Towards a self-sovereign identity management in the IoT environement

- **Lydia Ouaili (PhD student)**, Samia Bouzefrane, Elena Kornyshova, Pierre Paradinas

- Conservatoire National des Arts et Métiers, Paris, France
- Trasna Solutions, Marseille, France

Plan

Introduction: Evolution of the Internet identity

Context: The decentralized identity model (Self-sovereign identity:SSI)

Concepts: Blockchain technology and decentralization

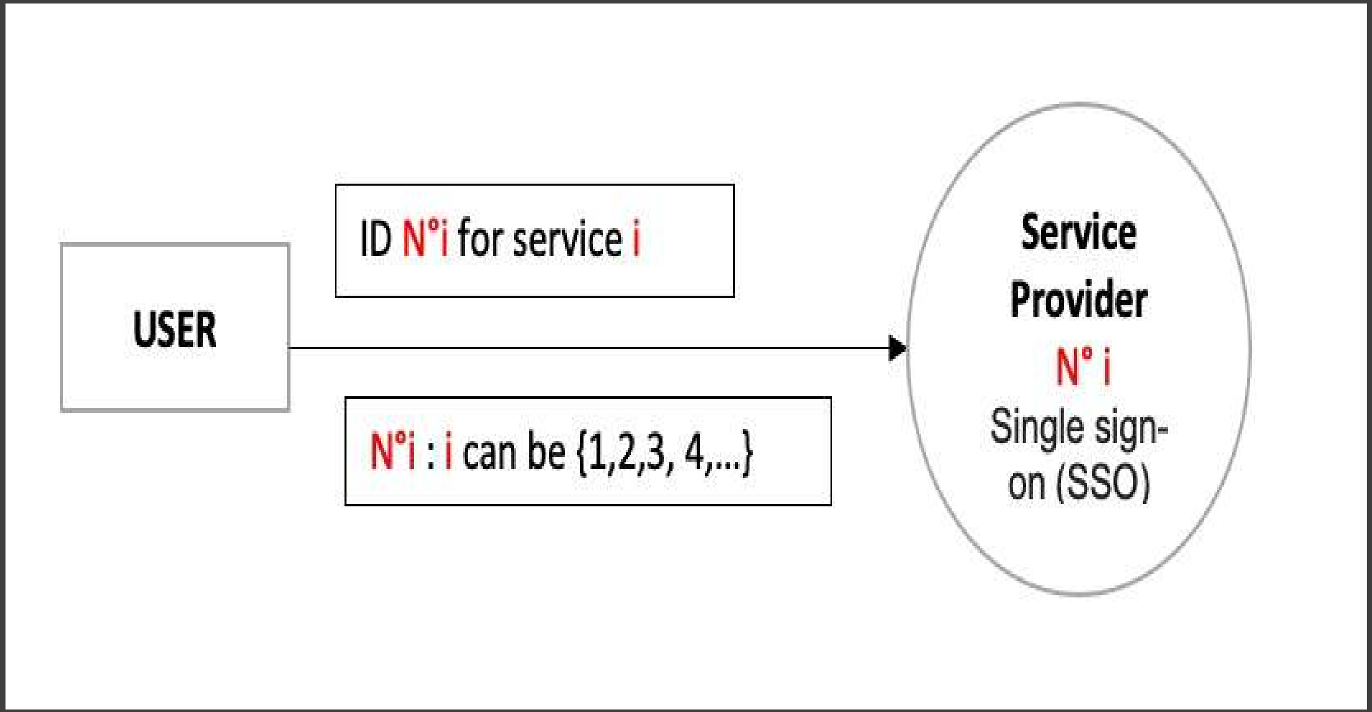
Open issues: Self-Sovereign identity and IoT

The centralized identity model

Remembering and managing all the usernames and passwords

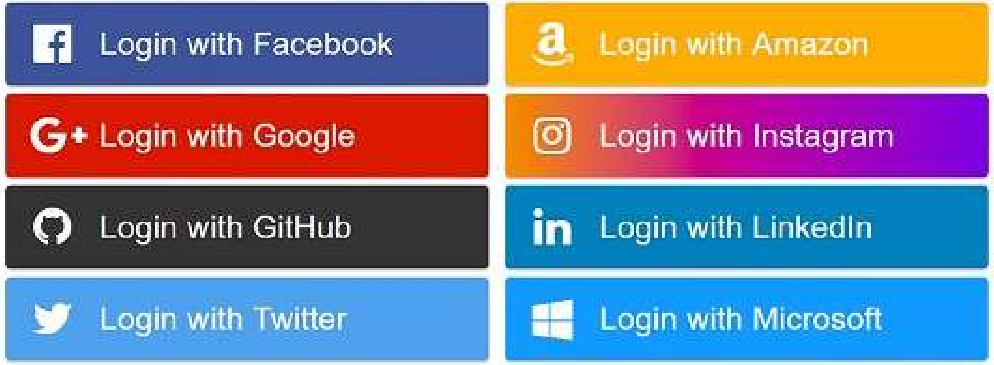
Every site enforces its own security and privacy policies

