From Blockchain to Cybersecurity and the EBSI

Miguel Pupo Correia

Universidade de Aveiro, 7/20/2022

Several pictures @CEF Digital

inesc-id.pt
Motivation: vast interest world-wide
Outline

1. Blockchain
2. Bitcoin and cryptocurrencies
3. Ethereum and smart contracts
4. Permissioned blockchains
5. European Blockchain Partnership
6. European Blockchain Services Infrastructure
7. EBSI Use Cases
8. EBSI Early Adopters & DE4A
1. Blockchain
Decentralization: who shall we trust?

**Client-Server**
trust a server/provider

**Peer-to-Peer**
trust the community

clients

peers

*decentralized*
“Blockchain” has two meanings

1) Data structure – append-only, chain of blocks of transactions – ledger
“Blockchain” has two meanings

2) **Distributed system** – set of Internet nodes/peers
   - They execute software and keep a *copy* of the chain
   - They run a consensus algorithm to agree on the next block to append to the data structure
1) **Data structure** – append-only, *chain* of blocks of transactions – *ledger*

- Block of transactions
- Block of transactions
- Block of transactions

2) **Distributed system** – set of Internet nodes/peers
   - They execute software and keep a copy of the chain
   - They run a consensus algorithm to agree on the next block to append to the data structure
Blockchain relevant properties

- **Availability & integrity** – works even if some nodes are compromised
- **Auditability** – the ledger is visible to “everyone”, so it can be verified
- **Immutability** – once a transaction is appended, it’s not removed
- **Decentralization** – properties above without trust on a third party – this is what is new in Blockchain!
2. Bitcoin and cryptocurrencies
Bitcoin

- Bitcoin is a **cryptocurrency**
  - ~= fiat currencies (e.g., Euro), but not issued by a central bank
  - It’s a **digital asset**

- **Who issues the coin? Who ensures we can trust it?**
  - A blockchain (system) that
  - that execute Bitcoin software
  - and contain copies of the blockchain (data structure)
  - Decentralized!
Bitcoin as a distributed system

REACHABLE BITCOIN NODES
Updated: Wed Sep 28 17:43:29 2022 WEST

14394 NODES

IPv4: -1.6% / IPv6: -1.9% / .onion: +2.8%

Top 10 countries with their respective number of reachable nodes are as follows.

<table>
<thead>
<tr>
<th>RANK</th>
<th>COUNTRY</th>
<th>NODES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>n/a</td>
<td>7426 (51.59%)</td>
</tr>
<tr>
<td>2</td>
<td>United States</td>
<td>1915 (13.30%)</td>
</tr>
<tr>
<td>3</td>
<td>Germany</td>
<td>1403 (9.75%)</td>
</tr>
<tr>
<td>4</td>
<td>France</td>
<td>431 (2.99%)</td>
</tr>
<tr>
<td>5</td>
<td>Netherlands</td>
<td>384 (2.67%)</td>
</tr>
<tr>
<td>6</td>
<td>Canada</td>
<td>313 (2.17%)</td>
</tr>
<tr>
<td>7</td>
<td>Finland</td>
<td>240 (1.67%)</td>
</tr>
</tbody>
</table>
Bitcoin’s service: currency transactions

- **Service** = transactions, transfers of currency between accounts
  - Currency is associated to accounts (~bank accounts)
  - Another service is no transactions: storage of value

- The nodes keep a chain that stores all transactions of bitcoins
  - Solves the **double payment** problem, i.e., avoids that the same account uses the same coin in two transactions
Bitcoin components – miners

Mini-cluster of GPUs

Bitcoin mining datacenter (China)
Bitcoin components – wallets

- **Wallets** – store account info & request money transactions
  - Store **private keys** corresponding to user accounts; randomness and secrecy of these keys ensure owning of the account
  - **Custodial wallets** – a third party stores / manages the private keys
  - **Non-custodial wallets** – the users stores / manages the private keys
Bitcoin – authenticity / integrity

- How to enforce only the owner can do transactions on his account(s)?
- Using a cryptographic scheme: digital signatures
  - Alice’s transactions take a signature created with the private key $K_r$ stored in her wallet
  - Bob can verify the signature with the public key $K_u$
  - Trudy can’t forge the signature (doesn’t have $K_r$)

users are anonymous
account address = hash($K_u$)
Bitcoin – consensus mechanism

• Appending transactions / blocks to the chain:
  – Collect transactions and create a block
  – Try to solve the cryptopuzzle and find a Proof-of-Work (PoW)
  – If it finds a PoW before receiving a block+valid_PoW:
    • Send the block+PoW to all miners
    • Otherwise stop and try again for the next block

