



UNIVERSITY OF PADUA
UNIVERSITA' DEGLI STUDI DI PADOVA

Zero Knowledge Proof per voto verificabile e anonimo

Dipartimento di Matematica "Tullio Levi Civita" -Università di Padova
Corso di Laurea in Informatica

Esame di Laurea
14 Dicembre 2023

Laureando: Pietro Lauriola

- ❑ **L'azienda**
- ❑ **L'idea**
- ❑ **Tecnologie**
- ❑ **Implementazione**
- ❑ **Obiettivi raggiunti**



S Y N C L A B



Nascita
2002
Napoli

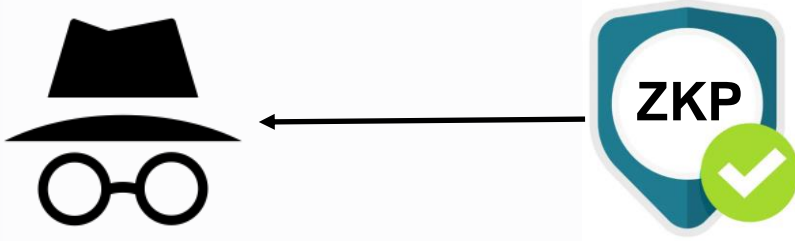
Sedi
6

Clienti
150+

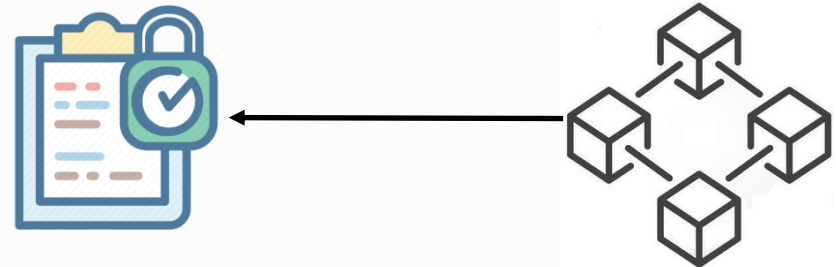
Dipendenti
300+

Realizzare un sistema di votazione online
che garantisca:

