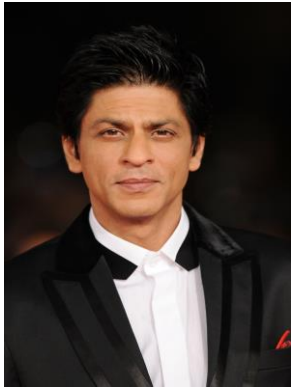
Decentralized Identity Management using Blockchain

Group: Shawal Khalid, Nikhil Ram, Ashish Aggarwal, Srujan Vithalani

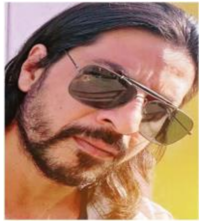
Motivation

Over the last 25 years, advertising-based business models, lack of consumer awareness, and weak privacy legislation have enabled service providers to capture massive amounts of private information.

- ❖ 2017 Equifax breach exposed the private and personally identifying information of more than **140 million** American consumers.
- ❖ Facebook/Cambridge Analytica scandal revealed that the private records of more than **87 million** Facebook users
- ❖ One spammer in India was responsible for **202 million** scam calls in 2021, which works out at 27,000 fraud attempts per hour.
- ❖ Yahoo 2013 - **3 billion** user accounts exposed



original



theft

impersonation

fake

Research Problem

- Study of traditional systems.
- Literature review of system which curbs issues in traditional systems.
- Present a few enhancements which we think are the most secure.
- Discuss security issues in these enhancements.
- Compare and contrast offerings in the market.

Traditional Systems

- Physical documents given to officials or representatives.
- No visibility to document safekeeping or shredding.
- Loose and unsecure means of acceptable document sharing
  - “pls send on *everyonecanthissee* email”,
  - “pls whatsapp”,
  - “can you xerox from this shop that has 1000 visitors daily”
- No visibility if company’s database is still using “*admin, admin”* as the credentials.

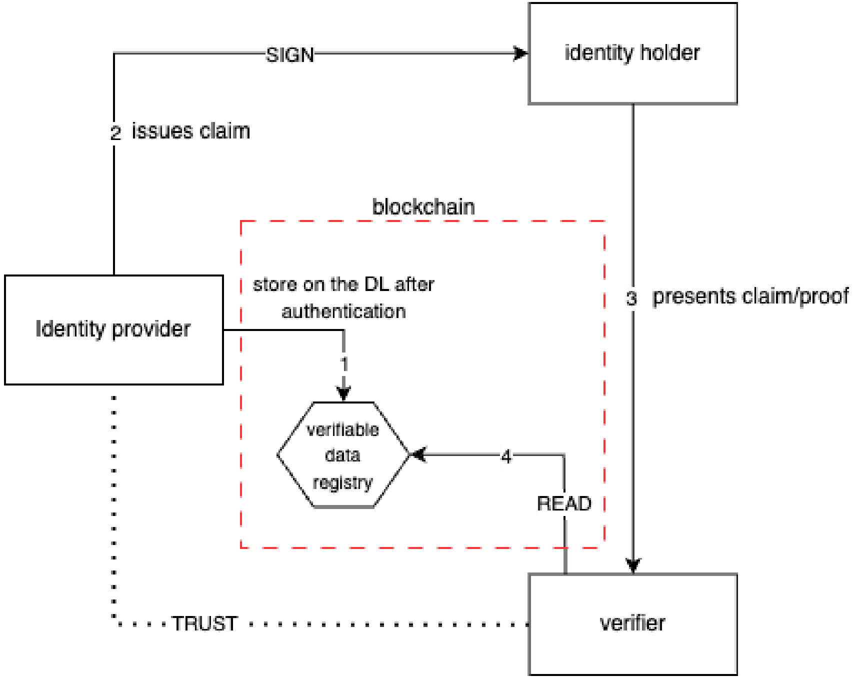
Outcomes?

- “you have won $1M in lottery, reply to avail”
- “Hi we are from the homeland security, your documents are missing”
- “5000$ daily income, Apply now!”

