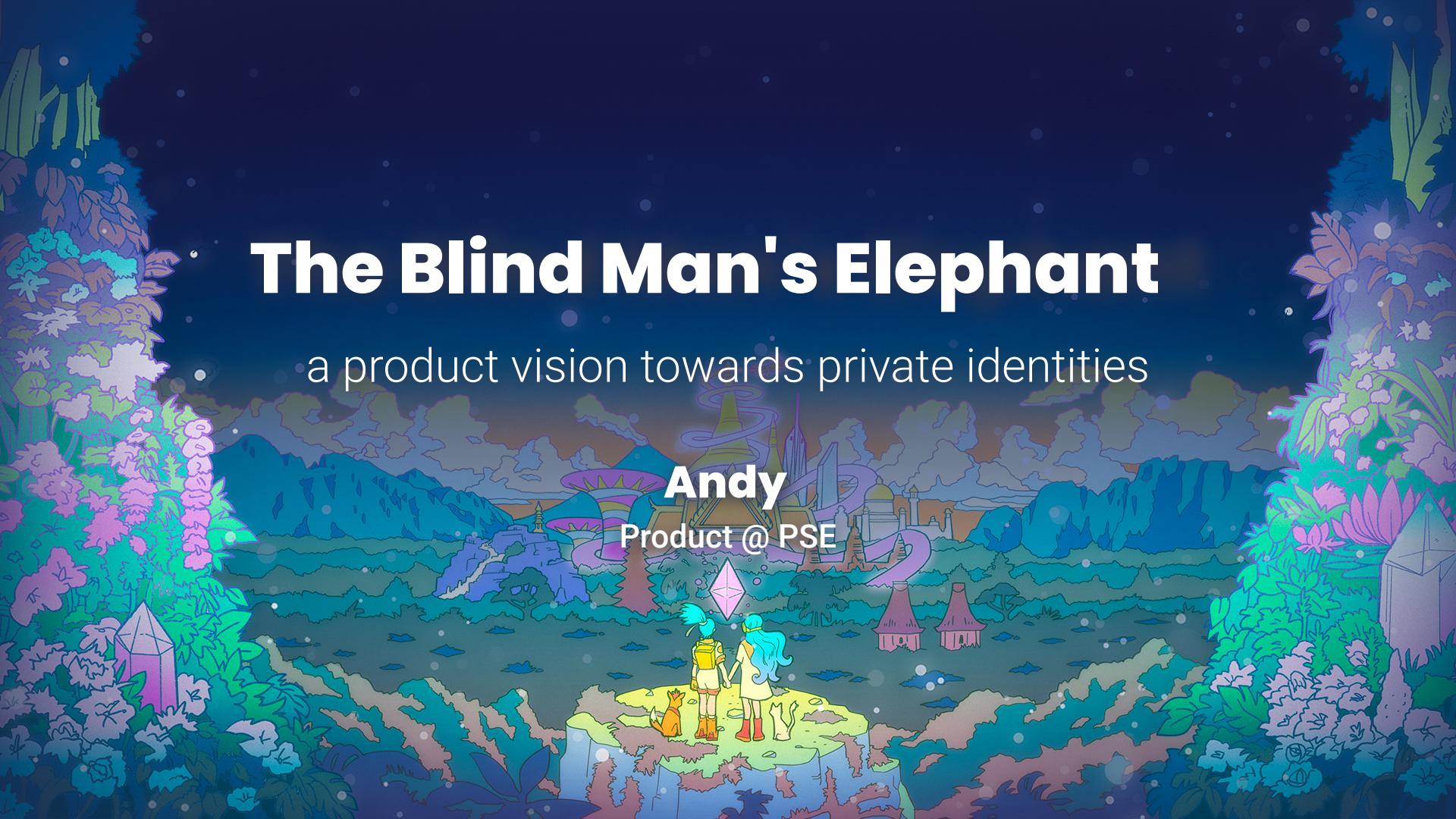
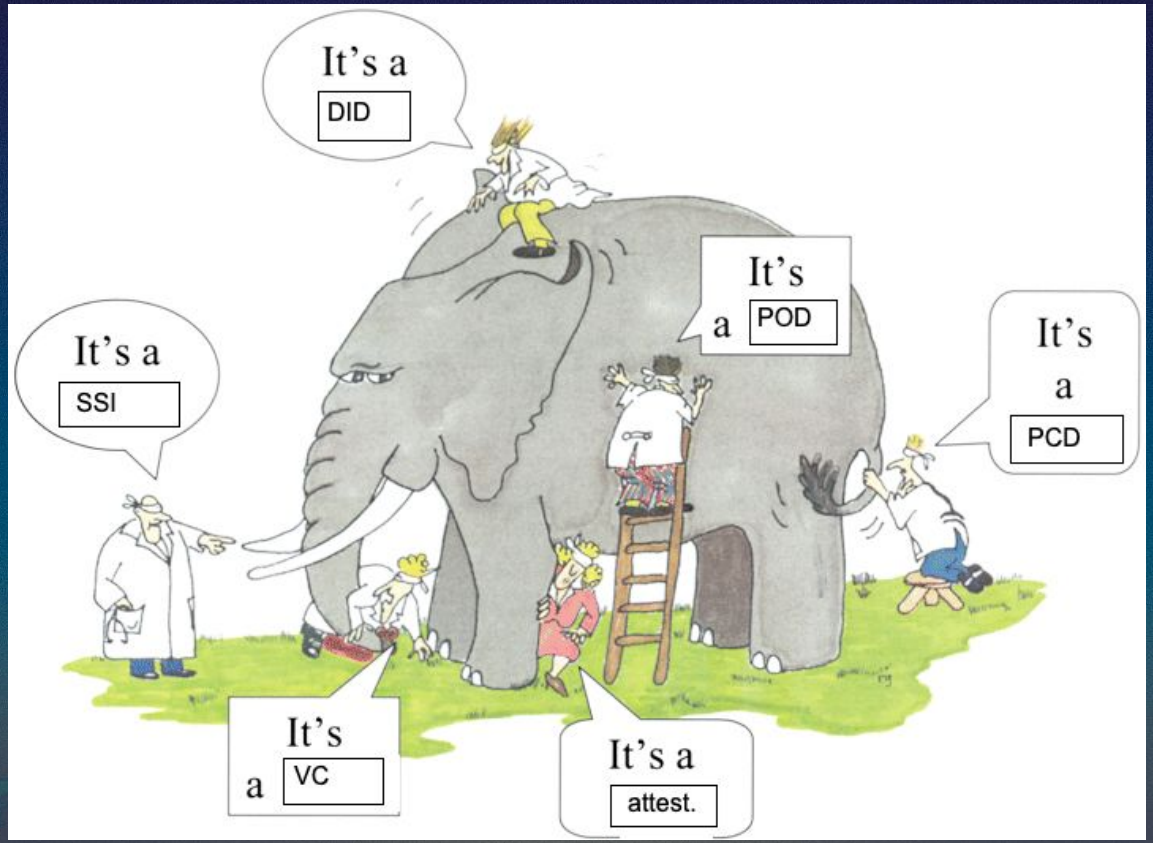

