Robust Anonymous UX

with the UniRep Protocol

1. What is anonymous data?
2. Example applications

Anonymous User Data

- Users control a private key
- Each user has their own data
- Applications can change data without knowing user identity
  - Unirep uses short lived “epoch keys” to identify users anonymously
- Data can be proven anonymously

Anonymous Applications

- User identity is not *always* known
- Users prove data as needed to perform actions

Can we build anonymous applications with the same user experience as non-anonymous applications?

Can we build Facebook where users are anonymous to the platform?

Can we build Amazon where users are anonymous to the platform?

Pros/cons of anon applications

Pros:

- Negate risk of user data hacks/sale
- More identity flexibility
- More interoperability (anyone can verify proofs)
    - Fewer walled gardens
- Users can leave the platform without deleting data

Cons:

- Complex/difficult to implement
- Potential false sense of security

Universal Reputation

- Allows ~200 bytes of data to be stored per user
- Applications can change data anonymously
  - Users can create ephemeral identifiers called “epoch keys”
- Users can prove data anonymously

- **Changing** user data requires write access to blockchain
- **Verifying** user data requires read only access to the blockchain

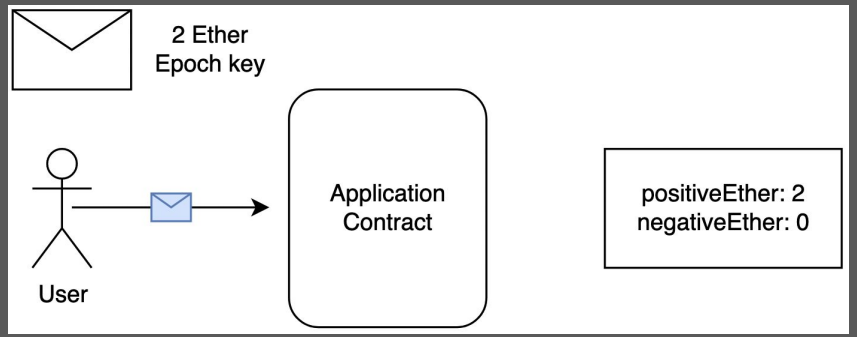
Examples

Anonymous payment system

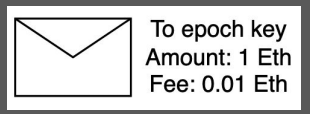
Transactions

- Ethereum address to epoch key (deposit)
- Epoch key to epoch key
- Epoch key to Ethereum address (withdrawal)

positiveEther: 0
negativeEther: 0



Sending Ether



(or Ethereum address)

positiveEther: 2
negativeEther: 1.01

KYC/AML verification

positiveEther: 2
negativeEther: 1.01
verified: 0

ID Verification

positiveEther: 2
negativeEther: 1.01
verified: 1

positiveEther: 2
negativeEther: 1.01
verified: 1
verifiedAt: 1677897237

Anonymous group chat for Ethereum addresses

Example groups

- ETH2 stakers
- ERC20/721 owners
- Addresses that sent a transaction before 2018

Every message contains a zk proof with

- Hash of message
- Proof of address ownership
- Proof of group membership

Proof of address = ~5 minutes

Prove address once, store it in user data

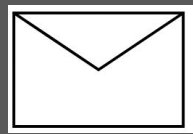
Proving user data = ~1 second

https://zketh.io

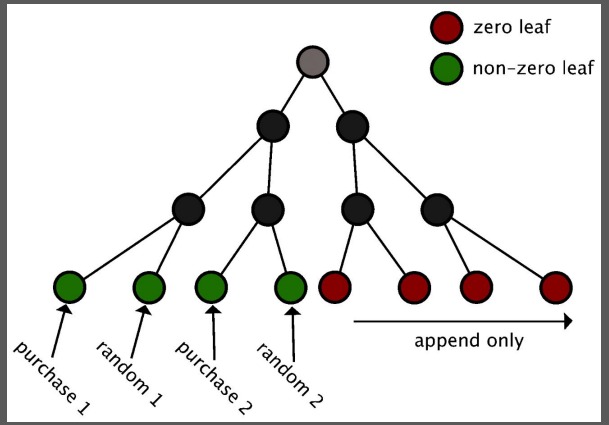
Online marketplace

- Buy things
- Store purchase history
- Recommend items based on purchase history
- Create/save lists of items

historyRoot: 0xa9b22f...
savedHash: 0x209bacf0...
positiveEther: 0
negativeEther: 0



Payment: 1 Eth
Encrypted purchase list
Encrypted deliver address



random(X) = H(idSecret, X)

Thank you!

https://zketh.io

https://demo.unirep.io

https://explorer.unirep.io