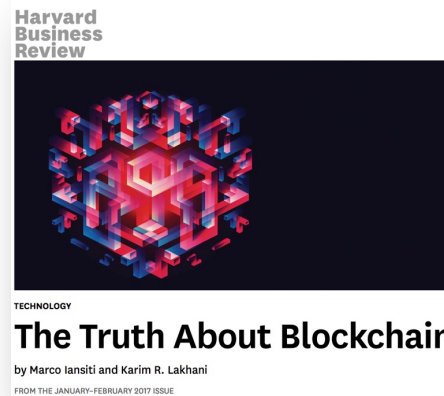


# Blockchain and Digital Identity SSI, DIDs, VCs, and the EBSI



Miguel Pupo Correia



# Motivation: blockchain



Cryptos: 16.34M Exchanges: 822 Market Cap: \$3.31T

Name	Price	1h %	24h %	7d %	Market Cap 
 Bitcoin BTC <a href="#">Buy</a>	\$105,357.25	▲ 0.37%	▼ 2.95%	▼ 5.17%	\$2,093,658,004,669

# Motivation: blockchain

A blockchain is a distributed infrastructure that  
is cybersecure by construction

*Not the usual question: not “how to secure it?”  
but “what can we do with something that is secure?”*

# Blockchain killer apps

- **Tokenization:** dependable, secure, decentralized & transactionable value and rights
- **Virtual organizations:** dependable, secure & decentralized organizations and services
- **Identity:** dependable, secure & decentralized identity

# Schedule

- Digital Identity
- Decentralized Digital Identity
- The EBSI
- Key takeaways

# Schedule

- Digital Identity
- Decentralized Digital Identity
- The EBSI
- Key takeaways

# Digital identity (online) of what?

- Persons
- Organizations
- Devices
- Digital services
- ...

