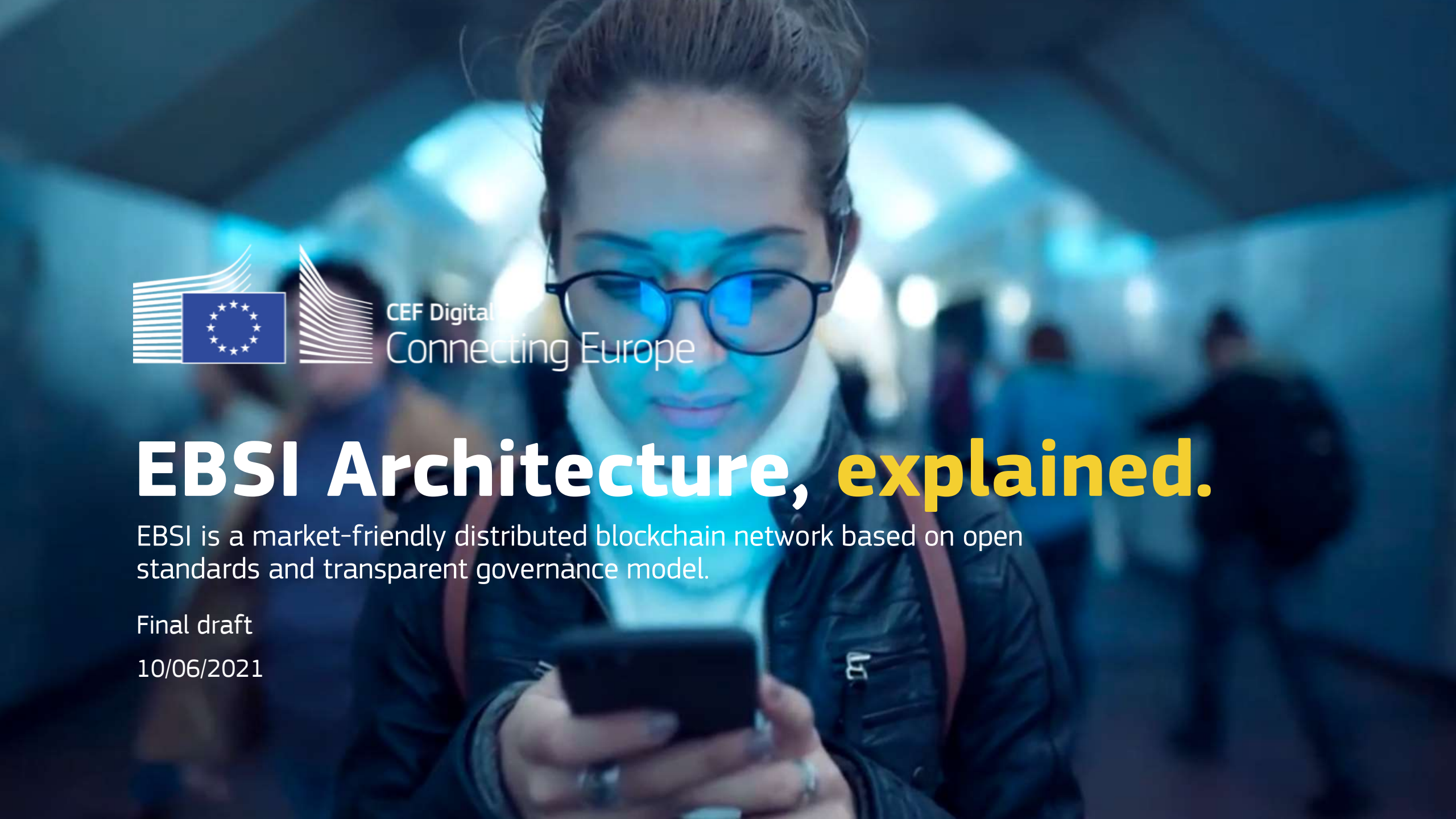


CEF Digital
Connecting Europe

EBSI Architecture, explained.

EBSI is a market-friendly distributed blockchain network based on open standards and transparent governance model.

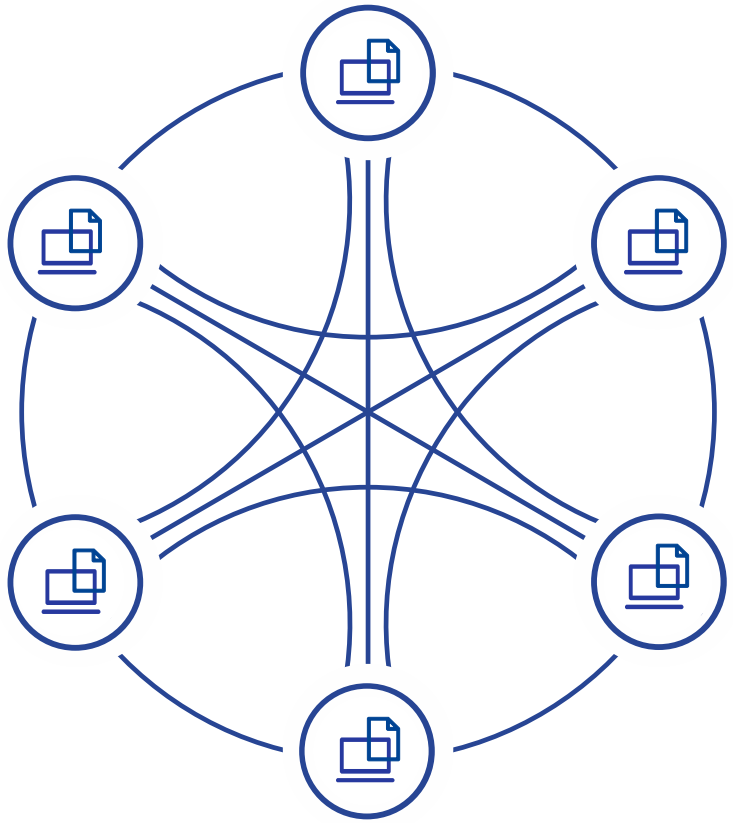
Final draft

10/06/2021

01

How to build trust through blockchain and EBSI ?

Blockchain is a distributed ledger to decentralise permanent digital records / transactions.



