MOZO – SMART CONTRACTS

Authors: Thang Ton

Revision: <1.0>

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| DOCUMENT CHANGE LOG | | | | | | |
| Revision | Description | Author | Date | Approved | Date |
| 0.1 | Draft version | Thang Ton | Apr 20, 2018 |  |  |
| 1.0 | For audit | Thang Ton | Apr 27,2018 |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | | | | | | |

Contents

[1. References 4](#_Toc518285427)

[2. General description 5](#_Toc518285428)

[2.1 Objectives 5](#_Toc518285429)

[2.2 Scopes 5](#_Toc518285430)

[2.3 Organisation of this document 5](#_Toc518285431)

[2.4 Abbreviations 5](#_Toc518285432)

[3. Overview 7](#_Toc518285433)

[4. Smart Contracts 8](#_Toc518285434)

[4.1 Accounts 8](#_Toc518285435)

[4.1.1 Ethereum Accounts 8](#_Toc518285436)

[4.1.2 Ethereum accounts creating 10](#_Toc518285437)

[4.2 Token distributions 10](#_Toc518285438)

[4.2.1 Mozo token smart contract 10](#_Toc518285439)

[4.3 Common ICO 11](#_Toc518285440)

[4.3.1 ICO smart contract 11](#_Toc518285441)

[4.3.2 Presale 11](#_Toc518285442)

[4.3.3 Crowd Sale 12](#_Toc518285443)

[4.3.4 ICO Ending 14](#_Toc518285444)

[4.4 Agency smart contract 14](#_Toc518285445)

[4.5 After ICO - Token exchange with other cryptocurrency 15](#_Toc518285446)

[4.5.1 Exchange platform 15](#_Toc518285447)

[4.5.2 Mozo token exchange between investors 15](#_Toc518285448)

[4.6 Vested Token 16](#_Toc518285449)

[4.6.1 Individual Vested Token smart contract 16](#_Toc518285450)

[4.6.2 Process 17](#_Toc518285451)

[4.6.3 Sample Vested Token smart contracts 17](#_Toc518285452)

[5. ICO requirements approved by Founder 21](#_Toc518285453)

[5.1 List of baseline smart contracts 21](#_Toc518285454)

[5.1.1 Mozo Tokens (ERC20) specification 21](#_Toc518285455)

[5.1.2 ICO (ERC20) specification 22](#_Toc518285456)

[5.1.3 Investment discount smart contract specification 22](#_Toc518285457)

[5.1.4 Time Lock smart contract specification 22](#_Toc518285458)

[5.1.5 Vested token smart contracts specification 22](#_Toc518285459)

[5.2 ICO technical component proposal 24](#_Toc518285460)

[6. APPENDIX A: List of tables 25](#_Toc518285461)

[7. APPENDIX B: List of figures 26](#_Toc518285462)

# References

Table 1: References

|  |  |  |  |
| --- | --- | --- | --- |
| Abbr. | Name | Status | Note |
|  |  |  |  |
| MOZO WHITE PAPER | MOZO - The Token of Discovery | Working | On Website http:// mozocoin.io |

# General description

## Objectives

This document provides the specification of Mozo smart contracts for auditing.

## Scopes

This document is for internally using between Biglabs and auditors only.

## Organisation of this document

Table 2: The format of document

|  |  |  |
| --- | --- | --- |
| No. | Item | Description |
| 1. | References | * Provide the list of reference documents |
| 2. | General description | * Provides the explaination of objectives, scopes and the format of this document * Abreviation used in this documents |
| 3. | Overview | * The overview of SOLO |
| 4. | Smart contract | * Common description for Mozo smart contracts |
| 5. | ICO requirements | * Specification for ICO |
| 6. | List of tables | * List of table in document |
| 7. | List of figures | * List of figures in document |
|  |  |  |
|  |  |  |