Self Sovereign Model (SSI)

Properties

- allows users to have full control over the credentials they hold and it's usage.
- users have the flexibility to store and use the digital wallet at their discretion
- permits users to disclose their personal information at their own discretion.
- Decentralization of control
- Security

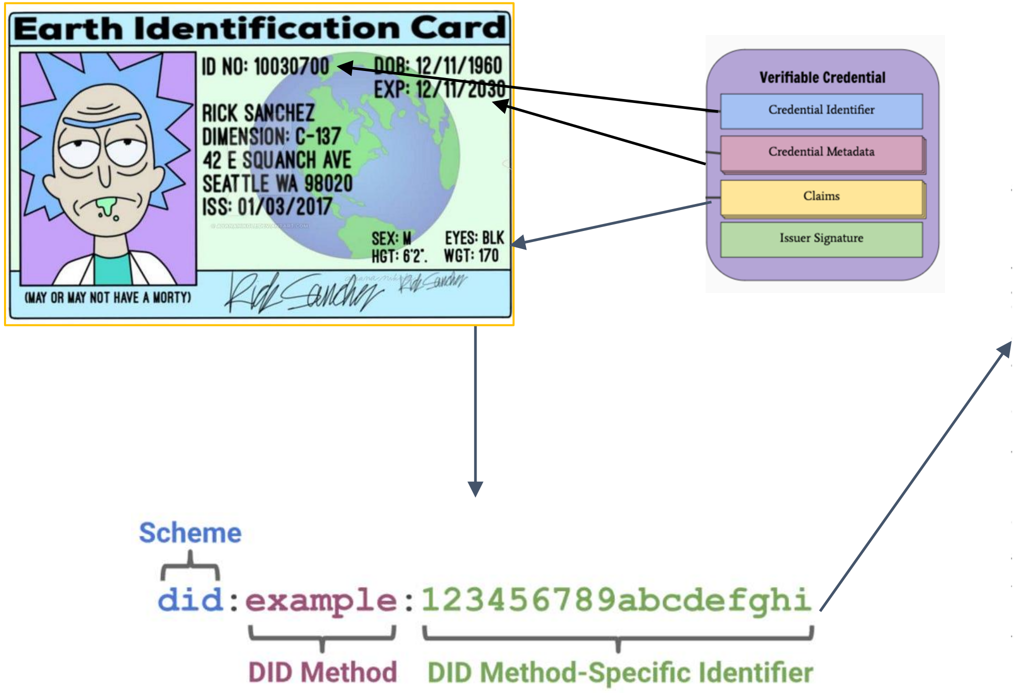


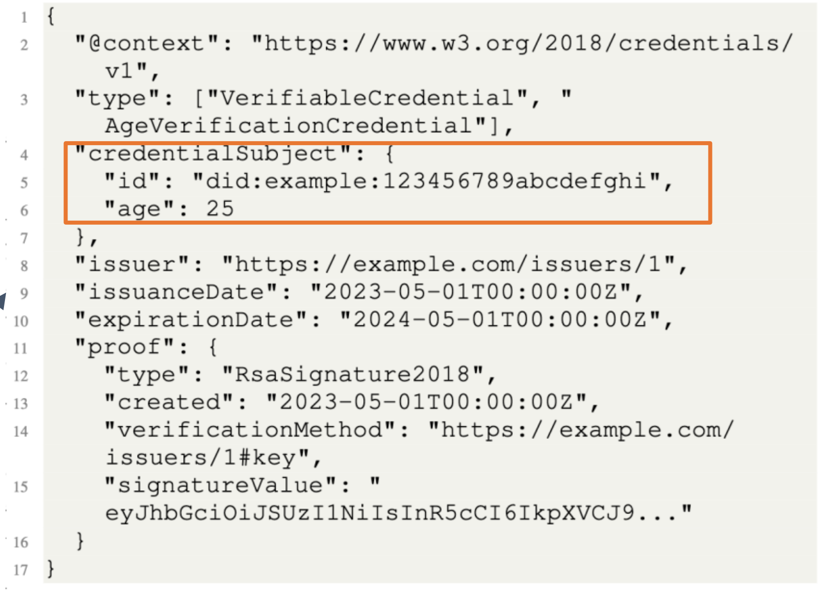
SSI - System Model

VCs and DIDs form the foundation of the SSI.

- ❖ Verifiable Credentials (VCs): Cryptographically secure, machine-readable, & tamper-resistant digitized alternative to physical, realworld credentials such as a passport, national ID card, or driving license.
- ❖ Decentralized Identifiers (DIDs): Unique identifiers, self-generated by individuals or organizations, Linked to VCs and used to establish a verifiable link between an individual and their personal data.

