

XRPL



SOLVENCY

Enhance privacy, Prove solvency

CONTENT

The problem

Our solution

Ring signatures ?

Use cases

GTM Strategy

Roadmap

The team

THE PROBLEM

How can we enhance privacy with proof of solvency ?

**No user-friendly and scalable
solution for solvency proofs**

**SECP256K1 implementation
curves are not ZK-SNARK
friendly (ZKP)**

**Solvency proofs are technically hard to implement using ZK.
Using ZKPs requires changes on the blockchain protocol.**

THE SOLUTION : RING SIGNATURE

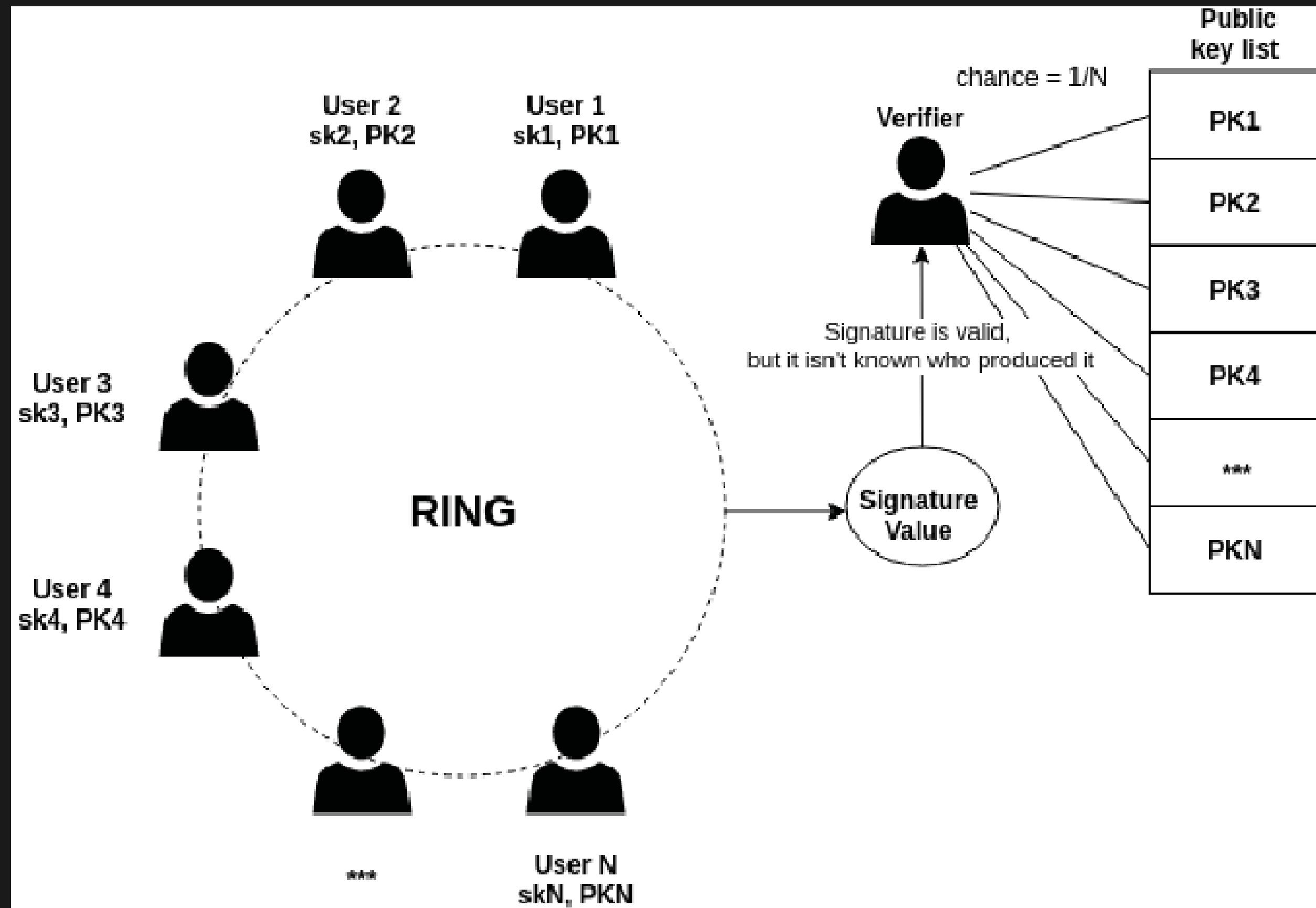
