UniRep Protocol

Chance Hudson

1. What is UniRep
2. Improving ZK/blockchain UX
3. Scaling ZK on blockchain

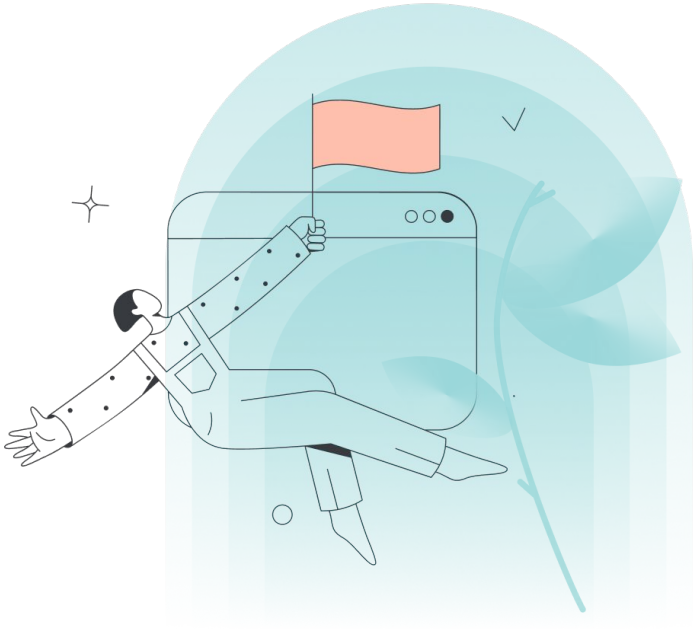
Universal Reputation

- Identity system
  - Public keys that change over time
- Attestation system
  - Attesters give reputation
  - Each attester has own reputation system
  - Positive/Negative rep
    - uint[2]
  - Graffiti
    - bytes32
- Users are anonymous
- Attestations are non-confidential

UniRep identity system

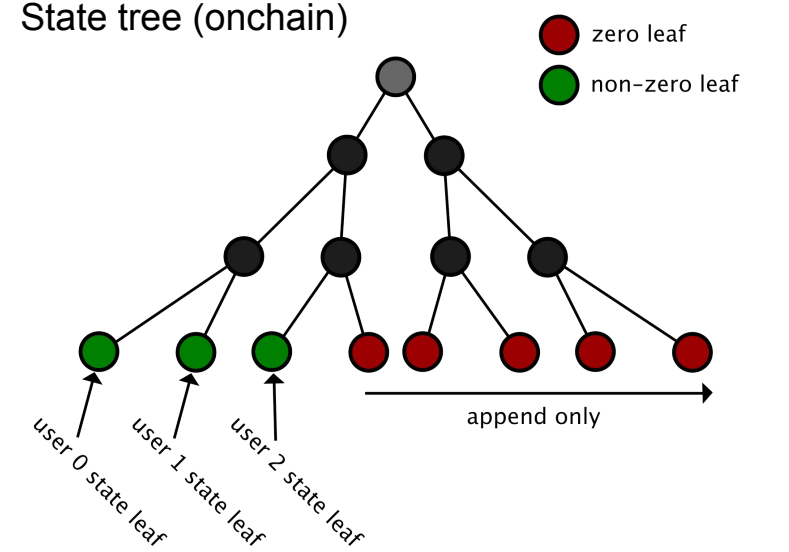
- Semaphore
  - Two secrets: **trapdoor**, **nullifier**
  - Public key: H(H(nullifier, trapdoor)
    - Aka “identity commitment”
  - H = Poseidon
  - ZK friendly/extensible identities

- UniRep anonymity
  - Epoch key = H(nullifier, attesterId, epoch, nonce)
  - Changes over time
  - Multiple keys per epoch (nonce)
  - Extensible



UniRep data structures

State tree (onchain)

