|  |  |  |
| --- | --- | --- |
| **SR. NO.** | **PARTICULARS** |  |
| 1 | Preface/ Abstract | 2-10-21  8-10-21 |
| 2 | Project Overview   * Project Title & Definition |
| 3 | Introduction   * Detailed explanation of study area |
| 4 | Literature Review   * Study undertaken on similar concept * Citation |
| 5 | Research Methodology   * Objective * Scope of study * Limitations * Significance of Research * Description of Algorithms / procedures / data collection methods / logic | 11-10-21 |
| 6 | Experimental setup   * Tools * Architecture/Framework * Software Language | 15-10-21 |
| 7 | Results   * Screen Layout * Testing report | 25-10-21 |
| 8 | Summary and conclusion   * Findings of Project work * Application area | 30-10-21 |
| 9 | Further Research |
| 10 | Bibliography   * Books * References (Conference Papers/ Journal Papers etc.) * Websites |

**634 - Sagar Parker**

**Equity crowdfunding with blockchain smart contracts.**

**Sagar Parker**

[sagar8parker@gmail.com](mailto:sagar8parker@gmail.com)

+919137427570

Ramnarain Ruia College - ( M.Sc ) Computer Science department

**Abstract**

At present, Crowdfunding source of raising funds typically for startups or projects has gained popularity with most startups resorting to the use of Crowdfunding platforms to raise funds in exchange of equity because it is relatively inexpensive and uncomplicated in nature. In the existing model, Pool of people contribute small amounts of money towards a project or cause and expect some financial returns. The call for a solution to issues related to security, investor abuse and, illegal transactions that could plague crowdfunding has lead me to investigate the implications of blockchain in Crowdfunding. Blockchain technology is a decentralized ledger, more efficient, safe and tamper-proof system of nodes in connection. Introduction of blockchain in crowdfunding will make it more reliable, transparent, trusted, decentralized, cost-efficient and convenient. A crowdfunding platform which was acting as an intermediary before will only provide the technology and its own crypto-currency which will act as a medium of transaction and exchange. I highly anticipate that this project will drive the attention of researchers to delve into the applications of blockchain technology in Crowdfunding practicality.

**Project Title :**

**Collective** - An equity crowdfunding platform managed with blockchain.

**Introduction :**

A global challenge facing start-ups is the raising of the required funds. Although there are many sources of funds available to entrepreneurs who wish to start new businesses or expand existing ones, the challenge of getting inexpensive funding at the right time still remains a challenge in the small business domain. The emergence of crowdfunding as a brainchild of

crowd-sourcing provides an alternative form of funding for start-ups.

**Collective** is an online equity crowdfunding platform managed by smart contracts on Ethereum. The platform enables start-ups and projects to raise funding in return of equity. Individual can invest a relatively small amount of money in-order to receive stake in a company at an early stage hoping to get good returns in the long-term as the startup/project grows. Along with funding, Collective also enables startups/projects to find the required talent for their projects.

What makes Collective truly unique is its decentralized and autonomous approach towards crowdfunding using smart contract that are deployed on the Ethereum blockchain and a mobile app created using Google’s Flutter which can be used on both Android and IOS.

Startups on the platform can create camps in which normal users can purchase equity by investing CTV ( Collective token ) a ERC20 fungible token exclusive only to the Collective platform. This platform exclusive ERC20 token along with smart contracts enables Collective to tackle the issue of trust and security that plagues all the existing crowdfunding platforms.

**Literature Review :**

**The Tokenization of Assets: Using Blockchains for Equity Crowdfunding**

One of the biggest challenges for small startups and new projects is to ﬁnd investors, willing to support the company with seed capital (Schwien-

bacher, 2019; Tomczak and Brem, 2013). After having accessed all avail-

able resources from the FFF group (friends, family and fools), startups

tend to turn to banks or angel investors for funding in the earliest stages

(Tomczak and Brem, 2013). However, due to the lack of collateral of

these young ﬁrms and the high information asymmetries involved, ﬁnan-

cial intermediaries are usually reluctant to invest (Deffains-Crapsky and

Sudolska, 2014). Tomczak and Brem (2013) argue that small startups in

particular have a lower probability to obtain funding. In the last decade,

this fueled the rise of crowdfunding as a new way to raise seed capi-

tal for small startups, through the consolidated investment of investors

(Tomczak and Brem, 2013).

Crowdfunding models are usually categorized in two broad classes: (i)

reward- and donation-based crowdfunding and (ii) investment-based

crowdfunding (Belleﬂamme et al., 2015). In reward- and donation-based

crowdfunding, investors are not reimbursed ﬁnancially, but receive some

other kind of reward (e.g. the product once the ﬁrst production round is

realized) or have other motivations for supporting the project. The sec-

ond class is divided into lending-based, equity-based and royalty-based

crowdfunding, from which investors expect to receive interest, dividends

or other forms of ﬁnancial gains. In this paper Fabian, Jabok and Aljosch focus on the ﬁeld of equity-based crowdfunding. Crowdfunding is usually organized by an internet-based intermediation platform which connects investors with campaign creators3(Belleﬂamme et al., 2015). Platforms charge various fees for their services from the creators (if the campaign was successful), accumulating to approximately 7 to 10 percent of the total amount raised (Belleﬂamme et al., 2015).