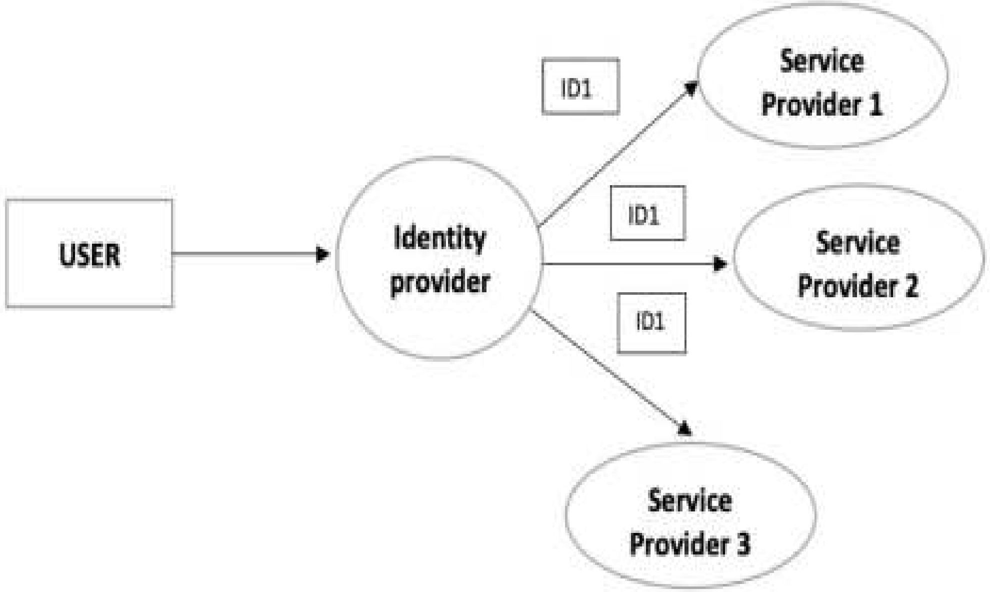
Centralized databases of personal data (data breaches)



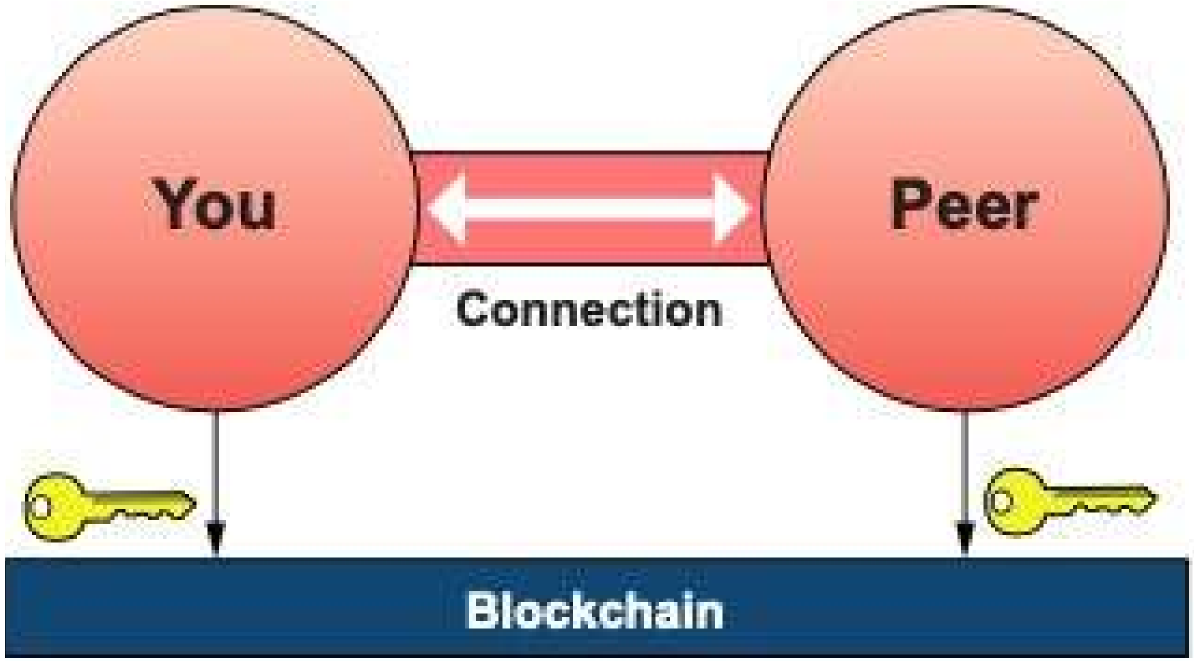
The federated identity model

There isn’t one identity provider that works with all sites, services, and apps.
IDP can surveil a user’s login activity across multiple sites.





