

# 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**

**Solvency proofs are technically hard to implement using ZK**

# THE SOLUTION : RING SIGNATURE

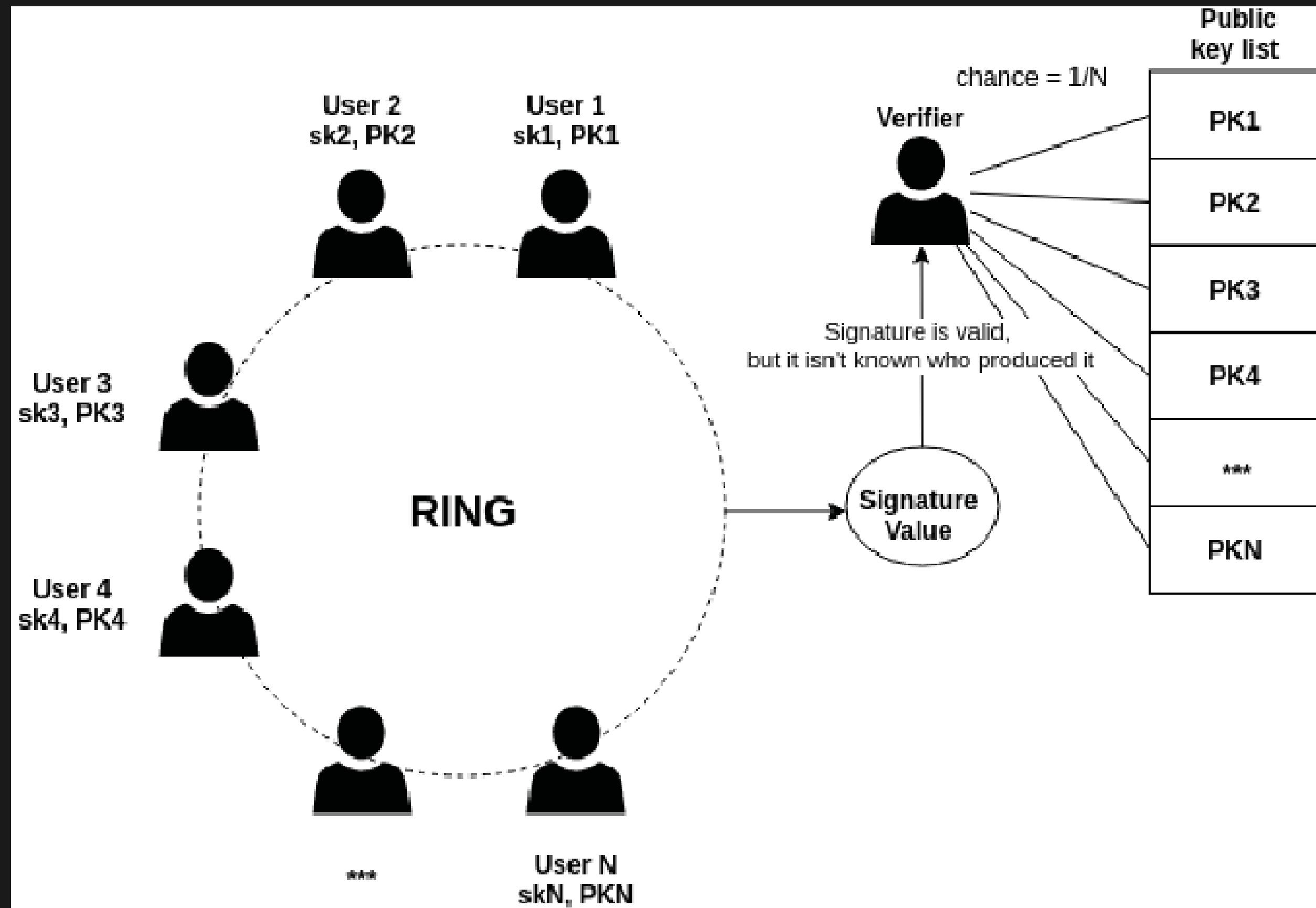
