



# 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?

Blockchain tech cannot go mainstream unless we have usable privacy

All Ethereum transactions are public

② From: [0xab5801a7d398351b8be11c439e05c5b3259aec9b](#) (Vb)

② Interacted With (To): [Contract 0x7a250d5630b4cf539739df2c5dadb4c659f2488d](#) (Uniswap V2: Router 2)

↳ TRANSFER 0.313761505136062667 Ether From [Wrapped Ether](#) To → [Uniswap V2: Router 2](#)

↳ TRANSFER 0.313761505136062667 Ether From [Uniswap V2: Router 2](#) To → [Vb](#)

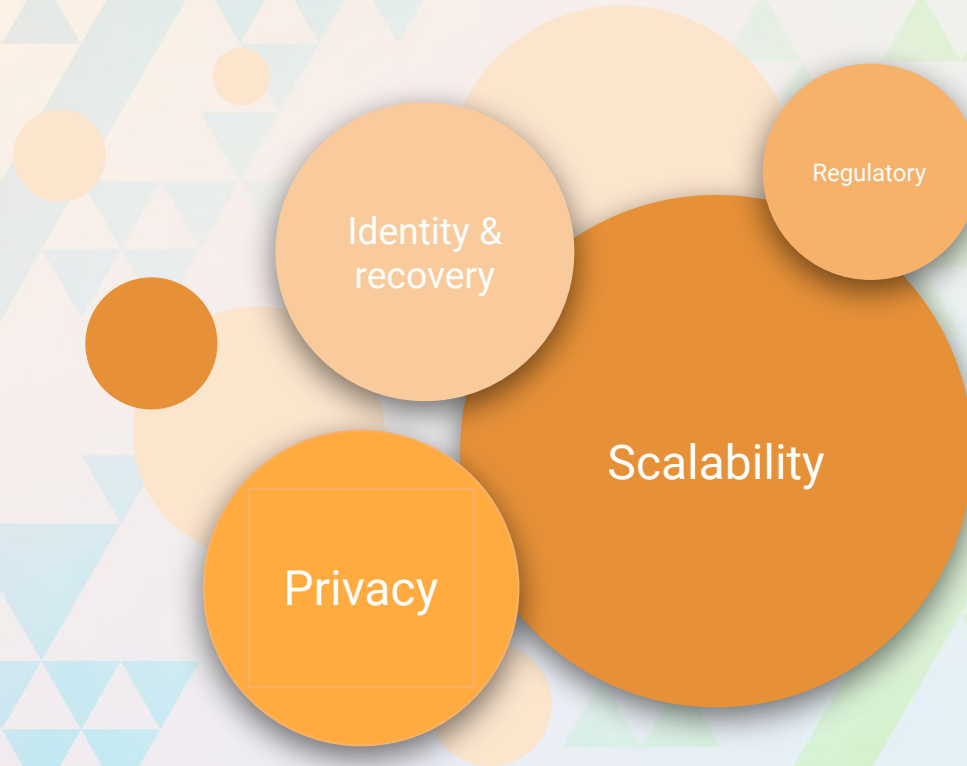
---

② Tokens Transferred: 2

↳ From [Vb](#) To [Uniswap V2: ERC20](#) For 111,000,000 (\$1,028,149.71) [ERC20 \(ERC20\)](#)

↳ From [Uniswap V2: Router 2](#) To [Uniswap V2: Router 2](#) For 0.313761505136062667 (\$493.61) [Wrapped Ether \(WETH\)](#)

# One main hurdles to mainstream adoption



# 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?**

# Transparent

🔍 From: [0xab5801a7d398351b8be11c439e05c5b3259aec9b](#) (Vb) 


🔍 Interacted With (To): [Contract 0x7a250d5630b4cf539739df2c5dacb4c659f2488d](#) (Uniswap V2: Router 2)  


↳ TRANSFER 0.313761505136062667 Ether From [Wrapped Ether](#) To → [Uniswap V2: Router 2](#)

↳ TRANSFER 0.313761505136062667 Ether From [Uniswap V2: Router 2](#) To → [Vb](#)