## Abbreviations

Table 3: Abbreviations

|  |  |  |
| --- | --- | --- |
| Index | Abbreviation | Description |
| C | CRC | Cyclic Redundancy Check |
| D | DApp | Decentralized Application |
| E | ERC | Ethereum Request for Comments |
|  | ERC20 | ‘20’ is the unique proposal ID number.  ERC20 defines a common list of rules that an Ethereum token has to implement. Giving developers the ability to program how new tokens will function within the Ethereum ecosystem. |
|  | ETH | Ethereum |
| I | ID | Identifier |
|  | IEEE | Institute of Electrical and Electronics Engineers |
|  | IoT | Internet of things |
| M | MEW | My Ethereum wallet (myethereumwallet.com) |
| P | POS | Point of sale |
| S | SHA | Secure Hash Algorithm |
| U | UUID | Universally Unique IDentifier |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Overview

Project Mozo’s vision was to build a universal platform to attract foot traffic to physical stores. Mozo allows consumers to mine and collect a cryptocurrency, called a Mozo coin, when they use Mozo APP to discover new products at physical stores (ie. sales floors which are digitized and converted into smart stores by the Mozo system). Mozo coins can be converted into reference currencies such as Bitcoin or Ethereum, used as discounts for products and services at Mozo-enabled stores, and redeemed at Mozo Redemption marketplace; making it attractive to build a universal membership and reward system for retailers.



**Figure 1: Mozo’s blueprint**

Initially, Project Mozo shall use Ethereum blockchain network to support our transactions, and switch to Solo, when it becomes available. Our proprietary technology Solo is a new blockchain network that was designed to support peer-to-peer transactions in micropayments (Loyalty, IoT, Lending, Cybersecurity etc.).

Refer to Mozo White Paper for more information.

# Smart Contracts

## Accounts

### Ethereum Accounts

The following table depicts the list of Ethereum accounts in Mozo

Table 4: List of Ethereum accounts

|  |  |  |
| --- | --- | --- |
| Account | Description | Note |
| Founder’s Ethereum wallet | This Ethereum wallet owned by founder of Mozo | Use for:   * Collect fund * Hold all Mozo tokens at the starting up * Hold all Mozo sale tokens at ICO starting up * Create smart contracts * Exchange Mozo tokens with investor, team, smart contracts |
| Foundation and advisor team member ‘s Ethereum wallets | Each foundation and advisor team member should have an Ethereum wallet to capture the Mozo tokens | Use for:   * Hold Mozo tokens * Exchange Mozo tokens (when available) |
| Invetors’ Ethereum wallets | Each investors should have an Ethereum wallet to capture the Mozo tokens | Use for:   * Use Ethereum to buy Mozo tokens * Hold Mozo tokens * Exchange Mozo tokens |
| Merchants’ Ethereum wallets | Merchant should have an Ethereum wallet and use their Ether to buy Mozo tokens | Use for:   * Use Ethereum to buy Mozo tokens * Hold Mozo tokens * Exchange Mozo tokens * Use Mozo token to buy Mozo coins |
| Consumers’ Ethereum wallet | Optional. Consumer can have an Ethereum wallet to hold Mozo tokens | Use for:   * Use Ethereum to buy Mozo tokens * Exchange Mozo tokens * Use Mozo token to buy Mozo coins |
| Mozo tokens Smart contract | Created by Founder once  This smart contract use to hold Mozo tokens distribution (ERC20) |  |
| Individual Vested Token smart contrat | Created by Founder Wallet for each member of foundation and advisor team. And founder wallet will call transfer function of [Mozo tokens Smart contract] to transfer a number of tokens to this smart contract | See Vested Token for more information |
| ICO smart contract | Created by Founder Wallet once. And founder wallet will call transfer function of [Mozo tokens Smart contract] to transfer a number of tokens to ICO smart contract | This is used to hold sale tokens in ICO period (ERC20) |
| Treasury smart contract | Created by Founder Wallet once. And founder wallet will call transfer function of [Mozo tokens Smart contract] to transfer a number of tokens to Treasury.  These tokens will be used in Mozo operation such as merchant acquisition, consumer airdrop… | This is not available in this phase. |

### Ethereum accounts creating



**Figure 2: Wallet and main smart contracts creating**

See token distribution for more information.

