BlockBits.IO General Offering

Blockbits team

January 2018

Contents

1 Abstract

Blockbits is a decentralized open-source crowdfunding/investing platform. Its most innovative feature is that it eliminates blind trust requirements, thus providing a significantly safer investing experience. This is achieved via blockchain contracts, built-in features that allow it to become fully maintained and governed by its token holders.

2 Introduction

2.1 Motivation

2.1.1 Blind Trust requirements

In the past years, the Ethereum network has seen the launch of numerous ICOs. This is good, but unfortunately, most ICOs still ultimately rely on investors' blind trust. This attracts only the more risk inclined investors, while even the moderately risk adverse will rightly avoid investing in what looks like get-rich-fast schemes or even outright scams.

The main issue with a classic ICO is the fact that its token is often not linked to any meaningful action in its system. Even when it is, in the overwhelming majority of cases, the investor is expected to blindly trust that the project initiators will deliver on their promises.

2.1.2 Risk of incorrect or manipulated reviews

The ecosystem addresses the problem of trust through a couple of websites that provide ICO reviews and assess the potential risk of investment. This solution to the problem of trust is inherently suboptimal: not only are these services highly centralized, but they are also paid for by the ICO under review. Bias? and even abuse? is very likely, even with the best of intentions.

2.1.3 Problems of existing crowd funding platforms

In existing platforms, the owners have ultimate control over which projects get to launch through the platform. Thus investors skip an investigation phase that would make sense before investing in a project. Their agency is thus relegated to the owners of the platform who vet projects for launching.

Furthermore, some projects even create their "internal currency" token, which, in turn, comes with its own set of problems and significant risks. One of them is the requirement to mint it and sell it at will, in order to maintain a stable price, this dilutes the initial supply. Another one, is the need to rely on the platform's success in order to find buyers for a recently funded campaign.

Finally, from a security perspective, most platforms are not backed by transparent open source code. Instead, they are closed source centralized entities that use human labor for day-to-day operations.

One could argue that the venture capitalists/serial entrepreneurs who own the platforms, as well as the human labor they rely on to run the closed systems, are perhaps best qualified to vet and run investment projects. However, we maintain, the problem of trust/risk remains

unaddressed, insofar as such a system will be fraught with issues of competence, integrity, and natural human error.

2.1.4 Project delivery risk

Existing projects fail, in most cases, to provide a coherent system for linking the project to its roadmap and its tokens.

2.1.5 Ecosystem price damage through large dumps

A common phenomenon unaddressed by existing platforms, is that, each time a new ICO is funded, a large amount of ETH is subsequently dumped on the exchanges. This drives the token's price down and removes value from the network.

2.1.6 Token supply and mechanics

In an ideal system, the collected ETH is used for covering development expenses, while owners' remaining token supply should be seen as the main source of profits. Having a larger stake in the project incentives the owner to deliver.

Owners should lock their tokens until project delivery in order to limit their ability to dilute token market value during development.

2.1.7 PRE ICO funding phases

In trying to emulate classic systems, the ICO pre sale has mostly missed the point, i.e., that a pre-sale is usually targeted at already existing investors, with contractual rights to buy newly created shares. Instead, in the ICO model, pre-sale has become merely a means to raise funds for marketing or logistic purposes, by offering a substantial discount to anyone who wishes to participate and undertake the initial risk.

This creates the inability to refund participating investors in the case of a funding failure, and also fuels reckless investment and hoarding for the purpose of dumping at a better price once the sale period ends.

3 The Blockbits Platform

3.1 Description

We introduce Blockbits, the platform that provides the optimal solution to the problem of risk and trust in investing. Our innovation consists of built-in features and mechanisms that take into account general rules of human psychology in relation to risk and investment. Our ultimate goal is to provide a safe investing experience, where: 1. Projects advance insofar as they are viable 2. Risk inherent to human bias or error is minimized. This, in turn, will mean that investing will become accessible and relatively risk-free.

