onbotting.eth

How to onbot the masses?
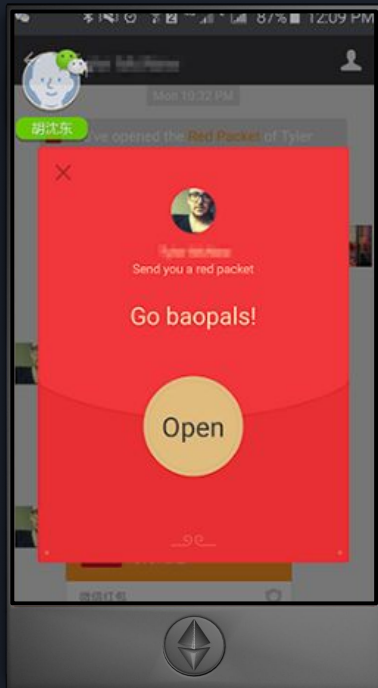
Volcà

brainbot
TECHNOLOGIES AG

Hacking "Universal Login" EIP1077 to include "invite link" functionality

Learning from the best

WeChat "Red Packets"
650+ million users at peak

PokemonGo
23+ million users in 14 days

Assumptions of "invite link" scheme

- Bob is a new user without ETH, wallet or any prior crypto knowledge

- Alice has an EIP 1077 identity contract and a spare ERC721 Robot

- Alice share the invite link with Bob over a secure channel e.g Whatsapp

- There is an incentive in place (on a user, dapp or relay level) to pay gas

Invite link via an ERC721 robot gift

Link to deployed "robotwars" ERC721 ropsten contract

Invite link scheme

1. **Alice** shares an **invite link** to **Bob**
2. Link includes a **transit private key** and a **signature**
3. Bob is directed to a **webpage**
4. Bob generates **his own** private key stored in the **browser**
5. Bob uses **transit private** key to **sign** Bob's private key
6. Bob's **browser** sends his **two signatures** to the **relayer**
7. Relayer **calls Alice's identity contract**
8. Alice's identity contract **creates** an identity contract for **Bob** and sends a Robot
9. **Bob** is now onboarded to Ethereum and **owns a robot** that he can play with!
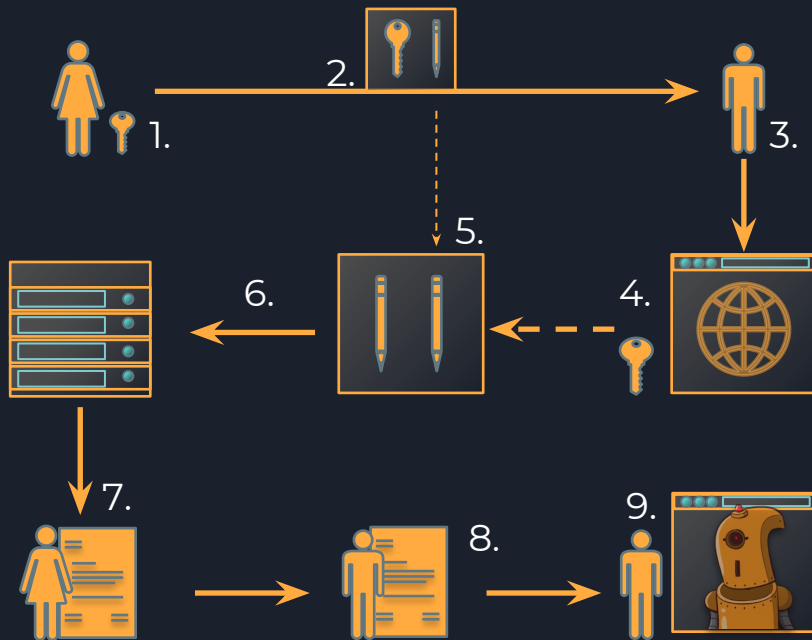
What is the added value to EIP 1077

From a user experience

- New users can receive crypto assets and get an identity contract and ENS name, without needing or understanding any things about crypto

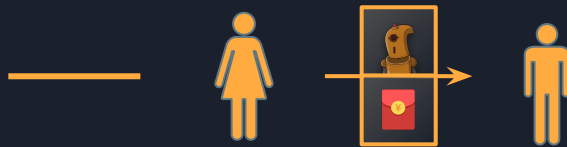- Easier possibility for sending social key recovery links

From a technical perspective

- Invite link functionality added to identity smart-contract deployed on ropsten

- Updated relay server endpoints, Universal Login SDK & UI to demo invite links

Why would anyone pay the gas?

User to user

- Digital gifts (sender covers cost)

Dapps

- User acquisition scheme (Paypal/Uber/Airbnb)
- Charge tx fees (WeChat charges 0.1 %)

Relay server operators

- Off-chain tx/subscription/KYC/work model

Future improvements

Private Key Format

- Include `salt` to counter Rainbow Attacks

Links

- Including social recovery option
- Include expiration
- Allow to send multiple invites to a closed group (Red Packet Groups)
- Combining multiple transfers into one link

Relay Servers

- Decentralized interrelay protocol e.g Tenzorum