XRPL Friendly

Scalable

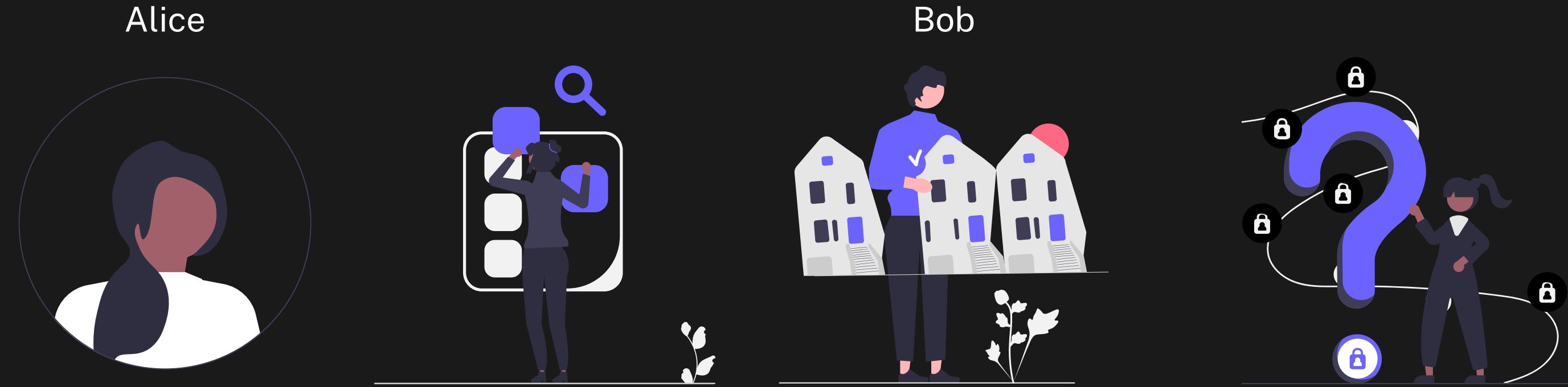
Secured by advanced
cryptography

How do we use it? For what ?

RING SIGNATURES ?



USE CASE : APARTMENT RENTAL



✓ Alice wants to rent Bob's apartment paying by crypto.

? Bob asks Alice for proof of solvency guaranteeing that she has enough funds to pay the rent for X months.

✗ The problem is that Alice does not want to reveal to Bob her Wallet in which she holds all these funds because she does not want to associate her on-chain activity with her identity.