---

🔍 Tokens Transferred: 2

▶ From [Vb](#) To [Uniswap V2: ERC20](#) For 111,000,000  ERC20 (ERC20) (\$1,028,149.71)

▶ From [Uniswap V2: ERC20](#) To [Uniswap V2: Router 2](#) For 0.313761505136062667  Wrapped Ether (WETH) (\$493.61)



# Anonymity

② From:

0x!#%^!#\$@\$\$^

② Interacted With (To):

🔍 Contract [0x7a250d5630b4cf539739df2c5dacb4c659f2488d](#) (Uniswap V2:

Router 2) ✓ 📄

↳ TRANSFER 0.313761505136062667 Ether From [Wrapped Ether](#) To →

[Uniswap V2: Rou...](#)

↳ TRANSFER 0.313761505136062667 Ether From [Uniswap V2: Rou...](#) To →

[Vb](#)

② Tokens

Transferred:

2

▸ 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 Ethe... \(WETH\)](#)

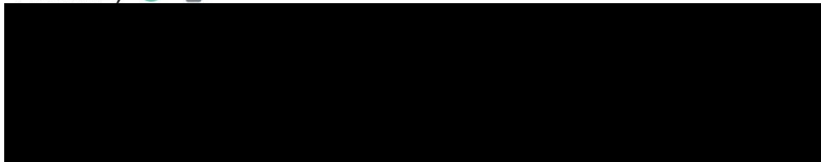
# Confidentiality

① From:

0xab5801a7d398351b8be11c439e05c5b3259aec9b (Vb) 

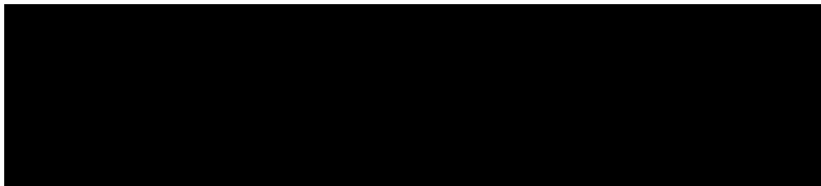
② Interacted With (To):

 Contract 0x7a250d5630b4cf539739df2c5dacb4c659f2488d (Uniswap V2:  
Router 2)  






③ Tokens  
Transferred:

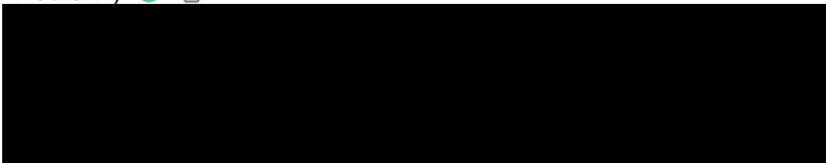
2




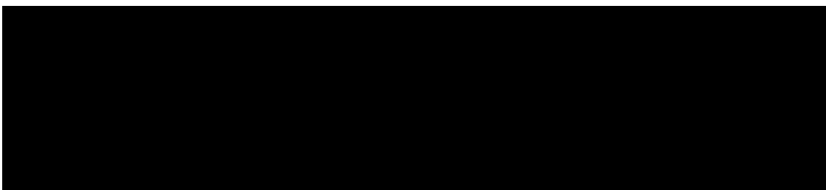
# Confidentiality is hard

② From: [0xab5801a7d398351b8be11c439e05c5b3259aec9b](#) (Vb) 

② Interacted With (To): [Contract 0x7a250d5630b4cf539739df2c5dacb4c659f2488d](#) (Uniswap V2: Router 2)  





---

② Tokens Transferred:  

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

# Anonymity is “easy”

From: 0x!#%^!#\$@\$^


Interacted With (To): [Contract 0x7a250d5630b4cf539739df2c5dacb4c659f2488d](#) (Uniswap V2: Router 2)  


TRANSFER 0.313761505136062667 Ether From [Wrapped Ether](#) To → [Uniswap V2: Rou...](#)

