

A European Blockchain Services Infrastructure (EBSI): breve apresentação

1. Introdução: O Contexto da DLT na Europa

A European Blockchain Services Infrastructure (EBSI) é o projeto de infraestrutura de tecnologia de registo distribuído (Distributed Ledger Technology - DLT) de maior escala na União Europeia. Lançada em 2018 pelo European Blockchain Partnership (EBP), a EBSI não é uma rede blockchain comercial; é uma infraestrutura pública de interoperabilidade.

A sua génese responde a uma necessidade estratégica: permitir que os Estados-Membros, as instituições da UE e os cidadãos partilhem dados e serviços de forma segura, com o mesmo nível de fiabilidade de um sistema centralizado, mas com a resiliência e a transparência inerentes a um sistema descentralizado.

A EBSI funciona como uma camada de transporte de confiança (um middleware) que liga os sistemas existentes da administração pública.

Não substitui os seus sistemas: Se o Estado Português emitir um diploma ou uma identidade digital, os dados não "saltam" para uma rede de criptomoedas pública. Eles são "ancorados" (o seu hash ou impressão digital é registado) na rede privada da EBSI.

Isto permite que, por exemplo, uma universidade alemã consulte a rede da EBSI para validar um diploma emitido em Portugal. A "rede" onde tudo isto corre é, na verdade, um conjunto de servidores geridos pelos próprios países europeus, funcionando em conjunto através de protocolos padronizados pelo EBP.

A EBSI já atingiu a maturidade necessária para alojar serviços em ambiente de produção. Isto significa que a infraestrutura técnica (a rede de nós distribuídos pelos Estados-Membros) está

operacional e apta a suportar aplicações do mundo real.

Entidades públicas e instituições académicas já estão, neste momento, a integrar os seus sistemas com os serviços da EBSI.2.

O projeto não começou ontem, tendo passado por várias fases críticas desde 2018:

- **2018-2020 (Conceção e Testes Iniciais):** Definição da visão, criação do consórcio European Blockchain Partnership (EBP) e lançamento dos primeiros testes de conceito (PoCs).
- **2021-2023 (Pilotos e Estruturação):** Implementação de casos de uso específicos (como diplomas universitários e identidade digital) e expansão da rede de nós para cobrir a maioria dos Estados-Membros.
- **2023-2025 (Transição para Produção e Maturidade):** Foco na robustez, segurança de nível governamental e integração de novos validadores. Projetos como o EBSI-NE (um dos consórcios que trabalhou na expansão da rede) focaram-se especificamente em preparar a infraestrutura para uma utilização em larga escala e sustentável.
- **2026-2029 (Operacionalidade Plena):** A infraestrutura encontra-se atualmente a consolidar a adoção, servindo como a camada de confiança tecnológica para

os novos regulamentos europeus, incluindo o quadro da Identidade Digital Europeia (EUDI Wallet).

2. A Arquitetura Técnica: Para além da "Blockchain" convencional

A EBSI é estruturada sobre uma arquitetura de múltiplos níveis, desenhada para lidar com as complexidades da legislação europeia:

- **Modelo de Consenso (Besu e Hyperledger Fabric):**

Diferente das blockchains públicas (que usam Proof of Work ou Proof of Stake com validadores anónimos), a EBSI utiliza protocolos como o Hyperledger Besu e o Hyperledger Fabric. O consenso é alcançado através de mecanismos de Proof of Authority (PoA), onde a identidade dos validadores (os nós da rede) é conhecida e autorizada.

- **Por que escolheram isto?**

O Hyperledger Besu permite utilizar a linguagem de programação da Ethereum (Solidity) para criar os "contratos inteligentes" da EBSI. Isto significa que os desenvolvedores europeus podem tirar partido do vasto ecossistema de ferramentas de desenvolvimento da Ethereum, mas num ambiente privado, seguro e controlado pelo consórcio EBP (European Blockchain Partnership).

- **A "Rede":**

A rede em si é um sistema distribuído de nós espalhados pelos Estados-Membros (incluindo Portugal). Em vez de um consenso energético (como o Proof of Work da Ethereum pública), a EBSI utiliza o Proof of Authority (PoA), onde a confiança é depositada nas instituições governamentais que gerem os servidores.

- **O Nó da EBSI:**

Cada Estado-Membro opera o seu próprio conjunto de nós. Estes nós validam transações e mantêm uma cópia sincronizada do ledger. Esta arquitetura permite uma soberania de dados

distribuída, onde o controlo reside nos Estados-Membros.

- **Interoperabilidade via API Gateway:**

Para que as aplicações existentes (legados) nos governos nacionais se liguem à EBSI, esta utiliza uma camada de abstração (APIs RESTful). Isto permite que um sistema de registo predial ou um sistema de gestão académica nacional interaja com a blockchain sem necessidade de modificar a sua arquitetura interna de bases de dados SQL ou NoSQL.

- **Friendly:**

O Hyperledger Besu é um cliente Ethereum amigável para empresas, adequado tanto para redes blockchain públicas quanto privadas com permissão, e sendo compatível com a EVM (Ethereum Virtual Machine), significa que a EBSI pode suportar a implantação de contratos inteligentes escritos em Solidity, executáveis pela EVM de forma descentralizada.