A **LEDGER** is a well-known concept used in business as a log keeping a definitive record of transactions.

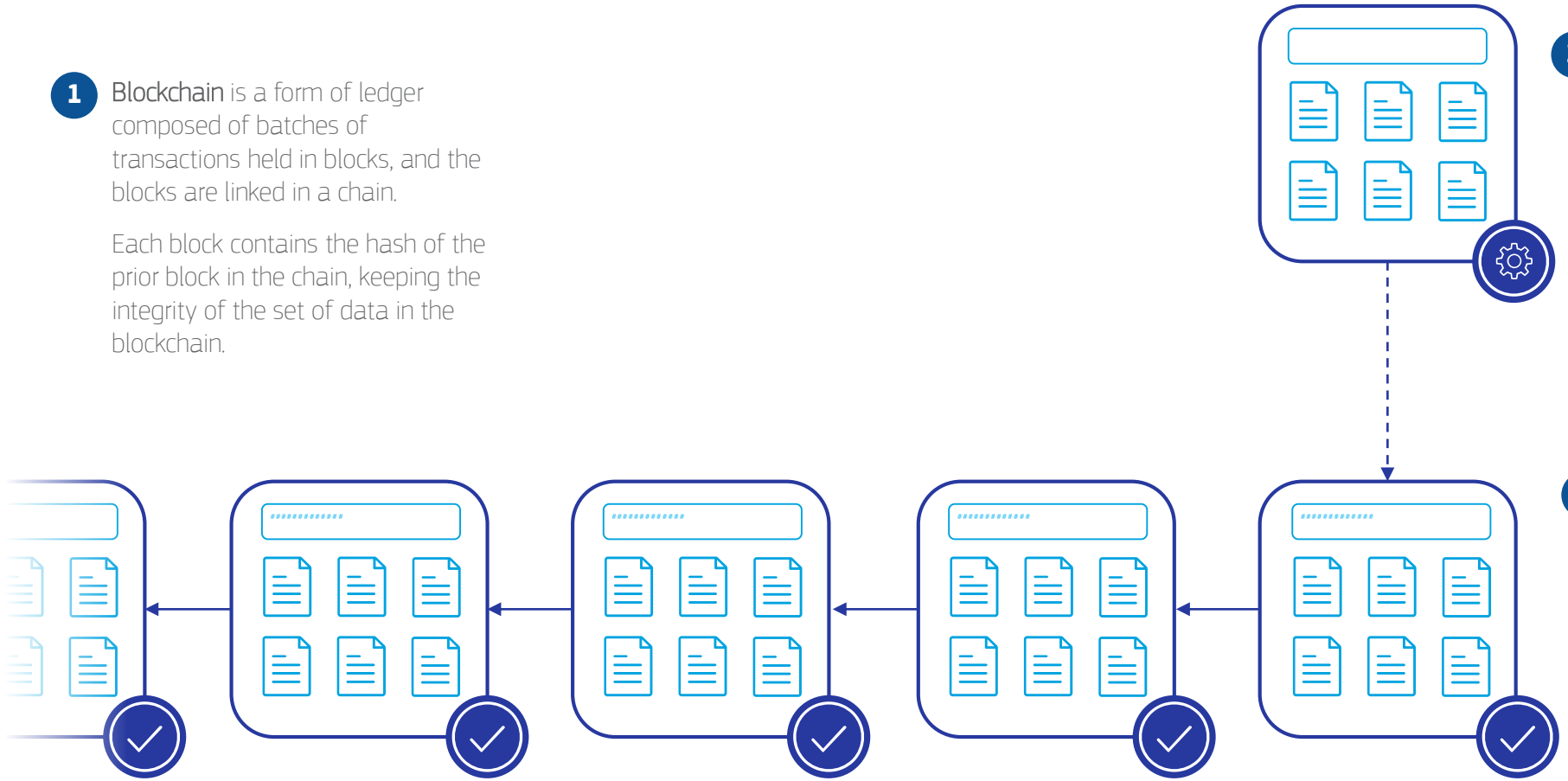
LEDGERS are used to record transactions of almost any type. For example, the status of a document.

A **DISTRIBUTED LEDGER** is a ledger that has its entries stored across a series of nodes in a network, rather than in a single location making it "tamper-resistant".

Blockchain uses cryptographic methods that creates trust between disparate systems.

1 **Blockchain** is a form of ledger composed of batches of transactions held in blocks, and the blocks are linked in a chain.

Each block contains the hash of the prior block in the chain, keeping the integrity of the set of data in the blockchain.



2 *Each block can contain transactions, data and a **reference to the previous blocks** (creating the chain)*

3 *Transactions recorded **chronologically** and **cannot be changed** once added to the chain*

*For **blocks to be added** to the blockchain, it must be achieved through **consensus***

The finality of each new block is agreed via a shared consensus mechanism. EBSI is based on the Proof of Authority consensus.

