Ensuring Privacy in Digital Identity to Prevent a Dystopian Crisis

Jordi Baylina
Co-Founder of Polygon & Privado ID

Oleksandr Brezhniev
CTO at Privado ID

Privado.iD

Digital Identity Now

Privado.iD

Controlled by Corporations

Fragmented

Bad UX

Privado.iD

Identity in Web3

Privado.iD

Controlled by **(Web3)** Corporations

(Even more) Fragmented

(Even worse) UX

Privado.iD

Public Immutable Ledger

+

Sensitive Data

=

Problems

Surveillance

Unforgiving Algorithms

Privacy Erosion

Privado.iD

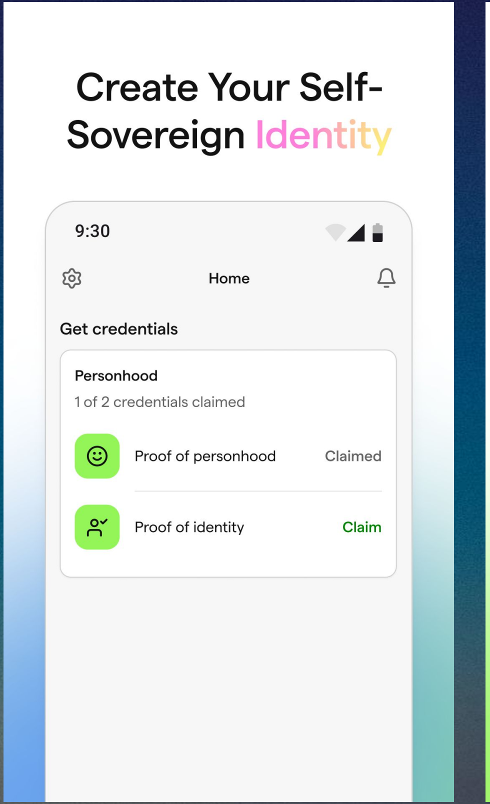
The Solution

- **Self Sovereign** Identity
- Single decentralized database of the truth.
- Privacy by design and by default (ZK)
- Simple Open Standard that comes from the roots

Privado.iD

Privado ID

- **SSI Middleware Infrastructure** for identity on any chain, any device
    - Built on top of iden3 protocol.
- Compliant with **W3C DID** & **Verifiable Credentials** Data Model Standards.
- Powered by **Zero-Knowledge Proofs** to enable **privacy-preserving** verifications.