# Before – Centralized Identity

user authentication



Sign in

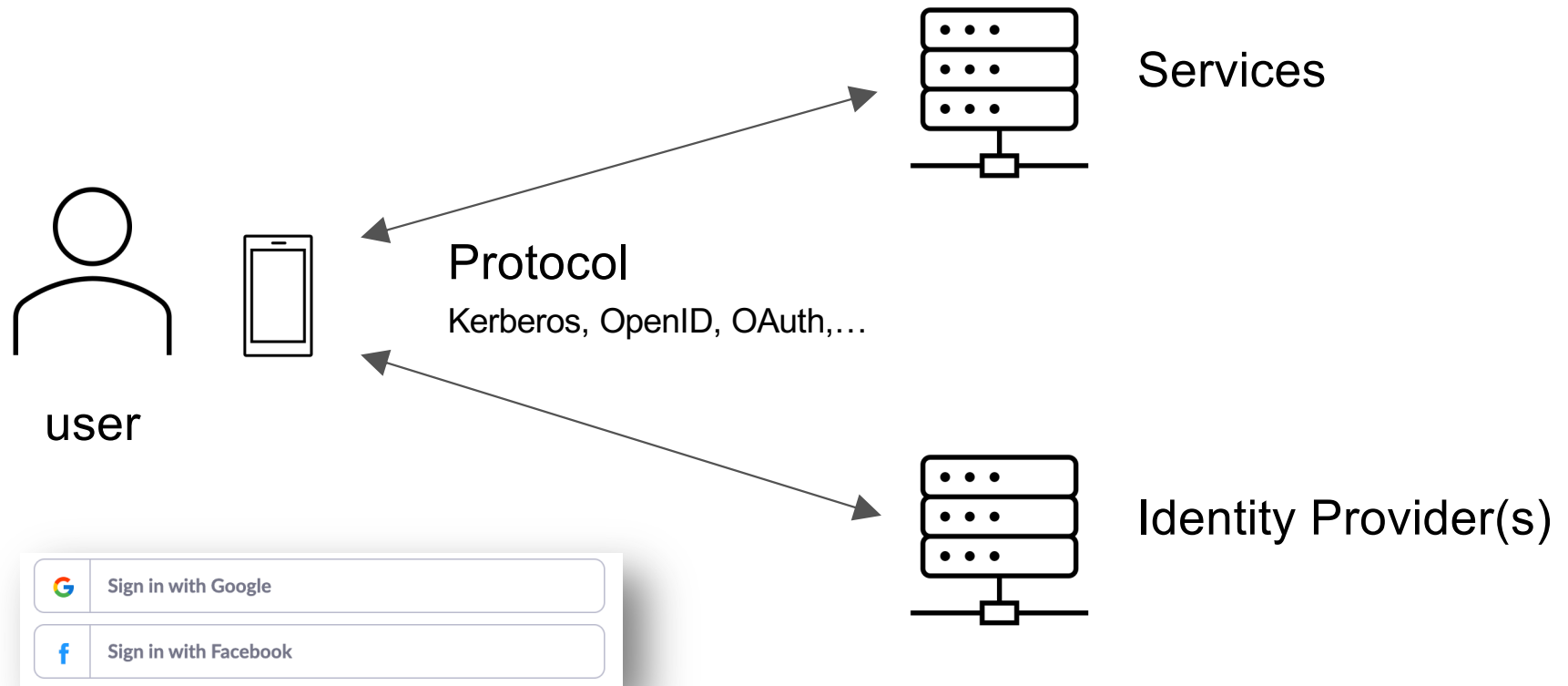
Username

Password



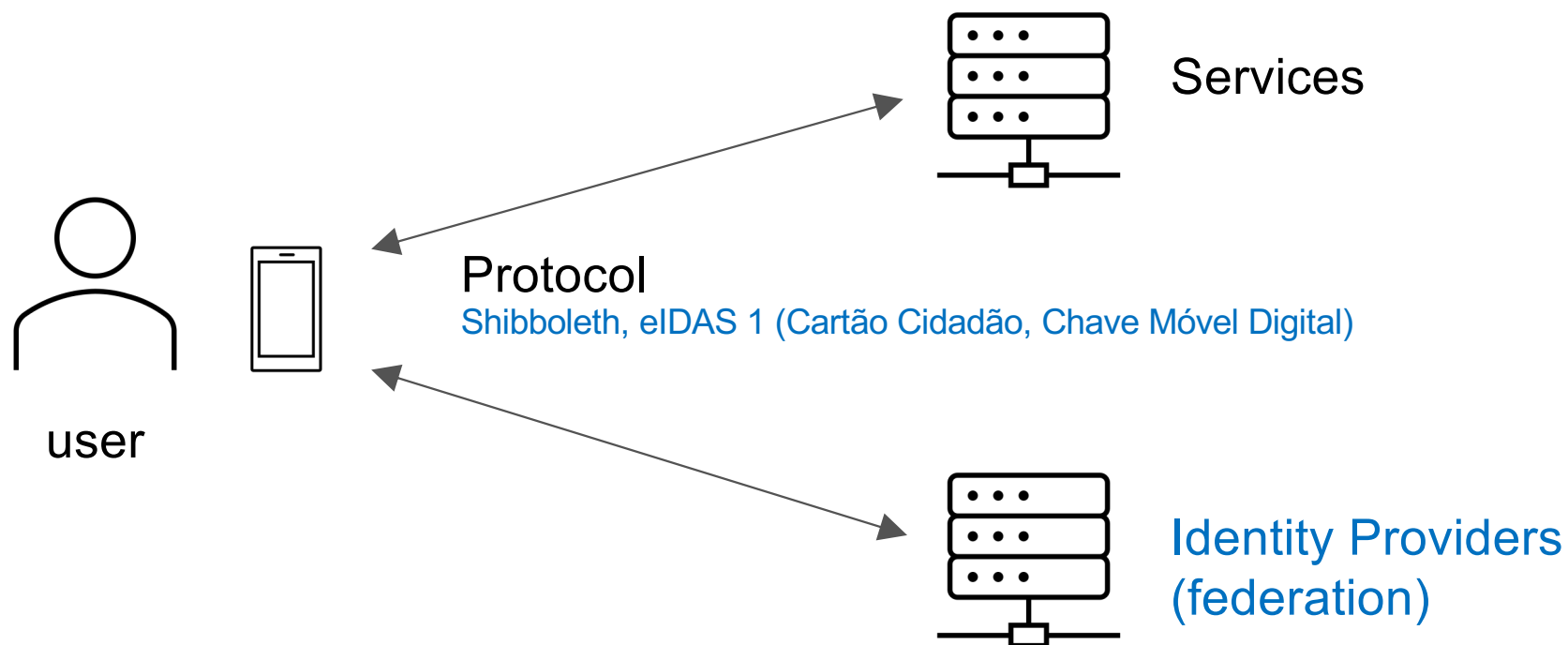
