Encode.club
zkBootcamp Q1

Blade Runner

kill bots & replicants

Group 1

@TheLizards @Janio @aalenaqvi @aquental @_manza_ @Mirna

Goal

Create a tool using Zero Knowledge primitives to increase the effectiveness of an AirDrop from a Blockchain without revealing user's identities.

1. Air Drop

The goal of an AirDrop is to incentivize the use of the blockchain or app: to attract using an incentive to try and continue to use the DApp.

➔ **Scaling the network**

Attract new users by offering free tokens .

➔ **Stimulate adoption**

Create market buzz and attract media attention.

➔ **Build a community**

Offer real value to build a strong community.

The main issue in an AirDrop is to grow the human backed user base!

Tip

FIltering the humans from the replicants is **hard.**

Incentivize the human users to prove they are "real" and earn more value by doing it..

How to talk to humans only.

(kill the replicants!)

Tip

Incentivize humans to prove their humanity while remaining anonymous

The *prover* will convince he is human to the *verifier* (Dapp) without revealing their identity (*zero knowledge*).

2. How

The human will bind his wallet to an OAuth provider without revealing his identity.

➔ **OAuth**

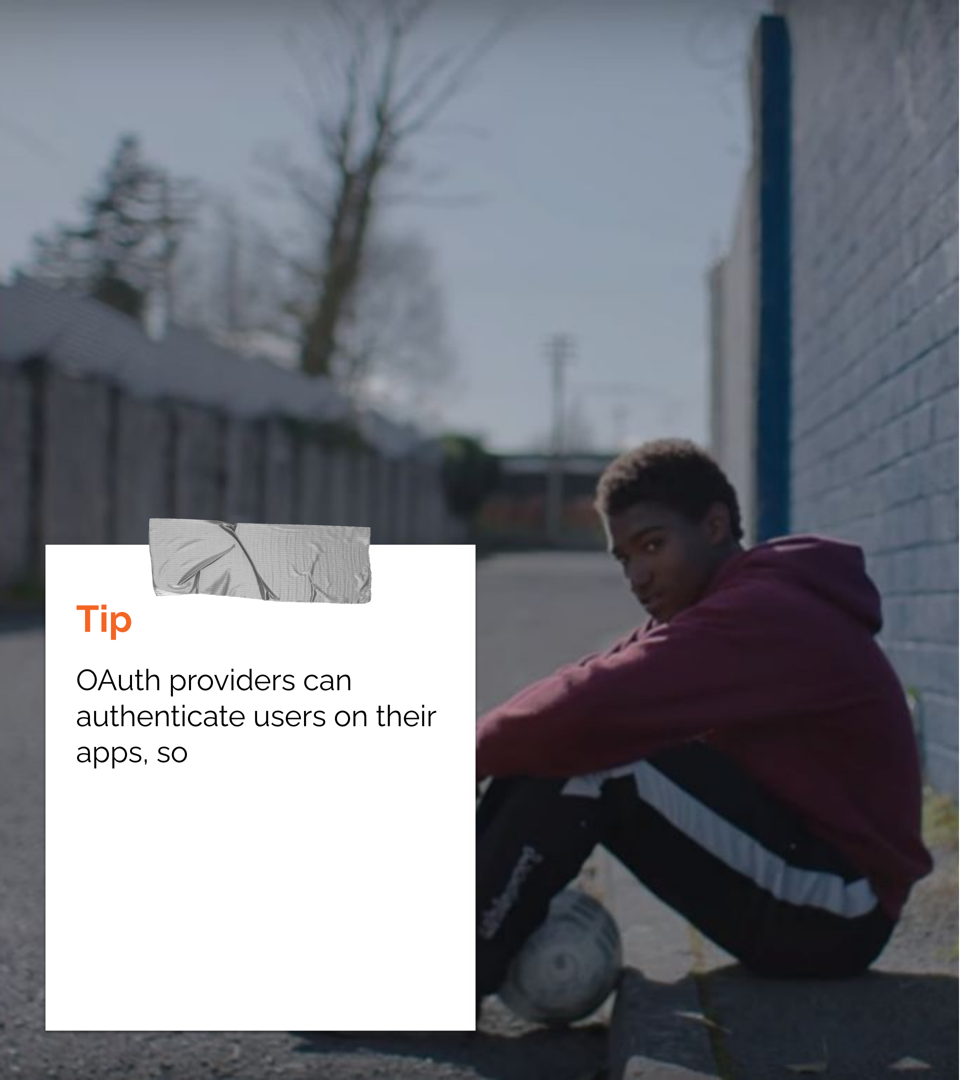
secure and convenient way for websites to leverage existing authentication systems, promoting a smoother user experience

➔ **Biometry**

Use other ways to prove humanity.

➔ **Binding**

Associate his wallet with a proof that he can login in one or more OAuth providers.