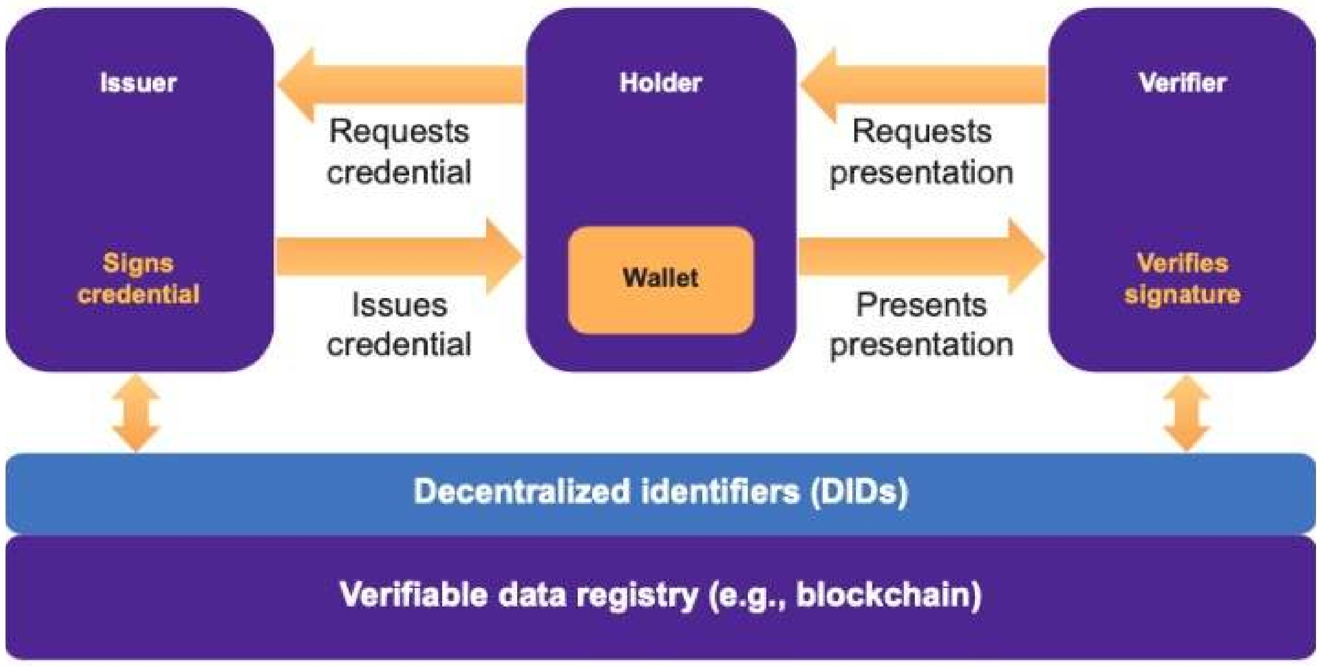
The decentralized identity model: SSI



- Extracted from : Preukschat, A., & Reed, D. (2021). *Self-sovereign identity*. Manning Publications.

Decentralized IdMSs (Self-Sovereign Identity)

The next standard for internet communication

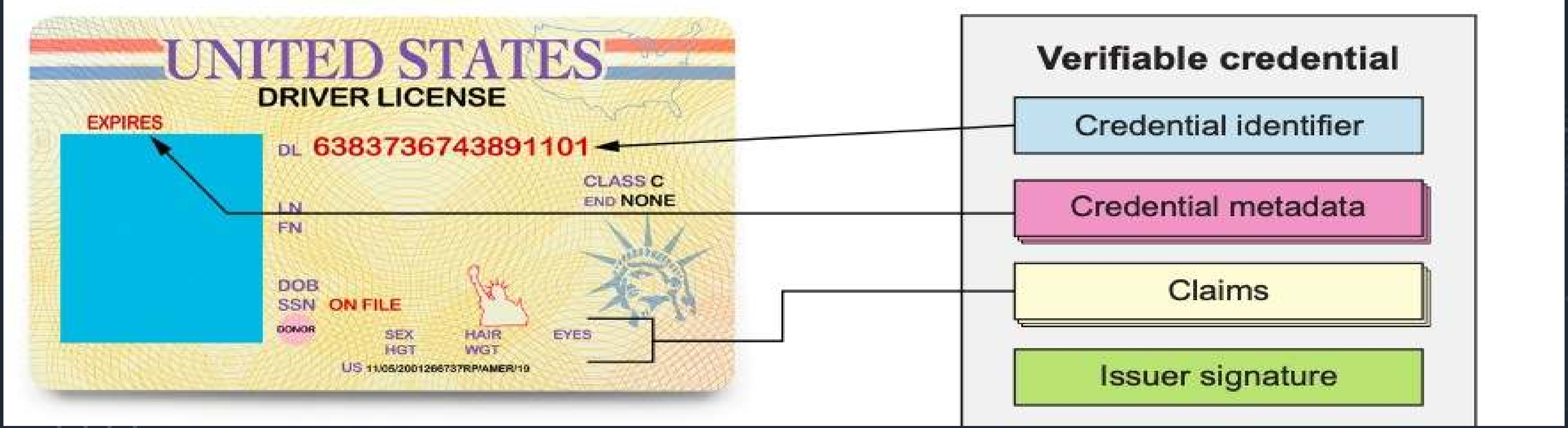


Extracted from : Preukschat, A., & Reed, D. (2021). *Self-sovereign identity*. Manning Publications.