Proof of Work

Proof of Stake

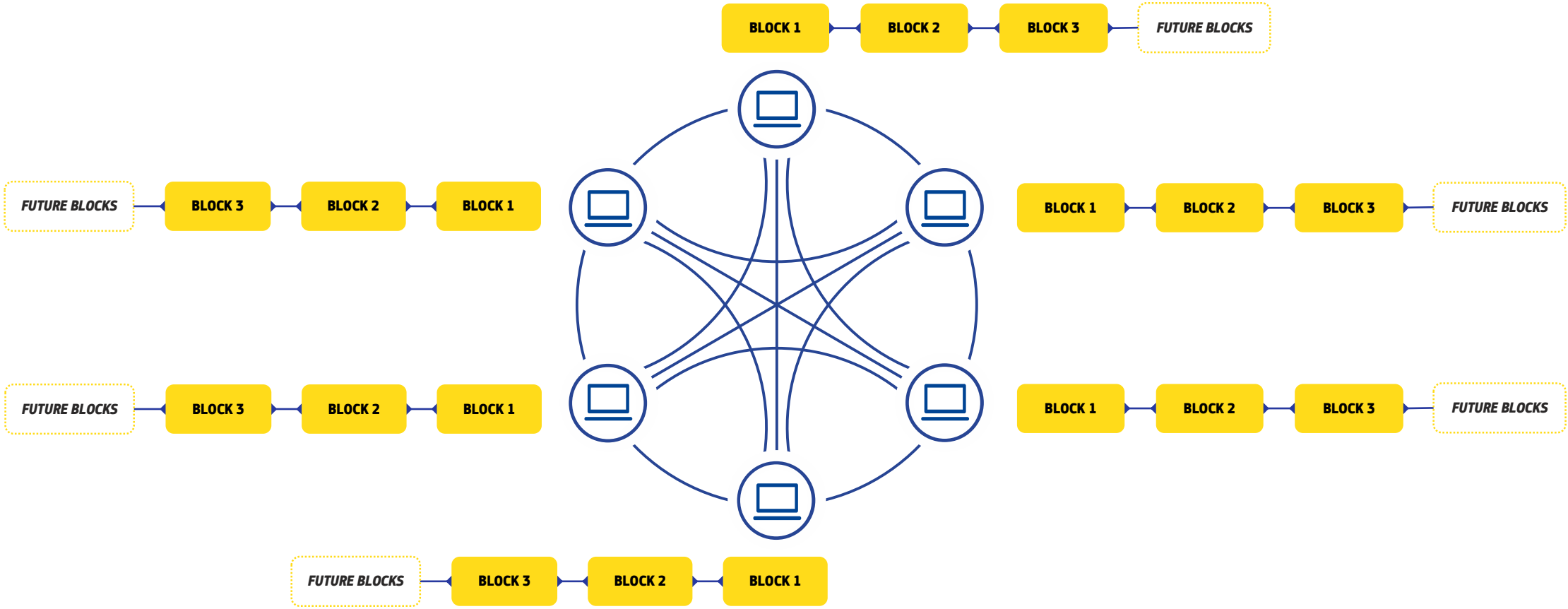
Proof of Authority

Permissionless
No authentication needed to write on the blockchain [Miners]

Permissioned
Transactions and blocks are validated by approved accounts [Validators*]

*Every MS has elected a representative to perform the validation

When transactions are added to a block, the blocks are validated by the network. Every node maintains an identical copy of the blockchain



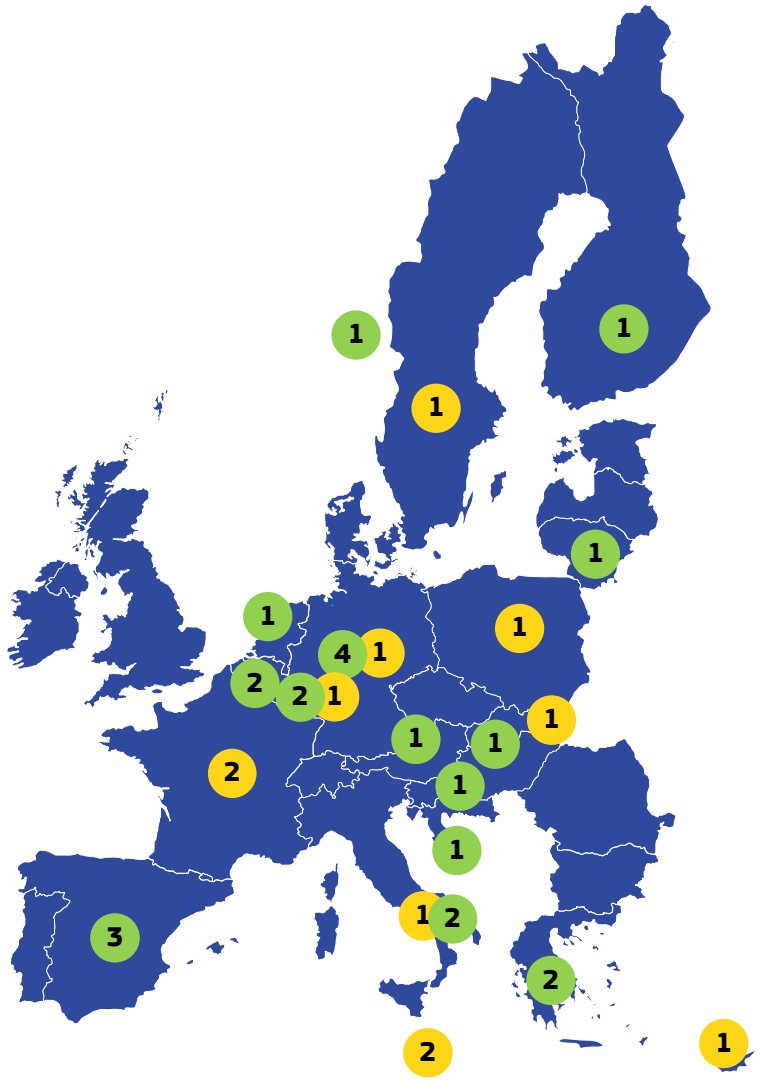
02

How does the EBSI architecture work?

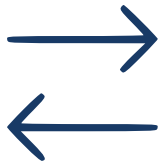
The European Blockchain Partnership is a group of 29 countries and the EC. We help public administrations accelerate the creation of trustworthy cross border digital services.

Having this opportunity in mind, the EBSI (European Blockchain Services Infrastructure) has been developed. **Our vision is to accelerate the creation of cross-border services and put blockchain technology at the service of public administrations for the purpose of verifying information, making the services trustworthy**.

EBSI is the first EU-wide blockchain infrastructure, driven by the public sector, in full respect of European values and regulations. EBSI is supported by 29 countries (All EU Member States, Norway and Liechtenstein) and the EC forming the European Blockchain Partnership (EBP).



EBSI is designed as a market-friendly distributed blockchain ecosystem based on open standards and a transparent governance model. The EBP has approved five key principles.

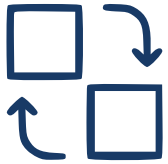


Public good

EBSI's administration must be in the public good, and it is responsible for limiting its usage to public and private services that provide a net public good to the citizens of the Member States as a whole

Governance

The EBSI governance system shall ensure that decisions are reached through building consensus among stakeholders,



Harmonization

EBSI governance should encourage and maintain the harmonisation of technical requirements and architecture to prevent the proliferation of protocols supported or conflicting architectural assumptions.

