St Petersburg University
www.spbu.ru

Zero-Knowledge Proof in Self-Sovereign Identity

Nataliia Kulabukhova

NEC 2019, Budva, Montenegro, 04.10.2019

History

July 5, 1993 - Peter Steiner's famous cartoon about Internet anonymity:

"On the Internet, nobody knows you're a dog"

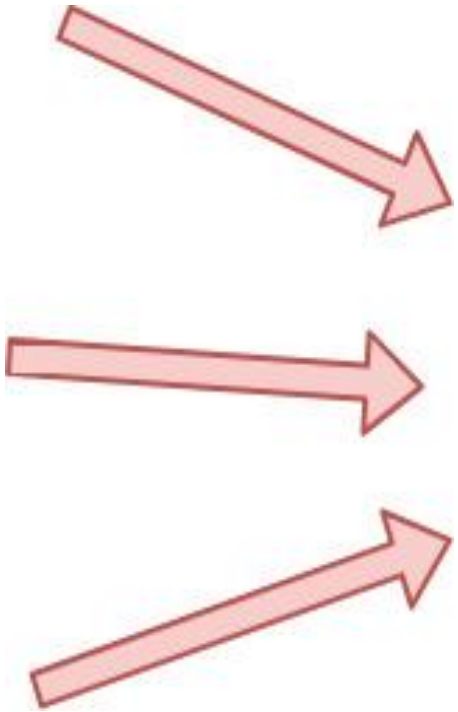
"On the Internet, nobody knows you're a dog."

History

Privacy-ABC

Zero-Knowledge Proof

Anonymous Credentials

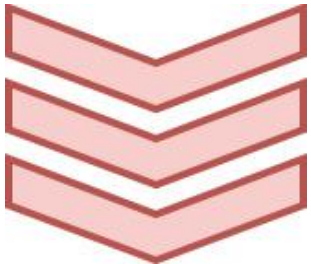


Self-Sovereign Identity (SSI)

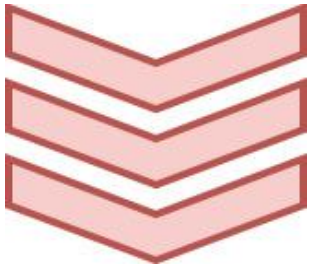
Reasons for SSI

First. Giving private information to the third parties to proof our rights.

Second. Database is stolen.



