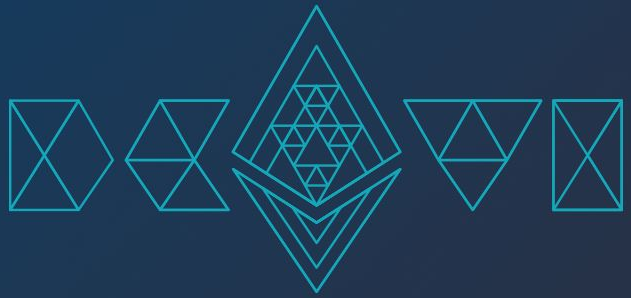


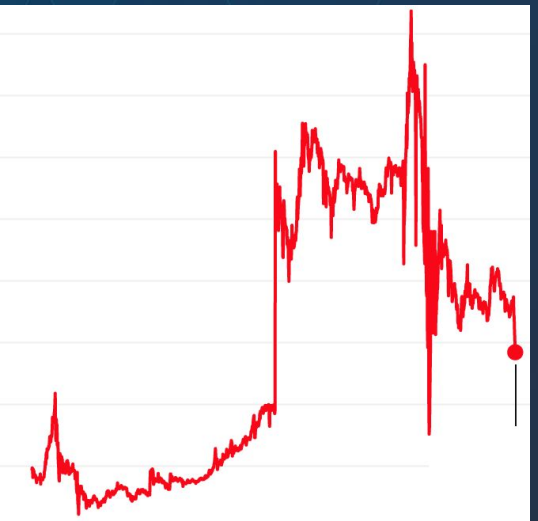
DeFi is missing a primitive. Privacy

How Aztec Connect allows for private access to DeFi

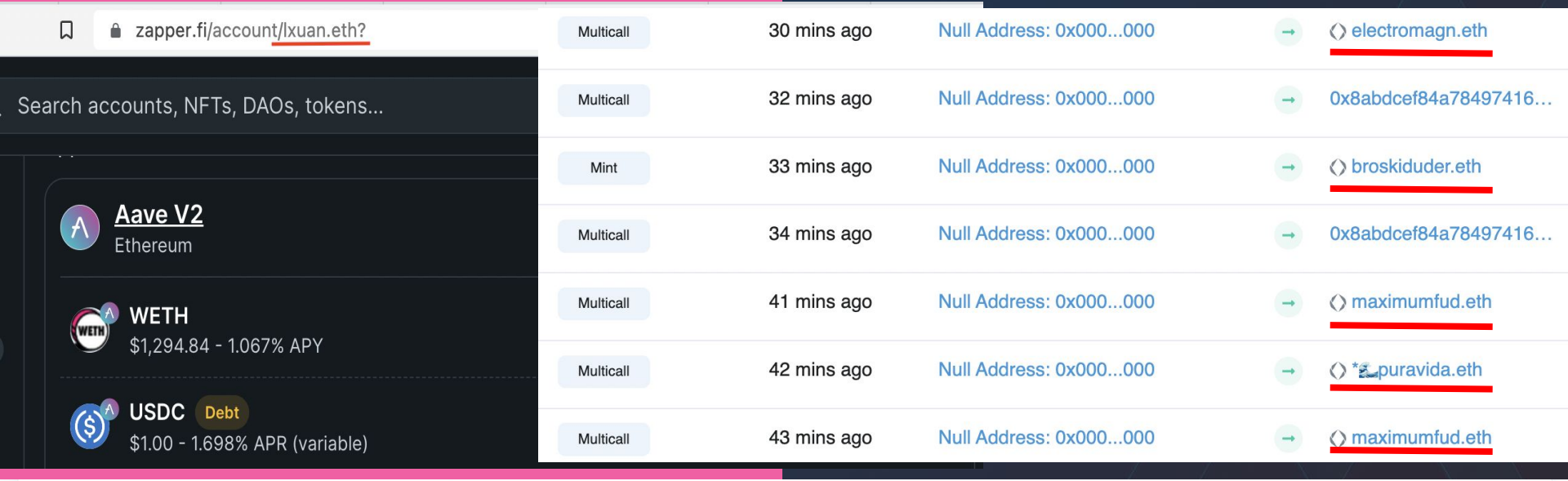
Jan Beneš

Aztec Network

GameStop short squeeze - Information leak in Web2.0



Situation in Web3 is even worse



0xe538eb7387bfc663c3f...	Exact Input Sing...	15725923	22 hrs ago	0x33c6b73432b3aea0c1...	IN	Uniswap V3: Router	0 Ether	0.00591225
0x1a5979ef0bec53cc75f...	Exact Input Sing...	15725921	22 hrs ago	0x33c6b73432b3aea0c1...	IN	Uniswap V3: Router	0 Ether	0.00543643