## Token distributions

*Please note that the distribution of token is not secret. Anyone join to Ethereum blockchain can see the distribution of Mozo tokens. Of course they only saw the addresses that hold token but easily to guess the person behind an Ethereum address.*

### Mozo token smart contract

The Mozo token smart contract will hold a map of address to number of token belongs to the address

Table 5: Mozo Token distribution example

|  |  |  |
| --- | --- | --- |
| Account | Description | Percentage |
| Founder | Keep token for his own | a1 |
| Foundation and advisor team | a2 |
| ICO | Presale and crowd sale | a3 |
| Treasury | For operation | a4 |
|  | **Total** | **100% = S** |
|  | **Where** | |

At step 3 of Ethereum accounting, after founder created the Mozo token smart contract, he will hold total supplying of Mozo token

Address[Founder Wallet] = S

At step 10, founder will transfer to ICO smart contract a3.S token

Address[Founder Wallet] = S – a3.S

Address[ICO smart contract] = a3.S

And so on, the last distribution is

Address[Founder Wallet] = (a1+a2).S

Address[ICO smart contract] = a3.S

Address[Treasury smart contract] = a4.S

This distribution is at the starting of ICO.

## Common ICO

### ICO smart contract

ICO smart contract will be an ERC20 itself. It means that ICO smart contract will hold the temporary token (sale token) distribution until it is released by owner. This distribution will be reflecting to Mozo tokens smart contract.

* Created by Founder wallet once
* Has Founder Wallet address: Ether transfer to this smart contract will go to Founder Wallet
* Has a start date and end date: funds getting only in this period
* Has an interface of [Mozo tokens Smart contract] to set the token distribution.

### Presale

At the beginning of presale phase, Founder will create all Presale smart contract (refer to Sample of Sale Smart Contract for more information).

*Note: Sale Smart Contract may have some rules to send bonus tokens to some person (investor, sell agency…) but not depicts in the process.*



**Figure 3: ICO presale’s process**

### Crowd Sale

If the hard cap is not reached in the presale stage, Founder will begin the crowd sale stage by creating some Crowd Sale smart contract (refer to Sample of Sale Smart Contract for more information).

*Note: Sale Smart Contract may have some rules to send bonus tokens to some person (investor, sell agency…) but not depicts in the process.*



**Figure 4: ICO crowd sale’s process**

### ICO Ending



**Figure 5: ICO Ending’s process**

## Agency smart contract

This smart contact allows owner to set the bonus rule for agency depends on number of sold tokens

When this contract is released, calculate the number of bonus tokens based on rules set up by owner and transfer these sale token to agency address.

Agency must register on ICO Website or contact directly with Founder. Agency will provide his wallet address to receive bonus Mozo tokens.



**Figure 6: Agency smart contract**

## After ICO - Token exchange with other cryptocurrency

When ICO ending, investor can exchange token with other cryptocurrency.

### Exchange platform

Marketing and operation team will perform token listing job with well-known exchange platforms so that investor can exchange Mozo token to other cryptocurrency and vice versa.

### Mozo token exchange between investors

Investor holds Mozo tokens can exchange to other cryptocurrency and vice versa. They can exchange Mozo tokens privately with their own risk. Mozo will support by providing smart contract for Mozo token exchange using ether.

Investor 1 want to sell Mozo tokens to investor 2, he will create an Exchange smart contract with predefined rate. If investor 2 accept this rate, he can use ether to buy Mozo tokens.



**Figure 7: Exchange smart contract**

## Vested Token

### Individual Vested Token smart contract

* Created by Founder wallet for each member in foundation and advisor team
* Founder can choose any smart contract type (see sample section below for more information) to create a smart contract for team member.

### Process



**Figure 8: Individual Vested smart contracts creating process**

### Sample Vested Token smart contracts

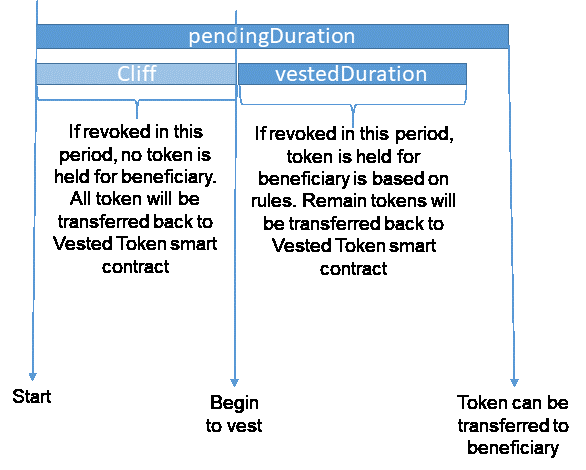
#### Time Lock Token smart contract

This is a token holder contract that will allow a beneficiary to extract the tokens after a given release time



**Figure 9: Time Lock Vested tokens smart contract**

#### Revocable Vested token smart contract



**Figure 10: Revocable vested smart contract**

Only owner of smart contract (normally the Founder) can revoke the contract. If owner revoke after pending time, vested tokens will be move to beneficiary address. Number of tokens is depending on the rules was setting up.