Oferece uma interface de linha de comando e uma API JSON-RPC para gerenciamento de nós Ethereum, acessível via HTTP ou WebSocket. Ele suporta Pub/Sub e ferramentas comuns de desenvolvimento de contratos inteligentes, como Truffle, Remix e web3js. Mas, embora o Besu não suporte gerenciamento de chaves, o Ethsigner pode ser usado em conjunto com o Besu para acessar o keystore e assinar transações.

Licenciado sob a Apache 2.0 e escrito em Java, o Hyperledger Besu é um cliente Ethereum de código aberto mantido por uma ampla comunidade e pela Hyperledger Foundation. É amplamente utilizado em empresas para estabelecer redes blockchain públicas ou privadas e foi selecionado como a solução ideal para a iniciativa EBSI.

3. Governança e Conformidade: O desafio do RGPD

Um dos maiores diferenciais da EBSI face a projetos privados é a sua conformidade nativa com o RGPD (Regulamento Geral sobre a Proteção de Dados).

- **Zero-Knowledge Proofs (ZKP):**

A EBSI incorpora técnicas criptográficas que permitem provar a veracidade de uma informação (ex: "tenho mais de 18 anos" ou "sou residente na UE") sem revelar os dados brutos. Esta minimização de dados é a resposta direta ao princípio do "Direito ao Esquecimento".

- **Gestão de Identidade Distribuída (DID):**

A EBSI utiliza o modelo de Self-Sovereign Identity (SSI). O cidadão não é "proprietário" dos seus dados na blockchain, mas detém as chaves privadas que lhe permitem autorizar o acesso a credenciais verificáveis, armazenadas nas suas wallets digitais pessoais (ex: EUDI Wallet).

- **O Papel da Autoridade:**

A governança é exercida pelo EBP, que define as regras de adesão, os padrões de segurança e a atualização dos contratos inteligentes. Existe uma clara separação entre a camada de dados (que pode residir off-chain) e a camada de prova (que reside on-chain).

4. Pilares Funcionais e Casos de Uso Avançados

A EBSI operacionaliza-se através de "Use Cases" que visam resolver ineficiências transfronteiriças:

- **Credenciais Educacionais:**

Cria um ecossistema onde universidades emitem diplomas digitais assinados com chaves públicas. O empregador ou o Estado verifica a assinatura na blockchain em milissegundos, tornando as traduções juramentadas e autenticações notariais obsoletas.

- **Identidade Digital:**

Serve como o sistema de trust anchor para a carteira de identidade digital europeia, permitindo que cidadãos autenticuem a sua identidade em qualquer portal da administração pública na UE, sem depender de provedores de identidade centralizados e proprietários.

- **Registo Comercial (EBSI-CARGO):**

Facilita a verificação da existência de empresas entre países. Evita o envio de certidões permanentes em papel entre jurisdições, automatizando a conformidade em concursos públicos transfronteiriços.

- **Apoio a Documentos de Segurança:**

Utilizado para a gestão de licenças de condução, cartões de cidadão e outros documentos de segurança, impedindo a falsificação através da imutabilidade do ledger.

5. Integração com a Estratégia do Euro Digital e o Setor Financeiro

Embora a EBSI seja, primariamente, pública, a sua influência estende-se ao setor financeiro. O Banco Central Europeu (BCE) observa a EBSI como uma infraestrutura de referência para a gestão de provas de identidade e conformidade (KYC - Know Your Customer) necessárias para o Euro Digital. A capacidade da EBSI de certificar a identidade de um cidadão de forma segura e descentralizada é um pré-requisito fundamental para a adoção em massa de uma moeda digital de banco central.

6. Desafios de Implementação e Escalabilidade

Apesar do sucesso dos pilotos, existem lacunas que estão a ser endereçadas nesta fase de maturidade:

- **Standardização:**

A necessidade de harmonizar os formatos de dados entre 27 Estados-Membros é um desafio logístico imenso. Sem semântica comum, a tecnologia é inútil.

- **Adopção de "Legacy":**

A migração de sistemas públicos obsoletos para a arquitetura EBSI exige investimento e vontade política nos níveis regionais e municipais, e não apenas a nível central.

Segurança Quântica: Com o avanço da computação quântica, a UE está a investigar a transição para algoritmos de criptografia pós-quântica para garantir que as assinaturas digitais na EBSI se mantenham seguras nas próximas décadas.

7. Conclusão

A EBSI não é apenas um projeto técnico, mas um instrumento de política pública. Ela representa a transição de uma Europa fragmentada em "silos de dados" para um ecossistema de confiança digital onde a informação flui livremente, mas de forma soberana e controlada. Ao eliminar a necessidade de confiança num intermediário

central (nacional ou privado), a Europa cria uma vantagem competitiva inegável na economia digital global.

Este documento é uma base técnica. Para aprofundamento adicional, sugere-se a consulta dos relatórios técnicos de arquitetura disponibilizados no portal oficial da Comissão Europeia (EU Blockchain Observatory and Forum).

Espero que esta versão cubra a profundidade que procurava. Gostaria que eu focasse um destes pontos (por exemplo, a parte técnica de Zero-Knowledge Proofs ou a Governança do EBP) com ainda mais detalhe ou um estudo de caso específico?