DeFi is missing a primitive. Privacy

How Aztec Connect allows for private access to DeFi

Jan Beneš
Aztec Network
GameStop short squeeze - Information leak in Web2.0
Situation in Web3 is even worse
User’s financial information is public

doxxed.eth's portfolio

V3 LP ETH-DAI

AAVE position with health factor 1.7

USD amount of available collateral
Why is this bad?

- Solvency assessment based on on-chain data. This info can be used by:
  - MEV bots
  - Adversarial parties in general

- Risk of doxing and consequences in the physical world
  - Frens shaming you for your bad trades
  - Target of crime
Solution?

Privacy preserving rollups!
Aztec Connect

- “VPN for Ethereum”
- web2 - replacing your IP address with shared one
- web3 - replacing your ethereum address with Aztec’s
The private DeFi yield aggregator for Ethereum.

zk.money is your portal to using Ethereum DeFi services with full privacy and up to 100x cost savings. Shield funds to start accessing!

Looking for old zk.money? What is Shielding? Read our FAQ
Pick a memorable alias

Your alias makes it simple for your friends to send you crypto.

⚠️ If you forget your alias, your account cannot be recovered.

@jan

Register
Creating your account...

This may take several minutes, please don't close the window.

Encrypting Data

Confirming account key and generating spending key
Shielding consists of:

a. A tx on Ethereum,

b. A creation of a cryptographic note allowing the user to spend the funds (called value note)
Net Worth

$343.31

$0.00 available

Shield additional funds from L1

Shield more

Tokens
Earn Positions

0.200000 zkETH

$343.31

Shield

0 available
Opportunities

**Euler Lending zkETH**
Lend ETH on Euler and earn yield by holding weWETH in exchange.
- APY: 2.43%
- L1 LIQUIDITY: $82M
- NEXT BATCH: ~7 mins
- USERS IN BATCH: 0/40

**Euler Lending zwstETH**
Lend wstETH on Euler and earn yield by holding weWstETH in exchange.
- APY: 0.56%
- L1 LIQUIDITY: $181M
- NEXT BATCH: ~7 mins
- USERS IN BATCH: 0/40

**Euler Lending zkDAI**
Lend DAI on Euler and earn yield by holding weDAI in exchange.
- APY: 1.16%
- L1 LIQUIDITY: $76M
- NEXT BATCH: ~7 mins
- USERS IN BATCH: 0/40
- L2 tx gets sent
- This tx gets processed by Aztec node and gets submitted on-chain in a rollup block
Join split circuit:
- Original value note is destroyed
- Claim note and a new value note is created

Claim note: Gives users a claim on the results (DeFi is composable - output tokens)
Value note: (remaining ETH)
How can this be private when the interaction happens on Ethereum?

- Thanks to ZKPs the info about which user initiated the interaction is secret
- Multiple users per one interaction

<table>
<thead>
<tr>
<th>From Aztec: Connect</th>
<th>To 0xfb554253737c4...</th>
<th>For 48.4 ($48.37) Dai Stablecoin (DAI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Aztec: Connect</td>
<td>To 0xa7133d17e0e65...</td>
<td>For 5,000 ($4,997.15) Dai Stablecoin (DAI)</td>
</tr>
<tr>
<td>From Aztec: Connect</td>
<td>To 0xdf97d89123d401...</td>
<td>For 10,000 ($9,994.30) Dai Stablecoin (DAI)</td>
</tr>
<tr>
<td>From Null Address: 0x00...</td>
<td>To 0xe71a50a78cccff...</td>
<td>For 0.014461543121571788 WETH yVault (ywWETH)</td>
</tr>
<tr>
<td>From 0xe71a50a78cccff...</td>
<td>To Alchemix Finance:...</td>
<td>For 0.014693 ($19.09) Wrapped Ethers (WETH)</td>
</tr>
<tr>
<td>From 0xe71a50a78cccff...</td>
<td>To Aztec: Connect</td>
<td>For 0.014461543121571788 WETH yVault (ywWETH)</td>
</tr>
<tr>
<td>From Aztec: Connect</td>
<td>To 0xe71a50a78cccff...</td>
<td>For 99 Dai yVault (ywDAI)</td>
</tr>
<tr>
<td>From 0xe71a50a78cccff...</td>
<td>To Null Address: 0x00...</td>
<td>For 99 Dai yVault (ywDAI)</td>
</tr>
<tr>
<td>From Alchemix Finance:...</td>
<td>To 0xe71a50a78cccff...</td>
<td>For 102.528836137458026867 ($102.47) Dai Stablecoin (DAI)</td>
</tr>
<tr>
<td>From 0xe71a50a78cccff...</td>
<td>To Aztec: Connect</td>
<td>For 102.528836137458026867 ($102.47) Dai Stablecoin (DAI)</td>
</tr>
</tbody>
</table>
Does it scale?

1 L1 transaction per multiple users

\[
\frac{\text{cost of posting a rollup}}{\# \text{ of txns in a rollup}} + \text{per-txn cost of call data} = \text{total cost pertxn}
\]

- \text{share of fixed costs}
  - Aztec can scale this!

- \text{variable costs}
  - Aztec can't scale this (It's up to Ethereum)

- With EIP-4844 user's cost gets close to \((L1 \text{ call gas costs}) / \text{(num users)}\)
How to integrate?

- Multi-sig free bridges
- "Token in - token out"
Limitations

- Long settlement time - (problems with slippage, liquidations)
- Limited amount of information on the input of bridges (only 64 bits of data - setting slippage a bit more tricky)
- Esoteric tokens having insufficient anonymity sets
- Protocols working with msg.sender (and not just with tokens) are non-trivial to integrate (e.g. borrowing on Liquity requires fixing CR)
Advantages

- Smart contracts don’t need to be redeployed on L2
  - Liquidity not fractured
  - Low risk for integrated protocols
Non-DeFi usecases

- Private DAO voting, private NFT purchase or minting etc.
Thank you!

Jan Beneš
Aztec Network
jan@aztecprotocol.com

@janbenes16