Privacy Layers for Ethereum

Why? What? How?

Wei Dai
Research Partner, Bain Capital Crypto

@_weidai
Privacy Layers for Ethereum

What?  Why?  How?
Privacy for Ethereum

Why?
All Ethereum transactions are public

Blockchain tech cannot go mainstream unless we have usable privacy
One main hurdles to mainstream adoption

Scalability

Privacy

Identity & recovery

Regulatory
Privacy <> Regulation & Sanctions

Self-sovereign privacy

Information and control of funds only by the user.
Users can still selectively disclose.
Ex. Tornado

Self-sovereign Authority-friendly privacy

Authority controlled blacklists or viewing keys
Ex. CAP from Espresso systems

Authority-controlled privacy

Authority controlled viewing keys & blacklist
Users still have privacy against other parties.
Ex. CBDC
Privacy for Ethereum

What?
<table>
<thead>
<tr>
<th>From:</th>
<th>0xab5801a7d398351b8be11c439e05c5b3259aec9b (Vb)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interacted With (To):</td>
<td>Contract 0x7a250d5630b4cf539739df2c5dacb4c659f2488d (Uniswap V2: Router 2)</td>
</tr>
<tr>
<td></td>
<td>TRANSFER 0.313761505136062667 Ether From Wrapped Ether To Uniswap V2: Router 2</td>
</tr>
<tr>
<td></td>
<td>TRANSFER 0.313761505136062667 Ether From Uniswap V2: Router 2 To Vb</td>
</tr>
</tbody>
</table>

**Tokens Transferred:**

<table>
<thead>
<tr>
<th>From:</th>
<th>To: Uniswap V2: ERC20 For 111,000,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vb</td>
<td>ERC20 (ERC20) ($1,028,149.71)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>From:</th>
<th>To: Uniswap V2: Rout... For</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uniswap V2: ERC20</td>
<td>Uniswap V2: Rout...</td>
</tr>
<tr>
<td>0.313761505136062667</td>
<td>($493.61) Wrapped Ether... (WETH)</td>
</tr>
</tbody>
</table>
Anonymity

From:

Interacted With (To):

Tokens Transferred:

- From Vb
  - To Uniswap V2: ERC20 For 111,000,000
    - ($1,028,149.71) → ERC20 (ERC20)

- From Uniswap V2: ER...
  - To Uniswap V2: Rout... For
    - 0.313761505136062667 ($493.61) → Wrapped Ether... (WETH)
Confidentiality is hard

Either require **trusted operating nodes** (zk-verified, e.g. STARKEKX exchanges) or requires more **sophisticated cryptography** (homomorphic encryption, MPC) or **trusted hardware** (TEEs)

https://wdai.us/posts/navigating-privacy/
Anonymity is “easy”

Withdraw

Contract calls

Deposit

We need to make this more usable!
**Goal:** Anonymity by default for Ethereum

<table>
<thead>
<tr>
<th>Txn Hash</th>
<th>Method</th>
<th>Block</th>
<th>Age</th>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>0xb150b4853e9db3a2b7...</td>
<td>Transfer</td>
<td>15712382</td>
<td>16 secs ago</td>
<td>0x!#%^!#$@$^</td>
<td>→ 0x47fc890be8b1070c114...</td>
</tr>
<tr>
<td>0xf65181af9a03a9ba05b...</td>
<td>Transfer</td>
<td>15712382</td>
<td>16 secs ago</td>
<td>0x!#%^!#$@$^</td>
<td>→ 0x643979a095a44ae43...</td>
</tr>
<tr>
<td>0xfa16e78a5d354ac121...</td>
<td>Claim Rank</td>
<td>15712382</td>
<td>16 secs ago</td>
<td>0x!#%^!#$@$^</td>
<td>→ 0x06450dee7fd2fb8e390...</td>
</tr>
<tr>
<td>0x920d06c3e8b687c9c3...</td>
<td>Renounce Ownersh...</td>
<td>15712382</td>
<td>16 secs ago</td>
<td>0x!#%^!#$@$^</td>
<td>→ 0x850f2f58556c6433e0...</td>
</tr>
<tr>
<td>0xe76b0527a224f10df6...</td>
<td>Contribute</td>
<td>15712382</td>
<td>16 secs ago</td>
<td>0x!#%^!#$@$^</td>
<td>→ 0x9080892d77c0013fcd...</td>
</tr>
<tr>
<td>0xdd25019b21564103f...</td>
<td>Submit</td>
<td>15712382</td>
<td>16 secs ago</td>
<td>0x!#%^!#$@$^</td>
<td>→ Lido: stMATIC Token</td>
</tr>
<tr>
<td>0xb9ed5d7ca6ad68eb...</td>
<td>Claim Rank</td>
<td>15712382</td>
<td>16 secs ago</td>
<td>0x!#%^!#$@$^</td>
<td>→ 0x06450dee7fd2fb8e390...</td>
</tr>
<tr>
<td>0x6e0993e5502958f28b...</td>
<td>Mint</td>
<td>15712382</td>
<td>16 secs ago</td>
<td>0x!#%^!#$@$^</td>
<td>→ 0x50ae01ec60059b60b6...</td>
</tr>
<tr>
<td>0x715bf75c196dd00eb...</td>
<td>Approve</td>
<td>15712382</td>
<td>16 secs ago</td>
<td>0x!#%^!#$@$^</td>
<td>→ Maker: Dai Stablecoin</td>
</tr>
<tr>
<td>0xa3779945451681ed27...</td>
<td>Claim Rank</td>
<td>15712382</td>
<td>16 secs ago</td>
<td>0x!#%^!#$@$^</td>
<td>→ 0x06450dee7fd2fb8e390...</td>
</tr>
<tr>
<td>0x6bf60712778de72d8f5...</td>
<td>Claim Rank</td>
<td>15712382</td>
<td>16 secs ago</td>
<td>0x!#%^!#$@$^</td>
<td>→ 0x06450dee7fd2fb8e390...</td>
</tr>
</tbody>
</table>
Anonymity by default for all dApps?