**Citation :**

Schär, Fabian & Roth, Jakob & Schöpfer, Aljoscha. (2019). The Tokenization of Assets: Using Blockchains for Equity Crowdfunding. 10.2139/ssrn.3443382.

# **The Applications of Blockchain in Crowdfunding Contract**

The emergence of crowdfunding as a brainchild of crowdsourcing provides an alternative form of funding for business start-ups (Belleflamme, Pambert, and Schwienbacher 2014). The concept of crowdfunding simply involves selling a business idea to a specific group of individuals via the internet to convince them to contribute widows might each to the tune of the total fund required to transform that idea into a reality. This means that the possibility of getting investors could hinge on how valuable an idea sounds. Crowdfunding could take several forms, investors could swap their money for shareholder status where they can vote and receive dividends, investors could simply donate without expecting any form of returns, investor can lend to the business and expect their principal plus interest back after a period of time and, finally investors can invest in anticipation of a reward (Schwienbacher and Larralde 2010). Crowdfunding is preferred for business startups ahead of other sources of funds because of the relatively lower cost of raising the funds, the speed with which funds can be raised and the lower entry barrier for businesses (Bradford 2012).

In practice, crowdfunding could have potential challenges if not regulated, as reported by Hu (2014) investor interest can be damaged in a situation where regulations are not properly administered causing illegal transactions to become the order of the day. Information asymmetry is key to any financial decision and the lack of accurate information on the credit ratings of fundraisers, clear description of rights of investors could also hamper the security of investing in a crowd contract (Wang 2016, Liu 2014). How do we secure the interest of shareholders? how do we prevent illegal businesses from raising funds through a crowdfunding contract? The crowdfunding market is fast developing and there is the need to ponder on the security of the tradings that take place on this market (Wang 2016; Lou 2015; Dong, Mei, Zhou, Liu, Zhang, and Yuan 2014).

**Citation :**

Zhao, Hongjiang & Coffie, Cephas. (2018). The Applications of Blockchain Technology in Crowdfunding Contract. SSRN Electronic Journal. 10.2139/ssrn.3133176.

**Research Methodology**

**Objective:**

The primary objective of the project is to get a deeper understanding of the core blockchain fundamentals and undertaking a practical approach to establish a decentralized, trusted and transparent platform for equity crowdfunding with the help of smart contracts deployed on the Ethereum blockchain network.

**Scope of study:**

### The project aims to study how blockchain can be used to manage equity crowdfunding. Equity crowdfunding includes investors investing in startups and projects in early stage in return of equity/stake. In the recent years the crowdfunding platform like AngelList, Microventures, and Fundable are getting traction due to ever increasing entrepreneurial spirit among millennial and younger generations.

These crowdfunding platform enables startups to raise funding at an early stage and allows its investors to invest into budding ideas with relatively smaller investments hoping to gain exponential return as the project grows. Every platform has their own methodologies to handle equity crowdfunding.

**AngelList** has three main ways to invest in companies they are as follows:

Deal by deal investment : Registered investors can partner with investor syndicates led by notable lead investors — usually venture capitalists with extensive Silicon Valley experience.

Access fund :The AngelList Access Fund offers access to dozens or hundreds of individual deals. All are vetted by AngelList, cutting down on users due diligence responsibilities.

Professional Investor :This service is limited to high net worth individual and institutional investors (including family offices) that can afford to invest at least $500,000 at once. Professional investors get their own AngelList representative, plus rare access to company founders and executives.

### Microventures is a full-service investment bank with a robust equity crowdfunding arm that caters both to non-accredited and accredited investors. Offerings span a wide range of industries with a bias toward consumer-facing opportunities and opportunities in high-growth niches.

**Fundable** offers rewards-based crowdfunding, a la Kickstarter or GoFundMe, as well as equity crowdfunding.For companies interested in equity crowdfunding, Fundable provides hands-on help with onsite profile building, pitch construction, and even business plan development.

**Limitation**

Every platform mentioned above has their own way of handling crowdfunding. One common theme that we can observe in all of them is centralized authority and lack of equal opportunity for investors.

While preaching equal opportunity these platform still favour the affluent society by various schemes, whether it be higher base investment amount or favouring the rather rich due to their status.

These platforms handle all the data and investments raised during the crowdfunding campaign which leads to a centralized service and lack of transparency among the angel investors.

Adopting blockchain technology can solve these issues by implementing its immutable and transparent properties. Smart contract allows such campaigns to achieve autonomy and make decisions without a third party intermediary.

**Significance of Research**

The study suggests that crowdfunding could have potential challenges if not regulated, investor interest can be damaged in a situation where regulations are not properly administered causing illegal transactions to become the order of the day. Information asymmetry is key to any financial decision and the lack of accurate information on the credit ratings of fundraisers, clear description of rights of investors could also hamper the security of investing in projects.

Blockchain technology although is seen by the utopian view a disruptive technology that threatens to substitute the role of all intermediaries in different fields of application, it can alter the intermediation of platforms. It is a technology that can solve most problems of human-related transactions.