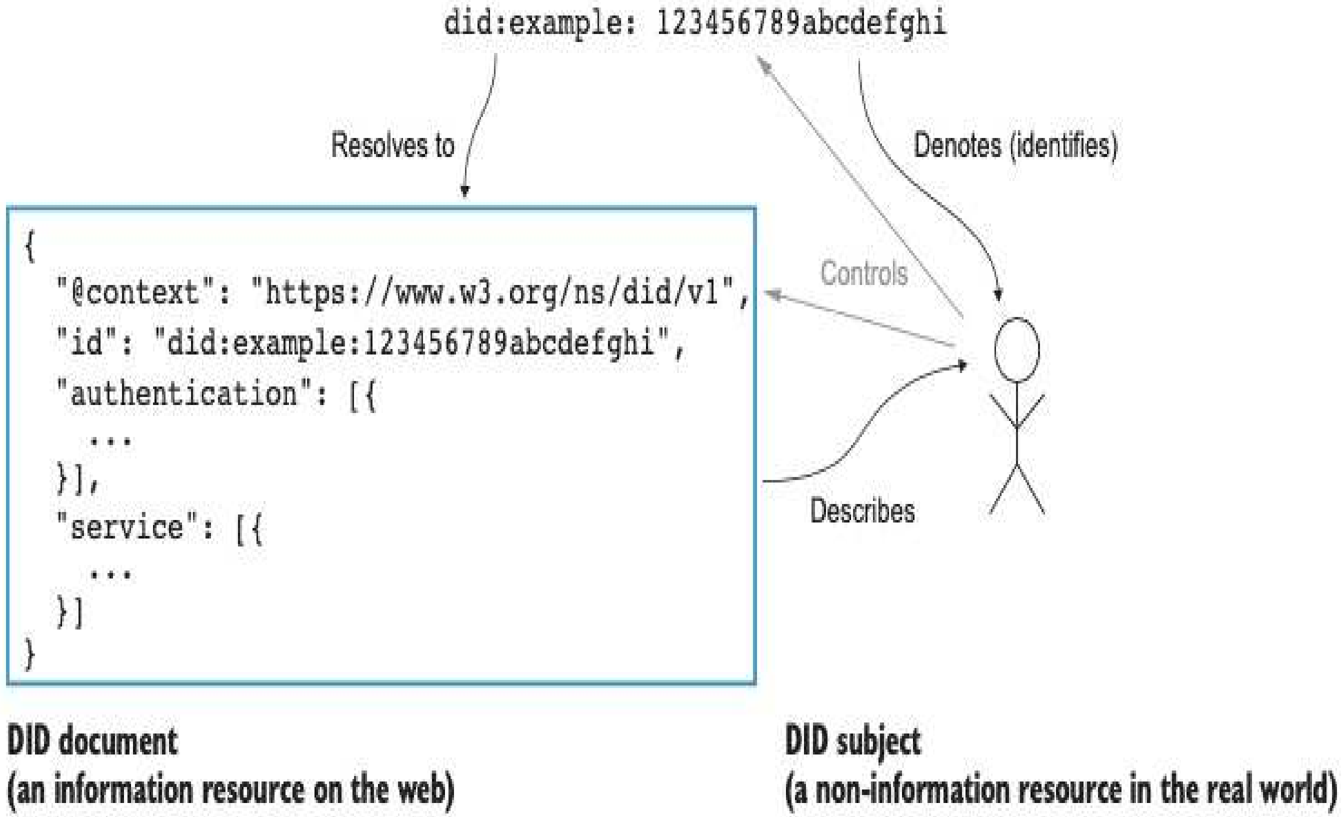
- Verifiable credentials (aka digital credentials)
- The trust triangle: issuers, holders, and verifiers
- Decentralized identifiers (DIDs)
- Blockchains and other verifiable data registries

Verifiable Credentials (VCs)

- Verifiable Credentials Data Model (W3C Recommendation)
- https://www.w3.org/TR/vc-data-model/
- Zero-knowledge proof is a cryptographic method where an entity can prove to another entity that they know a certain value without disclosing the actual value



Decentralized Identifiers (DIDs)