# Before – Single-Sign On

user authentication



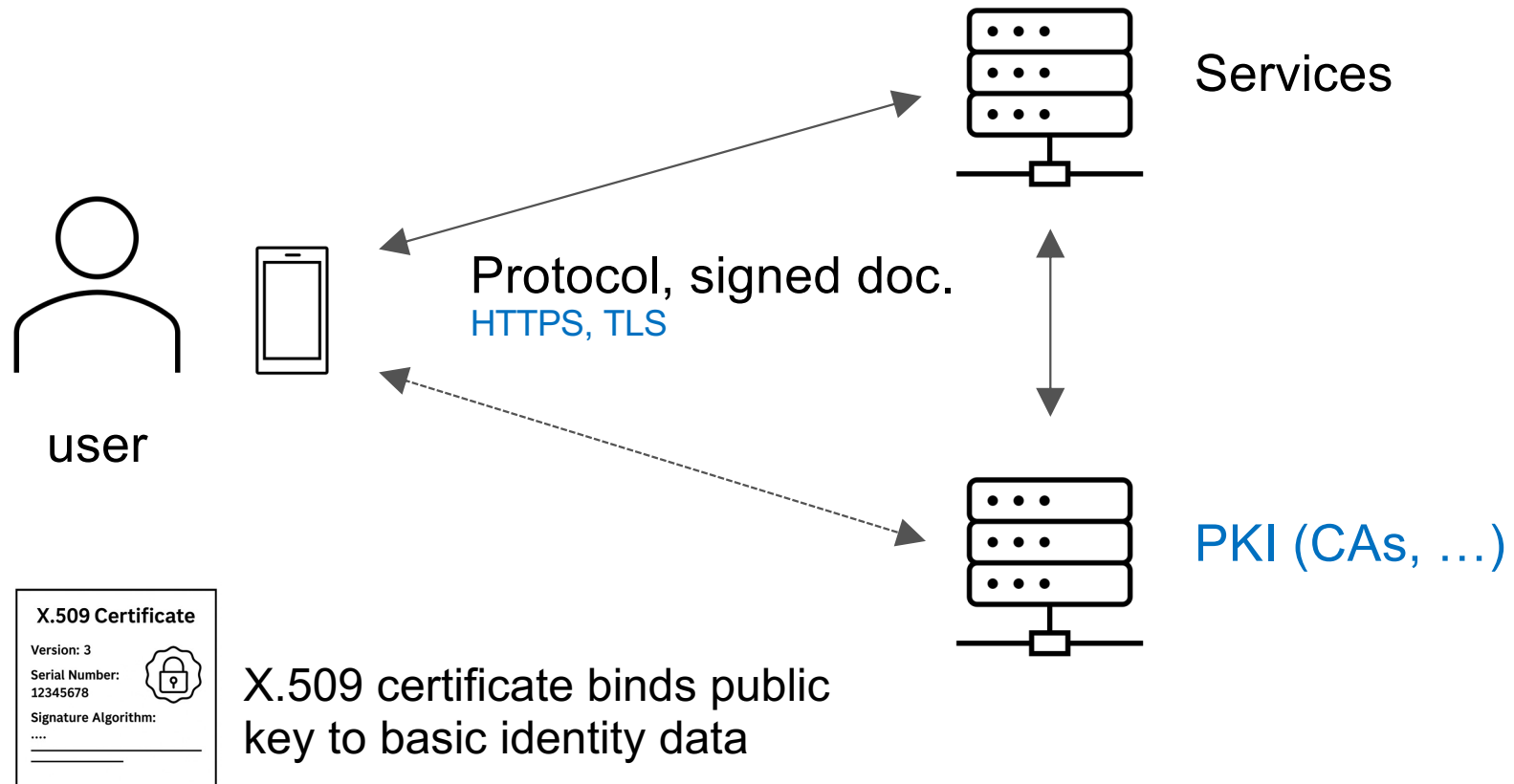
# Before – Federated Identity

user authentication



# Before – PKI

user & service authentication, doc. signing,...



