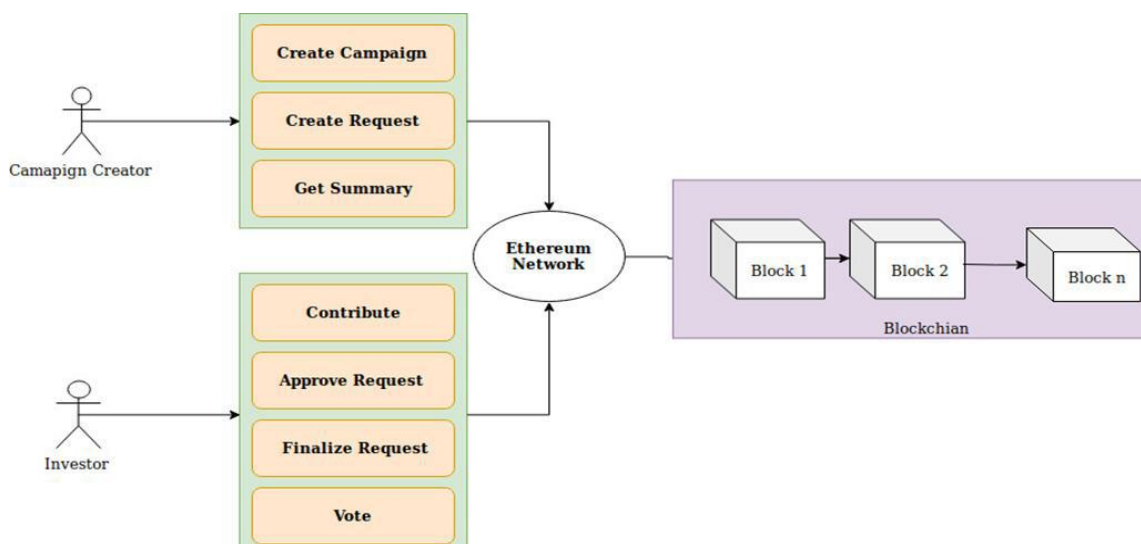
- Not Transparent
- High Charges
- Donor guarantee policy not available
- No track of Records

In the proposed system, the campaign creators will post their project ideas in the campaign and the interested people will donate the fund to the project idea. Where it differs from the old crowdfunding is that all the money is now digital currencies like ether. All ether coin will be recorded and keep tracks in the blockchain. Where the blockchain is an immutable ledger. The Donor has control over the funded money. With the Request approval module, the donor has full control over the money they invested. Only if one by two of the investors need to approve the request made by the creators. By giving control on invested money the Trust is built.

- Trust
- Control over money
- No charges
- Donor Guarantee Policy
- All transactions are recorded
- Money is Stored Securely.

• *Overview*

Both Crowdfunding and Cryptocurrency is a trend on the Internet and they match perfectly. Blockchain technology is one solution that can be used to reduce the problems that occur in crowdfunding. The contract is written in a way that all money will be added to the pool. When the request meets the specified condition then all the money will be transferred to the recipient. Ethereum is an open-source, public, blockchain based distributed platform and operating to featuring smart contract functionality. It is the modified version of Bitcoin via transaction-based state transitions. Ether is a cryptocurrency which is generated and used by the Ethereum platform. Ethereum provides a decentralized operating, the Ethereum Virtual Machine (EVM), which can execute an application on the public nodes.



• *Blockchain*

The blockchain is originally originated from the Bitcoin, invented by unknown people. The Blockchain is a list of continuously growing records called blocks. Each Block is linked to each other and they were secured using cryptography. Blockchain has the characteristics of integrity, decentralization, Immutability, Security, Anonymity. Blockchains can be divided into three types: 1) public blockchain (Bitcoin and Ethereum); 2) consortium blockchain (Hyperledger and Ripple) and 3) private blockchain.



- *Peer to Peer*

The very important part of how blockchain works are based on Peer to Peer (P2P) system. The whole blockchain is connected to all the node in the network. This means information stored on blockchain cannot be lost or destroyed, to do so have to destroy every single node on the network and that is impossible.

- *Consensus Protocol*

Consensus protocol is the most important one in the blockchain technology. The Blockchain consensus protocol is what which keeps the blocks on all the node to synchronize with each other. The term 'Consensus' means that the nodes have to agree with the same state of the blockchain. Consensus protocol allows blockchain to be updated every minute (depends on the network) and ensures that every block in the chain is true. The aim of the consensus protocol is to guarantee a single chain is used and followed by all the nodes.

IV. PROPOSED ALGORITHM

Step 1: Create Metamask account.

