Privacy on the Blockchain

The need for privacy

- Supply chain privacy:
  - A manufacturer does not want to reveal how much it pays its supplier for parts.
- Payment privacy:
  - A company that pays its employees in crypto wants to keep list of employees and salaries private;
  - End users need privacy for rent, donations, purchases;
- Business logic privacy:
  - Smart Contracts code

Blockchains cannot reach their full potential without some form of private transactions

Types of privacy

- Pseudonymity: (weak privacy)
- Full anonymity: User’s transactions are unlinkable

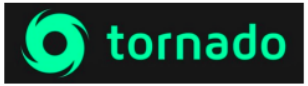
Types of privacy

No privacy:
Everyone can see all transactions

Privacy from the public:
Only a trusted operator can see transactions

Semi-full privacy:
only “local” law enforcement can see transactions

full privacy:
no one can see transactions

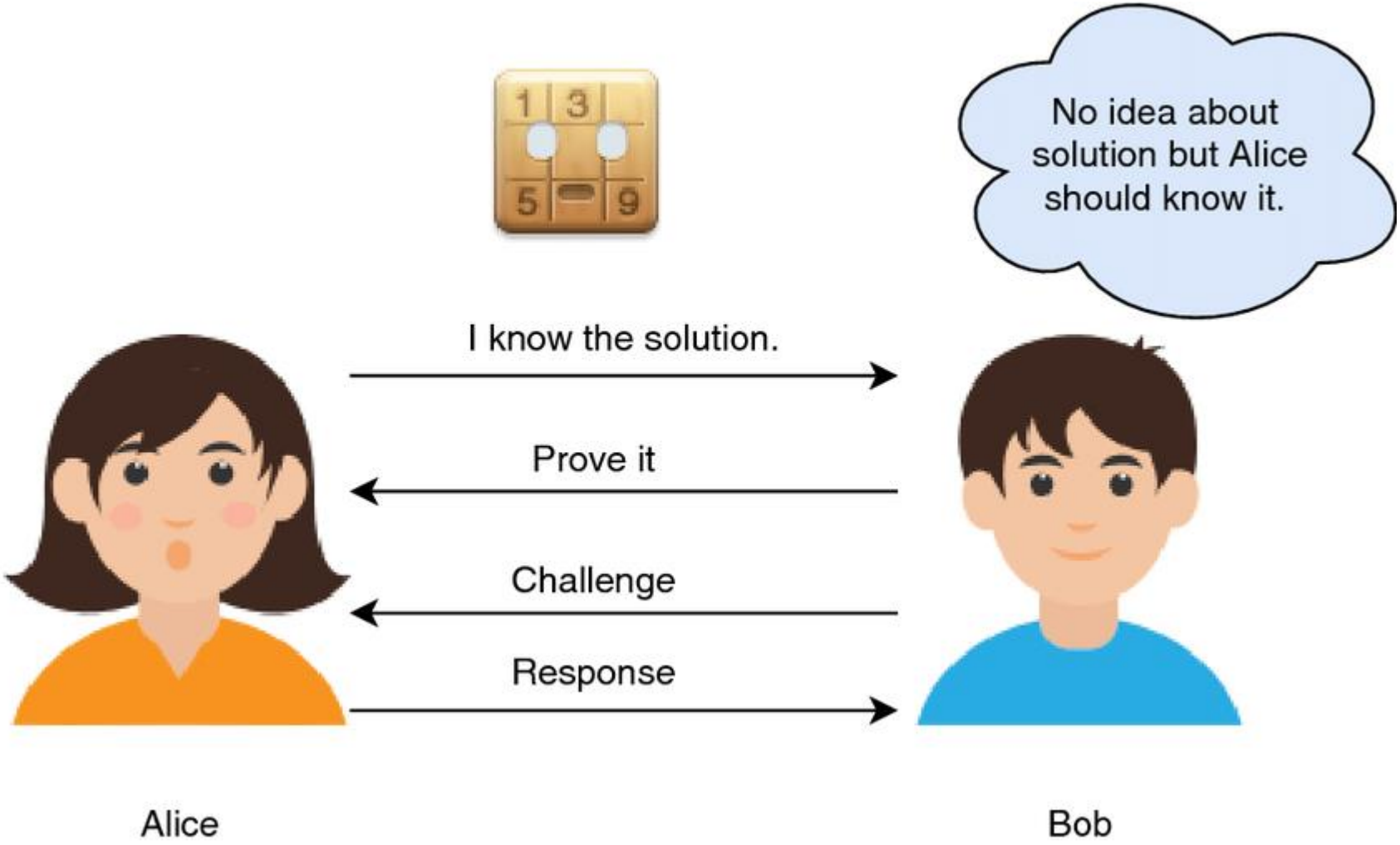


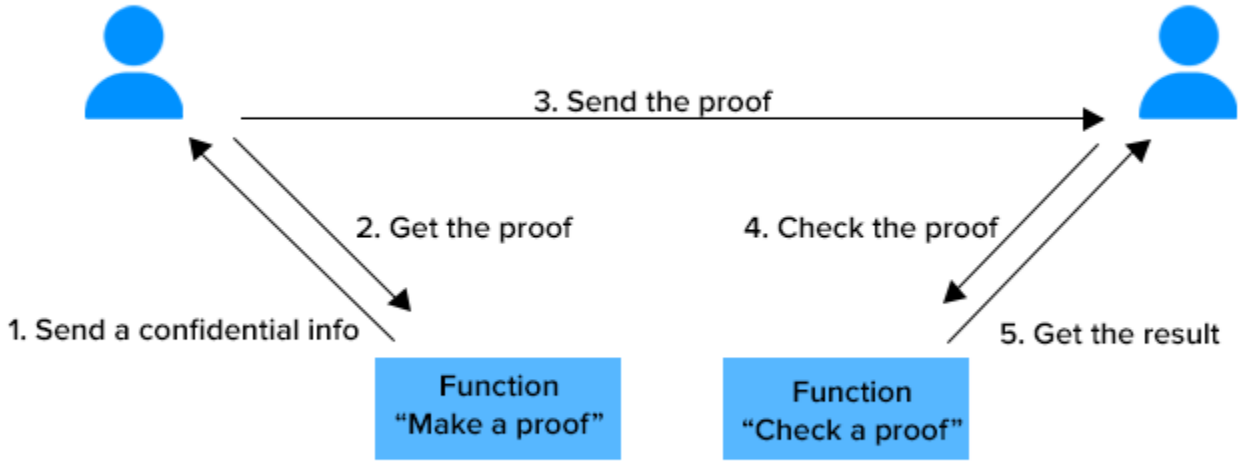
Negative aspects of complete privacy