SSI - System Model

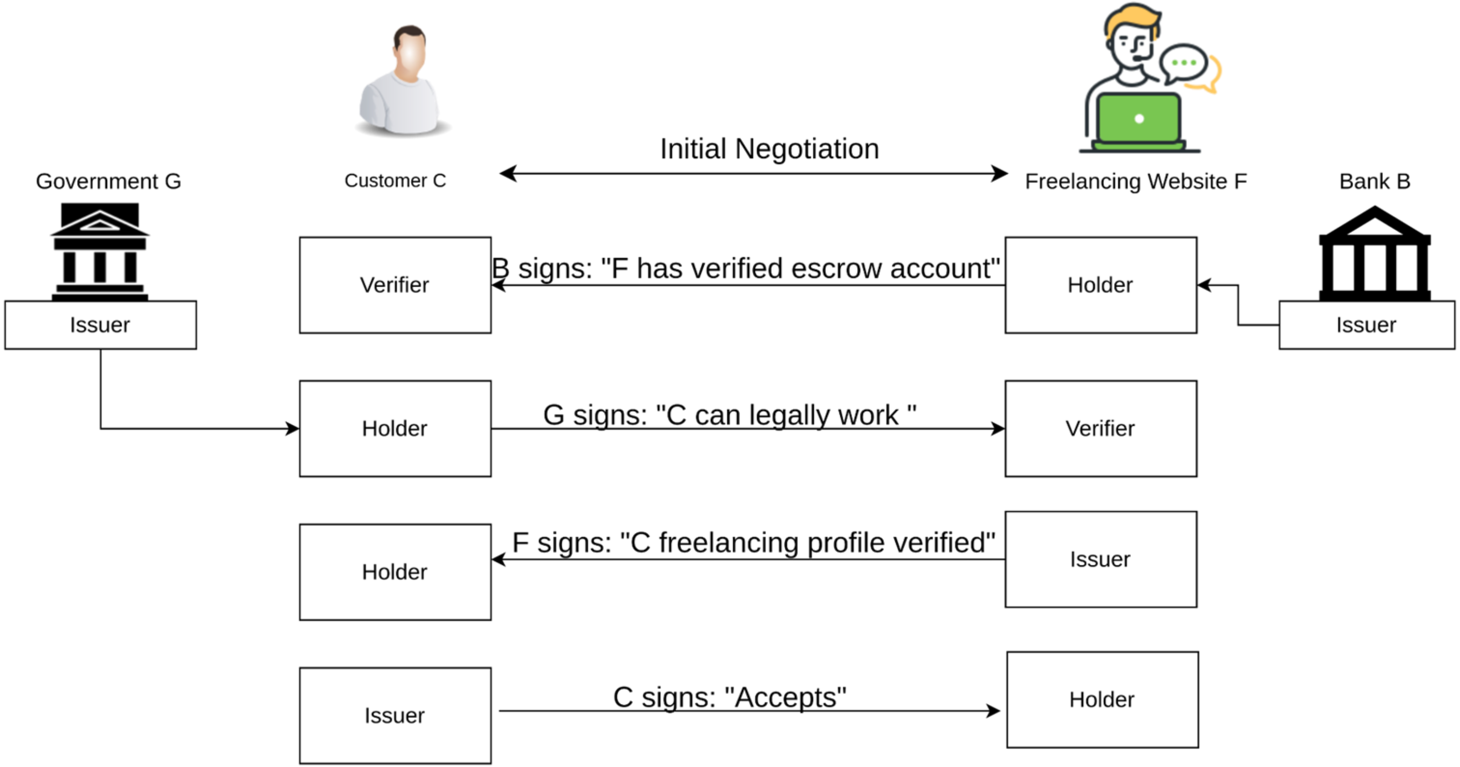




```
{
  "@context": "https://www.w3.org/2018/credentials/
    v1",
  "type": ["VerifiableCredential", "
    AgeVerificationCredential"],
  "credentialSubject": {
    "id": "did:example:123456789abcdefghi",
    "age": 25
  },
  "issuer": "https://example.com/issuers/1",
  "issuanceDate": "2023-05-01T00:00:00Z",
  "expirationDate": "2024-05-01T00:00:00Z",
  "proof": {
    "type": "RsaSignature2018",
    "created": "2023-05-01T00:00:00Z",
    "verificationMethod": "https://example.com/
    issuers/1#key",
    "signatureValue": "
    eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9..."
  }
}
```