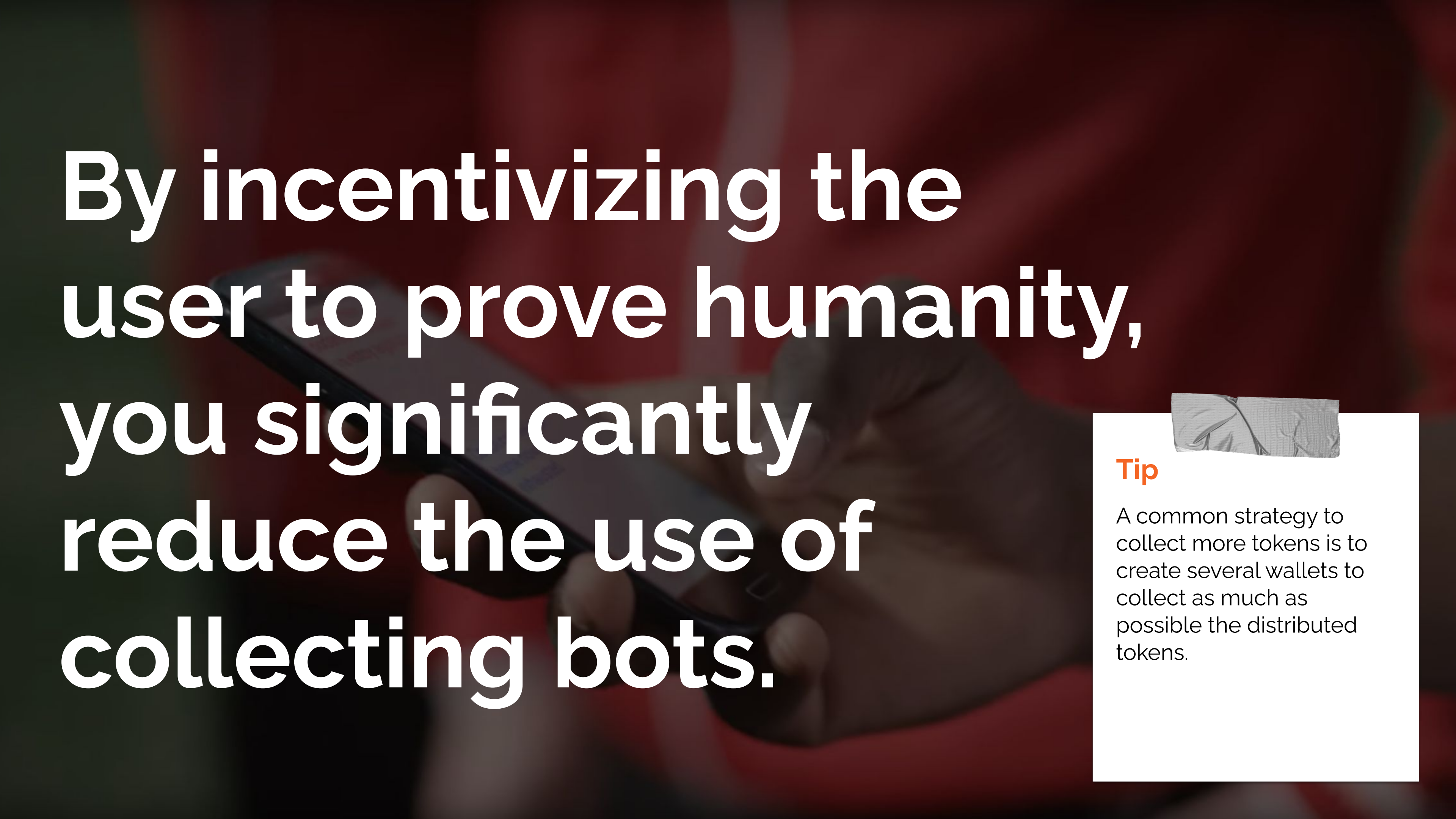
Tip

OAuth providers can authenticate users on their apps, so

Incentives

The more associations with OAuth providers, the greater the human score is.

Increasing the human score would benefit the user by multiplying their drop.



By incentivizing the user to prove humanity, you significantly reduce the use of collecting bots.

Tip

A common strategy to collect more tokens is to create several wallets to collect as much as possible the distributed tokens.

The technology

Explain the technology of ZKG and FHE.

Defense in depth: never store the user ID anywhere but its hash salted by the campaign ID.

Use FHE to verify if the hash of user ID was already used in the campaign becoming sybil resistant.

Tip

ZKG creates a bond between the wallet and the user ID without revealing the user ID.

FHE (Fully Homomorphic Encryption) is used to check if the user ID was associated with other wallet without decrypting..

3. Example

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque justo orci, imperdiet in ultricies eget, vestibulum non felis. Morbi nisl leo, pharetra at mauris non, porttitor euismod tellus.

➔ **Maecenasn**

Donec malesuada varius dui in commodo.

➔ **Curabitur**

Commodo nec quam ut, sollicitudin cursus orcido.

4. Closing

Sed sed pulvinar purus, et eleifend quam:

➔ **Milestones**

Steps to create the solution…

➔ **Testimony**

More Loren Ipsum…

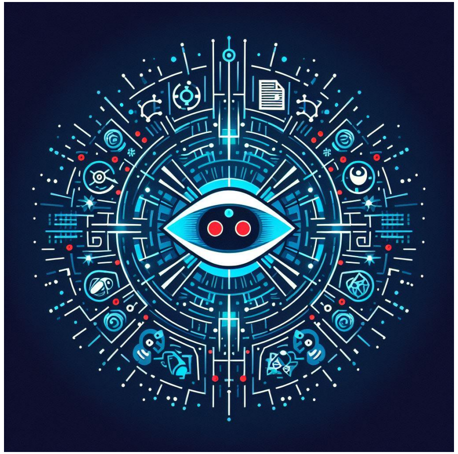
➔ **Whats next?**

How to implement it.?

Thank you!

Get in touch for a trial..

For more tips and information
https://bladerunner.com/trial



More information ...

. . . .

. . . .

. .. .