Make Ethereum Cypherpunk Again

Why we need privacy

Zac Williamson

CEO, Aztec

The information age has eroded the foundations of trust that bind humanity

We need new information networks to bring it back

A memento from 1998

Aztec Labs

Information Networks, Communication Complexity and Society

Romeaboo Trigger Warning

The following 5 minutes will contain a monologue involving the Roman empire.

PROMISE ME YOU WONT CRY
I promise
ROME WASN'T BUILT IN A DAY, BUT BURNED IN ONE
I won't cry....

Aztec Labs

New information networks

[insert 5 minute tangent about cavemen]

Aztec Labs

Privacy and why it matters

What is privacy technology?

- Prove a statement derived from undisclosed information
  - “This is a UK epassport signature for [name redacted]”

- Privacy = information asymmetry

- Privacy technology is:
  - Identity technology
  - attestation technology
  - trust infrastructure technology

Why privacy?

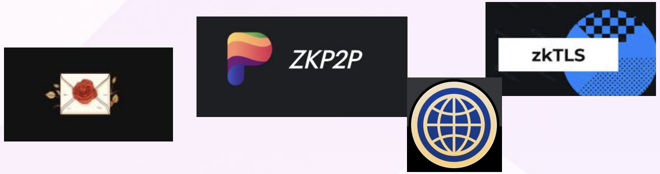
Q: Where is web3's fundamental value sourced from?

...and what is missing?

Composable Privacy

- Web3 composability: a force-multiplier akin to vertical integration
- Every dapp/code deployed to the network enhances network value
- ***Private Composability*** must be unlocked for apps to leverage privacy at scale

You are being composed. Do not resist.

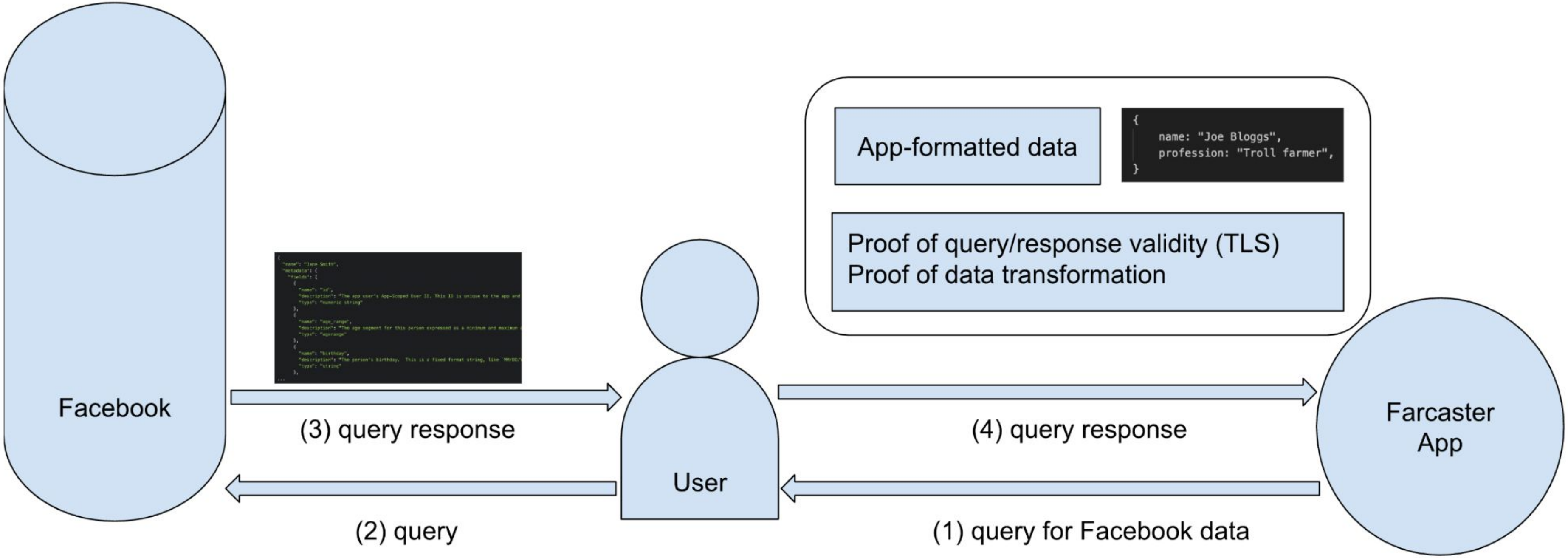


- zk-email can prove data from 3rd party emails without their participation
- zk-passport can prove citizenship credentials without govt participation
- zk-TLS enables access to userdata from web2 apps (mostly) trustlessly

