COUGER

zkC.R.E.A.M

Zero-Knowledge Confidential Reliable Ethereum Anonymous Mixer

Index

zkC.R.E.A.M

- zkC.R.E.A.M is **an open-source product based on the technology of Ethereum**.
- Taking advantage of the characteristics of the blockchain, the specifications do not require a centralized third party and **the voting results cannot be tampered with**.
- Furthermore, by introducing mixer technology and exchanging encrypted tokens, we have created **a system that allows a third party to fairly verify the results while maintaining a high level of anonymity**.

Features of zkC.R.E.A.M ① Confidentiality

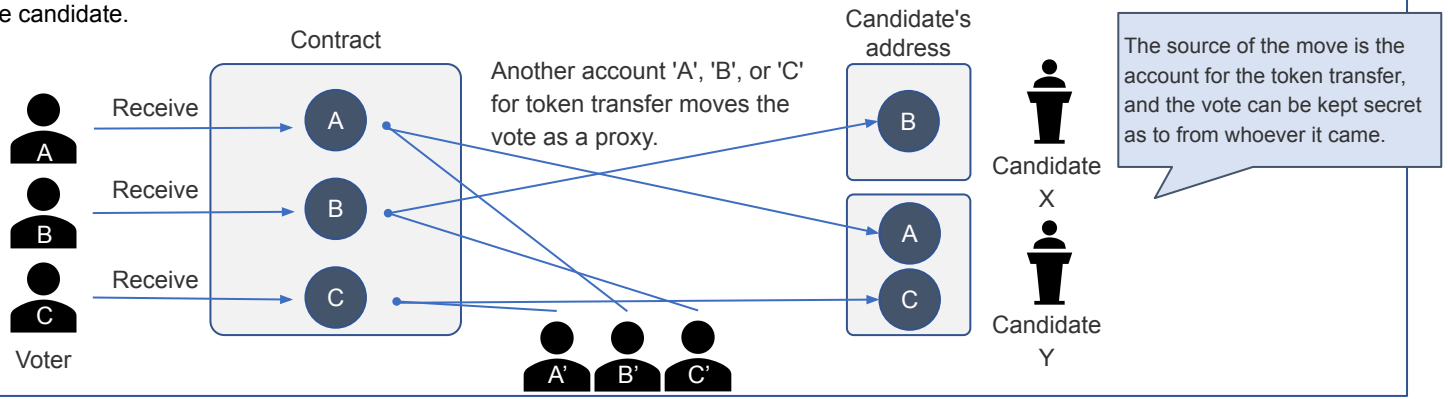
Features of zkC.R.E.A.M

- It introduces a revolutionary mixer technology* that assumes zero-knowledge proof, implemented by Vitalik Buterin, the inventor of Ethereum.
  This technology is used in tornado.cash and other applications.
- It issues irreplaceable voting tokens and obfuscates transactions with a decentralized protocol.

What it can do

- Voters can **cast their votes completely anonymously**.
- Third parties can only check statistical information, such as the ballot distribution and the overall turnout in preparation for voting.
  The voter's voting address and other information **cannot be viewed by third parties**.

***Mixer technology**: Technology that keeps secret who votes for whom by pooling voting tokens into a contract and having a separate account for token transfer move them to the candidate.



Features of zkC.R.E.A.M ②

Preventing Complicity and Collusion

Features of zkC.R.E.A.M

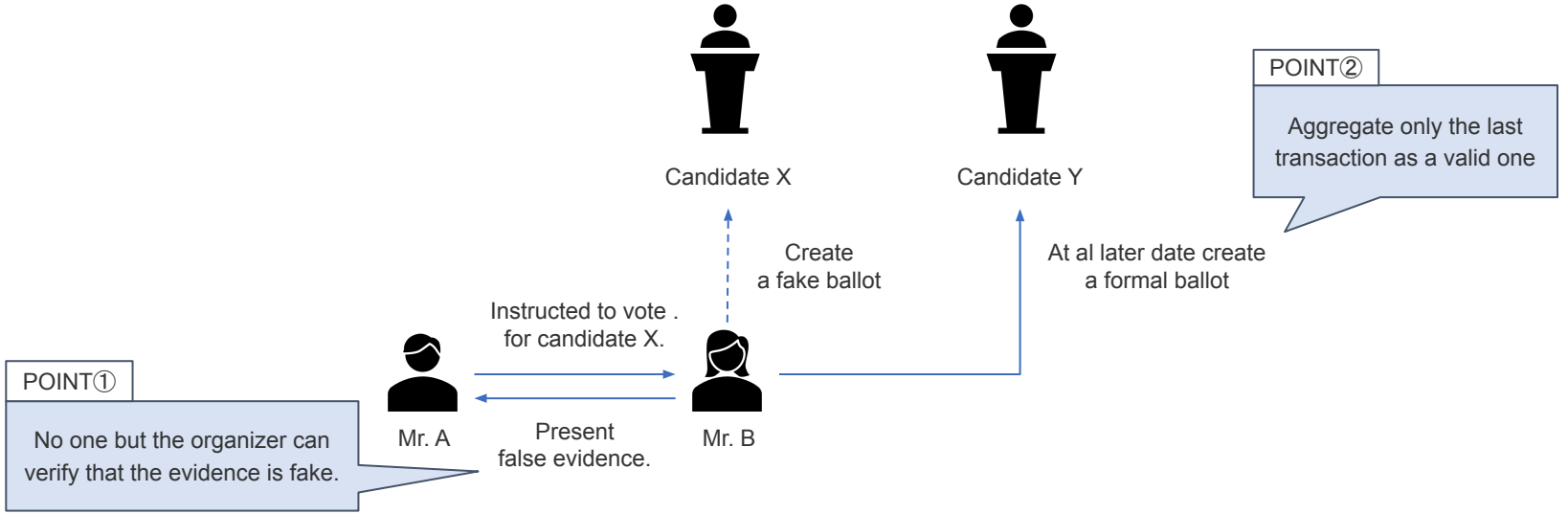
- For future research and development, we are incorporating the MACI protocol (Minimal Anti-Collusion Infrastructure protocol), also developed by Vitalik Buterin.

