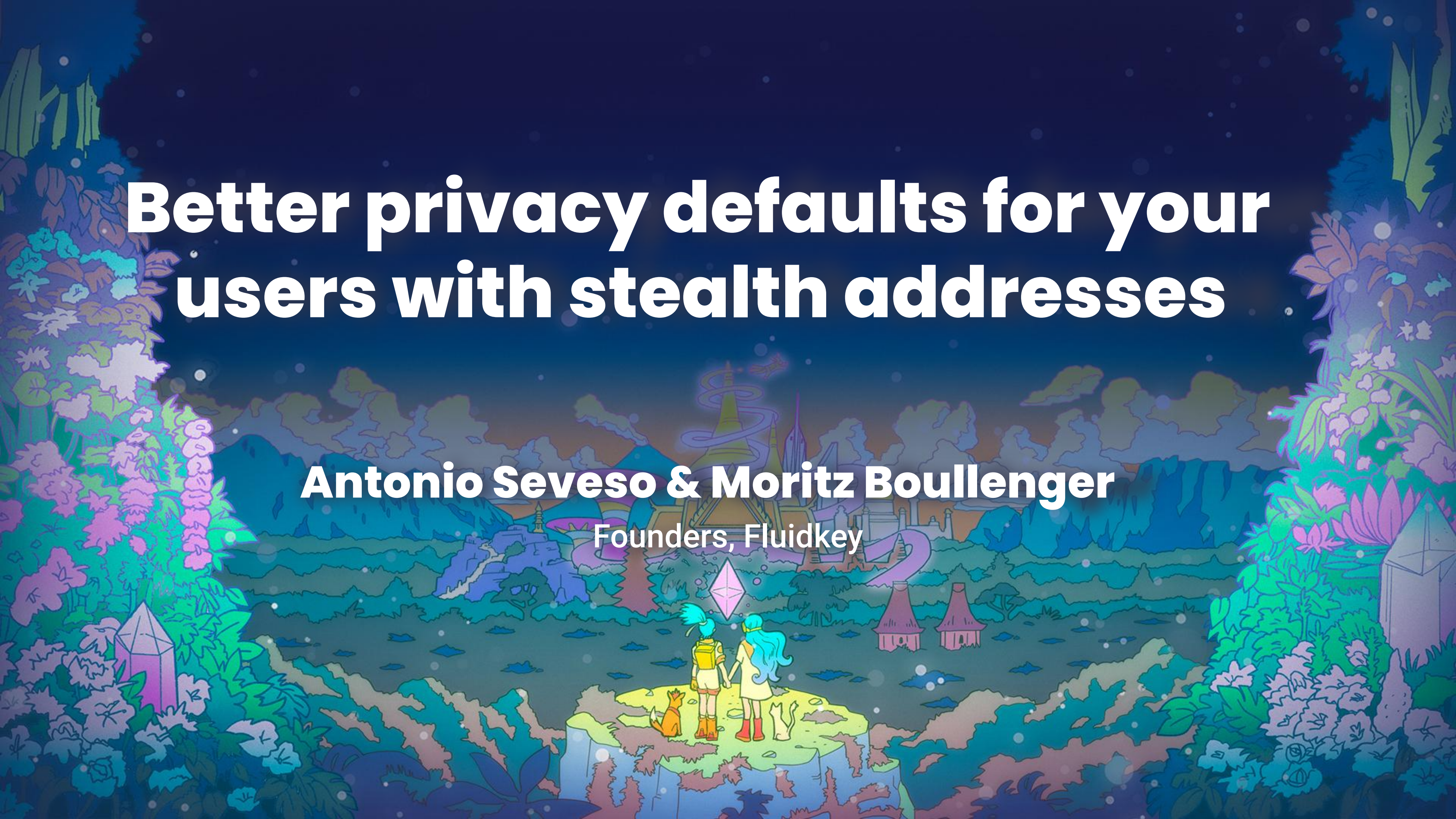
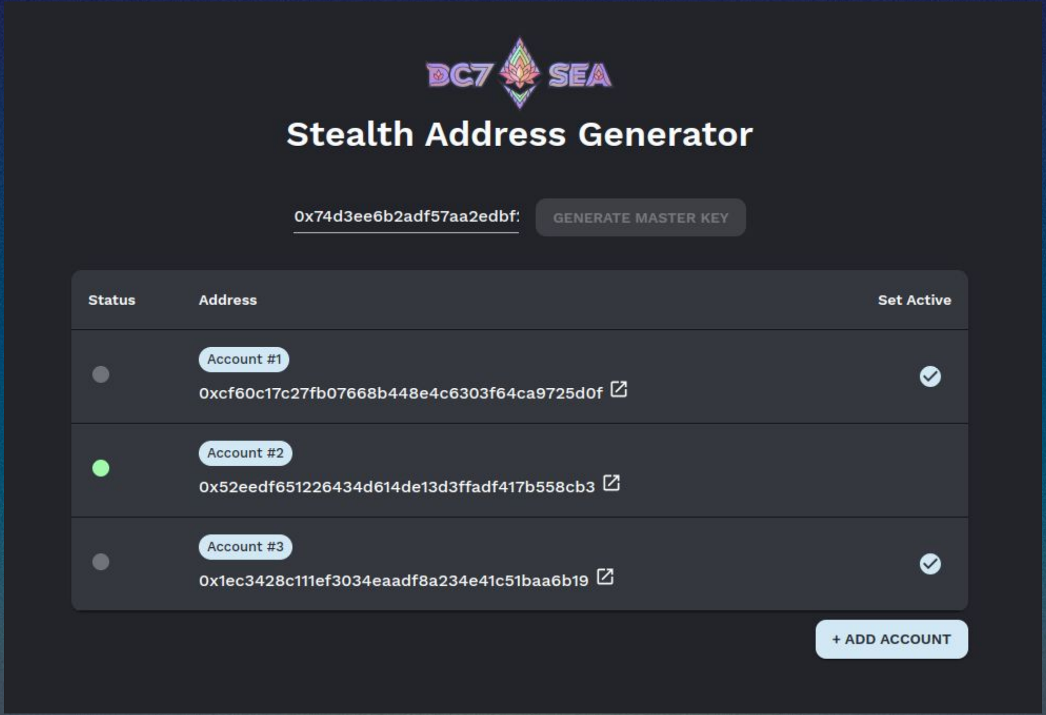
Better privacy defaults for your users with stealth addresses

