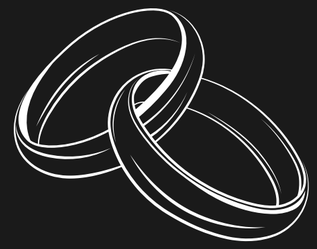
# ALICE'S  RING

## Proof of solvency

# CONTENT

# THE PROBLEM

How can we enhance privacy with proof of solvency ?

**No EVM based 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

EVM Friendly

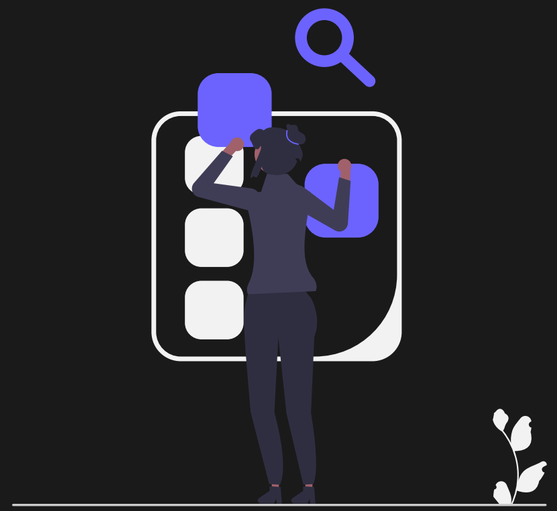
Scalable

Secured by advanced cryptography

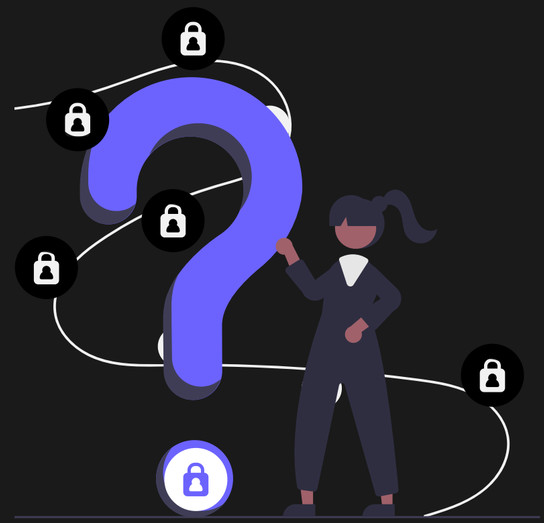
How do we use it? For what ?

