GENTE

Data Privacy and Smart Language ABC

D7.3

SUMMARY

This document develops a detailed description of the Smart Contract tools provided by the PROSUME Technology.

Website genteproject.com

Contact hello@genteproject.com

Impressum

Internal Reference

Deliverable No.	D 7.3 (2024)
Deliverable Name	Data privacy and Smart Language ABC
Lead Participant	PROSUME
Work Package No.	7
Task No. & Name	T 7.3 Development and implementation of asset tokenization tools and Smart Contracts for Green Energy Communities
Document (File)	GENTE-D7.3-Data privacy and Smart Language ABC-PU-P_R1
Issue (Save) Date	R0: 2024-08-27 R1: 2025-01-24

Document status

	Date	Person(s)	Organisation
Authors	2024-08-22	Alessia Borge, Alex D'Elia	PROSUME
Verification by	R0: 2024-08-26 R1: 2025-01-24	Peter Allenspach Josephine Harris	HSLU HSLU
Approval by	R1: 2025-01-24	Roman Lötscher	HSLU

Versions

	Date	
Version R0	2024-08-27	First release version - consortium only
Version R1	2025-01-24	Removal of sensitive content to enable report to be released to the public

Document sensitivity

☐	**Not Sensitive**	Contains only factual or background information; contains no new or additional analysis, recommendations or policy-relevant statements
☐	**Moderately Sensitive**	Contains some analysis or interpretation of results; contains no recommendations or policy-relevant statements
x	**Sensitive**	Contains analysis or interpretation of results with policy-relevance and/or recommendations or policy-relevant statements
☐	**Highly Sensitive Confidential**	Contains significant analysis or interpretation of results with major policy-relevance or implications, contains extensive recommendations or policy-relevant statements, and/or contain policy-prescriptive statements. This sensitivity requires SB decision.

Disclaimer

About ERA-Net Smart Energy Systems

ERA-Net Smart Energy Systems (ERA-Net SES) is a transnational joint programming platform of 30 national and regional funding partners for initiating co-creation and promoting energy system innovation. The network of owners and managers of national and regional public funding programs along the innovation chain provides a sustainable and service oriented joint programming platform to finance projects in thematic areas like Smart Power Grids, Regional and Local Energy Systems, Heating and Cooling Networks, Digital Energy and Smart Services, etc.

Co-creating with partners that help to understand the needs of relevant stakeholders, we team up with intermediaries to provide an innovation ecosystem supporting consortia for research, innovation, technical development, piloting and demonstration activities. These co-operations pave the way towards implementation in real-life environments and market introduction.

Beyond that, ERA-Net SES provides a Knowledge Community, involving key demo projects and experts from all over Europe, to facilitate learning between projects and programs from the local level up to the European level.

www.eranet-smartenergysystems.eu

Abstract

This report explores the use of blockchain technology in achieving the Sustainable Development Goals (SDGs) and highlights its potential risks if misapplied. While blockchain is valuable for decentralization, excessive reliance on it can lead to technocratic solutions that overlook the real needs of the SDGs. Self-Sovereign Identity (SSI), privacy control, and human-readable languages are proposed as mechanisms to emphasize the technology's limitations.

We hereby discuss Europe's leadership in SSI and sustainability, particularly through the EU's eIDAS directive, and how Distributed Ledger Technologies (DLTs) can support clean energy production and sustainability initiatives. However, SSI emphasizes the need for careful data management, privacy protection, and GDPR compliance, especially in decentralized environments like Local Energy Communities (LECs).

To ensure privacy and interoperability, innovative technologies like Zero-Knowledge Proof (ZKP) and Multi-Party Computation (MPC) are considered. The Zenroom software stack, chosen for its adaptability and cryptographic strength, was implemented to provide a scalable and trustworthy layer of trust for the GENTE project, enabling secure smart contract execution and data certification across multiple blockchain networks. The report details the deployment of these technologies in energy management, showcasing their potential in optimizing energy use within LECs while maintaining strict confidentiality and interoperability standards. The integration of these tools illustrates the necessity of balancing technological innovation with privacy, legal compliance, and real-world applicability in achieving sustainable development.

Table of Contents

Impressum 2
Abstract 4
List of Figures 6
List of Abbreviations 7
1. Introduction 8
2. Building the Layer of Trust 10
3. Technology Used 12
4. Smart Contracts 16
5. Toolkit for Energy Communities 25
Conclusion 27
References 28

List of Figures

Figure 1 - Blockchain and DLTs applied to energy infrastructure.....9

Figure 2 - Zenroom interaction with GENTE Platform.....13

Figure 3 - Zenroom applied Business Logic in a settlement procedure.....15

Figure 4 - A Flow diagram of a Smart Contract related information exchange.....16

Figure 5 - Zenchain, DB, Blockchain interaction diagram within PROSUME Platform.....18

Figure 6 - Smart Contract PROSUME API screenshot.....19

Figure 7 - DID Document registration flow.....23

Figure 8 - DID Document revocation process.....24

Figure 9 - Zenroom interaction and positioning in GENTE Platform.....26

List of Abbreviations

API	Application Programming Interface
BDD	Behaviour Driven Development
CELL	Collaborative Energy Living Lab
DB	Database
DID	Decentralised IDentifiers
DLT	Distributed Ledger Technology
DSL	Domain Specific Language
DSO	Distribution System Operator
ER	Exploitable Results
ETH	Ethereum Layer-1 Blockchain
EV	Electric Vehicle
GDPR	General Data Protection Regulation
HSLU	Lucerne University of Applied Sciences and Arts
IDE	Integrated Development Environment
IoT	Internet of Things
KPI	Key Performance Indicators
LEC	Local Energy Community
MQTT	Message Queue Telemetry Transport
MPC	Multi-Party Computation
NFT	Non-Fungible Token
PV	Photovoltaics
SDG	Sustainable Development Goals
SSI	Self Sovereign Identity
UC	Use case
WASM	Web Assembly
ZKP	Zero-Knowledge Proof

1. Introduction

The ERANET GENTE project aims to develop a distributed governance toolbox for local energy communities (LECs). This toolbox includes advanced digital technologies such as the internet of things (IoT), distributed ledger technology (DLT), edge processing and artificial intelligence (AI) for autonomous energy resource management within and across LECs and for flexibility provisions to energy networks.

This document presents the tools that PROSUME adopted, developed and customized for the specific purpose of the GENTE project. With the intention to build a strong cryptographic layer of trust implementing also blockchain technology, but at the same time providing and higher level of interoperability and modularity, PROSUME focused its activities on properly picking open source tools that can easily be adapted to the context of LECs ensuring the modularity requested for the GENTE toolbox.

Blockchain technology is often seen as a solution for all things related to decentralization [i]. However, if used improperly, it can threaten the Sustainable Development Goals (SDGs) by shifting the focus from the specific goals to a technocratic solution, rather than addressing the actual needs and problems.

Self-Sovereign Identity (SSI), privacy control, and human-understandable languages can help highlight the limitations of blockchain. While blockchain is a powerful tool for decentralization, not everything should be transparent and immutable, and not all problems can be solved by technology alone. Europe is leading the way in SSI and sustainability [ii], with the EU's eIDAS directive providing guidance to address certain issues [iii].

Distributed Ledger Technologies (DLTs) can offer transparent and trustworthy support for promoting clean energy production and sustainability plans while certifying renewable sources. They also incentivize affordable energy provision and increase awareness of consumption [iv], thus accelerating the transition to a more sustainable and conscious society with stronger impact development.

To achieve transparency and awareness in energy consumption and production, data acquisition and handling must be automated, certified, and properly linked to its source(s) but also so that it can be analyzed and evaluated by all stakeholders involved. This must be done while respecting privacy and ensuring that sensitive information is not publicly disclosed. Privacy and confidentiality constraints, particularly those related to General Data Protection Regulation (GDPR) compliance, are crucial to consider. Legally, it may be sufficient to demonstrate that a participant benefits from sharing their data to justify the exclusion of GDPR application. However, this should not be considered satisfactory. Instead, application proponents must take effective measures to ensure confidential data management. In this context, distributed identity management must be handled carefully, as it is essential for all other applications.

A balance should be found between data that can be recorded on a distributed ledger and data that must not be recorded. For this reason, PROSUME experts have considered implementing innovative technologies like Zero-Knowledge Proof (ZKP) and Multi-Party Computation (MPC) in this project.

Our goal is to provide trustworthy and scalable services that can be easily integrated into the main GENTE platform, ensuring privacy and confidentiality while preserving the benefits of strong cryptographic tools and interoperability between services and blockchains.