XRPL Friendly

Scalable

Secured by advanced  
cryptography

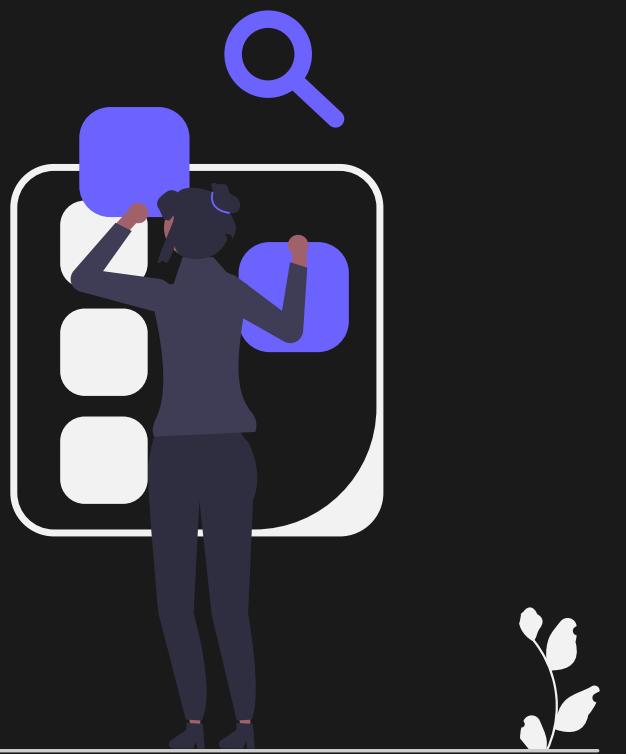
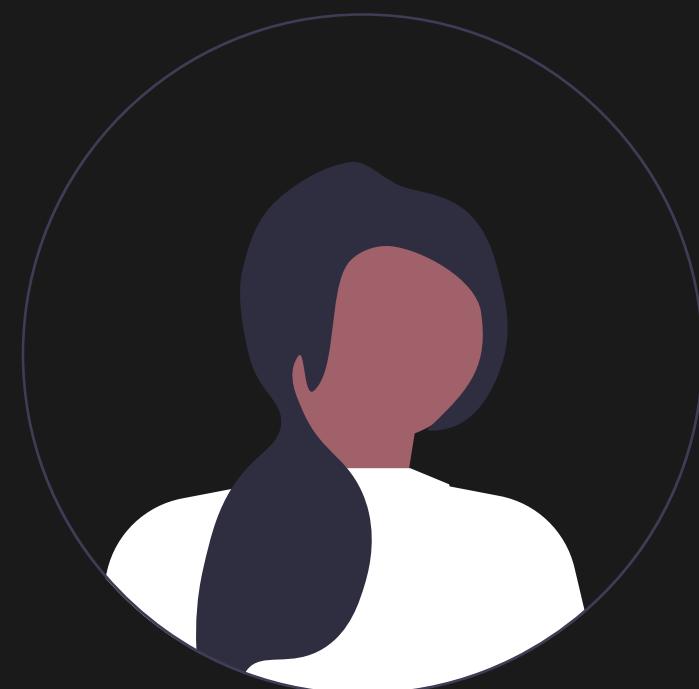
How do we use it? For what ?