• Creator of the winning block gets a reward: 6.25+…BTC today
  – Why is it a PoW? Requires many tries; consumes much energy
  – Difficulty set for 1 success every ~10 minutes worldwide (!)
Bitcoin is the first of many

Bitcoin is listed as #21,093 in Sep. 26, 2022

![Scryfall](https://scryfall.com/home)

### Top 10 Cryptocurrencies Based on Market Cap

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Price</th>
<th>1h %</th>
<th>24h %</th>
<th>7d %</th>
<th>Market Cap</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin BTC</td>
<td>$19,123.66</td>
<td>▽ 0.20%</td>
<td>▲ 1.04%</td>
<td>▼ 2.12%</td>
<td>$366,388,569,574</td>
</tr>
<tr>
<td>2</td>
<td>Ethereum ETH</td>
<td>$1,326.01</td>
<td>▽ 0.09%</td>
<td>▲ 2.52%</td>
<td>▼ 2.50%</td>
<td>$162,324,921,606</td>
</tr>
<tr>
<td>3</td>
<td>Tether USDT</td>
<td>$1</td>
<td>▽ 0.00%</td>
<td>▼ 0.01%</td>
<td>▼ 0.01%</td>
<td>$67,954,848,462</td>
</tr>
<tr>
<td>4</td>
<td>USD Coin USDC</td>
<td>$1.00</td>
<td>▲ 0.02%</td>
<td>▲ 0.01%</td>
<td>▲ 0.01%</td>
<td>$49,424,803,767</td>
</tr>
<tr>
<td>5</td>
<td>BNB BNB</td>
<td>$274.91</td>
<td>▲ 0.14%</td>
<td>▲ 0.14%</td>
<td>▲ 2.09%</td>
<td>$44,319,213,585</td>
</tr>
<tr>
<td>6</td>
<td>XRP XRP</td>
<td>$0.4723</td>
<td>▲ 0.20%</td>
<td>▼ 5.18%</td>
<td>▲ 22.81%</td>
<td>$23,535,006,108</td>
</tr>
<tr>
<td>7</td>
<td>Binance USD</td>
<td>$1.00</td>
<td>▲ 0.10%</td>
<td>▲ 0.05%</td>
<td>▲ 0.05%</td>
<td>$20,525,231,541</td>
</tr>
<tr>
<td>8</td>
<td>Cardano ADA</td>
<td>$0.4451</td>
<td>▼ 0.12%</td>
<td>▼ 0.11%</td>
<td>▼ 1.82%</td>
<td>$15,215,832,355</td>
</tr>
<tr>
<td>9</td>
<td>Solana SOL</td>
<td>$33.54</td>
<td>▼ 0.32%</td>
<td>▲ 3.10%</td>
<td>▲ 2.17%</td>
<td>$11,858,620,084</td>
</tr>
<tr>
<td>10</td>
<td>Dogecoin DOGE</td>
<td>$0.06093</td>
<td>▼ 0.14%</td>
<td>▼ 1.07%</td>
<td>▲ 4.18%</td>
<td>$8,083,967,494</td>
</tr>
</tbody>
</table>

Source: Coinmarketcap.com
3. Ethereum and smart contracts
• Why provide only one service – transactions?
Smart contracts

• Notion introduced by **Ethereum**
  – another blockchain that also implements a cryptocurrency (ether)

• **A smart contract** is:
  – Software, i.e., a program
  – Stored in the blockchain nodes
  – Executed in those blockchain nodes
  – May involve money transfer (in ether)
  – Not smart, not contracts
Blockchain black-box model

Properties of the Blockchain black-box:
- Availability & Integrity – provides service even if nodes fail / are corrupted
- Auditability – visible to all
- Immutability – appended data can’t be changed
- Decentralization – no central controller
Example: Non-Fungible Tokens (NFT)

- **NFT** – data that expresses ownership of a digital asset
  - An NFT is a token that is non-fungible, i.e., unique

- Implemented by a smart contract
  - Allows selling it and proving authenticity

*Beeple, “Everydays: the First 5000 Days”*
March 2021, Christie’s, $69,346,250
Decentralized Applications – DApps