What it can do

- The introduction of MACI will **prevent typical collusion and conspiracy** among voters.
  - Collective Voting
  - Unauthorized transfer of voting rights
- Voters can use MACI to intentionally create false information so that **no one but the organizer can determine the authenticity of the information**.

Preventing Complicity and Collusion (Example)

- Mr. A asks Mr. B to vote for candidate X.
  Mr. B created fake data that made it look like he voted for candidate X, and that he had fulfilled the request. In reality, he voted for candidate Y. (Not voting for anyone is another possibility)



Only the last voting transaction will be counted, thereby preventing collusion and threats of fraud from other companies.

Features of zkC.R.E.A.M ③

Verifiability

Features of zkC.R.E.A.M

- With the introduction of MACI, MACI verification tools are now available.

MACI verification tools:
https://github.com/appliedzkp/maci/blob/master/cli/README.md#demonstration

What it can do

- Each voter can verify that **his or her vote has been counted correctly**.
- Voters can verify the number of ballots issued and the voter turnout **without having to rely on a central** authority.

Features of zkC.R.E.A.M ④

Impartial participation

Features of zkC.R.E.A.M

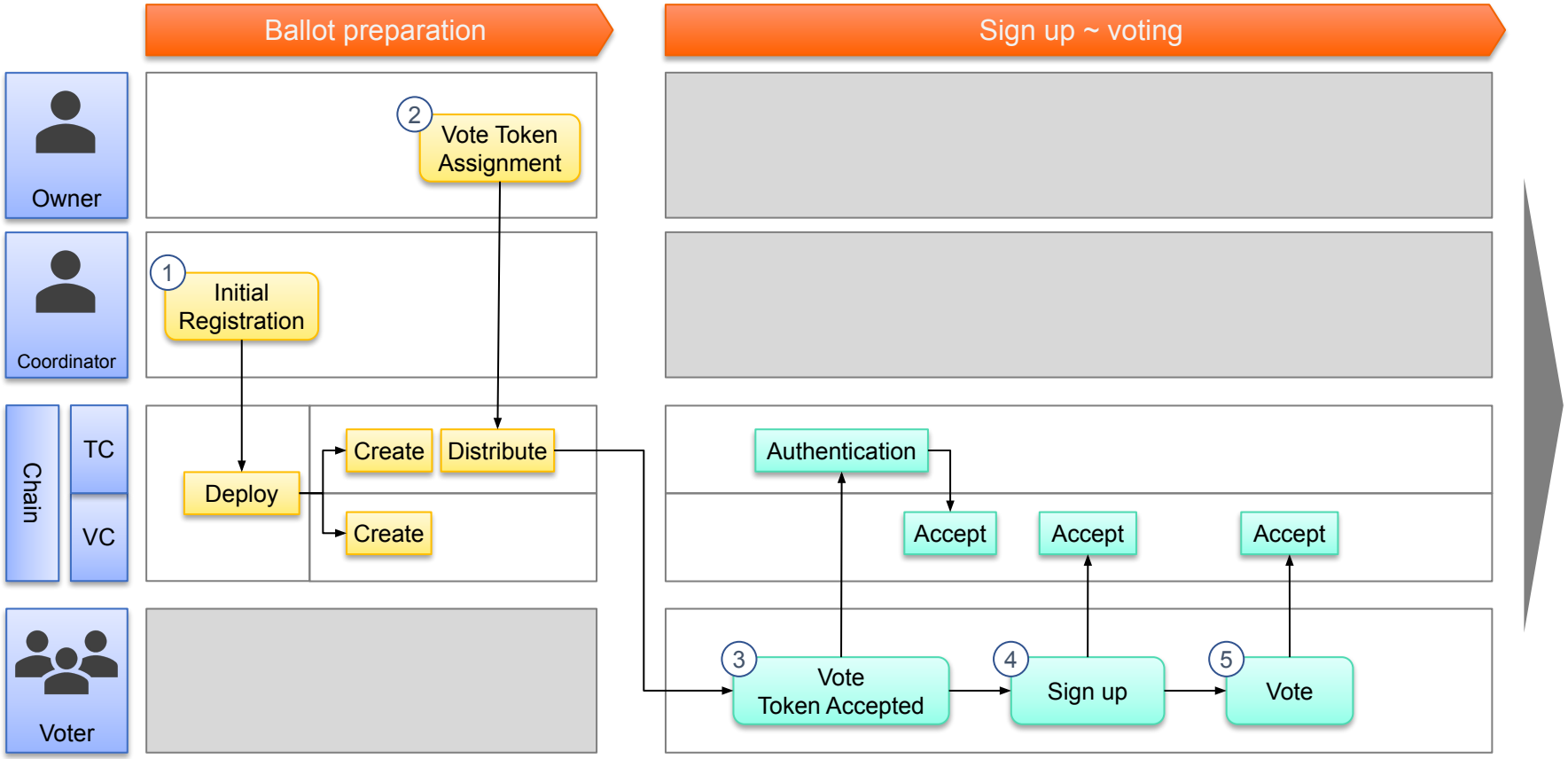
- In order to achieve zero-knowledge proofs, steps called "trusted setup" and "ceremony" are taken.
- In recent years, this process has also been decentralized through browser applications, which zkCREAM also plans to introduce.