The implementation described in the following chapters tries to tackle the challenges of energy management within Local Energy Communities (LECs) by offering tools designed to calculate rewards based on patterns of energy consumption and production, all while maintaining privacy and security.

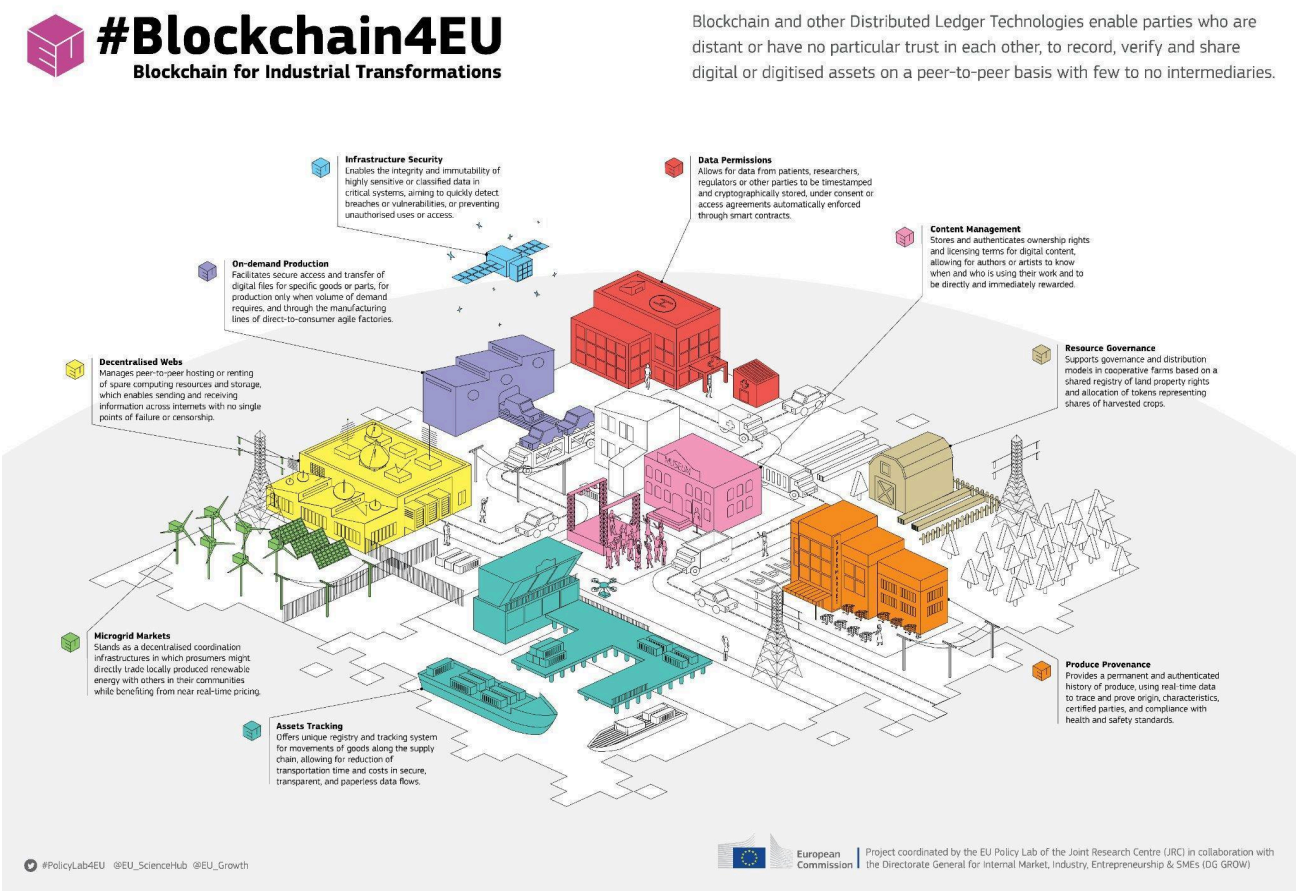

Figure 1 - Blockchain and DLTs applied to energy infrastructure

2. Building the Layer of Trust

Blockchains are still under development and rapidly changing and adapting. To provide an interoperability layer of trust to the GENTE project and to enable an open approach to further development of tools we scouted and implemented the Zenroom software stack developed by the Dyne foundation. The software is a result of various successful EU funded projects. The Zenroom Stack is a powerful multi platform technology that can be stripped into many microservices adapted to the specific use cases.

In this project, we implemented software tools that utilize a human-readable smart language to help us develop smart contracts tailored to the specific requirements of energy communities. The first type of services we can provide with these tools are:

1. computing of rewards for users who use (or do not use) energy when requested by the grid operator
2. computing of rewards for users who consume less energy or produce more energy in specific time frames depending on the performance request as demanded by the local energy provider

Thanks to the specifically implemented software stack, the functionalities provided by the smart contracts can be listed as:

1. reading data stored in multiple sources and organised in an ontology bypassing specific protocol limitations
2. computing rewards for an arbitrary number of users without depending on time constraints or limits imposed by the databases or blockchain technology in use
3. recording data in the blockchain of choice for certification purposes
4. transacting tokens into other blockchains of choice
5. strong cryptographic layer implementing various elliptic curves
6. smart contracts easily made in human understandable language (plain English)

The smart contracts developed depend on the specific interaction between the services provided by the platform. They can easily be adapted for future purposes as they are decoupled from the blockchain and executed by the finite state virtual machine of Zenroom, providing a higher layer of interoperability and trust, which is strongly needed in complex environments like Local Energy Community (LEC) projects.

LECs are legal entities that effectively control their members, are locally rooted and whose goals must be to provide environmental, economic and social benefits rather than only financial profits[1].

Privacy and confidentiality among community members are fundamental principles. It is essential to ensure effective communication between the different stakeholders. However, the information that is

[1] **Clean Energy for All Europeans Package**: This legislative package, introduced in 2019, established the concepts of Renewable Energy Communities (RECs) and Citizen Energy Communities (CECs).
https://energy.ec.europa.eu/topics/markets-and-consumers/energy-consumers-and-prosumers/energy-communities_en

disclosed must be limited to the greatest extent possible. This limitation is necessary to protect individual privacy while still allowing for the execution of all automated processes. These processes should operate without requiring human interaction, particularly in settlement procedures. Despite this automation, it is crucial that the information remains accessible for auditability requests. This balance ensures both the integrity and transparency of the system, fostering trust among community members.

The benefits that an LEC can provide to its members such as controlled energy pricing, availability of energy resources and exchange of value amongst them, are promising, but there are still many challenges in operating them. First, it is uncertain how to design an LEC that achieves economic, self-dependence, or environmental goals. Besides, LECs do not know which composition of users is more suitable for their interests. Moreover, regulations are constantly changing, giving rise to various energy allocation strategies that need evaluation to optimise the LEC's performance [v].

Blockchain interoperability is a crucial feature that allows different blockchain networks to communicate and exchange data, facilitating the transfer of tokens or assets across various distributed ledger technologies. This capability is essential for the development of cross-chain decentralized applications and enables a more decentralized and collaborative ecosystem. The technology we implemented for GENTE and described in the following chapter has been chosen exactly for these reasons. The objectives we wanted to achieve are those of providing technological solutions that can easily be adopted for the development of energy communities, avoiding bottlenecks and lock-in effects that can result from the implementation of a highly verticalized technology stack that could easily be disrupted by newly developed solutions, without giving up to interoperability features that can foster rapid development of LEC models.

3. Technology Used

The technology used to write the smart contracts implemented by PROSUME within the mobile app developed in React Native is called Zenroom and it is described in the following paragraphs [vi].

Zenroom is a tool that offers significant blockchain interoperability, supporting multiple blockchain networks such as Bitcoin, Ethereum, Fabric, Sawtooth, Iota, and Planetmint. With Zenroom, a single smart contract can operate across these ledgers, enabling functionalities like Non-Fungible Tokens (NFT) and token transfers, as well as multilayer and multi-source data notarization. This interoperability feature has been instrumental in the development of Zenswarm, a blockchain oracle that facilitates communication between blockchains. Zenswarm oracles leverage Zenroom's capabilities to perform a wide range of cryptographic operations and data exchanges, enhancing the interoperability between different blockchain networks. These oracles can listen to transactions on one blockchain and produce corresponding actions on others, bridging the gap between isolated blockchain environments. This interoperability is vital for creating innovative blockchain-enabled products and services that utilize the strengths of multiple blockchain networks simultaneously.