HOW IT WORKS IN 3 STEPS

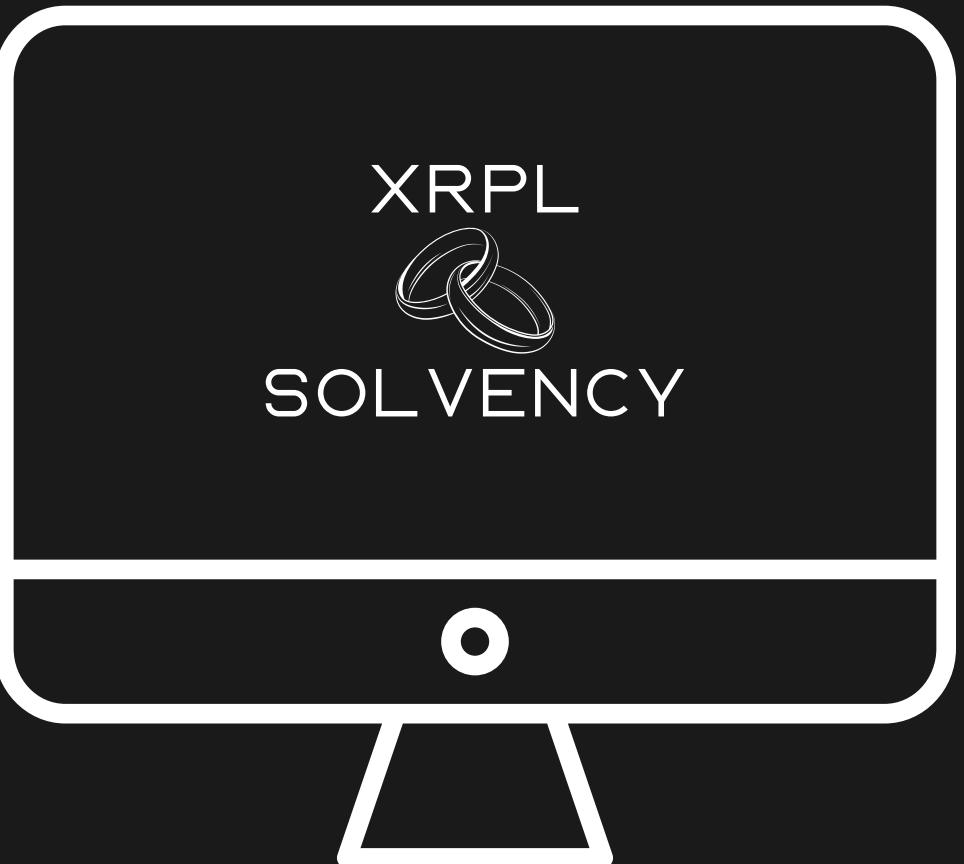
Step 1: Generating the solvency proof



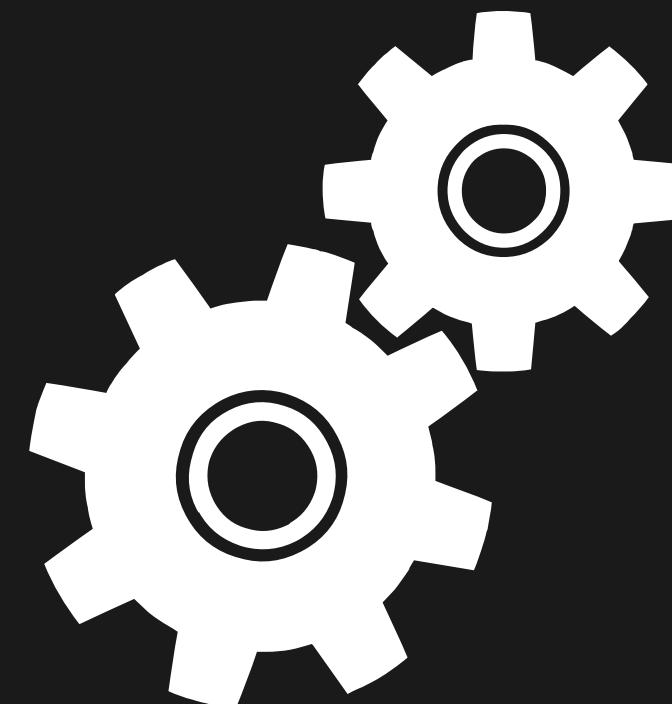
ALICE



- RECEIVING ADDRESS
- SECRET ADDRESS
- TOKEN + AMOUNT
- *SHARED SECRET



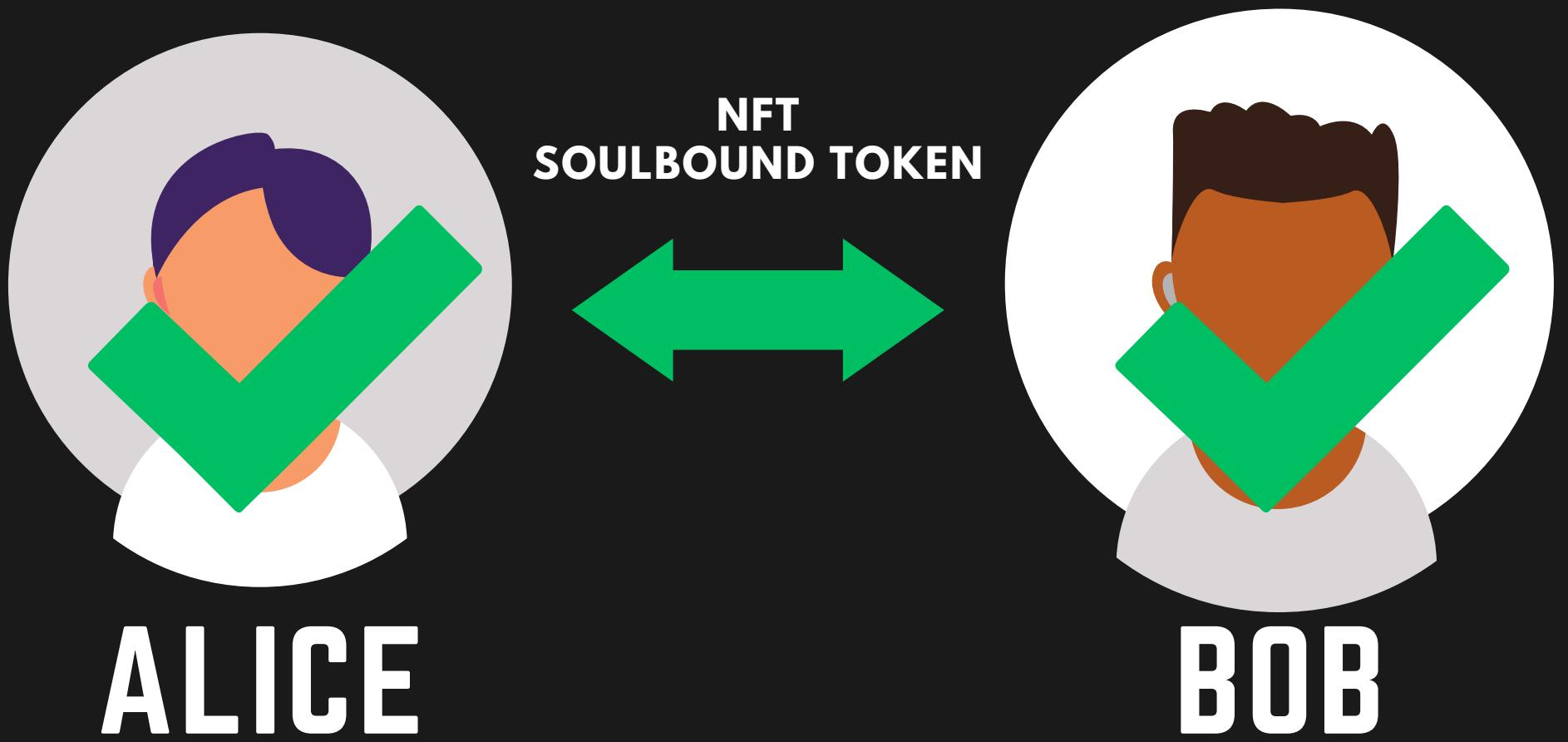