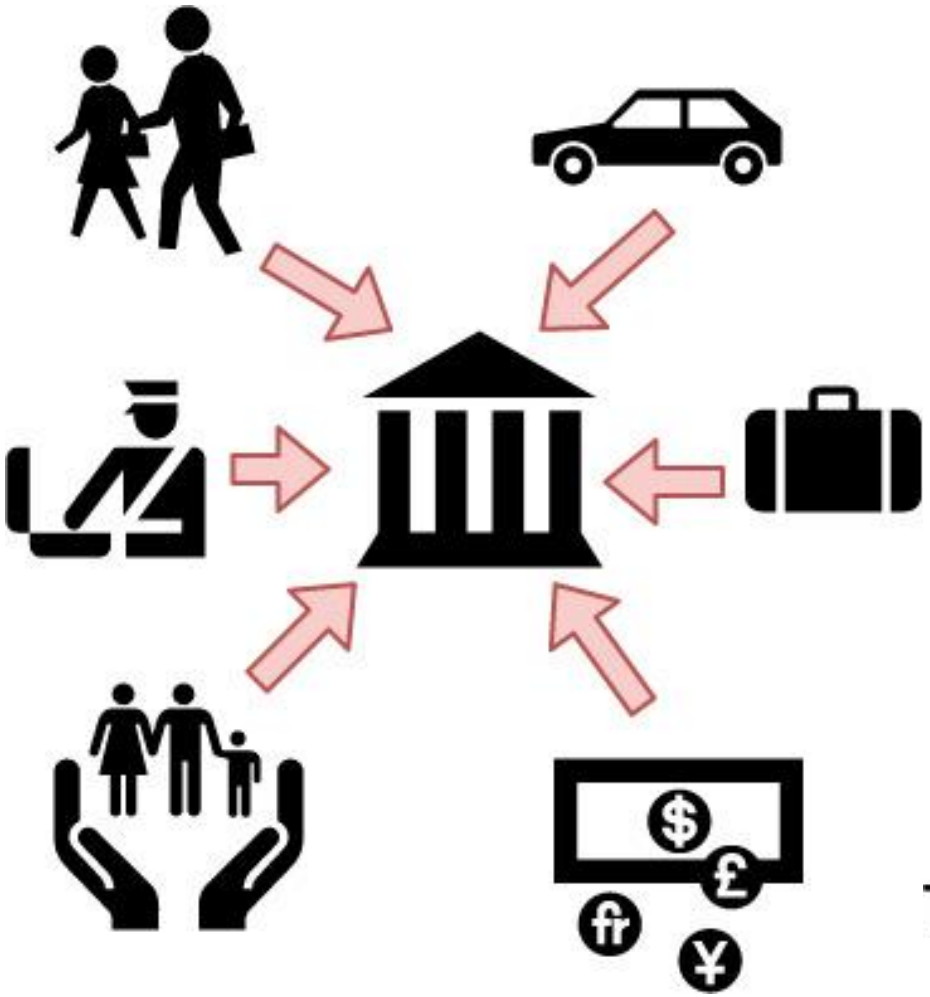
reuse



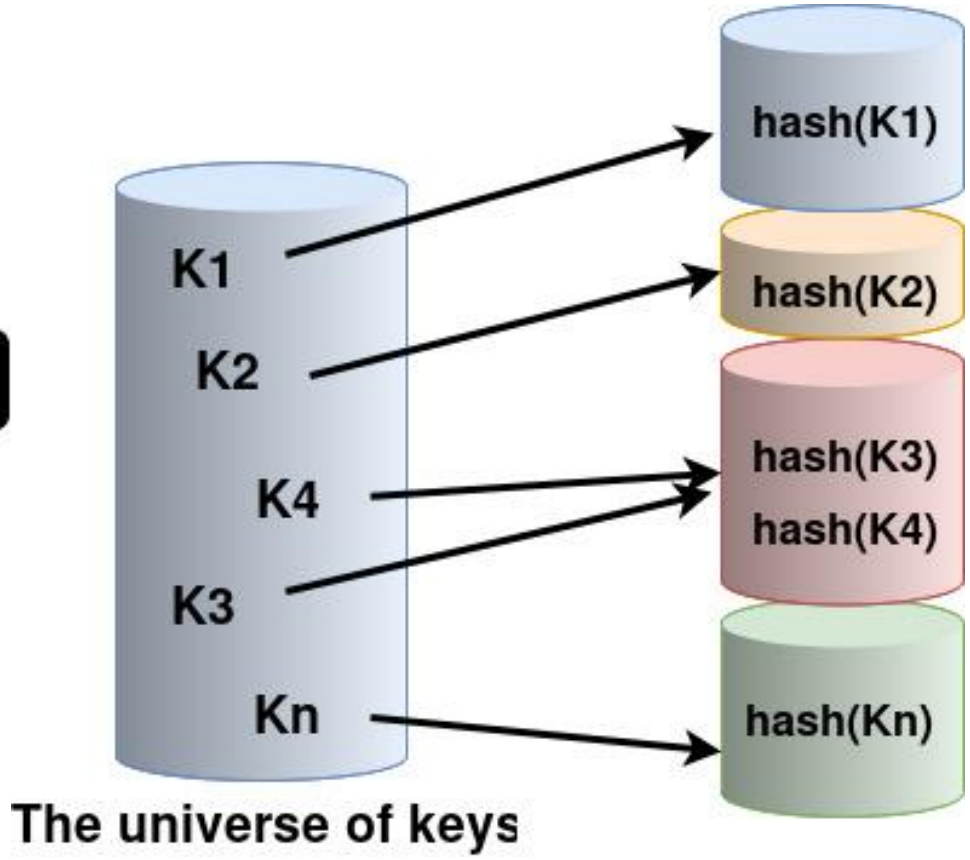
manipulate

profit

Before Distributed Ledgers

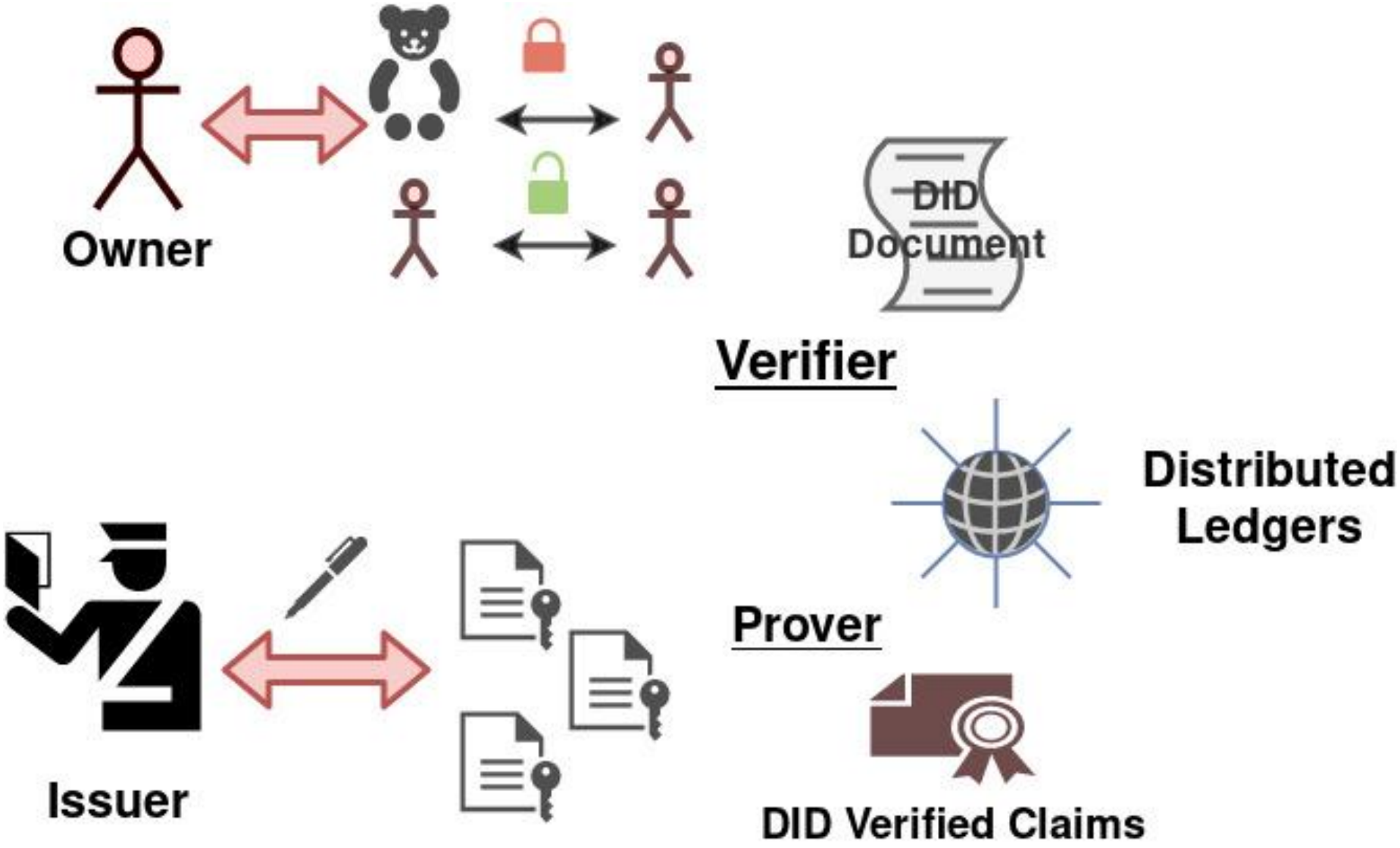


Centralized athority

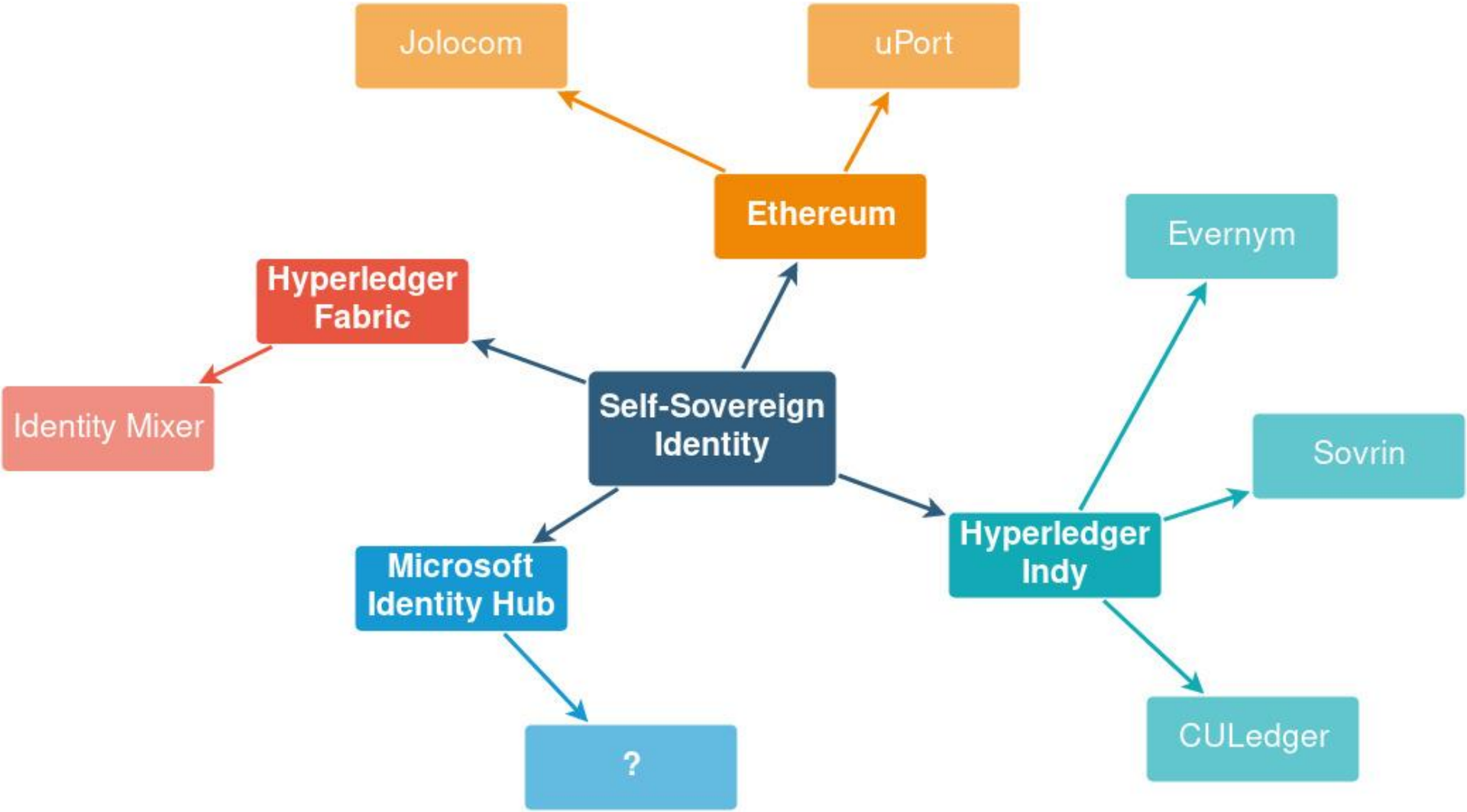


Hash tables

Using Distributed Ledgers



Variety of solutions



Variety of solutions

Solution	Aspect	
	Protocol	Source
Sovrin	Hyperledger Indy	Open-source
Civic	Ethereum	Closed-source
uPort	Ethereum	Open-source
Jolocom	Ethereum	Open-source
Veres one	Custom	Open-source
Ontology	Custom	Open-source
Remme	Hyperledger Sawtooth	Open-source

Some problems

In Ethereum and Bitcoin:

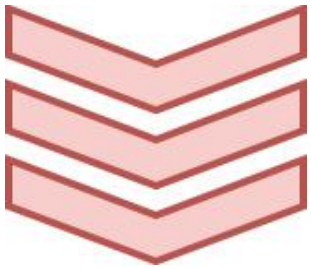
- transaction cost for the creation of DID record;
- transaction processing time is a lottery;

Some problems

IOTA example: Snapshot mechanism

+ allows to perform transactions on a public network really fast and free of charge