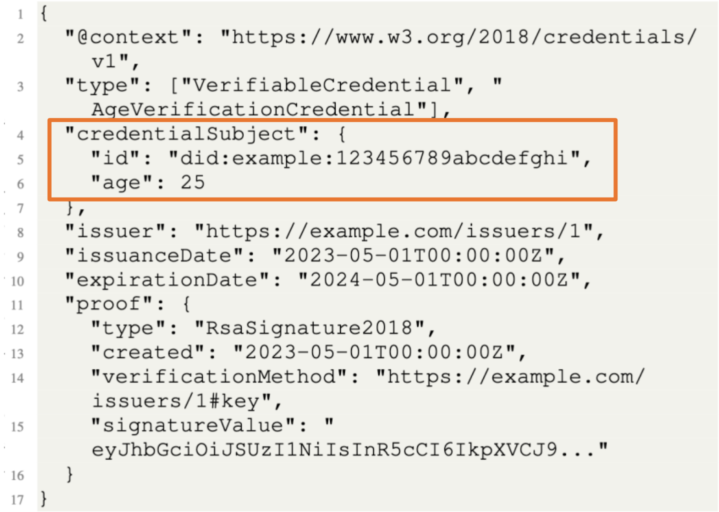
Verifiable Credential

SSI - Real life Application

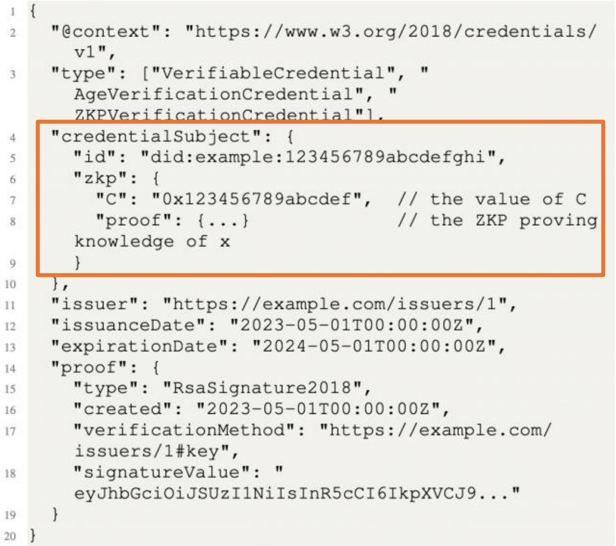


Secure SSI - System Model

- Different types of implementations allow us to control what data we send to the verifier.
- How can we hide **all** our personal data, even the metadata?



```
{
  "@context": "https://www.w3.org/2018/credentials/
    v1",
  "type": ["VerifiableCredential", "
    AgeVerificationCredential"],
  "credentialSubject": {
    "id": "did:example:123456789abcdefghi",
    "age": 25
  },
  "issuer": "https://example.com/issuers/1",
  "issuanceDate": "2023-05-01T00:00:00Z",
  "expirationDate": "2024-05-01T00:00:00Z",
  "proof": {
    "type": "RsaSignature2018",
    "created": "2023-05-01T00:00:00Z",
    "verificationMethod": "https://example.com/
    issuers/1#key",
    "signatureValue": "
    eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9..."
  }
}
```



```
{
  "@context": "https://www.w3.org/2018/credentials/
    v1",
  "type": ["VerifiableCredential", "
    AgeVerificationCredential", "
    ZKPVerificationCredential"],
  "credentialSubject": {
    "id": "did:example:123456789abcdefghi",
    "zkp": {
      "C": "0x123456789abcdef",  // the value of C
      "proof": {...}             // the ZKP proving
    knowledge of x
    }
  },
  "issuer": "https://example.com/issuers/1",
  "issuanceDate": "2023-05-01T00:00:00Z",
  "expirationDate": "2024-05-01T00:00:00Z",
  "proof": {
    "type": "RsaSignature2018",
    "created": "2023-05-01T00:00:00Z",
    "verificationMethod": "https://example.com/
    issuers/1#key",
    "signatureValue": "
    eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9..."
  }
}
```

What is Zero-Knowledge Proof ?

BOB

Do we make same money?