Beneficiary can claim to get tokens any time before smart contract is revoked and after pending duration. Number of tokens is depending on the rules was setting up.

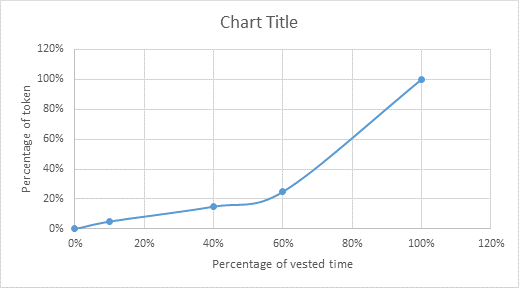
Cliff can be 0. It means that vest can begin at the start

Vested duration can be 0. It means that after cliff time, token will be held for beneficiary.

Pending duration can be less than or greater than the sum of Cliff and Vested duration.

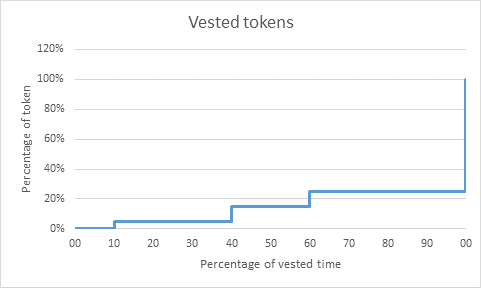
Rule:

* Linear: means number of tokens = total tokens \* (time passed) / vestedDuration
* Progressive:
  + Linear at each brackets:



**Figure 11: Progressive vested with linear bracket**

* + Step



**Figure 12: Progressive vested with step bracket**



**Figure 13: Revocable Vested smart contract processing**

# ICO requirements approved by Founder

## List of baseline smart contracts

### Mozo Tokens (ERC20) specification

* Total tokens: parameter – default is 5g
* Description: Mozo tokens
* Decimals: 2
* Symbol: MOZO

### ICO (ERC20) specification

* Description: Mozo sale tokens
* Decimals: 2
* Symbol: SMZO
* When releasing or reaching hard cap:
  + If hard cap is reached: burn all unsold tokens
  + If not, distribute to all investors

### Investment discount smart contract specification

* Based on number of wei contribution
* Founder will define array of contribution accordingly with bonus percentage
  + For example: (3, 5, 7, 20) (0, 10, 12, 20)

=>

* + - Min contribution: 3
    - Contribution from < 5: bonus 0%
    - Contribution from < 7: bonus 10%
    - Contribution from < 20: bonus 12%
    - >20: bonus 20%

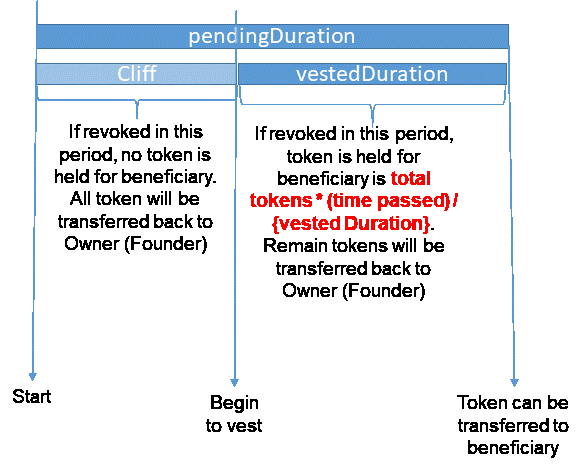
### Time Lock smart contract specification

These contracts will be created by Founder after presale for consultant/advisor/team. When smart contract is released by Owner or claimed by Agency, token will be transferred to beneficiary.