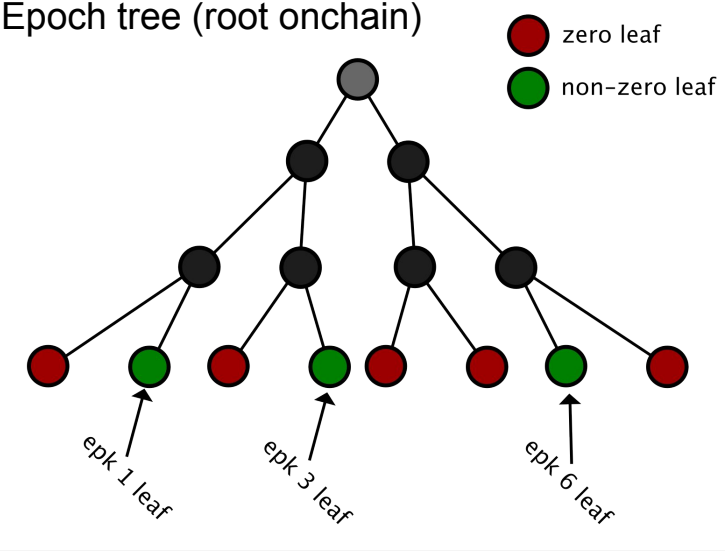


state leaf = H(idNullifier, attesterId, epoch, posRep, negRep)

private input

public input

Epoch tree (root onchain)

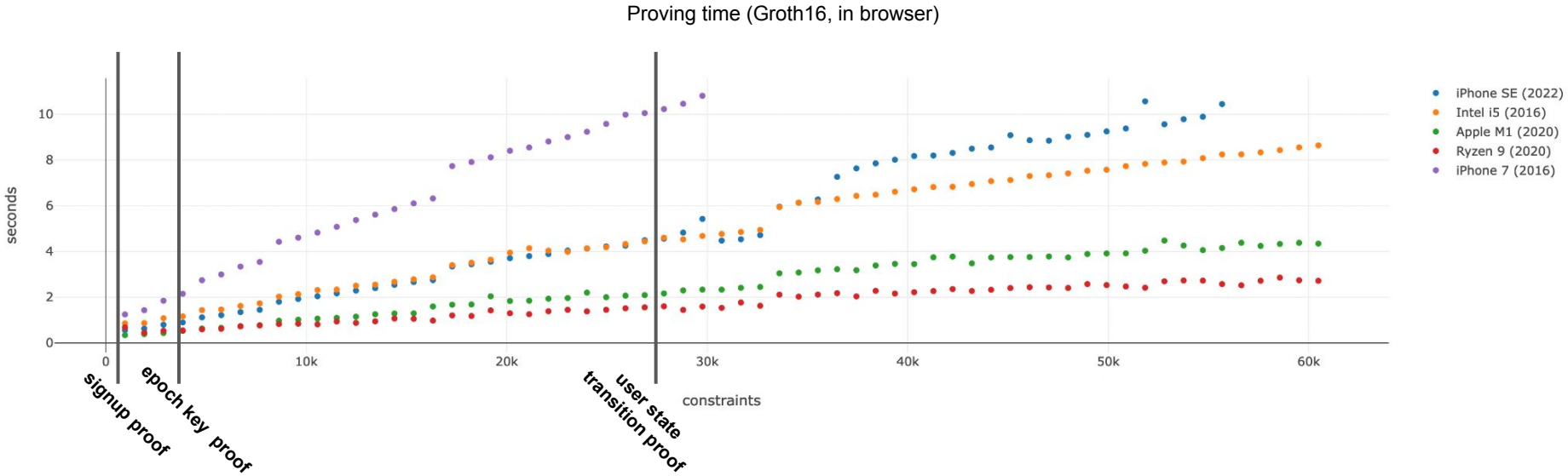


epoch tree leaf = H(posRep, negRep)

zero leaf = H(0, 0)