PROOF



**OFF/ON CHAIN
VERIFIER**

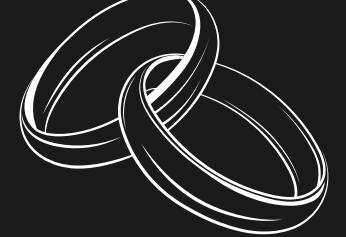
HOW IT WORKS IN 3 STEPS

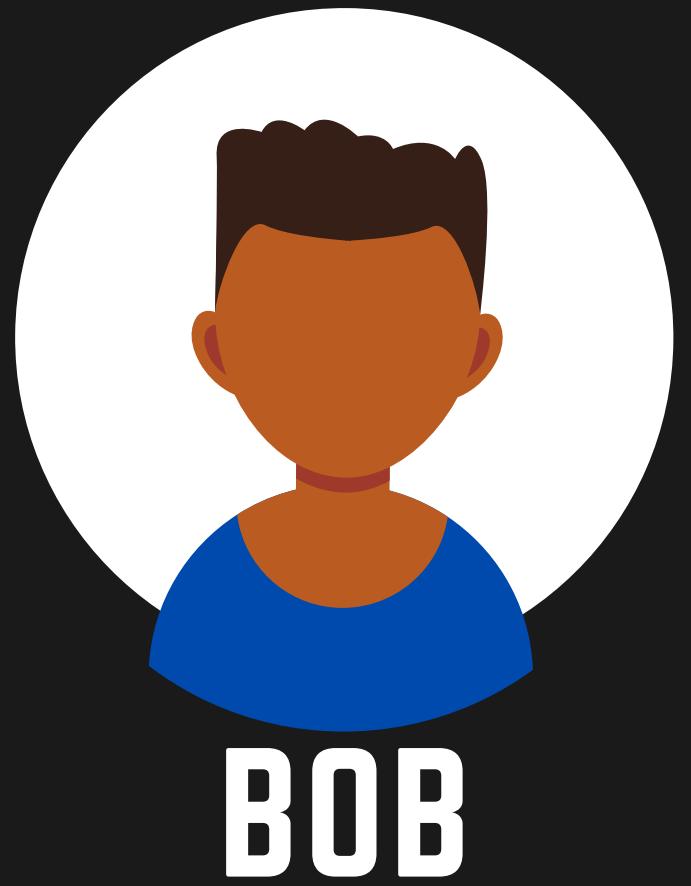
Step 2: Agreement



HOW IT WORKS IN 3 STEPS

Step 3: Transferring the funds via a "zk channel" (in development)