### Vested token smart contracts specification

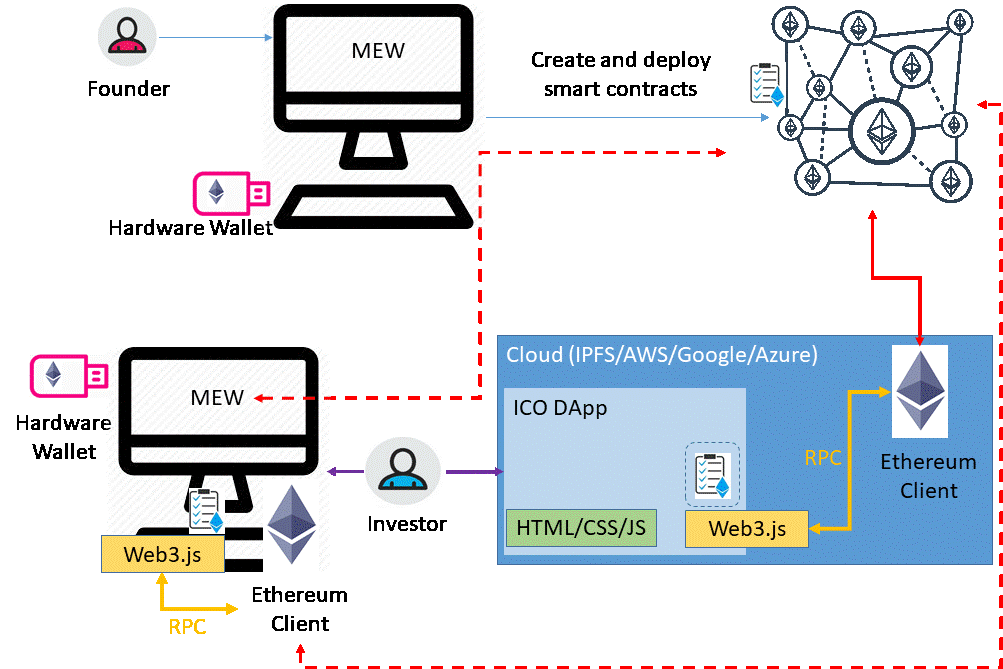
Simple revocable vested token smart contract.

* Has a pending duration (setting up by founder when creating smart contract)
* Has a cliff duration (setting up by founder when creating smart contract)
* {Vested duration} = {pending duration} – {cliff duration}
* Linear achievement by time
  + No of tokens = total tokens \* (time passed) / {vested Duration}



**Figure 14: Simple Revocable Vested token smart contract**

## ICO technical component proposal

****

**Figure 15: ICO App – System architecture**

# APPENDIX A: List of tables

[Table 1: References 4](#_Toc518285463)

[Table 2: The format of document 5](#_Toc518285464)

[Table 3: Abbreviations 5](#_Toc518285465)

[Table 4: List of Ethereum accounts 8](#_Toc518285466)

[Table 5: Mozo Token distribution example 10](#_Toc518285467)

# APPENDIX B: List of figures

[**Figure 1: Mozo’s blueprint** 7](#_Toc518285468)

[**Figure 2: Wallet and main smart contracts creating** 10](#_Toc518285469)

[**Figure 3: ICO presale’s process** 12](#_Toc518285470)

[**Figure 4: ICO crowd sale’s process** 13](#_Toc518285471)

[**Figure 5: ICO Ending’s process** 14](#_Toc518285472)

[**Figure 6: Agency smart contract** 15](#_Toc518285473)

[**Figure 7: Exchange smart contract** 16](#_Toc518285474)

[**Figure 8: Individual Vested smart contracts creating process** 17](#_Toc518285475)

[**Figure 9: Time Lock Vested tokens smart contract** 18](#_Toc518285476)

[**Figure 10: Revocable vested smart contract** 19](#_Toc518285477)

[**Figure 11: Progressive vested with linear bracket** 20](#_Toc518285478)

[**Figure 12: Progressive vested with step bracket** 20](#_Toc518285479)

[**Figure 13: Revocable Vested smart contract processing** 21](#_Toc518285480)

[**Figure 14: Simple Revocable Vested token smart contract** 23](#_Toc518285481)

[**Figure 15: ICO App – System architecture** 24](#_Toc518285482)