To achieve this, Blockbits relies on a set of smart contracts onto which we've built a complex ecosystem of rules and business logic. This breakthrough technological innovation allows token holders to moderate and validate the development process of the platform. The requirement of blind trust into the platform's development team is virtually eliminated and so are many of the problems that would stem from this problem thereafter.

Blockbits offers two types of project funding, namely, Direct funding and Milestone funding. For both, an innovative Vault mechanism is put in place to protect against hacking. The Vault isolates each investor's funds into a separate contract, with two enforced hardcoded output addresses: the platform and the investor wallets.

The Milestone funding mechanism mitigates project delivery risk by locking up investor funds until a milestone delivery is reached. At this point the investor has the choice to validate and accept the delivered content and thus release locked funds to the project owners for the milestone in question. In turn, the investor will receive previously locked tokens as compensation.

If, instead, the majority of investors do not deem the delivered content as acceptable, all investors who voted NO on the proposal, can choose to use the CashBack mechanism to retrieve their remaining locked ETH. Essentially, this gives the investors the power to decide if the project delivered on its promises or not. Furthermore, voting NO does not require an investor to actually resort to CashBack - it may just signal disagreement with the delivery.

Investing into Blockbits awards BBX Tokens. These tokens allow the participation in Internal funding phases of projects launched through the platform. This does not only provide bonus discounts, but also genuine involvement as an investor with the ability to initiate code upgrade proposals. If such upgrades are accepted by the community, they will yield revenue and possible return of initial investment through the token buyback program.

This unique ensemble of process makes Blockbits and all the projects launched through it stand out starkly among its competitors. They provide an objective and transparent risk analysis based on risk indicators built into the software contracts used to run the investment campaign. We call them "Platform testable risk indicators".

3.2 Features

3.2.1 Upgradeable Smart Contract Architecture

Ethereum Smart Contracts, are immutable by design. That means that once deployed their code is not changeable.

In order to facilitate a milestone based development process, we created a modular upgradeable architecture that allows for the swapping of logic entities with new ones. In order

to preserve mutual interest, such changes can only be initiated at first by the platform owner, and accepted by investors through a democratic voting process, where the owner has no vote.

Once the project reaches the "Development Complete" stage, any token holder can initiate code upgrades, and all token holders including the development team (that just got their tokens unlocked) can approve or disapprove the proposed upgrade. If approved, the contributing party will be compensated using an amount of ETH available in the revenue stream contract.

It should be noted that each entity in the first version of the application is immutable and hardcodes addresses and values for the resources they use. The only contract that is not, is the Application Entity, which serves as the application's hub. This means we can introduce new features, override existing functionality, but never change the data as well as the logic of existing ones (ex: the ones tied to Vaults or Development).

3.2.2 Funding Vaults

Each Investor has their own separate smart contract, that stores and locks ETH and tokens until an action is available. This contract mitigates issues that can arise from hacking attempts, by enforcing 2 hardcoded output addresses, namely, the platform and investor wallets.

3.2.3 Development Milestones

Just like in software development, most projects can be split up in "Phases". We call them Development Milestones and each one has a percentage of the raised funds linked to it, and requires community acceptance in order for funds and tokens to be released.

3.2.4 Direct Funding Payments

Direct Funding payments will lock ETH until either the project is successfully funded, or it fails. If the project is successfully funded, the ETH is released to the platform's multi signature wallet address, and tokens get sent to the vault's owner wallet address. If the project's funding fails, the funds are unlocked and can be claimed back by the vault's owner.

NOTE: This is the traditional way of investing into ICOs where one gives "value" and receives "tokens" but with the additional enforcement that denies anyone from spending the value until the funding outcome is known.

3.2.5 Milestone Funding Payments

Milestone Funding payments adhere to the same rules as Direct funding when it comes to incoming funds and release in case of funding failure. The fundamental difference is that, if the project's funding is successful, funds and tokens get released only upon successful completion and voting by investors in development milestones.