# Digital identity before and now



## Before the focus was on:

**Authentication:** prove I am who I say I am

**Authorization:** access control



## Now the focus is on:

**Claims/attributes:** to prove that I have certain characteristics

**Privacy, user control,...**

# Schedule

- Digital Identity
- Decentralized Digital Identity
- The EBSI
- Key takeaways

# Self-Sovereign Identity (SSI)

- Initially a **manifesto**, not a technology
  - Christopher Allen, The Path to Self-Sovereign Identity, 2016
- Identity belongs to the user, not the IDP (e.g., a Big Tech)
- Identity controlled by the user
- Many IDPs, not federated, but with interoperability

# SSI

- Two W3C proposals related to SSI:
  - Decentralized Identifiers (DIDs)
  - Verifiable Credentials (VCs)

# Decentralized Identifiers (DIDs)

- **DID**: a unique, cryptographically verifiable, **identifier** in URI format

Scheme  
did:example:123456789abcdefghi  
DID Method DID Method-Specific Identifier

- A DID is verified with the assistance of a Trusted Data Registry: a Blockchain/Ledger
  - TDR stores a **DID document** with verification information, no identify info (e.g. PII)

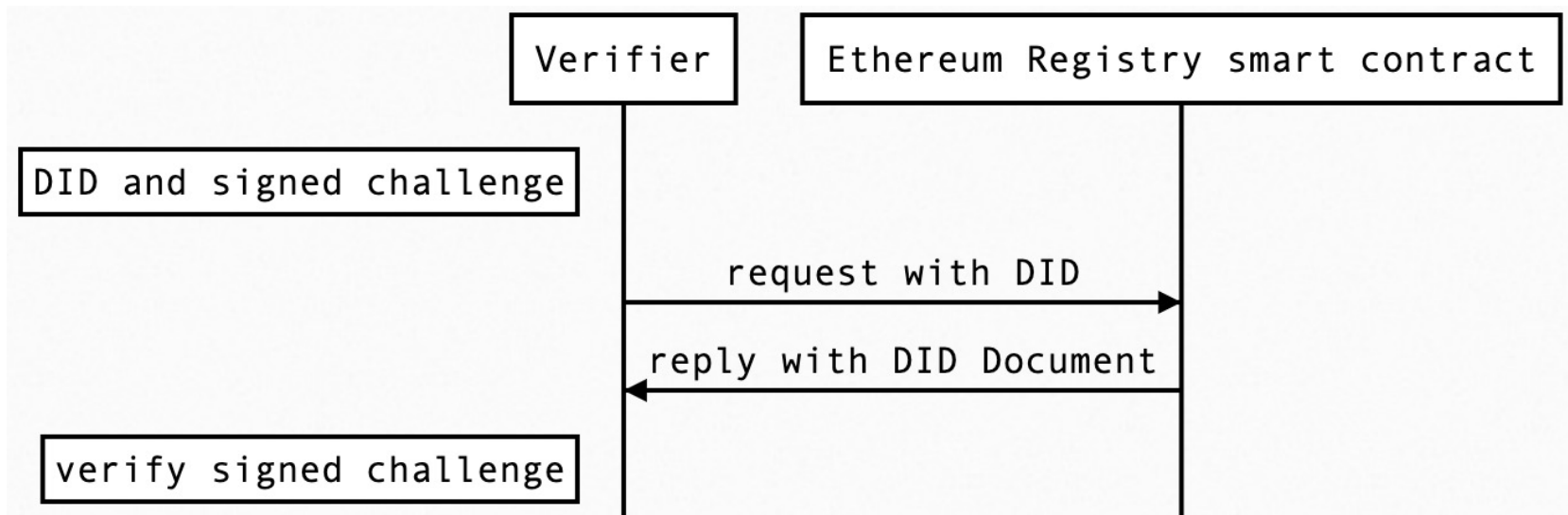
```
{
  "@context": [...],
  "id": "did:web:w3c-ccg.github.io",
  "verificationMethod": [
    {
      "id": "did:web:w3c-ccg.github.io",
      "type": "JsonWebKey2020",
      "controller": "did:web:w3c-ccg.github.io",
      "publicKeyJwk": {
        "kty": "OKP",
        "crv": "Ed25519",
        "x": "0-e2i2_Ua1..."
      }
    }
  ]
}
```



# did:ethr – Ethereum

- Format: "did:ethr:" [ethr-network ":"] ethereum-address / public-key-hex
  - Ex: **did:ethr:**0xf3beac30c498d9e26865f34fcaa57dbb935b0d74
  - The address is function of the public key (hash of the key)
- Create (register) :
  - Create a key pair (an account)
  - Store the **DID document** in the **registry smart contract** of that network
    - Registry in the Ethereum mainnet and in most networks has address  
0xdca7ef03e98e0dc2b855be647c39abe984fcf21b
- Read (resolve) / Update / Delete (revoke): in the registry smart contract