# RING SIGNATURES ?



# USE CASE

Alice



Bob



# HOW IT WORKS IN 3 STEPS

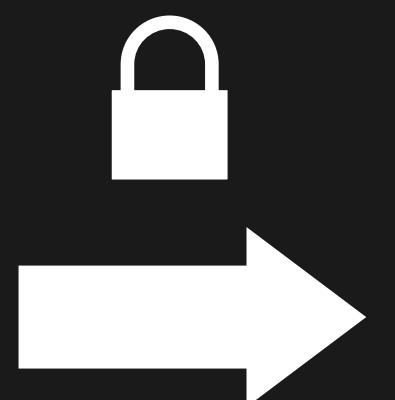
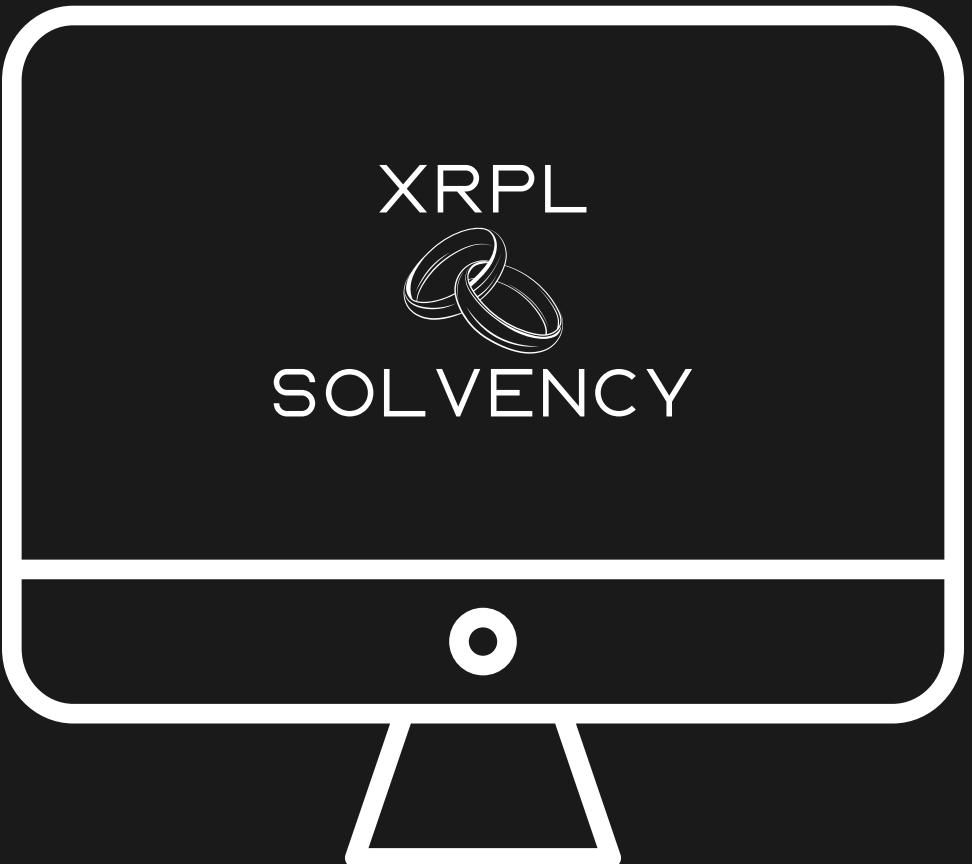
## Step 1: Generating the solvency proof