Zenroom is a tiny secure execution environment written in C (a lightweight and ultra-portable crypto virtual machine) that runs on any platform (Linux, Windows, Mac, Android, iOS) on any architecture (X86/64, ARM32/64 Cortex-M) as well as in the browser (via WASM). The Zenroom stack allows you to spin-up microservices that can authenticate, sign and verify, encrypt and decrypt data via execution of human-readable scripts, for all sorts of applications. It helps to implement cryptography keeping it simple, understandable, and maintainable.

Zencode is a domain-specific language (DSL) designed to be accessible to non-programmers. It is based on Gherkin, a behavior-driven development (BDD) language, allowing users to write code with minimal training. Zencode can be developed using Apiroom, an online integrated development environment (IDE) that offers features like auto-complete, statement examples, and comprehensive documentation. Zenroom supports multiple programming languages through bindings and provides a single API to execute Zencode, returning outputs as buffers. The system is modular, functioning as a collection of microservices with minimal dependencies.

Apiroom facilitates the creation of Dockerfiles and installers for these microservices, all programmed using Zencode. Zenroom supports advanced cryptographic operations, including signing and verifying with ECDSA, EdDSA, and Schnorr [vii] on popular elliptic curves such as SECP256K1, BLS381 [viii], and ED25519 [ix]. It also handles zero-knowledge proofs, multi-party computation, W3C-DID, W3C-VC (W3C Verifiable Credentials), and quantum-proof cryptography, making it suitable for next-generation cryptographic applications[2].

Since our contribution is centered on delivering the smart contract layer and certifying data stored on a blockchain with a focus on privacy and security, the responsibility for how and from where the data is collected does not fall under our purview. For this reason, we designed the connection of our tools to

[2] W3C DID compliancy: https://dyne.org/W3C-DID/

the systems developed by the other GENTE partners with modularity and simplicity in mind, keeping specific interaction separated yet easily available and deployable in case of changes and updates in the overall architecture [x].

This choice has proven to be valuable as the partner Reengen had to leave the project and our main interface to HSLU changed in time. The tools being implemented will help in the process of future updates and changes. Demo data was used to complete our work in building a smart contract feature and an oracle for the Decentralized IDentifiers (DID) provisioning. This gave us the opportunity to complete the solution and structure the system in a way that allows easy updates and changes in our modules and in the communication with the main platform, without the need to reprogram the system or develop from scratch a new solution.

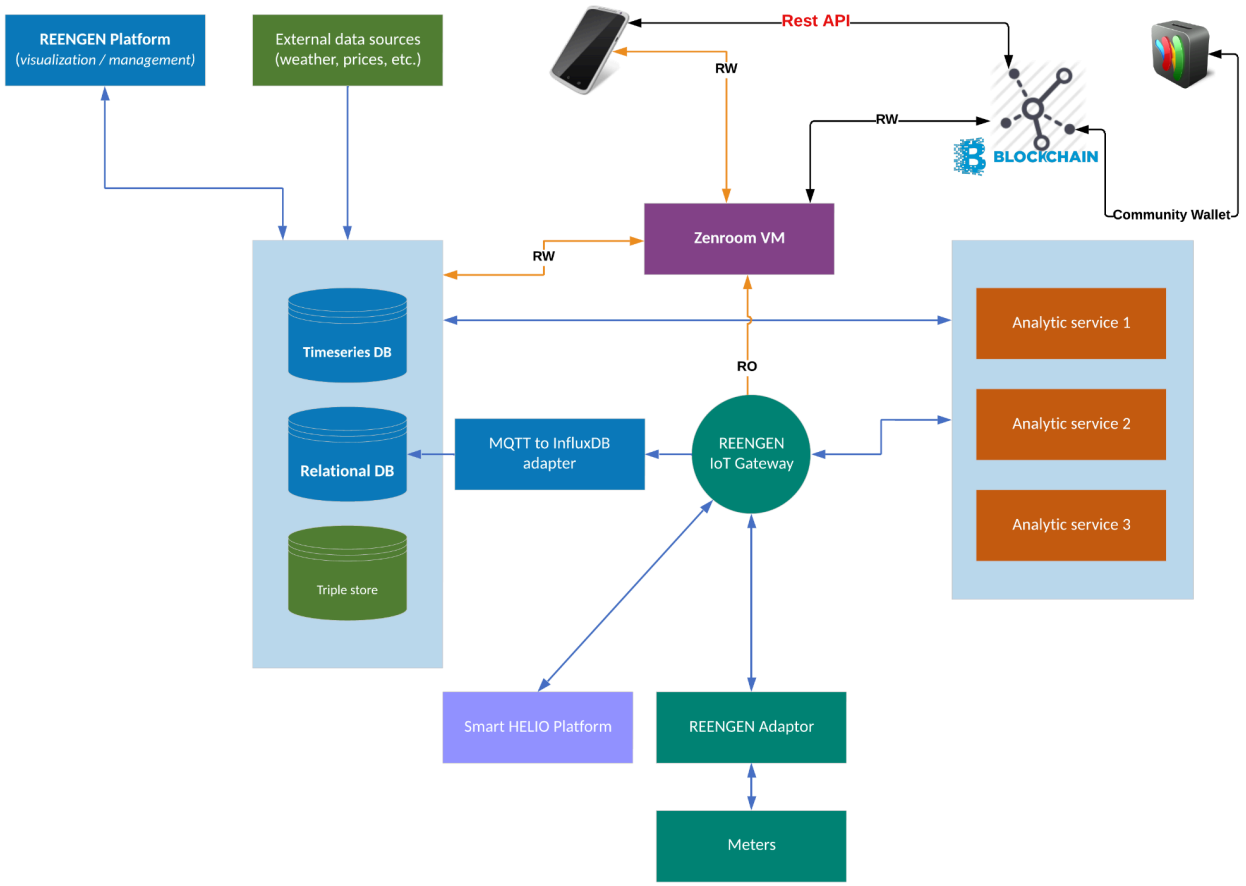

Figure 2 - Zenroom interaction with GENTE Platform

In the above figure, we have outlined the architecture design we used to interact with the main GENTE platform.

Within this architecture, the mobile application was developed without the need to have access to the Reengen platform. The Zenroom Virtual Machine (VM) acts as middleware that can read data from the

gateways or from the main databases (be that a relational database and a timeseries database), and write data to external databases or blockchains of choice.

The development of tools for blockchain interoperability is guided by principles similar to those used in standard Order Management Systems (OMS) in stock market exchanges. These tools aim to provide participants with the ability to establish market and limit orders, recording these transactions as immutable records on a distributed ledger. This approach circumvents the limitations of blockchain technology, such as the constraints on handling heavy data flows during quarterly settlement procedures.

To achieve a "digital single market," smart contracts are executed off-chain within a distributed system based on specific attributes. Order Management Systems are crucial in financial markets for executing and tracking securities orders efficiently. They facilitate real-time monitoring and compliance, helping firms manage orders and asset allocations effectively. Zenroom extends these principles to blockchain interoperability, enabling operations across multiple blockchains, including Bitcoin, Ethereum, and others. This allows for functionalities like NFT and token transfers, as well as multilayer data notarization, without being hindered by blockchain's inherent limitations. By executing smart contracts off-chain, Zenroom enhances the scalability and efficiency of blockchain interactions. This off-chain execution is supported by decentralized oracle networks, which connect blockchains to external data sources securely. Such a system not only maintains the integrity of transactions but also expands the computational capabilities of blockchains, allowing for more complex and scalable applications. This approach is exemplified in the development of Zenswarm, a blockchain oracle that facilitates interoperability across different blockchain networks.

Given the specific attributes, it is important to have the order booking logic separated from the DLT system and the Accounting systems who might inherit attributes from other systems and run at different locations, times, constraints.