The application of blockchain technology has been tested and verified with the success of bitcoin. Blockchain technology is the creation, insertion and using of blocks to help solve problems related to the needs of people in society. Blockchain technology endorses transparency in records, supports decentralization, encourages trust and provide a low-cost alternative to a platform for the recording of business activities

The call for investor protection and security in Crowdfunding contracts could be answered by the introduction of the blockchain technology which functions on a trust-free system where individuals have little to do to make it work.

**Experimental Setup**

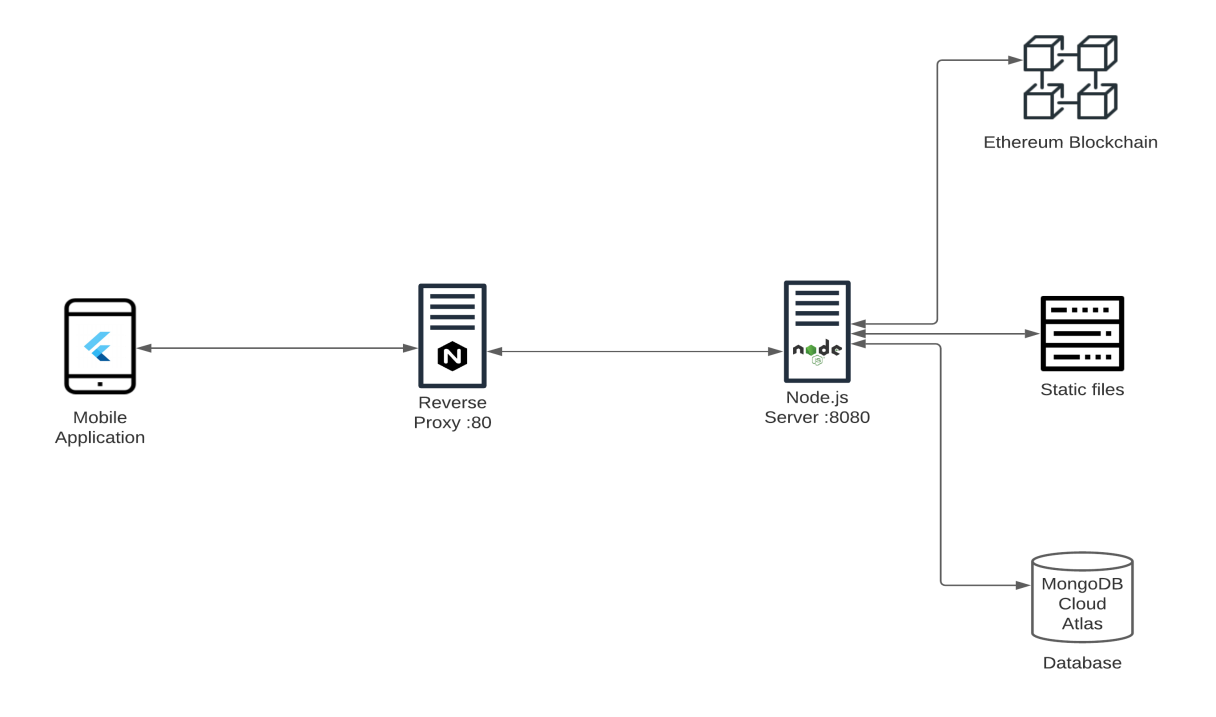
**Tools**

1. Visual Studio Code
2. Android Studio ( Emulator )
3. Remix
4. Truffle
5. Ganache
6. Infura
7. OpenZeppelin
8. Postman
9. PuTTY
10. Git & Github
11. AWS console
12. MongoDB compass

**Architecture/Framework**

* The Node.js backend follows MVC ( Model-View-Controller ) architecture for increased modularity and maintenance.
* Express framework provides a thin layer of fundamental web application features, without obscuring Node.js features and enabled me to create robust APIs for the platform.
* The mocha framework along with assert enabled in-depth testing of the smart contracts to cover every test case and make the platform as safe and tamper proof as possible.
* Web3.js is a collection of libraries that allowed users to interact with remote ethereum node using HTTP and make state and memory changes to the smart contracts and also fetch data.

**High level System Design**



* The Node.js backend API server is hosted on the AWS EC2 instance and is connected to the express static file server, MongoDB cloud database and the Ethereum blockchian.
* The Flutter app interacts with APIs hosted on the cloud through a NGINX reverse proxy which adds a extra layer of security.