- allows full nodes to remove a transaction history



public key registry would be simply eliminated

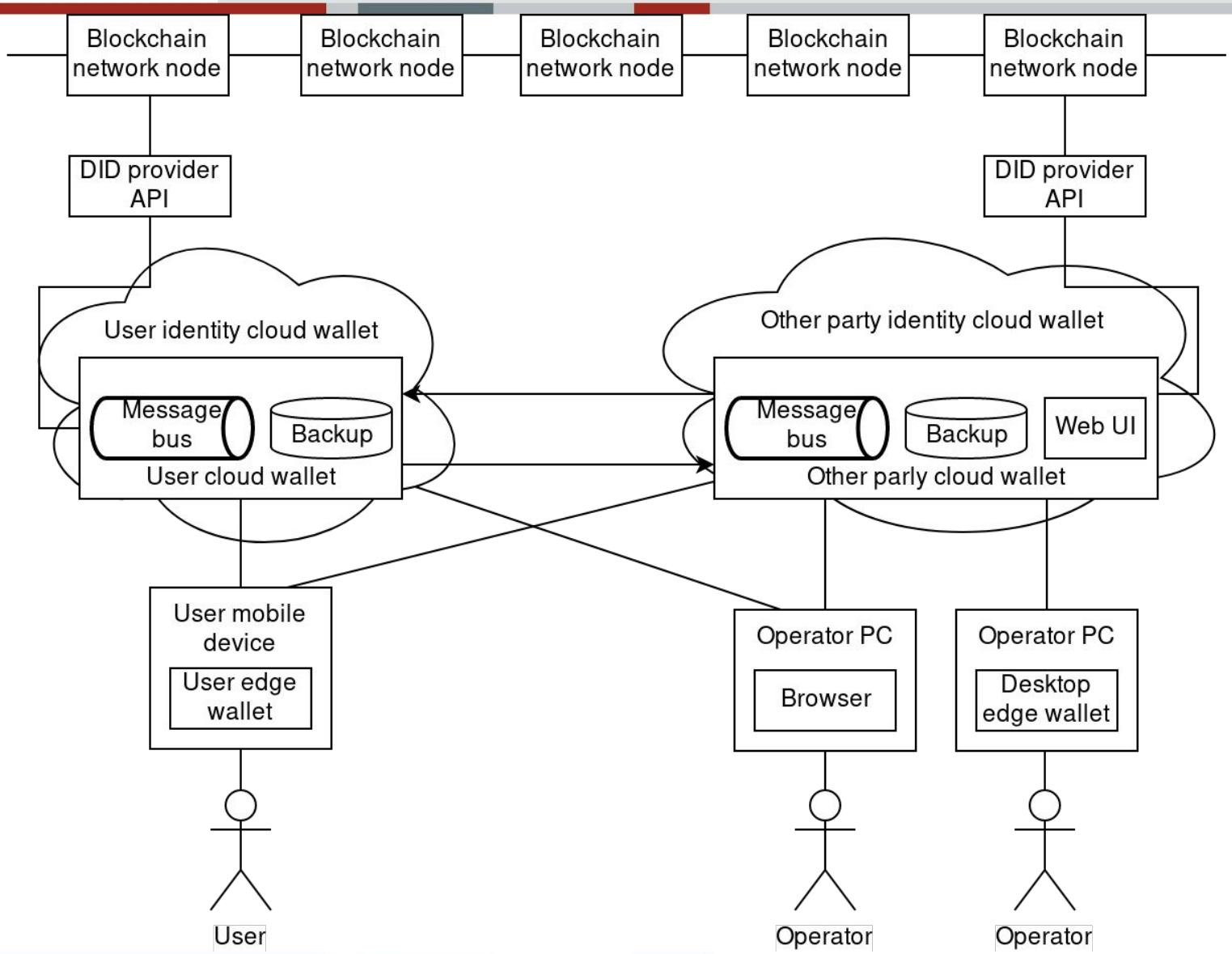
DIDs

DID - Decentralized Identifies

The W3C Community Group says:

“DIDs are the new type of identifiers for verifiable “self-sovereign” digital identity”

General scheme



DID Components

Functionality:

- Create
- Read
- Verify
- Update
- Deactivate

DID

Options:

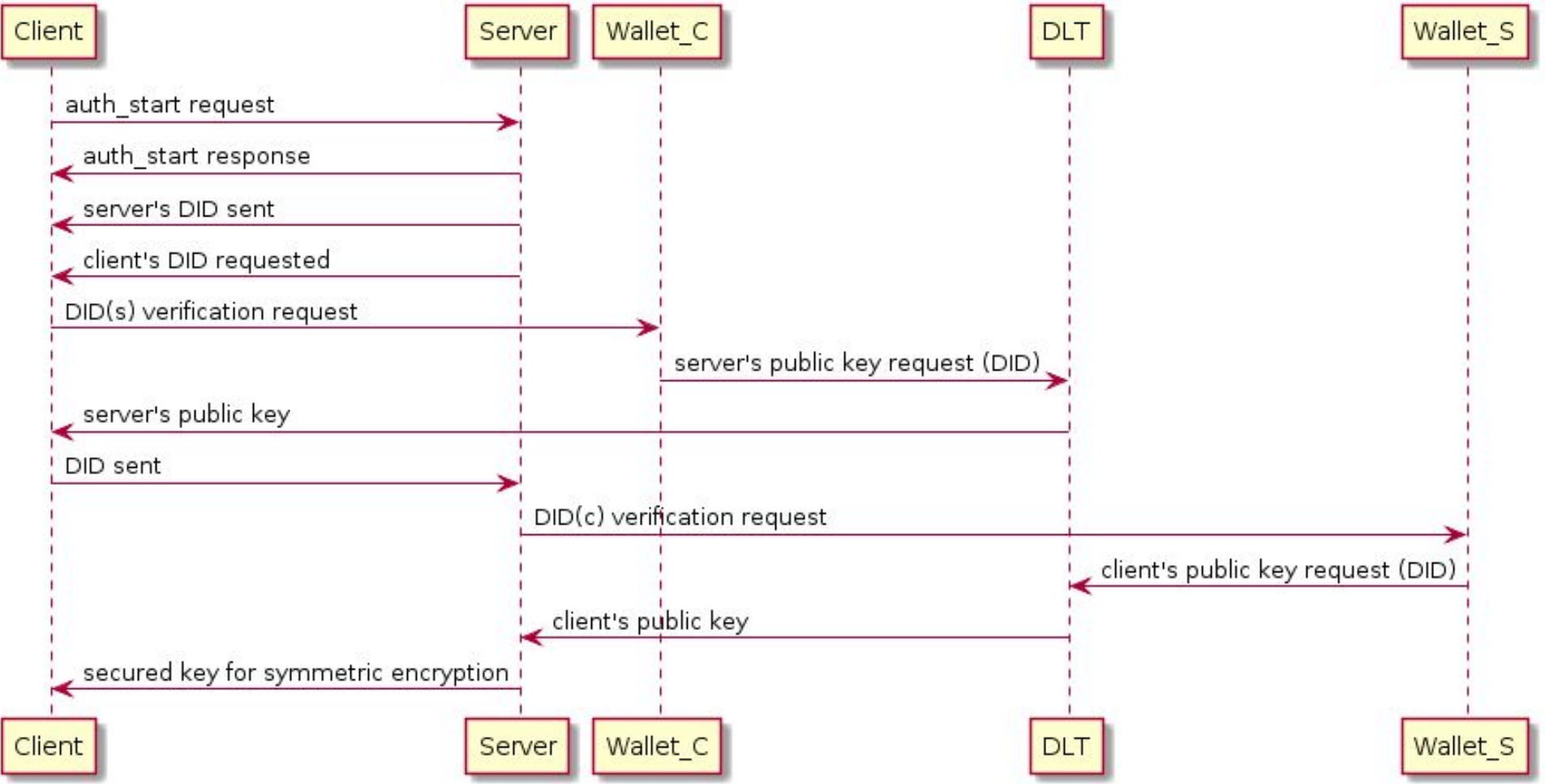
- Context
- DID Subject
- Public Keys
- Authentication
- Delegation
- Service endpoints
- Proof
- Extensibility

