# Ventureum: A Milestone-driven Community-governed Crowdfunding Protocol for Blockchain Projects

**Timothy Wang, Nathan Liu, Lucas Gu**
dev@ventureum.io

Version 0.1.28

## Abstract

**Ventureum** is an innovating crypto-crowdfunding protocol specifically designed for the Ethereum ecosystem to provide better control for investors over blockchain projects. This protocol implements a **Milestone-Driven Funds Management Module**. Milestone-Driven Funds Management Module acts as a Decentralized Autonomous Organization (DAO), which releases funds to project founders only if milestone deliverables have been delivered on time. It consists of a set of smart contracts, with which investors can vote to release or delay milestone payments. In the event that project promises are not met, investors can vote for a refund. The Milestone-Driven Funds Management Module is completely open source, and any blockchain projects can choose to integrate it into their own project by themselves without the Ventureum dev team's endorsement. If the founders of a blockchain project want the endorsement from the Ventureum team on their usage of the Milestone-Driven Funds Management Module, we will perform audits and security reviews of the source codes they deploy, and the use of Ventureum Network Token (VTH) to activate ETH refund is mandatory.

# Contents

# 1 Introduction

## 1.1 Background

Initial coin offering (ICO) or Token Sale is a way of crowdfunding via use of cryptocurrency[1]. The process of a token sale involves a project founder issuing cryptographic tokens and distributing the tokens to investors and contributors of the project as a representation of a stake or interest in the project. A blockchain project usually involves technical innovations for blockchains (Ethereum, EOS) or various application scenarios of blockchain + X, such as blockchain + Instant Messaging (Status), or blockchain + Identity Verification and Protection (Civic), etc.

Token sales provide unique features and more flexibility to blockchain project founders and investors, compared to traditional capital funding mechanisms such as Venture Capital or Initial Public Offering. First, investors use cryptocurrencies, such as Bitcoin, Ether (ETH) instead of fiat currencies to participate in a token sale. Second, the exclusion of expensive intermediaries, such as investment banks, reduces the cost of capital funding and creates a fast and direct channel to deliver the committed capital from investors to project founders. Third, the tokens issued in a token sale can be traded immediately or shortly after the token sale period is over, thus creating high liquidity for investors to take profit and exit their positions. This is in sharp contrast with traditional venture financing in which early investors have almost no measure to exit shortly after they have committed their capital. These features combined with the breakthrough of blockchain technologies, especially the fast evolving Ethereum ecosystem, have made token sales grow abruptly from its inception in 2013 to a phenomenal capital market wonder in the first half of 2017 (Figure 1)[2].

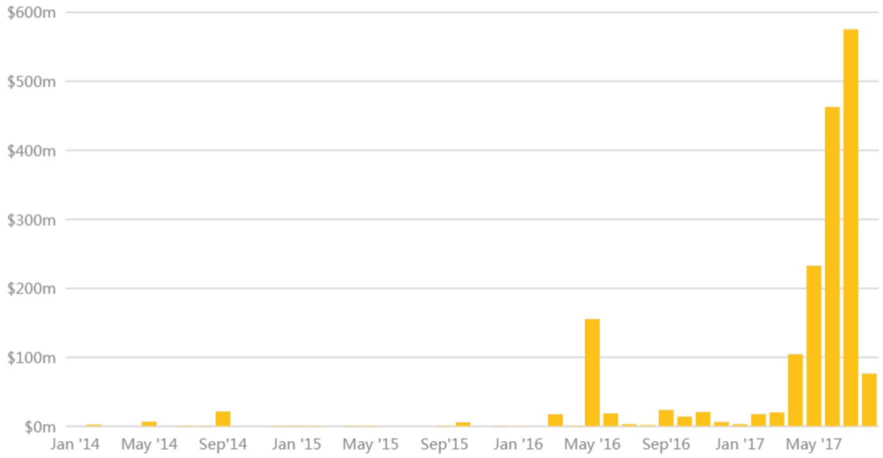

Figure 1: Monthly New Token Sale Funding (source: www.coindesk.com/ico-tracker/)

## 1.2 Problem Overview

However, the cryptocurrency world, including token sales, is still a largely unregulated territory that unfortunately provides rich soil for scam projects[3]. ICOrating.com lists a prolonged list of scam or Ponzi blockchain projects[4]. CHAINANALYSIS estimated that phishing, Ponzi schemes, and other scams account for about 10% of ICOs[5], and several cryptocurrencies have been announced as illegal by regulatory bodies across countries ([6, 7]). Another big issue is, even for blockchain projects with true motivation and goals, after receiving excessively large amounts of funding during crowdsales, the project founders have little to no incentive to deliver their products, as the investors have no voice or power to influence the progress of the projects[8].

The explosive growth of token sales has drawn close attention from the regulatory bodies of securities and finance across countries[9, 10, 11]. If the savage growth of token sales, especially the proliferation of scam token sales, continues and no self-regulatory mechanism emerges, it will be only a matter of time before token sales, and even the whole cryptocurrency world, are hit in a hard way. Regulatory bodies could unleash harsh control over token sales, or even ban them altogether in their jurisdictions.

It is a pressing call for a self-regulating mechanism or platform for token sales for anyone who wants the long-term existence and prosperity of crypto-token crowdfunding.

### 1.3 Ventureum: A Solution to Token Sale Self-regulation

To address the pressing issue of lack of self-regulation in token sales, the Ventureum team envisioned a mechanism of milestone-driven based funds management, implemented with the very spirit of Decentralized Autonomous Organization (DAO), to protect the interest of investors. The essential idea is that risk control over projects can only be realized by mobilizing the decision power of the whole community of investors with the help of open sourced smart contracts running on the Ethereum blockchain. To put it simply, investors won't betray themselves, and open sourced code does not lie.

The Ventureum team is fully aware of some crowdfunding platform competitors who claim to provide risk control over token sales. Yet, to our best knowledge, all of them rely on human effort (mostly the staff of their own crowdfunding platforms or a centralized governing body such as a board) to make decisions and filter out fraudulent projects, and most importantly, to manage funds. Again, this kind of crowdfunding platform works against the very spirit of DAO, and does not entitle investors to their deserved voice and power to monitor and influence the progress of projects and the release of funds. In the worst-case scenario, they could collude with project founders and harm investors' interests by pretending to have performed their due diligence and investigations.

The Ventureum project is the first ever proposed solution to self-regulating token sales, implemented in a decentralized way with total transparency. A benefit of the Ventureum protocol is the network effects it creates:

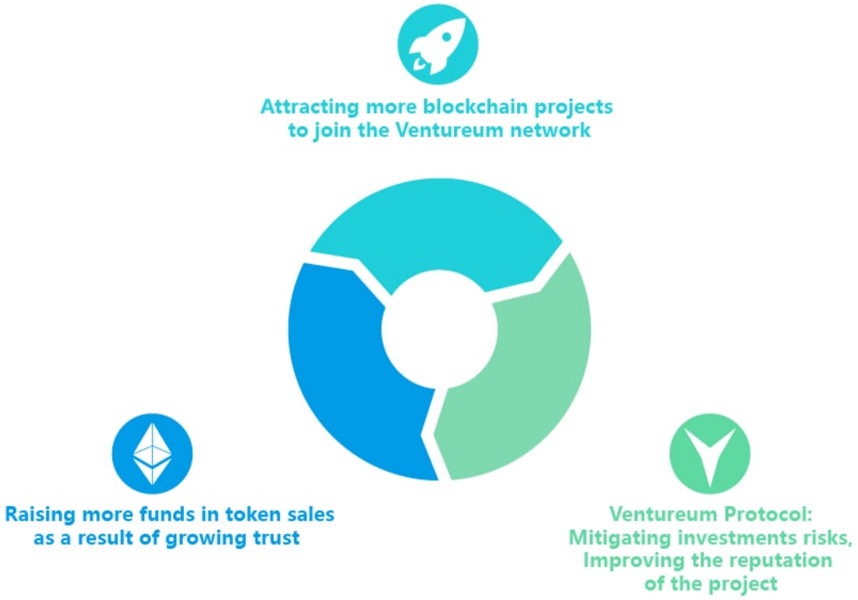
Attracting more blockchain projects
to join the Ventureum network
Raising more funds in token sales
as a result of growing trust
Ventureum Protocol:
Mitigating investments risks,
Improving the reputation
of the project

Figure 2: Network Effects

In the following sections, we present the technical details of the **Milestone-Driven Funds Management Module**. An elaborated description of the Ventureum token (VTH) allocation and the roadmap of development is also presented in Section 4.2 and 7.

## 2 Milestone-Driven Funds Management

One of the major problems of existing ICOs is that investors have no control over how funds are used. For instance, investors who participate in ICOs can be taken advantage of because usually they do not have voting rights over projects. Worst of all, after receiving excessively large amounts of funding during crowdsales, project founders have little to no incentive to deliver their products. Another critical issue is that it is difficult for inexperienced investors to distinguish legitimate projects from projects designed to be exit scams for their founders. These exit scam projects have caused investors to lose a large amount, or even all, of their investments. Without having a well-defined set of milestones, performance metrics, and independent auditors, an ICO is more of a gamble for investors.

To mitigate these issues, we propose **Milestone-Driven Funds Management** to protect investors. One of the major contributions of this system is the ability to refund investors' initial investments (partially) if project founders failed to complete milestone objectives. Voting procedures are used to determine whether the objectives of a milestone have been met or not.

Funds raised during token sales is first transfered from token sale contracts to **Milestone-Driven Funds Management Contract**, which then either (1) releases funds to project founders, or (2) refunds investors.

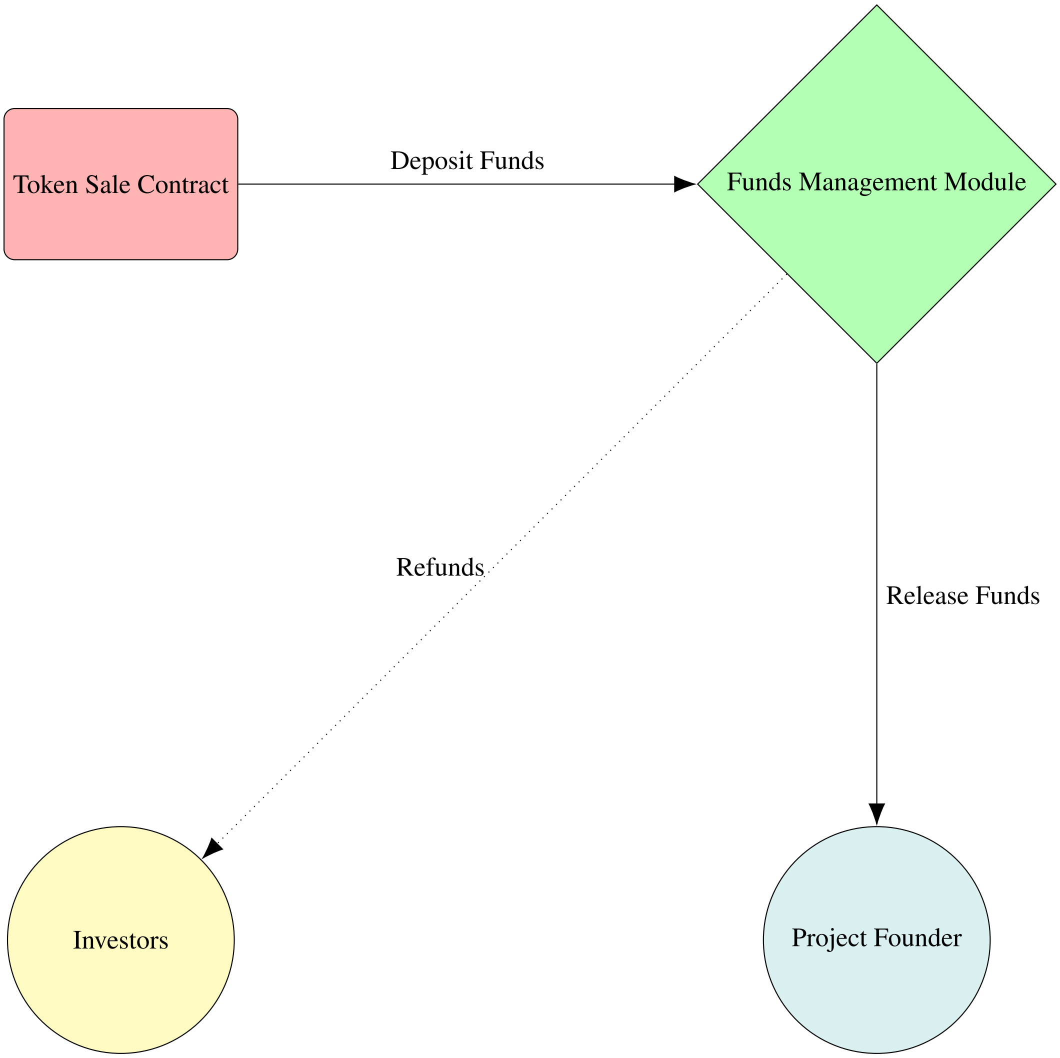

Figure 3: Funds Management Module Workflow

Before we start, it is necessary to have a few definitions:

**Definition 2.1.** *Milestone Node*
*A* ***milestone node*** *is represented by a tuple* $(\mathbf{d}, \mathbf{t_{ttc}}, \mathbf{p})$, *where* $\mathbf{d}$ *is a description of objectives,* $\mathbf{t_{ttc}}$

*(**Time-to-completion**) is the maximum amount of time required to complete theses objectives, and* $\mathbf{p}$ *is the percentage of total funds locked inside this milestone.*

**Definition 2.2.** *Investor*
*An investor is represented by an address that participated in a **Token Sale** of a blockchain project.*

### 2.1 Milestone Structure

In the simplest form, each milestone node is composed of data and a reference (in other words, a link) to the next milestone node in the sequence in chronological order.

**Example 2.1.** *Example of a Milestone List*

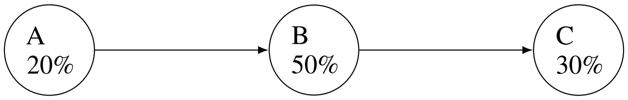

Figure 4: Example of a Milestone Linked List

Each milestone node points to the next milestone node. Percentage of total funds ($\mathbf{p}$) for a milestone is also shown below its label.

Suppose project founders failed to complete milestone B, then the funds of milestone B will be returned to investors. We continue moving forward on a milestone list even if some of them failed. In this example, 50% of total funds are refunded. The refund result is shown below:

**Example 2.2.** *Refunds of a Milestone List*

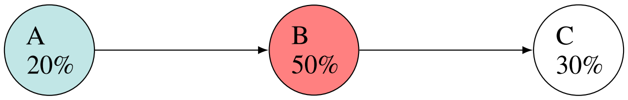

Figure 5: Refunds of a Milestone Linked List

Funds locked in nodes colored in red are returned to investors.

### 2.2 Milestone States

Let $t_{due}$ denote the due date of a milestone. $W$ stands for 1 Week. A milestone node has the following states:

- **In Progress** (Starting state)
  Developers are working on this milestone. At $t_{due} - W$, **Voting Period** automatically starts and the milestone state changes to **Voting Period**.
- **Complete**
  This period begins immediately after **Voting Period** if investors have approved the decision to mark this milestone complete. Funds locked are (partially) released to the project owners (See more details in Section 3.2). Investors who voted 'Reject' are eligible for a refund. This period lasts for one week.
- **Voting Period (Voting for Completion)**
  **Voting Period** automatically starts at $t_{due} - W$, and ends at $t_{due}$. Investors vote to decide if the milestone objectives are met. This voting period lasts for one week.
- **Refund Period (Failure to Meet Milestone Objectives)**
  This period automatically starts at $t_{due}$ if a majority of investors vote for rejection in **Voting Period**. Investors are able to withdraw funds locked inside the milestone before the period ends. The amount of funds refunded is proportional to the number of tokens (details can be found in Section 3.2) held by an investor. This period lasts for one week.

Let **IP**, **VP**, **RP**, **C** denote state **In Progress**, **Voting Period**, **Refund Period** and **Complete** respectively. We represent the above state transitions with a finite-state machine:

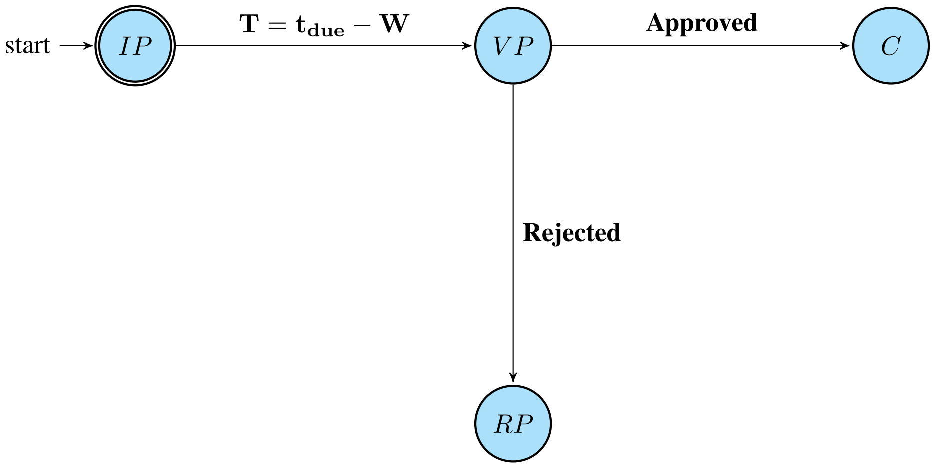

Figure 6: Workflow of Milestone-Driven Funds Management

## 3 Voting

The voting method is used to determine state transitions covered in Section 2.2. To prevent malicious manipulations by project founders, whales, and exchanges, project founders are required to issue two classes of tokens:

- Class A — Issued and sold to regular investors during a token sale. Held by regular investor with regular voting rights and eligibility for a refund.
- Class B — Not issued and sold to regular investors during a token sale, e.g., tokens held by project founders, or tokens unsold during a token sale. No voting rights and ineligibility for a refund.

**There is *no difference* between Class A and Class B tokens in terms of their token functions.** Class A tokens and Class B tokens are merged into **one type of tokens** when a project finishes.

Also, token holders are required to stake Class A tokens before **Voting Period** to be eligible to vote. The minimum staking length is set to 30 days. Specifically, in order to participate in a vote with X Class A tokens, token holders must send X Class A tokens to the staking contract controlled by the Milestone-driven Funds Management Module, and stake for at least 30 days before **Voting Period**. The staked tokens are returned to investors after the voting (Specifically, tokens are returned when milestone state transits to either state **Complete** or state **Refund Period**.

Specifically, a vote of an address **addr** is weighted by the number of Class A tokens staked for at least 30 days, normalized by the total number of Class A tokens The voting weight $W$ of an address for a vote is defined as

$$W(\text{addr}) = \frac{\text{Class A Tokens Staked by the Addr}}{\text{Total Number of Class A Tokens}} \tag{1}$$

The voting weight $W$ is used to determine the final outcome of a vote. Abstention is casted as "Approval". The decision to release milestone payments is approved if majority ($\geq 50\%$) of investors support it. The exact refund amount depends on the number of Class A tokens staked.

### 3.1 Approval

In the event of approval, we transit to state **Complete**. Funds locked inside the milestone are released to project founders.

### 3.2 Rejection and Refund

In the event of rejection, we transit to state **Refund Period**. The refund amount is proportional to the number Class A project tokens staked.

**Example 3.1.** *Refund Calculation I*
*Suppose the average crowdsale price of XYZ tokens is 1000 XYZ/ETH. Assuming Tom staked 5000 XYZ Class A tokens for a vote, and there are total of 100000 XYZ Class A tokens staked. Suppose the milestone corresponding to the vote has 5000 ETH locked. Then, these XYZ tokens entitle Tom to a refund of maximum*

$$\frac{5000}{100000} \times 500 = 25\,\mathit{ETH} \tag{2}$$

#### 3.2.1 A Special Case

In the event of cryptocurrency bear market, investors cannot make rational decisions regarding the voting procedure. In this situation, project founders are eligible to merge the current milestone with the next one in the case of rejection. Specifically, funds locked inside the current milestone is moved into the next milestone, and milestone objectives are added into the next milestone. Once the merge procedure is invoked by project founders, we immediately move to the next milestone and proceed as usual. If the next (merged) milestone is approved, funds locked inside that milestone are released to the project founders.

If the merged funds are greater than 50% of total funds, or there is only one milestone left (assuming this milestone is the result of the previous merge), then project founders are able to freeze the milestone process for a maximum of 6 months. Freeze procedure can only be initiated once. During the freeze period, project founders are provided with a one-time option to resume the milestone process, once the milestone process is restarted, another voting period for this milestone will begin, and proceed as normal.

We will open source our bear market indicator to the public in Ventureum 1.0 release.

In the future, the freeze procedure may be replaced by arbitration which will be provided by top auditing firms, such as PwC.

## 4 Ventureum Network Token (VTH) - An ERC20 Token to purchase refundable Class A Tokens

Ventureum Network Token (VTH) is required to purchase refundable Class A tokens

### 4.1 Eligibility for Purchase of Class A tokens

To purchase X class A tokens in a Ventureum compatible crowdsale, investors need to transfer a one-time non-refundable activation fee: 0.01X (or 1% of X) ETH worth of VTH.

Formally, obtaining up to **X** ETH worth of Class A tokens requires paying

$$0.01\hat{p}X \ \text{VTH} \tag{3}$$

where $\hat{p}$ is **Approximated VTH Price** in term of ETH. Initially, $\hat{p}$ is set to be the average Ventureum crowdsale price of VTH.

In a long term, $\hat{p}$ will be periodically and automatically updated to ensure that fees will not exceed 3% of the cost of purchasing Class A tokens, in terms of ETH value.

**Example 4.1.** *Class A Token Calculation I*
*For example, Alice wants to cover up to 100 ETH of her investment and would like to purchase 100 ETH worth of Class A tokens. The* ***Approximated VTH Price*** *$\hat{p}$ is 50 VTH/ETH. She needs to pay*

$$0.01 \times 50\,\mathit{VTH/ETH} \times 100\,\mathit{ETH} = 50\,\mathit{VTH} \tag{4}$$

### 4.2 VTH Token Allocation

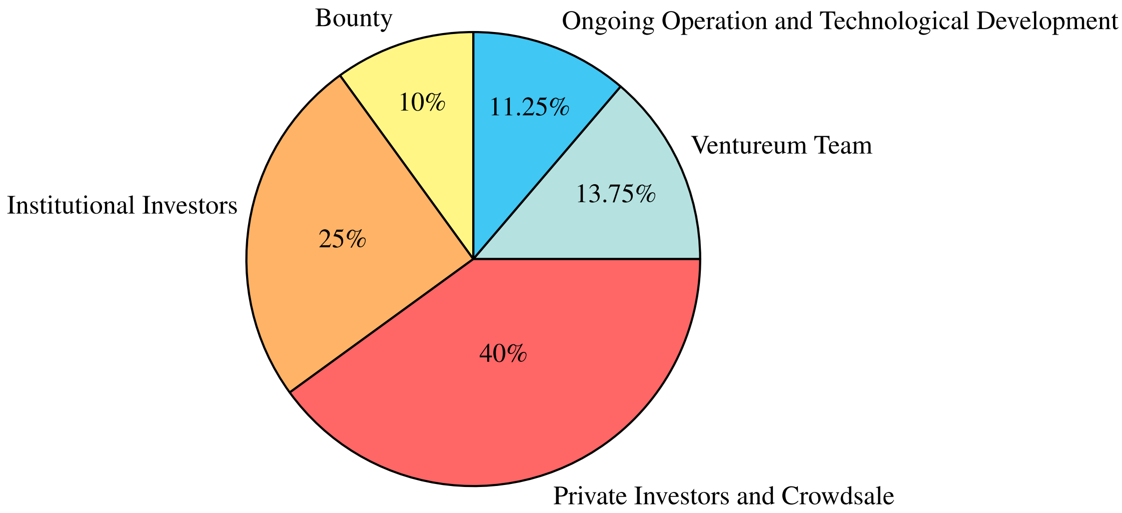

Figure 7: VTH Token Allocation

- 1,000,000,000 (1 Billion) VTH will be created. The total supply of VTH is fixed.
- 40% of VTH tokens are created during the Contribution Periods and allocated to public contributors and private investors.
- 10% of VTH tokens are allocated to founders and developers to compensate the current and future efforts for the Ventureum project and to attract new talent on board, and will be locked in a smart contract with a 10-month vesting period which starts at the end of crowdsale.
- 25% of VTH tokens are reserved for institutional investors.
- 10% of VTH tokens are reserved for bounty programs.
- 11.25% of VTH tokens are reserved for Ongoing Operation and Technological Development.

## 5 Official Endorsement from the Ventureum Team

The Milestone-Driven Funds Management Module is completely open source, and any blockchain projects can choose to integrate it into their own project by themselves without the Ventureum dev team's endorsement. In this case, the following rules apply:

- The use of the word "Ventureum", the Ventureum logo, and any mention of the Ventureum project or team are strictly prohibited. The Ventureum team reserves all the rights to take legal actions against anyone who violates this rule.
- The use of VTH tokens is optional.
- The Milestone-Driven Funds Management Module will provide an option to turn off the use of VTH tokens and set the ETH refund quota for all investors automatically to infinity.

If the founders of a blockchain project want the endorsement from the Ventureum team on their usage of the Milestone-Driven Funds Management Module, the following rules apply:

- The Ventureum team will perform audits and security reviews of the source codes of the Milestone-Driven Funds Management Module they deploy.
- The founders are required to strictly distinguish between Class A and Class B project tokens defined in Section 3 to comply with the requirements of the Milestone-Driven

Funds Management Module. The Ventureum team will oversee their compliance with this requirement.

- The use of VTH tokens is mandatory.
- Results of audits and security reviews are published and stored in blockchain. A DApp will be developed for viewing these results.

## 6 Extra Funding via Staking

In this section, we introduce a staking mechanism to provide extra funds to project founders, which also implies extra refunds for investors in the event of project failure. The decision to activate this part lies with project founders. **Casper** is a planned future change in the way the Ethereum network forms distributed consensus and is primarily aimed at reducing energy waste. Casper achieves this goal by using a consensus mechanism called **Proof of Stake**. Extra funds comes from "staking" – earning interest by locking up funds for a predetermined amount of time. Specifically, the Milestone-Driven Funds Management Module's smart contract deposits funds into the **Casper Contract**, and withdraws funds when a milestone state is in either the **Refund Period** or **Complete**. Meanwhile, interest earned by staking funds is transferred back to the smart contract.

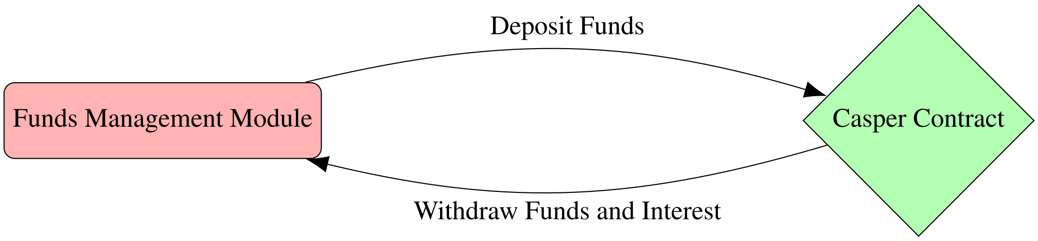

Figure 8: Interaction Between the Funds Management Module and the Casper Contract

It is important to note that Casper is not a finished protocol and is still under heavy development. The Ventureum development team will keep a very close eye on the Casper development process and react accordingly.

## 7 Ventureum Development Roadmap

### 7.1 A Brief Review of the Ventureum Team's Work

The team of Ventureum is a group of software engineers and data scientists who have worked at companies such as Amazon and Bank of Nova Scotia. We are also University of Waterloo alumni, blockchain tech enthusiasts and active cryptocurrency investors. We have followed the evolution of Ethereum since its very beginning, when Vitalik Buterin released the whitepaper for the Ethereum crowdsale. When ICOs entered a state of frenzy in the beginning of 2017, we started to notice two serious phenomena that plague Ethereum, and even the whole cryptocurrency universe, in both the short term and the long term. The first one is the network congestion on the Ethereum blockchain when a hot ICO opens to the public, which causes both frustration for investors and price fluctuations of ETH. The second one is the proliferation of scam ICOs. The true blockchain tech enthusiasts and proponents of Ethereum have been looking for a solution to both issues since then.

The team of Ventureum started to form between late April and early May 2017. Since then, we have been intensively doing research, forming ideas, and collecting feedback to devise a solution to both aforementioned issues. In June 2017, our team envisioned a milestone-driven funds management mechanism, implemented with the very spirit of Decentralized Autonomous Organization (DAO), that would be essential for protecting the interest of blockchain project investors in the long run. We started the drafting of the whitepaper in late June 2017.

