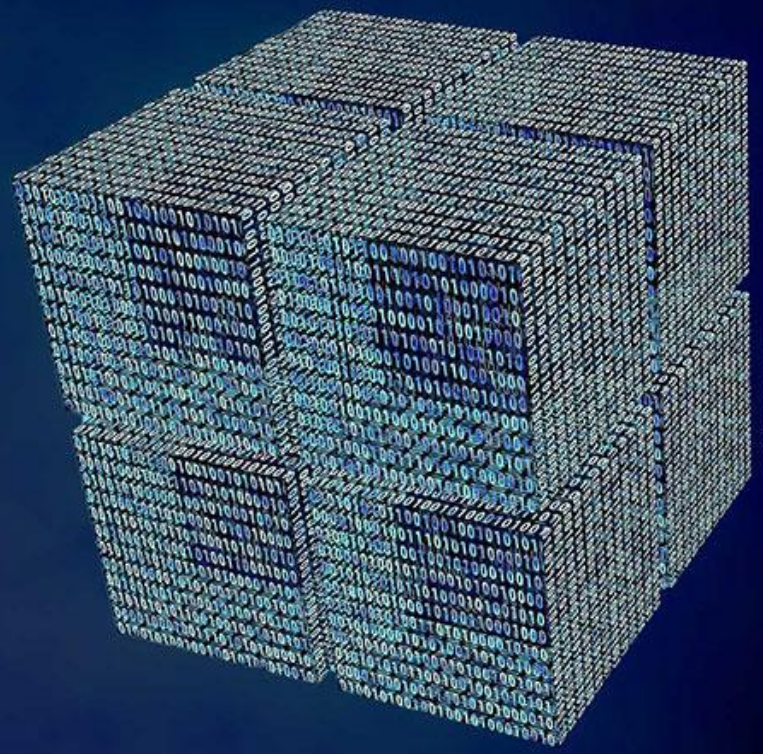
# Identity Management System Based on Blockchain Technology

Mohammad Shabib 19290116
Zaid Ibaisi 19290199
Mazen Houran 19290097

# Outline



# Overview

**What is an identity management system?**

**The problem with the current system**

**The solution**

# Current system challenges:

**The problem with the current system:**

- **identity theft, loss, or forgery.**
- **lack of control**
- **privacy concerns**

**Did anything go wrong in the past?**


# So what is the solution?

**Blockchain solves identity theft using cryptography**

**Blockchain solves the issue of lack of privacy using ZNP**

**Blockchain will eliminate the need for 3rd party KYC**

# Blockchain benefits:

1_Decentralization

2_Security

3_Consent

4_Universal ecosystem

5_Same source of truth

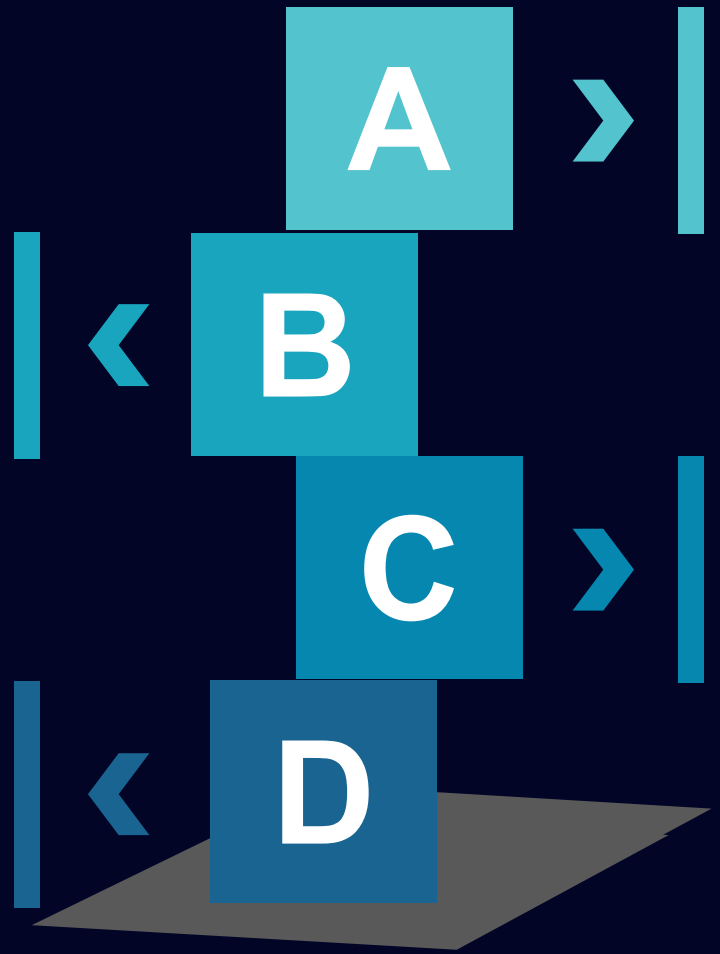
# Blockchain Based Identity Management System