0x36ac29776af4fc22ae7...	Exact Input	15725908	22 hrs 3 mins ago	yjfos.eth	IN	Uniswap V3: Router	0 Ether	0.00613723
0x877d779220c847e45f...	Exact Input	15725906	22 hrs 3 mins ago	0xa26c6be0770a1c62df...	IN	Uniswap V3: Router	0 Ether	0.00668768

User’s financial information is public

doxed.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?

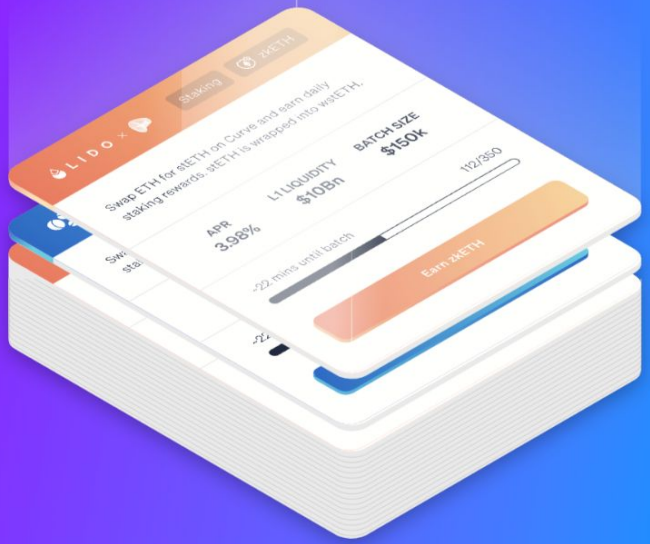
Privacy preserving rollups!

Aztec Connect

- “VPN for Ethereum”
- web2 - replacing your IP address with shared one
- web3 - replacing your ethereum address with Aztec’s

zk.money

Earn Trade Log In



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!

Shield Now

Looking for old zk.money?