ALICE

30k 40k 50k 60k 70k 80k 90k

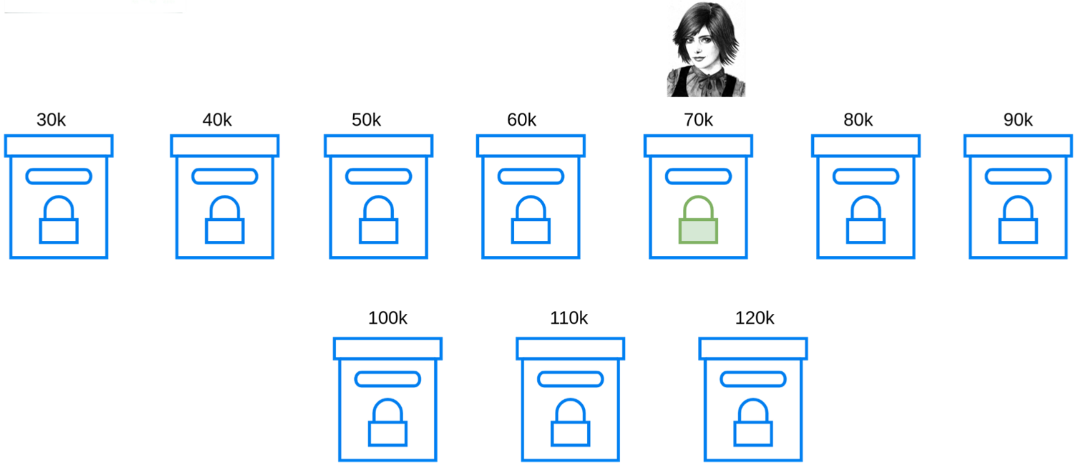
100k 110k 120k

What is Zero-Knowledge Proof ?

BOB

ALICE

Do we make same money?



30k

40k

50k

60k

70k

80k

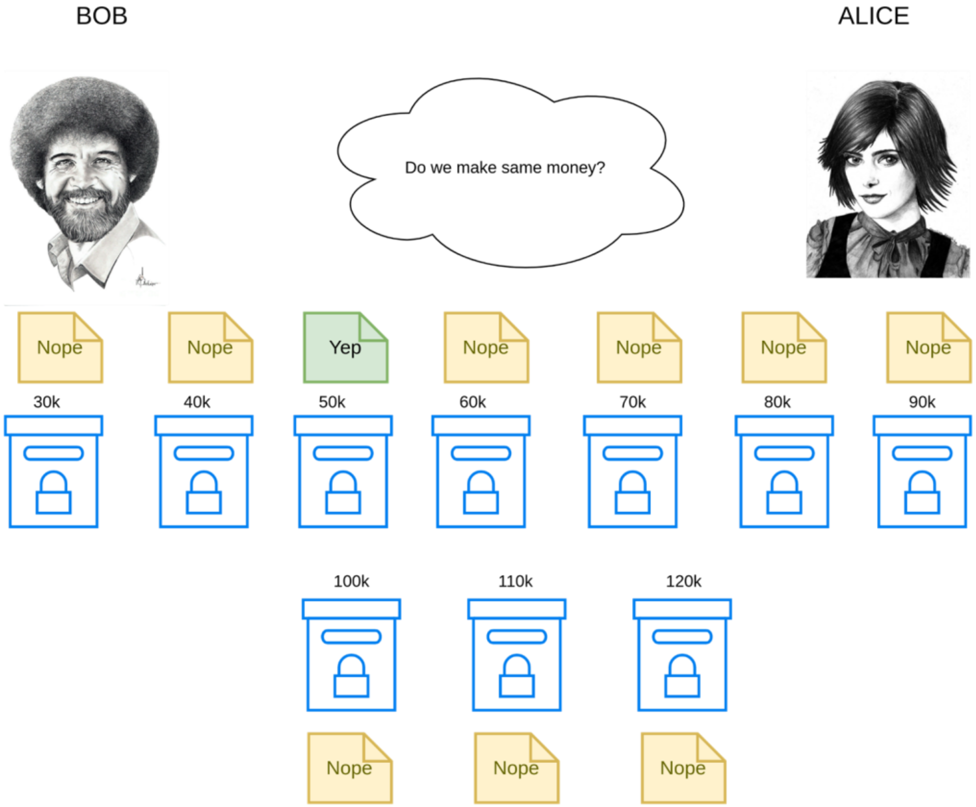
90k

100k

110k

120k

What is Zero-Knowledge Proof ?



BOB

ALICE

Do we make same money?

Nope Nope Yep Nope Nope Nope Nope

30k 40k 50k 60k 70k 80k 90k

100k 110k 120k

Nope Nope Nope

What is Zero-Knowledge Proof ?

