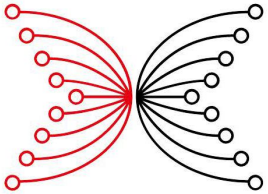
Treasury Coin - a prototype implementation of the treasury system



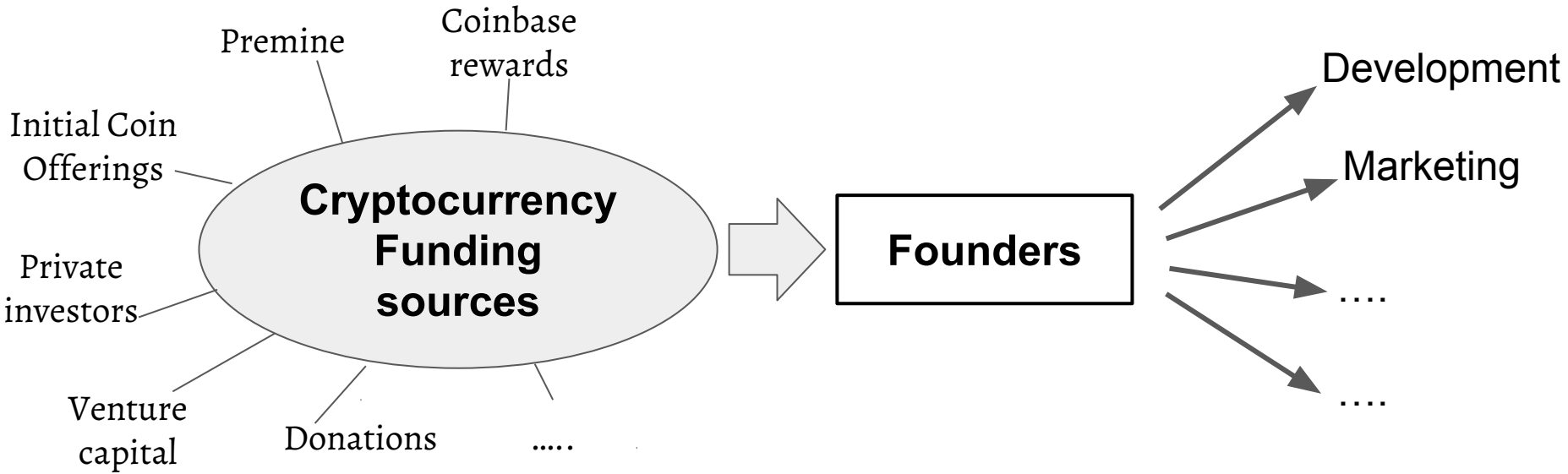
INPUT | OUTPUT

Lancaster University

May 11, 2018

Motivation

Most of the modern cryptocurrencies have centralized funding workflow



Motivation

- Modern cryptocurrencies are complex systems that require continuous maintenance. Even though it is usually proclaimed that such systems are completely decentralized, all existing cryptocurrency systems have core team of members that, at least, controls the development effort.
- It becomes crucial how the core team is funded. If it is paid by some standalone investor most likely they will follow his wishes that are not necessarily beneficial for a cryptocurrency general well-being.
- Treasury system aims to solve this problem by providing means for establishing collaborative consensus among all cryptocurrency stakeholders about financing a system.