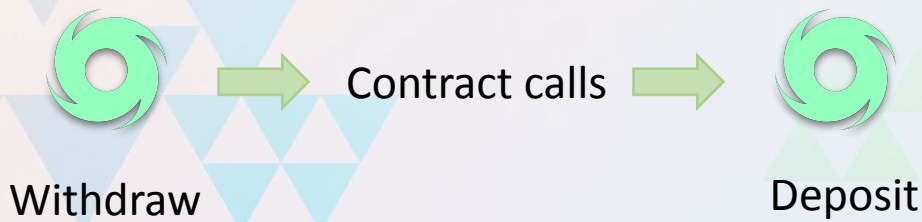
TRANSFER 0.313761505136062667 Ether From [Uniswap V2: Rou...](#) To → [Vb](#)

Tokens Transferred:

2
































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 Ethe...](#) (WETH)

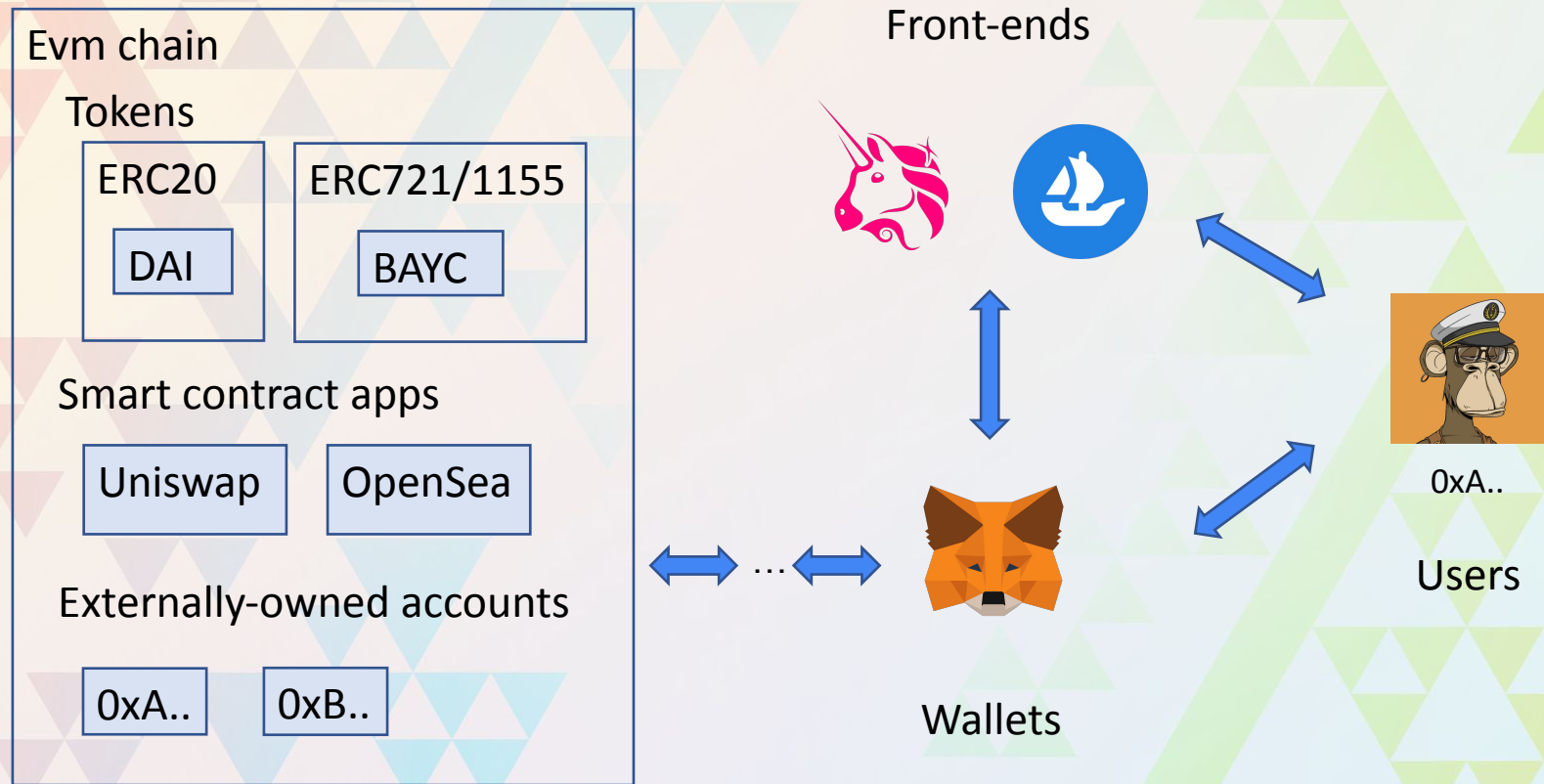


We need to make this more usable!