The Blind Man's Elephant
a product vision towards private identities
Andy
Product @ PSE

The Land of White Elephants



Properties

Privacy
Decentralization
Interoperability
Scalability
Security
Transparency
Self-ownership
Portability
Tamper-resistance

Usability
Verifiability
Flexibility
Trustlessness
Anonymity
Resilience
Auditability
Minimal disclosure
Soundness
Revocability
Efficiency

In summary, what do we want to be able to do?

1. **Import all my identities & data**
2. Generate proofs about them
3. **My proofs being useful everywhere**

Section 1

import all

my identities and data

support everything.
all guarantees.
great ux.

Anything signed!

national id cards, passports, driver licenses, signed documents, signed PDFs, digital certificates, email ownership, credit cards, JWT

Uber reputation, social graphs, social media networks, verifiable email interactions, spotify history, verifiable text messages interactions

permissionless: without asking for permission from the issuer
private actions: without the issuer knowing
verifiable: provable data

'web2 ux:' fast, smooth, few clicks (QR, NFC, 3 clicks)

technically...

Technically, this means supporting different

- hashing (SHA1, SHA256, Poseidon)
- signatures (RSA, EdDSA, ECDSA, BBS)
- data structures (JSON, JSON-LD, EAS)
- standards (VCs, DIDs, EAS schemas)

Technically, this means ‘hijacking’ existing infra:

- 2PC, MPC, proxies(notaries)

Technically, this means storing private data safely:

- wallet-like experience

Section 2

prove facts about them

prove facts about them.

Generating proofs
- enable selective disclosures
- expressive queries and responses
- well thought out defaults and confirmations

From my phone & browser
- <1 second

Few clicks
- cheap or free

Feeling safe
- transparent for me
- private to anyone else

flexibility.
performance.
ux.
security.

Targets:

- WASM (browser) & mobile native
- Short times, limited RAM, bandwidth, CPU,

Low cost:

- Proof aggregation
- Recursion. Folding.
- Verification layers.

Performance:

- coSNARKs
- Client side proving
- Proof Composition
- Proof Caching

Spartan (client), zkVM (aggregate), Groth16 (onchain)

technically...

Section 3

useful actions

everything.
everywhere.
all at once.