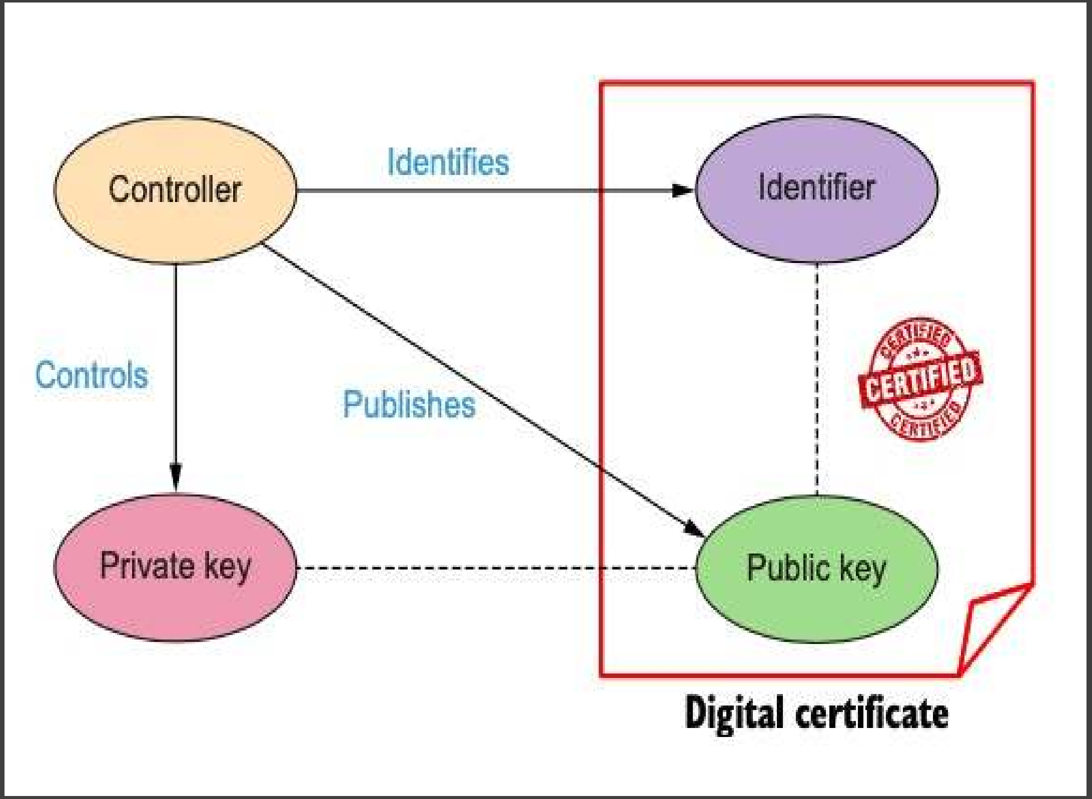
```
did:example: 123456789abcdefghi
```

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    ...
  }],
  "service": [{
    ...
  }]
}
```

Resolves to
Denotes (identifies)
Controls
Describes
DID document
(an information resource on the web)
DID subject
(a non-information resource in the real world)

- You will use it not juste for authentication, but for exchange Verifiable Credentials
- No central registration authority

Why decentralized identity ?
What do we mean by decentralization?



- Access to services
- The problem of Public Key Infrastructure (PKI) :
- *Who digitally signs this digital certificate ?*

•*Trusted third party* (TTP) certificate authority (CA)

Extracted from : Preukschat, A., & Reed, D. (2021). Self-sovereign identity. Manning Publications.

Setting the context :
Self-Sovereign identity is a field which is currently still maturing

1. Academia:

- Analysis and comparison of implementations (decentralization, type of blockchain,…)
- Uses cases
- The necessity of using a blockchain
- Survey research

2. Nonprofit organization and industry :

- W3C : explore the creation, storage, presentation, verification, and user control of credentials.
- Open source implementations
- IOTA
- Hyperledger (Open Source Blockchain Technologies), uPort,….

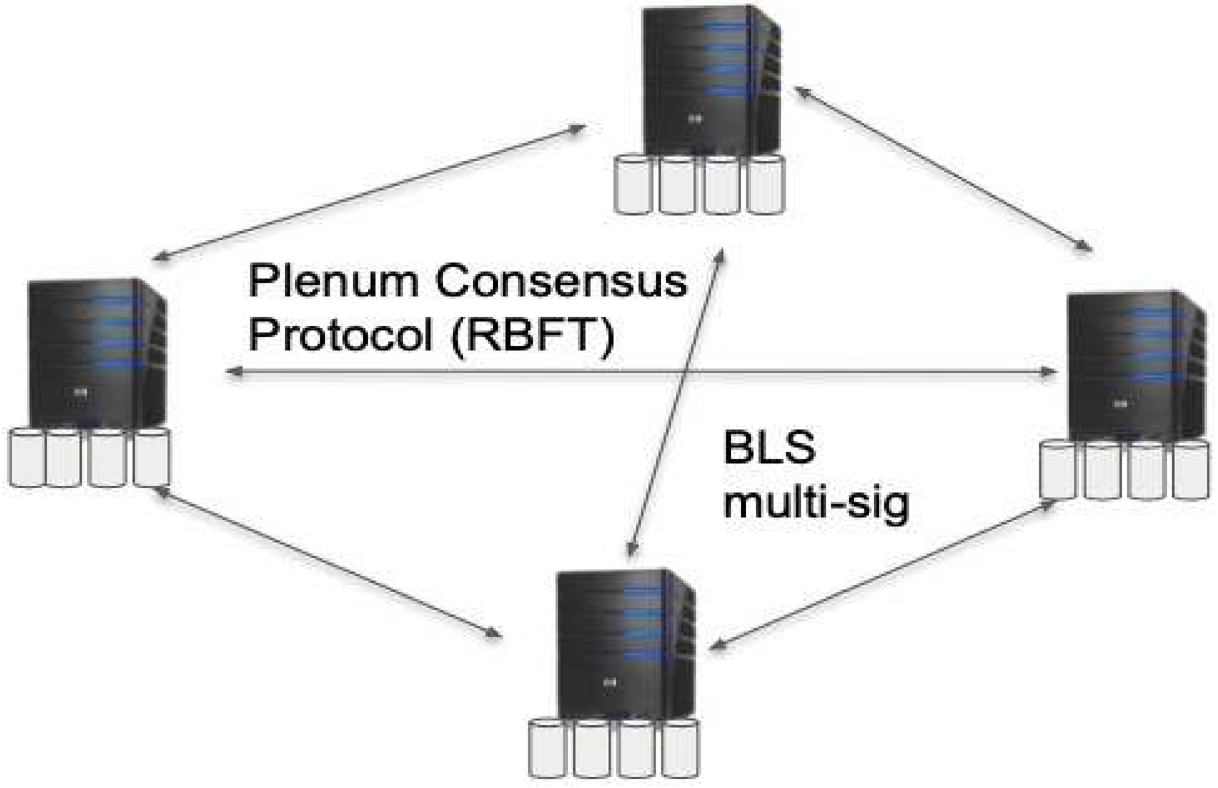
Some research axes in Self-Sovereign identity:

Decentrelization		Conception and use case