# Goal: Anonymity by default for Ethereum

Txn Hash	Method <sup>①</sup>	Block	Age	From	To
 <a href="#">0xb150b4853e9db3a2b7...</a>	Transfer	<a href="#">15712382</a>	16 secs ago	0x!#%^!#\$@\$^	 <a href="#">0x47fc890be8b1070c114...</a>
 <a href="#">0xf65181af9a03a9ba05b...</a>	Transfer	<a href="#">15712382</a>	16 secs ago	0x!#%^!#\$@\$^	 <a href="#">0x643979a095a44bae43...</a>
 <a href="#">0xfa16e78a5d354ac121...</a>	Claim Rank	<a href="#">15712382</a>	16 secs ago	0x!#%^!#\$@\$^	  <a href="#">0x06450dee7fd2fb8e390...</a>
 <a href="#">0x920d06c3e8b687c9c3...</a>	Renounce Ownersh...	<a href="#">15712382</a>	16 secs ago	0x!#%^!#\$@\$^	  <a href="#">0x850fb2f58556c6433e0...</a>
 <a href="#">0x8e76b0527a224f10df6...</a>	Contribute	<a href="#">15712382</a>	16 secs ago	0x!#%^!#\$@\$^	  <a href="#">0x9080892d77c0013fcd...</a>
 <a href="#">0xdd25019b2156e4103f...</a>	Submit	<a href="#">15712382</a>	16 secs ago	0x!#%^!#\$@\$^	  Lido: stMATIC Token
 <a href="#">0x1b9edb5d7ca6ad68eb...</a>	Claim Rank	<a href="#">15712382</a>	16 secs ago	0x!#%^!#\$@\$^	  <a href="#">0x06450dee7fd2fb8e390...</a>
 <a href="#">0x6e0993e5502958f28b...</a>	Mint	<a href="#">15712382</a>	16 secs ago	0x!#%^!#\$@\$^	  <a href="#">0x50ae01ec60059b60b6...</a>
 <a href="#">0x715bfb75c196dd00eb...</a>	Approve	<a href="#">15712382</a>	16 secs ago	0x!#%^!#\$@\$^	  Maker: Dai Stablecoin
 <a href="#">0xa3779945451681ed27...</a>	Claim Rank	<a href="#">15712382</a>	16 secs ago	0x!#%^!#\$@\$^	  <a href="#">0x06450dee7fd2fb8e390...</a>
 <a href="#">0x6bf60712778de72d8f5...</a>	Claim Rank	<a href="#">15712382</a>	16 secs ago	0x!#%^!#\$@\$^	  <a href="#">0x06450dee7fd2fb8e390...</a>

# Anonymity by default for all dApps?





# Privacy Layers for Ethereum



# Ethereum ecosystem and (asset) privacy solutions

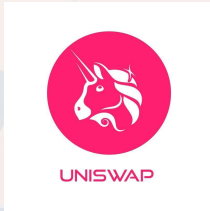
## Eth L1 and EVM L2s



## Evm applications



...

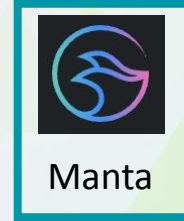


...