Evm chain

Tokens
- ERC20
  - DAI
- ERC721/1155
  - BAYC

Smart contract apps
- Uniswap
- OpenSea

Externally-owned accounts
- 0xA..
- 0xB..

Front-ends

Users

Wallets
Privacy Layers for Ethereum
Ethereum ecosystem and (asset) privacy solutions

- **Eth L1 and EVM L2s**
  - Mixers
  - Some evm defi inter-op

- **Evm applications**
  - zk curves
  - Aztec

- **“Alt” privacy chains**
  - Panther
  - Manta
  - Aleo
  - Swap only
  - Some evm defi inter-op

Privacy solution do not compose with most defi applications
What is a Privacy Layer

● Feature-complete
  ○ Support **usage with any** token-based smart-contract applications
    ■ Ideally with app-native interface
  ○ Support **verifiable disclosure** of asset ownership (like Semaphore)
    ■ Share that you have collection of NFTs and sign messages

● Backwards compatible
  ○ Support any ERC20/721/1155 tokens.
  ○ Support existing and legacy apps such as UniswapV2, etc.

● Anonymous (by default)
  ○ Every smart contract interaction should be from a one-time address
Privacy Layers for Ethereum

How?
Feature-complete and Backwards compatibility

● Feature-complete
  ○ Support **usage with any** token-based smart-contract applications
    ■ Ideally with app-native interface
  ○ Support **verifiable disclosure** of asset ownership
    ■ Share that you have collection of NFTs and sign messages

● Backwards compatible
  ○ Support any ERC20/721/1155 tokens.
  ○ Support existing and legacy apps such as UniswapV2, etc.

● Anonymous (by default)
  ○ Every smart contract interaction should be from a one-time address
Shielded Pool

“Zk Merkle” accounting
Deposit, withdraw

Deposit
Withdraw

Eth EOAs

?
Shielded Contract Wallet

1. Verify sig
2. Exec call

a) call = “0xC1, calldata1; 0xC2, calldata2; …”
b) Signature sig
Shielded Contract Wallet

Shielded Pool → Shielded Contract Wallet

Contract wallet
Shielded Contract Wallet

1. Verify \textit{sig}
2. Exec \textit{call}

**Shielded Pool**

“Zk Merkle” accounting

Deposit, withdraw

**Shielded Contract Wallet**

“Zk Merkle” accounting

Deposit, Withdraw, Call

**Smart contract wallet**
Shielded Contract Wallet

Uniswap

“Zk Merkle” accounting

Deposit, Withdraw, Call

OpenSea

Bonus: account abstraction (EIP-4337) compatible!
Problem 1: Arbitrary calls & Solution

**Shielded Contract Wallet** 0xSCW
“Zk Merkle” accounting
Deposit, Withdraw, Call
Owns: 20 WETH

**Vault** 0xV
Owns: 20 WETH

Solution

**Shielded Wallet** 0xSCW
“Zk Merkle” accounting
Deposit, Withdraw, Call

**Unshield 1WETH**
Call spends 20WETH

Owns: 1 WETH

Owns: 1 WETH
Alternative solution w/ Call Router

**Shielded Contract Wallet** 0xSCW
“Zk Merkle” accounting
Deposit, Withdraw, Call
Owns: 20 WETH

**Call Router 0xR**
Call

**Solution**

**Shielded Wallet** 0xSCW
“Zk Merkle” accounting
Deposit, Withdraw
Owns: 20 WETH

Unshield 1WETH
Call spends 20WETH

Owns: 1 WETH

Unshield 1WETH
Call spends 20WETH

Owns: 1 WETH
Problem 2: Unknown Output Amount

**Solution**

- **Shielded Contract Wallet 0xSCW**
  - “Zk Merkle” accounting
  - Deposit, Withdraw, Call

**Swap 1ETH to at least 1000 USDC**

**Note commitment determines refund amount**

- **Shielded Contract Wallet 0xSCW**
  - “Zk Merkle” accounting
  - Deposit, Withdraw, Call

**End of Call: Create note for anonAddr**

- **Swap 1ETH to at least 1000 USDC**
  - Refund to anonAddr
• **Privacy** is important

• **Shielded Contract Wallet** *(Anonymity by default)* is the best shot

• **We are building this out!**

Reach out if you are interested in contributing!

Wei Dai
Research Partner, Bain Capital Crypto
w.dai@baincapital.com
@_weidai