Open source

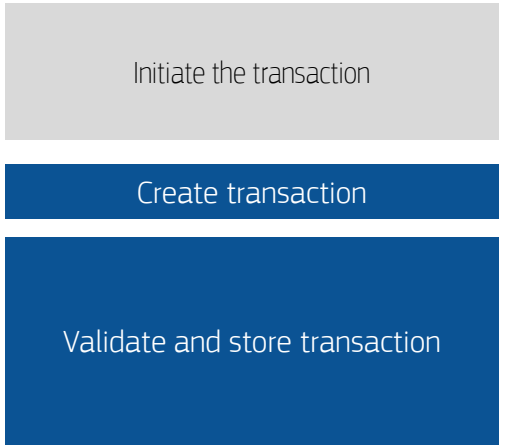
Wherever possible, the code-base for all EBSI services and structures should be open source to allow maximal auditing, security, and healthy competition between service providers, vendors, and private-sector concerns building on top of the infrastructure.

EU values and regulatory framework

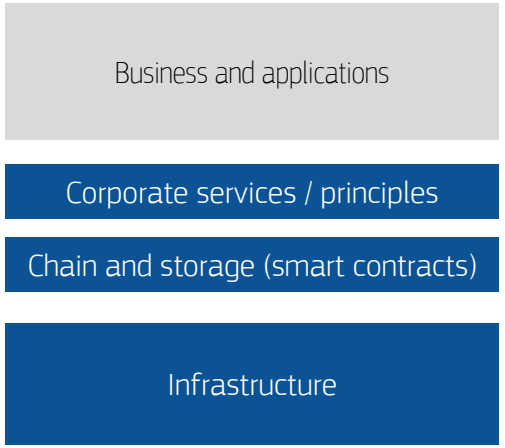
EBSI must not only comply with, but model compliance with the GDPR's current interpretation and ongoing refinement, **align with EIADAS and other regulations**

The EBSI architecture is being built alongside a fully distributed three-tier architecture and is extending the typical EA stack with the core services layer.

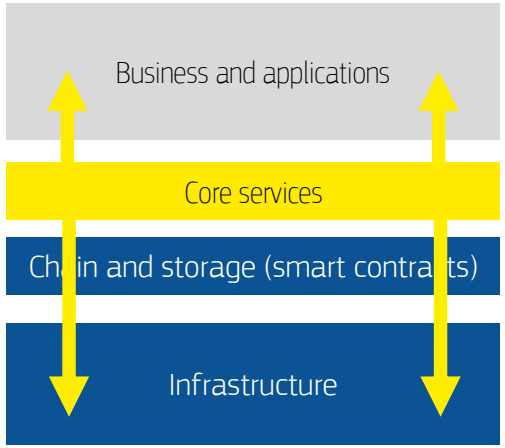
Most essential flow of **a transaction**



Typical architecture to support a transaction flow



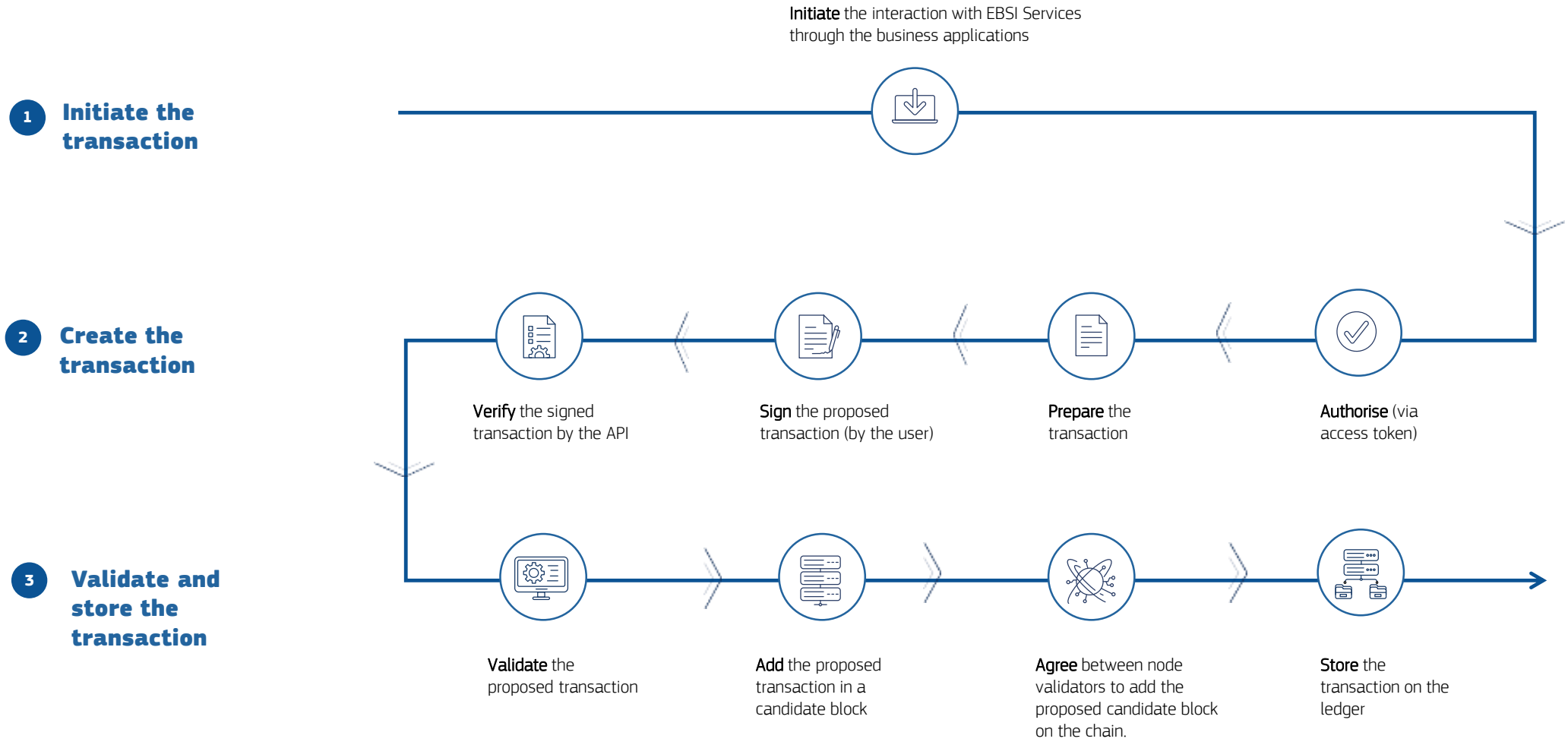
EBSI architecture to comply with EBP's guiding principles



- Public good.
- Governance.
- Technology harmonisation.
- Open source.
- GDPR compliant.