Anonimato

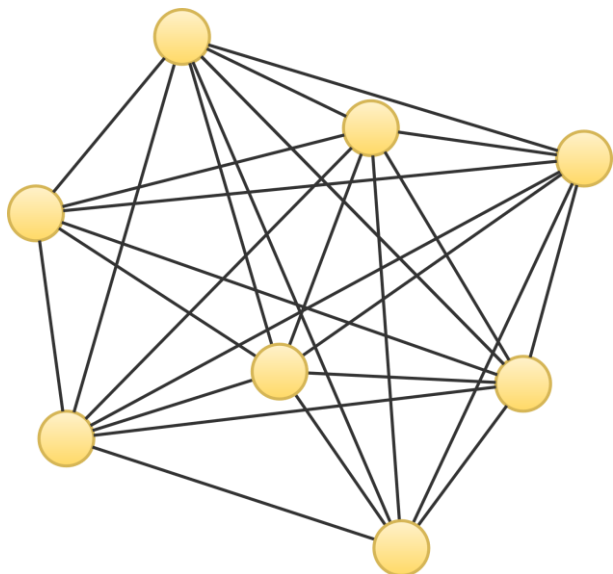


Integrità dei dati

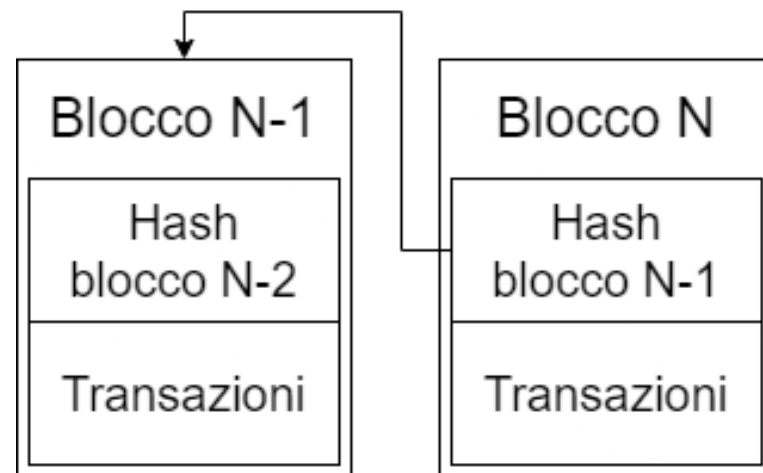


Garantire integrità e immutabilità dei dati

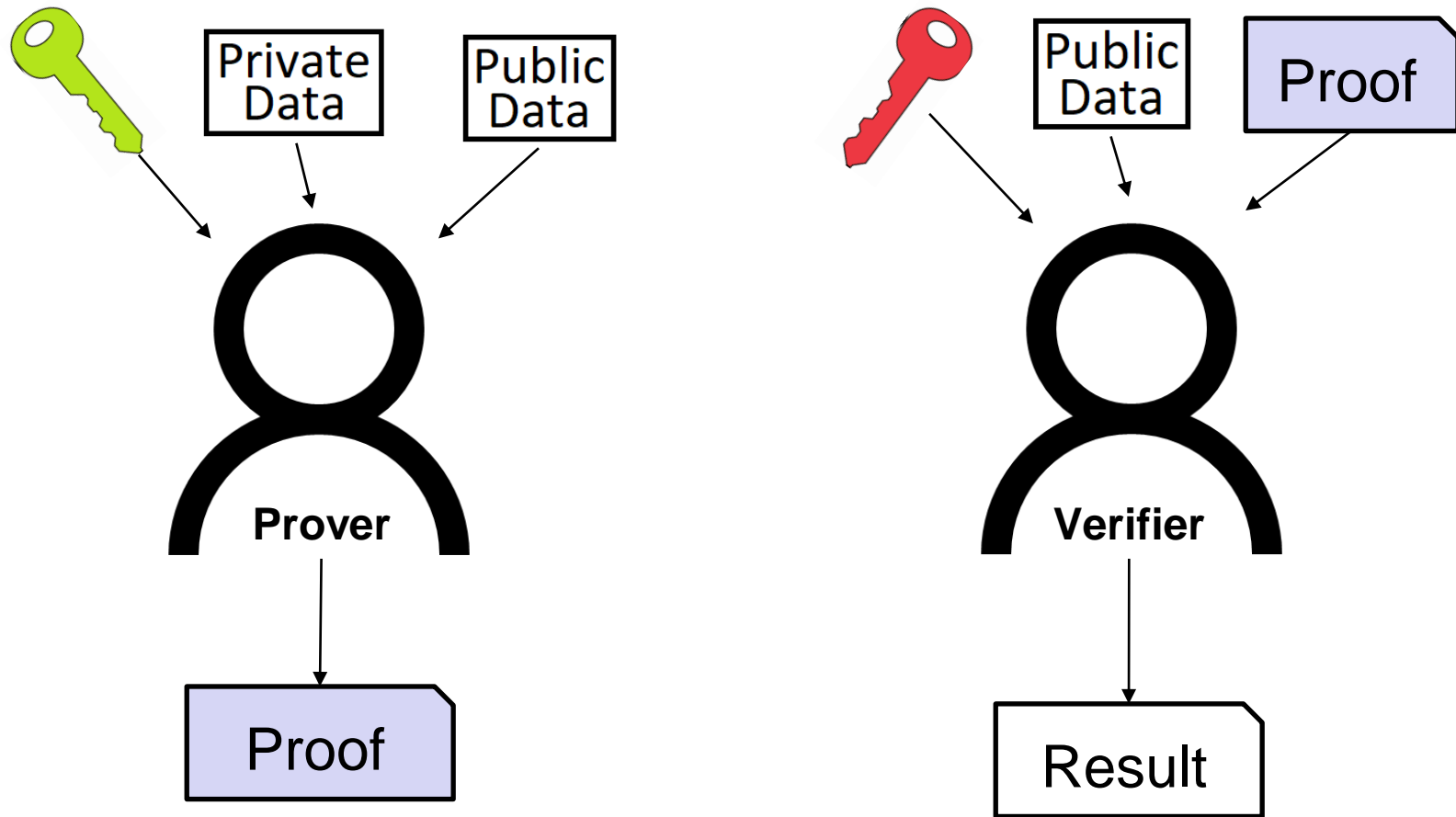
Rete decentralizzata.
Consente la registrazione
sicura e trasparente
di transazioni.