What is Shielding? Read our FAQ

zk.money

Earn Trade Log In

1 2 3

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

zk.money

Earn Trade

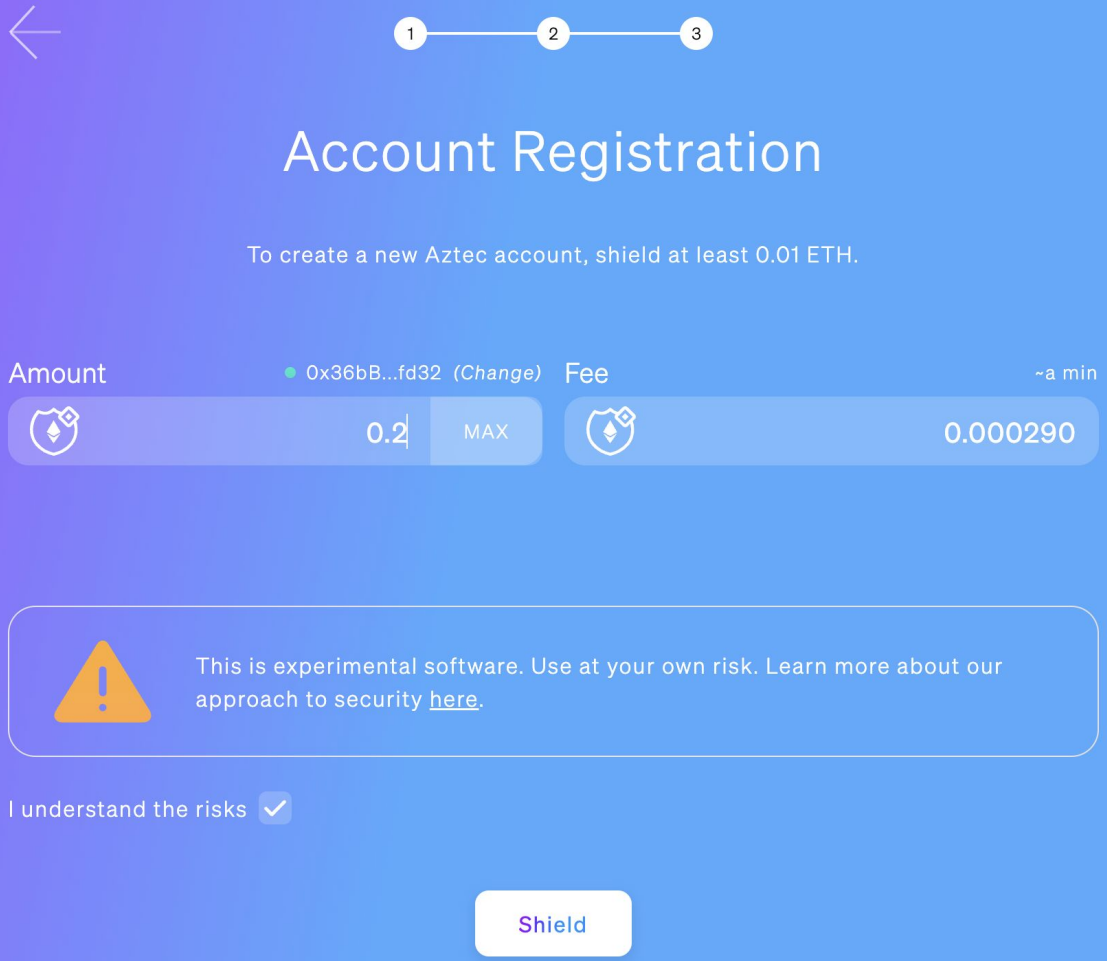
1 2 3

Creating **your** account...

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

Encrypting Data

Confirming account key and generating spending key



1. 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)

zk.money

Earn Trade Wallet @jan

Net Worth

$343.31

$0.00 available

Shield additional funds from L1

Shield more

Tokens Earn Positions

0.200000 zkETH
0 available

$343.31

Shield

zk.money

Earn Trade Wallet @jan

Opportunities

Type Project Asset Search...

Euler — Lending — zkETH

Lend ETH on Euler and earn yield by holding weWETH in exchange.

APY	L1 LIQUIDITY	NEXT BATCH
2.43%	$82M	~7 mins

USERS IN BATCH 0/40

Earn

Euler — Lending — zkwstETH

Lend wstETH on Euler and earn yield by holding wewstETH in exchange.