Core services are a set of standardised interfaces which (1) provide the capabilities for third-parties to develop applications and (2) ensure compliance with guiding principles defined and approved by the EBP on the technology and infrastructure layers.

Before explaining the architecture in more details, let's have a look at how a basic transaction flow work using EBSI.



Let’s illustrate EBSI layers interactions based on a simple blockchain transaction flow.

Business applications

A The legal entities / citizens call business interfaces

Core services

B The business interfaces call the EBSI exposed API interfaces for performing ledger transactions

C The APIs request to perform a transaction to a smart contract (SC)

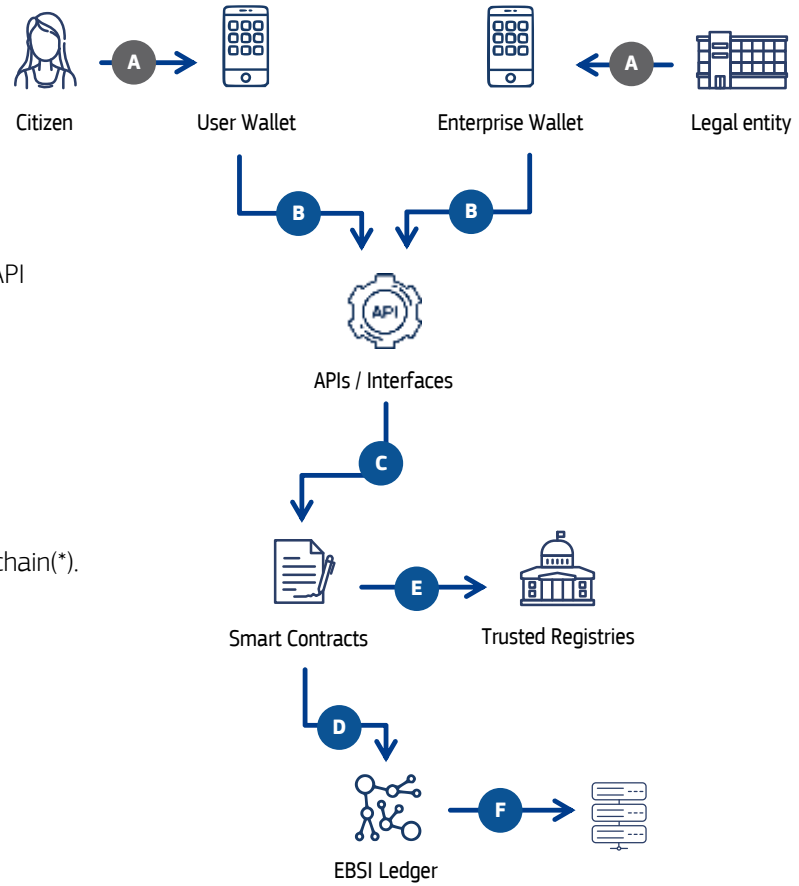
Chain and storage

D SCs control and enable the execution of trusted transactions, that will be recorded on the blockchain(*).

E SCs are also used to for manage Trusted Registries.

Infrastructure

F The ledger validates, authorises and stores the proposed transaction(s) on the chain of blocks



Governance

(*) The smart contracts (SC) are self-executing trusted contracts, with the terms of the agreement written in the SC Code. The SC code are deployed on distributed blockchain network. The SC code controls the execution of trusted transactions following the agreement in the code, between the parties, without the need of a central entity to enforce the decision

EBSI Core services are interfaces that the EBSI platform exposes to the use case layer, for leveraging the EBSI capabilities.

Identity

- Verifiable Presentation API/Library
- Verifiable Credential API/Library
- Identity Hub API
- DID Authentication Library
- DID Registry API

Trusted Registries

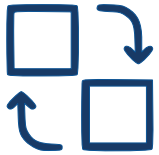
- Trusted Apps Registry API
- Trusted Issuers Registry API
- Trusted SC Registry API
- Trusted Schemas Registry API
- Trusted IAM Registry API

Wallet Libraries

- Signing blockchain transactions
- Reference implementations
- Key management

API Security Management

- Reverse Proxy



Integration API

- Timestamp API
- Storage API
- Ledger API
- Authorization API
- Notification API
- Revocation API

Integration tools

- API Catalog
- EBSI Generic Libraries
- Apps Onboarding
- User onboarding
- EBSI Trusted Appstore

*Critically, external applications do not have direct access to the lower layers, but do so through the interfaces of this layer

EBSI uses smart contracts to ensure that data sent through APIs are correctly recorded in a trustworthy way on the EBSI Infrastructure.

EBSI smart contracts

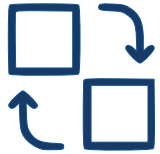
- Trusted Apps Registry
- Trusted Issuers Registry
- Trusted Schema Registry
- Trusted IAM Registry
- Trusted SC Registry
- Proxy template
- Admin Multi-Sig
- DID Registry
- Timestamp

Pluggable protocols

- Besu
- Fabric
- Cross Ledger Integration

Blockchain monitoring

- Besu Block Explorer
- Fabric Block Explorer
- Network statistics



Off-chain storage

- Distributed Storage
- Private Storage
- External Storage

*A smart contract is a computer program intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement.

03

How to build cross-border services using EBSI Core Services?

This part of the presentation will focus on identity and diploma use cases.

EBSI supports the creation of cross-border services e.g. allowing citizens to manage their identity, diploma and register documents.

