Zero Bridge: Make Permissioned Blockchains Interoperable

Ph.D. Alessandro Bigiotti, Prof. Leonardo Mostarda, Prof. Alfredo Navarra, Prof. Andrea Pinna, Prof. Roberto Tonelli

DLT WorkShop 2026

Santa Margherita in Pula (SU), Sardinia, Italy,
6th June, 2026

Zero Bridge Objectives

Project motivations:

- **Gap in literature**: In the literature we have found a lack of interoperability protocols between private and permissioned blockchains.

- **Practical needs**: Blockchain adoption in enterprise contexts can benefit from efficient and privacy-friendly interoperability protocols.

Project proposal:

ZeroBridge: *Designing and implementing a permissioned blockchain* ***interoperability protocol*** *that is inherently* ***secure****, highly* ***efficient****, broadly* ***applicable****, and* ***privacy-preserving*** *by design.*

Challenges: Access Control & Privacy

In interoperability protocols between private and permissioned blockchains, special attention must be paid to access control mechanisms and privacy that:

- Ensure inability of off-chain processes to **access writing to communicating blockchains**;
- Avoid **disclosing confidential information** to third parties;
- Allow **access only** to the portion of **data** that is the **subject of interchain transactions**;
- Allow the exchange of information **without resorting** to complex cryptographic primitives such as **Zero Knowledge Proof**.

Challenges: Efficiency & Security

Private and permissioned blockchains can have shorter block production times than public ones and transaction costs can be lowered to zero. The off-chain component for managing interchain transactions must be efficient, secure and have little or no cost:

- Design off-chain processes that are decentralised, are not connected with each other, and **avoid consensus algorithms**;
- Keep interchain transaction **costs constant or low**;
- Allow an interchain transaction to be finalised **using only two transactions** (one on the source blockchain and one on the destination blockchain).
- Implement **off-chain & on-chain verification** mechanisms for validating inter-chain transactions;