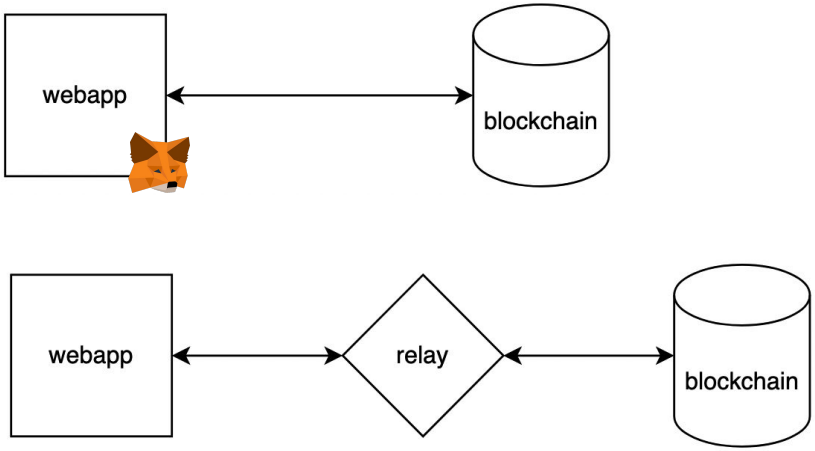
ZK UX

Better performance = better experience



ZK UX

Goal: users don’t need a wallet to use the blockchain

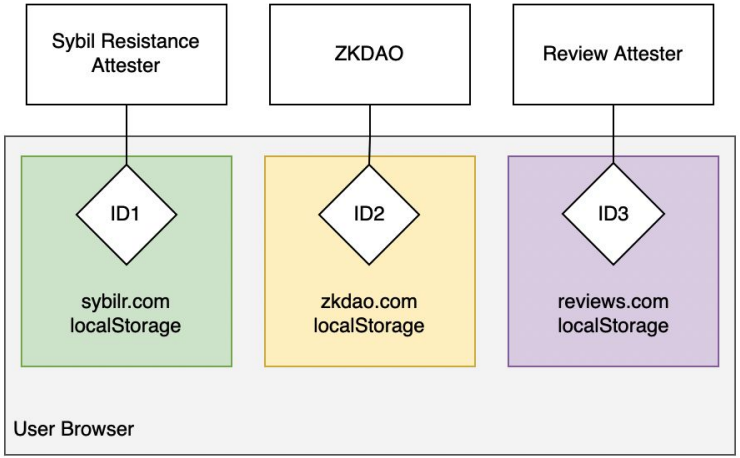


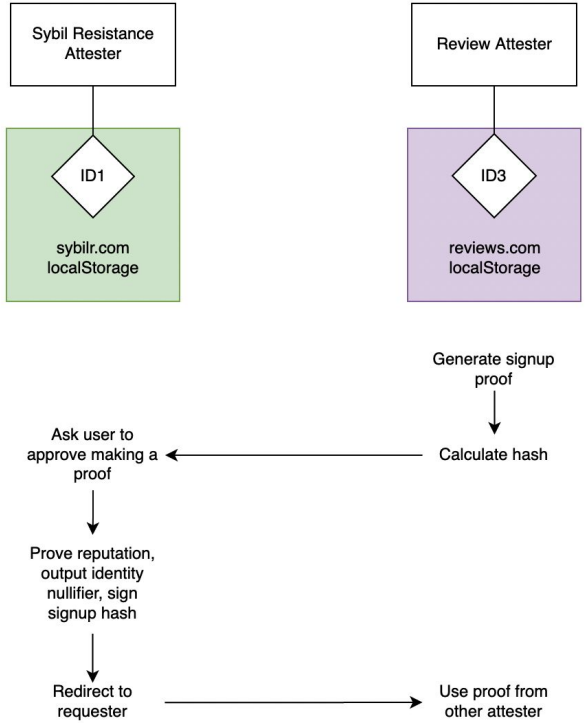
< 5 seconds

- Generate zk proof
- Send proof to relayer
- Relay sends tx to L2 node
- L2 node gives instant finality guarantee