**Software Language**

* Dart ( Flutter )
* JavaScript ( Node.js )
* Solidity ( Ethereum Smart contracts )

**Description of Algorithms / procedures / logic**

The platform is primarily divided into two sections they are as follows:

1. Angel investing
2. Collaboration

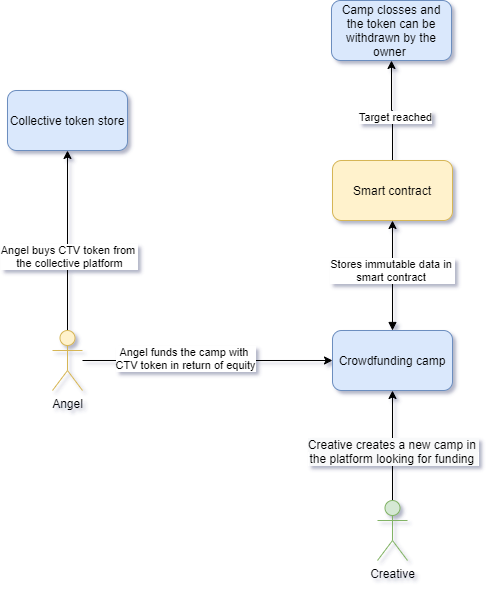
Smart contracts hosted on Ethereum blockchain network plays a key role in the working of both investing and collaboration.

**The login and registration system**

* New users on the platform can start by creating a new account by entering their email,username and password.
* The password is securely saved in the MongoDB cloud database by hashing the plain text and passing it through ten rounds of salting.
* For every new account the platform automatically creates a new Ethereum account and links it to the users account and saves the Ethereum account address into the database along with the accounts private key.
* The private key plays a key role in the account safety. Storage and handling of this private key is rather a very important task that is widely researched and debated across the cyber security industry.
* The collective platform encrypts these private key with the help of AES encryption and stores them securely into the database after the registration of the user.
* After creating a new account the user can login into the system by entering his/her email/username and password.
* The entire login system is made secure by implementing JWT authentication which encrypts the payload with RSA algorithm.
* Once the user enters the correct credentials a encrypted JWT token is returned by the back-end server containing the users public account address along with the encrypted private key which is then stored into the smartphones local storage using shared preferences.
* At every instance of signing a transaction on the Ethereum blockchain the mobile application has to send the encrypted token containing the private key back to the server which is stored in the local storage of the device using shared preferences.
* This entire flow ensures the secure and trusted working of the login and registration system for the Collective platform.

**The Crowdfunding system**

Collective manages crowdfunding with the help of smart contracts that are deployed on the Ethereum blockchain.

****

**CTV** - Collective token (CTV) is a ERC20 token hosted on ethereum blockchain created using OpenZeppelin.

**Creative** - Creative is a user who creates camps on the platform to raise funding for their startups/projects.

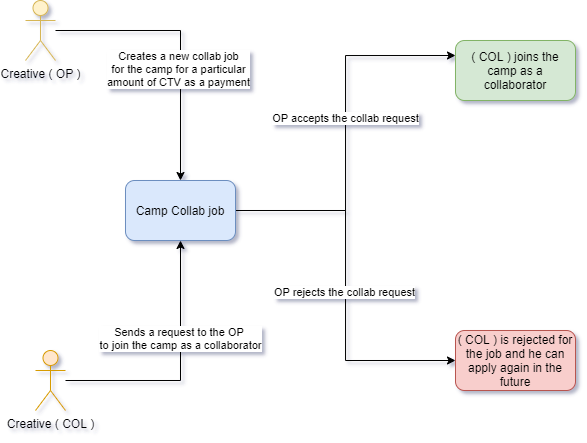
**Angel** - Angel is a type of user who is trying to invest into various camps on the platform using CTV token.

**The equity crowdfunding flow**

* Users on the platform can start by buying CTV token from the store in exchange of their local currency by making payments using Gpay.
* CTV a token ( Crypto currency ) created by using ERC20 standard plays a key role in the entire investment strategy of the collective platform.
* Creating a platform exclusive fungible token ensures that the the investments medium used to invest in camps is only valid inside the platform itself.
* The token does not hold any real world value outside the platform since the CTV token is only purchasable and sellable inside the platform. In-case a rouge user manages to steal these token and transfer them to another account outside the platform the tokens will essentially will be of no value since CTV token only holds a value inside the collective platform.
* When a new user creates a camp on the platform he/she has to enter the amount of CTV they are trying to raise along with the amount of equity they are offering in exchange of the investment.
* A new Ethereum account is automatically created when a new camp is created by the user. When an investor is trying to invest in a camp the respective CTV is transferred to the Ethereum account that is linked to the new camp.
* The valuation of the camp is calculated by taking the target and the equity offered by the camp into consideration.
* The smart contract holds various sensitive camp data like target, equity, funding raised, investor list.
* When a users tries to invest in a camp with CTV, the investment amount is stored on the smart contracts that are hosted on the ethereum blockchain ensuring that all the data is immutable and trusted.
* All the investments done by all the users is visible to everyone in the angels tab maintaining a high level of transparency in the system.
* Once the target of a camp is reached the camp is automatically closed with the help of various conditions defined in the smart contract without the need of a intermediary third party.
* The owner of the camp can withdraw the amount raised once the target is reached and the camp is closed.
* This smart contract enabled crowdfunding system manages to create a transparent, trusted and secure platform for the next generation of budding investors.

**The collaboration system**

The collab feature of collective not only allows user to invest money but also contribute to the projects they believe in as a creative.