## Mixers



## "Alt" privacy chains



Swap only

Some evm defi inter-op

OpenSea



Compound

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

Smart contract wallet

- 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

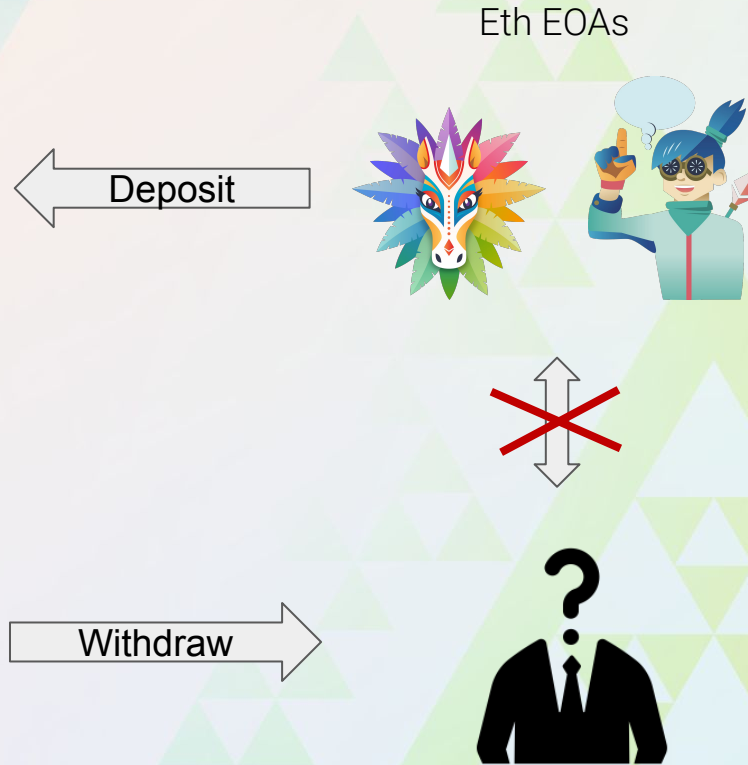
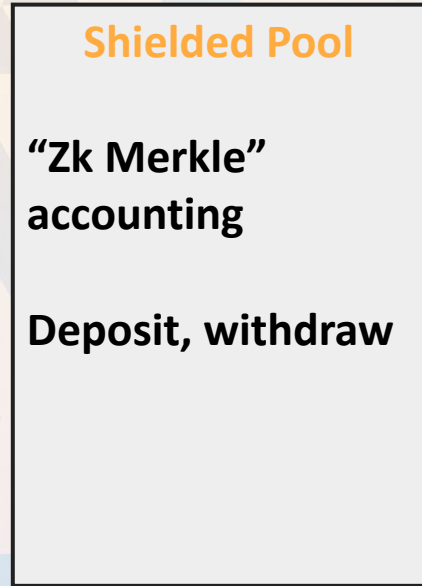
- Support any ERC20/721/1155 tokens.
- Support existing and legacy apps such as UniswapV2, etc.