The citizen who wants to set-up a digital wallet and **manage Self-Sovereign Identity.**

Eva is 20 and she heard about the new digital wallet. She sets up her wallet and requests a Verifiable ID from the Trusted Registration Authority (TAR):

1. *Eva downloads the wallet and configures it.*
2. *Eva creates her DID and securely stores it in her wallet together with its associated public / private keys.*
3. *Eva requests the registration of the DID on the EBSI ledger.*
4. *The Trusted Registration Authority* helps in the registration of the DID including the public key on the EBSI ledger, issues a Verifiable ID and sends it to Eva.*
5. *Eva gets the Verifiable ID and stores it in her digital wallet.*

The student who wants to apply for a Master Degree and **manage his/her educational credentials.**

Eva requests the issuance of her Bachelor's diploma to the University of Ghent (BE) and then apply for a Master's diploma at University of Rovira I Virgili

1. *Eva initiates the request for the issuance of her Bachelor's Diploma*
2. *Eva requests the issuance of her Bachelor's Diploma from the University of Ghent.*
3. *The University of Ghent issues the Bachelor's Diploma.*
4. *Eva receives, accepts and stores the Bachelor's Diploma in her digital wallet.*
5. *Eva initiates the application to the University of Rovira i Virgili.*
6. *Eva shares her Bachelor's Diploma with the University of Rovira i Virgili.*
7. *The University of Rovira i Virgili verifies the Bachelor's Diploma of Eva.*
8. *Eva receives the student identifier and is therefore enrolled to the Master's Degree at the University of Rovira i Virgili.*

The young professional who wants to apply to a job and **manage his/her credentials**

Eva has now graduated and wants to apply for a 1st job / apprenticeship in a Spanish Company:

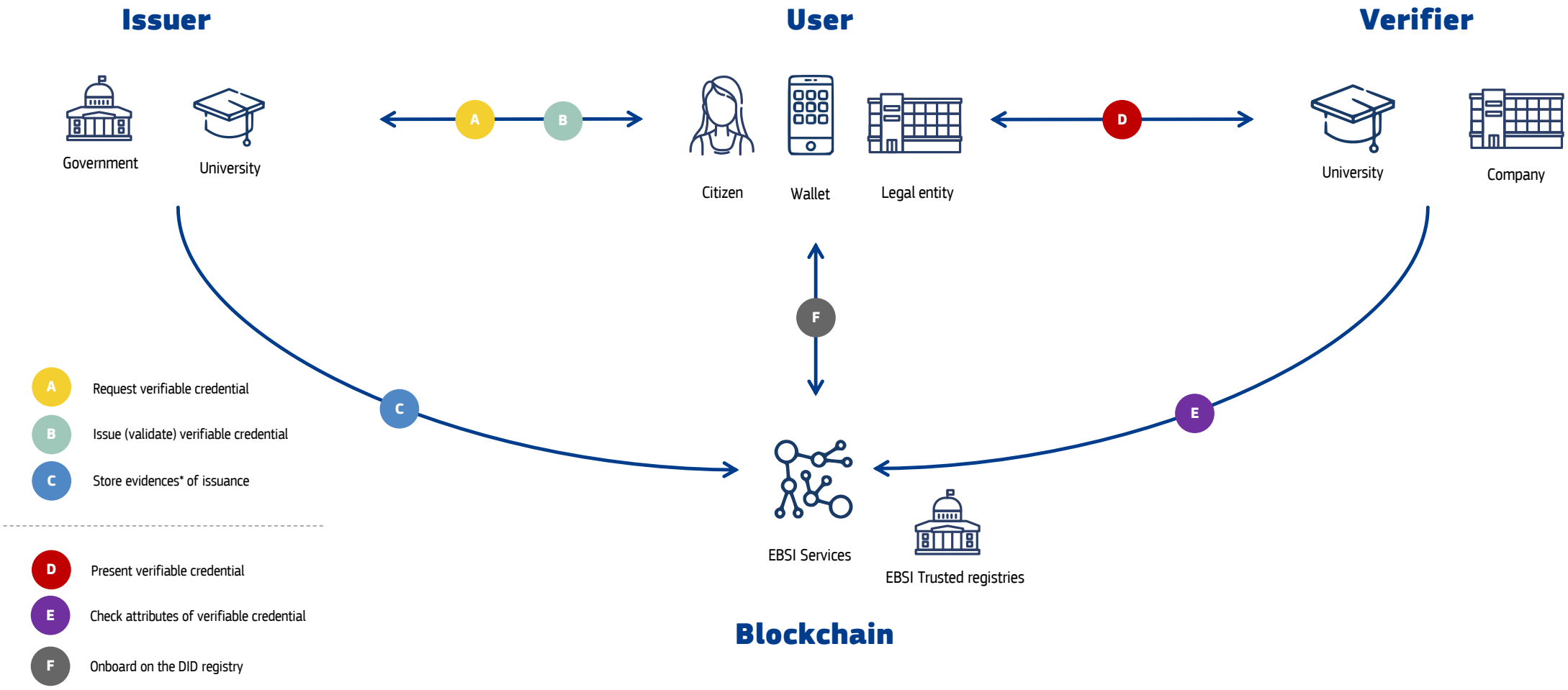
- *Eva initiates the application to the company in Spain.*
- *Eva shares her Master Diploma (VA) with the company.*
- *The company verifies the Master Diploma (VA) of Eva.*
- *Eva gets hired by the Spanish Company*

The entrepreneur who wants to create a company, apply for funding, **register and trace documents.**

Eva decides to start a business in Italy and participates in a call for proposals to get EU funding for her startup:

- *Eva's establishes her startup (StartupCo), creates an account and registers its identity on EBSI.*
- *StartupCo receives the grant. StartupCo uploads documents related to the grant application and registers the "documents'*
- *StartupCo grants access to their documents: the EU Audit Administration gets access to off-chain documents, all documents hashes and metadata related to grant funding.*
- *The EU Audit Administration checks that the content of these documents is effectively registered on the EBSI and produces a grant agreement in electronic form then registers the document on behalf of StartupCo*
- *The EU Audit Administration or StartupCo searches for a document using any metadata or hash and both can access the document found via search or otherwise*

Let’s have a look at the exchange of verifiable credential using blockchain (EBSI) to manage self-identity and diploma.