# USE CASE

Alice



Bob



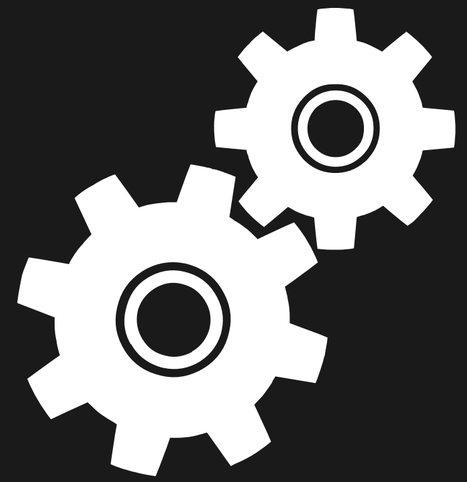
# HOW IT WORKS IN 3 STEPS

## Step 1 : Generating the solvency proof

ALICE

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

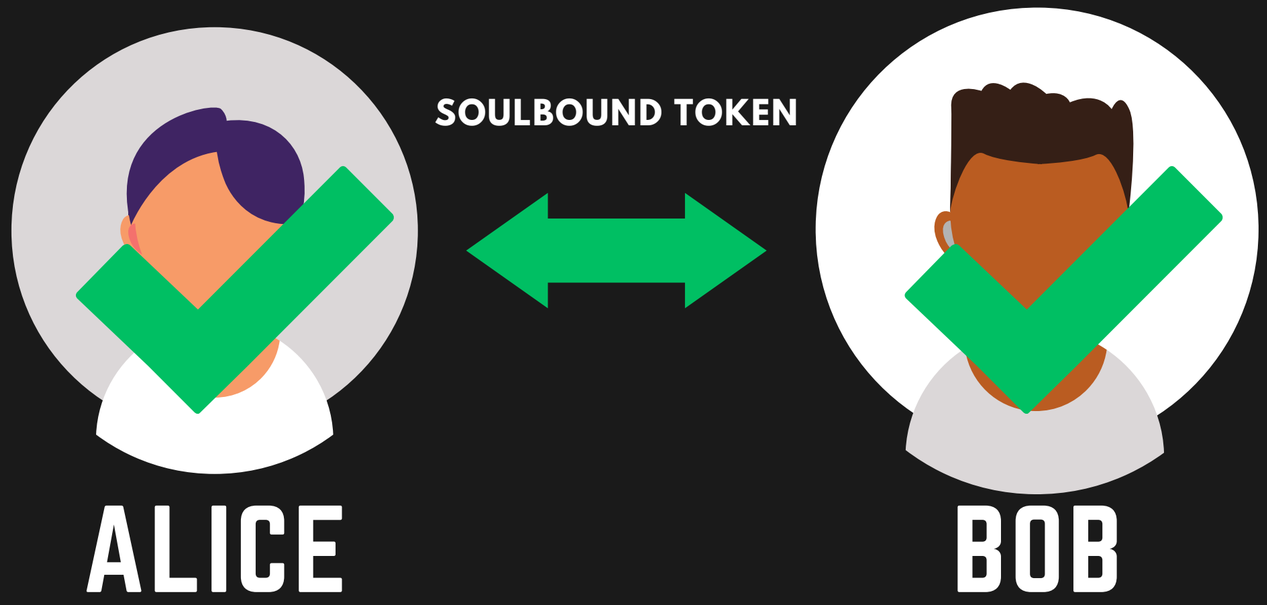

PROOF



ON CHAIN VERIFIER

# HOW IT WORKS IN 3 STEPS

## Step 2 : Agreement



# HOW IT WORKS IN 3 STEPS

## Step 3 : Transfering the funds

Alice's ring

Proof of solvency

zkBob

FUNDS

BOB

# TECHNOLOGY STACK

| INFURA | | polygon | | Scroll |
|---|---|---|---|---|
| • Multiple network deployment<br>• Truffle Boxes<br>• Infura's RPC endpoints<br>• Retrieve pubkey points via API | • Direct Deposit Integration | • Smart contract: proof verification and SBT minting<br>• Integration with the whole Polygon ecosystem (zkEvm...)<br>• Compatibility with zkBob for proof generation + transfert | • API requests to create the anonymity set | • Smart contract: proof verification and SBT minting |

# GTM STRATEGY

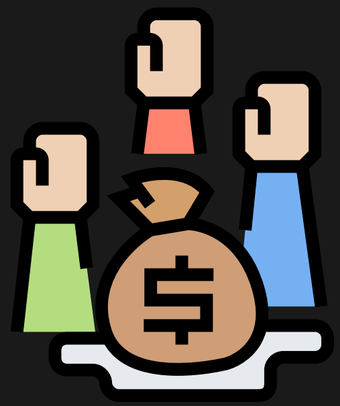
## Individuals

- Renting
- Loans
- Gaming

## Buisnesses

- Supply chain
- Investments

## Non-profit Organizations:



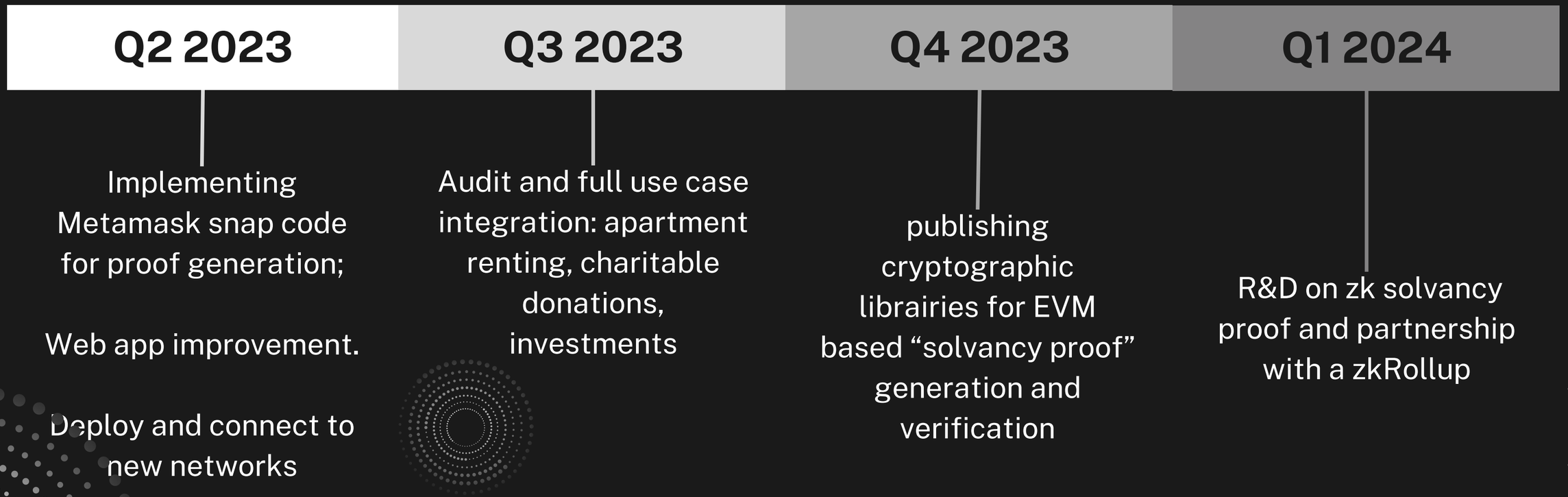
- Charitable donations
- Crowdfunding

## Financial Institutions

- Insurance
- Loans

# ROADMAP :

Here are some of the following steps for our project



# OUR TEAM MEMBERS

## Adam Dahmoul

- Data Scientist
- LinkedIn:  Adam Dahmoul
- Telegram : @kaiser216

## Thomas Hussenet

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

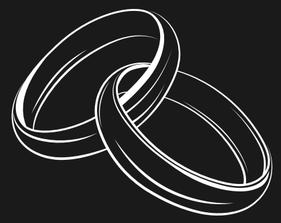
## Nathan Hervier

- FinTech Engineering Student
- LinkedIn:  Nathan Hervier
- Telegram :  @ellifromsea

## Maxime Dienger

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

# THANK YOU FOR YOUR ATTENTION



Alice's ring

Proof of solvency