In practice, an investor has the choice to fund a project by locking up their ETH in a smart contract, that upon their vote will release the funds to the project, in case the project delivered on what it promised . Otherwise, the investor can use the CashBack procedure to take their money back. This will require some involvement from the investor at validating the project's roadmap, and voting accordingly. Of course, they also have the choice to opt out of the voting process at any time by choosing to do nothing. In other words, the investor gets

to validate if the project is actually delivering on its promises, or take their money back. In the case it does deliver, one gets to "buy tokens at the PRE ICO or ICO price".

3.2.6 Proposals

Each time a major event happens in the system, a Proposal is automatically created. Any proposal that leads to a change in the system, or release of funds can only be voted by investors that have contributed using Milestone Funding.

Proposals that moderate the platform, like delisting a project from the website, can be created and voted on by all token holders.

3.2.7 Development Cycle

If the project is successfully funded, it enters the "Development Phase", which cycles through its Development Milestones. At the end of each Development Milestone, the project's team will present evidence that the work was done and investors that contributed using the "Milestone Funding" will be able to vote on whether the team delivered or not.

If at this point an investor votes NO, and the majority result is also NO, the investor can then choose to use the "CashBack" functionality in order to retrieve their remaining funds, thus receiving their remaining locked ETH, while the project owner gets their tokens back. If the investor does not "CashBack", they just express disagreement and the funding release process is not interrupted.

Votes can be toggled at any time during the voting period and are treated as final only once the period ends and votes are counted.

3.2.8 Economics and loss mitigation

Milestone development and funding process in itself mitigates some economic issues by allowing the investor to use the CashBack procedure when 1. the team does not deliver 2. the team bails out 3. the team is betting against their own project. In all such cases, the investor gets the remainder of their investment back, and the project team get back some useless tokens, that might have some sentimental value but that's about it.

From the team's point of view we look at the most asked question, "What if the ethereum price got 2-5-10 times higher? What's stopping investors from just cashing out for the sake of it ?". The answer is: Nothing. In most cases, if an investor leaves, the project tokens already have a value and can be sold on the free market or to the token buyback system by the team to recover the lost funds.

3.2.9 Market decided token price

In this type of funding there are no guaranteed discounts and token amounts, they are decided by actual participation into the sale. This means Hard cap can be reached in the PRE ICO if demand is as such.

As this can be quite hard to grasp, here are the details:

– Funding Phase 1 - PRE-ICO –

Once “Hard Cap”, or “Funding Phase Time” is reached one of the two can occur:
Case 1.1 - Hard cap is reached in PRE ICO Funding Phase.

- The whole token allocation (Global Token Sale allocation) is distributed to investors and Funding is complete. No other Funding Phases will take place.

Case 1.2 - Hard cap is not reached in PRE ICO Funding Phase.

- Based on the ETH raised amount, and the token allocated to PRE ICO Funding Phase, we calculate the Parity (raised amount divided by token supply) of current Funding Phase (PRE-ICO). We call this “PRE ICO - TOKEN PRICE”.

This parity to which the non guaranteed discount is applied, will be used as the starting floor price for selling tokens in the next Funding Phase (ICO Phase). We call this the “ICO START PRICE”.
– Funding Phase 2 - ICO –

Once “Hard Cap”, or “Funding Phase Time” is reached we have two new cases:

- We calculate ICO Phase parity. (raised amount divided by token supply)

Case 2.1 - Global Funding reached Soft Cap:

- Buy orders in PRE ICO Phase, will be awarded tokens using “PRE ICO - TOKEN PRICE”.
- If resulting parity is lower than ICO START PRICE then ICO - TOKEN PRICE is ICO START PRICE.
- If resulting parity is higher than ICO START PRICE then ICO - TOKEN PRICE is ICO Phase parity.
- For buy orders in ICO Phase, Tokens will be allocated using ICO - TOKEN PRICE.
- After ICO Token allocation, if any tokens remain unsold, they are distributed to ALL Funding Participants. This excludes the Project’s Team in order to maintain the token share balances.

Case 2.2 - Global Funding reached Hard Cap:

- Buy orders in PRE ICO Phase, will be awarded tokens using “PRE ICO - TOKEN PRICE”.
- Buy orders in ICO Phase, will be awarded tokens using “ICO - TOKEN PRICE”.