Wallet

List of basic functions:

- store user data and key pairs securely, so that no one else would be able to access them.
- be able to find, access and store public keys of another users by their DIDs.
- provide a way to encrypt, decrypt, sign and check signature.
- be able to receive messages from other wallets.

Authentication protocol

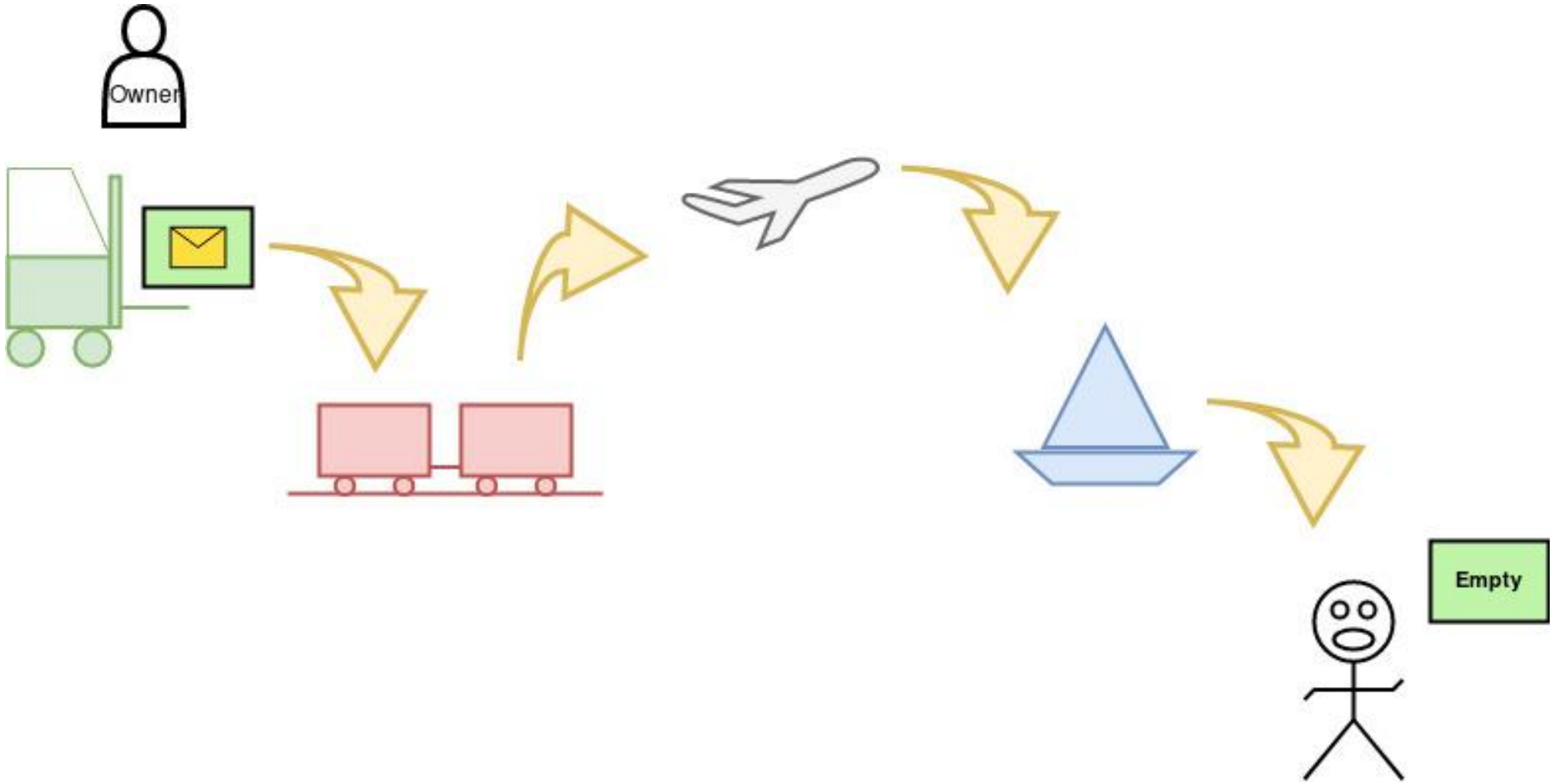