Create Your Self-Sovereign Identity

9:30

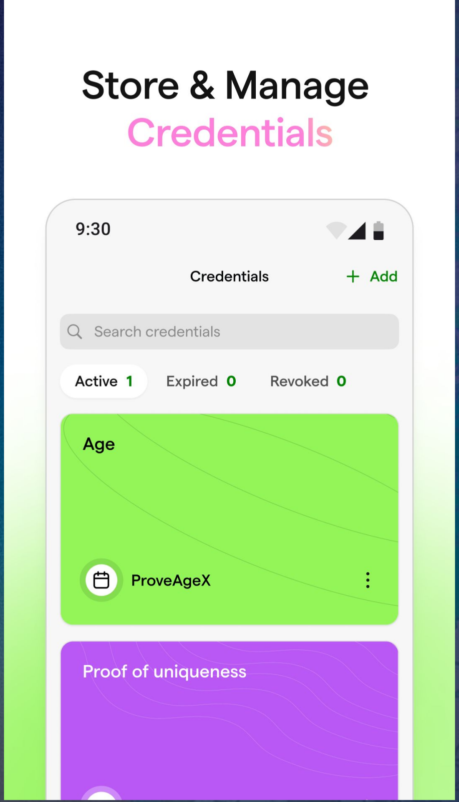
Home

Get credentials

Personhood

1 of 2 credentials claimed

Proof of personhood	Claimed
Proof of identity	Claim



Store & Manage Credentials

9:30

Credentials + Add

Search credentials

Active 1 Expired 0 Revoked 0

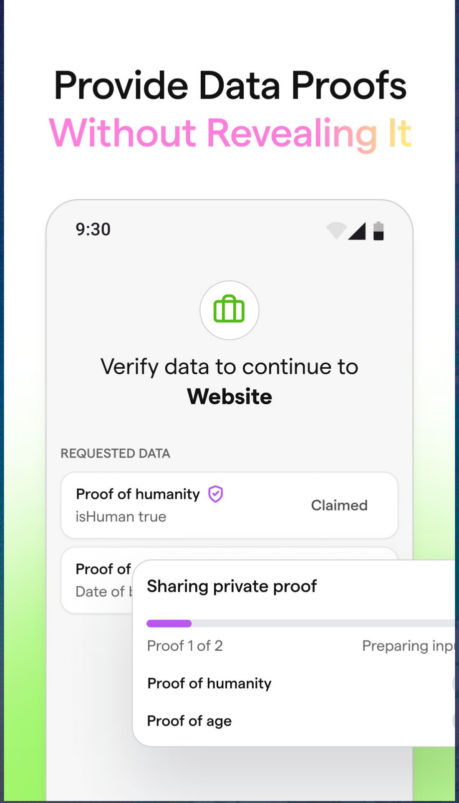
Age

ProveAgeX

Proof of uniqueness

Privado ID: Taking the Guesswork out of Identity

- Unified Identity; chains, devices, legacy systems
- Cross-chain Verification; Prove once, use forever
- Prove Statements without Revealing Private Data
- Selective Disclosure
- Privacy-Preserving Proof-of-Uniqueness
- Decentralized Trustless Issuance
    - Smart Contract Issuance



Provide Data Proofs
Without Revealing It

9:30

Verify data to continue to **Website**

REQUESTED DATA

Proof of humanity
isHuman true
Claimed

Proof of
Date of b

Sharing private proof

Proof 1 of 2
Preparing inp

Proof of humanity

Proof of age

Privacy-Preserving Proof-of-Uniqueness

- Proving uniqueness based on credentials
- Credential could be of any type
- Depends on the issuer verifying uniqueness before issuing a credential
- Uniqueness Nullifiers are generated for specific Verifier and Context

genesisID
secretNonce
credentialSchema ⇒ **ZK Circuit** ⇒
nullifier
verifierID
nullifierSessionID
...

Privado.iD

Privacy-Preserving Proof-of-Uniqueness Use Cases

Sybil Resistance for Onchain Incentives

- Stop overpaying bots!

DAO Proposal Voting

- Based on DAO Membership / Contributions
- Protects delegate independence of choice

Humanitarian Aid Distribution

- Based on Citizenship or Membership in Vulnerable Group
- Enables value distribution while minimizing harm to marginalized recipients

Company-wide Anonymous Survey

- Based on Employee Credential
- Compels honesty and authenticity without social repercussions

Nationwide Voting

- Based on Registered Voter Credential
- Protects the democratic process from outside influence

Privado.iD

Decentralized Trustless Issuance

- Complements regular trusted issuance model
- Allows smart contracts to issue **credentials from on-chain data**
- Allows users to **self-issue credentials from private off-chain data**

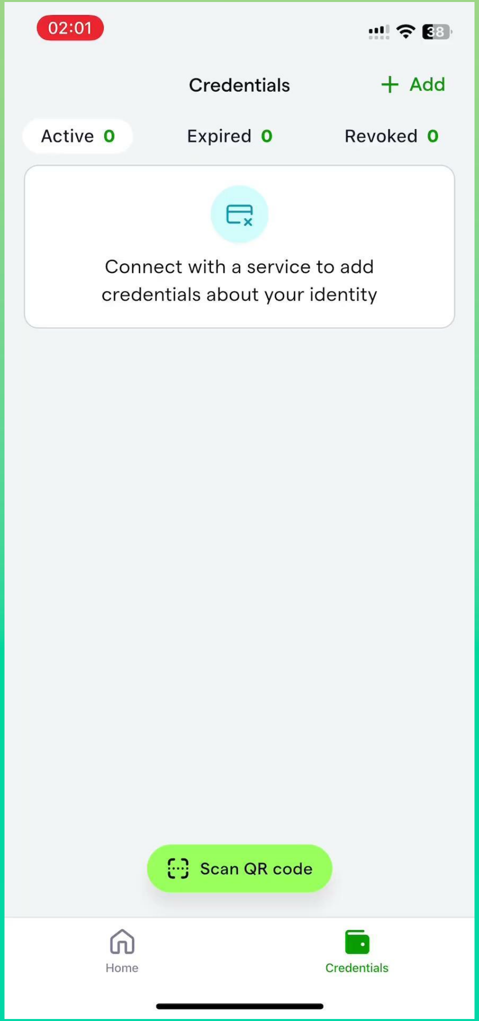
```
EthAddressIssuer.
    issueCredential(
        userProfileID
    )

AnonAadhaarIssuer.
    issueCredential(
        credentialHash,
        ZKP
    )
```

