Incendia

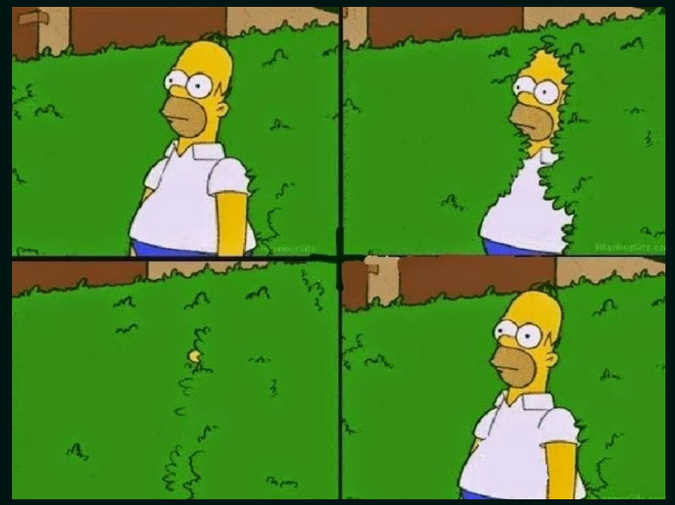
Anonymous On-Chain Auctions with ZK Passport registration

ETHGlobal Buenos Aires

Overview

Private Auction

- Private bids
- Private Identity
- On chain settlement (no third party)



Registration

ZK Passport registration

- keeping users identity private
- Inforce +18 age for bidding
- Prevent double bidding => address is bind to the identity

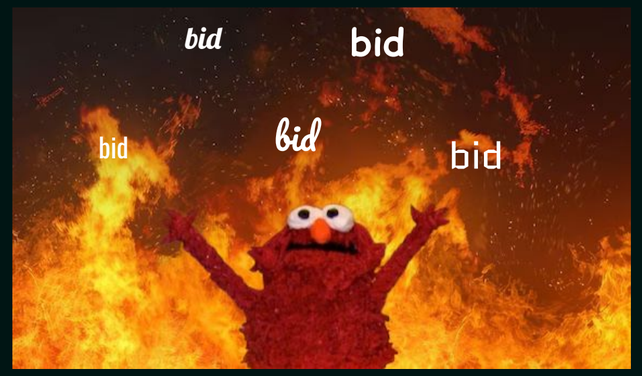
How?

Proof of Burn 🔥

- Generate a unspendable address

  Burn Address = hash(Ceremony data, Bid , zk passport ID . . .)

- Burn negligible amount Eth to that Address 🔥
- Generate and submit the burn proof
- Wait for the end of submission deadline …
- on chain settlement



Demo

future work

- Noir smart contracts
- Deploy on Aztec chain
  (encrypted bids)
- Add multiple auction scenarios
- Optimise the proof for smartphones

TEAM

Shahriar Ebrahimi

- Co-Founder – Zero Savvy Ltd
- Research Fellow at University of Warwick
- Website
- X Handle: @lovely_necro
- Github Handle: @lovely-necromancer
- LinkedIn
- Scholar link

Parisa Hassanzadeh

- Co-Founder – Zero Savvy Ltd
- Research Assistant at University of Warwick
- X Handle: @PHassanizadeh
- Github Handle: @parizad1188
- LinkedIn
- Scholar link

Pardis Toolabi

- ZK Engineer at Bermuda
- Research Assistant at University of Warsaw
- Github Handle: @pardis-toolabi
- X Handle: @ParVenture
- LinkedIn

Haniyeh Habibi

- Research Assistant at University of Warsaw
- Github Handle: @haniyeh-habibi
- LinkedIn

Thank you :)