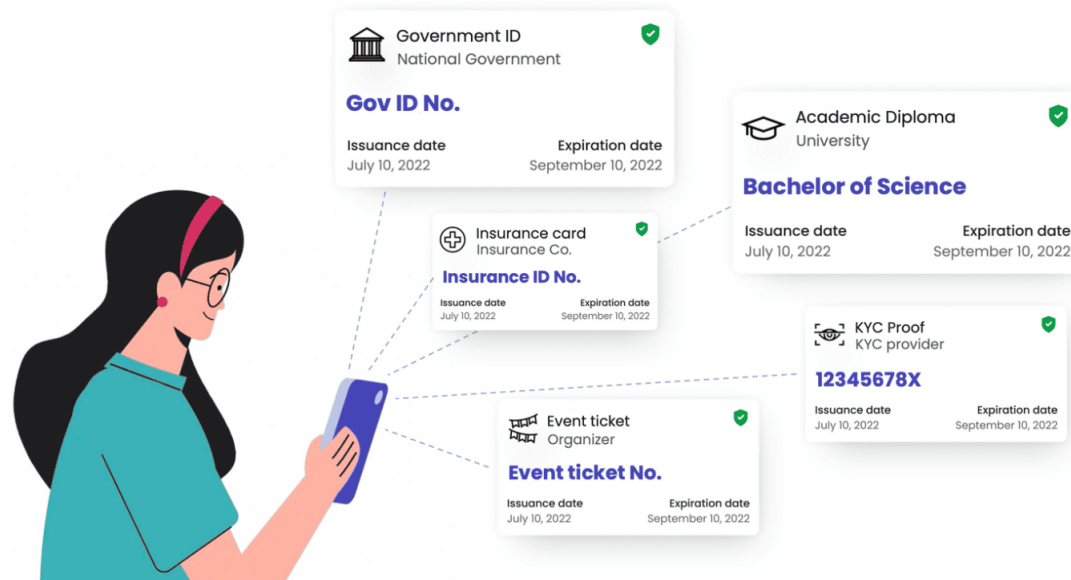
# did:ethr ID verification



- Similar to authentication with a PKI and X.509 certificates

# Verifiable Credentials (VCs)

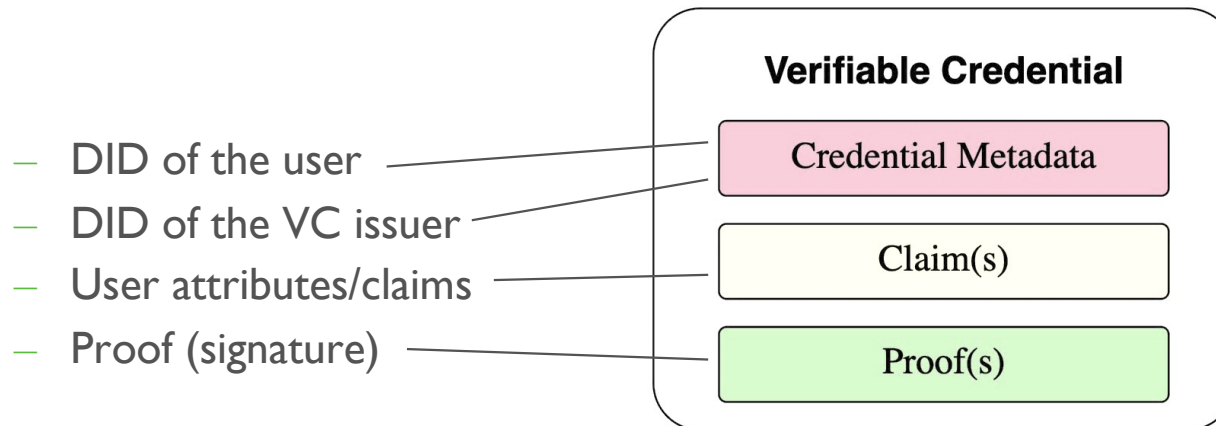
- **VC**: a digital document with identity data (e.g., personal data) whose authenticity can be verified online
  - Examples: university degree, personal data, product composition, passport



<https://gataca.io/blog/what-are-verifiable-credentials/>

# Verifiable Credentials (VCs)

- **VC**: a digital document whose authenticity can be verified online
  - Examples: university degree, personal data, product composition, passport
- A **VC** is a JSON or XML file that contains:

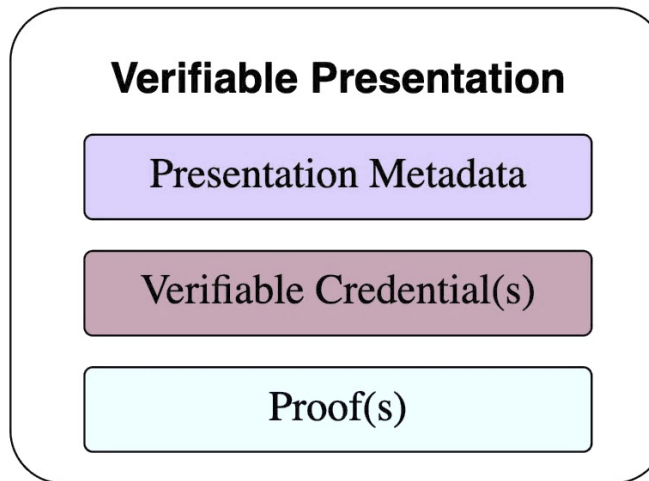


- *The DIDs are verified with DID documents stored in the blockchain*

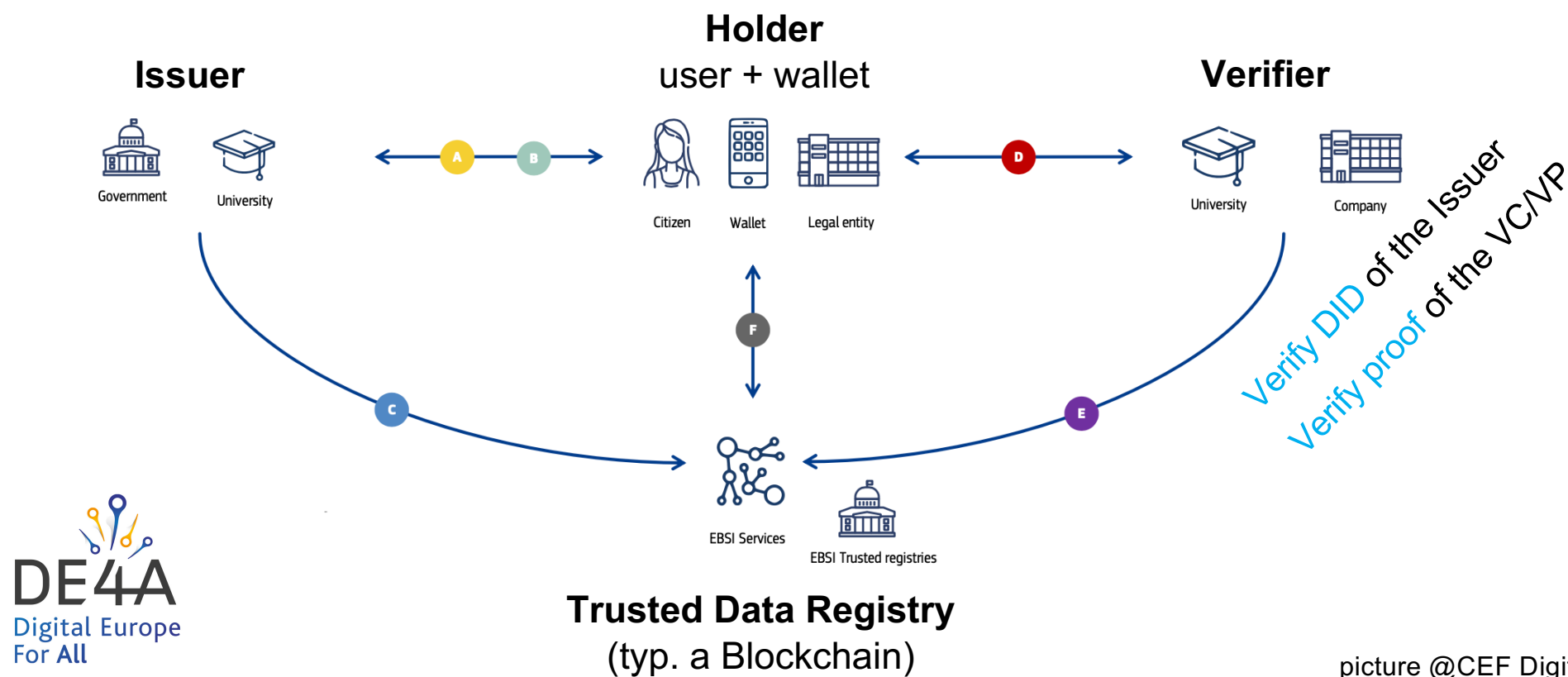
<https://www.w3.org/TR/vc-data-model/>

# Verifiable Presentations (VPs)

- **VP**: a subset/transformation of a VC provided to a verifier
  - Support for **selective disclosure** – data minimization