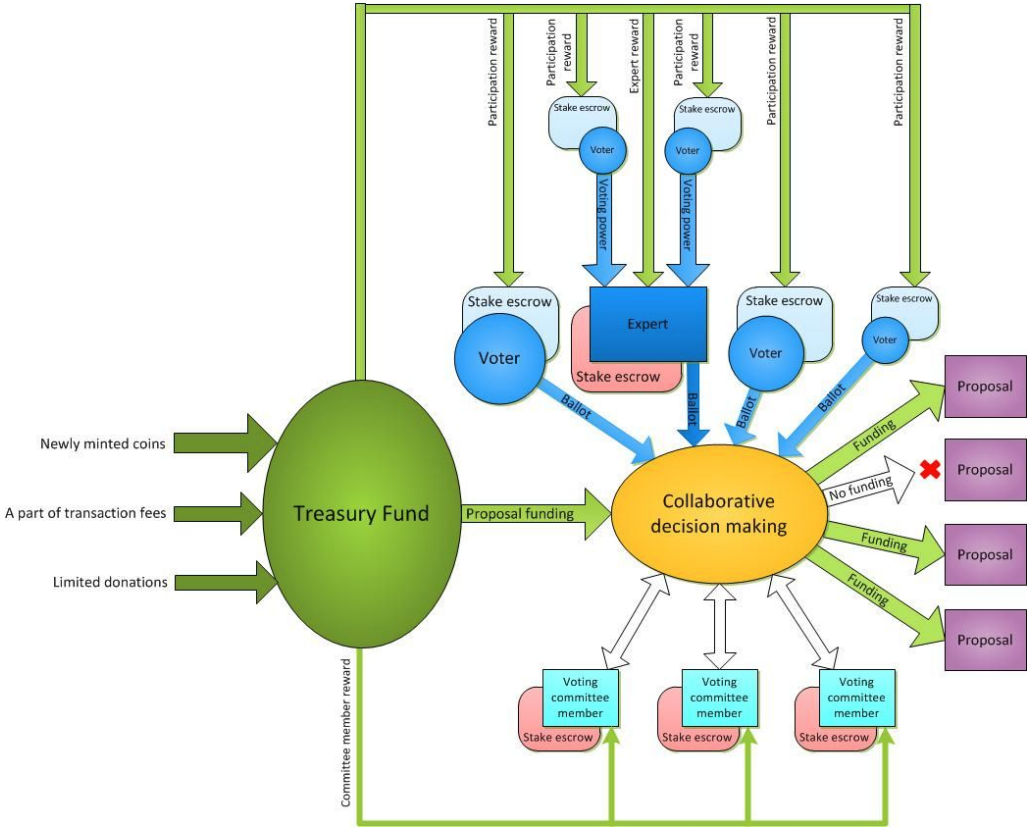
Treasury system

In the paper **“A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence”** (joint work of IOHK and Lancaster University) an advanced treasury system was proposed.

Treasury Coin - is an implementation of the proposed treasury system over the Scorex framework.

Treasury paper: https://iohk.io/research/papers/#S7KC2KGJ
Treasury presentation by prof. Bingsheng Zhang: https://www.youtube.com/watch?v=Hyh3h_yX-S0
TreasuryCoin implementation: https://github.com/input-output-hk/TreasuryCoin

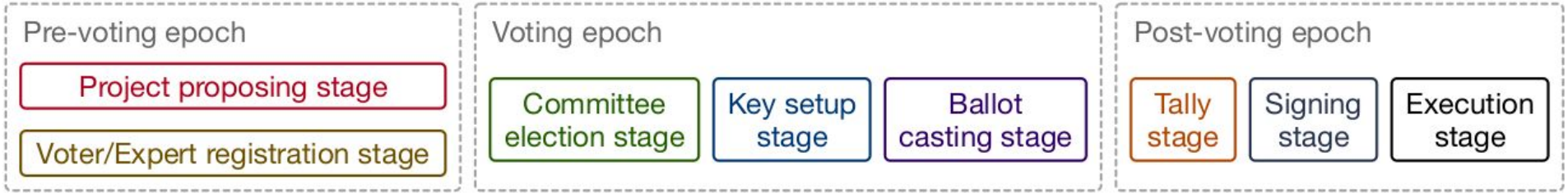
Treasury system (general scheme)



Main properties of the proposed treasury system

- Decisions about proposals funding are taken collaboratively by stakeholders through the voting process
- A special cryptographic voting protocol is developed
- Proposals funding is an iterative process. A notion of **epoch** is introduced to establish an independent period of decision-making process. It includes the following major stages:
  - Proposals/Voters registration
  - Voting
  - Payment
- Restricted delegation is allowed (voters can delegate their voting power to the specially registered experts)
- To become a voter/expert a special deposit is needed. Voting power is equal to the amount of the deposit

Treasury epoch



Main properties of the cryptographic voting scheme

- **Full verifiability** - everyone is able to verify the correctness of the voting result
- **Secrecy** - personal choice of a voter is not disclosed
- **Fairness** - no one has an advantage of knowing the partial results of the voting

Used cryptography

To meet all mentioned requirements a special **committee** is employed. Committee members run a set of cryptographic protocols to facilitate the secure voting protocol:

- Distributed encryption key generation (including VSS sharing of personal secrets of the committee members) - 6-rounds protocol
- Joint decryption of the result - 4-rounds protocol
- Joint randomness generation - 3-rounds protocol
- Non-interactive zero-knowledge proofs are used throughout all protocols for verifying validity of each message

Resilience to malicious behavior or failure of up to 50% of the committee members

Implementation

The full-fledged implementation of the proposed treasury system was done using the **Scorex** framework.

As an underlying blockchain the **TwinsCoin** implementation was taken (which is available in Scorex out of the box)

Existed TwinsCoin implementation was modified to introduce logic needed for treasury.

Features of Treasury Coin

- Proposals submission
- Voters/Experts/Committe members registration
- Locked deposits for all actors in the system
- Random selection of the committee
- Distributed key generation
- Ballots casting
- Joint decryption with recovery in case of faulty committee members
- Randomness generation
- Reward payments and deposit paybacks
- Penalties for faulty actors
- etc.

Testnet

Local testnet of 12 full nodes was launched and was operating successfully for 2 days.

The parameters of the testnet:

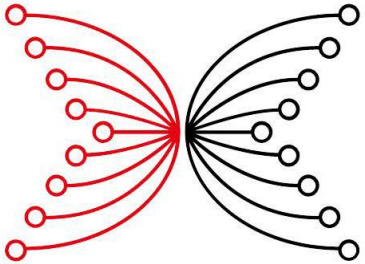
- Number of committee members - 12 (only 10 are chosen randomly each epoch to run protocols)
- Number of voters - 9
- Number of experts - 3
- Proposals per epoch - varying from 1 to 7
- Size of the epoch - 780 blocks (approx 50 blocks for each stage of the epoch)
- Block generation time - 10 sec (approx 2.5 hours per epoch)

Demo of running Treasury Coin local testnet

ZenCash integration options

- Altering core consensus
- Running in a sidechain

Thank you for your attention



INPUT | OUTPUT