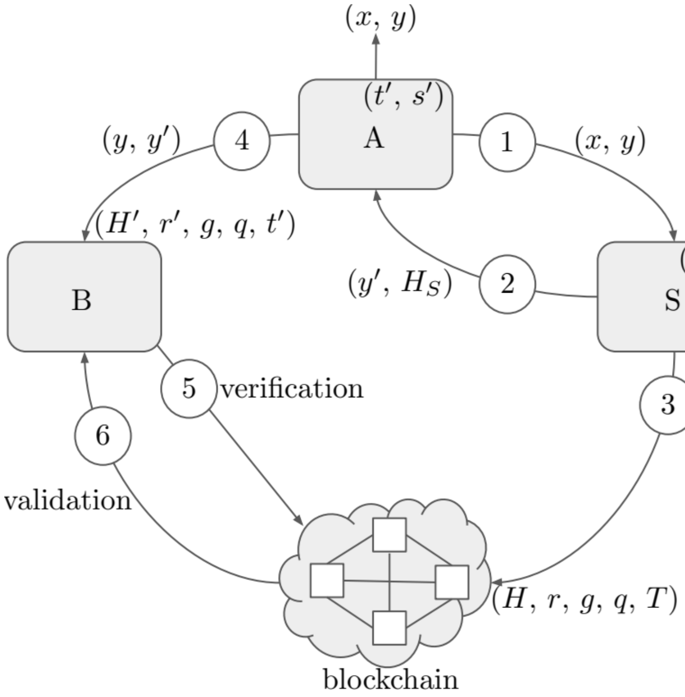
BOB

I opened the box with my secret
turns out we
DONT make same money

ALICE

How ZKP can be used in SSI?

To show how a prover can convince a verifier that they possess a secret attribute without disclosing the attribute



SSI generation protocol using a ZKP Schnorr: generation (1,2), registration (3) and verification (4,5,6) of a Self-Sovereign Identity

Threat Model

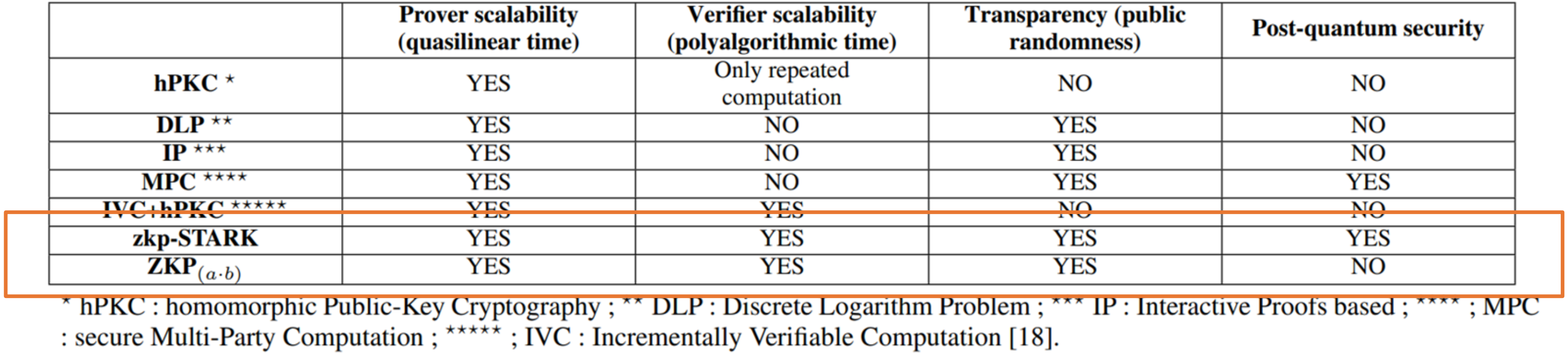
But, is even the best tool safe?

Threat Model

Despite the secure features offered by ZKP, is it still prone to some attacks.

- ❖ **Replay attacks**: Attacker intercepts & replays a valid ZKP message to the verifier, impersonating the original sender.
- ❖ **Denial-of-service attacks**: Attacker may attempt to launch a DoS attack against a ZKP protocol by flooding the system with requests or by disrupting the communication between the prover and verifier.
- ❖ **Computationally intensive**: ZKP protocols require significant computational resources to generate and verify proofs, which can limit their practicality.

Threat Model



	Prover scalability (quasilinear time)	Verifier scalability (polyalgorithmic time)	Transparency (public randomness)	Post-quantum security
hPKC *	YES	Only repeated computation	NO	NO
DLP **	YES	NO	YES	NO
IP ***	YES	NO	YES	NO
MPC ****	YES	NO	YES	YES
IVC+hPKC *****	YES	YES	NO	NO
zkp-STARK	YES	YES	YES	YES
$\mathbf{ZKP}_{(a\cdot b)}$	YES	YES	YES	NO

* hPKC : homomorphic Public-Key Cryptography ; ** DLP : Discrete Logarithm Problem ; *** IP : Interactive Proofs based ; **** ; MPC : secure Multi-Party Computation ; ***** ; IVC : Incrementally Verifiable Computation [18].