# VCs / VPs in action



# VPs support Selective Disclosure

- Goal: data minimization for **privacy**
- Key idea
  - **Holder** presents credential with **only** the data the Verifier needs
  - **Issuer** is not involved in the process (only provided the VC earlier)
  - **Verifier** is able to verify the credential (**challenge**: Issuer signs the VC)
- Solutions:
  - SD-JWT VC, with hashes
  - ZKP systems (e.g., Hyperledger AnonCreds)

# Digital identity Wallets

- Digital identity wallets store:
  - the user's DIDs
  - the user's VCs



# SSI platforms

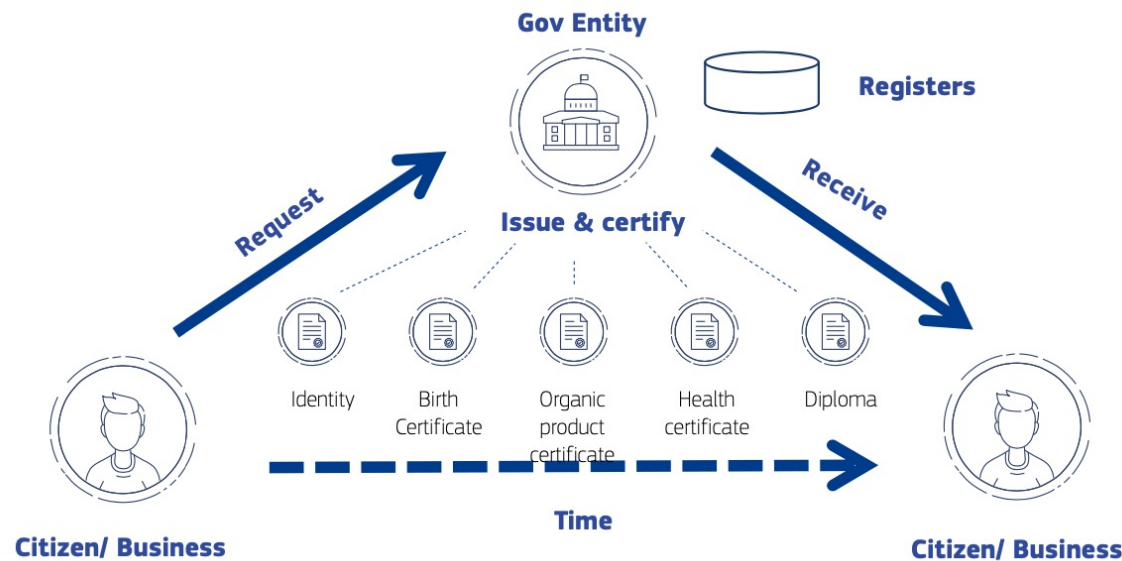
- There are several (Hyperledger Indy, Sovrin, etc.)...
- ... but what is the root of trust for issuers / VCs?

# Schedule

- Digital Identity
- Decentralized Digital Identity
- The EBSI
- Key takeaways

# European Blockchain Services Infrastructure

- Blockchain for EU-wide cross-border public services
  - Every country will have at least 1 node
  - Permissioned, only official nodes can join