Privacy is Decentralization

- A dapp that touches web2 or the real world requires identity standards
- To remain non-custodial, identity standards must utilize **zk and privacy**
- To remain composable, the data being proven must remain client-side

“zk transformers” - breaking down the data fortresses



Facebook

```
{
  "name": "Jane Smith",
  "metadata": {
    "fields": [
      {
        "name": "id",
        "description": "The app user's App-Scoped User ID. This ID is unique to the app and
        "type": "numeric string"
      },
      {
        "name": "age_range",
        "description": "The age segment for this person expressed as a minimum and maximum
        "type": "agerange"
      },
      {
        "name": "birthday",
        "description": "The person's birthday.  This is a fixed format string, like `MM/DD/
        "type": "string"
      },
...
```

(3) query response

(2) query

User

App-formatted data

```
{
    name: "Joe Bloggs",
    profession: "Troll farmer",
}
```

Proof of query/response validity (TLS)
Proof of data transformation

(4) query response

(1) query for Facebook data

Farcaster App

Enabling Web2<>Web3 interop with Verifiable Compute

- Web2<>Web3 interop needs

  ZK Cryptography

- “Prove this archaic web2 protocol is valid”
  - ...which contains sensitive user data
  - ...and session keys
  - ...and secret keys
  - ...and probably passwords

ZK EMAIL

TLSN

zkPassport

N.B. Real ZK, not the fake stuff!

Ethereum will be Cypherpunk again

Distributed privacy technology will be used to develop systems, protocols and products that increase human autonomy and agency

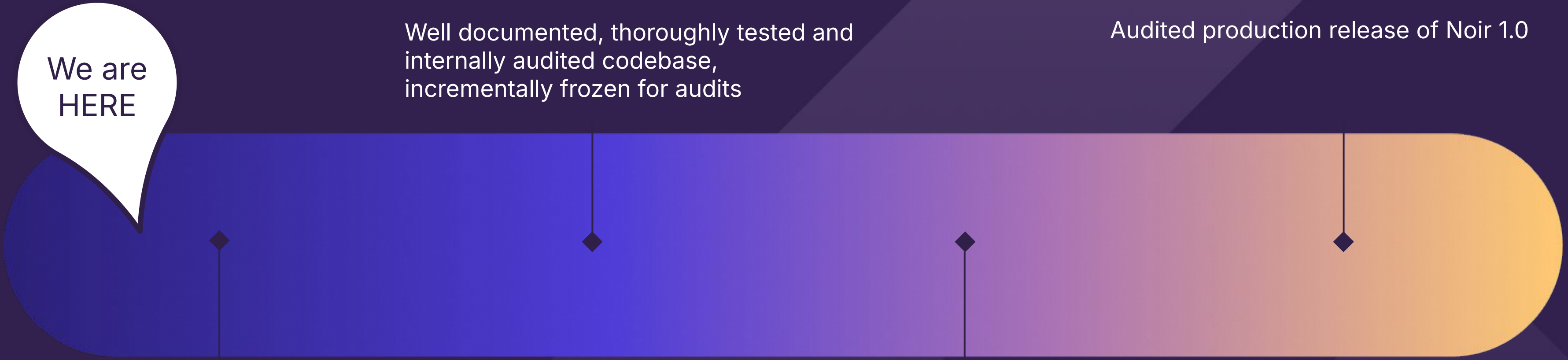
We are building human-centric networks...

where humans are their own agents...

that use their own data however they please...

and distinguish their actions, stories and achievements from ai flotsam & alternate facts

Noir 1.0 Roadmap



Pre-release - Q4’24

Early Access releases of Noir 1.0, motivate devs to build towards production

Audit Freeze - Q4’24 to Q1’25

Well documented, thoroughly tested and internally audited codebase, incrementally frozen for audits

Audits - Q1’25 to Q2’25

External security audits of codebase

Full Release - Q2’25

Audited production release of Noir 1.0

Aztec Labs

Get Involved With Noir

Linktree