XRPL

SOLVENCY



USE CASE: PROOF OF RESERVE (DEX/CEX)

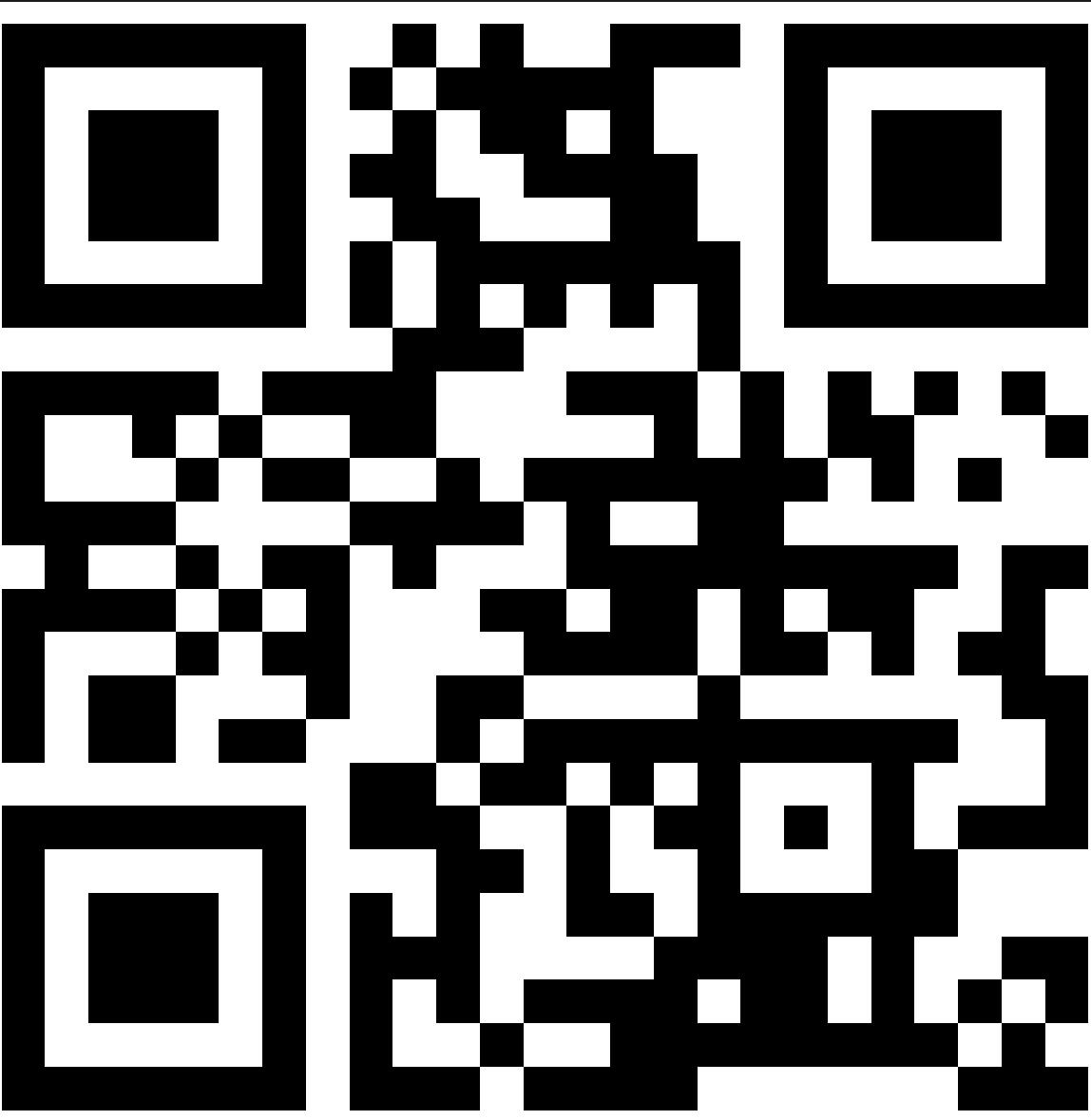
Current PoRs are carried out by independent entities.

✗ The problem is that users have no guarantee that the audit was well carried out.

