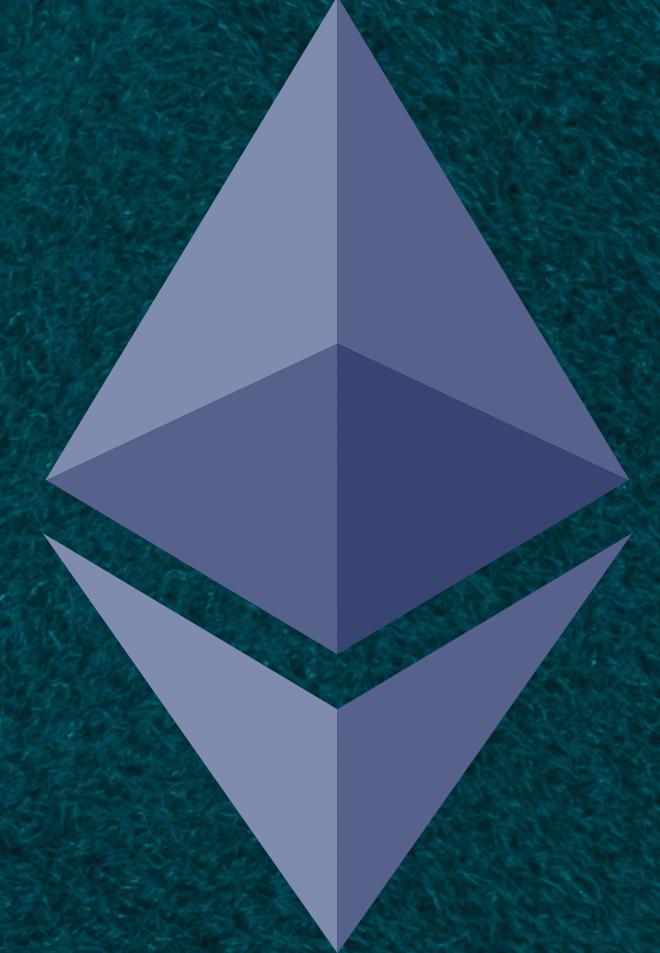


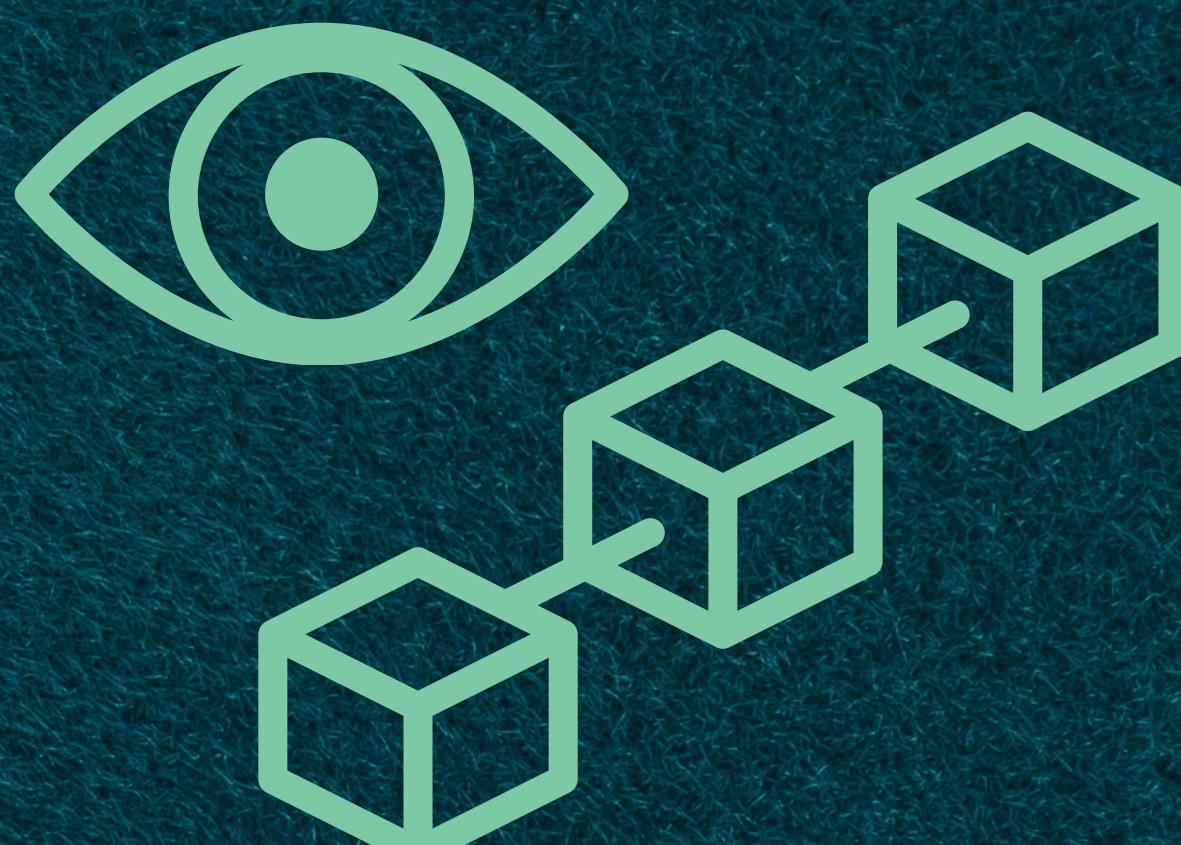
# Privacy on Ethereum Thanks to Zero Knowledge Proofs



Lukáš Častven, Koštál Kristián, Ing. PhD.

## MOTIVATION

- Blockchains are public
- No private transactions
- Alice wants to send ETH to Bob privately



Alice

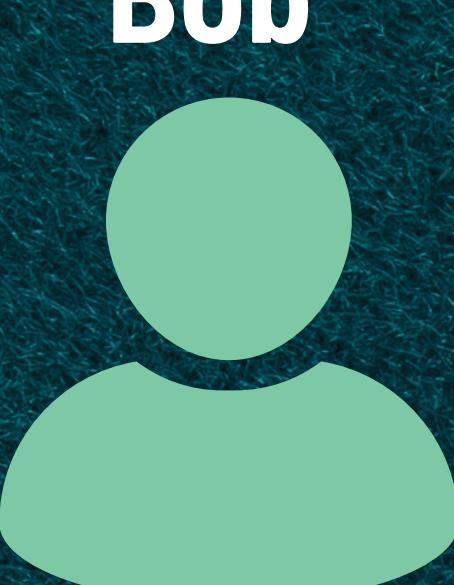
Send  
ETH



Smart  
contract  
with ETH

Submit  
Proof

Get  
ETH



## ZERO KNOWLEDGE PROOFS

- "Magic" math
- Prove anything without disclosing it

## RESULTS



Privacy  
preserving



Stealth Address  
Scheme with ZKP

## BUILD WITH

- Circom
- SnarkJS
- Solidity