Antonio Seveso & Moritz Boullenger

Founders, Fluidkey



Final result



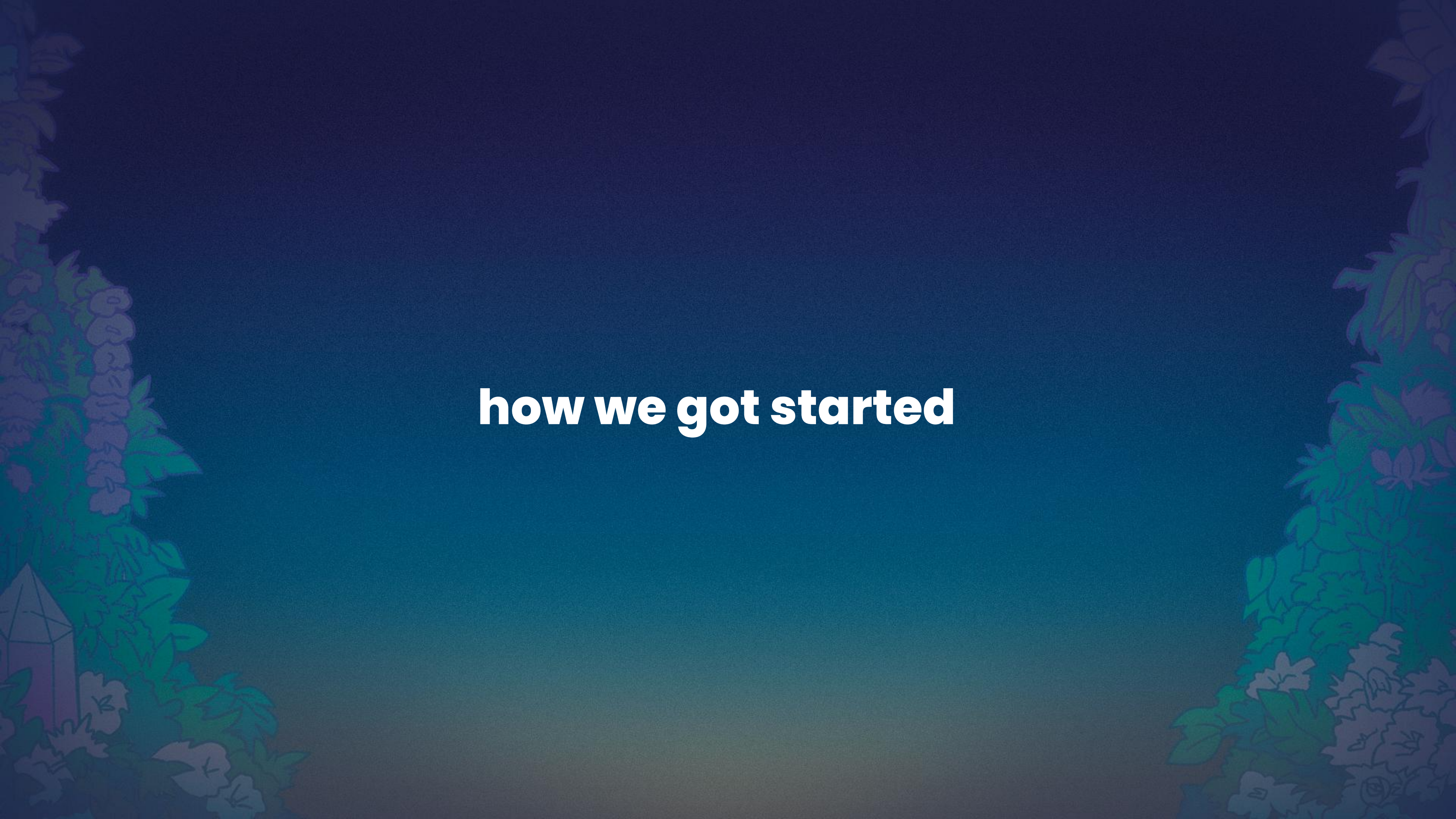
Stealth Address Generator

0x74d3ee6b2adf57aa2edbf

Status	Address	Set Active
●	Account #1 0xcf60c17c27fb07668b448e4c6303f64ca9725d0f	✓
●	Account #2 0x52eedf651226434d614de13d3ffadf417b558cb3	
●	Account #3 0x1ec3428c111ef3034eaadf8a234e41c51baa6b19	✓

Section 1

why stealth addresses?