✓ With our solution anyone (CEX/DEX...) can generate a PoR via an open source and verifiable mechanism based on cryptographic concepts.
Everyone will be able to know which mechanism was used!



LIVE DEMO - WEBAPP



LIVE APP



VIDEO

WHY IS XRPL A GOOD FIT?

- Blockchain solution that is scalable, sustainable, and decentralized
- Tx mechanisms allow us to retrieve data easily
- XRPL Protocol Consensus Algorithm, for high levels of scalability
- Lot of documentation, big community all around the world
- XRPL native cryptocurrency (XRP) can be used as a bridge currency for currency conversions, enabling transactions between different currencies without the need for multiple intermediaries, reducing transaction fees, and increasing transaction speed. Useful for business focus use cases.

FOR THE COMMUNITY

Our goal is to provide a set of tools for the community.

- ✓ Giving every builder the opportunity to create more innovative applications while respecting everyone's privacy.
- ✓ Participate in the development of the XRPL protocol.

GTM STRATEGY

Individuals



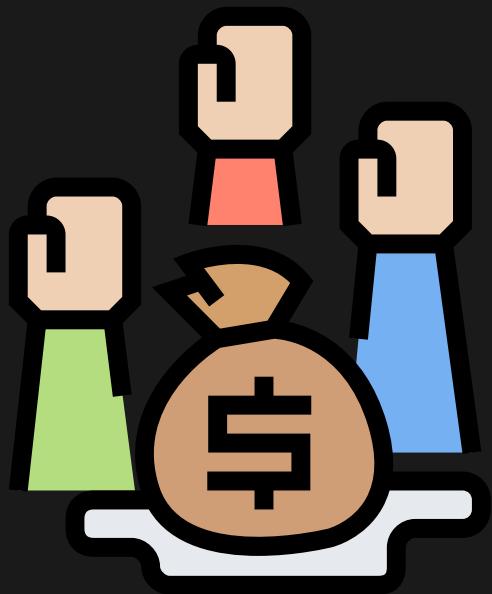
- Renting
- Loans
- DID

Businesses



- Real Estate
- Investments
- Proof of Reserve

Non-profit Organizations:



- Charitable donations
- Crowdfunding

Financial Institutions



- Insurance
- Loans
- Prevents bad debt

ROADMAP :

Here are some of the following steps for our project

Q4 2023	Q1 2024	Q2 2024	Q3 2024
<p>Switch from a python implementation of ring signatures to a typescript implementation.</p> <p>Development of a browser plugin to include directly the signature and verification process in the front-end.</p>	<p>Audit of the cryptographic implementation in typescript.</p> <p>Audit of the plugin.</p> <p>Release of the implementation as an open source library.</p> <p>Release of the v1 product (proof only possible on the XRP coin)</p>	<p>Creation of an indexer allowing to make proofs on the tokens and NFT present on XRPL</p> <p>v2 beta (proof possible on all tokens and NFT on XRPL)</p>	V2 release

HACKATHON - OUR TEAM



Thomas Hussenet

- FinTech Engineering Student
- Member of KRYPTOSPHERE®
- LinkedIn: [Thomas Hussenet](#)
- Telegram : @jamonix

Maxime Dienger

- FinTech Engineering Student
- Head of KRYPTOSPHERE®
- LinkedIn: [Maxime Dienger](#)
- Telegram : @krkmu

OUR TEAM MEMBERS



Thomas Hussenet

- FinTech Engineering Student
- Member of KRYPTOSPHERE®
- LinkedIn: [Thomas Hussenet](#)
- Telegram :@jamonix



Maxime Dienger

- FinTech Engineering Student
- Head of KRYPTOSPHERE®
- LinkedIn: [Maxime Dienger](#)
- Telegram :@krkmu



Adam Dahmoul

- Data Engineer
- Member of KRYPTOSPHERE®
- LinkedIn: [Adam Dahmoul](#)
- Telegram :@Kaiser256

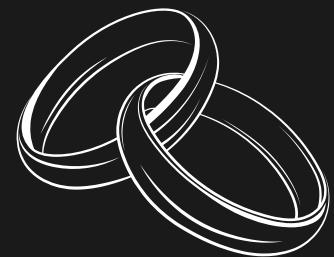


Nathan Hervier

- FinTech Engineering Student
- Member of KRYPTOSPHERE®
- LinkedIn: [Nathan Hervier](#)
- Telegram :@ElliFromSea

THANK YOU FOR YOUR ATTENTION

XRPL



SOLVENCY