The Zencode encoded Smart Contracts are useful to enable a modularized approach and provide a higher level of interoperability of complex systems. The logics adopted are described in the following figure:

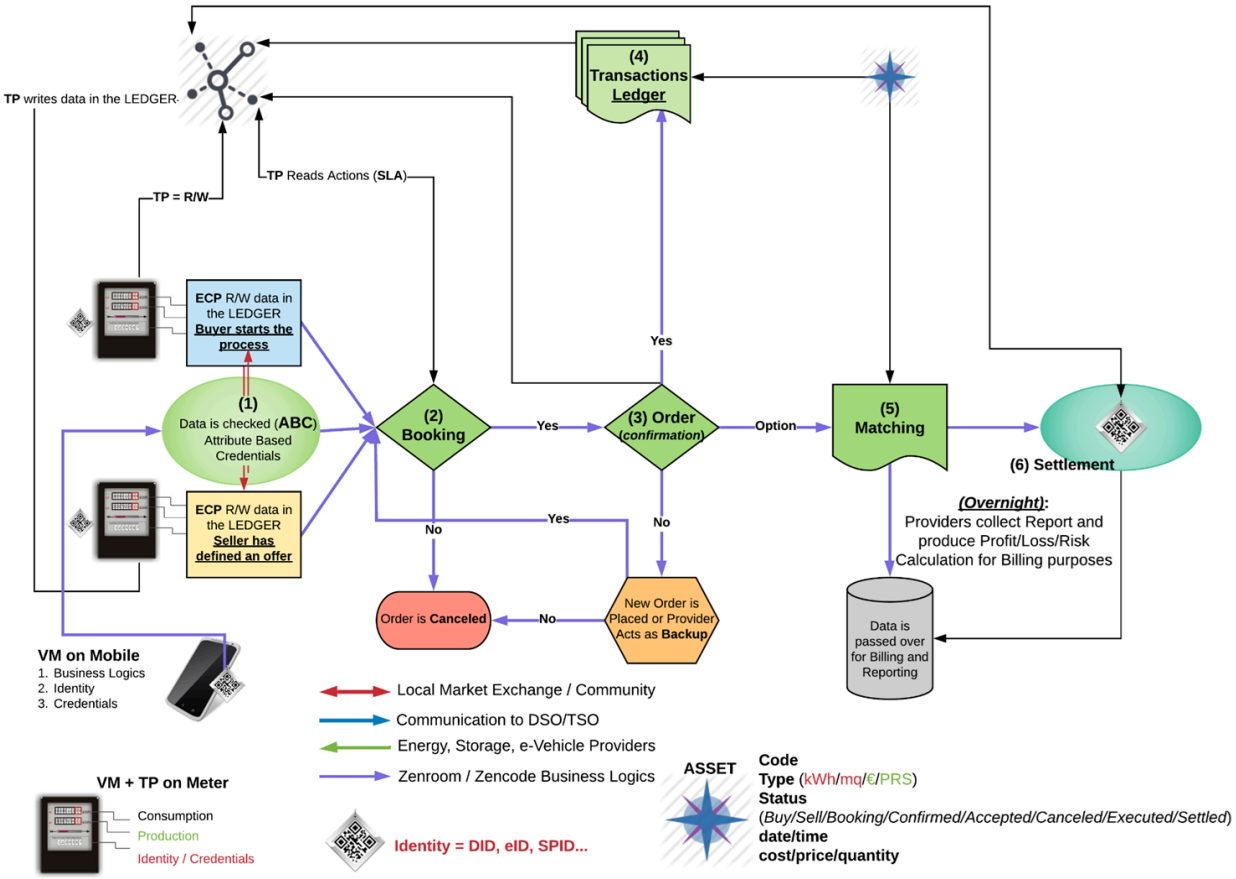

Figure 3 - Zenroom applied Business Logic in a settlement procedure

Considering the above applied logic, we have separated our piece of software and enclosed it in the Zenroom VM which can be executed independently from the other components of the GENTE Platform.

The smart contracts are implemented within the Zenroom VM and their architecture and development are described in the following section.

4. Smart Contracts

The technology adopted by PROSUME for the GENTE project takes a different approach that enables greater flexibility and makes the system more interoperable with different types of architectures and technologies. The following architecture diagram illustrates the deployed system which is composed of several interconnected components:

1. PROSUME Platform
2. Authorities/3rd Parties
3. REST API
4. Zenchain
5. Zencode Smart Contracts
6. Schedulers/Importer
7. Database (mariaDB)
8. Fabric Node
9. ETH Node (optional)

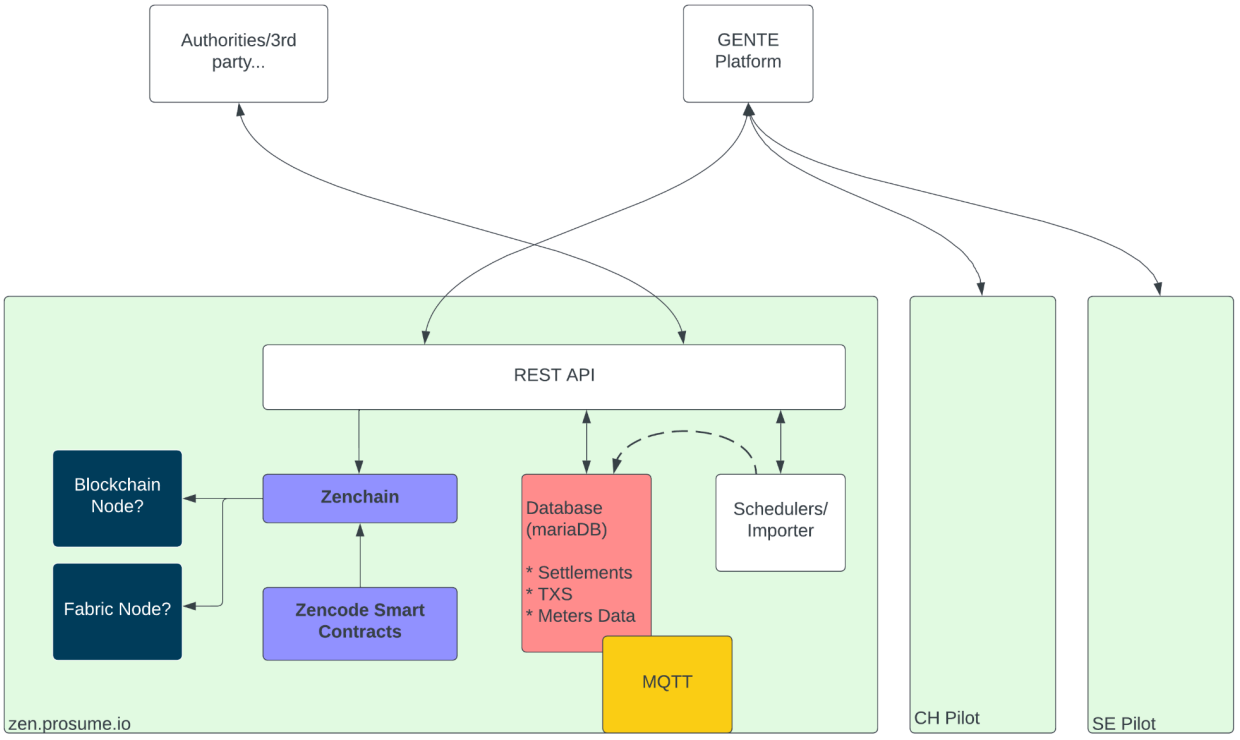

Figure 4 - A Flow diagram of a Smart Contract related information exchange

Authorities or third-party entities and the PROSUME Platform interact with the system through the REST API. The data or commands received from these external entities are processed and potentially affect

various components of the system, such as the **database**, **schedulers/importer**, and mainly the **Zenroom** related components.

The **PROSUME Platform** sends data or receives information related to system operations, which can involve updates on household-related information or metered data.

The **REST API** acts as the central communication hub for all external and internal interactions:

- It enables integration with the external platform, authorities, third parties, and regional pilots.
- Internally, it coordinates interactions between the database, the Zenroom system (*Zenchain, Zencode Smart Contracts*), blockchain components, and other modules.

Zenchain is the cryptographic layer that handles transactions and settlements, either through databases or blockchains:

- **Zencode Smart Contracts** are executed within Zenchain to manage various operations.
- Both components interact closely with the PROSUME **Fabric Node** (*and eventually an ETH Node*), which are potential Blockchain Networks (Ethereum and Hyperledger). These nodes represent potential blockchain networks that Zenchain can connect to for executing smart contracts and recording transactions.

The exact choice of the blockchain network might depend on the specific use case or configuration.

The **database** stores critical information for temporary management to simplify interaction with the various GENTE partners working on the project's development.

The **scheduler/importer**:

- handles scheduled tasks and data import operations.
- ensures that data from meters and other sources are regularly updated in the database.