### 7.2 Ventureum 1.0 (Q1 of 2018)

The Ventureum development team endeavors to achieve the following core features to enable the basic functionality of the Ventureum protocol.

**Development on the Ethereum blockchain**:

Smart contracts that implement milestone-driven funds management workflow, including key features:

- The investment in the form of ETH committed by the investors during a crowdsale will be distributed and locked in the milestones defined and published by the blockchain project founders by smart contracts.
- Smart contracts that implement the workflow of milestone-driven funds management as depicted in Figure 6.
- Smart contracts that implement Class A token staking.

**Frontend development**:

Two web user interfaces will be developed.

- A web user interface for project founders with the following functionalities:
  - Define project milestones' objectives and allocate (a percentage of) funds to them.
  - Deposit the funds(ETH) raised in a token sale into the Milestone-driven Funds Management module.
  - Initiate freeze period for a milestone.
  - Resume milestone procedure in a freeze period for a milestone
  - Access to voting results.
  - Withdraw funds (ETH) if milestone deliverables have been delivered on time. That is, investors have approved the decision to release funds to project founders in **Voting Period**, in which case the milestone is in state **Complete**.
- A web user interface for investors with the following functionalities:
  - Send Class A tokens for staking to obtain voting rights or for a refund.
  - Send VTH tokens to obtain ETH refund quota.
  - Vote during **Voting Period**.
  - Access to voting results.
  - View the balance of funds (ETH) they can withdraw.
  - Withdraw funds when refund criteria are met (such as a milestone reaches **Refund Period** state).
  - Withdraw Class A project tokens during **In Progress** (at least 30 days before the pending **Voting Period 1**), or during **Complete** or **Refund Period**.

### 7.3 Ventureum 2.0 (Q2 of 2018)

**Development on the Ethereum blockchain**:

- Smart contracts that implement the fund staking schedule.
- A mock **Casper contract**. The Ventureum team is fully aware that the exact time of the release of **Serenity** (the 4th release of Ethereum), on which the **Casper contract** runs, is highly unpredictable. To ensure a smooth development of the smart contracts that implement the fund staking schedule, a mock **Casper contract** will be developed to provide the underlying infrastructure. The mock **Casper contract** will only mimic the functionality and features of the **Casper contract** that are essential for running the fund staking module.

**Frontend development**:

- A web service to send notification emails will be developed to implement the following features:

- Notify project founders that the due date for a milestone is approaching.
- Notify project founders if they can initiate a **Voting Period** in the near future.
- Notify project founders of the result of a vote.
- Notify project founders of the balance of funds (ETH) they can withdraw.
- Notify investors of the result of a vote.
- Notify investors of the balance of funds (ETH) they can withdraw.
- Notify investors of the balance of Class A tokens they can withdraw.

## References

[1] Wikipedia. Initial Coin Offering.
https://en.wikipedia.org/wiki/Initial_coin_offering, .

[2] Smith and Crown. Smith and Crown Research.
https://www.smithandcrown.com/research-search/.

[3] John Koetsier. ICO Startups.
https://www.inc.com/john-koetsier/ico-bubble-startups-are-raising-hundreds-of-millio.html.

[4] ICOrating. ICOrating.
http://icorating.com/.

[5] CHAINANALYSIS. The Rise of Cybercrime on Ethereum.
https://blog.chainalysis.com/the-rise-of-cybercrime-on-ethereum/.

[6] Wikipedia. OneCoin.
https://en.wikipedia.org/wiki/OneCoin, .

[7] Garrett Keirns. GemCoin.
https://www.coindesk.com/gemcoin-ponzi-scheme-operator-hit-74-million-judgment/.

[8] Matthew Di Ferrante. Towards Responsible Token Sales (ICOs).
https://medium.com/@matthewdif/towards-responsible-token-sales-icos-291e69cc9ccf.

[9] SEC. SEC Rule on ICO.
https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings.

[10] MAS. MAS Rule on ICO.
http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx.

[11] Cointelegraph. Chinese Government Eyes ICO Crackdown Under New “Illegal Financing” Rules.
https://cointelegraph.com/news/chinese-government-eyes-ico-crackdown-under-new-illegal-financing-rules.