- **DApp** – a decentralized application based on smart contract(s)
  - Frontend – typically Web (HTML, JavaScript, CSS,…) or a mobile App
  - Backend – smart contract(s)
    - They store some data, typically only metadata (e.g., hashes)
  - Data storage – P2P, e.g., IPFS
    - For storing the bulk of the data, e.g., documents
28.9.2022

4.5 million

The Punk 2924 was bought for 3,300 ETH ($4,451,633.94 USD)
4. Permissioned blockchains
Blockchain variants

- 2014: financial institutions formed consortium to explore Blockchain (R3)
  - Barclays, Credit Suisse, Goldman Sachs, J.P. Morgan, …; GS and JPM left

- Open blockchains were not what they needed:
  - Not interested in anonymous users
  - Not interested in showing the chain to the world
Blockchain variants

- **Permissionless** (i.e., no permission needed to be a member):
  - examples: Bitcoin and Ethereum
  - any server can enter, but to participate actively must provide proof-of-work
  - for public use

- **Permissioned** (i.e., permission needed):
  - servers must have permission; no proof-of-work needed
  - for consortium or private (?) use
  - participants already have some degree of trust among them, but want to simulate the services of a neutral third party
Consensus in permissioned blockchains

- PoW is really bad for consensus: probabilistic, forks, energy
- In permissioned blockchains the set of nodes is well-defined, which allows doing better
  - Problem solved since 1980 (Lamport et al.), fast since 1998 (Castro&Liskov)!
5. European Blockchain Partnership
The Declaration

DECLARATION

Cooperation on a European Blockchain Partnership

In order to harness the many opportunities of blockchain and avoid a fragmented approach, the signatories of this declaration agree to cooperate to establish a European Blockchain Partnership with a view to developing a blockchain infrastructure that can enhance value-based, trusted, user-centric digital services across borders within the Digital Single Market.

Done in Brussels on 10 April 2018 in one original in the English language
The Partnership today

- All EU Member States, Norway and Lichtenstein
CEF Building Blocks

<table>
<thead>
<tr>
<th>Building Blocks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Big Data Test Infrastructure</td>
<td>A free big data analytics sandbox to power your data-driven decision-making</td>
</tr>
<tr>
<td>eArchiving</td>
<td>Preserve, migrate and reuse data securely, according to European Standards</td>
</tr>
<tr>
<td>eInvoicing</td>
<td>Send and receive electronic invoices in line with the European Directive</td>
</tr>
<tr>
<td>Once Only Principle</td>
<td>Reduce administrative burden for individuals and businesses</td>
</tr>
<tr>
<td>Blockchain (EBSI)</td>
<td>Build the next generation of European Blockchain Services Infrastructure</td>
</tr>
<tr>
<td>eDelivery</td>
<td>Exchange electronic data and documents in an interoperable and secure way</td>
</tr>
<tr>
<td>eSignature</td>
<td>Create and verify electronic, paperless signatures</td>
</tr>
<tr>
<td>Context Broker</td>
<td>Make data-driven decisions in real time, at the right time</td>
</tr>
<tr>
<td>eID</td>
<td>Offer services capable of electronically identifying users from all across Europe</td>
</tr>
<tr>
<td>eTranslation</td>
<td>Enable multilingual public services and communication</td>
</tr>
</tbody>
</table>

ensures legal validity of electronic documents (eIDAS regulation)

for EU-level, cross-borders, applications
6. European Blockchain Services Infrastructure
EBSI

• “a network of distributed nodes across Europe that will deliver cross-border public services.”

• Permissioned blockchain – target is to have nodes in all the countries and the EC
EBSI
EBSI – technical details

A node is/contains:
- Minimum of 3 servers
- Hyperledger Besu and Hyperledger Fabric
- Core services: eIDAS bridge, management,…
- Smart contracts
- Use case software, business applications
1st target: public services

Gov Entity

Registers

Request

Issue & certify

Receive

Identity Birth Certificate Organic product certificate Health certificate Diploma

Time

Citizen/ Business

for EU-level, cross-borders, applications
How to share documents securely?

