Moonfish

[Working Draft]

true

March 9, 2018

Abstract

Over the past year we've seen a staggering amount of capital raised using token sales - also known as Initial Coin Offerings (ICOs). Thanks to emerging standards such as ERC20, ERC720 and NEP5 it's becoming increasingly easy to digitize assets and to gain liquidity on public Blockchains. However, doing a token sale has become increasingly complex due to the rapidly changing technological and legal landscape. The fact that 10% of all ICO capital raised in 2017 is in the hands of criminals illustrates the growing need for a secure and reliable token sale process. The goal of the Moonfish platform is to create open, secure and reliable software for doing token sales. All core Moonfish code is free, open source and publicly auditable. The Moonfish platform codifies the latest legal, technical and security best practices in a single end-to-end solution for token sale processes.

Background

On 30 April 2016 a bold attempt was made to launch the world's first Decentralized Autonomous Organization (DAO) on the Ethereum blockchain [1]. This was the first attempt at the creation of a new kind of token that would empower it's holders to exert control on the asset they owned. Unfortunately, this first attempt blew up spectacularly after a security flaw was exploited and millions of dollars were drained from the DAO. This incident resulted in the Ethereum Classic (ETC) / Ethereum (ETH) hard fork - one of the first of its kind. Even though the DAO was a failure, it showed the world how powerful a crowd sale on the blockchain could be. The era of the Initial Coin Offering (ICO) - or token sale - had started.

Fast forward to today (Q1 2018) and there have been many hundreds of ICOs to date. Startups in 2017 raised $5.6BN dollars using token sales, despite a success rate of only 48% [3]. Q1 2018

saw a slowdown in the crypto markets at large, but given the fact that 30% of all seed stage capital came from ICOs [4], it's likely that the ICO as a fundraising vehicle will sustain. Right now most prominent ICOs are centered around some form of decentralization platform, but ICOs are increasingly seen as a means to raise funds for any kinds of startup or even later stage company (reverse ICOs).

It is not unreasonable to assume the long tail of publicly traded tokens will include new kinds of assets such as real estate, vehicles, collectables or even living animals [5]. As a result new ICOs have sprung up that attempt to create marketplaces centered around a given asset type.

Currently the crypto space is undergoing a Cambrian explosion of marketplaces. It's questionable whether we really need that many derivative marketplaces. Are these new marketplaces really contributing to an increase of overall asset liquidity? Or are they more like data silos impeding liquidity? Only time will tell.

An alternative narrative is that public blockchains - and in particular Ethereum - are perfectly suitable to incorporate any digital asset. The maturing contract standards - in particular ERC20 and ERC721 [7] - are an example of how much easier it has become to deploy assets directly on the public blockchains. Also, on other upcoming blockchain platforms such as NEO there are promising new standards such as NEP5 [9] and novel methods of allowing users to participate in these ICOs.

In order to facilitate the offering of new assets on public blockchains we need secure and reliable tools that make this process easy for both the seller and the buyer. 10% of all funds earmarked for ICOs in 2017 are in the hands of cyber criminals [13]. In addition to reducing security risks, doing a token sale has become a much more complex endeavor. Security best practices need to be followed, expectations with potential investors need to be managed, the technology needs to be sound, and fast changing regulatory requirements need to be met.

There are a variety of ICO platforms [10] that attempt to make these token sales easier, but ironically most employ a proprietary model and a new marketplace middleman is formed. It is Moonfish's goal to provide open, secure, publicly auditable and reliable open source software to facilitate token sales.

The Moonfish Platform

Typically the focus of token sales tools is to ease the creation and deployment of the smart contracts related to a token sale, but there is a lack of mature tools for managing the token sale end-to-end.

IMAGE

The Moonfish platform provides an end-to-end solution for all stages in the token sale process:

IMAGE

Token Sale Flow

Each token sale has their own crowd sale dynamics coded into the smart contracts. For example,

some token sales provide bonuses to those who participate during certain time periods. Additionally, there have been a wide variety of different user flows in acquiring these tokens in the sale process. These user flows can be categorized as follows:

A) Uncontrolled: Disclose Smart Contract address, and allow anyone to participate by sending funds.

B) Uncontrolled, but Tracked: Solicit basic information (e.g. email, acceptance of terms, and ETH address) and subsequently reveal a Smart Contract address that can be used for participation.

C) Semi-managed: Provide a limited login experience to facilitate communication and KYC compliance, but use a public Smart Contract address to participate.

D) Managed: Provide a full featured login experience to any applicant and then manage a wallet (private key and public key) for the user to participate.

Most of the early token sales were done using Flow A and B. There are numerous downsides to these approaches, such as underlying Blockchain congestion, limited means of communication, KYC compliance risk, and frustration on behalf of aspiring participants when limits are reached.

Flow D is used by a lot of popular ICOs. The benefit of managing wallets is that it makes it easier to allow for Bitcoin and other non-Ethereum currencies to be used for ERC20 token offerings. However, a very large downside is that funds are managed centrally by the token sellers, which means that a single hack can result in a massive loss of funds.

Moonfish's core token sale flow is based on Flow C - with added best practices to minimize security risks.

Applicant Management

In 2017, a total of $115M Ethereum was phished from ICO participants [14]. Safe-harboring communication between applicant and the token sellers is paramount. More exactly, there are two kinds of breaches that need to be protected against:

A. Loss of personal applicant data. B. Spoofed official communication to applicants.

In order to minimize breach A - Moonfish will not store any user generated passwords. Instead of providing applicants with an email/password login, we will only use second factor authentication to obtain access. This is initially done by obtaining a temporary session token - also known as a magic token - that is sent via email. At a later stage, we can make this process two factor by including secondary authentication mechanisms such as Google Authenticator and SMS.

In order to minimize breach B - Moonfish will generate a unique mnemonic phrase for each user that can be used to verify the authenticity of the communication. The Ocean Protocol's recent ICO used this clever mechanism to minimize

the potential of spoofed communication with the applicants [15].

In addition to this, Moonfish will integrate with third party email providers such as Postmark [16] that support additional identity and verification measures such as DKIM, SPF and DMARC [17].

Token Sale Portal & Administration System

The Moonfish token sale solution includes a default portal. This portal provides all promotional information about the token sale as well as the current status and parameters of the token sale process.

This portal will include best practice placeholder legal information such as Privacy Policy, Terms of Token Sale and additional regulatory warnings.

To increase the security of the portal, anti-phishing warnings and confirmations can be added as well as best practices for deployment behind an anti-DDOS firewall such as Cloudflare [20].

The user interface for applicants, the portal and the administration system is a self contained app that interfaces with a JSON API backend. This frontend application is implemented using React [21], Redux [22] and Semantic UI [23]. The backend system is fully controllable through well tested and documented JSON APIs.

Whitelisting Mechanics

It's become common practice for token sales to have a period of whitelist registration before starting the active token sale period. During this period, applicants can register to the whitelist and they will receive updates from the token sale administrators when participation in the token sale is possible. Having a whitelist of applicants allows for a token sale process that's more organized and controlled.

IMAGE

There are numerous configurations possible here. Some may choose to limit the number of applicants, and not allow any further registrations. Some may choose to allow oversubscribing of the whitelist so that applicants can participate in a future funding round. Or some may choose to also limit the number of whitelist applicants based on the amount of capital that's "soft-circled". Moonfish will support a plethora of different configurations here.

Open Software

The core Moonfish platform is completely free and open source. This allows us to strengthen the platform by harnessing the expertise of the open source community. Also, all source code is completely auditable by anyone that chooses to use the Moonfish platform for their ICOs. As is increasingly common, in the future, Moonfish can offer bounties for bug discovery and suggested patches.

Other Security Considerations

Moonfish will provide an open forum for the developer community to strengthen its security. In addition to the aforementioned security and reliability decisions, we've added the following requirements:

- Full unit test coverage of all business logic and APIs.
- Continuous integration of unit tests, listing and test coverage measurements.
- Enforced ES linting on all JavaScript and Node.js code.
- Administrative password hashed using BCRYPT password hashing best practice [24].
- Automatic checks for misconfiguration (default keys) for new deployments.
- Client-server communication using JSON Web Tokens [25]. Different private keys are used for admin accounts.
- Both JWT and magic tokens expire within a short time period (2 hours and 1 hour respectively).
- All solicited input fields are validated and that validation is unit tested.

Evolving Best Practices

The crypto and in particular the ICO space is a very nascent sector that's still developing it's best practices. These practices span across many different disciplines such as IT, software, marketing and legal.

It is the aim of Moonfish to provide a framework for discussion of these practices and to actively codify these practices into working systems.

A good starting point for this is providing templates for peripheral matters such as:

- Default ERC20 Smart Contracts. The approach here is to take what's best out there - such as the excellent work being done by the Zeppelin foundation - and incorporate it [26].
- Legal templates for different kinds of crowd sales.
- Technical white paper template. The white paper you're reading right now is an open source template freely available to anyone.
- The Moonfish token sale website is itself available in source code. It's the default portal that's available in the Moonfish token sale application. In the future additional "themes" and skins can be made available.

Moonfish Tokens

In the past year token offerings have become increasingly ambitious. There are countless large ICOs that have raised vast amounts of capital on little more than a sexy white paper with barely any working code. It is likely that future token offerings for startups are going to look more like traditional funding rounds, where early rounds are smaller and become larger as the project proofs out its ability to execute [27].