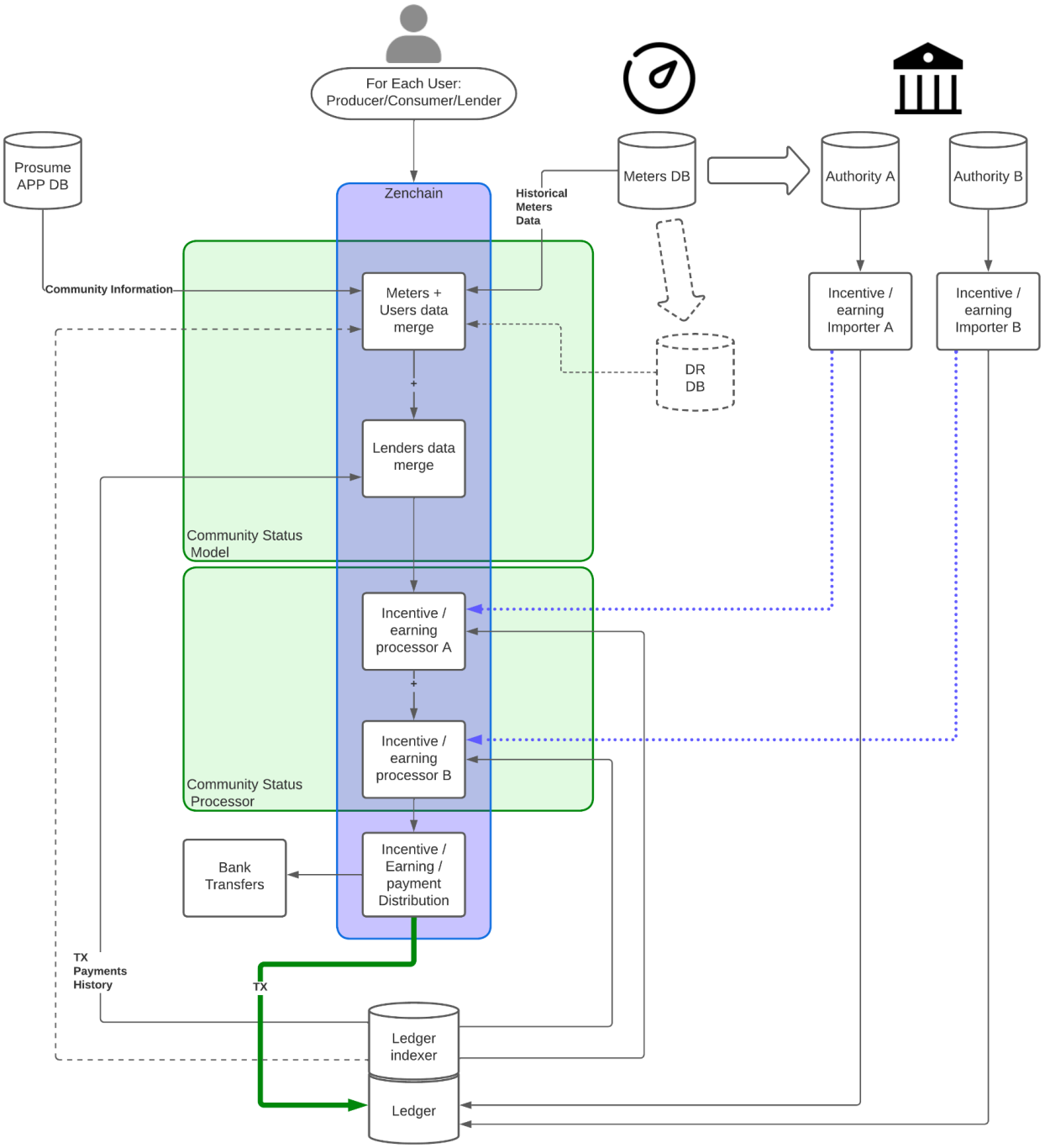

Figure 5 - Zenchain, DB, Blockchain interaction diagram within PROSUME Platform

Considering the architecture shown in the above figure, the main objective here is to enable off-chain smart contract execution, ensuring interoperability with other specific services, like the optimization of LEC performance, based on forecasted consumption and production information.

Smart contracts are not bound to a specific blockchain of choice: rather they are being enclosed in the VM delivered by the PROSUME API, installed on a server dedicated to the project specific use cases.

The Smart Contracts are written in Zencode Business Driven Language and elaborated in the Zenroom Virtual Machine. They are decoupled from the visualisation platform of choice. In this specific case, the contracts are being executed on a server that acts as a middle layer, to simplify interoperation with the data collection and forecasting services, thus providing a high layer of flexibility and enabling future interoperability with new automated remuneration processes and blockchain platforms that might be added by a third-party provider.

The result is a micro service, provided through several meters, gateways, and the PROSUME Platform and app, that performs a simple reward mechanism following specific presets which are defined based on the consumption and production habits of the demo data.

The following image shows a screenshot of the executed smart contract from the micro service:

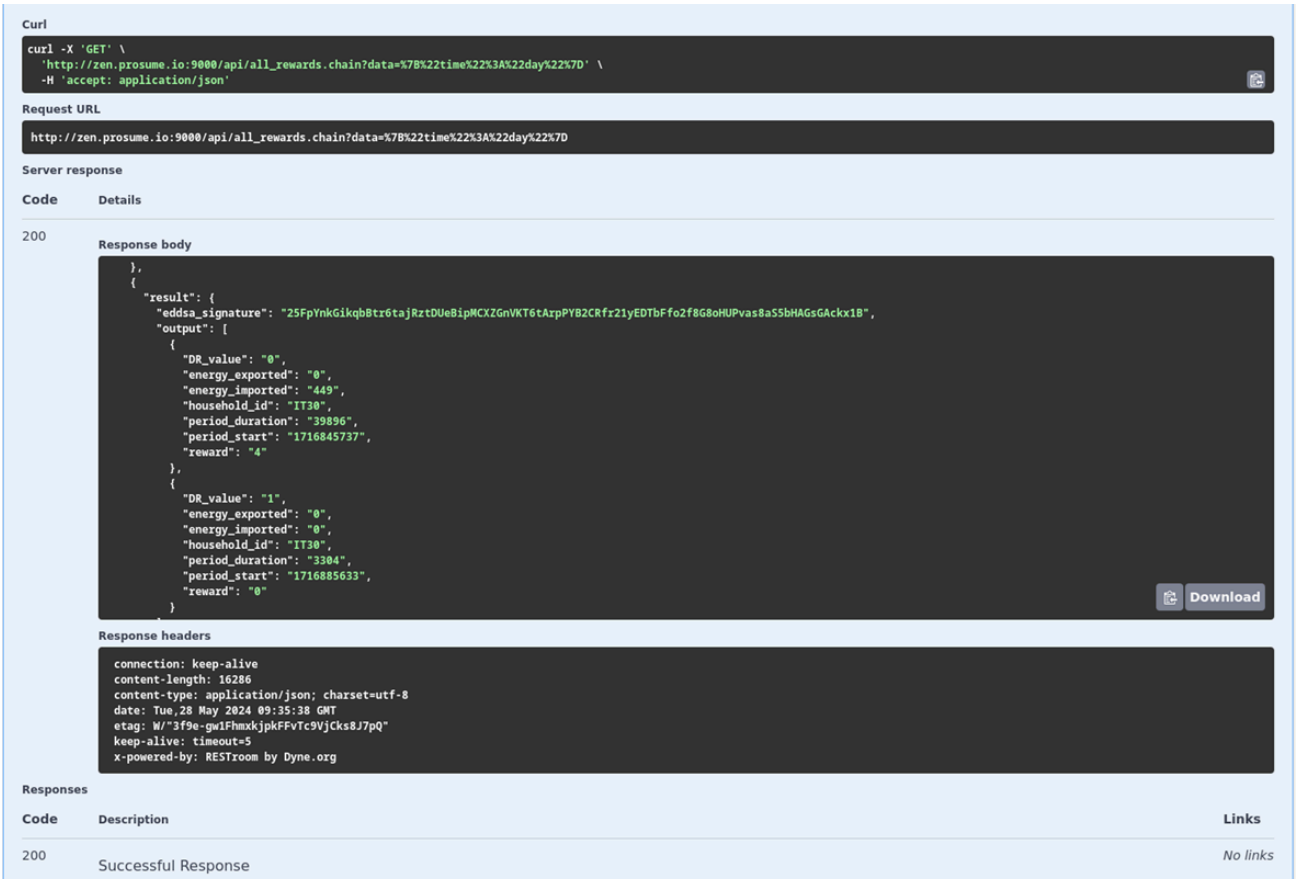

Figure 6 - Smart Contract PROSUME API screenshot

The reward computation considers the optimisation produced by the LEC optimizer developed by the other GENTE partners, and the presets defined by the users, and then the reward information is communicated to the PROSUME Blockchain via REST API.

The information provided is directly being signed using a secret key whose public key is registered in the DID Document following the W3C Decentralised Identifier standard, and signatures can be verified by 3rd parties directly on the PROSUME instance of the Zenswarm Oracle, adding trust to the data output.

The resulting JSON file from the PROSUME Oracle (after processing data collection and executing the specific smart contract) is the following:


```
{
  "didDocument": {
    "@context": [
      "https://www.w3.org/ns/did/v1",
      "https://w3id.org/security/suites/ed25519-2018/v1",
      "https://w3id.org/security/suites/secp256k1-2019/v1",
      "https://w3id.org/security/suites/secp256k1-2020/v1",
      "https://dyne.github.io/W3C-DID/specs/ReflowBLS12381.json",
      {
        "description": "https://schema.org/description",
        "url": "https://schema.org/url"
      }
    ],
    "description": "prosume_oracle",
    "id": "did:dyne:sandbox.zenswarm:8tEn6Er3QXjDZTM8Nk8US4hvo65t2sc988m8haJEUGS6",
    "proof": {
      "created": "1696320855814",
      "jws":
"eyJhbGciOiJFUzI1NksiLCJiNjQiOnRydWUsImNyaXQiOiJiNjQifQ..x6yqmo78dLSXaywmBCwYAuew7Pak3KRZXHdB6m9-C-r0
MK2JGjW8xu_F1hyOZeQs-UH6buN-jo1yaRpImD_Ehg",
      "proofPurpose": "assertionMethod",
      "type": "EcdsaSecp256k1Signature2019",
      "verificationMethod":
"did:dyne:sandbox.zenswarm_A:DZmuSi2WgdsN8Usbbw4ZF4cZfF31ecqzPRHwP6GnxNE4#ecdh_public_key"
    },
    "url": "http://zen.prosume.io:9000",
    "verificationMethod": [
      {
        "controller": "did:dyne:sandbox.zenswarm:8tEn6Er3QXjDZTM8Nk8US4hvo65t2sc988m8haJEUGS6",
        "id":
"did:dyne:sandbox.zenswarm:8tEn6Er3QXjDZTM8Nk8US4hvo65t2sc988m8haJEUGS6#ecdh_public_key",
        "publicKeyBase58":
"NNWsmRAFyPVsyUPEPPizuZzxJuMboAv1vke62WtikZjAgVzDyWm7ND6ZLHVaPPLAFByNRUPG8nxRHzTHmd8W3hwD",
        "type": "EcdsaSecp256k1VerificationKey2019"
      },
      {
```

```
        "controller": "did:dyne:sandbox.zenswarm:8tEn6Er3QXjDZTM8Nk8US4hvo65t2sc988m8haJEUGS6",
        "id":
"did:dyne:sandbox.zenswarm:8tEn6Er3QXjDZTM8Nk8US4hvo65t2sc988m8haJEUGS6#reflow_public_key",
        "publicKeyBase58":
"A6RME3PX8fcwPVdGYkwnzDQVsS3HdreXSVS92FAng6Xtj77k1X3buHDeigitQPUnQZagjwYpnXhfPdTvKSky53w9sHFawkEMHXjv
E2u6ceFmQhDMeseaa3Tv5FMan89F3y3DLRphuidhdx41asAsqQgDAMvsWD5EauBp2cp7zfAnQ23ne7ec4V4DYhQTMXaFS9i6vukXB
FKk8z4Af74JNpqZjbkudVSkrrowY2dUvv1fCVdeR4f8Yn5CHdSzMhqCG3Qsrt",
        "type": "ReflowBLS12381VerificationKey"
      },
      {
        "controller": "did:dyne:sandbox.zenswarm:8tEn6Er3QXjDZTM8Nk8US4hvo65t2sc988m8haJEUGS6",
        "id":
"did:dyne:sandbox.zenswarm:8tEn6Er3QXjDZTM8Nk8US4hvo65t2sc988m8haJEUGS6#bitcoin_public_key",
        "publicKeyBase58": "zMcuZfTqU6m1gDzNtYjRARU2KTujXKArMUZjEQs2FU2N",
        "type": "EcdsaSecp256k1VerificationKey2019"
      },
      {
        "controller": "did:dyne:sandbox.zenswarm:8tEn6Er3QXjDZTM8Nk8US4hvo65t2sc988m8haJEUGS6",
        "id":
"did:dyne:sandbox.zenswarm:8tEn6Er3QXjDZTM8Nk8US4hvo65t2sc988m8haJEUGS6#eddsa_public_key",
        "publicKeyBase58": "8tEn6Er3QXjDZTM8Nk8US4hvo65t2sc988m8haJEUGS6",
        "type": "Ed25519VerificationKey2018"
      },
      {
        "blockchainAccountId": "eip155:1:0x4ab32e663ea1dc6c0f63483f7e74c5c206472769",
        "controller": "did:dyne:sandbox.zenswarm:8tEn6Er3QXjDZTM8Nk8US4hvo65t2sc988m8haJEUGS6",
        "id":
"did:dyne:sandbox.zenswarm:8tEn6Er3QXjDZTM8Nk8US4hvo65t2sc988m8haJEUGS6#ethereum_address",
        "type": "EcdsaSecp256k1RecoveryMethod2020"
      }
    ]
  },
  "didDocumentMetadata": {
    "created": "1696320855814",
    "deactivated": "false"
  }
}
```

DID Documents can be retrieved to verify the digital identity of the specific asset and to verify validity in case a request for deactivation has been submitted for a decommissioned asset.

The two following flows show the underlying process of key generation, document creation, verification and registration of a Digital Identity Asset, and of deactivation requests being executed between the owner and the oracle as demonstrated in the PROSUME API documentation.

In summary, the entire system integrates various components to ensure seamless data flow and transaction management across different platforms and regions. External entities (authorities, GENTE platform, regional pilots) interact with the system via the REST API. The REST API coordinates data flow between external entities and internal components such as the Zenchain, Zencode Smart Contracts, database (mariaDB), and schedulers.

The main objective is to enable off-chain smart contract execution while ensuring interoperability with other specific on-chain contracts and notarization processed data.

The architecture is aligned with other architectures of similar projects where instead of a demand response remuneration module, a pay for performance mechanism is defined or where a different type of remuneration might be requested [xi].

The Zencode Smart Contracts are concatenated in chains (so called “Zenchain”) in order to execute REST calls and database operations, performed by the NodeJS based component “Restroom-mw” which is also programmed in Zencode and is part of the Zenroom modules. Zenchains offer a linear flow that is easy to read and is edited and tested inside the Apiroom online IDE (https://apiroom.net).

A Zenchain can be called via a REST API, once all the contracts in the chain are executed successfully, the output is returned to the caller. Extending the chain to perform database operations or posting the output on 3rd party services can be implemented and tested within minutes.

Here you can find the definition of the APIs exposed by the microservice. The swagger documentation is available at http://zen.prosume.io:9000/docs