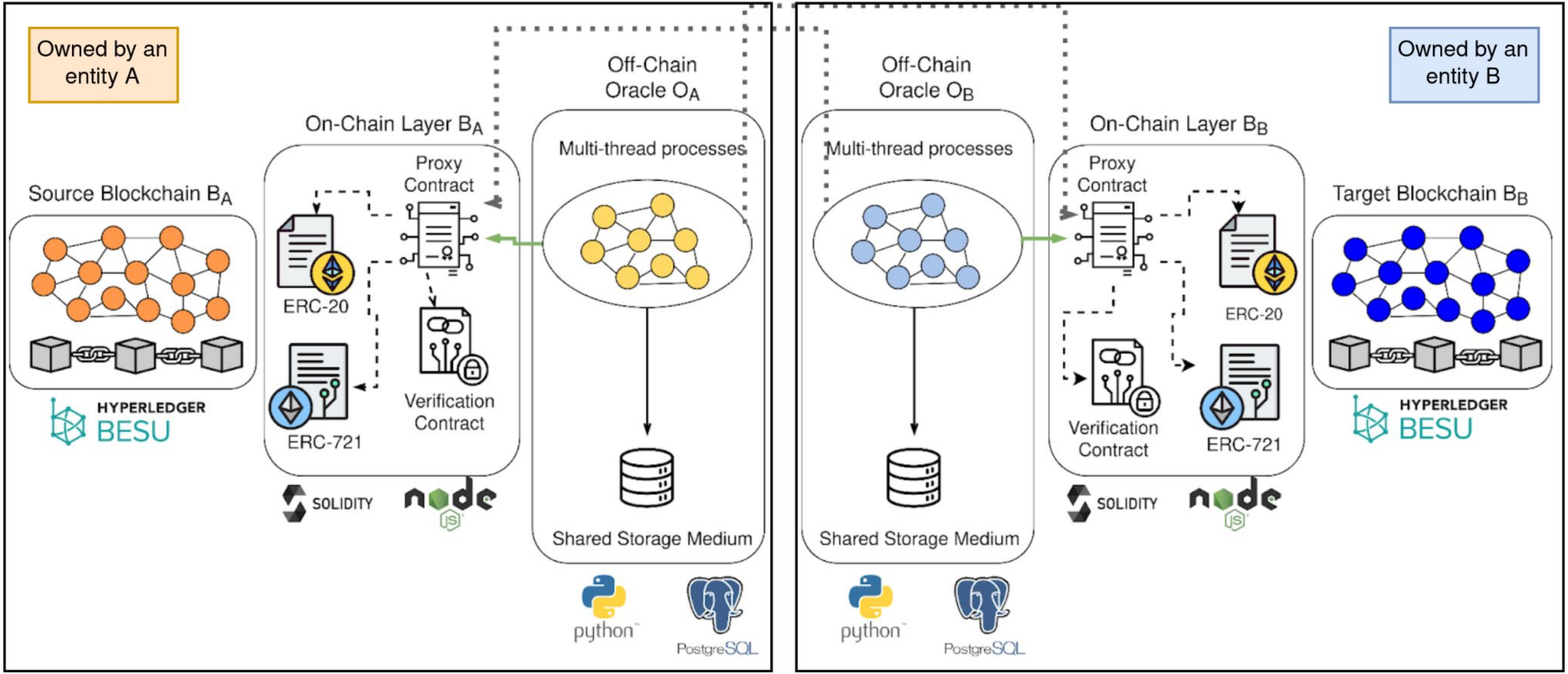
Challenges: General Purpose

In business contexts, blockchains can be used to implement logic and maintain data of different and arbitrary nature. In particular, in an interoperability scenario they:

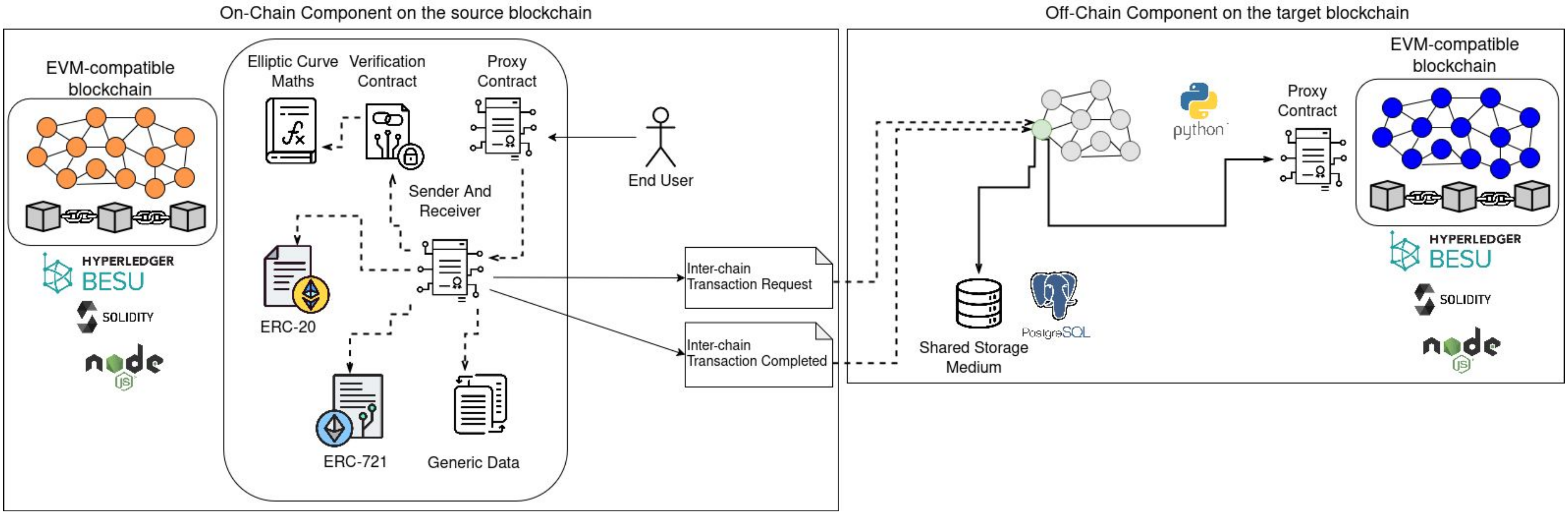
- **Abstract** from the **blockchain architecture** (cryptographic primitives, consensus algorithms, smart contract languages, etc...);

- Allow for **numerous use cases** such as: token transfer, data copying or synchronisation, or arbitrary invocation of smart contracts residing on different blockchains;