Attester ecosystem

Many attesters each managing unique user identity





Scaling ZK

Calldata

- Groth16: 0.13 KB
- PLONK: 0.51 KB

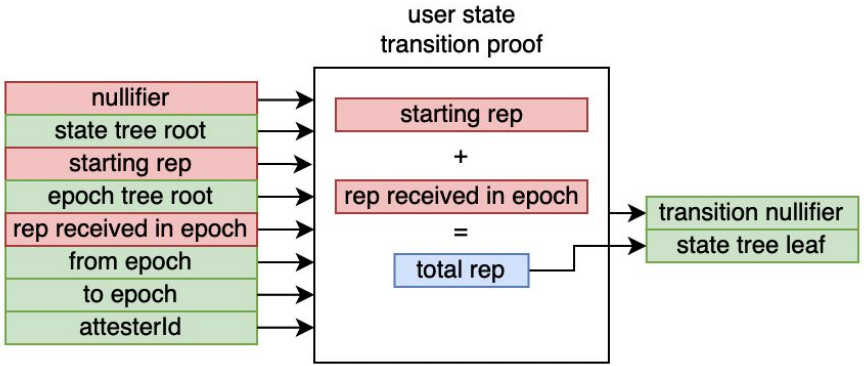
EIP 4844

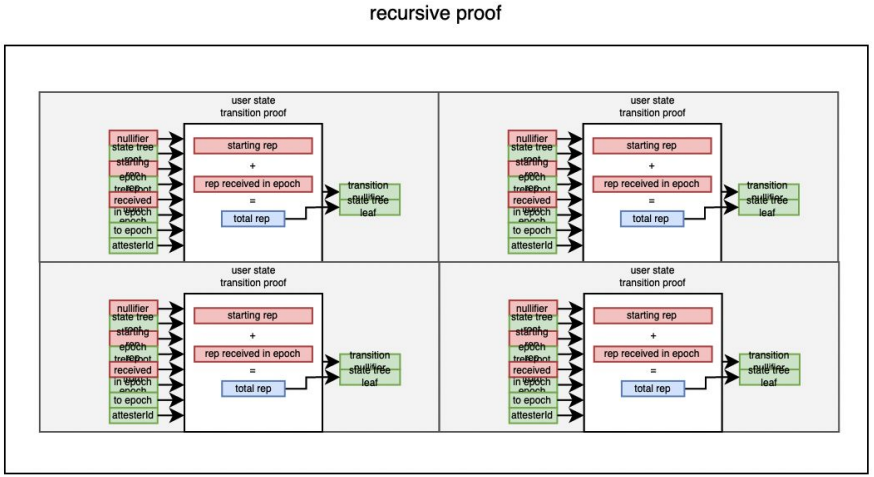
- 2 MB/block
- 1312 Groth16/second
- 335 PLONK/second

Verification

- Groth16/PLONK: ~250k gas
- Ethereum mainnet: 2.5M gas per second
- Arbitrum: 7M gas per second
  - 24 zk proofs per second

Scaling UniRep





~~Scale network throughput~~

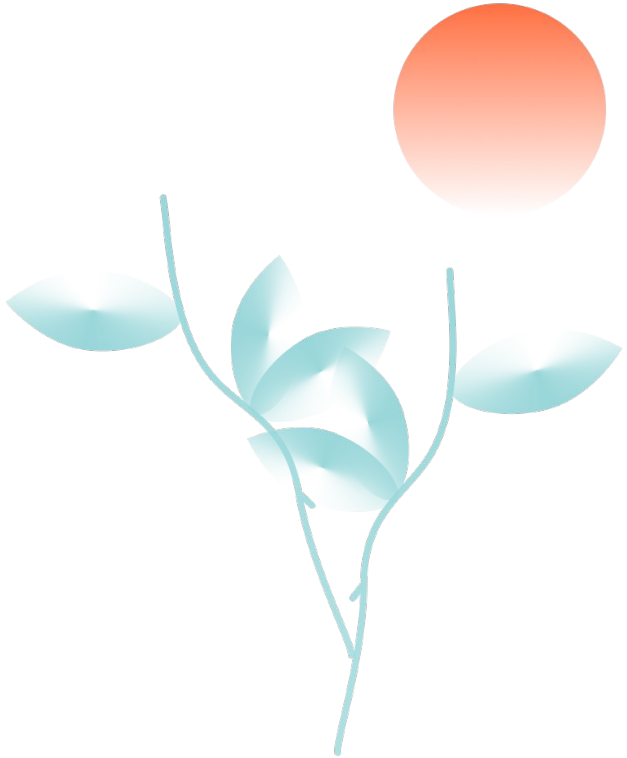
Scale offchain computation power

Attester ideas

- ZKDAO
- Anti-sybil reputation
- Recommendations
- Anonymously claim/prove a POAP

Nice to haves

- ZK directory
  - Hashes + human readable descriptions of zk proofs
- PLONK
  - After EIP 4844
  - No phase 2 trusted setup
- Easier browser proofs
  - Single WASM executable



Thank you!

- UniRep workshop (Friday, 10:30)
- Demo (Thursday, 15:00)
- github.com/unirep