In the spirit of this, we are planning a small initial token pre-sale for Moonfish. The goal of this "Moonfish PoC Token Micro-Sale" is twofold: 1. Prove out that we can do a token sale with the Moonfish software (ICO the ICO software if you will); 2. Get some modest funding in place to support the development efforts of the project.

The core Moonfish platform is open source and will remain open source. The Moonfish PoC tokens will not have any baked in tokenomics initially. However, once we've proven our the MVP (see Roadmap), the goal is to develop a commercial extension of the platform, at which point we will introduce tokenomics to align incentives. These Moonfish PoC tokens will convert into this secondary offering. The exact details of the tokenomics and secondary offering mechanics are to be determined as the roadmap evolves.

Roadmap

Phase 1: Proof of Concept Development

Before undertaking any token sale we want to get a first version of the software up and running. This version will at the minimum include the security best practices and considerations mentioned herein. In addition to this, it will have a first cut of the whitelisting mechanism and participation logic needed for basic token sales.

Phase 2: Moonfish PoC ICO

This will be a small capped token sale for Moonfish PoC Tokens. We will be using the Moonfish platform to do this token sale. Once completed, it will be the first ICO performed using the Moonfish software. See "Moonfish Tokens" for more details about these tokens.

Phase 3: Proof of MVP

This phase is the "rinse and repeat" stage where we solicit feedback from the marketplace. The goal is to add additional capabilities and security features to the Moonfish software and to have it used by future token sales. Once we're seeing steady usage of the software we will have proven out our Minimum Viable Product.

Phase 4: Tokenomics Development, Further Decentralization Roadmap & ICO

The MVP phase will give us a lot of feedback from the market. Based on this we can define a monetization strategy and longer term roadmap that incorporates tokenomics. This will involve a secondary token sale where we convert Moonfish POC tokens into the new token.

References

[1] V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," 2014 [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[2] "The dao (organization)" [Online]. Available: https://en.wikipedia.org/wiki/The_DAO_(organization)

[3] "Only 48% of icos were successful last year — but startups still managed to raise $5.6 billion" [Online]. Available: http://www.businessinsider.com/how-much-raised-icos-2017-tokendata-2017-2018-1

[4] "2017: A year in review - initial coin offerings" [Online]. Available: https://hackernoon.com/2017-a-year-in-review-initial-coin-offerings-91ec1c7367a5

[5] "These 3 cryptocurrencies could change how we look at real estate" [Online]. Available: https://steemit.com/cryptocurrency/@markjackson1989/these-3-cryptocurrencies-could-change-how-we-look-at-real-estate

[6] "Sentinel chain" [Online]. Available: https://sentinel-chain.org/

[7] "ERC20 token standard" [Online]. Available: https://theethereum.wiki/w/index.php/ERC20_Token_Standard

[8] "The anatomy of erc721" [Online]. Available: https://medium.com/crypto-currently/the-anatomy-of-erc721-e9db77abfc24

[9] "NEP5 proposal" [Online]. Available: https://github.com/neo-project/proposals/blob/master/nep-5.mediawiki

[10] "Cryptonomos ico marketplace" [Online]. Available: https://cryptonomos.com/

[11] "Waves platform" [Online]. Available: https://wavesplatform.com/

[12] "Blockstarter ico platform" [Online]. Available: https://blockstarter.co/

[13] "Coinlaunch ico platform" [Online]. Available: https://coinlaunch.co/

[14] "The rise of cybercrime on ethereum" [Online]. Available: https://blog.chainalysis.com/the-rise-of-cybercrime-on-ethereum/

[15] "Ocean protocol" [Online]. Available: https://token.oceanprotocol.com/

[16] "Postmark security" [Online]. Available: https://postmarkapp.com/why/security

[17] "DKIM" [Online]. Available: https://postmarkapp.com/guides/dkim

[18] "SPF" [Online]. Available: https://postmarkapp.com/guides/spf

[19] "DMARC" [Online]. Available: https://postmarkapp.com/guides/dmarc

[20] "Cloudflare" [Online]. Available: https://www.cloudflare.com/ddos/

[21] "React" [Online]. Available: https://reactjs.org/

[22] "Redux" [Online]. Available: https://redux.js.org/

[23] "React semantic ui" [Online]. Available: https://react.semantic-ui.com/introduction

[24] "BCrypt: Hash passwords correctly" [On-

line]. Available: http://davismj.me/blog/bcrypt/

[25] "JSON web tokens" [Online]. Available: https://jwt.io/

[26] "OpenZeppelin solidity contracts" [Online]. Available: https://github.com/OpenZeppelin/zeppelin-solidity

[27] "ICOs, don't bite off more than you can chew," 2017 [Online]. Available: https://hackernoon.com/icos-dont-bite-off-more-than-you-can-chew-d658aae9579e

[28] "ICO 'rounds' are coming" [Online]. Available: https://techcrunch.com/2018/01/31/ico-rounds-are-coming/