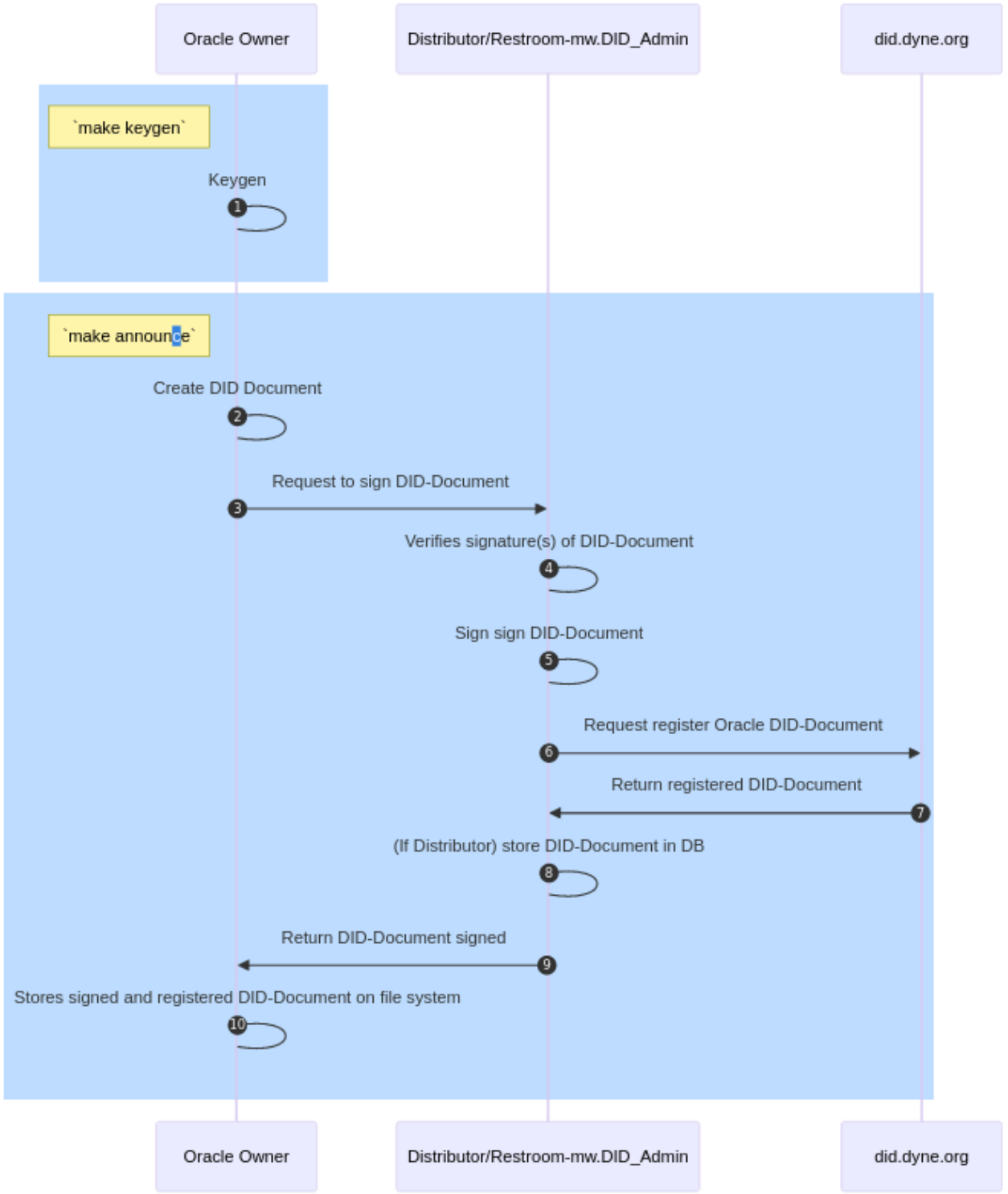

Figure 7 - DID Document registration flow

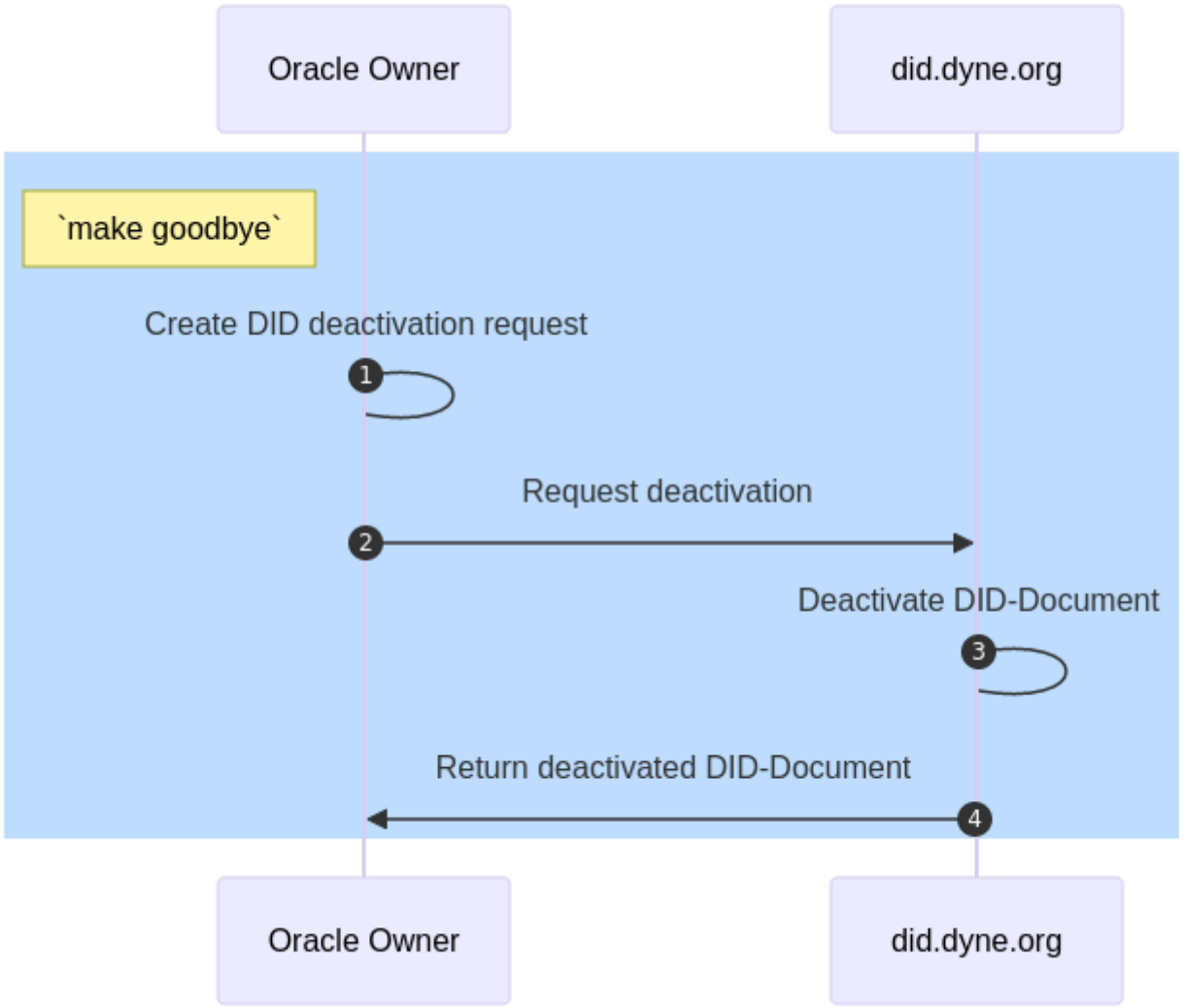

Figure 8 - DID Document revocation process

The above pictures represent the process of issuance and revocation of a DID Document and how it gets deactivated with the revocation process.

5. Toolkit for Energy Communities

PROSUME's contribution is limited to the tools described in the previous chapters, our intention is to outline some good practice and provide useful tools that could be considered a piece of the composing toolkit for energy communities in vision of a more dynamic local energy market.

Real peer-to-peer (P2P) trading based on blockchain environments is connected to a fully distributed key management for participants. Previously, trading of tokens was only done within decentralised exchanges on blockchain platforms. It is a novelty in the energy sector, and it has to be adapted to work fully automated and in line with the settings made by the participants, as well as restrictions given by the energy management systems.

A Digital Identity Wallet (the PROSUME APP) enables the user to establish relationships and interact with third parties in a trusted manner. While the wallet aspect is mainly dealing with key management, storage aspects and the graphical interface, the third-party interactions are organised by agents. Software agents handle third-party interactions on behalf of a user's interest. This piece of software helps to stay in control of assets, security, privacy, purchases, etc. This is the critical part that has to be developed to establish a real P2P trading mechanism as well as compliance with GDPR and integration with the fiat payments in the banking system as provided by the PROSUME Platform.

This development is not in the scope of the GENTE project. Within the project, we are demoing an architecture where such complexity and automation provided by off-chain smart contracts could easily be added to the actual system in place at an LEC.

Building a modular toolkit for energy communities it is not an easy task because each community can differ a lot from another one, not only in terms of what type and how many members can constitute the community but also and mostly, on what type of energy source, composition and design of the infrastructure (often defined as a Micro-Grid) the community is made of. For these reasons and for the specific role and limited budget PROSUME had in this project, the tools adopted were implemented for a flexibility use case with the goal to be easily modified or substituted by other instruments.