how we got started

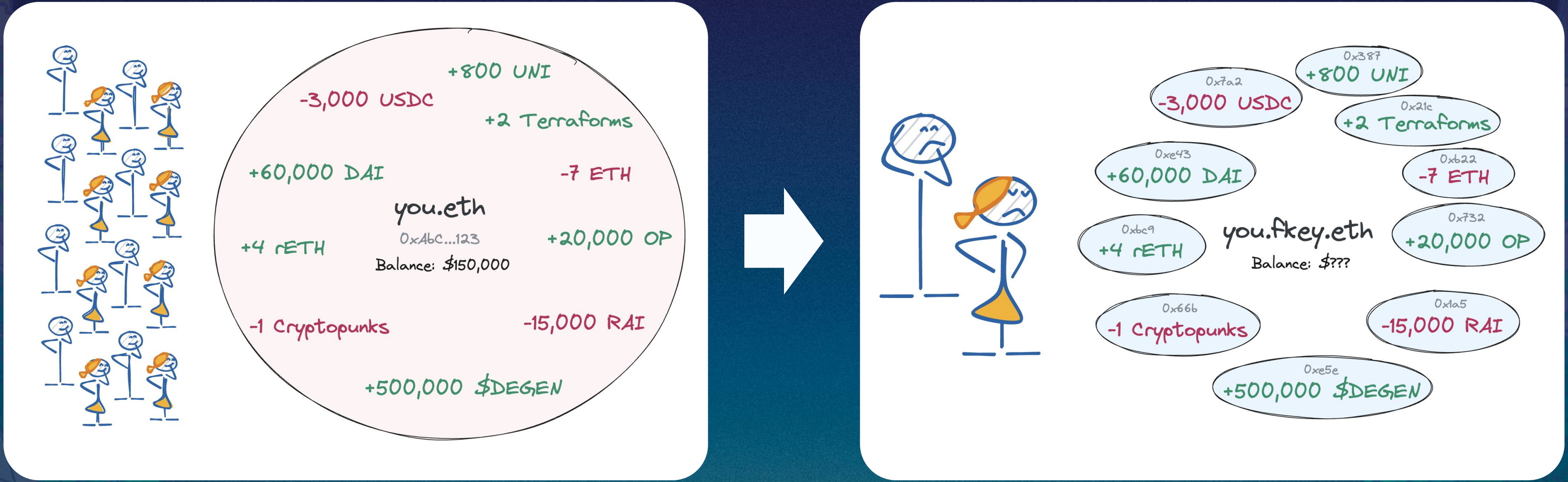
show of hands, who here:

1. **has heard of stealth addresses before?**
2. **has used a product that uses stealth addresses?**
3. **is working on a product that could benefit from better privacy?**

how stealth addresses work

unlock:

generate self-custodial accounts that are not publicly linked to a user’s main account


+800 UNI
-3,000 USDC
+2 Terraforms
+60,000 DAI
-7 ETH
you.eth
0xAbC...123
Balance: $150,000
+4 rETH
+20,000 OP
-1 Cryptopunks
-15,000 RAI
+500,000 $DEGEN
0x387
+800 UNI
0x7a2
-3,000 USDC
0x21c
+2 Terraforms
0xe43
+60,000 DAI
0xb22
-7 ETH
0xbc9
+4 rETH
you.fkey.eth
Balance: $???
0x732
+20,000 OP
0x66b
-1 Cryptopunks
0x1a5
-15,000 RAI
0xe5e
+500,000 $DEGEN

1. Receive

$$\underbrace{\texttt{user meta pubkey}}_{\text{openly shared}} * \underbrace{\texttt{secret}}_{\text{known by sender / trusted 3rd party}} = \underbrace{\texttt{stealth address pubkey}}_{\text{communicated to recipient via:}}$$

- encrypted onchain announcement (ERC-5564)
- trusted third party offchain indexing
- pseudo-random secret regeneration

2. Send

$$\underbrace{\texttt{user meta privkey}}_{\text{known only by user}} * \texttt{secret} = \texttt{stealth address privkey}$$

