zenbridge

What can Zenbridge do for EBSI?

Zenbridge is a microservice architecture for multi-DLT systems: it is powered by tiny computation units named ***VM-lets*** that **vastly improve scalability** by:

- Performing **sharding** and **caching**, from a dynamically allocated cloud of Kubernetes instances and IoT devices.
- Off-loading peaks of load on blockchain nodes by means of an **elastic computational distributed network** of authenticated micro-services
- Offering **multilayered interoperability** implemented by an array of existing blockchains

The **tiny footprint and extreme portability** of *VM-Lets* make them capable to run on any major OS, in a browser, on mobile phones, as well on embedded hardware and IoT, enabling point-to-point secured edge computing, and allowing anchoring EBSI to people as well as real world objects.

VM-Lets **extend the blockchain** capabilities by offering advanced cryptography and they can be programmed in a **human-like language** designed to be effortlessly read by non-programmers.

Zenbridge is **fully open source**, and will include hooks for existing closed-source technologies: the consortium believes that fostering an open source community is key for the success of EBSI and is fully committed to this vision.

How does Zenbridge work?

Zenroom is the open source component at the core of the *VM-lets*: it is the outcome of the flagship European *Horizon 2020* project *DECODE* (grant nr. 732546), it packs in a cryptographic virtual machine that enables blockchain interoperability, advanced cryptography and its smart-contracts can be programmed in the English-like language ***Zencode***.

VM-Lets also have a state and network manager built-in, that can be deployed in *Kubernetes* using *operators*, the deployment can be performed in an ad-hoc IDE that allows, on one hand, to prototype and test *Zencode* smart contracts, along with setting up the deployment strategy.

Zenroom can compute traditional cryptography, such as ECDSA signatures and hashing with multiple algorithms, along with advanced cryptography such as zero knowledge proof, multi-party computation, secret sharing, BLS and Schnorr signatures, all of this on a very wide range of cryptographic curves (currently 26 curves, including the secp256k1 and BLS12-381).

Along with its ecosystem, *Zenroom* contains capabilities to perform blockchain interoperability, currently implemented with *Ethereum*, *Hyperledger Sawtooth* and *Fabric*, *BigchainDB*, *Bitcoin*, *Cosmos*.

The whole consortium has undergone extensive work that resulted in the porting of *Zenroom* to *ARM*, *RISC-V* and *Cortex-M* devices, making edge-to-edge computing possible in a vast array of situations, allowing every hardware device to turn into a secure digital wallet, as well as allowing retrofitting to existing and/or legacy hardware (eg: point-of-sales, barcode scanners, passport readers, routers and access points, smart meters, etc.).

A compatibility layer with RFID chips has also been developed, making it possible to use real world objects or documents belonging to physical or legal persons as sources of trust.

bitcoin HYPERLEDGER SAWTOOTH BIGCHAIN DB HYPERLEDGER FABRIC ethereum

Enhanced scalability

Zenbridge's *VM-Lets* allow to perform some of the heavy computation, far away from the blockchain on smaller hardware, along with offering caching and sharding capabilities. The solution's multilayered blockchain stores a limited amount of data onto the "Level 0" EBSI blockchain, enabling the core blockchain to keep faster transaction speeds.

Zenbridge combines an ultra-light client that can turn all mobile devices, sensors etc into 'light nodes', leading to a highly robust, scalable and energy-efficient blockchain infrastructure

Energy efficiency

Superior energy efficiency is achieved in different ways:

- The underlying preferred blockchain, *BigchainDB*, is considerably less computation intensive than the competitors (*Ethereum*).
- The *VM-Lets* can run on less expensive, smaller, and less energy intensive hardware, as well as being retrofitted on existing hardware, thus cutting the emissions needed for production of hardware while performing extra cryptography on hardware that is already running, with neglectable extra energy consumption.
- Separating some of the heavy computation from the blockchain node to the *VM-Lets*, will allow to distribute the energy consumption onto areas that use green technology, without the need to set up a server farm.

Security

Zenbridge is based on confidential computing and trusted execution environments, located decentrally in various European data centers. These secure systems are the where the initial generation of cryptographic secrets is happening and where oura role-based management of all digital assets is based upon

Object identification / data processing

Zenbridge introduces self-certifying infrastructure on the machine, sensor or vehicle level and by offering full audit trail capabilities developed for the Swiss banking industry, we can make sure that transparency as well as GDPR-compliant data management is becoming a reality.

Zenbridge also allows to turn sensors, machines, vehicles or objects into trusted data sources, by adding or embedding crypto chips as a root of trust into devices. This enables highly secure end-to-end management of data and to trigger transactions based on trusted underlying (threshold) data

Robustness

The architecture of **Zenbridge** is resilient by design: it functions as a "computation distribution network" drawing on the elastic properties of scalable cloud setups and reacting to real-time demand of transactions. It is ready to hold peaks: its decentralized nature always provides a pathway to blockchains also in case of network disruptions.

Technical maturity

BigchainDB, is a widely used blockchain with a sizable European community behind it. The solution's core component, **Zenroom**, is deployed in production by city-wide pilots (DECODE project) and is widely tested and covered by benchmarks.

Interoperability

Zenbridge already supports interoperability with: **BigchainDB**, *Ethereum*, *Hyperledger Fabric* and *Sawtooth*, *Bitcoin*, *Cosmos*. Interoperability with other blockchains can be implemented with minimal efforts.

Use cases

Bring EBSI to life: enabling use cases in different industries with different legal and environmental circumstances will prove the robustness and performance of **Zenbridge** as a unique layer of trust proliferation

Cryptographic product passport for steel

Zenbridge allows to implement the digitalization of existing business processes, by offering advanced tools to create Digital Twins and securely manage trustworthy business process data. In the steel and metal industry, we build on existing regulatory requirements and show how Certificates of (material) Conformity can be digitized, notarized on the blockchain and linked with trustworthy physical oracles based on our machine identity solutions. Once this trust level has been established, **Zenbridge** can be built out into a data handling layer that adds e.g. energy consumption data during production, the kind of energy used as well as dates and location of production or transportation or re-purposing of used materials or components- Only such a trusted product passport regime will allow us to track the energy consumption, CO2 emissions and recycling or customs processes a product will have to undergo in the EU.

IPR for free and open source software licenses

The licensing notarization will provide time-based evidence of software licensing adopted on hardware devices, for a transparent and consistent record of their changes across time. This is **useful for makers and fab-labs** and all those people making and distributing hardware devices combining software publicly available.

This will be a step forward to notarize adoption of licensed software with a timestamp, because licensing may change in time and needs to be correctly recorded to reward all contributors. Also this will help us track use of open source software and claim the rights it grants to all its users: to study, modify, and redistribute modifications. We plan to leverage the **REUSE standard** by our associate organization the Free Software Foundation, a step forward to claim our legitimate **right to repair in Europe**.

The consortium

Dyne.org, **RIDDLE&CODE** and **InfoCert** have joined forces to power Europe with strong and durable technology for blockchain notarization. The consortium gathers unique know-how in open source community development, cryptography, security and identity management along with outstanding global market positioning.

Write enquiries to **info@dyne.org** or visit **https://zenroom.org/zenbridge/**

©2021 European Union and Dyne.org. This document is created by Dyne.org as contractor that is participating in the European Blockchain Pre-Commercial Procurement (PCP) under Framework Contract nº FW00110987. The European Blockchain PCP aims to prepare for the future evolution of the European Blockchain Service Infrastructure (EBSI). All rights reserved