- Criminal activity
- Challenge:
  - How to support positive applications of private payments, but prevent the negative ones?
  - Can we ensure legal compliance while preserving privacy?
  - Answer: **zero knowledge proofs**

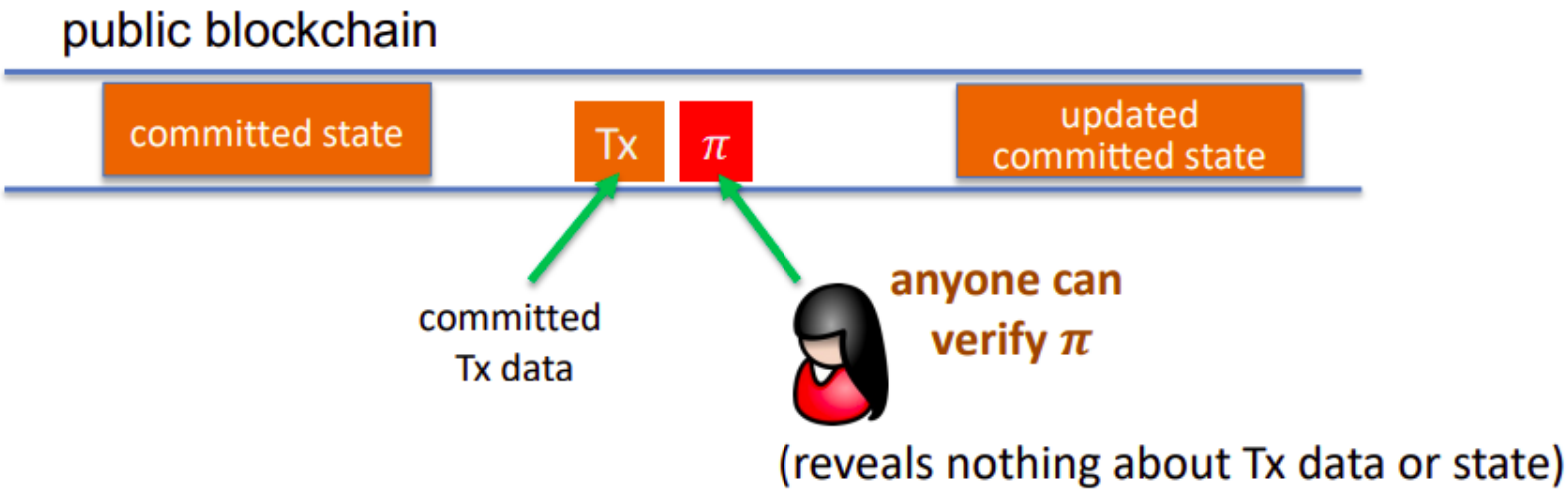
Privacy in Ethereum / MultiversX

- Every account balance is public
- For Dapps: code and internal state are public
- All account transactions are linked to account
- In time: Linking an addresses to an identity


1 3
5 9
No idea about solution but Alice should know it.
I know the solution.
Prove it
Challenge
Response
Alice
Bob


3. Send the proof
2. Get the proof
4. Check the proof
1. Send a confidential info
5. Get the result
Function
“Make a proof”
Function
“Check a proof”

Paradigm for Private Transaction



zk-SNARK

- Succinct zero knowledge proofs
- Example statement:
  - “I know an ***m*** such that SHA256(***m***) = 0”
- SNARK: the proof is “short” and “fast” to verify
  - Even if ***m*** is 100 TB of data