Overall Architecture



On-Chain and Off-Chain Components



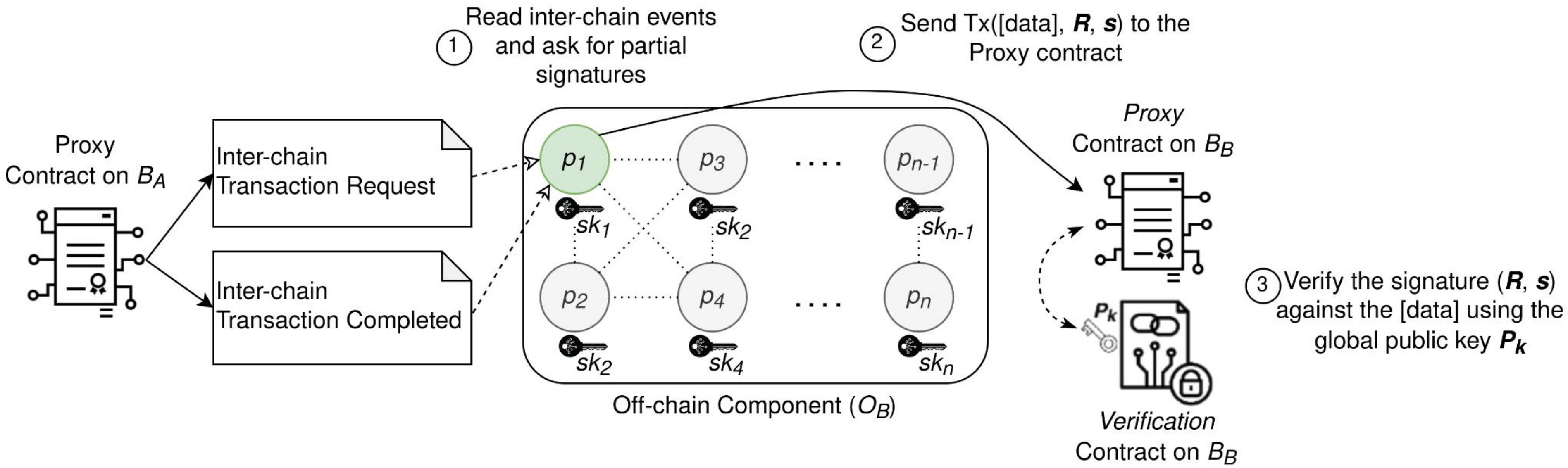
Event Semantic

The events that drive off-chain processes contain JSON-formatted messages that enable a variety of use cases:

```
"header": {
        "source_chain": <chain id>,
        "timestamp": <current timestamp>,
        "sender": <address from source chain>
    },
```

```
"body": {
        "instructions": {
            "service": <service name>,
            "function": <function name>
            “roll_back”: <bool [True, False]>
        },
        "content": {
            "key_1": value_1,
              ...     ...
            "key_n": value_n,
        }
    }
```

Inter-chain Transaction Finalisation



Supported Standards

The proposed solution supports and requires compatibility with the following standards:

- **ERC-20, ERC-721, ERC-1151.** The protocol supports well-known standards for token representation.

- **ERC-1822, ERC-1967.** The protocol implements the Universal Upgradeable Proxy Standard;

- **ERC-173.** The protocol implements the Contract Ownership Standard;

- **ERC-2771.** Depending on the use case, the protocol requires compatibility with Secure Protocol for Native Meta Transactions.

Scalability and Security

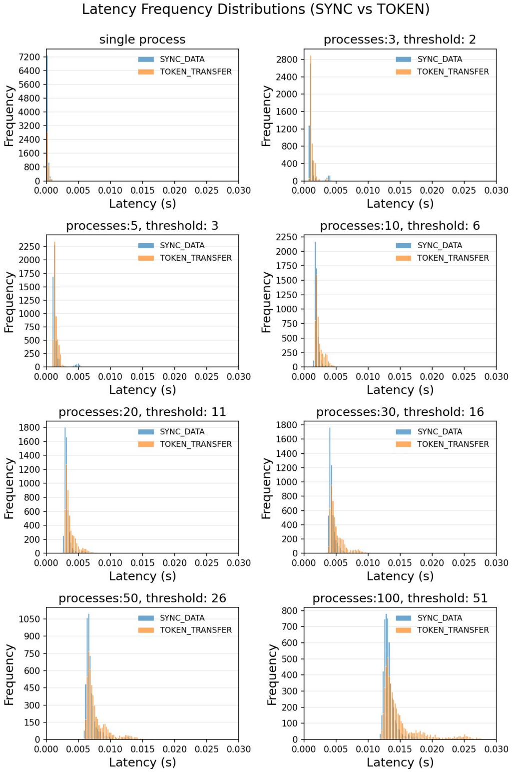
Using a threshold signature in interchain transactions allows for more scalable off-chain processes and verifying signatures on-chain reduces the possibility of validating fraudulent transactions:

- The off-chain component implements a **distributed key generation algorithm** following Pedersen's Commitments, Verifiable Secret Sharing (VSS) and Feldman's commitments for an **ECDSA-based threshold signature**.