**COL -** User who wants to join the camp as a collaborator.

**OP -** The owner of the camp who handles the collab requests and payments.

**The collaborations flow**

* OP that is the owner of the camp can create collab jobs for the camp which other users can apply to in return of CTV as a payment.
* The collab job can include jobs from various fields of engineering, designing and commerce.
* The collaborators ( COL ) can get payments for their work in the form of the platform exclusive CTV token once their request is accepted by the camp owner ( OP ).

**Result : Screen Layouts**

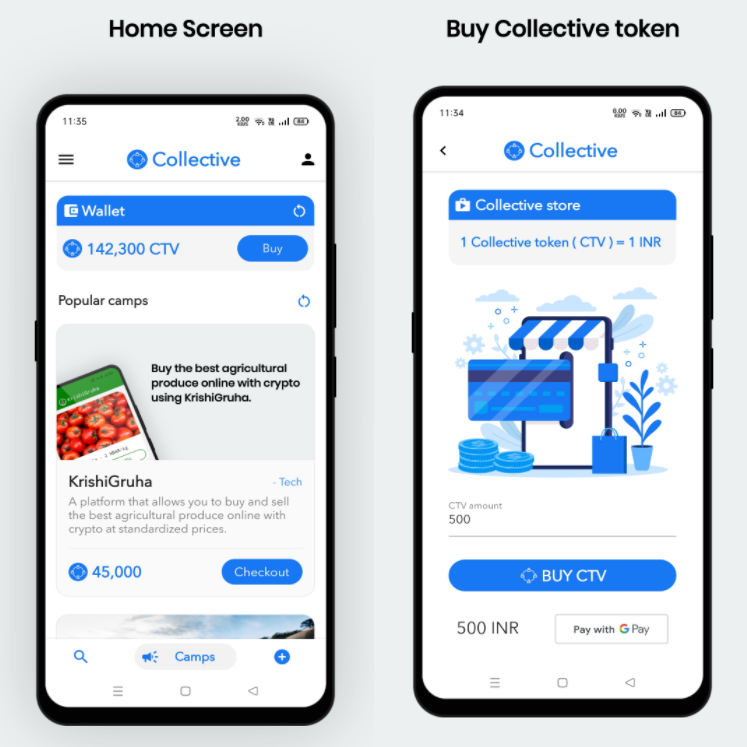
**Register Screen :** The user can create a new account by entering their email, username and password. Every time a user create an account on collective the platform automatically creates a new Ethereum account for the user.

**Login Screen :** The user can use their email or username along with their password to login to the platform.



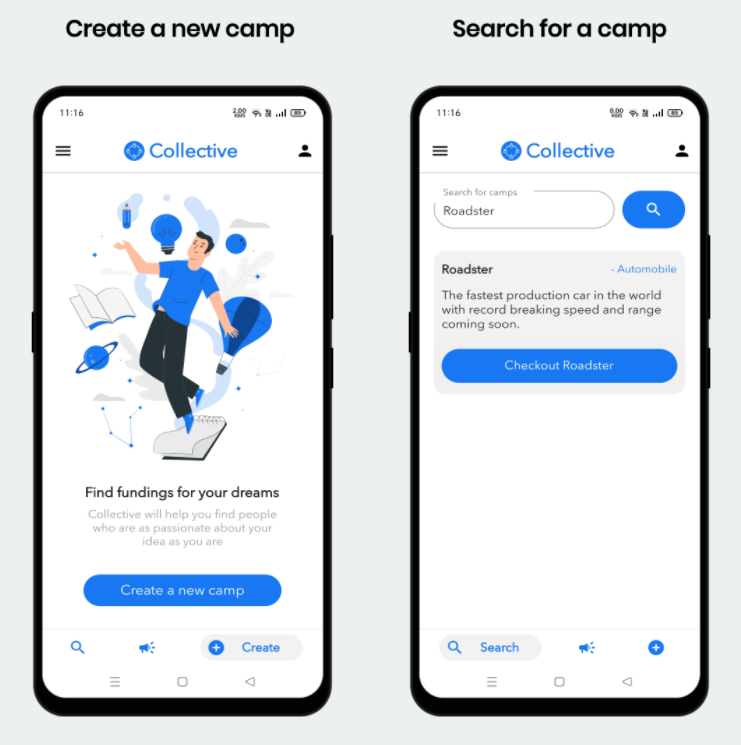
**Home Screen :** The home screen displays all the camps that the users/angels can invest into along with tab view to switch between screens.