APY	L1 LIQUIDITY	NEXT BATCH
0.56%	$181M	~7 mins

USERS IN BATCH 0/40

Earn

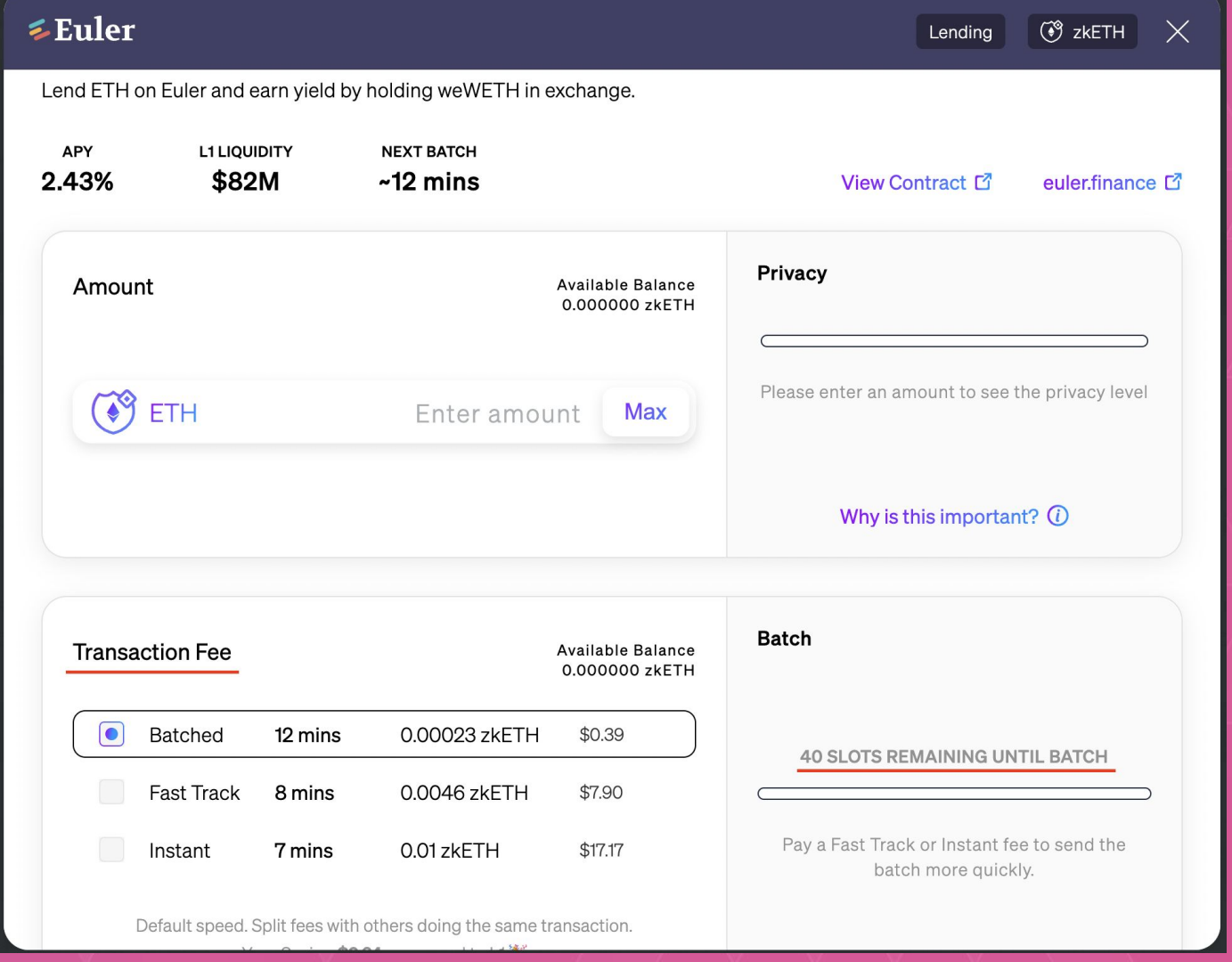
Euler — Lending — zkDAI

Lend DAI on Euler and earn yield by holding weDAI in exchange.