Consensus algorithms	**Distributed ledger**	**Software development, application cases, standardization, system diagrams and architectures, modeling.**
- PoW (Proof of Work) - PoS (Proof of Stake) - RBFT (Redundant Byzantine Fault Tolerance) - (PoET) Proof of Elapsed Time…	- Blockchain or not? - Type of blockchain - Permissioned and Permissionless Blockchains - Ethereum, Bitcoin,… - Ripple (XRP) - Tangle	- **W3C** Recommendations - Hyperledger Foundation - Academic research - Industries: IBM, Accenture, J.P. Morgan, Walmart, IOTA,…

How decentralization can be achieved?
An illustrative example:

HYPERLEDGER INDY

- **No private data is written to the Blockchain**
- **Only Public data (such as Issuer's Public Key) is there.**
- **Validators nodes (Handles Writes and Reads and come to consensus)**
- **Each Node replicates all ledgers**



- **Distributed systems:**

Consensus:

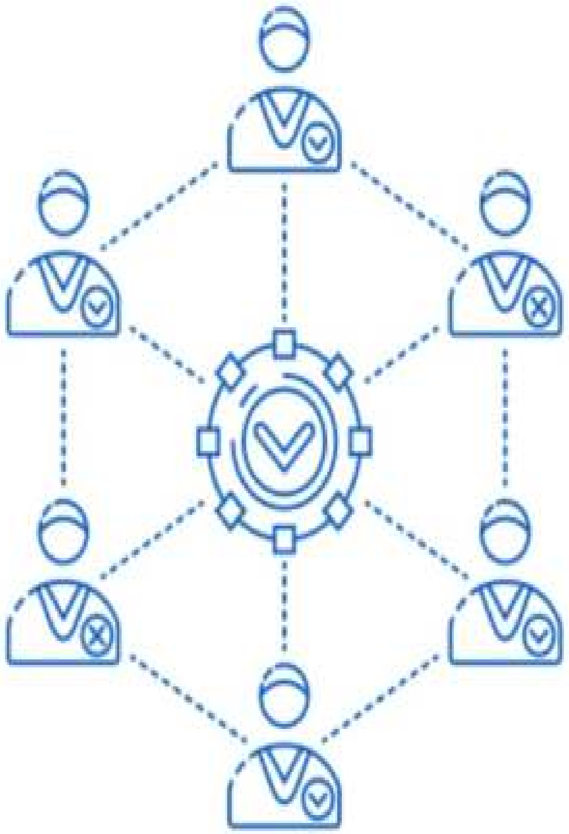
1. Safety/ Consistency
2. Liveness/ availability

A family of state-machine replication protocols :

Byzantine fault-tolerant (BFT) : state-machine replication protocols.

Historically, BFT have been recognized as very difficult to design and implement

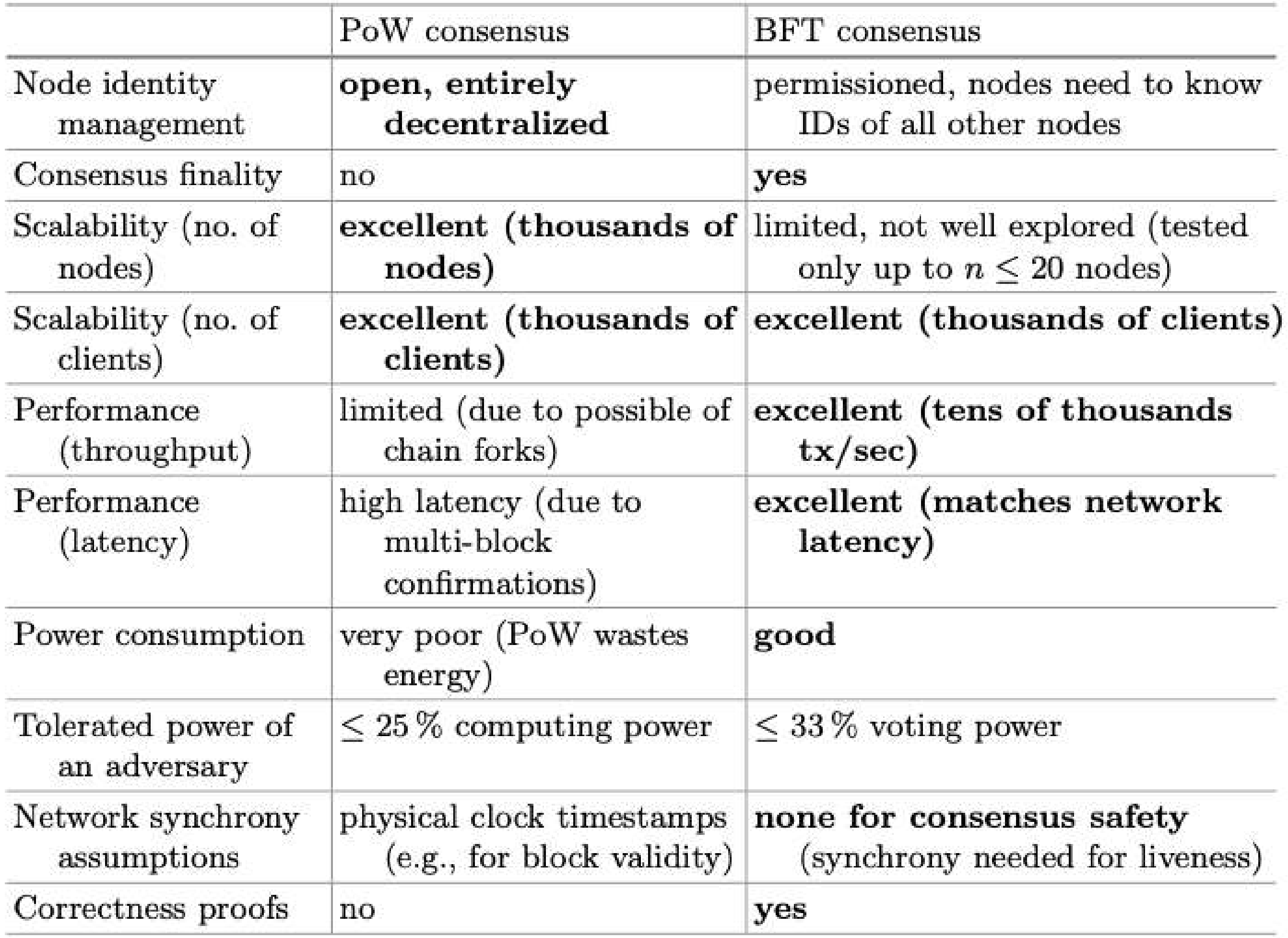
Consensus



- The Byzantine generals problem (Leslie Lamport et all) 1982
- Impossibility of distributed consensus with one faulty (M.J Fischer et all)1985
- Practical Byzantine fault tolerance and proactive recovery . (Castro, M., Liskov, B.) 2002

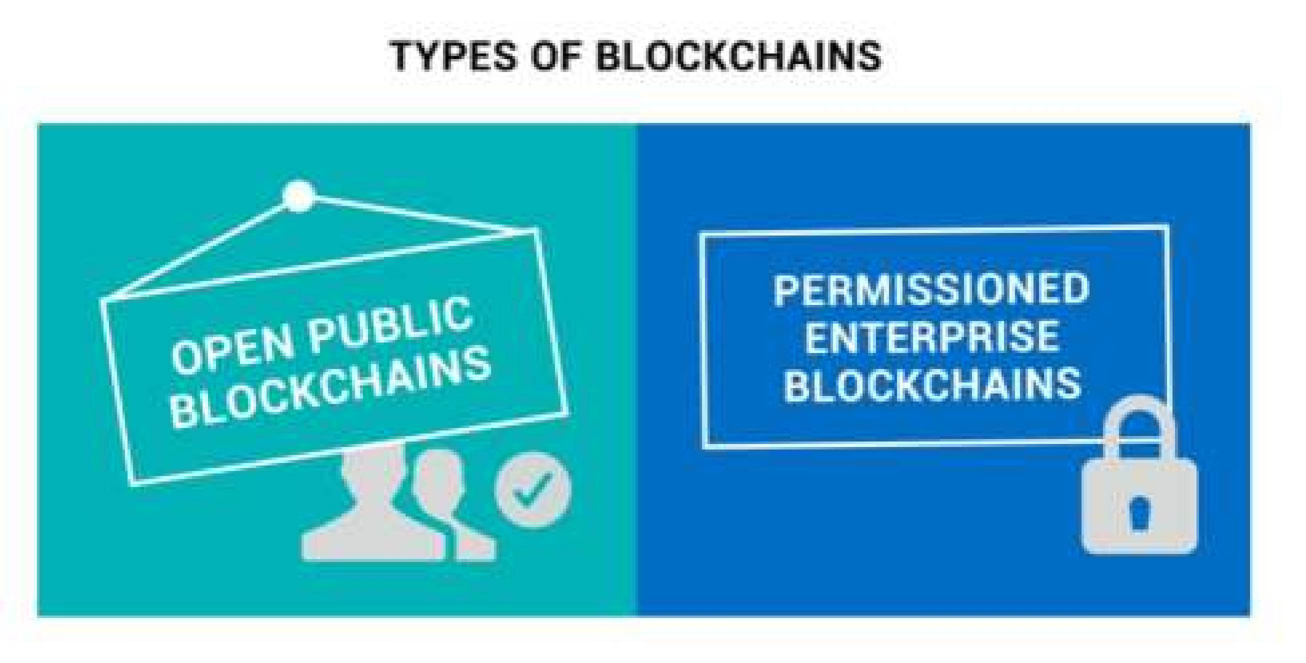
Blockchain and distributed systems