NOTE: The goal is to have the market decide the value of the token, while still providing early investors a bonus in the case where interest in the project is low.

3.2.10 CashBack Procedures

At this stage of development the Blockbits platform offers three CashBack procedures which unlock ETH to be retrieved back by the investors from their respective Funding Vaults. Each CashBack case is hardcoded into Funding Vaults and forces the Funding Vault to unlock ETH in case it is triggered.

Funding Failed CashBack This mechanism is triggered if the funding of the project Failed, or if the funding period should have ended and 7 days have passed and funding processing has not been initiated.

Development Milestone Completion CashBack This mechanism is triggered if the Investor votes NO to a Development Milestone Completion Proposal.

Project Owner Missing In Action CashBack This mechanism is triggered if the project owner misses a Development Milestone Completion Meeting.

3.2.11 Inside Blockchain Revenue Stream

The Platform's revenue is created by investments into projects launched through it, directly tied into the platform's smart contract by child contracts. The revenue distribution is coded into and enforced by the smart contract.

The Blockbits Platform will charge a Dynamic Fee which can range from 0 to 50% of a project's total raised ETH. In most cases the Fee will be 1%. Depending on the actual spending of the owner, captured by the project parameters, certain bounties or external contracts will increase the fee.

One exception to the rule is Full Milestone Funding Only projects, that will have a 0% fee (if they have bounties limited to 1%).

This has been implemented in such a way as to deter reckless spending by the project owner. The fee will be collected only if a project is successful and, in case of milestones, when a certain milestone is complete.

Note: This feature will be deployed and activated using a Code upgrade in the 2nd Development Milestone.

3.2.12 Direct Investor Repayment using Token Buyback

This is done directly in the Platform's Smart Contract using funds generated by the Revenue Stream.

Note: Will be deployed and activated using a Code upgrade in the 3rd Development Milestone.

3.2.13 Distributed Application with NO OWNER

For the duration of the Development Milestones, the deployer address is the one that "owns" the gateway ,application contract and ENS name BlockBits.io . Through this, we ensure that code upgrades are only initiated by the development team, but once the Development

Milestones are complete, the application revokes access to this account and allows any token holder to do so.

Plans to provide a way for the platform itself to reward such token holder upgrades exist. (See Technical Documentation - Code Upgrades for more details)

3.2.14 Fully open source

Every asset created by this project is available in source format on github repository and is licensed under the MIT license.

This includes all solidity smart contracts, unit and integration test suites, deployment scripts, web application and as a bonus each stage of our Technical Documentation and Functional Diagrams.

3.2.15 Blockbits as a tool

Since everything is open source, one can use our tools to speed up the process of creating and deploying a crowd funding or investing program for their project, with tested and 3rd party audited smart contracts and visual tools, with no fees.

The downside of doing this is that not being able to list the project on the Blockbits Platform, as that requires the actual use of our BlockChain Validator and Deployer to ensure that nothing was changed in the code. Not being listed will then require deployment of one's own campaign management tools in order for contributors to be able to vote on proposals.

3.3 Targeted audience

3.3.1 Project owners

A Project owner also needs to be protected by clear and predictable rules which permit legitimate and good willed owners to perform when they indeed present a viable project offer.

Fundamentally, we want the project owners to expect personal economic enrichment from increasing the value of their tokens and not from the ETH they collected trough funding. This is a crucial step towards full legitimization of digital currency on the market as the technological innovation that it represents versus how it's currently perceived as a speculation tool.

3.3.2 Investors

By using the Milestone Funding method in the Ethereum network, we are now able to target even medium to high risk-adverse investors, who actually look for economic value rather than capitalizing on the currency's volatility.

3.3.3 Speculators

We understand that any market needs to provide ways of contributing to projects that do not require any kind of time investment, but rather just hearing or being advised about it in order to invest. Thus we provide Direct Funding method for parties who just want in, while forgoing both the initial investigation process of understanding the application and the direct involvement into its day to day operations.