Data Syndicates (Marketplaces)
Anon Chats
Voting
Forums
Reimburse
Compliance
‘KYCs’
Multisigs
Content access
Airdrops
UBI
Contracts

technically...

useful actions

Common and composable interface to consume this ‘identity proofs’

Strong nullifier:

Lvl0: no nullifier

Lvl1: discoverable by government

Lvl2: discoverable by collusion app + government

Lvl3: discoverable by collusion of OPRF network

Lvl3+: discoverable by collusion of vOPRF network

Section 4

everything secured.

everything secured.

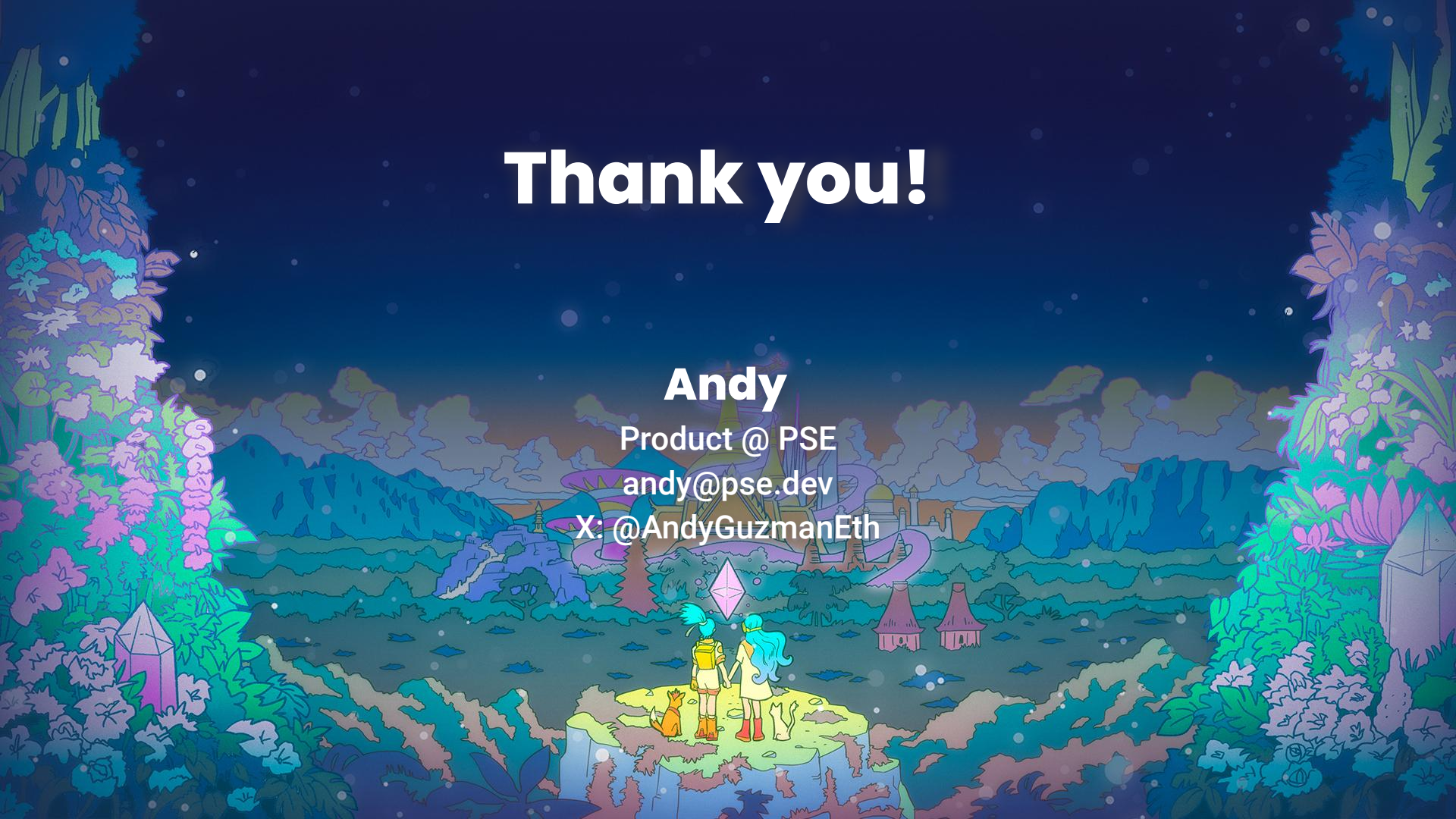
Post-quantum resistant
Interoperable
Movable from wallet to another
Shared verifiable infrastructure

Optional:

- key rotation
- liveness checks
- active authentication
- resistance from government removal

present and future
access.
privacy.
security.

let’s hijack more identity sources
let’s discover novel use cases
let’s build new LEGO blocks


Thank you!
Andy
Product @ PSE
andy@pse.dev
X: @AndyGuzmanEth