VoteOnChain

Dizme Hackathon_21

VoteOnChain

- Progetto per la gestione di votazioni online sicure
- Basato sulle tecnologie di **Blockchain** e **Self-Sovereing Identity** (**SSI**)
- Gestisce sia la votazione palese che segreta
- Utilizza **Dizme** come sistema di gestione dell'identità dei votanti e la verifica del diritto al voto
- I voti sono consolidati sulla BlockChain **Algorand**

Tipologie di voto

Voto Palese

Si può associare l'identità della persona alla propria opinione.

La dichiarazione del voto può avvenire in diverse modalità (alzata di mano, scheda elettorale nominale).

Voto Segreto

Modalità di voto attraverso la quale la preferenza espressa dall'elettore rimane segreta e non viene conosciuta da terzi.

Il voto espresso rimane segreto e slegato dalla persona che lo ha espresso.

Caratteristiche di sicurezza

- **Eleggibilità** (segreto / palese)
  - *Può votare solo chi è in possesso di diritto di voto*
- **Non riutilizzabilità** (segreto / palese)
  - *Nessuno può votare più di un'unica volta*
- **Non tracciabilità** (segreto)
  - *Nessuno può determinare la preferenza espressa da altri*

Caratteristiche di sicurezza

- **Non duplicabilità** (segreto / palese)
  - *Nessuno può duplicare il voto di altri*
- **Immutabilità** (segreto / palese)
  - *Nessuno può cambiare la preferenza espressa da altri*
- **Verificabilità** (segreto / palese)
  - *Ogni votante può controllare che il suo voto è stato conteggiato nel computo finale*

Architettura

- Gli attori coinvolti sono
  - **Organizzazione**
    - Entità che indice il voto
    - Gestisce le identità dei votanti
    - Attribuisce diritto la voto
  - **Third Trusted Party** (**TTP**)
    - Gestisce le procedure di voto
  - **Votante**
    - Tramite wallet Dizme si identifica all’Organizzazione e riceve il diritto di voto
    - Tramite wallet Algorand esprime il suo voto

Fase Preliminare

- Gli utenti dovranno dotarsi di una identità **Dizme** LoA1 e di un wallet **Algorand**
- L’Organizzioni dovranno riconoscere i propri utenti, tramite l’identità Dizme LoA1, per poi distribuirgli la credenziale Dizme **Member**