- The signature generation follows the **Schnorr scheme** (FROST 2020), with the difference that the proposed approach is a fully on-line leader-based two-round variant.

- The **signature (*R*, *s*) is verified on-chain** on a dedicated smart contract implementing a highly optimised library written in YUL and assembly.

Experimental Results



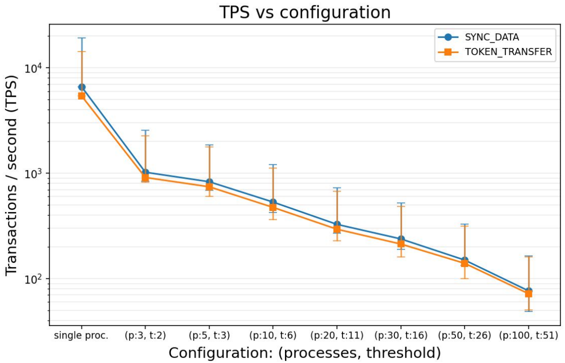


Table 5.1.: Latency and TPS registered during the experiments.

Configuration		Latency (s)			TPS	
n° nodes	threshold	min	avg	max	avg	max
single	process	0.00008	0.000197	0.001181	5076	12500
3	2	0.00065	0.00112	0.0056	892	1538
5	3	0.0009	0.0012	0.0068	833	1112
10	6	0.0014	0.0018	0.0091	555	714
20	11	0.0025	0.0030	0.0175	333	400
30	16	0.0035	0.0041	0.0208	244	286
50	26	0.0056	0.0066	0.03582	151	179
100	51	0.0114	0.0136	0.0606	74	88

References

1. Bigiotti, A., Mostarda, L., Navarra, A., Pinna, A., Tonelli, R., Vaccargiu, M. (2024). "*Interoperability Between EVM-Based Blockchains*". In: Barolli, L. (eds) Advanced Information Networking and Applications. AINA 2024. Lecture Notes on Data Engineering and Communications Technologies, vol 200. Springer, Cham. https://doi.org/10.1007/978-3-031-57853-3_9

2. A. Bigiotti, L. Mostarda, A. Navarra, P. Shah and R. Trestian, "*Threshold Signature in Off-Chain Components to Manage Inter-chain Transactions,*" *2024 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, Berlin, Germany, 2024, pp. 1-4, doi: 10.1109/BRAINS63024.2024.10732513

3. A. Bigiotti, L. Mostarda, A. Navarra, A. Pinna, and R. Tonelli. "Blockchain Agnostic Protocols: An Analysis of the State of the Art". In: ACM Computing Surveys 58.2 (2025). issn: 0360-0300. doi: 10.1145/3758089. url: https://doi.org/10.1145/3758089

4. A. Bigiotti, L. Mostarda, A. Navarra, A. Pinna, R. Tonelli, and M. Vaccargiu. "Smart Listeners: a Hybrid-Optimistic Inter-Blockchain Communication Protocol". In: Blockchain: Research and Applications (2025), p. 100339. issn: 2096-7209. doi: https://doi.org/10.1016/j.bcra.2025.100339.url: https://www.sciencedirect.com/science/article/pii/S2096720925000661

5. Bigiotti, A., Mostarda, L., Navarra, A., Pinna, A., Tonelli, R. ZeroBridge project, winner of the Open Call 4 from NGI Trust Chain. Funded by European Union under the agreement n° 101093274. https://trustchain.ngi.eu/zerobridge/

BILANCIO CO2 ZERO

NGI TRUST CHAIN

AGILE BY CHAIN

ZERO BRIDGE

A.D. 1308 unipg

UNIVERSITÀ DEGLI STUDI DI PERUGIA

UNICAM Università di Camerino 1336

Università di Camerino

UNICA

UNIVERSITÀ DEGLI STUDI DI CAGLIARI

alessandro.bigiotti[at]unicam.it

https://www.linkedin.com/in/alessandro-bigiotti

https://www.researchgate.net/profile/Alessandro-Bigiotti-3