APY	L1 LIQUIDITY	NEXT BATCH
1.16%	$76M	~7 mins

USERS IN BATCH 0/40

Earn



- 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

From Aztec: Connect	To 0xfb554253737c4…	For 48.4 ($48.37)	Dai Stableco... (DAI)
From Aztec: Connect	To 0xa7133d17e0e65…	For 5,000 ($4,997.15)	Dai Stableco... (DAI)
From Aztec: Connect	To 0xf97d89123d401…	For 10,000 ($9,994.30)	Dai Stableco... (DAI)
From Null Address: 0x00…	To 0xe71a50a78cccff…	For 0.014461543121571788	WETH yVault (yvWETH)
From 0xe71a50a78cccff…	To Alchemix Finance:…	For 0.014693 ($19.09)	Wrapped Ethe... (WETH)
From 0xe71a50a78cccff…	To Aztec: Connect	For 0.014461543121571788	WETH yVault (yvWETH)
From Aztec: Connect	To 0xe71a50a78cccff…	For 99	DAI yVault (yvDAI)
From 0xe71a50a78cccff…	To Null Address: 0x00…	For 99	DAI yVault (yvDAI)
From Alchemix Finance:…	To 0xe71a50a78cccff…	For 102.528836137458026867 ($102.47)	Dai Stableco... (DAI)
From 0xe71a50a78cccff…	To Aztec: Connect	For 102.528836137458026867 ($102.47)	Dai Stableco... (DAI)

>50000 users

Does it scale?

1 L1 transaction per multiple users

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

↑ **share of fixed costs**

Aztec can scale this!

😁

↑ **variable costs**

Aztec can't scale this
(It's up to Ethereum)

😔

- With EIP-4844 user's cost gets close to (L1 call gas costs) / (num users)

```
interface IDefiBridge {
    function convert(
        AztecTypes.AztecAsset calldata _inputAssetA,
        AztecTypes.AztecAsset calldata _inputAssetB,
        AztecTypes.AztecAsset calldata _outputAssetA,
        AztecTypes.AztecAsset calldata _outputAssetB,
        uint256 _totalInputValue,
        uint256 _interactionNonce,
        uint64 _auxData,
        address _rollupBeneficiary
    )
        external
        payable
        returns (
            uint256 outputValueA,
            uint256 outputValueB,
            bool isAsync
        );
```

How to integrate?

- Multi-sig free bridges
- “Token in - token out”

```
if (_auxData == 0) {
    // Issuing new shares - input can be ETH
    if (_inputAssetA.assetType == AztecTypes.AztecAssetType.ETH) {
        WETH.deposit{value: _totalInputValue}();
        inputToken = address(WETH);
    }
    // If input asset is not the vault asset (or ETH if vault asset is WETH) the following will revert when
    // trying to pull the funds from the bridge
    outputValueA = IERC4626(_outputAssetA.erc20Address).deposit(_totalInputValue, address(this));
} else if (_auxData == 1) {
    // Redeeming shares
    // If output asset is not the vault asset the convert call will revert when RollupProcessor tries to pull
    // the funds from the bridge
    outputValueA = IERC4626(_inputAssetA.erc20Address).redeem(_totalInputValue, address(this), address(this))

    if (_outputAssetA.assetType == AztecTypes.AztecAssetType.ETH) {
        IWETH(WETH).withdraw(outputValueA);
        IRollupProcessor(ROLLUP_PROCESSOR).receiveEthFromBridge{value: outputValueA}(_interactionNonce);
        outputToken = address(WETH);
    }
```

Limitations

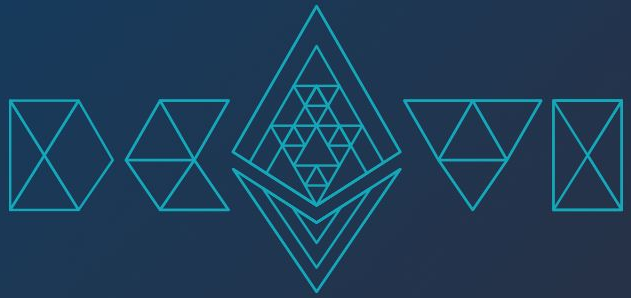
- Long settlement time - (problems with slippage, liquidations)
- Limited amount of information on the input of bridges (only 64 bits of data - setting slippage a bit more tricky)
- Esoteric tokens having insufficient anonymity sets
- Protocols working with msg.sender (and not just with tokens) are non-trivial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