Moonfish - An Open Platform for Token Distribution

[Working Draft]

Dominiek Ter Heide
Rekall.ai

Kirk McMurray
Rekall.ai

March 20, 2018

Abstract

In 2017 a staggering amount of capital was raised via token sales also known as Initial Coin Offerings (ICOs). By utilizing emerging standards such as ERC20, ERC720 and NEP5 it's becoming increasingly easy for companies to digitize assets and gain liquidity on public blockchains. However, doing a token sale has also become increasingly risky due to a rapidly changing technological and legal landscape. The fact that an estimated 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 in a risk-free manner for both the token issuer and token purchaser. The first version of Moonfish is an open source software that can be audited, configured and deployed by any software developer. This solves the imminent need for secure, open, standardized and reliable token sale software. However, it is the long term goal of the Moonfish project to create a blockchain-powered network that provides a comprehensive ecosystem for token sales.

1. Background

On 30 April 2016 the world's first Decentralized Autonomous Organization (DAO) was launched on the Ethereum blockchain [1]. This was the first attempt at the creation of a new kind of token that would empower its holders to exert control over the asset they owned. Unfortunately, this gamble blew up spectacularly after a security flaw was exploited and $150m worth of ether was drained from the DAO. This single hack threatened the existence of the entire Ethereum project and resulted in the contentious Ethereum Classic (ETC) / Ethereum (ETH) hard fork. Even though the DAO was a failure, it did show the world how powerful a crowd sale on the blockchain could be. The era of the Initial Coin Offering (ICO) or token sale had begun.

Fast forward to today (Q1 2018) and we have already seen many hundreds of ICOs to date. Startups in 2017 raised $5.6bn dollars using token sales, but shockingly an estimated 48% of these sales have already resulted in failures [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 kind of startup and even later stage companies (reverse ICOs) [5].

Moreover, we expect to see that the long tail of publicly traded tokens will represent new kinds of assets such as real estate, vehicles, collectables or even living animals [7]. As a result, new ICOs will continue to spring up that attempt to create marketplaces centered around a given asset type.

However it's questionable whether we really need this many derivative marketplaces. Are these new marketplaces really contributing to an increase of overall asset liquidity and value? Or are they more like data silos built around tokens that don't have a real reason to exist?

An alternative solution 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 [9] - have made it much easier to deploy assets directly on existing public blockchains. Also, other upcoming blockchain platforms (NEO, EOS, Qtum, Tezos, and others) are promising new standards such as NEP5 [11] and novel methods of allowing users to participate in these ICOs.

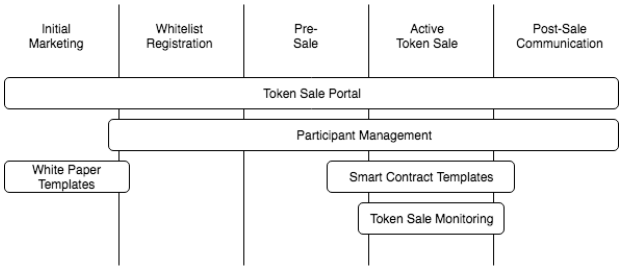
In order to facilitate the offering of new assets on public blockchains we need secure and reliable tools that make this process easy and safe for both the seller and the buyer. 10% of all funds earmarked for ICOs in 2017 are in the hands of cyber criminals [13]. A company newly entering this space faces a host of novel challenges. 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 [12] that attempt to make token sales easier, but ironically most employ a proprietary model, which just creates a new marketplace middleman. Moonfish's goal is to provide open, secure, publicly auditable and reliable open source software to facilitate token sales in a simple, risk-free manner. Moonfish is accessible to anyone and at the same time true to the spirit of the space.

2. 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 process end-to-end.

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



2.1 Token Sale Flow

Each token sale has its own crowd sale dynamics coded into 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 for acquiring 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 either 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 has recently been 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.

2.2 Applicant Management

In 2017, a total of $115m Ether was phished from ICO participants in various ways by scammers [16]. Safe-harboring communication between applicant and the token sellers is paramount. Specifically, 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 [17].

In addition to this, Moonfish will integrate with third party email providers such as Postmark [18] that support additional identity and verification measures such as DKIM, SPF and DMARC [19].

2.3 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.

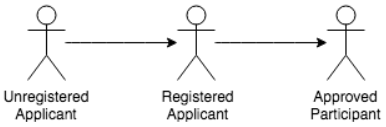
To increase the security of the portal, anti-phishing warnings and confirmations can be added as well as best practices for deployment behind an anti-DDOS firewall such as Cloudflare [22].

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 [23], Redux [24] and Semantic UI [25]. The backend system is fully controllable through well tested and documented JSON APIs.

2.4 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.



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.

2.5 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.

2.6 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 [26].
- Automatic checks for misconfiguration (default keys) for new deployments.
- Client-server communication using JSON Web Tokens [27]. 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.