**Buy tokens screen :** The users can buy Collective token ( CTV ) by making payments using Gpay on the buy screen.



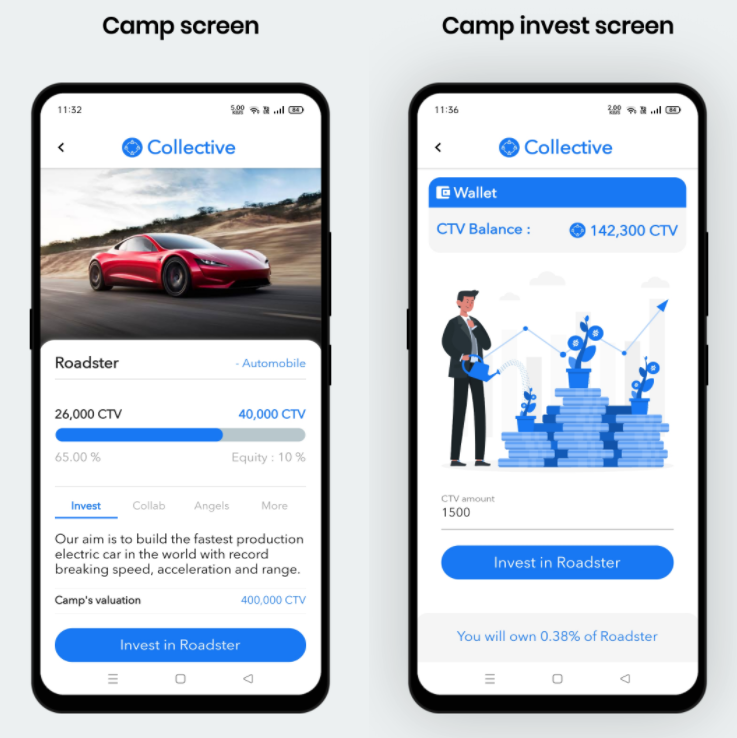
**Create new camp screen :** The create a new camp screen allows the users to create new camps by entering various details and also gives an option for uploading camp cover option. Every camp on the platform actually is a Ethereum account.

**Search screen :** The search page allows users to search for camps on the platform by using the camps name as the keyword.



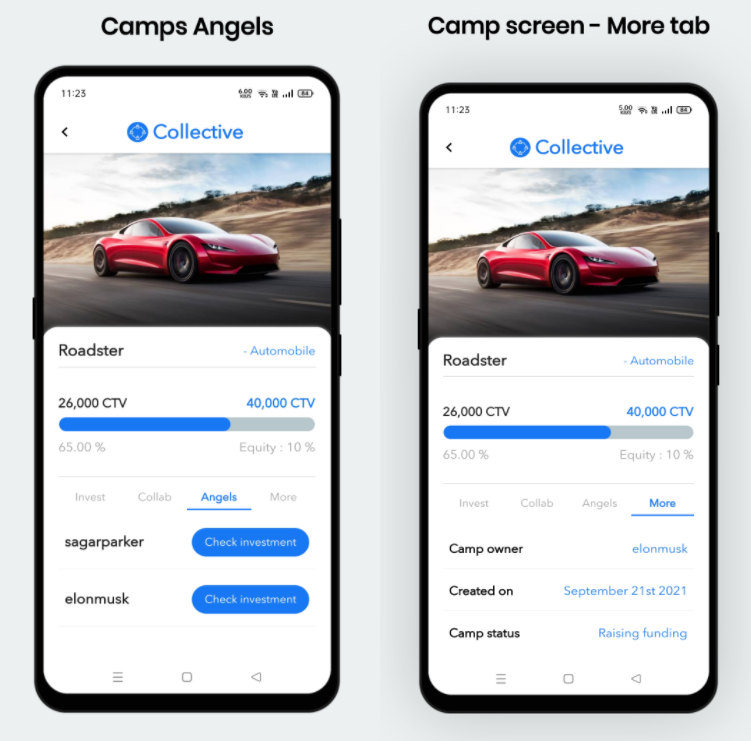
**Camp screen :** The camp screen displays a lot of vital information including the camp image, description, target, amount raised, valuation, etc.

**Camp investment screen :** The camp investment screen allows the users to invest in the camps using the platform exclusive CTV token.



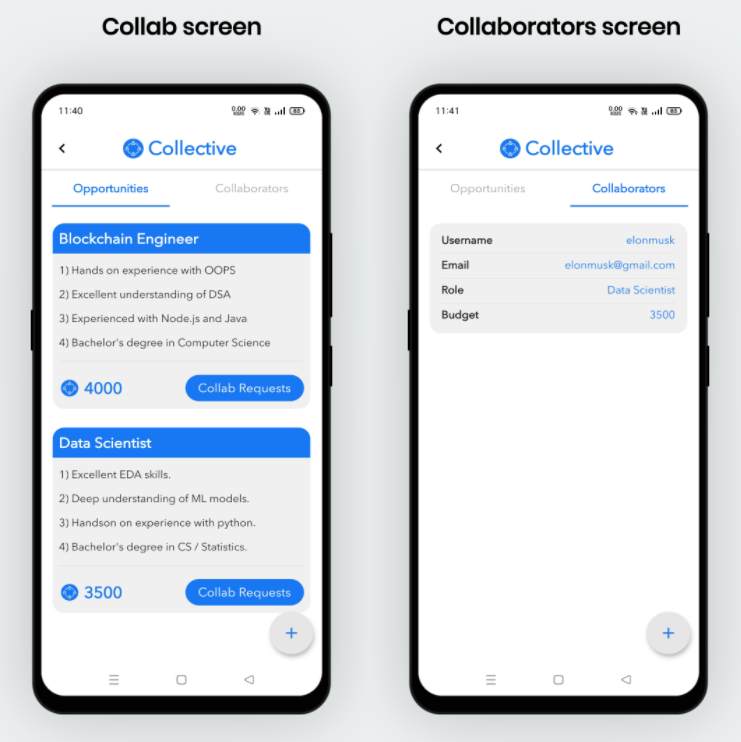
**Camp angels tab :** The camp angels tab show all the angels/investors who have invested in the camp and also shows the equity they own in the camp after clicking the check investment button.