Dati registrati in blocchi
collegati in modo crittografico.



Dimostrare di possedere delle informazioni senza condividerle



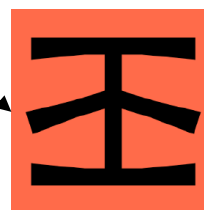
Metamask : portafoglio digitale di criptovalute

Ci permette di effettuare transazioni su reti blockchain.

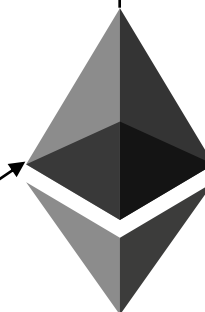
Collegamento alla blockchain tramite Infura



Metamask

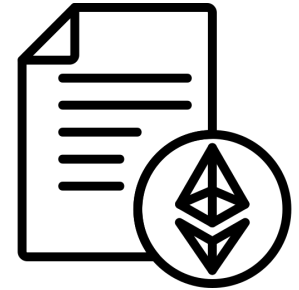


Infura



**EVM
Blockchain**

Smart contracts, codice autonomo
per eseguire contratti su blockchain



Scritti in linguaggio **Solidity** specifico
per smart contracts

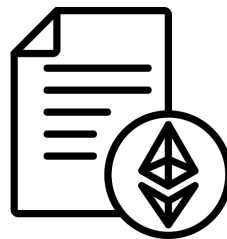
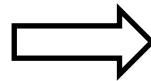
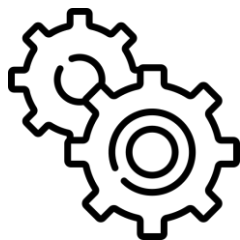
Sfruttando l'efficienza e la robustezza
del framework **Hardhat**