- Extracted from: The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication Marko Vukolic IBM Research, Zurich, Switzerland



	PoW consensus	BFT consensus
Node identity management	**open, entirely decentralized**	permissioned, nodes need to know IDs of all other nodes
Consensus finality	no	**yes**
Scalability (no. of nodes)	**excellent (thousands of nodes)**	limited, not well explored (tested only up to $n \leq 20$ nodes)
Scalability (no. of clients)	**excellent (thousands of clients)**	**excellent (thousands of clients)**
Performance (throughput)	limited (due to possible of chain forks)	**excellent (tens of thousands tx/sec)**
Performance (latency)	high latency (due to multi-block confirmations)	**excellent (matches network latency)**
Power consumption	very poor (PoW wastes energy)	**good**
Tolerated power of an adversary	$\leq 25\,\%$ computing power	$\leq 33\,\%$ voting power
Network synchrony assumptions	physical clock timestamps (e.g., for block validity)	**none for consensus safety** (synchrony needed for liveness)
Correctness proofs	no	**yes**

What type of blockchain for decentralized identity ?

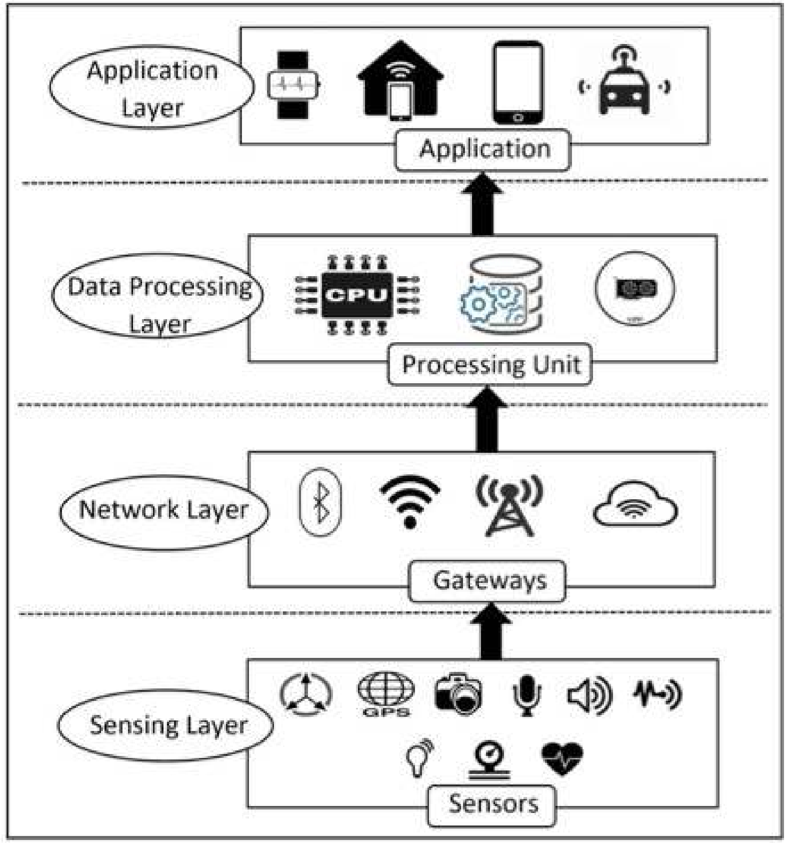


- Permissionless (like Bitcoin or Ethereum)

- Permissioned (like the different Hyperledger blockchain frameworks)
- Hyperldger Indy (Self-Sovereign identity)

Research perspectives in Self-Sovereign identity with IoT

IoT environement



- Top 5 security threats within the IoT sector: (IBM)

1. Secure constrained devices
2. Authorize and authenticate devices
3. Manage device updates
4. Secure communication