3.4 Token Sale

The project funding will be split into two funding phases, specifically PRE-ICO and ICO.

The accepted contribution currency is ETH.

3.4.1 Accepted Funding Methods

3.4.2 Direct Funding Method

Once funding has started, visit https://blockbits.io to get the address where ETH needs to be sent to.
Set a gas limit of 2,6 mil and price it accordingly in order to have it processed by the network.
See Eth Gas Station for Safe Pricing at https://ethgasstation.info

NOTE: This gives all the tokens once funding is successful.

3.4.3 Milestone Funding Method

Once funding has started, visit https://blockbits.io to get the address where ETH needs to be sent to.
Set a gas limit of 2,6 mil and price it accordingly in order to have it processed by the network.
See Eth Gas Station for Safe Pricing at https://ethgasstation.info

NOTE: This gives a percentage of the tokens each time the team delivers on a milestone.

3.4.4 Marketing limited Public Sale

Marketing limited Public Sale Is a special pool which we created in order to help with raising funds for marketing the platform. It sells tokens at a fairly big discount, but comes with no returns in case of funding failure.

- Start Date: 1st of February 2018
- End Date: 10th of March 2018
- CAP is 300 ETH * is included in global Hard Cap
- 1 ETH = 20000 BBX
- Allocates tokens and transfers ETH to the platform instantly.

3.4.5 Token Supply

- Format: ERC20
- 3 % is allocated to the Advertising Bounty Program
- 57% is allocated to funding
- 40% is allocated to the project development team and is locked for the full duration of Milestone Development

3.4.6 Funding Goals

Minimum received ethereum for successful funding (Soft cap) is 5000 ETH. Maximum received ethereum (Hard cap) is 35000 ETH.

3.4.7 Sale Periods

PRE-ICO Funding Phase

- Start Date: 1st of February 2018
- End Date: 28th of February 2018
- PRE-ICO stops when a CAP of 7000 ETH is reached!
- 1 ETH = 9800 BBX
- PRE-ICO bonus 40

ICO Funding Phase

- Start Date: 10th of March 2018
- End Date: 1st of May 2018
- ICO stops when a CAP of 35000 ETH is reached!
- 1 ETH = 7000 BBX

NOTE: Final token supply is allocated based on the amount sold in funding!

3.5 Advertising Bounty Program

We offer an Advertising Bounty Program that will distribute 3% of total available token supply to anyone that wants to let the world know about our project.

In the same manner that the funding mechanism works, this is setup to be as fair as possible. In order to waive gas costs from participants they are asked to trust us and submit entries into the Bug Bounty Portal for validation and awarding.

Please see Technical Documentation - Advertising Bounty Program for details.

3.6 Bug Bounty Program

We offer a Bug Bounty Program that will pay out rewards to anyone that finds issues and alerts us about them.

Please see Technical Documentation - Bug Bounty Program for details.

4 Roadmap

4.1 Phase 1 - Proof of Concept

- Date: June 2017 - January 2018
- Technical Documentation,
- Functional Diagrams,
- Deployment Strategy and Flows
- Bounty Portal and Bounty Program Tools
- Android and iOS Mobile Notification Application
- Backend Application MVP
- On the Ethereum BlockChain
- 300+ Unit and Integration Tests
- Testnet deployments in different stages
- Platform identity - Logo and Design
- Campaign Ofering Whitepaper
- Campaign Landing Page

4.2 Phase 2 - Funding

- Date: February 2018 - May 2018
- Campaign Landing Page Launch
- Announcement
- Ask Me Anything (AMA) interviews and press releases
- PRE ICO - February 2018 - March 2018
- ICO - March 2018 - May 2018
- Token Allocation - Date: 2nd of May 2018

4.3 Phase 3 - Development

- Development Start: 5th of May 2018

4.3.1 Development Milestone 1

- Title: Minimalistic Platform
- Estimated Duration: 90 days
- Team expansion
- Swarm / IPFS Storage
- Platform Payload
- Campaign Details and News feed
- Campaign Message Boards
- Platform Web Application
- Campaign Page
- Campaign Status
- Campaign News Feed
- Campaign Management Tools
  - Proposal Viewing, commenting and voting
- Campaign CashBack
- Chats and or Message Boards
- Campaign Listing and filtering
- My Profile
- My Statistics
- My Contributions
- My Required Actions (Voting)
- MainNet / TestNet Testing environments
- Deployment Tools
- Application State Processing Daemon

NOTE: Minimum required functionality in order for token holders to be able to validate and vote on proposals.

4.3.2 Development Milestone 2

- Title: 3rd Party Launch Functionality
- Estimated Duration: 180 days
- Platform Web Application
- Campaign Page
- Campaign Status improvements
- Campaign Management Tools
  - Token holder Voted Delisting proposals
- Campaign Listing and filtering improvements
- Project Creation Wizard - v1
- Presents Basic choices already implemented
- BBT Token holder entry settings
- BBT Internal Funding Periods
- BlockChain Application Deployer
- Wizard Choice Validator
- Listing Linker
- Platform - Revenue Stream Storage Contract
- Mobile Application Update
- adds News Items for Listed Projects.

Nice to have:

- Basic Risk Indicators and Analysis

NOTE: Minimum required functionality to allow 3rd party projects to launch through the platform and allow token holders to participate in funding events that include discount programs.

4.3.3 Development Milestone 3

- Title: Code Upgrade Tools and Token Buyback
- Estimated Duration: 90 days
- Campaign Page
- Code Upgrade Tools with in platform code diff viewer
- Token Buyback functionality that uses funds in Revenue Stream Storage

NOTE: Minimum required functionality to allow Code Upgrades to be processed in order to enable Token Buyback for the main platform and launched children projects.

4.3.4 Development Milestone 4

- Title: Basic Risk indicators and Collaboration tools
- Estimated Duration: 90 days
- Campaign Page
- Campaign Risk indications and analysis
- Campaign listing and filtering based on risk indicators and scoring
- Project Creation Wizard - v2
- Collaboration Tools
- New Discount programs,
- New Funding algorithms

NOTE: Basic Risk analysis and indicators for projects and Collaboration tools for the Creation Wizard.

4.3.5 Development Milestone 5

- Title: Advanced functionality
- Estimated Duration: 90 days
- Project Creation Wizard - v3
- Funding Auction Bidding
- Campaign Page
- Advanced Risk indications and analysis

NOTE: Advanced functionality for project creation, risk analysis and indicators for project page details.

4.3.6 Development Milestone 6

- Title: Token Holder Upgrades
- Estimated Duration: 90 days
- Token holder initiated Code Upgrades that get paid from the Revenue Stream Storage Contract

NOTE: Allows token holders to propose upgrades and get paid for them.

4.3.7 Development Milestone 7

- Title: Full Decentralization
- Estimated Duration: 90 days

Full Decentralization Support

- ENS Ownership (ENS annual renewal payments)
- Storage Ownership with renewal

NOTE: Project gets prepared for completion, where no one owns it.

4.4 Phase 4 - Development Completed

From here on, project owner becomes a token holder, and any token holder can propose a code upgrade and vote for it.

5 The Team

Core members:

Micky Socaci	Main Developer
Mihai Iliescu	Security Expert / White Hat
Ionut Toader	Frontend Developer
@lynceus	Bussines Analyst / Software Developer
Radu Dumitru	Graphic / UX Designer
Vlad Morar	Video / Marketing Specialist
Arthur Birnbaum	Animation / Motion Graphics

6 Changes

1. Changed Token SCADA from "Market Decided Token Price" to "Selling a variable amount of tokens for a fixed price"
2. Added bonus of 40% in PRE-ICO.
3. Lowered the soft cap to 5000 ETH due to the ETH price appreciation on the market.
4. Increased Bounty program supply to 3% of total tokens
5. Changed funding period start / end times for a longer funding time
6. Added Arthur Birnbaum to team
7. Added Marketing limited Public Sale