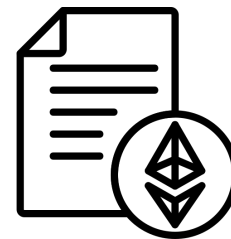


SnarkJS: Libreria JavaScript per costruzione di ZKP

Piattaforma di privacy decentralizzata che sfrutta la ZKP: **Tornado-Cash**

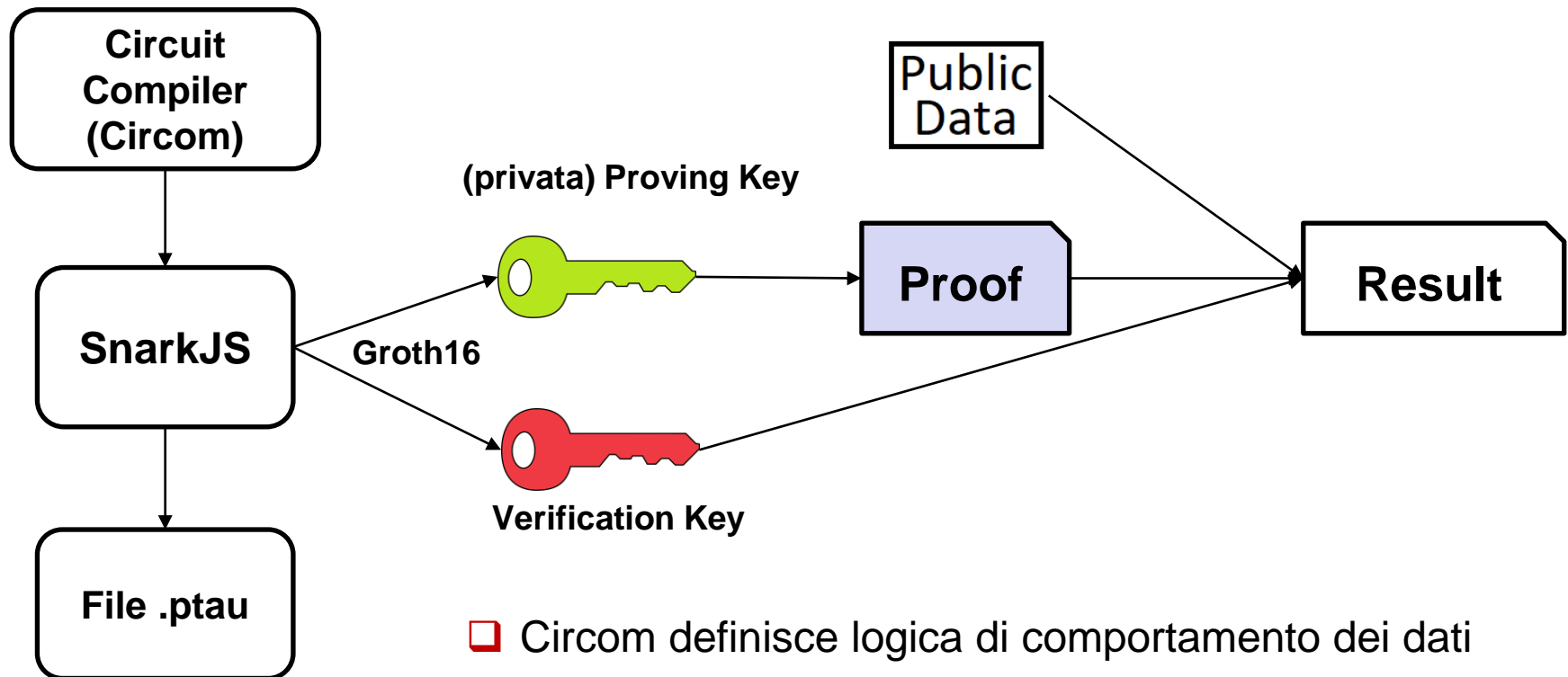


By Tornado-Cash



By me

Gestione chiavi e prove



- ❑ Circom definisce logica di comportamento dei dati
- ❑ File .ptau per memorizzare parametri crittografici
- ❑ SnarkJS usa file .ptau per generare le chiavi
- ❑ Groth16 : tipo di ZKSNARK proof system



Commitment e Nullifier



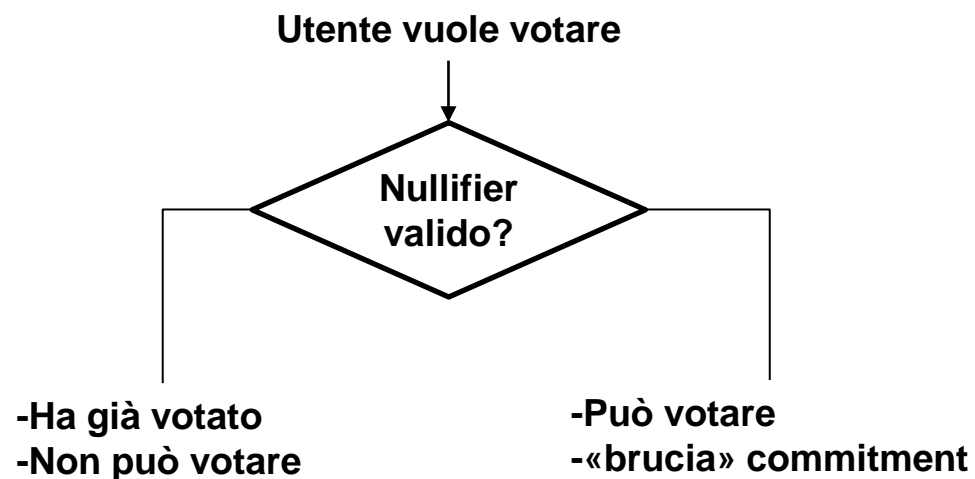
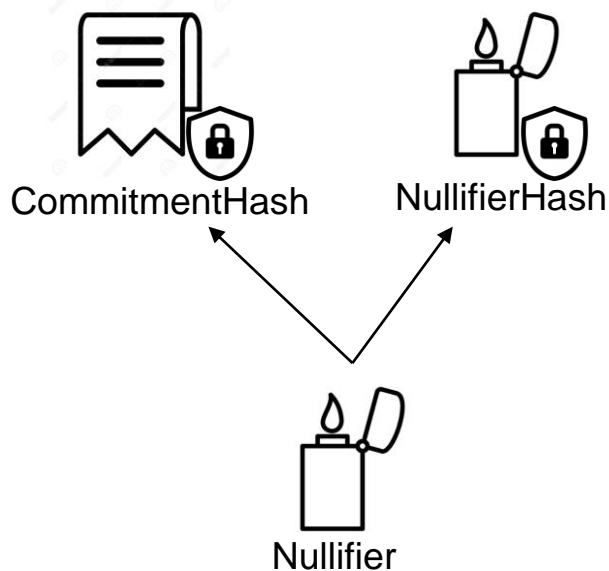
Generazione di Commitment e Nullifier quando un utente guadagna diritto di voto