Cases for DIDs

1. **for IoT (Chainbox project)**

2. **for Expert Systems (Experts Ledger project)**

1 - SSI in Logistic Chain



1 - SSI in Logistic Chain

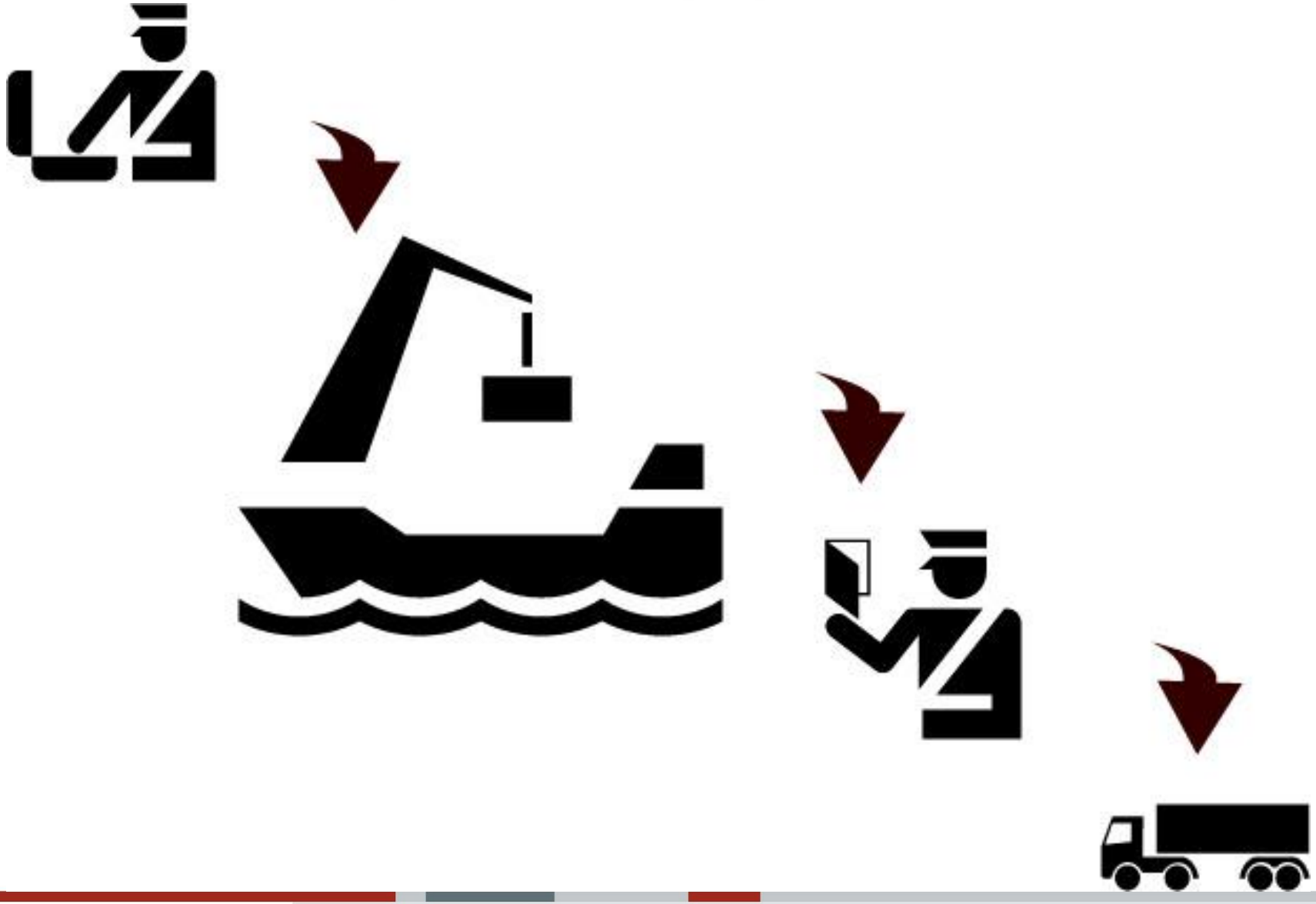
“Chainbox” SSI :

- the identity number;
- the weight;
- the size;
- the owner;
- other properties.

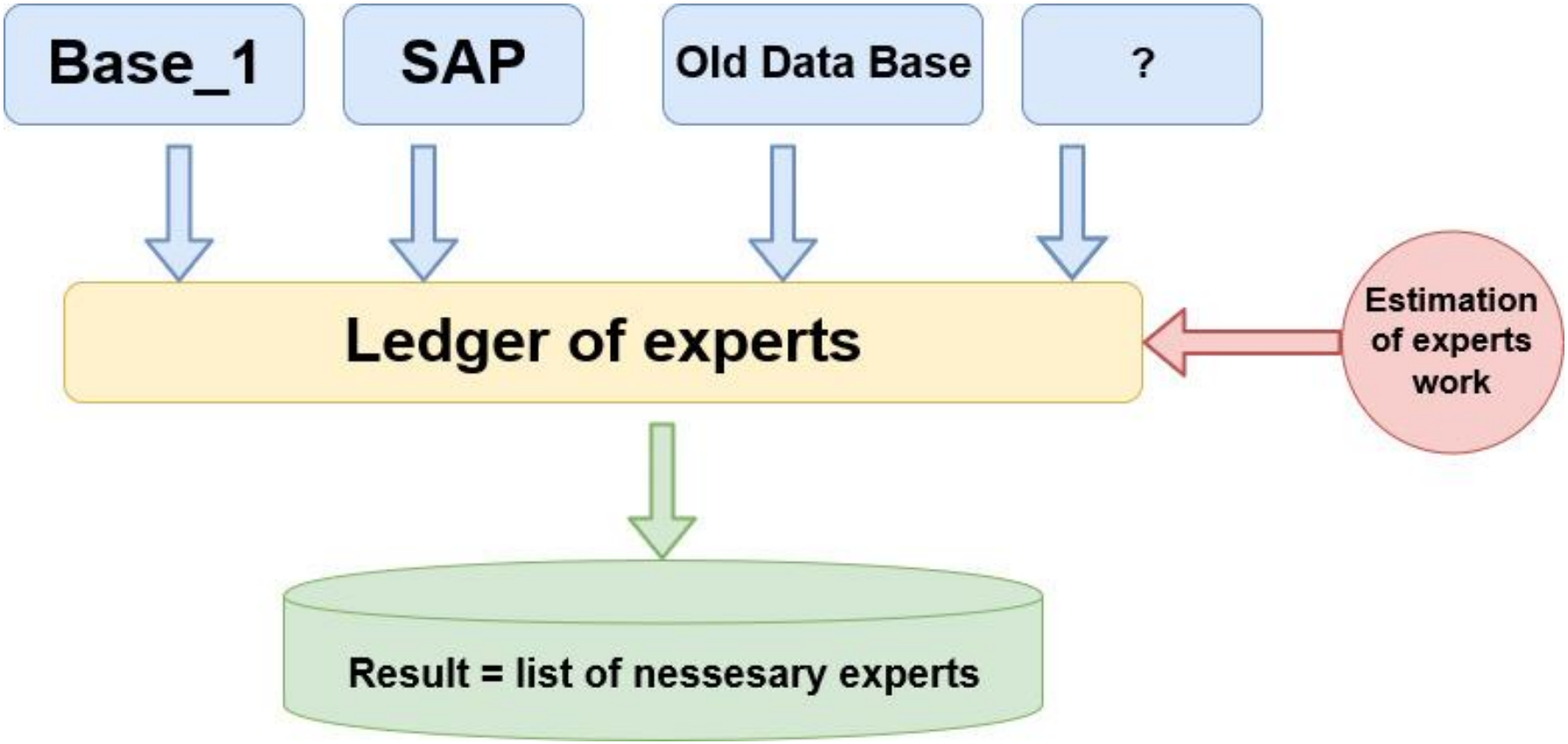
“Chainbox” IoT:

- GPS coordinates;
- temperature;
- humidity;
- shaking;
- etc.

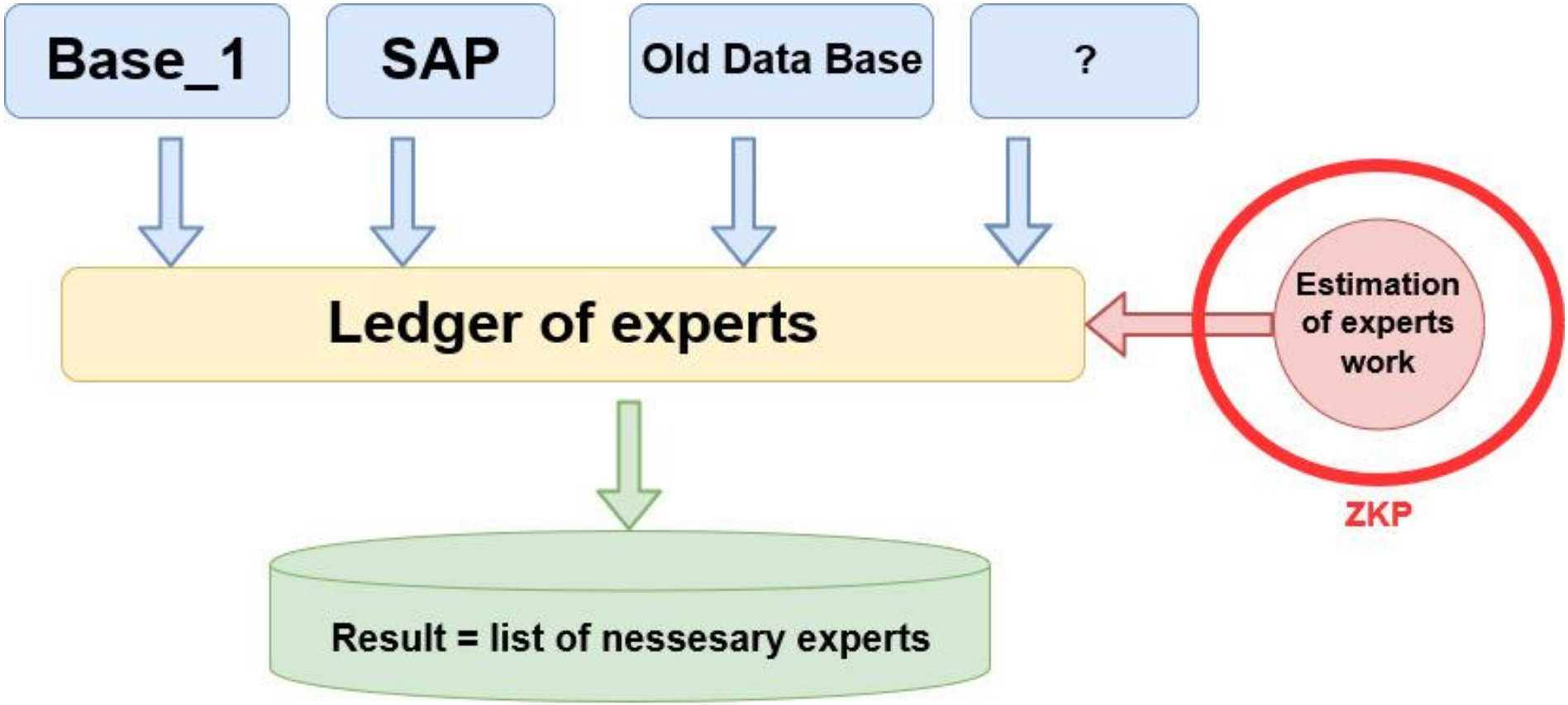
1 - SSI in Logistic Chain



2 - Experts Ledger project



2 - Experts Ledger project



Reasons for ZKP

We need:

- Anonymization;
- Opportunity to give the right of control to another entity.

Zero-Knowledge Proof

Anonymization

Comparison of anonymization technology:

Main aspects	**Technology**	
	Idemix	**U-Prove**
Signature scheme	Camenisch-Lysyanskaya's signature	Brand's signature
Implementation instantiation	**Elliptic curves**	**Standard subgroup**
Untraceability and unlinkability	Has both	Untraceable, but linkable between presentations
Revocation, Inspectation	Shared	Shared
Languages	Java	C#