**Camp more tab :** The camp more tab display the owner of the camp, the time and date the camp was created and also the current status of the camp.



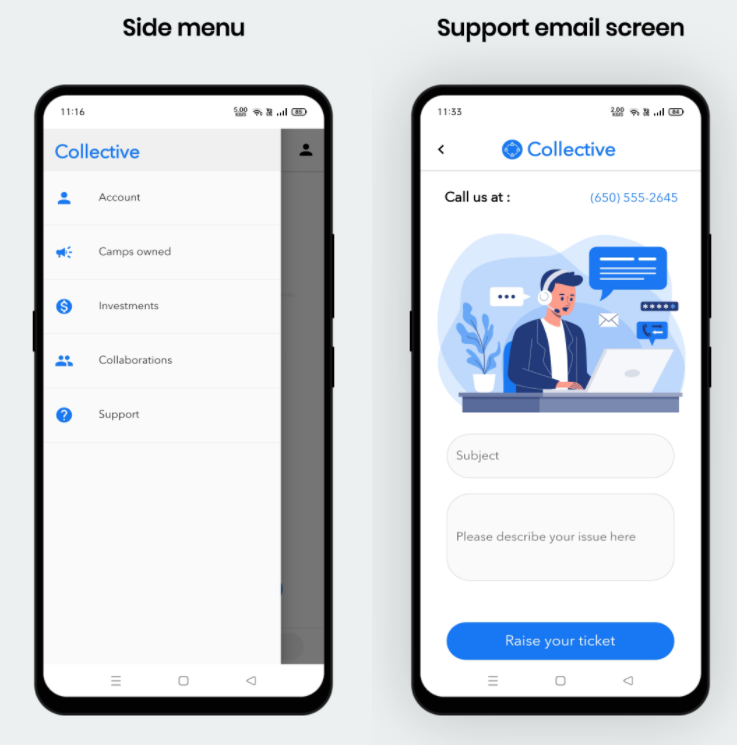
**Collab opportunity tab :** The collab screen opportunity tab shows all the collab jobs created by the camp owners.

**Collaborators tab :** The collaborators tab displays all the existing collaborators for the particular tab.



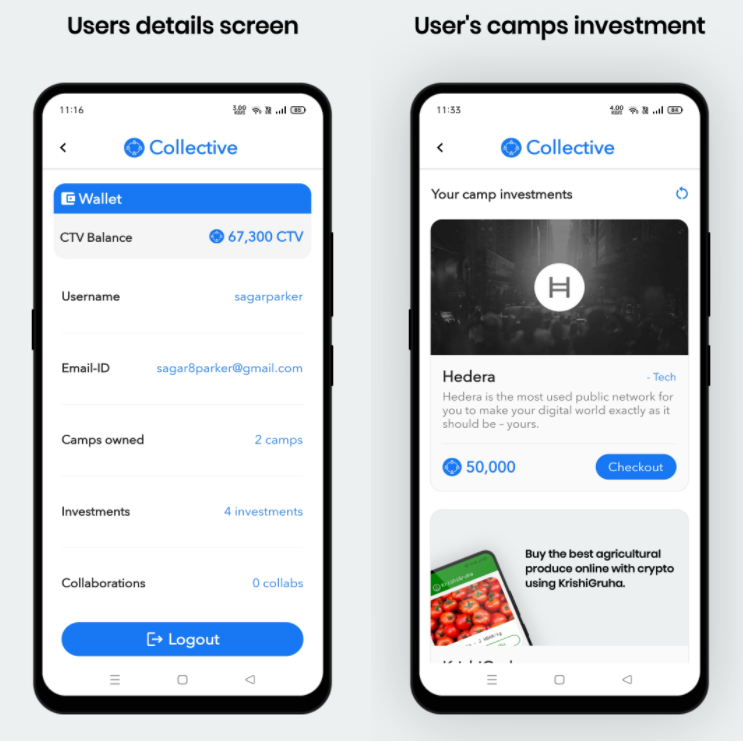
**Side menu :** The side menu allows the users to quickly navigate between various screens.

**Support email screen :** The support email screen allows the users to send emails to the collective team in-order to get tech-support.



**User details screen :** This screen displays the users CTV balance, username, email id, camps owned, investments, collaborations.