2.7 Evolving Best Practices

The crypto and in particular the ICO space is a nascent sector that's still developing its best practices. These practices span many 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. Moonfish will provide a number of templates and default technical solutions across areas such as:

- Default ERC20 Smart Contracts. The approach is to take the standards available, such as the OpenZeppelin smart contract framework - and incorporate them [28].
- Legal templates for different kinds of crowd sales that take into account the quickly developing regulatory landscape [29]
- Technical white paper template. (The white paper you're reading right now is an open source template freely available to anyone.)
- The token sale website. 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 will be made available.

3. Towards a Decentralized Token Sale

Today, the transaction mechanics for buying tokens are handled primarily by existing blockchains such as Ethereum and standards such as ERC20, but most other aspects of the token sale process are handled through custom centralized software.

The first version of Moonfish is open source software that can be configured and deployed by any software developer. This solves the pressing need for secure, open, standardized and reliable token sale software. However, the long term goal of the Moonfish project is to evolve these OSS instances into a DLT-powered network that provides an ecosystem for token sales.

Creating a decentralized infrastructure for end-to-end token sales has numerous benefits:

- Increased data security, integrity and resilience.
- Secure and signed communication to counteract cybercrime.
- Enhancing KYC by integrating with emerging Blockchain-powered person identification platforms and self-sovereign identity. [31]
- Leveraging the network to create social network effects to spread information about current token sales.
- Increased potential for automation and derivative investments (for example buying into bundles or indices of certain asset classes).
- Leveraging the new wave of cross-blockchain interoperability [34]

In order to incentivize the token sale ecosystem, there are numerous tokenomics mechanisms possible. At the basic level, the network could require a fee from token sellers to make use of the network. This fee (paid in Moonfish tokens) could get distributed among Moonfish token holders. More interestingly, there are many secondary fees that could be built into the mechanics. For example, token sellers could pay a promotional fee to increase visibility and propagation through the network. Or finders fees or affiliate fees could be paid to participants that actually promote a sale, etc.

Today, most token sales are done by organizations with legal entities that are grounded in the real world. These entities are subject to all the

relevant securities laws in their respective countries. However there are ongoing attempts at creating completely virtual and anonymous Decentralized Autonomous Organizations, organizations that exist online in a completely digital jurist diction.

DAO's have yet to come to full fruition, but they are the natural end result of distributed ledger technology, and they will play an important role in the evolution of the blockchain world [37]. The Moonfish decentralized token sale network can be instrumental in the march towards true DAOs and a self-sovereign digital republic.

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] "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

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

[7] "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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[23] "React" [Online]. Available: https://reactjs.

org/

[24] “Redux” [Online]. Available: https://redux.js.org/

[25] “React semantic ui” [Online]. Available: https://react.semantic-ui.com/introduction

[26] “BCrypt: Hash passwords correctly” [Online]. Available: http://davismj.me/blog/bcrypt/

[27] “JSON web tokens” [Online]. Available: https://jwt.io/

[28] “OpenZeppelin solidity contracts” [Online]. Available: https://github.com/OpenZeppelin/zeppelin-solidity

[29] “A securities law framework for blockchain tokens” [Online]. Available: https://www.coinbase.com/legal/securities-law-framework.pdf

[30] “Howey test for blockchain tokens” [Online]. Available: https://docs.google.com/spreadsheets/d/1QxOV2dgxO3C_TyVE0-41ZwLlzPmB-EE1NNshJGuedCU/edit#gid=0

[31] “Civic secure identity ecosystem” [Online]. Available: https://www.civic.com/

[32] “Using blockchain for identity management” [Online]. Available: https://www.civic.com/

[33] “Identity as a bottleneck for blockchain” [Online]. Available: https://blockchainhub.net/blog/blog/decentralized-identity-blockchain/

[34] “Enabling crypto networks to become cross-chain using witnet” [Online]. Available: https://medium.com/witnet/enabling-crypto-networks-to-become-cross-chain-using-witnet-2c8d3731fcb5

[35] “Atomic action: Will 2018 be the year of the cross-blockchain swap?” [Online]. Available: https://www.coindesk.com/atomic-action-will-2018-year-cross-blockchain-swap/

[36] “Cosmos network: Internet of blockchains” [Online]. Available: https://cosmos.network/

[37] “Introducing the aragon network” [Online]. Available: https://blog.aragon.one/introducing-the-aragon-network-20b998e2caba

[38] “What is dao may never die: The dao, daos, and the future of organization” [Online]. Available: https://blog.gnosis.pm/what-is-dao-may-never-die-the-dao-daos-and-the-future-of-organization-4d3b7e7c3f50

[39] “AI daos, and three paths to get there” [Online]. Available: https://blog.bigchaindb.com/ai-daos-and-three-paths-to-get-there-cfa0a4cc37b8

[40] “How to create the future of decentralized autonomous organizations” [Online]. Available: https://blog.singularitynet.io/how-to-create-the-future-of-decentralized-autonomous-organizations-7919d4e5ce36