5. Ensure data privacy and integrity

How can SSI help IoT ?

Main research areas

- How to assign an identity to IoT devices?
- i.e. use already existing concepts and propose identities adapted to a use case (DID, DIDdocument, Verifiable Credential,...).

Decentralization of SSI in an IoT environment:

- Distributed consensus algorithms and distributed registers (scalability, latency)
- Storage capacity and computational performance

Self-Sovereign Identity
Is a BIG TOPIC which depends mainly on :

1. Cryptography:

- DID and Verifiable Credentiels
- Camenisch-Lysyanskaya Zero-Knowledge Proof system…
- See (W3C recommandations)

2. Distributed Systems for Decentralization:

- Distributed ledger technology
- Consensus algorithms

Communication and Network:

- peer-to-peer (P2P)

3. Conceptualization, software development, standards and use cases:

- W3C recommandations
- Bitcoin
- Ethereum
- Hyperledger
- IOTA

Open issues and work in progress :

1. Captured Challenges of incorporating SSI in IoT

- Not all types of blockchain are capable of serving IoT devices' needs.
- Proof-of-Work consensus algorithms that are computationally expensive high bandwidth overheads and delays
- The alternative is to utilize a permissioned blockchain for a possible IoT IdMS but they are recognized as non-scalable
- In industrial IoT, real time constraints must be respected
- Constrained devices; Asymmetric Cryptography; Communication overhead; DID Resolution.

2. Propose a scalable consensus algorithm

Thank you for your attention