* pseudocode

Privado.iD

Demo

Privado.iD



Credentials

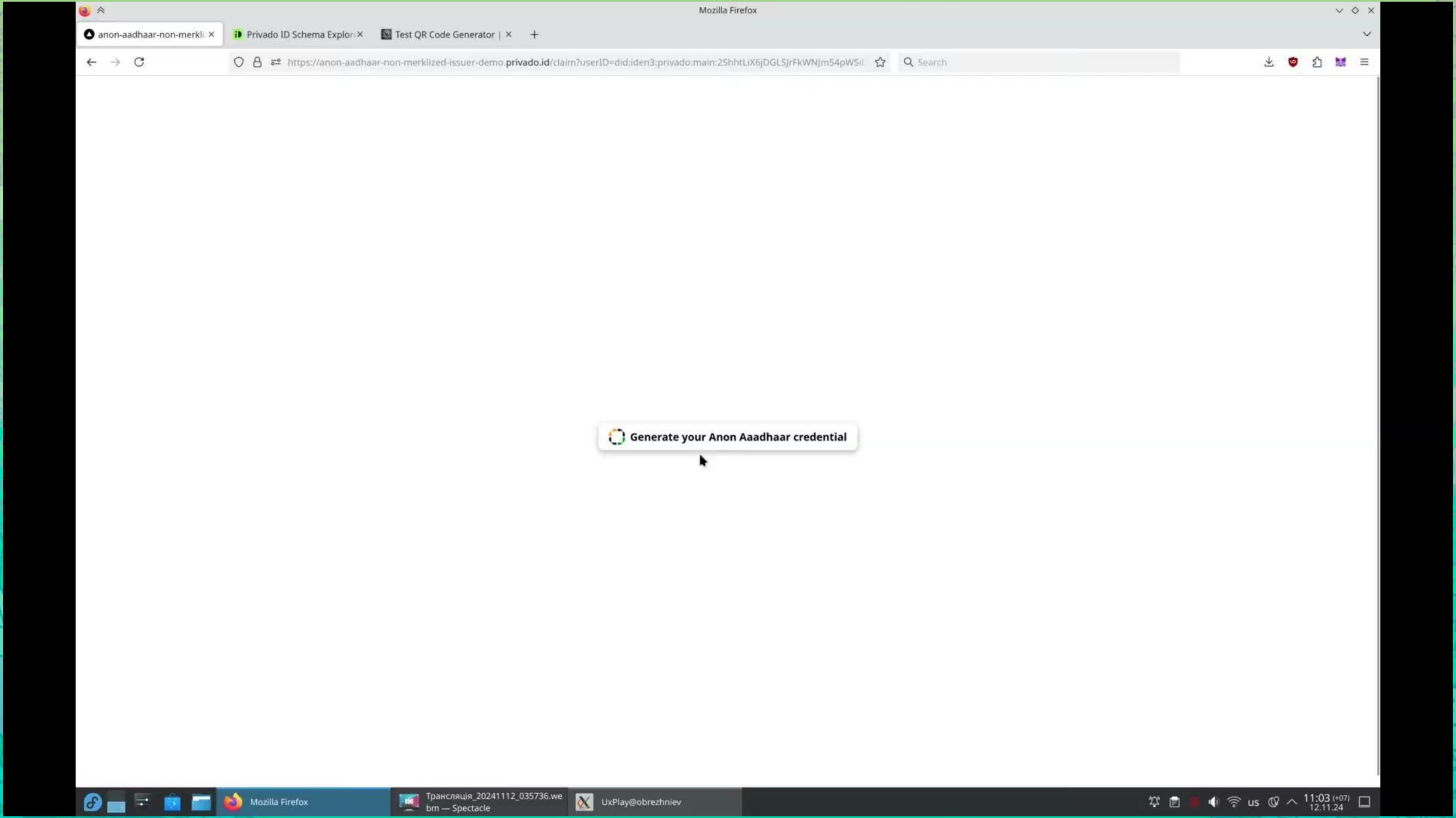
Active 0

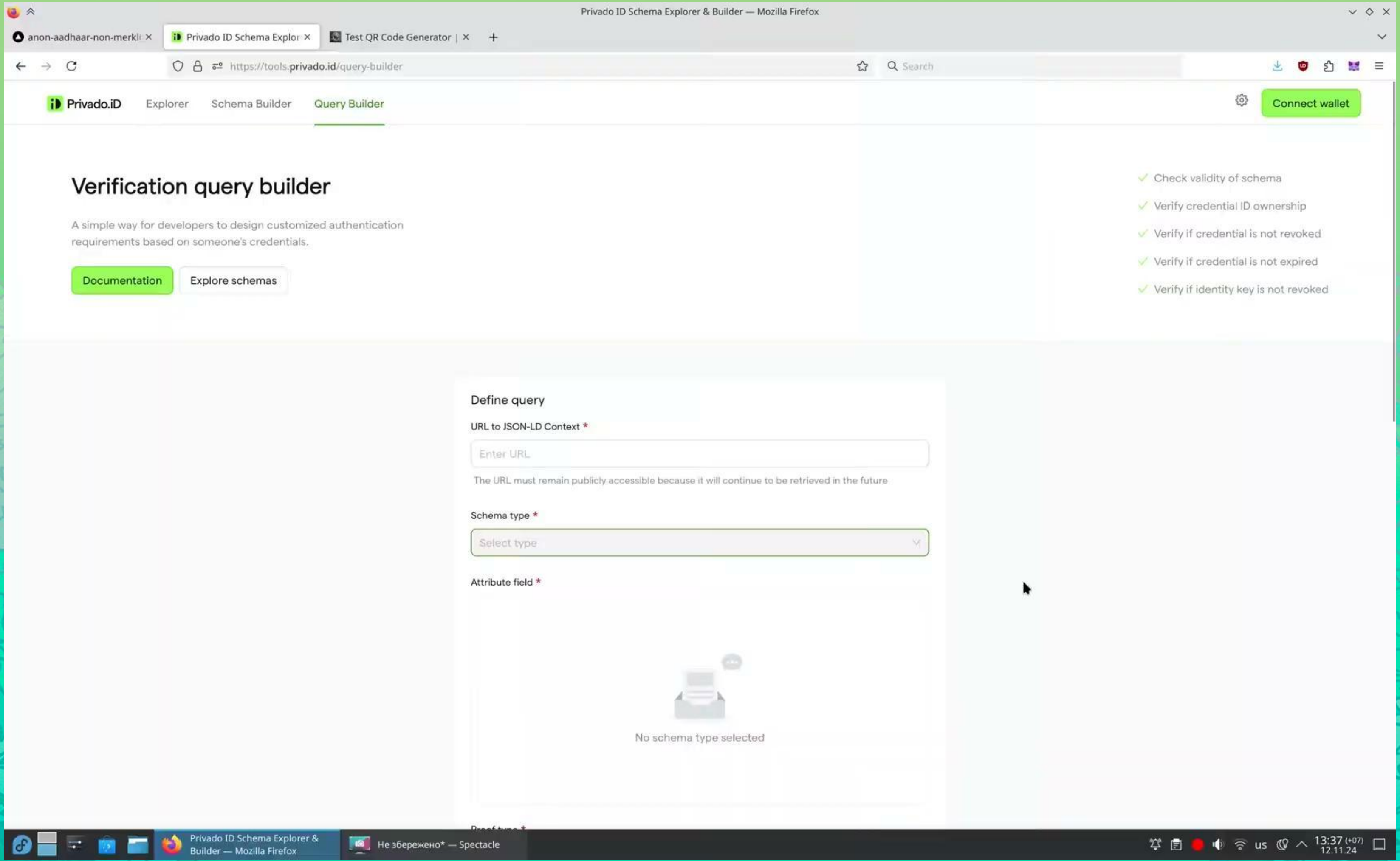
Expired 0

Revoked 0

Connect with a service to add credentials about your identity

Privado.iD


Mozilla Firefox
anon-aadhaar-non-merkli
Privado ID Schema Explor
Test QR Code Generator |
https://anon-aadhaar-non-merklized-issuer-demo.privado.id/claim?userID=did:iden3:privado:main:2ShhtLiX6jDGLSJrFkWNJm54pWSi
Search
Generate your Anon Aaadhaar credential
Mozilla Firefox
Трансляція_20241112_035736.webm — Spectacle
UxPlay@obrezhniev
us
11:03 (+07)
12.11.24


Privado ID Schema Explorer & Builder — Mozilla Firefox
anon-aadhaar-non-merkl
Privado ID Schema Explor
Test QR Code Generator |
https://tools.privado.id/query-builder
Search
Privado.iD
Explorer
Schema Builder
Query Builder
Connect wallet
Privado ID Schema Explorer & Builder — Mozilla Firefox
Не збережено* — Spectacle
us
13:37 (+07)
12.11.24

Verification query builder

A simple way for developers to design customized authentication requirements based on someone's credentials.