1.1: Then create an Ethereum account on Rinkeby Test Network.

Step 2: Create Smart Contract.

2.1: Create Campaign Contract.

2.2: Create Factory Contract.

Step 3: Deploy Campaign Factory contract. (It creates instances of Campaign Contract)

Step 4: Deploy Campaign contract.

Step 5: Start the server by running the command “npm run dev” in terminal.

Step 6: Open localhost:3000 in browser:

Main page will be loaded which shows the list of all campaigns created so far.

Step 7: Create a campaign (By clicking Create Button) by entering minimum contribution in wei.

Step 8: View a particular campaign detail:

The view campaign page shows:

- Address of Manager who created the campaign.
- Minimum contribution.
- Number of requests.
- Number of approvers.
- Campaign balance.

Step 9: Contribute to the campaign to become approver.

Step 10: Manager creates the spending request to spend the campaign money.

The request is created by providing:

- Description about the request.
- Amount to be spent on that request.
- Address of the recipient.

Step 11: Request are approved by the approvers.

```
if (approvalCount > (approversCount/2))
```

```
{
```

```
    Then request is approved.
```

```
}
```

```
else
```

```
{
```

```
    Request is not approved.
```

```
}
```

Step 12: Manager will finalize the request if it is been approved and the requested amount will be sent to the recipient.

V. IMPLEMENTATION

In order to implement and run the project there are some software requirements that need to be installed and configured as mentioned below:

- Metamask wallet:

Metamask allows to run Ethereum decentralized applications in the browser itself without running a full Ethereum node and it is a self-hosted wallet to store, send, and receive Ethereum or ERC20 tokens. It allows to create n number of accounts which are just like bank accounts. Metamask wallet has to be installed from the chrome browser and network has to be set to Rinkeby test network which is available in options at top of the wallet. Then in order to test



and run the project some fake Ethereum(currency) is transferred from Rinkeby faucet to the account being used in the project by giving its address.

• Infura key:

This key can be obtained from the infura.io website which is specific to the Rinkeby test network so that an Ethereum environment can be established.

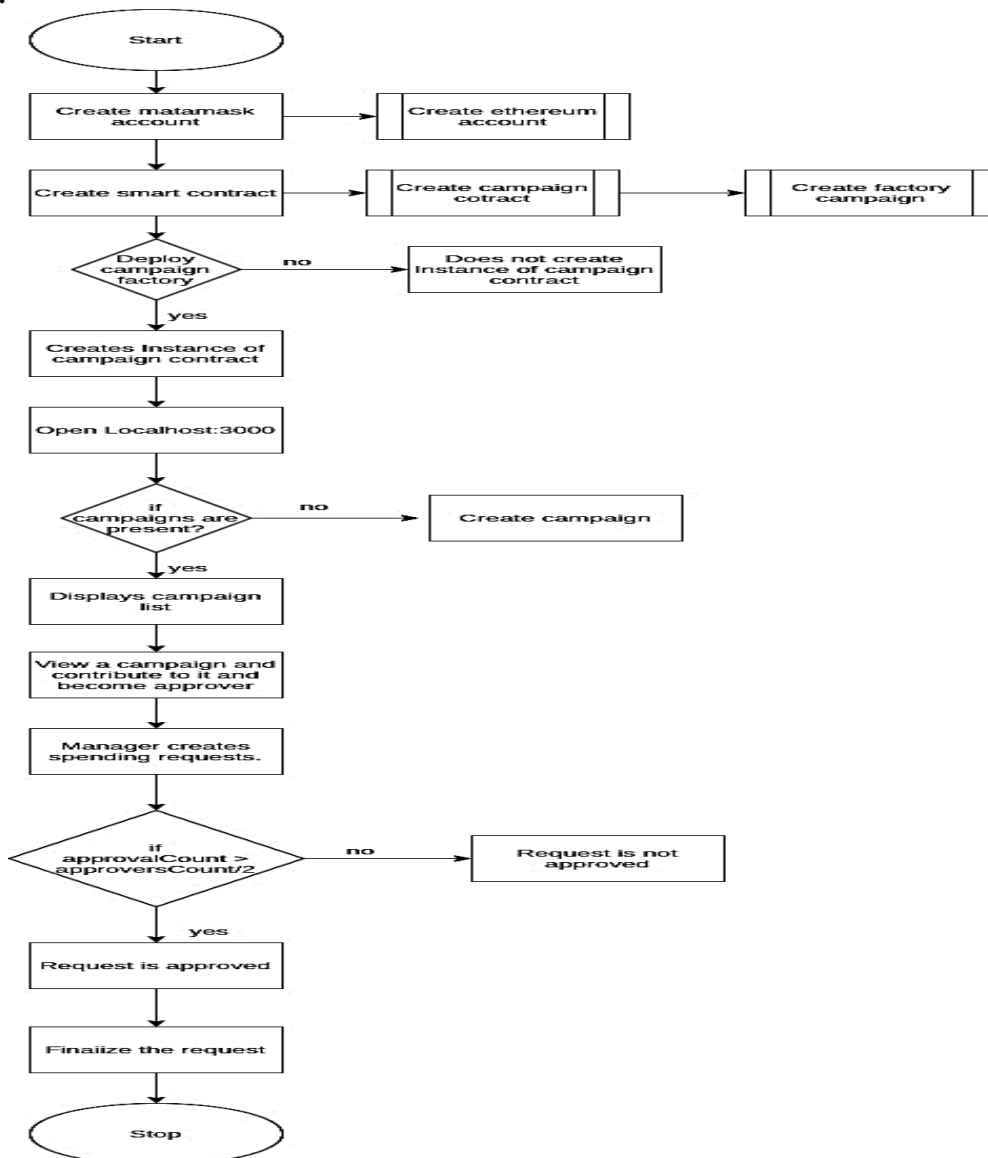
• Atom:

It is a free and open-source source code editor. First tests have to be performed on the smart contract in remix solidity. After that a folder has to be created in the directory which can have any name for ex: kickstart. Then, the contract tested in remix solidity is taken and stored in folder which was created in the beginning. Then before performing any further activities dependencies mentioned in have to be installed by just typing this command in terminal inside the folder kickstart npm install—save dependency name.

• Ethereum

Ethereum is an open-source, public, blockchain based distributed platform and operating to featuring smart contract functionality. It is the modified version of Bitcoin via transaction-based state transitions. Ether is a cryptocurrency which is generated and used by the Ethereum platform. Ethereum provides a decentralized operating, the Ethereum Virtual Machine (EVM), which can execute an application on the public nodes.

System flow:



Flowchart of the project



Modules:

When the web application is started the first page that is seen is campaign page where existing campaigns are displayed and a new campaign can also be created as shown in Fig. 5.1. All these operations can be performed provided that Metamask is installed in the browser.



Fig. 5.1: View of campaigns webpage

When create campaign is clicked it will redirect us to the page where a transaction needs to be performed in order to create a new campaign as shown in Fig. 5.2.



Fig. 5.2: Campaigns creation webpage

When view campaigns button is pressed which is present in first web page it will be redirected to this page which consists of campaigns details like address of person who created the campaign (Manager), minimum contribution, number of requests created by manager, number of approvers and campaign balance as. Investors can contribute to the campaign and become an approver. Fig. 5.3 below represents the campaigns show webpage.



Fig. 5.3: Campaigns show webpage

When contribute button is pressed after entering the contribution in ether you become an approver to the campaign.

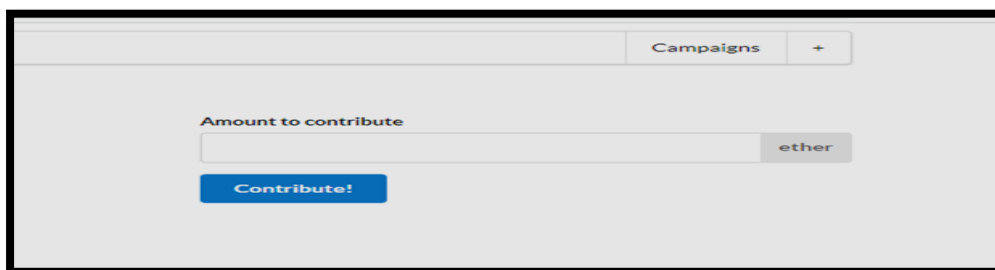


Fig. 5.4: Campaign contribution webpage



When view requests button is pressed it will be redirected to the view requests page as shown in Fig. 5.5. It consists of all the requests created by the manager. It also consists of approve and finalize button. Approve buttons used by approvers to vote and Finalize button is used by manager to finalize the payment once the request gets enough number of votes.



Fig. 5.5: View request webpage

When add request button is pressed it will be redirected to create request web page as shown in Fig. 5.6 where a request can be created by specifying description of spending request, value in ether that you want to spend and address of recipient to whom manager wants to send money (vendor address).



Fig. 5.6: Create a request webpage

After approving the request if the request gets enough approvals/ majority votes then the request turns green indicating that it can be finalized by manager as shown in Fig. 5.7. It also consists of add request button which is used to create a spending request and this can be only done by the manager (person who created campaign).