unlinkability vs untraceability

enabled by stealth addresses

✅ fast

✅ compatible with every counterparty and smart contract on public EVM chains

🟠 doesn’t break traceability

enabled by privacy pools

🟠 slow

🟠 limited set of operations

✅ breaks traceability

unlinkability + untraceability

stealth addresses + privacy pools

✅ fast

✅ compatible with every counterparty and smart contract on public EVM chains

✅ breaks traceability when needed

ux problems to solve

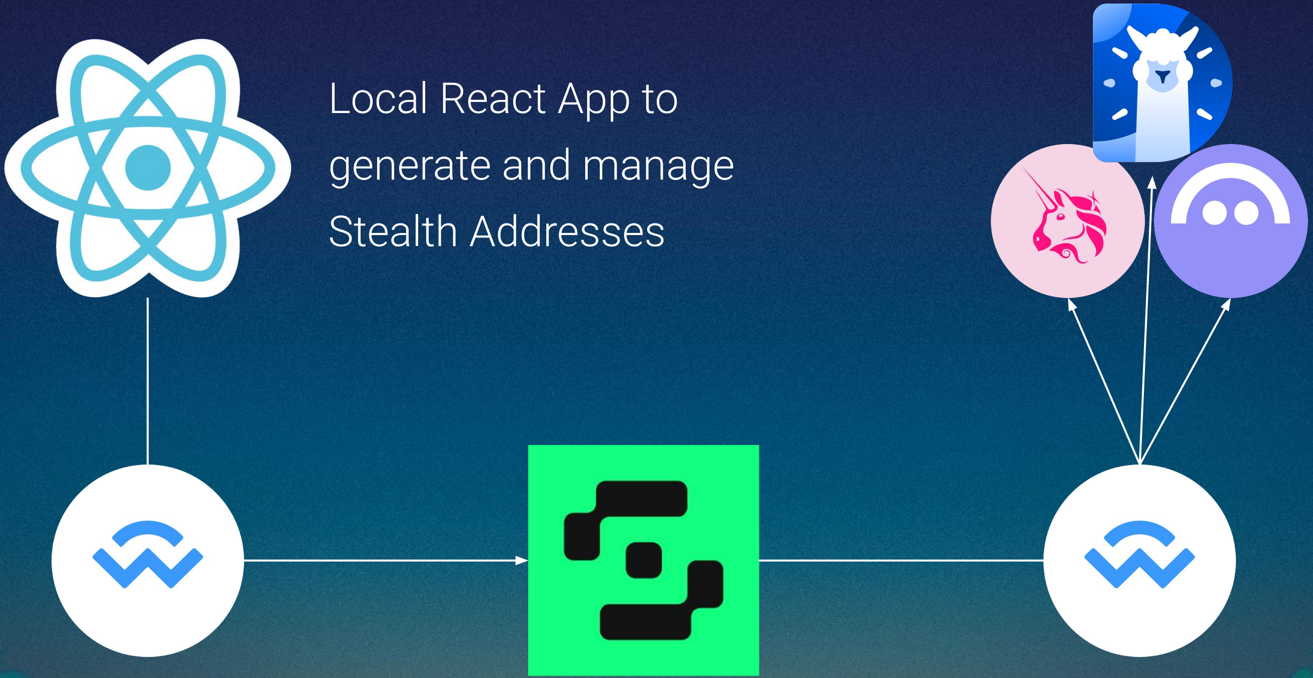
key management → keystore rollups (see key.space)

dapp interactions → just-in-time address funding (ERC-5792)

Section 2

let’s build stealth Safe signers!