Limitations of SSI

- **Sybil attacks**: A single user creates multiple identities to gain control of the system or to disrupt its operation.
- **Man-in-the-middle attacks**: An attacker intercepts communication between two parties to steal data or to manipulate the communication.
- **Identity revocation**: Difficult to resolve in SSI systems since no central server can simply revoke users' cryptographic keys.
- **Key Leakage**: In the overall setting of SSI, proper key management is vital to its widespread adoption.
- **Interoperability**: Lack of interoperability between different SSI systems could limit their widespread adoption.

Market Offerings

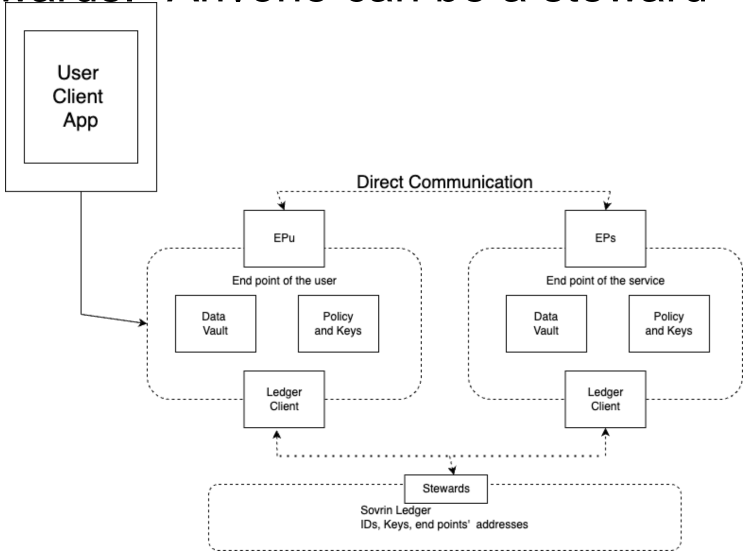
- What are the current market leading SSI Solutions?
- We discuss 3 products
  - Sovrin,
  - ShoCard
  - uPort.

Sovrin

- ➢ Sovrin has three networks for SSI. All are based on HyperLedger Indy, which is a type of distributed ledger software.
- ➢ The decentralized party here is their stewards. “Anyone can be a steward”

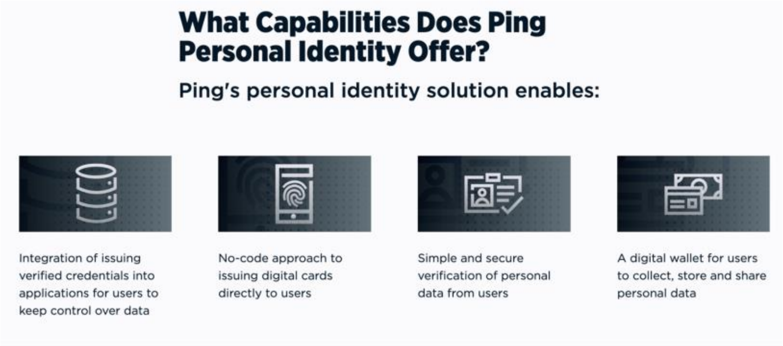
absa AyanWorks bloqzone CERTIZEN

Stewards



ShoCard

- ShoCard like others, is also a commercial SSI solution which runs on bitcoin blockchain and is solely working on replacing banking and credit card identification process.



What Capabilities Does Ping Personal Identity Offer?

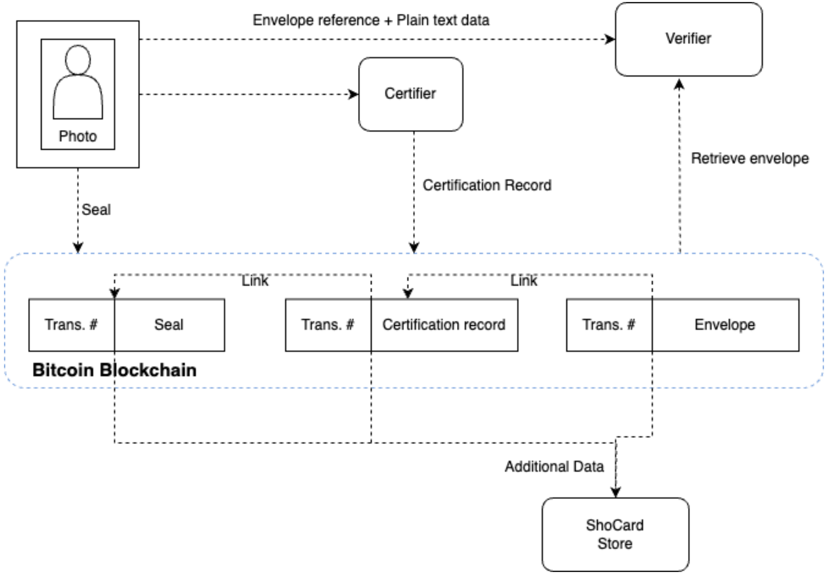
Ping's personal identity solution enables:

Integration of issuing verified credentials into applications for users to keep control over data

No-code approach to issuing digital cards directly to users

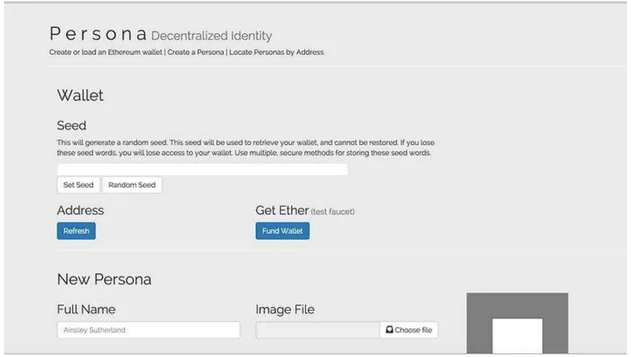
Simple and secure verification of personal data from users

A digital wallet for users to collect, store and share personal data



uPort

- ❖ uPort is rather a different SSI solution, which works on Ethereum Blockchain. It confirms transparency and identity of an individual.
- ❖ It will associate an Ethereum Address with a Name and Profile Picture, and potentially other info like email address, Twitter handle, etc.,



Persona Decentralized Identity

Create or load an Ethereum wallet | Create a Persona | Locate Personas by Address

Wallet

Seed

This will generate a random seed. This seed will be used to retrieve your wallet, and cannot be restored. If you lose these seed words, you will lose access to your wallet. Use multiple, secure methods for storing these seed words.

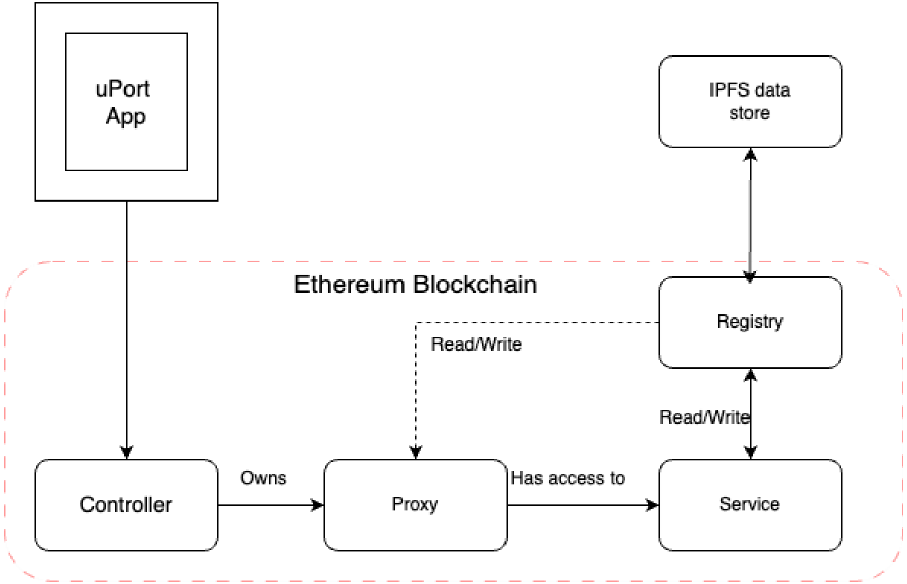
Address

Get Ether (test faucet)

New Persona

Full Name: Ainsley Sutherland

Image File



Contributions

- Review of **traditional systems**.
- **Decentralized architecture** to enable individuals to control their identity.
- Introduction to **self-sovereign identity** (SSI) systems.
- Discussed how **ZKP** can secure SSI.
- Studied potential **adversarial attacks** on ZKP based SSI.
- Provided insights into **limitations** & **challenges** of blockchain-based IDMS.
- Commercial **market offerings** regarding applicability of BC-based SSI solutions.

References

1. https://www.w3.org/TR/did-core/
2. https://freecontent.manning.com/the-basic-building-blocks-of-ssi/
3. https://ieeexplore.ieee.org/document/9927415
4. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10105959
5. https://sovrin.org/stewards/
6. https://medium.com/shocard/why-shocard-is-the-premier-blockchain-based-mobile-identity-platform-6fad15410106
7. https://freecontent.manning.com/the-basic-building-blocks-of-ssi/
8. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9371034/

Thank You!