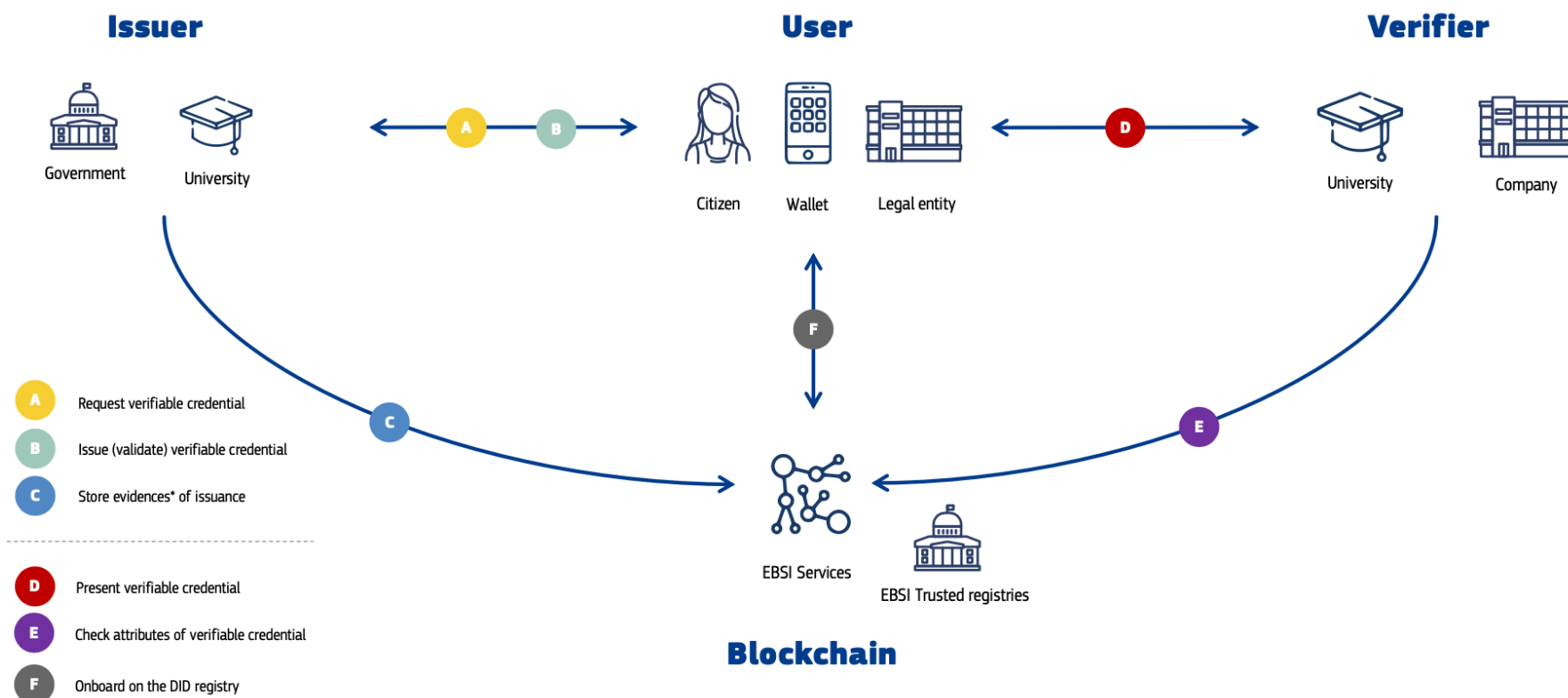


picture @CEF Digital

# The EBSI is mainly a SSI platform

- EBSI registers DID documents for:
  - Trusted Accreditation Authorities (TAOs) from each country
- Trusted Issuers are registered by a TAO
  - Their DID documents are stored in the EBSI
- Holders get VCs directly from Issuers
- Verifiers verify VCs using the Issuers DID documents
  - that they retrieve from the EBSI

# Use case: Diplomas



picture @CÉF Digital

# EBSI's status

- Status: Pre-production
- Governance
  - Initially: European Blockchain Partnership
  - Now: EUROPEUM-EDIC
- Community:
  - Ecosystem of +500 public & private orgs from 30+ countries
  - Incubation program – services & tools for pilot implementation
- Infrastructure / tech.
  - 41 nodes of which 28 are validators
  - 30+ conformant wallets



# EU Digital Identity

- eIDAS regulation – 2014, revised in 2024
- **eIDAS 2** provides a framework for **European Digital Identity Wallets**



# PKI vs Decentralized Digital Identity

	PKI	Decentralized Digital Identity
Certificates	X.509 certificates (limited identity data)	DIDs (limited), VCs (rich)
Authentication / signatures / secure channel establishment	Supported	Supported
Attributes/claims	Limited	Arbitrary (VCs)
Root of trust	Root stores (Web), Trust List Manager (ETSI ITS PKI)	Ad-hoc, EBSI
Other trust sources	CAs, RAs, etc.	Issuers



# Schedule

- Digital Identity
- Decentralized Digital Identity
- The EBSI
- Key takeaways

# Key takeaways

Digital Identity / SSI is a first order application for Blockchain technology



W3C DIDs and VCs play a key role



The EBSI will be an important platform for SSI, but still in pre-production



Many use cases, e.g., cross-border mobility, education, real estate



<https://www.linkedin.com/in/miguelpcorreia/>