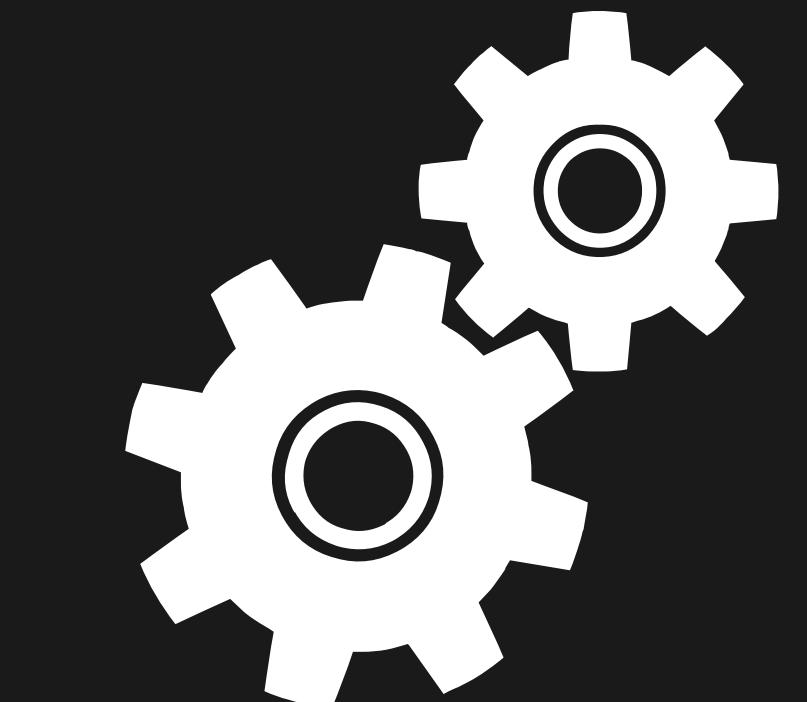
**ALICE**



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



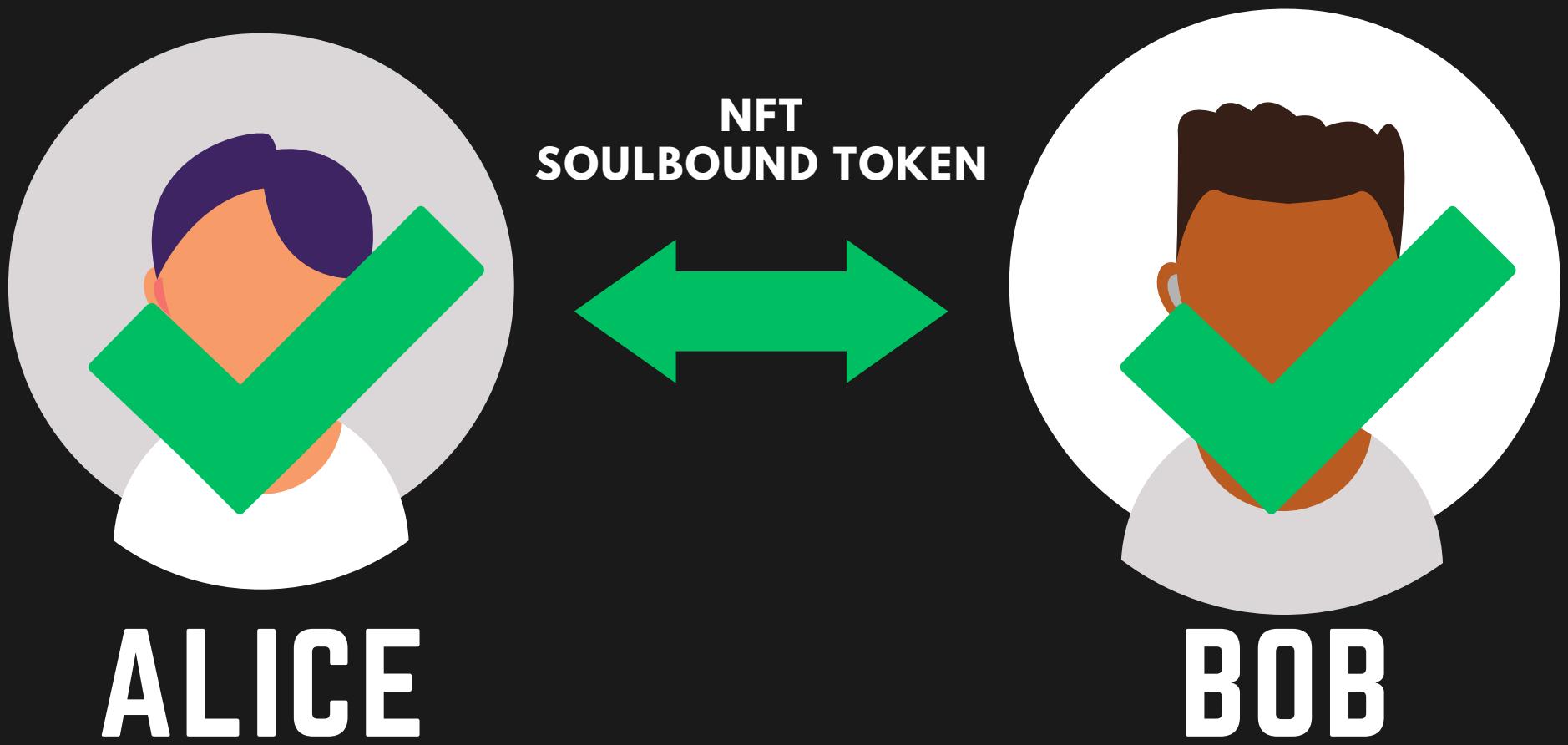
**PROOF**



**OFF/ON CHAIN  
VERIFIER**

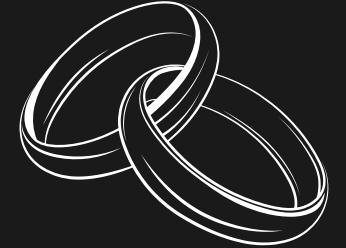
# HOW IT WORKS IN 3 STEPS

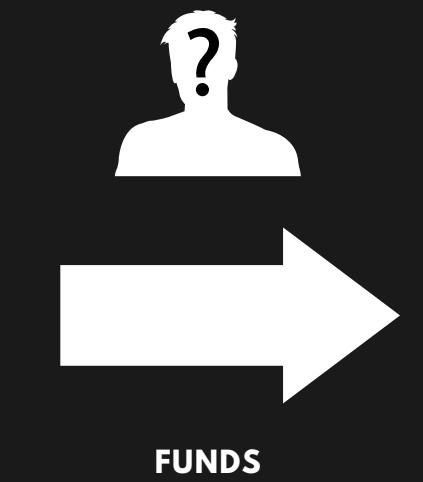
## Step 2: Agreement



# 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.

# WHY IS XRPL A GOOD FIT?

- Blockchain solution that is scalable, sustainable, and decentralized
- Smart contract deployment and hosting via "Codius platform" like or use of Hooks, useful for fast and efficient validation of transactions regarding proof generation and verification
- 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.