**Actors**

- Identity owners
- identity auditors
- identity verifiers
- the registrar

**Security and privacy**

- Multiple auditors
- Zero-knowledge
- Hashing
- InterPlanetary file system




**Functionality**

- Permissioned blockchain

**Trust score**

- Trustworthiness
- Encouragement

# The Blockchain

BLOCK CHAIN

HYPERLEDGER INDY

## Hyperledger Indy

Hyperledger Indy provides tools, libraries, and reusable components for providing digital self sovereign identities rooted on blockchains

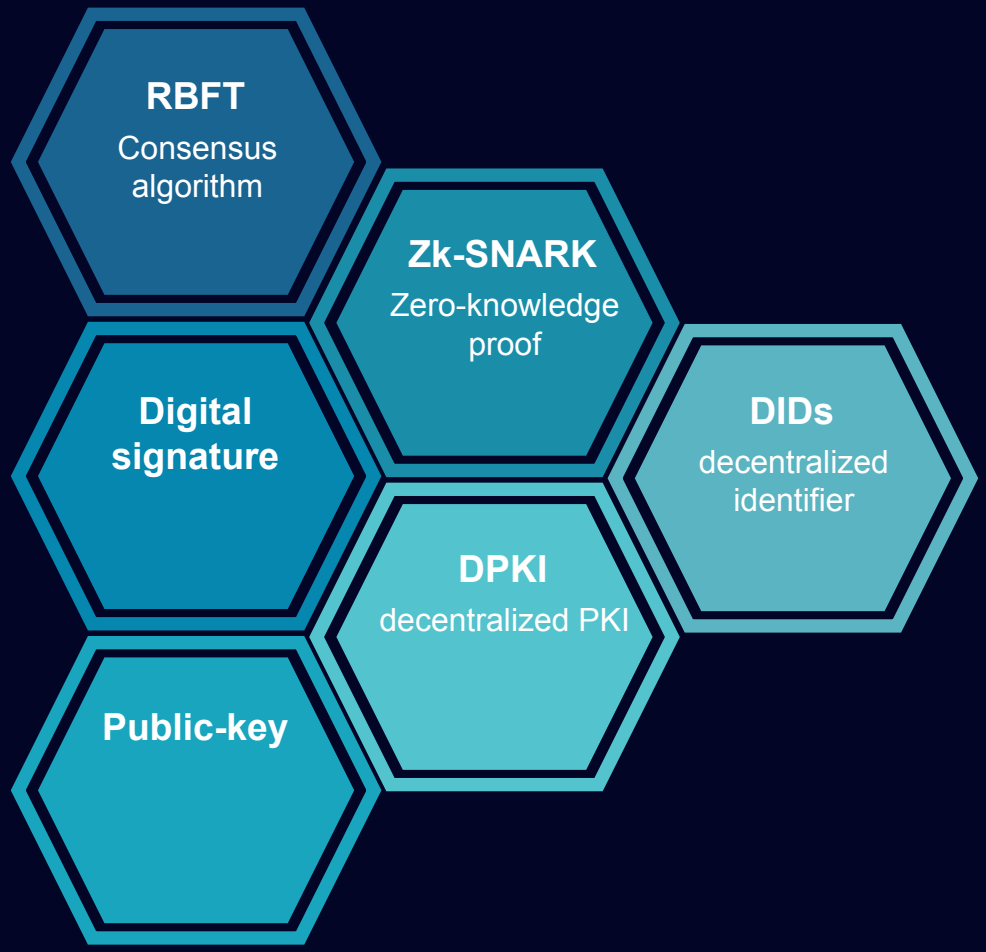
sovrin
identity for all

## Sovrin Network

Sovrin provides the infrastructure to build a blockchain designed as a global public utility exclusively to support self-sovereign identity

| Access | Validation: Permissionless | Validation: Permissioned |
|---|---|---|
| Public | Bitcoin<br>Etherium | Indy/Sovrin |
| Private | Enterprise Ethereum Alliance | Hyperledger Fabric<br>Hyperledger Sawtooth<br>R3 Corda |

# Blockchain Plenum




# Redundant Byzantine Fault Tolerance - RBFT

- ☑ Tolerance against Byzantine Faults
- ☑ Tolerance against malicious primary that can slow the performance down to the detection threshold (F). Compared to PBFT
- ☑ IRI = 3F + 1 where F is the maximum number of replicas that may be faulty and R is the total number of nodes