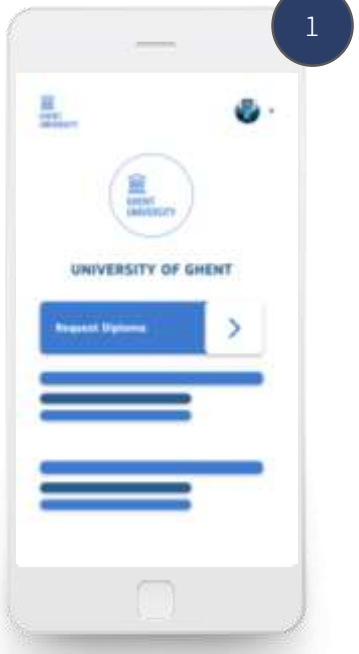


The interaction needs to happen via an EBSI compliant wallet. (1)

Example (1): Eva requests the issuance of her Bachelor's diploma to the University of Ghent (BE)

Eva initiates the request for the issuance of her Bachelor's Diploma

1



- Connect to University platform
- Initiate the action

Eva requests the issuance of her Bachelor's Diploma from the University of Ghent

2

- Select Verifiable ID
- Submit the request

The University of Ghent issues the Bachelor's Diploma

3

- Check list of students
- Select the students
- Submit the credential

Eva receives and accepts the Bachelor's Diploma.

4

- Get notification
- Accept the credential
- Store in the wallet.

The interaction needs to happen via an EBSI compliant wallet. (2)

Example (2): Eva requests her enrolment at the University of Rovira i Virgili (ES).

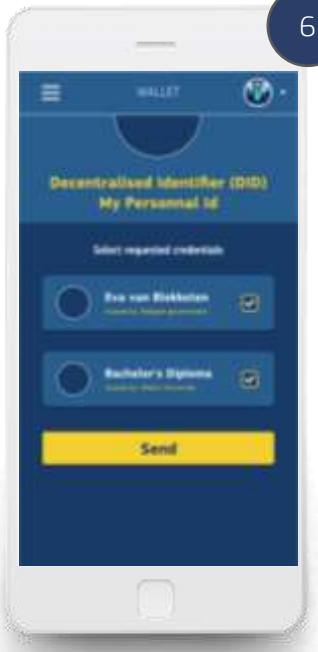
Eva initiates the application to the University of Rovira i Virgili

5

- Connect to University platform
- Initiate the action

Eva shares her Bachelor's Diploma with the University of Rovira i Virgili

6



- Select Verifiable ID
- Select Bachelor's diploma
- Submit the request

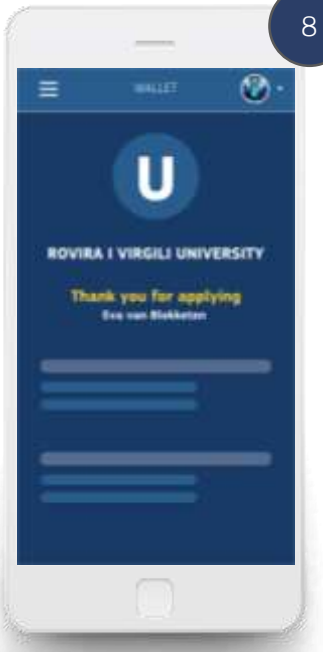
The University of Rovira i Virgili verifies the Bachelor's Diploma of Eva

7

- Get notification
- Check list of requests
- Check details of diploma

Eva enrols for a Master's Degree at the University of Rovira i Virgili

8



Building applications using EBSI Core Services APIs

Example (1): Eva requests the issuance of her Bachelor's diploma to the University of Ghent (BE)

Eva initiates the request for the issuance of her Bachelor's Diploma

Eva requests the issuance of her Bachelor's Diploma from the University of Ghent

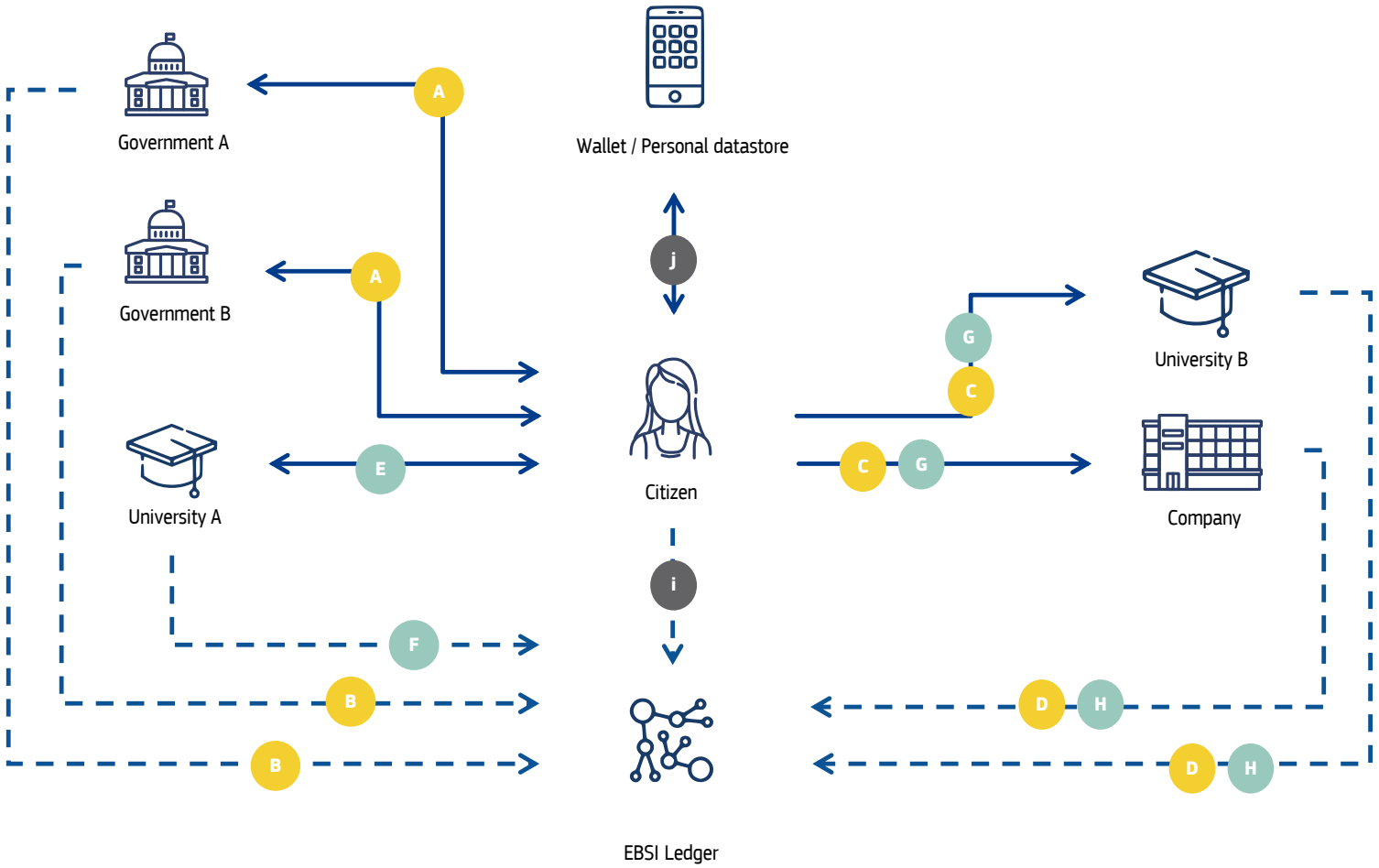
The University of Ghent issues the Bachelor's Diploma