Documentation | Explore schemas

- ✓ Check validity of schema
- ✓ Verify credential ID ownership
- ✓ Verify if credential is not revoked
- ✓ Verify if credential is not expired
- ✓ Verify if identity key is not revoked

Define query

URL to JSON-LD Context *

Enter URL

The URL must remain publicly accessible because it will continue to be retrieved in the future

Schema type *

Select type

Attribute field *

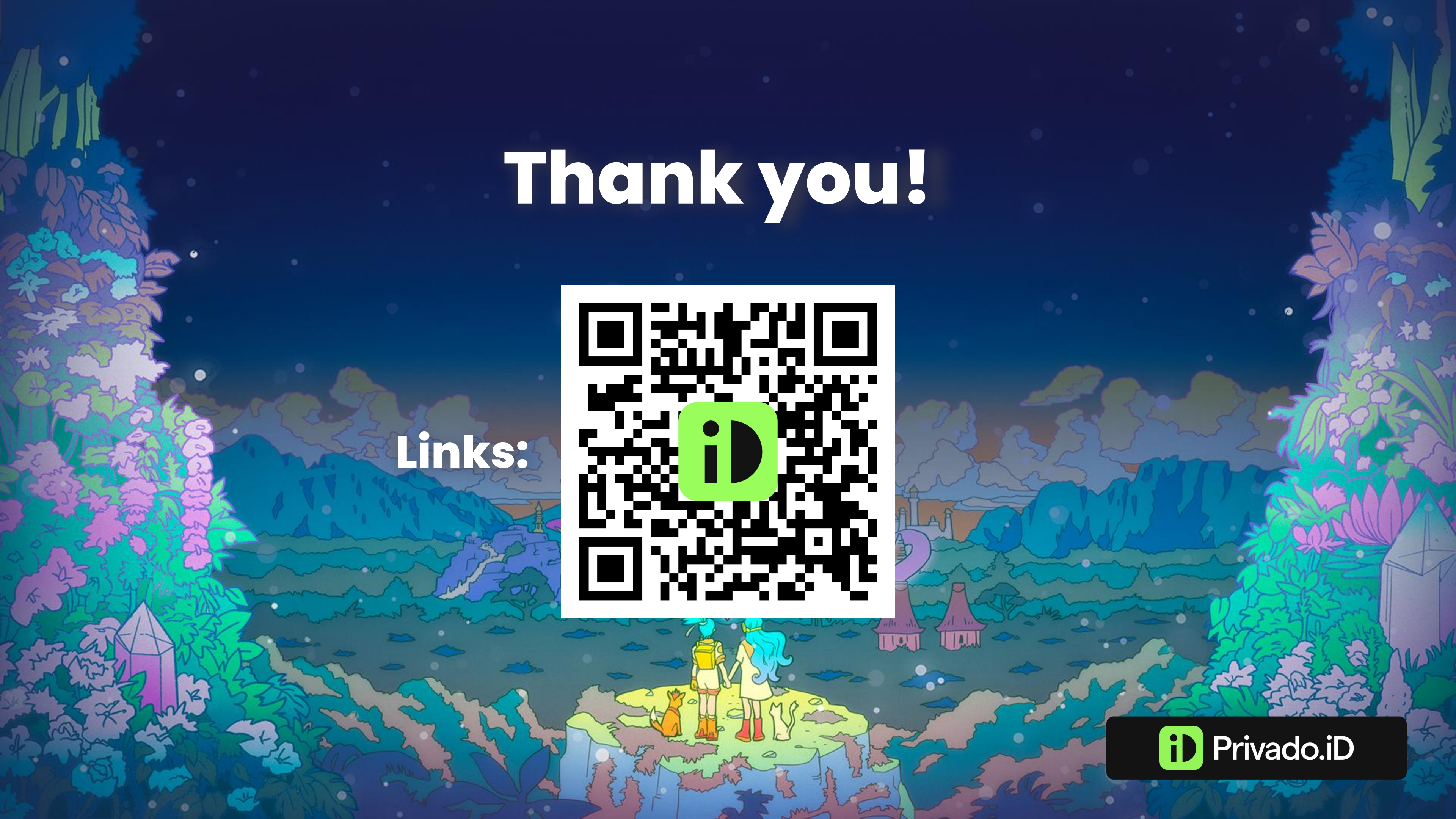
No schema type selected

Proof type *

Q & A

Privado.iD

Thank you!



Links:

Privado.iD