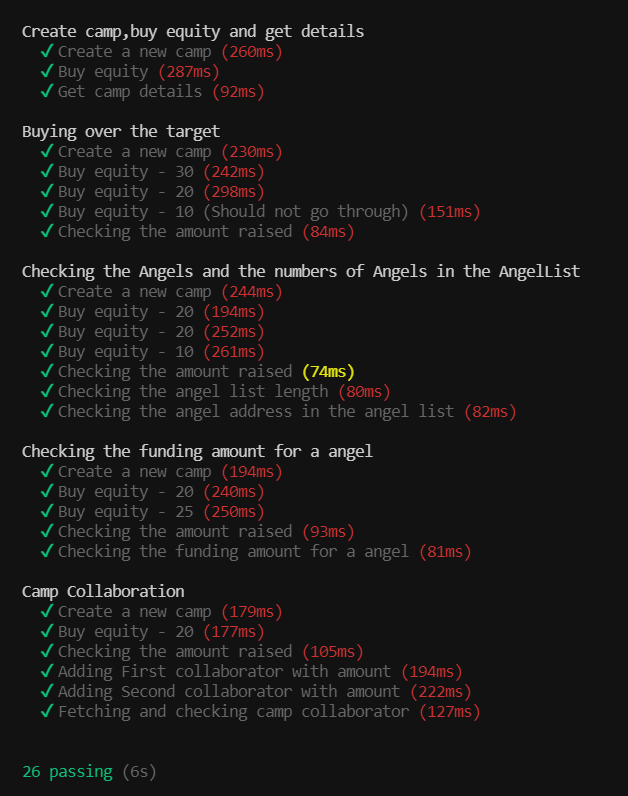
**Users camps investment :** This screen displays all the camps that the user has invested in the past using CTV token.



**Testing**

Tools used for testing : Mocha & Assert

Mocha and Assert allows developers to perform in-depth testing of the smart contracts. Developers can define various custom test cases as shown in the image below to thoroughly test all the aspects of the system.



**Summary and conclusion**

*Blockchain is a technology that can solve most problems of*

*human-related transactions - Glaser, 2017.*

**Findings of Project work**

* The possible application of Blockchain technology in different fields is still under study and this is an indication of the possibility of blockchain technology resolving most of the problems related to humans in terms of the trust.
* The call for investor protection and security in Crowdfunding contracts could be answered by the introduction of the blockchain technology which functions on a trust-free system where individuals have little to do to make it work.
* There are challenges with Crowdfunding in relation to abuse, trust and confidentiality and the adoption of blockchain technology in Crowdfunding contracts could provide the much-needed solution. Blockchain technology provides cheaper, easy, and secure and a convenient means for the exchange of information and transfer of funds.
* The technology is programmable and can be extended to cater for any other requirement in the Crowdfunding contract where necessary. Although currently the technology can be used to modify the role of the platforms (intermediaries), in future the technology could be used to execute Crowdfunding contracts without the need for the institutional platforms.

**Application area**

* The applications of blockchain in various aspects of our society are infinite. From solving the smallest issue of document authentication to replacing age old financial institution, blockchain is a technology can change how the people handle their private data.
* With an every increasing demand for decentralization among the society Blockchain or DLT in-general can form the basis of a decentralized internet also known as Web3.

**Further Research / Improvements**

**Migrating to a micro-service based architecture**

* Currently the back-end architecture of he platform follows a MVC architecturefor modularity.
* A micro-service base architecture using RabbitMQ can truly bring granular control to the platform and will improve upon the modularity of the existing MVC pattern.

**Moving all the camp images/media to IPFS or AWS S3 bucket.**

* The current system uses the hard disk storage of the AWS EC2 instance to store images and servers them with the help of express static server.
* While the current system being completely acceptable the cost of storing media files on the EC2 will grow exponentially as the platform grows and new users upload more and more media.
* This issue can be addressed by implementing a dedicated AWS S3 bucket in the system design which might also help to improve the media loading speeds.
* In-order to improve upon the current decentralized nature of the platform the media files can be stored on IPFS.

**Hedera hashgraph integration**

* Blockchain is a technology that has potential to change how the world handles their data, but it doesn’t come without its flaws. Scalability, Gas fees, Transaction speeds are few of the issues that plague the technology at this moment and might just be the hurdle for the mass adoption.
* Hedera hashgraph is a 3rd generation DLT ( Distributed ledger technology ) which uses direct acyclic graphs to store data and improve transaction speeds and reduce the transaction costs.
* HTS ( Hedera token service ) is a service provided by Hedera which enables engineers to create smart contractless fungible tokens like CTV and vastly improve their security by abstracting the underlying complexities. Hedera smart contract service 2.0 can also bring improvements to the platform by decreasing the transaction fees and improving the transaction speeds.

**Bibliography**

**Books**

Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin, and popular Blockchain frameworks - *Imran Bashir (2017)*

**References (Conference Papers/ Journal Papers etc.)**

Schär, Fabian & Roth, Jakob & Schöpfer, Aljoscha. (2019). The Tokenization of Assets: Using Blockchains for Equity Crowdfunding. 10.2139/ssrn.3443382.

Zhao, Hongjiang & Coffie, Cephas. (2018). The Applications of Blockchain Technology in Crowdfunding Contract. SSRN Electronic Journal. 10.2139/ssrn.3133176

**Websites**

<https://ethereum.org/en/>

<https://web3js.readthedocs.io/en/v1.5.2/>

<https://docs.openzeppelin.com/contracts/2.x/api/token/erc20>

<https://www.dappuniversity.com/articles/web3-js-intro>

<https://flutter.dev/docs>

<https://pub.dev/>

<https://www.npmjs.com/>

<https://www.javatpoint.com/aws-tutorial>

<https://nodejs.org/en/docs/>