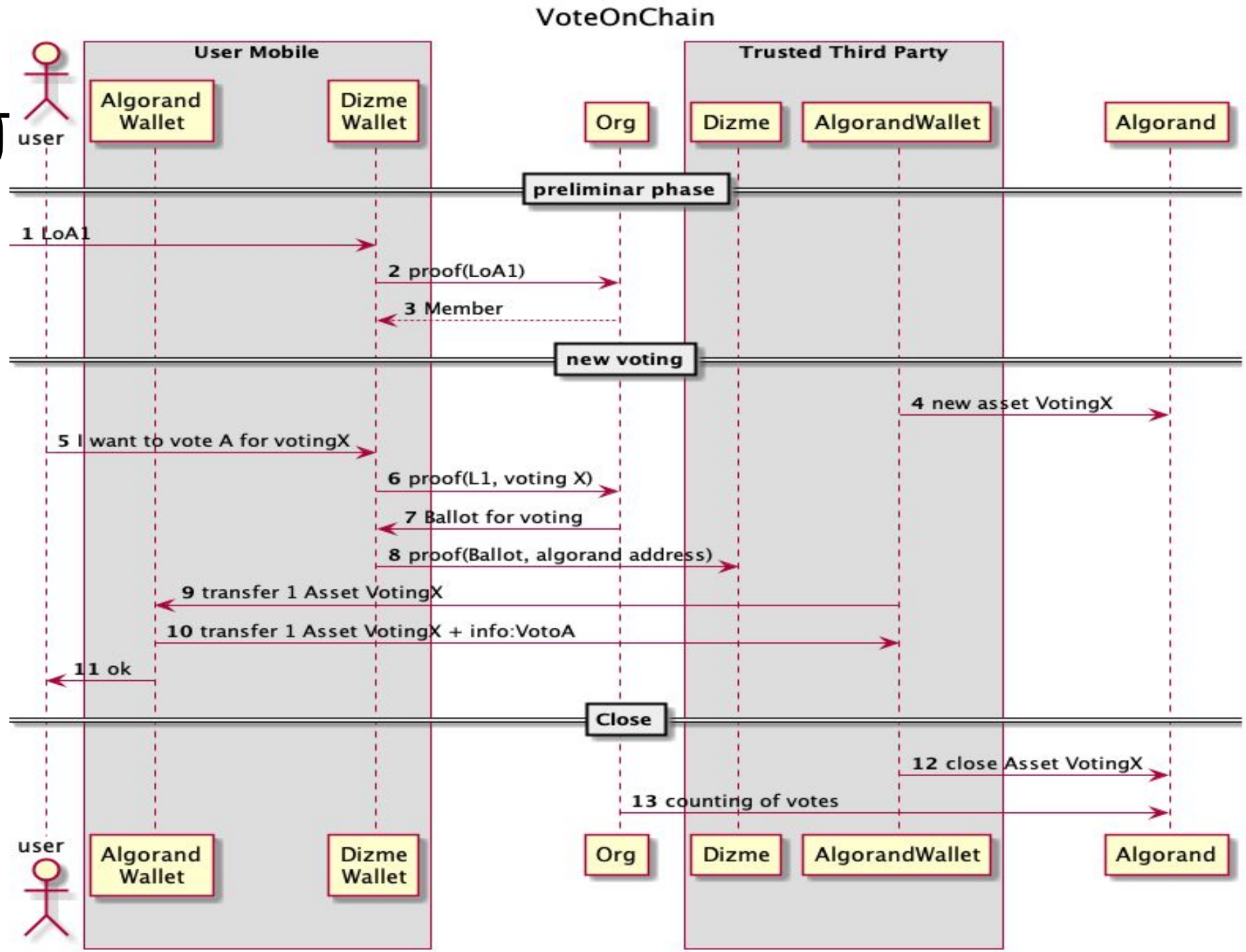
Nuova Votazione

- L'Organizzazione rilascerà agli utenti che hanno diritto al voto la credenziale Dizme **Accreditation**
- La **TTP**, crea un nuovo Asset Algorand dedicato alla votazione, generando un numero sufficiente di token
- Il votate che intende votare, dovrà
  1. presentare all'Organizzazione la Proof della propria **Member** per avere la credenziale **Accreditation**
  2. presentare al **TTP** la Proof dell'**Accreditation** aggiungendo come attributo self-attested l'indirizzo del wallet Algorand
  3. Se ha diritto a votare, riceverà sull'indirizzo dedicato un Asset dalla TTP, che dovrà rimandare alla TTP indicando nelle note la sua intenzione di voto

Chiusura Votazione

- La votazione termina quando la **TTP** “chiude” l’Asset dedicato alla votazione
- I voti sono espressi tramite le transazioni **Algorand** per quel specifico Asset
- Il conteggio si effettua parsando tutte le transazioni di quell’Asset verso il **TTP**

Sequence vo


VoteOnChain
User Mobile
Trusted Third Party
user
Algorand Wallet
Dizme Wallet
Org
Dizme
AlgorandWallet
Algorand
preliminar phase
1 LoA1
2 proof(LoA1)
3 Member
new voting
4 new asset VotingX
5 I want to vote A for votingX
6 proof(L1, voting X)
7 Ballot for voting
8 proof(Ballot, algorand address)
9 transfer 1 Asset VotingX
10 transfer 1 Asset VotingX + info:VotoA
11 ok
Close
12 close Asset VotingX
13 counting of votes
user
Algorand Wallet
Dizme Wallet
Org
Dizme
AlgorandWallet
Algorand

Voto Palese / Segreto

- I voti sono transfer di Asset sulla blockchain **Algorand**, quindi pubblici e immutabili
- La **TTP** per effettuare il transfer dell'Asset verso un utente dovrà ricevere dall'utente la Proof con
  - il Ballot, che esprime solo il diritto di voto senza svelare l'identità
  - l'Address Algorand dell'utente
- Per il voto palese, l'utente userà il proprio **Algorand** Address reso pubblico all'Organization
- Per il voto segreto, l'utente dovrà generare ogni volta un **Algorand** Address per la specifica votazione, così da restare anonimo

Analisi

- **Eleggibilità:** *Può votare solo chi è in possesso di diritto di voto*
  - Solo l'Organizzazione distribuisce a chi ne ha diritto la credenziale Accreditation
- **Non riutilizzabilità**: *Nessuno può votare più di un'unica volta*
  - La **TTP** trasferisce 1 solo Asset di voto per ogni credenziale Accreditation presentata
- **Non tracciabilità** (segreto): *Nessuno può determinare la preferenza espressa da altri*
  - Il voto è un transfer di Asset Algorand da un Address anonimo

Analisi

- **Non duplicabilità**: *Nessuno può duplicare il voto di altri*
  - I voti sono transfer di Asset Agorand, solo la TTP li può distribuire
- **Immutabilità:** *Nessuno può cambiare la preferenza espressa da altri*
  - I voti sono transfer di Asset Agorand, quindi consolidati sulla blockchain
- **Verificabilità:** *Ogni votante può controllare che il suo voto è stato conteggiato nel computo finale*
  - L'utente può verificare che il transfer dell'Asset sia sulla blockchain

Implementazione

- Una Organizzazione è una Dizme-Organization
  - Proof **LoA1** -> Credential **Member**
  - Proof **Member** -> Credenziale **Accreditation**
- La TTP è una Dizme-Organization
  - Proof {**Accreditation** , **Algorand Address** (self-attested) }
  - Transfer 1 Asset Votazione sul **Algorand Addr**ess
- Votante
  - Usa Dizme App e Algorand Wallet
  - Tramite Dizme gestisce le credenziali di Identità, Member e Accreditation
  - Per la votazione effettua un transfer di 1 Asset Votazione sul **Algorand Addr**ess del **TTP** indicando nelle info il suo voto

Conclusioni

- E-Voting è uno dei problemi più complessi dal punto di vista della sicurezza informatica
- Il binomio **Dizme-Algorand** ha fornito gli strumenti necessari per disegnare una soluzione completa, funzionale, ma soprattutto che garantisce un elevato livello di sicurezza
- La POC ha simulato l'integrazione tra Dizme e Algorand, ma sarebbe auspicato una integrazione nativa a cura della Fondation