Fig. 5.7: View request webpage

After finalizing the request, the amount goes to the vendor address that was specified and the whole request turns grey as shown in Fig.5.8 indicating that the request has been closed. The money/currency in the wallet is checked before and after finalizing the request in order to ensure that the transaction executed successfully.



Fig. 5.8: After finalizing request



VI. RESULTS

In Crowd Funding using blockchain to raise money for a startup first a campaign has to be created and a unique 64 character public key is assigned to that particular campaign to which investors can use as an address to donate. Investors can contribute the money in the form of ether. The contributed money will remain in the smart contract itself and will not be directly given to the campaign creator. If the campaign creator wants to spend the money he/she has to make a spending request which will consist of the amount of the ether needed and also the address or the public key of vendor to whom the ether should be sent so that campaign creator can get the required material which ensures that the contributed ether is always securely kept inside the smart contract and contributors have to vote to spending request created. If the percentage of the votes is at least 51 % then the amount will automatically be transferred to the vendor. This method of Crowd Funding is lot more faster and secure as compared to the existing system. In current system the contributed amount is in the direct hands of the campaign creator and he/she can run away with that money, the time taken to transfer of the money raised to the campaign creator or the startup is slow and also there is fee that will be cut from the contributed amount as a third party like Kickstarter is involved or used in raising the required capital. Hence, the Crowd Funding using blockchain is more revolutionary and efficient method for raising capital for the startups .

VII. CONCLUSION AND FUTURE WORK

Implementation of blockchain technology to crowdfunding platform provide more transparent transactions. As a result, users can feel more confident when they want to donate to a campaign. The application of smart contract on spending request also can help contributors to know how their money are being spent.

The purpose of a smart contract based solution is to enable secure way of crowd funding by ensuring that the money donated by the investors is safe and also each and every step taken in the startup with help of donated money involves investor's opinion i.e. whenever the campaign creator wants to spend the money he/she has to make a spending request where the purpose of using the money, to whom the money is being sent (vendor) and the amount needed should be mentioned. The main advantage of using the smart contract is the concept of blockchain that it is resilient against many threats. Also, it provides many features like improved reliability, faster and efficient operation. Web Application has been computed successfully and was also tested by taking "test cases". It is user friendly, and has required options, which can be utilized by user to perform the desired operation. The goals achieved by the website are:

- creating a campaign
- Contributing to campaign
- Creating a spending request
- Approving the spending request
- Finalizing the request

REFERENCES

- [1].Maher Alharby, Aad van Morse," Blockchain based smart contracts:A systemetic mapping study", School of Computing Science, Newcastle University, Newcastle, UK,2017.
- [2].Md.Nazmus Saadat, Syed Abdul Halim, Rasheed Mohammad Nassr," Blockchain based crowdfunding systems in Malaysia Perspective", 2019.
- [3].Chibuzor Udokwu, Alexandr Kormiltsyn, Kondwani Thangalimodzi and Alex Norta, "An Exploration of Blockchain enabled Smart-Contracts Application in the Enterprise", 2018.
- [4].Rafat M. Abushaban," Crowdfunding as a Catapult for Innovation in the Middle East: Obstacles and Possibilities", Global Humanitarian Technology Conference, IEEE, 2014.
- [5].S. Benila, V. Ajay , K. Hrishikesh, R. Karthick , "Crowd Funding using Blockchain", GRD Journals- Global Research and Development Journal for Engineering , Volume 4 , Issue 4 , ISSN: 2455-5703, March 2019.
- [6].Agata Stasik, Ewa Wilczyńska," How do we study crowdfunding? An overview of methods and introduction to new research agenda",2017.
- [7].Hiroki Watanabe, Jay Kishigami "Blockchain contract: A complete consensus using blockchain", DOI: 10.1109/GCCE.2015.7398721, October 2015.
- [8].He Zhu, Changcheng Huang, and Jiayu Zhou. "Edge Chain: blockchain-based multi-vendor mobile edge application placement", 4th IEEE Conference on Network Softwarization and Workshops (NetSoft). IEEE, 2018.
- [9].Suankaewmanee, Kongrath, et al. "Performance analysis and application of mobile blockchain." 2018 international conference on computing, networking and communications (ICNC). IEEE, 2018.
- [10].Raymond Allan G. Vergara, Ramon V. Del Rosario College of Business De La Salle University Manila, Philippines," Extending the Definition of Crowdfunding Success: The Case of the Flight of Super", March 4, 2017.