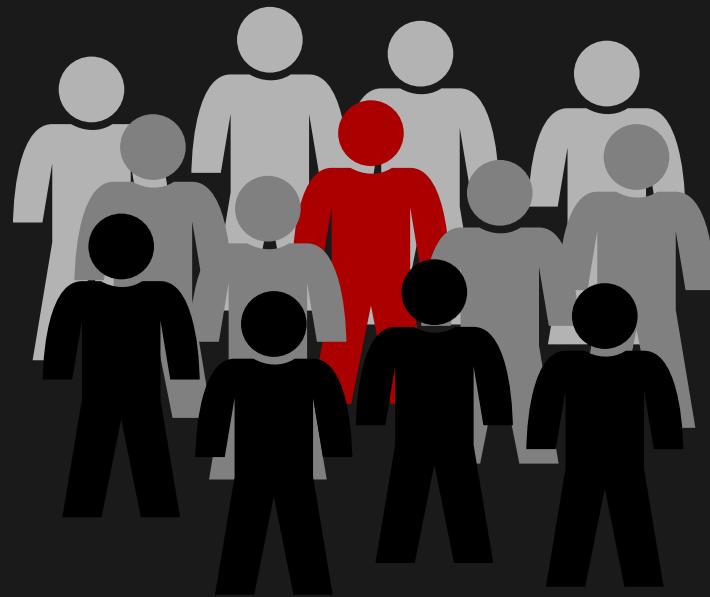
# FOR THE COMMUNITY

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



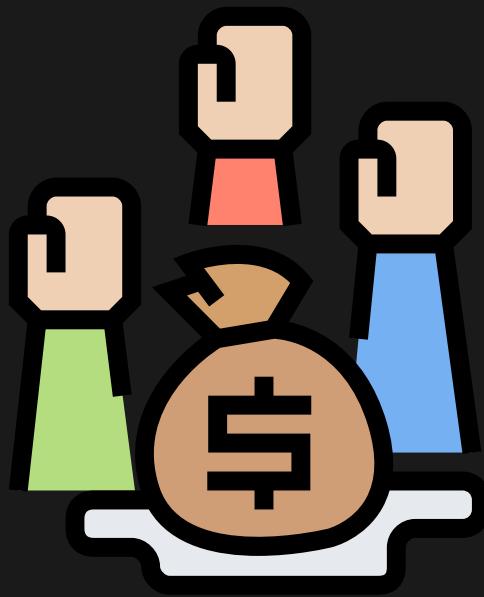
- Renting
- Loans
- Gaming

Buisnesses



- Supply chain
- Investments

Non-profit Organizations:



- Charitable donations
- Crowdfunding

Financial Institutions



- Insurance
- Loans

# ROADMAP :

Here are some of the following steps for our project

Q3 2023	Q4 2023	Q1 2024	Q2 2024
---------	---------	---------	---------

Dev. a front-end isolated environment where programs have access to a limited set of capabilities, determined by the permissions they were granted by the user during installation

Audit and full use case integration: apartment renting, charitable donations, investments

Creation of an XRPL indexer

Creation of a fund transfer channel using zk technology

First partnerships and integrations with protocols, real word business...

# OUR TEAM MEMBERS



## Thomas Hussenet

- FinTech Engineering Student
- LinkedIn: Thomas Hussenet
- Telegram : jamonix

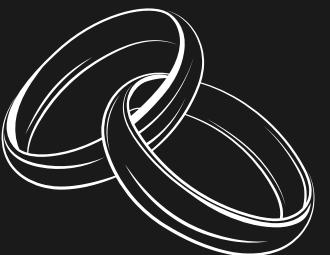


## Maxime Dienger

- FinTech Engineering Student
- LinkedIn: Maxime Dienger
- Telegram : @krkmu

# THANK YOU FOR YOUR ATTENTION

XRPL



SOLVENCY