Eva receives and accepts the Bachelor's Diploma

		1	2	3	4
Business app		✓	✓	✓	
Wallet	Wallet Library		✓	✓	✓
Identity	DID Registry API			✓	✓
	DID Authentication API		✓		
	VC API		✓	✓	
	ID Hub API		✓		
	VP API		✓		
Trusted registries	TSR API			✓	✓
	TIR API			✓	✓

EBSI ecosystem, explained.

EBSI applied in the context of identity and diploma management



Identity

- A — Request and issue identity credential
- B — Store evidences* of issuance (of identity credential)
- C — (Present identity credential)
- D — Check validity identity credential
- i — Anchor decentralized ID

Diploma

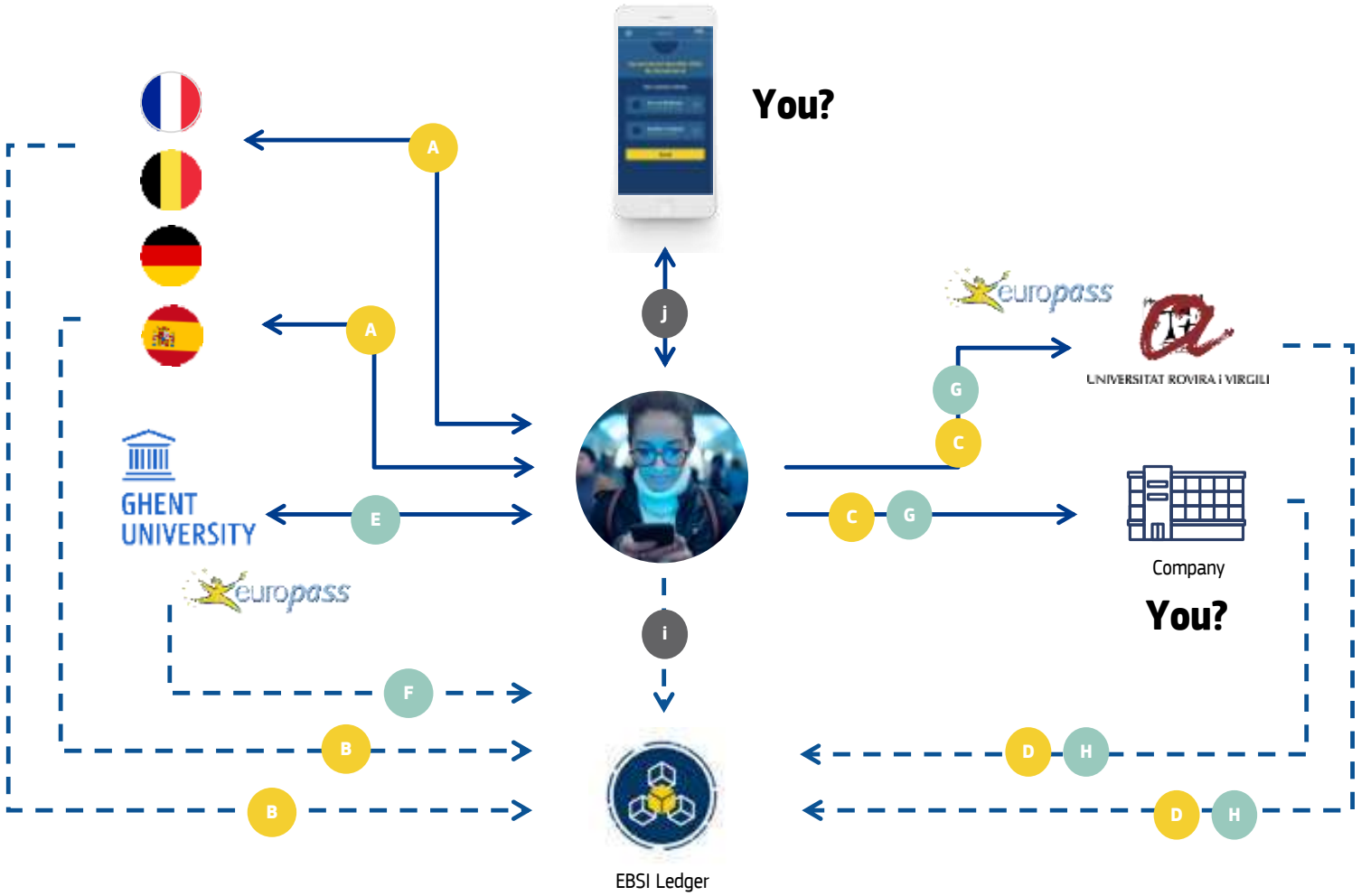
- E — Request and issue diploma credential
- F — Store evidences* of issuance (of diploma credential)
- G — Present diploma credential
- H — Check validity diploma credential

Wallet

- j — Authenticate and store credentials

Interested? Connect. Make. Grow.

Interested to join the ecosystem of EBSI and shape the future of Digital Europe?



Identity

- A — Request and issue identity credential
- B — Store evidences* of issuance (of identity credential)
- C — (Present identity credential)
- D — Check validity identity credential
- i — Anchor decentralized ID

Diploma

- E — Request and issue diploma credential
- F — Store evidences* of issuance (of diploma credential)
- G — Present diploma credential
- H — Check validity diploma credential

Wallet

- j — Authenticate and store credentials