## ● Anonymous (by default)

- Every smart contract interaction should be from a one-time address

Shielded pool

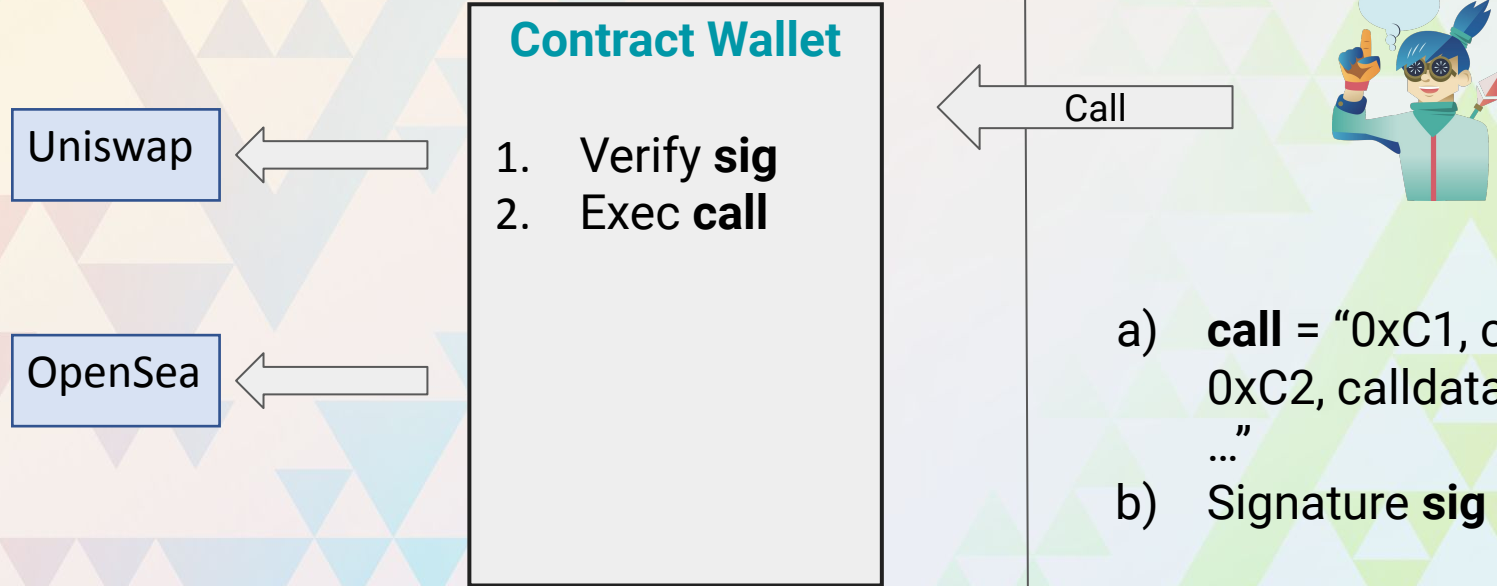
# Shielded Pool



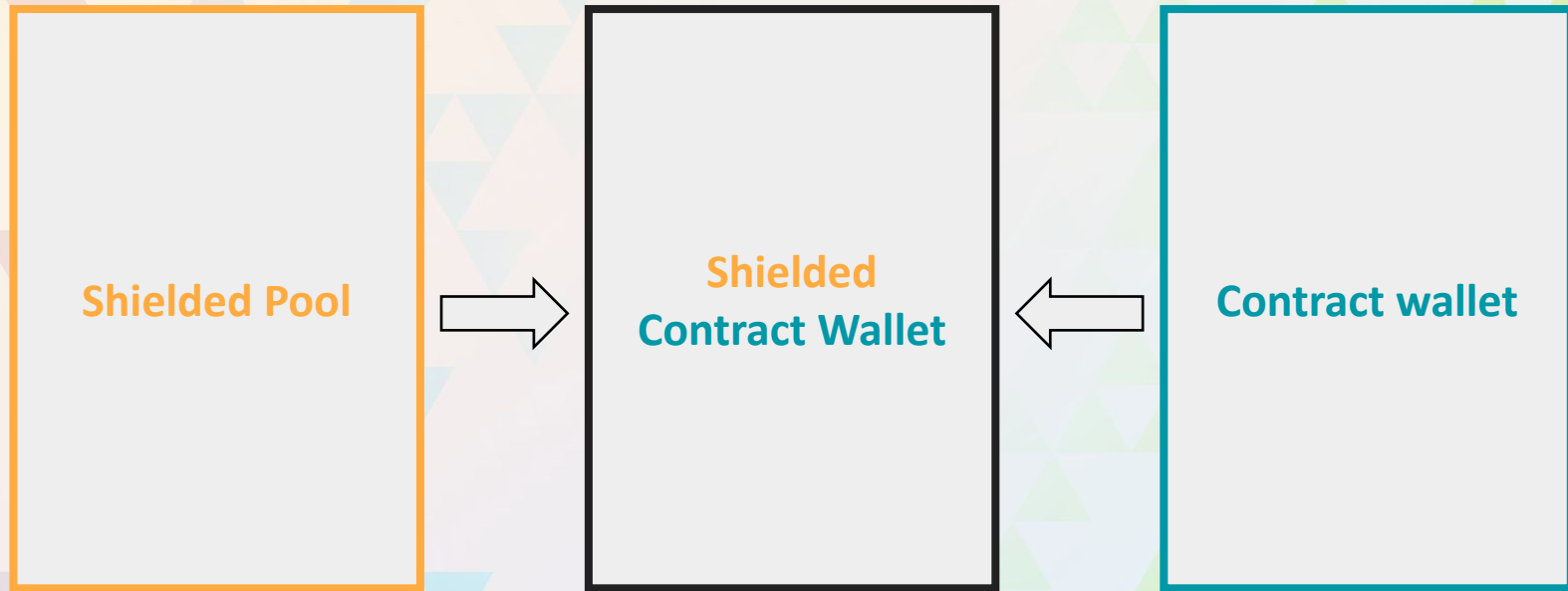
# Shielded Contract Wallet

Eth contracts and EOAs

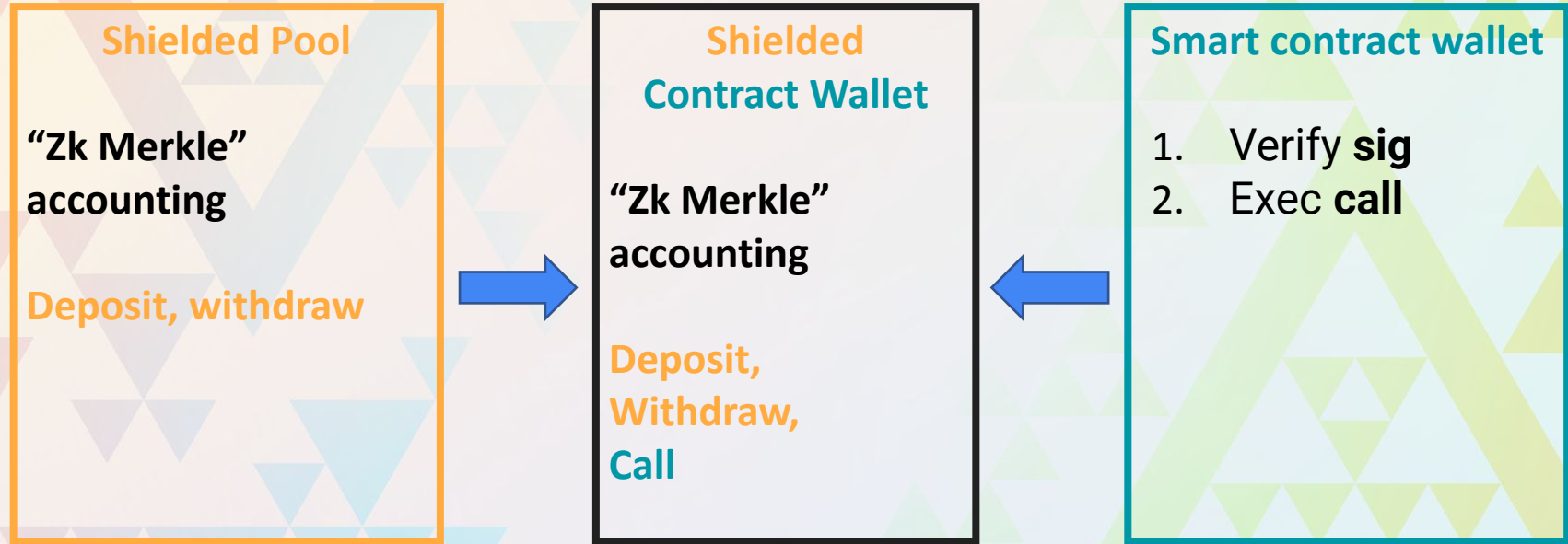
Shielded Wallet users



# Shielded Contract Wallet

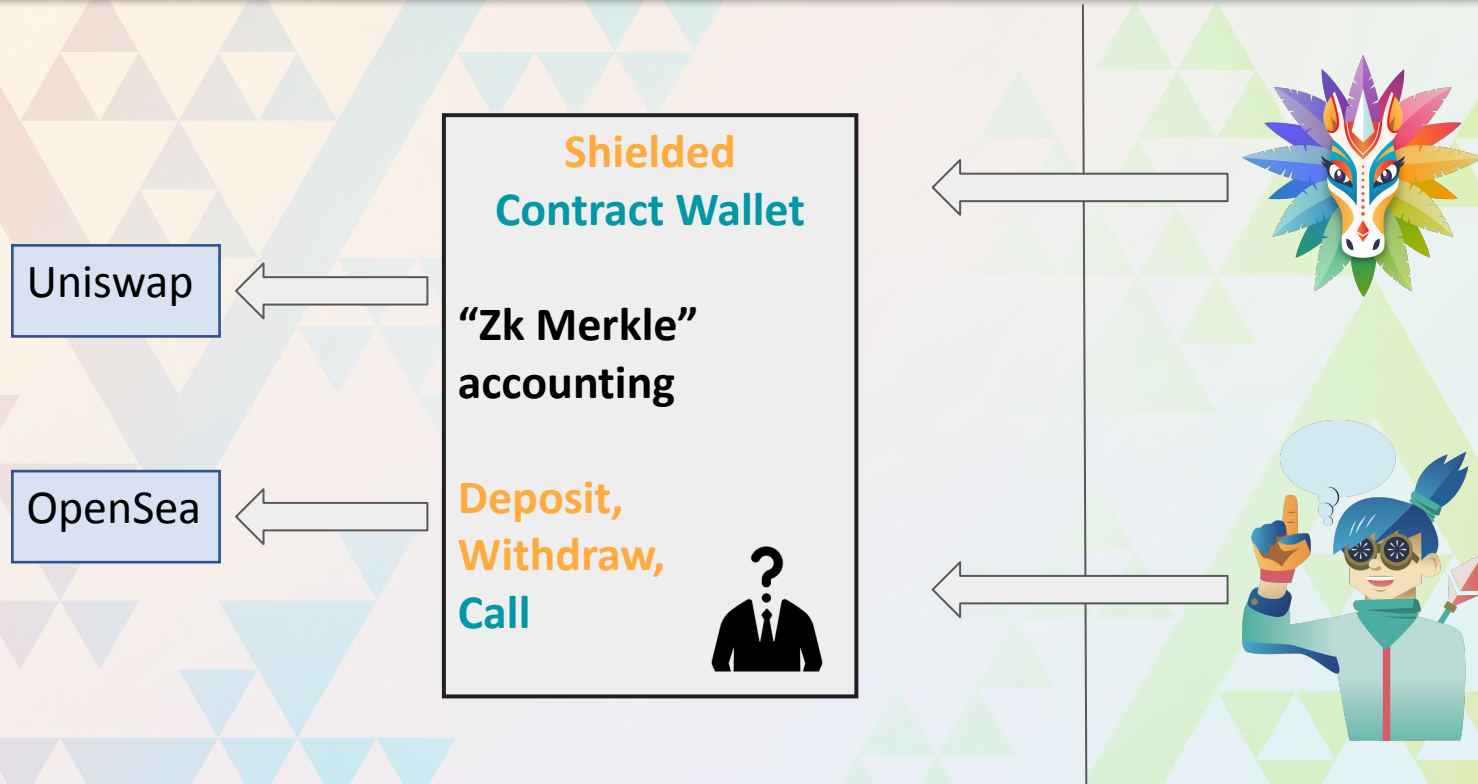


# Shielded Contract Wallet





# Shielded Contract Wallet



**Bonus: account abstraction (EIP-4337) compatible!**



# Problem 1: Arbitrary calls & Solution

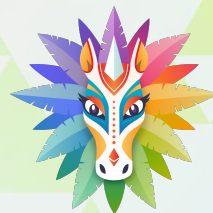
Shielded Contract Wallet 0xSCW

"Zk Merkle" accounting

Deposit, Withdraw, Call

Owens: **20 WETH**

**Unshield 1WETH**  
Call spends 20WETH



Owens: 1 WETH

**Solution**

Vault 0xV

Owens: 20 WETH

Shielded Wallet 0xSCW

"Zk Merkle" accounting

Deposit, Withdraw, **Call**

Unshield 1WETH  
**Call spends 20WETH**



Owens: 1 WETH

# Alternative solution w/ Call Router

Shielded Contract Wallet 0xSCW

"Zk Merkle" accounting

Deposit, Withdraw, Call

Owens: 20 WETH

**Solution**

Call Router 0xR

Call

Shielded Wallet 0xSCW

"Zk Merkle" accounting

Deposit, Withdraw

Owens: 20 WETH

Unshield 1WETH  
Call spends 20WETH



Owens: 1 WETH

Unshield 1WETH  
Call spends  
20WETH



Owens: 1 WETH

# Problem 2: Unknown Output Amount

Shielded Contract Wallet 0xSCW

“Zk Merkle” accounting

Deposit, Withdraw, Call

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



Note commitment determines refund amount

**Solution**

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



# Thank you! & Final Remarks

- **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