Considering the tools described in previous chapters and the overall architecture of GENTE Platform, the following image describes the GENTE Platform architecture as developed by the main project partners and shows where our tools are actually located in the overall architecture:

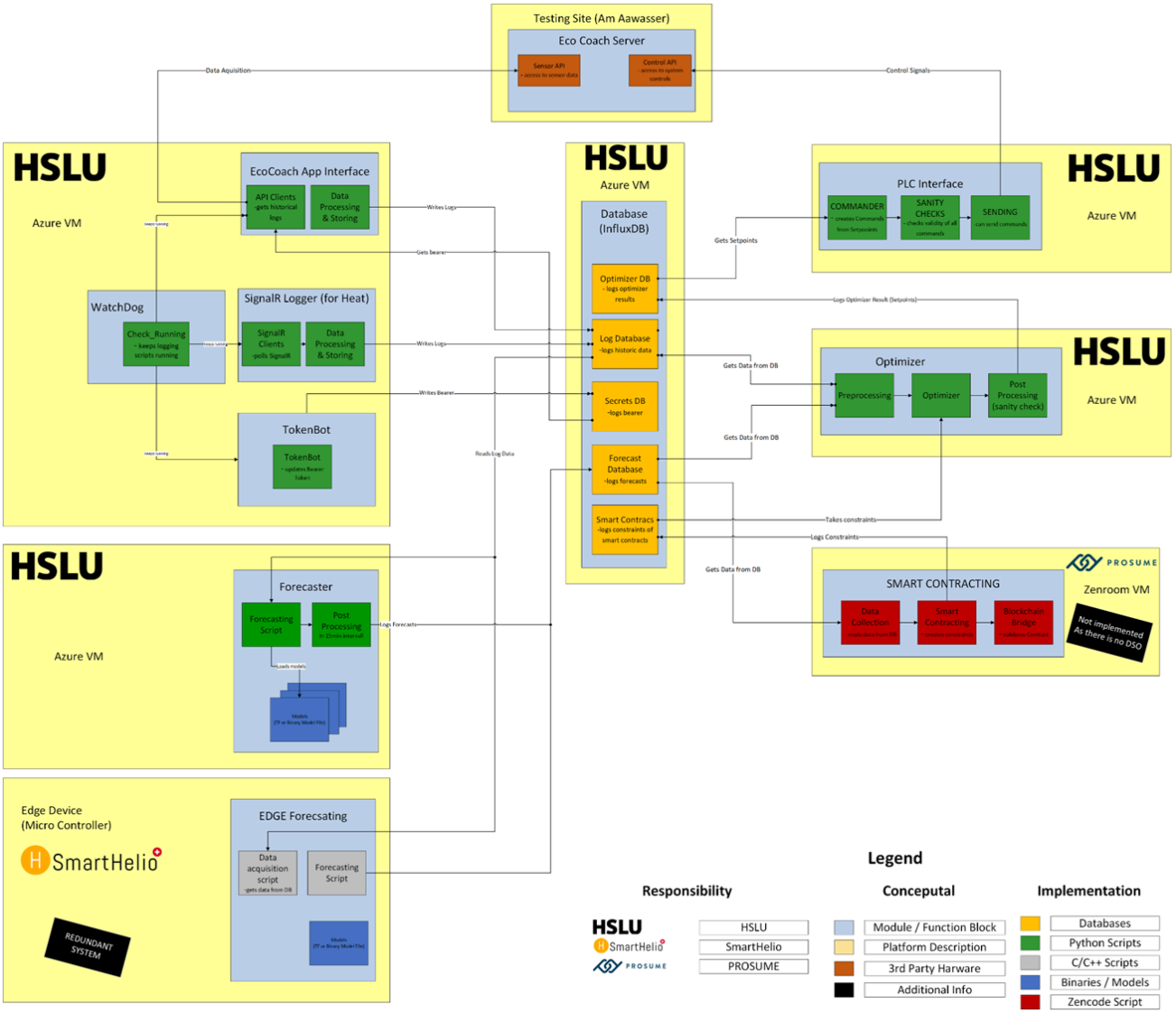

Figure 9 - Zenroom interaction and positioning in GENTE Platform

The architecture shown above represents the GENTE Platform architecture. The tools developed and provided by PROSUME are positioned in the architecture so to simplify as much as possible the interaction with other commonly used pieces of software that are needed for the management of "on cloud" infrastructures.

In this case, the Zenroom implementation here is connected to the main architecture so to provide an example of how smart contract technologies can be made of use by LEC creators and operators (like Energy Community Managers) to manage and automatize activities that are connected to financial settlement operations and that require an high level of trust and security.

Conclusion

Within this deliverable, PROSUME explored the integration of the Zenroom software stack to enhance blockchain interoperability and smart contract functionality within the GENTE project, focusing on Local Energy Communities (LECs). The Zenroom stack, developed by the Dyne foundation, offers a robust multi-platform technology that supports various cryptographic operations and blockchain interoperability. It enables the creation of smart contracts in humanreadable language and allows for seamless integration across different blockchain networks. The implementation aimed to address the challenges of energy management within LECs by providing tools for computing rewards based on energy consumption and production patterns, while ensuring privacy and security. The Zenroom stack demonstrated its capability to support complex cryptographic operations and maintain interoperability across multiple blockchain platforms. The Zenroom stack provides a scalable and adaptable solution for developing energy community business models, fostering innovation and collaboration in the energy sector.

In particular, we can conclude that the tools we developed can provide:

1. **Interoperability and Flexibility**: The Zenroom stack's ability to operate across various blockchain networks and its modular design make it a highly flexible solution for energy community projects, allowing for easy adaptation to future technological advancements.
2. **Privacy and Security**: The implementation ensures strong cryptographic protection, addressing privacy concerns within LECs by enabling secure data handling and smart contract execution without compromising user confidentiality.
3. **Scalability**: The stack supports the development of scalable energy management solutions, capable of handling complex reward systems and data integration from diverse sources, which is crucial for the dynamic nature of LECs.

Future work will focus on enhancing data accessibility and exploring additional use cases to further validate the technology's applicability in real-world scenarios.

FUNDING

This project has received funding in the framework of the joint programming initiative ERA-Net Smart Energy Systems' focus initiative Digital Transformation for the Energy Transition, with support from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883973.

References

[i] Blockchain is seen as a tool for decentralization, transferring authority from centralized entities to distributed networks. This approach reduces the need for trust among participants and addresses issues like digital identity and asset ownership

https://www.blockchain-council.org/blockchain/what-is-decentralization-in-blockchain/

[ii] Europe plays a significant role in defining Self-Sovereign Identity (SSI) and sustainability through various initiatives and regulations. The European Union has been actively working on integrating SSI with existing frameworks like eIDAS to enhance digital identity management

https://www.selfsovereignidentity.it/self-sovereign-identity-and-eidas-part-2/

[iii] The eIDAS Bridge project, for example, aims to align SSI with the eIDAS regulation, allowing for secure and efficient identity verification across public services. This initiative is part of the European Blockchain Services Infrastructure and is designed to improve the management of personal data while ensuring privacy and security

https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf

[iv] Blockchain is being explored as a tool for decentralizing energy markets, enabling peer-to-peer energy trading, and providing transparency and security in transactions

https://consensys.io/blockchain-use-cases/energy-and-sustainability

https://digitalcommons.georgiasouthern.edu/cgi/viewcontent.cgi?article=1143&context=information-tech-facpubs

[v] **Renewable Energy Directive (EU) 2023/2413**: This directive promotes the development of energy communities in offshore wind and district heating and cooling networks. It encourages cooperation with local authorities to mainstream renewable energies in buildings

Energy Efficiency Directive (EU) 2023/1791: This directive requires local heating plans to assess the potential of energy communities to develop renewable energy-based heating projects, emphasizing the role of energy communities in achieving energy efficiency goals

Electricity Market Design Reform: The reform clarifies and reinforces the rights of energy communities to share energy among members, supporting active consumer participation through demand-response and storage services

Social Climate Fund Regulation (EU) 2023/955: This regulation allows EU countries to target vulnerable households and micro-enterprises through energy communities, providing a framework to alleviate energy poverty

https://energy.ec.europa.eu/topics/markets-and-consumers/energy-consumers-andprosumers/energy-communities_en

[vi] **Forkbomb Software Stack**: https://forkbomb.solutions/component/zenroom/

[vii] **Schnorr Crypto**: https://github.com/wires/zenschnorr

Schnorr signature: https://en.wikipedia.org/wiki/Schnorr_signature

[viii] Implementing **pairing-based cryptography** for zero knowledge proofs (ZKPs)

https://medium.com/asecuritysite-when-bob-met-alice/explaining-bls12-381-the-zeroknowledge-proof-curve-aa5eabec8261

[ix] The **EdDSA** signature algorithm and its variants **Ed25519** and **Ed448** are technically described in the RFC 8032

[x] *DID registration methods*: https://w3c.github.io/did-spec-registries/#did-methods

and Dyne.org Quantum-Proof revocation paper as recently published on arxiv:

https://arxiv.org/abs/2406.19035v4

[xi] **Energy Community Flexibility Solutions**:

https://www.sciencedirect.com/science/article/pii/S2352467723001959