**Old model** – just in time evidence issuance

**New model** – verifiable credentials (stored in wallet)
Why is this interesting?

- **Data control by the citizen**
- **Enhanced selective data discloser**
- **Improved traceability of the origin and of the recipient**
- **Increased efficiency (no need of “just-in-time evidence issuance”)**
- **Reduced verification costs (once at scale)**
Example: trusted university diplomas

1. Workflow

Issuer

- Government
- University

User

- Citizen
- Wallet
- Legal entity

Verifier

- University
- Company

EBSI Services

EBSI Trusted registries

Blockchain

Events:

A. Request verifiable credential
B. Issue (validate) verifiable credential
C. Store evidence of issuance
D. Present verifiable credential
E. Check attributes of verifiable credential
F. Onboard on the DID registry
Example: trusted university diplomas

2. Obtaining the diploma with Wallet

**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. Connect to University platform
   - Initiate the action

2. Select Verifiable ID
   - Submit the request

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

4. Get notification
   - Accept the credential
   - Store in the wallet
Example: trusted university diplomas

3. Showing the diploma

- Eva initiates the application to the University of Rovira i Virgili
- Eva shares her Bachelor’s Diploma (VA) with the University of Rovira i Virgili
- The University of Rovira i Virgili verifies the Bachelor’s Diploma (VA) of Eva
- Eva enrolls for a Master’s Degree at the University of Rovira i Virgili
7. EBSI Use Cases
Main use cases

- **European Self-Sovereign Identity**
- **Diplomas management**
- **Document Traceability**
- **Trusted data sharing**

(Reserved for TAXUD’s Community at this stage)
Use case 1: ESSIF

- **Self-Sovereign Identity (SSI)** allows a person/organization:
  - Create an identity (DID – Decentralized Identifier)
  - Get Verifiable Credentials (VCs) with claims about himself
  - Selective disclosure: only the desired claims are shown to each entity (to each online service)
  - Cross-borders identification

- **European SSI Framework (ESSIF)**
  - Supported by the EBSI
  - Connection to eIDAS to generate and verify VCs
Use case 2: Diplomas

- The example we saw
- The objective is to create an ecosystem:
Use Case 3: Document Traceability

- **Register**: to record a data/document imprint in the EBSI
  - Imprint = hash + metadata of the data
  - Data = pdf, image, text message, action, etc.
- **Verify**: check authenticity/integrity of the data

2 operations:

1. Generate imprint on document (including metadata) and store hash in the blockchain. Metadata are stored off-chain.
2. Compute hash on document and compare hash of document to what is on the blockchain.
New Use Cases

- SME financing
- European social security number
- Asylum demand
Road Ahead

- EBSI v2 entering production
  - Launched ~April 2021
- Governance
- Regulatory/legal
8. EBSI Early adopters & DE4A
EBSI Early adopters programme

- Goal: jumpstart EBSI use
- Limitations:
  - Focus on current use cases (ESSIF, etc.)
  - Focus on pilots and production in public services
- Benefits:
  - Support and co-creation with EBSI experts
  - Open information sharing
DE4A

- H2020 EC project
  - Leader: ATOS  |  Participants: INESC-ID,…. (~22 partners)
- Goals
  - Contributing for the Digital Single Market, **simplifying cross-border exercise** by citizens and business
  - Simplifying migration towards European Digital Public Services co-delivered across borders
  - Full implementation of **once-only and digital-by-default principles**, **user centricity** and take into account new technologies (blockchain)
DE4A pilots

- **Studying Abroad**
  - Paperless procedures for students’ mobility:
  - Application for Higher Education
  - Applying for Study Grant
  - Diploma/Certificate/Studies, professional recognition - EBSI

- **Doing Business Abroad**
  - Meet business needs retrieving and keep up-to-date company data from authentic sources: Starting of business; Digital Annual Reports

- **Moving Abroad**
  - Enabling citizens’ mobility across EU enabling: Registering change of address; Civil Status Certificates; Retiring
Key Takeaways
Do you need a blockchain / DLT?

Real question is: what applications can benefit from decentralization and the other blockchain properties? Where is the added value?
Blockchains

• Cryptocurrencies vs Programmable blockchains (smart contracts)

• Permissionless/public blockchains vs Permissioned blockchains

• Blockchains provide integrity, availability, auditability, decentralization

• Many relevant subtopics: tokens/NFTs, identity/SSI, traceability,…
What the EBSI is (not)

- It is **not** a:
  - Testbed / a Blockchain infrastructure to develop products
- **It is** a:
  - European-level blockchain infrastructure
  - For cross-border applications
  - For public services, at least for now
  - Pioneer initiative: 1st Blockchain created by set of countries
- Initial set of use cases + early adopters program
Thank you

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

https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI