Blockchain, a resilient source of truth

The concept of the ledger is as old as the written word

This 5000 y.o. Sumerian tablet is a ledger of transactions of goods
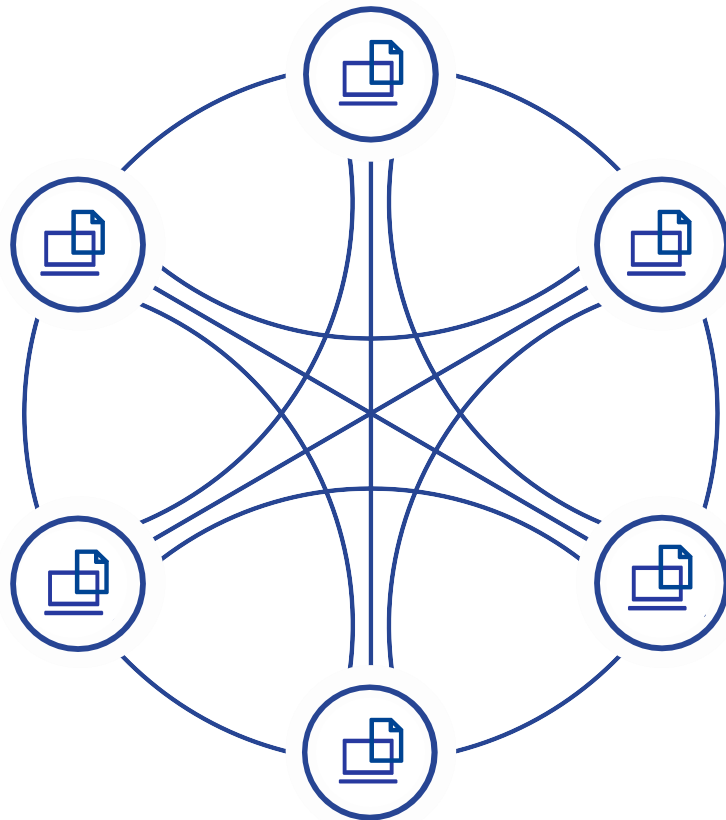– grains, sheep – used for verification* and record-keeping.

We became more sophisticated with centralised ledgers and registries.

The creation of national registers was a major advancement to distinguish fake from real information.

What is blockchain?

Blockchain is simply a decentralised / distributed ledger

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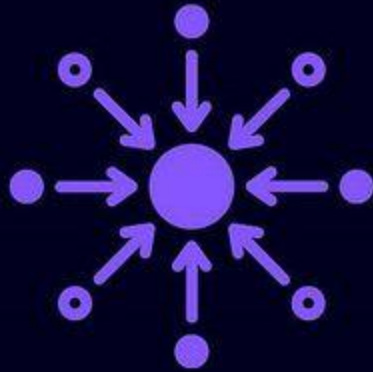
A **DISTRIBUTED LEDGER** is a ledger that has its entries stored across a series of nodes in a network, rather than in a single location, making it 'tamper-resistant'.

It is a whole new approach

...To managing data...

Centralised Approach

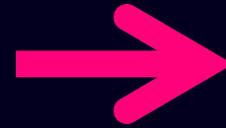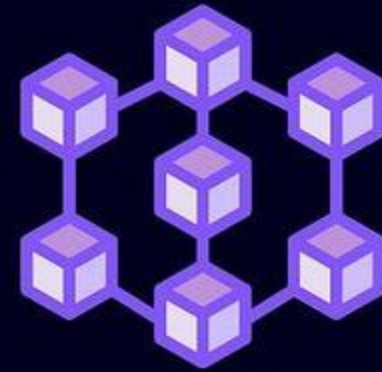Federated Approach

Distributed Approach

Web 1.0

Web 2.0

Web 3.0

How does blockchain work?

Explaining blockchain through a metaphor

Imagine each block as a **page in a ledger** or a folder in a filing cabinet. Just like a ledger or filing cabinet, a blockchain can be used to store and manage a variety of different types of information, such as financial transactions, contracts, or other records.

However, unlike a traditional ledger or filing cabinet, a blockchain is **distributed across a network of computers**, which makes it highly secure and resistant to tampering or modification.
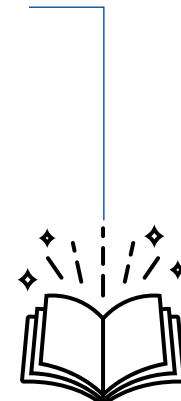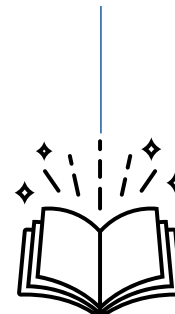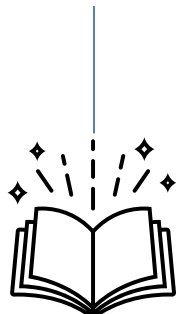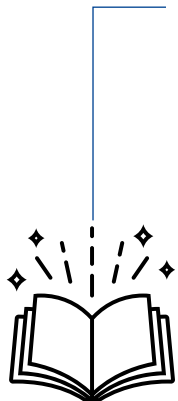
A blockchain is a linked list – *blocks* of information are cryptographically linked together, forming a *chain*

1 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).*

Hash of block 1

3 *Each block has a hash that is derived from the block's content.*

Hash of block 1

Hash of block 2

4 *Each new block contains the hash of the previous block. Transactions are recorded chronologically and cannot be changed once added to the chain.*

Hash of block 3

Hash of block 2

5 *For blocks to be added to the blockchain, it must be achieved through consensus.*
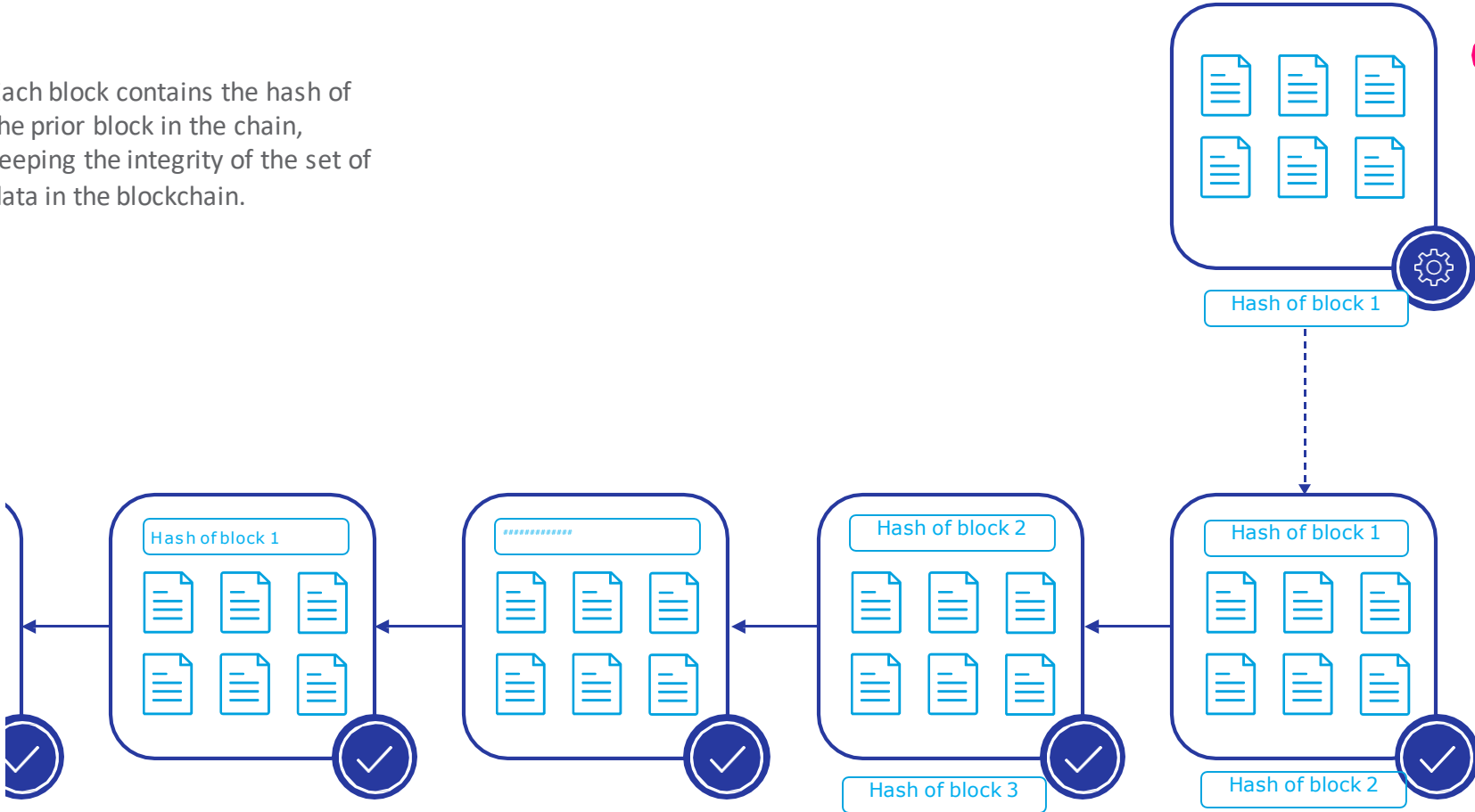
When transactions are added to a block, the blocks are validated by the network. Every node maintains an identical copy of the blockchain.
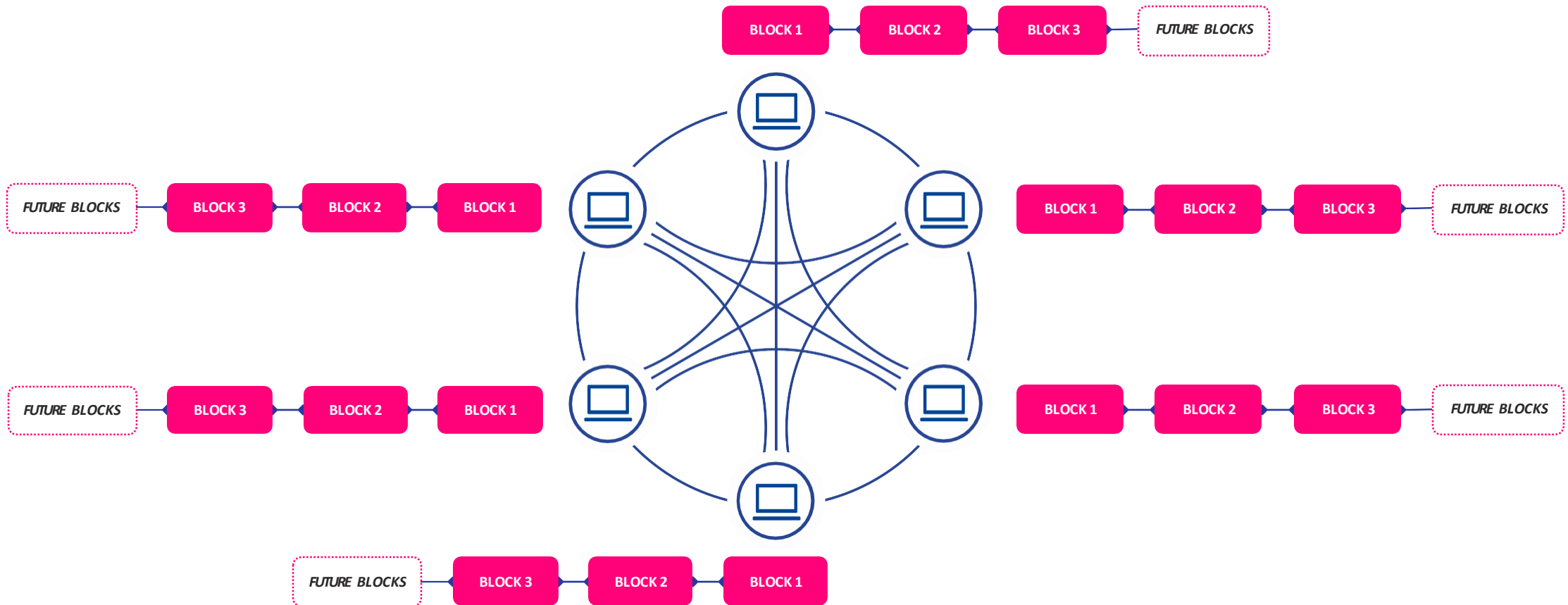
The truth being decentralised means the truth is resilient
Blockchain supports a resilient, tamper-proof trust model

Scalable, collective truth

New information (truth) is agreed upon by **consensus** between nodes. This decentralises the truth. It also means information can be added faster, and the infrastructure can withstand **many simultaneous requests**.

Synchronised copies on several nodes agreeing on new blocks via consensus.

No rewrites & in order

The data is added chronologically, and the ledger is **append-only** due to its innate cryptographic properties**.** We cannot change the history without compromising the system. This creates **accountability.**

Chronological set of data records, with a full history of key rotations – you can check signature validity back in time.
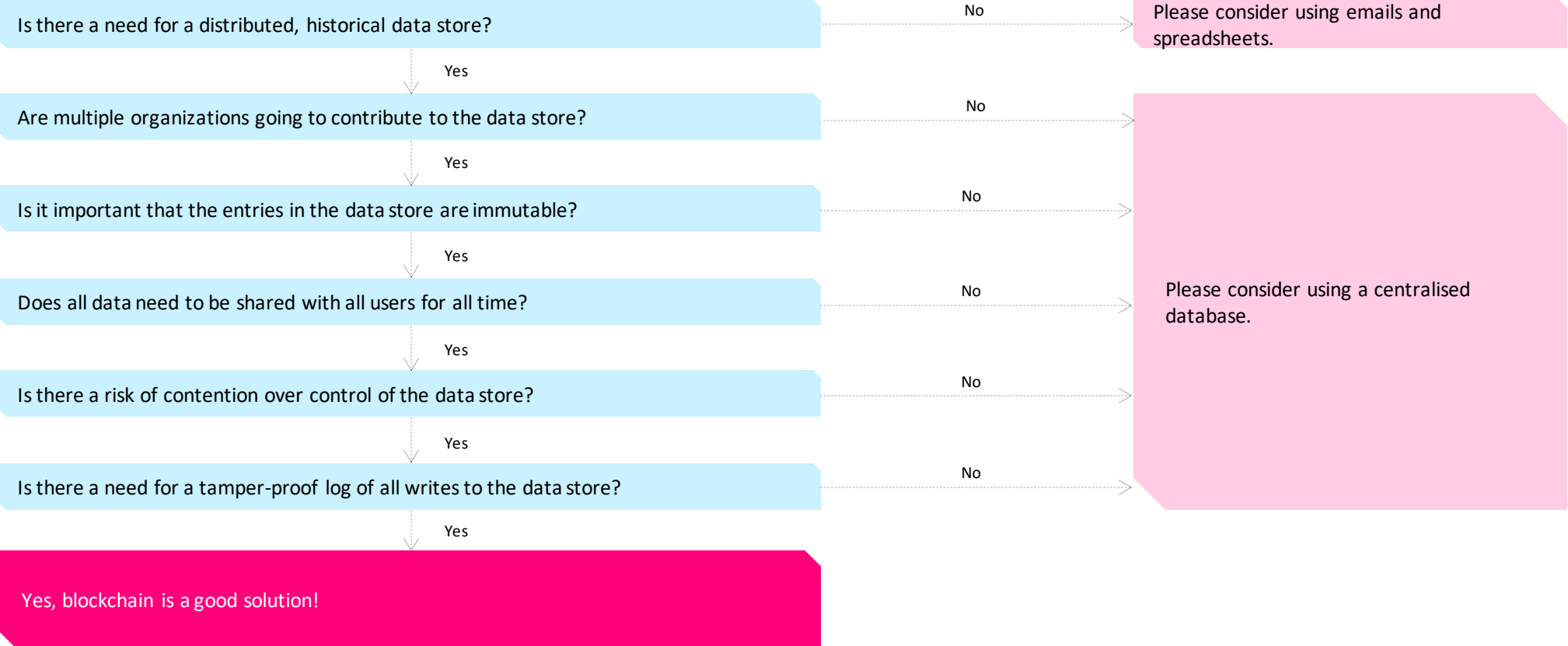
Resilience to bad faith actors

Even if one actor goes rogue, the collective truth persists. Blockchain prevents lies from taking hold.

No single point of failure. The infrastructure is resilient and resistant to cyberattacks.

Blockchain is not always the best solution for every problem.

While blockchain has many potential benefits, it's important to recognise that it's not always the best solution and evaluate whether blockchain is the best option for a particular use case. To consider using blockchain as a solution, certain conditions need to be met.

Is there a need for a distributed, historical data store? — No → Please consider using emails and spreadsheets.

Yes ↓

Are multiple organizations going to contribute to the data store? — No →

Yes ↓

Is it important that the entries in the data store are immutable? — No →

Yes ↓

Does all data need to be shared with all users for all time? — No → Please consider using a centralised database.

Yes ↓

Is there a risk of contention over control of the data store? — No →

Yes ↓

Is there a need for a tamper-proof log of all writes to the data store? — No →

Yes ↓

Yes, blockchain is a good solution!

Consider the opportunities & challenges that come with blockchain

Blockchain is ideal for technical, business, and societal needs due to its resilient and self-healing systems that can operate under duress, promote open technology platforms, and foster a competitive marketplace. However, there are challenges with interoperability, key management, and immature smart contracts.