What it can do

- By using parameters created by multiple people for proof, it is possible to **prevent fraud by the organizer (e.g., tampering with the voter's authority)**.

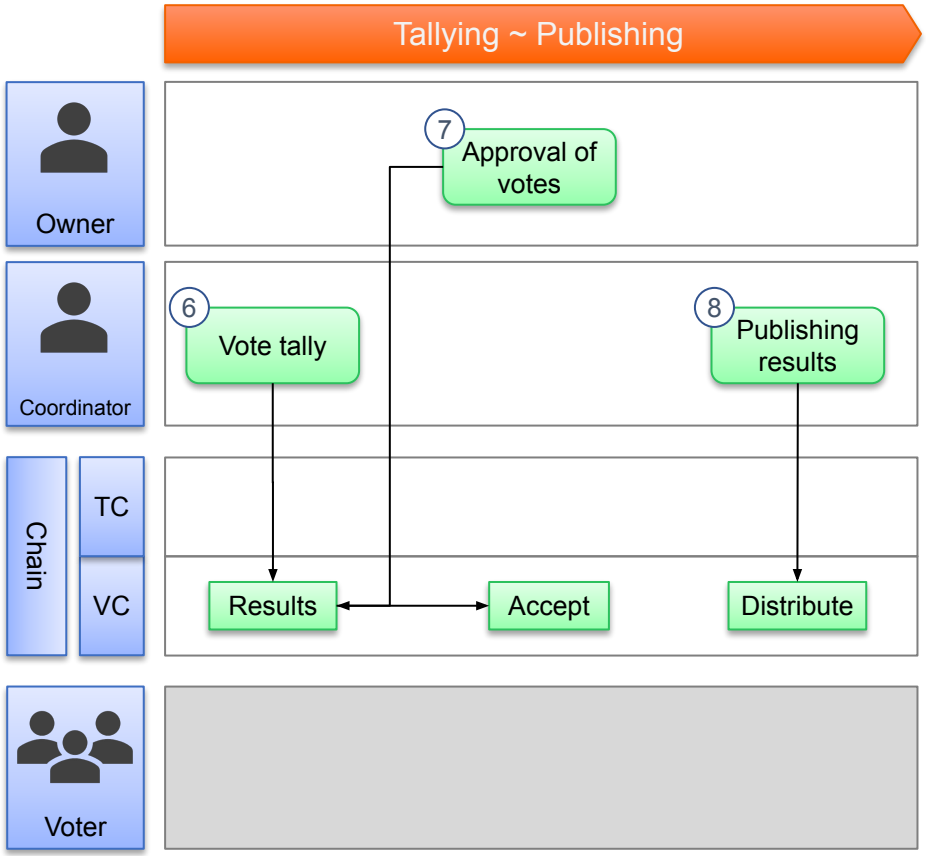
Usage Flow Chart（1/ 2）

COUGER



*TC = Token Contract, VC = Voting Contract

Usage Flow Chart（2/ 2）



*TC = Token Contract, VC = Voting Contract

Inquiries

COUGER

https://couger.co.jp/
Couger Inc.

Koshiichi Building #201, 6-19-16 Jingumae, Shibuya-ku
Tokyo 150-0001, Japan

Attn: zkC.R.E.A.M
info@couger.co.jp