Project structure

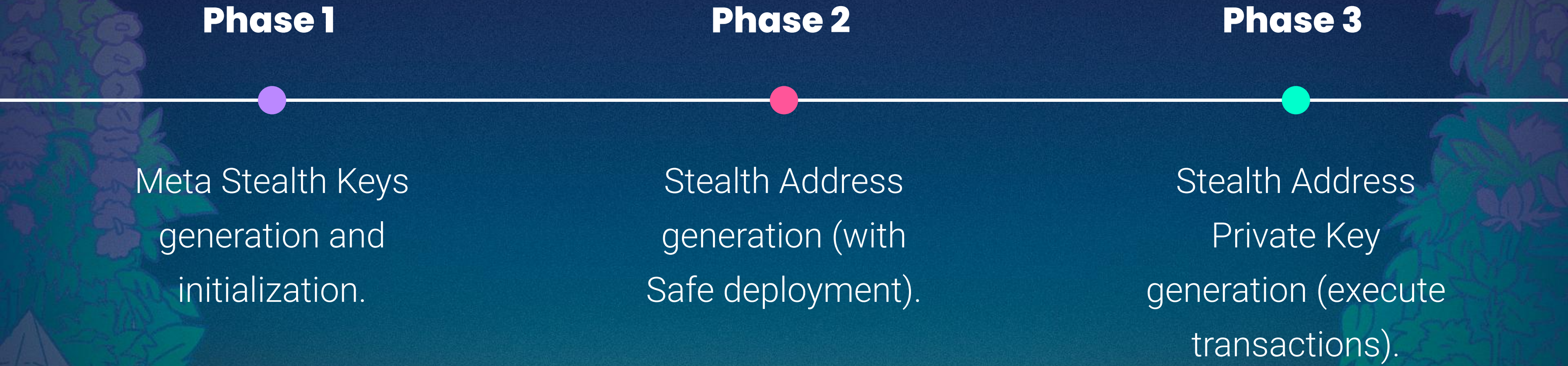


Local React App to generate and manage Stealth Addresses

Implementation Details

- Stealth Addresses Pseudo-randomly generated
  - Use viewing key to derive the ephemeral private key [secret]
  - Can be easily recreated (knowing the secret)
  - No-need to emit an event
  - Meant for trusted third party or personal projects
  - Public viewing key must be kept confidential
- Implemented with Stealth Account Kit

Goals



Phase 1

Meta Stealth Keys generation and initialization.

Phase 2

Stealth Address generation (with Safe deployment).

Phase 3

Stealth Address Private Key generation (execute transactions).

Goals

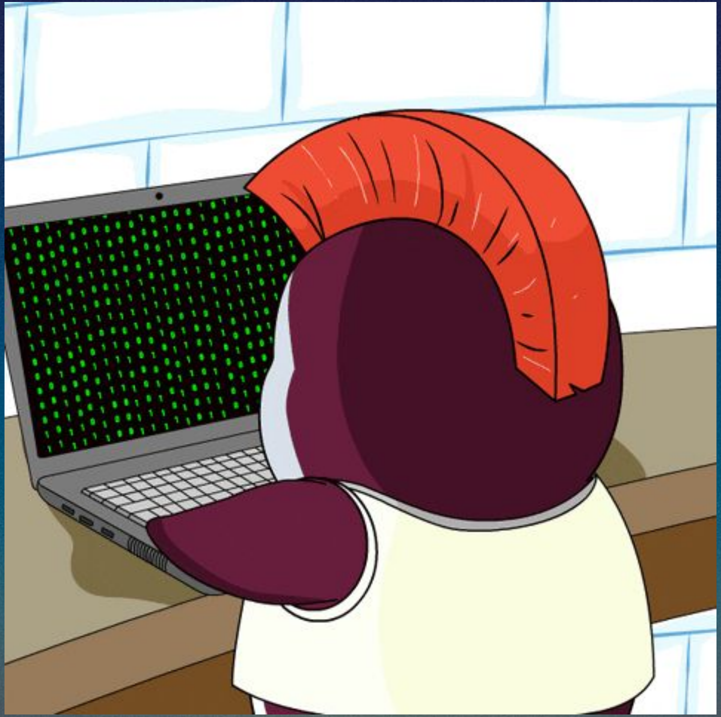
Phase 1

Meta Stealth Keys generation and initialization.

Phase 3

Stealth Address Private Key generation (execute transactions).

Let’s Code!