Rather than trying to force-fit blockchain into every possible application, **EBSI uses blockchain and its strengths** (immutability, tamper-evidence, decentralisation) **where it makes sense**. This is also why EBSI does not put any personal data on-chain and tries to **minimise on-chain storage** in its use cases.

| Append-only | Tamper-proof & immutable | Decentralised | Blockchain's properties |

Use cases that support the public good through developing specifications in collaboration with the ecosystem & promoting adoption | How we use it

Values-driven, regulation-compliant and privacy-respecting | Our values
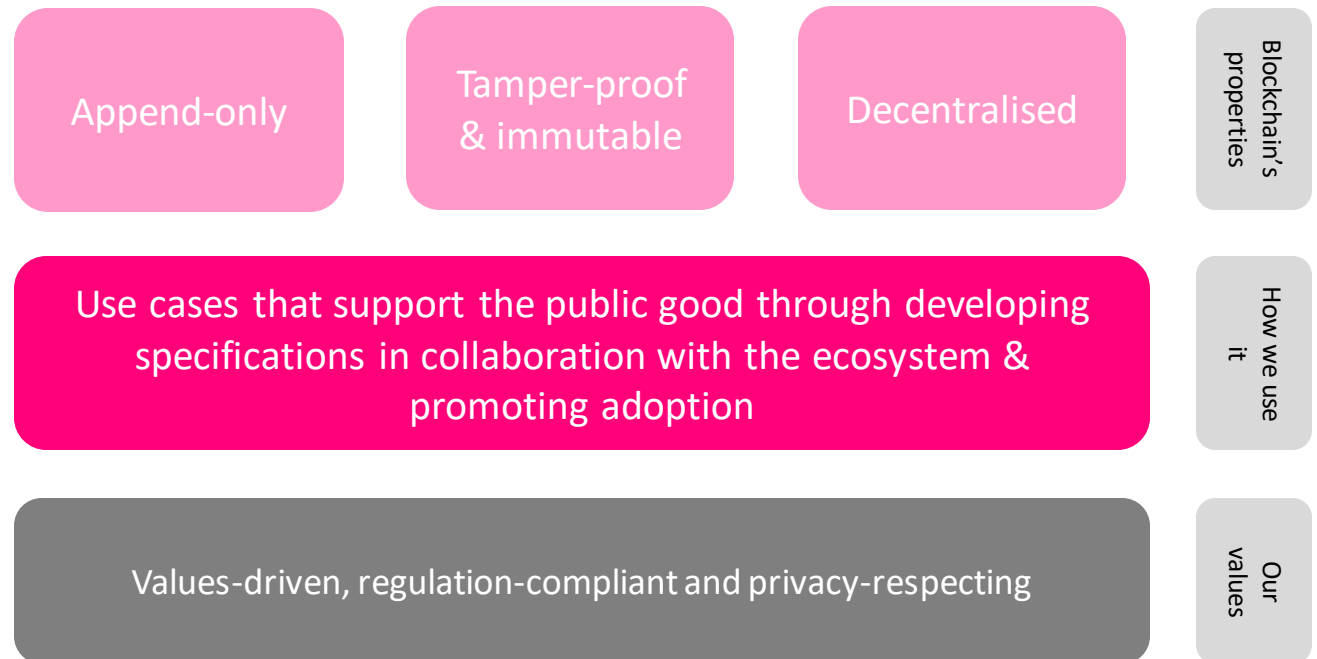
Busting Blockchain Myths

Three things you need to know!

01

EBSI is not a blockchain project.

We are a Web3 project, looking to find ways to use blockchain to support decentralised public services.

02

Blockchain is not just cryptocurrencies.

Blockchain is a decentralised ledger. It can serve many other purposes – a repository of trusted information, value chain management…

03

Blockchain doesn't have to be energy-consuming.

EBSI uses Proof of Authority, which consumes significantly less energy than Proof of Work or Proof of Stake.

EBSI is a blockchain technology being applied in the public sector

Our work extends beyond Verifiable Credentials. Here are some of our other use cases:

TRACK AND TRACE

Ensuring integrity and tracing data evolution or documents; monitoring products in supply chain through their digital passport

VERIFY INFORMATION

Giving control back to citizens when managing their credentials, e.g. diplomas or posting certificates for mobile workers linked to their digital identity, significantly reducing verification costs and improving authenticity trust

TRUST DATA EXCHANGE

Enhancing implementation of EU policy and compliance procedures between administrations e.g. asylum demand management or exchange of VAT number for import products

MANAGE IP

Facilitating right holders checking and management of intellectual property and fight against IP criminal activities

This is done notably through the establishment of electronic ledgers as **new qualified trust** services, as proposed in the **EU digital identity regulation**

EBSI is participating in the EU digital identity regulation and the creation of the **EU Digital Identity wallet**