# Zk-SNARK

**Zk** ›

**Zero-Knowledge**

Completeness, Soundness, Zero-knowledge

**Succinct**

easy to verify, even the concept being verified is complicated

‹ **S**

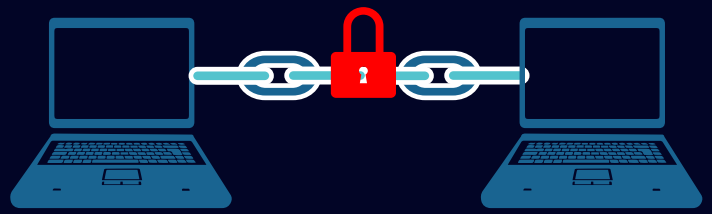
**NA** ›

**Non-Interactive**

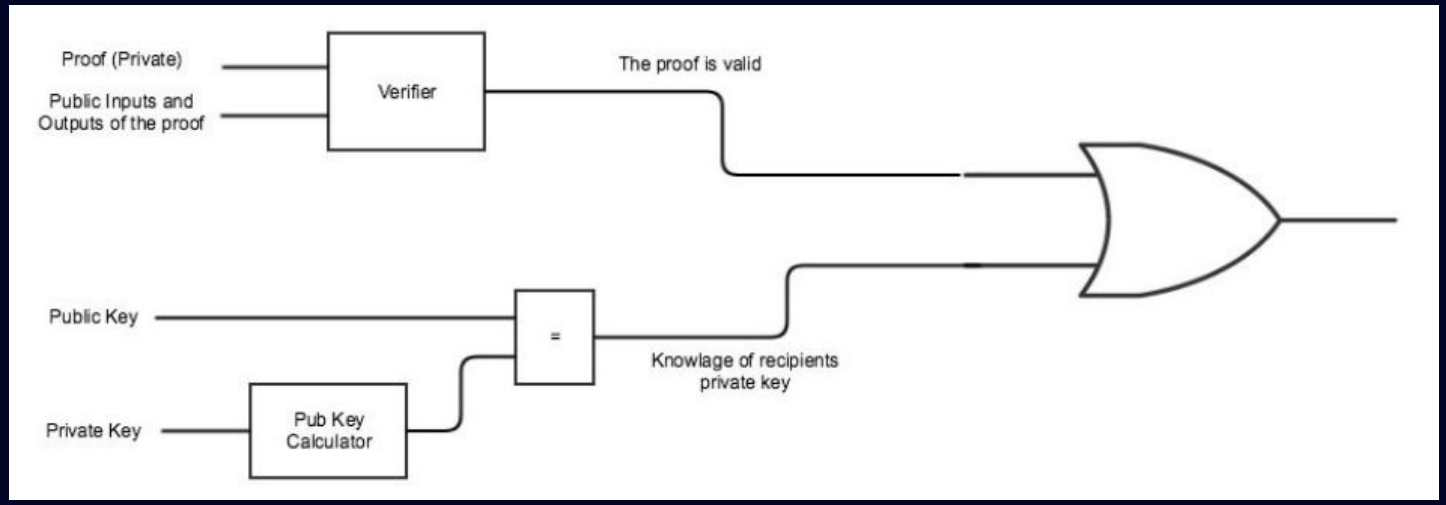
No Back-And-Forth Communication

**Argument**

‹ **A**

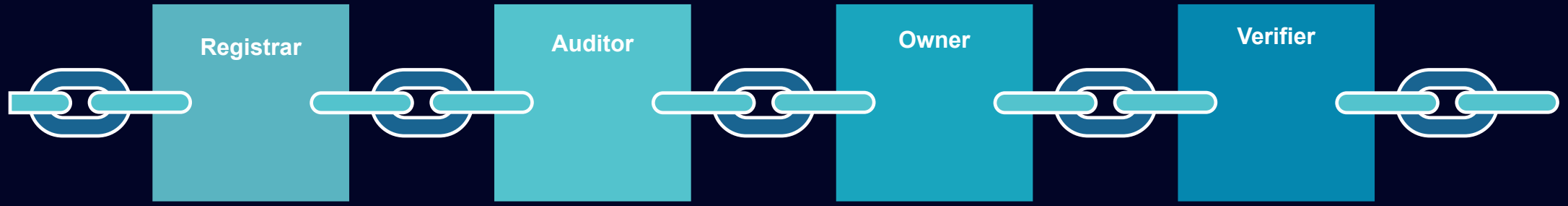


# Privacy: non-reusable proofs




- A received proof is not valid to send to a third identity.
- To prove A, you create a new proof A' that is valid either if A is valid OR you know the private key of the recipient

# Registration




Governmental Entity (civil registry department, Immigration department), registrars will be added in the genesis block

Governmental Certification Authority (CA), Auditors will be added by registrars

Individuals

Business entities, Organization. **every verifier is an owner**

# Decentralised Identifiers- DIDs

DIDs provide a standard way for individuals and organizations to create permanent, globally unique, cryptographically verifiable identifiers entirely under the identity owner’s control. No one can take DID away from whomever owns or controls the associated private key

# Challenges

- Lost Private Key
- Cost

# Thank you for listening!

> If you don’t believe it or don’t get it, I don’t have the time to try to convince you, sorry.
>
> **SATOSHI NAKAMOTO**