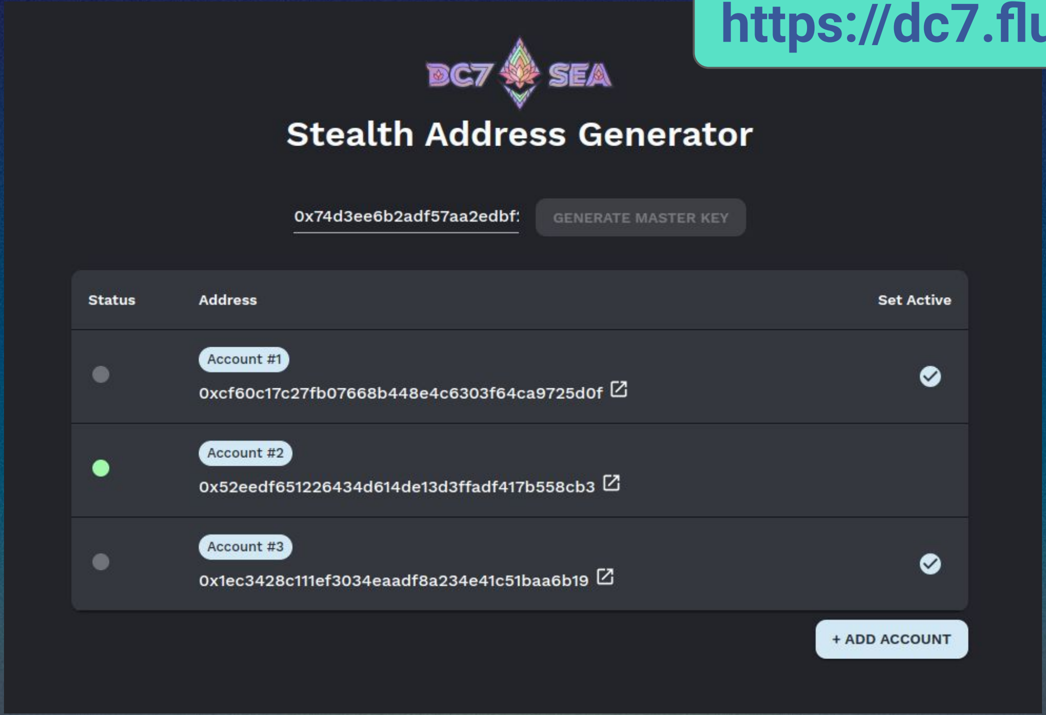


Clone the repo

fluidkey/dc7-stealth-address

Final result

https://dc7.fluidkey.com

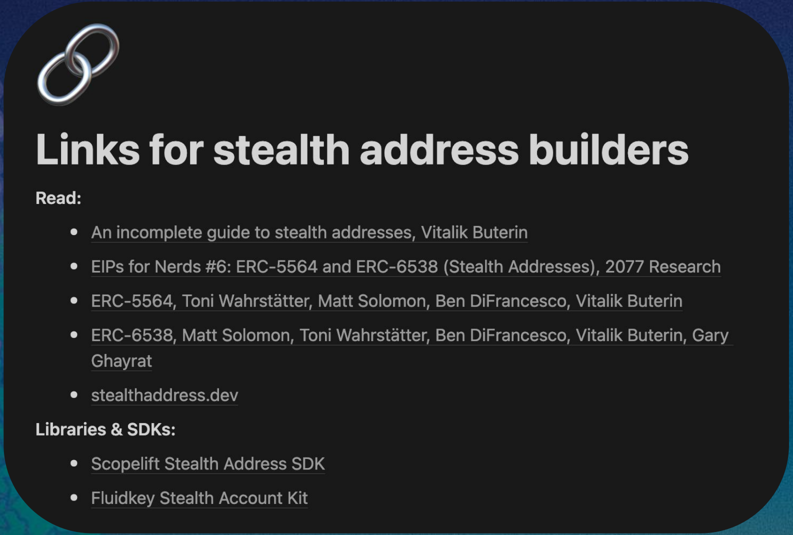


Stealth Address Generator

0x74d3ee6b2adf57aa2edbf

Status	Address	Set Active
●	Account #1 0xcf60c17c27fb07668b448e4c6303f64ca9725d0f	✓
●	Account #2 0x52eedf651226434d614de13d3ffadf417b558cb3	
●	Account #3 0x1ec3428c111ef3034eaadf8a234e41c51baa6b19	✓

where to learn more and get started building?



🔗

Links for stealth address builders

Read:

- An incomplete guide to stealth addresses, Vitalik Buterin
- EIPs for Nerds #6: ERC-5564 and ERC-6538 (Stealth Addresses), 2077 Research
- ERC-5564, Toni Wahrstätter, Matt Solomon, Ben DiFrancesco, Vitalik Buterin
- ERC-6538, Matt Solomon, Toni Wahrstätter, Ben DiFrancesco, Vitalik Buterin, Gary Ghayrat
- stealthaddress.dev

Libraries & SDKs:

- Scopelift Stealth Address SDK
- Fluidkey Stealth Account Kit

Stealth address TG group & reach out → @moritz_fluidkey

Thank you!

Moritz & Antonio

Fluidkey

@moritz

@metony