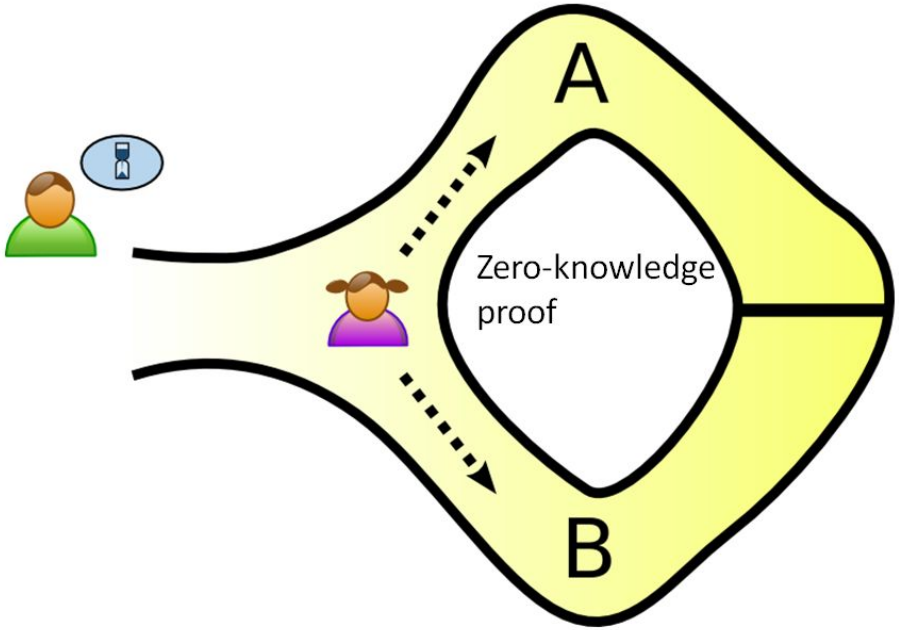
ZK-STARK*

Y = f(x)

Post Quantum Cryptography Algorithms

Merkle hash-tree signatures

Secure



*Zero-Knowledge Scalable Transparent ARguments of Knowledge

ZK-STARK

\+

- Resistance to hacking by quantum computers
- Relatively rapid generation of evidence
- Relatively quick proof check
- No toxic waste

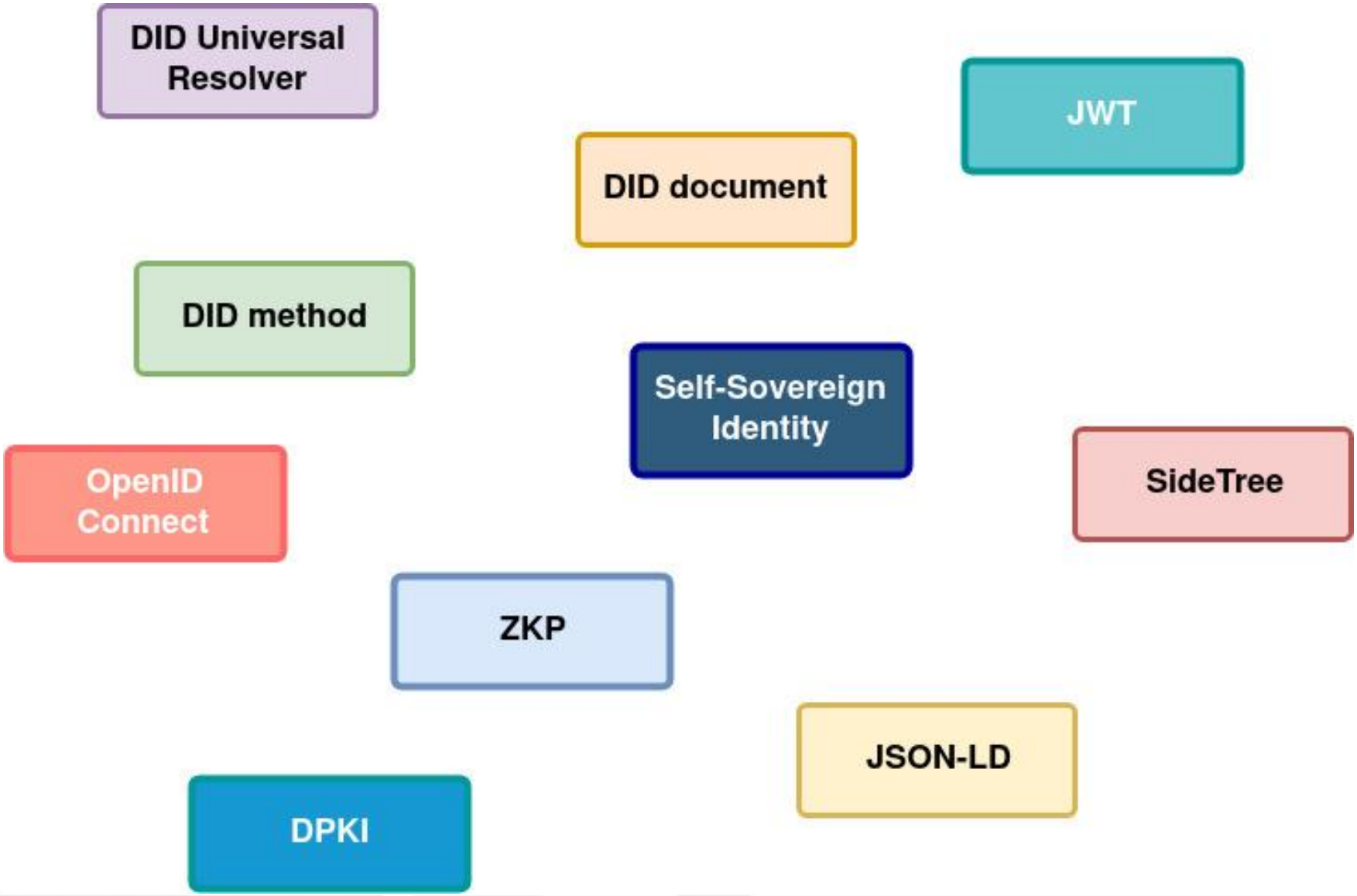
\-

- The complexity of the technology
- Large proof size

But not yet finished!

Conclusion

- We have tried to consider the main key points of the SSI technology;
- Discussed difficulties in modern distributed application;
- We have tried to describe the most important problems that modern developers of DIDs and ZKP have to face;
- In the future, we plan to expand the use of the opportunities described here to other cases;
- Work is in progress.


DID Universal Resolver
JWT
DID document
DID method
Self-Sovereign Identity
OpenID Connect
SideTree
ZKP
JSON-LD
DPKI

St Petersburg University
www.spbu.ru

Thank you for your attention!

Zero-Knowledge Proof in Self-Sovereign Identity

Nataliia Kulabukhova