Commitment

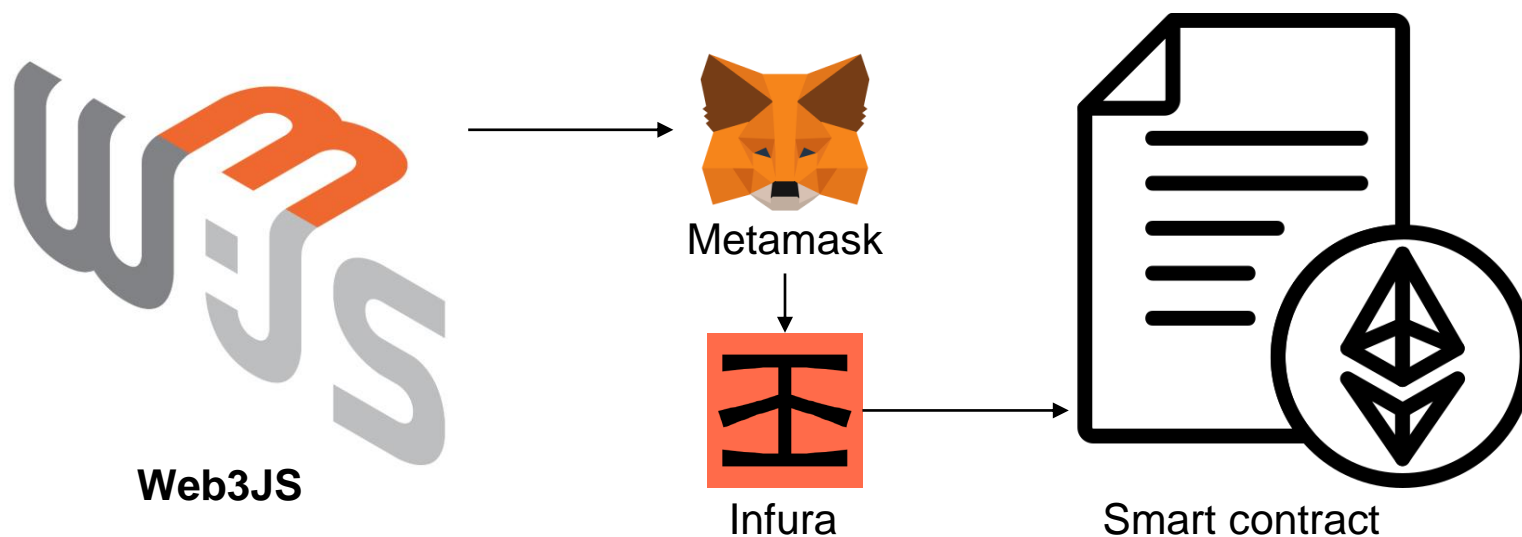
Diritto di voto dell'utente che
si impegna ad effettuare una votazione
Memorizzato in smart contract

Nullifier





Consuma il relativo commitment
se presente



Dal frontend agli smart contract



Problema principale

- ☐ File di definizione di tipo (.d.ts) del modulo «snarkjs» 
- ☐ File di definizione di tipo (.d.ts) del modulo «circomlibjs» 
- ☐ Gestione delle prove tramite Angular 
- ☐ Gestione delle prove «manualmente» 

Consuntivo

Attività	Ore spese
Incontri e analisi	30
Studio di fattibilità	15
Formazione	100
Sviluppo backend	75
Sviluppo frontend	50
Sviluppo test di unità	30
Verifica e validazione	20

File Prodotti
16

LoC
1032

Commenti
137

Metodi
71