tecnalia

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

MINE.IO

Bridging Private & Public Blockchains: A zk-SNARK Framework for Secure ERC-1155 Transfers

Darío Valarezo-Castañeda, Aitor Gómez-Goiri and **Cristina Regueiro**

7th International Congress on Blockchain and Applications

26th June, 2025
Lille (France)

Table of contents

tecnalia

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

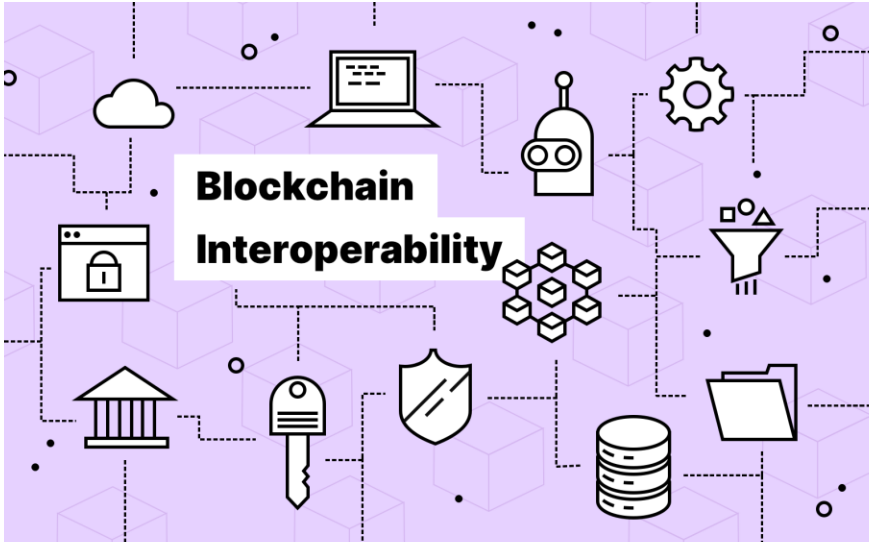
MINE.IO

Context

Motivation

Blockchain ecosystem remains highly fragmented

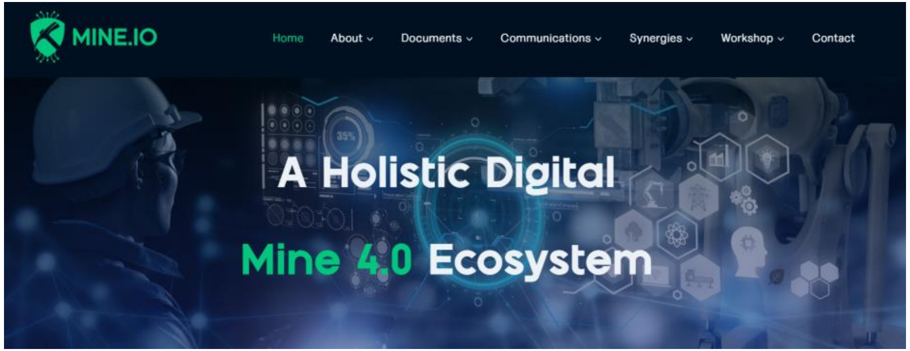
- Public and private blockchains operate in silos.
- Enterprises need secure, private asset transfer.
  - Current focus on public-to-public interoperability.
  - Some approaches for private-to-private interoperability (Hyperledger Cactus).
  - Lack of standards for private-to-public interoperability



Context

MINE.IO: Blockchain based traceability platform

- Mining waste management.
- ERC-1155 standard: fungible and non-fungible tokens.
- Hyperledger Besu: private deployment.
- It should be publicly extended to make circular economy a reality as well as to unlock monetization opportunities.
    - Interoperability with a public blockchain is recommended



https://mineio-horizon.eu/

Objective

Propose a hybrid interoperability solution in cross-chain private-to-public transactions

- Hashed Timelock Contracts (HTLCs) based locking.
- Zero knowledge Proofs (ZKPs)
- Relayer-assisted proof coordination

- Allow interoperability of MINE.IO solution (Hyperledger Besu) with public Ethereum compatible networks.

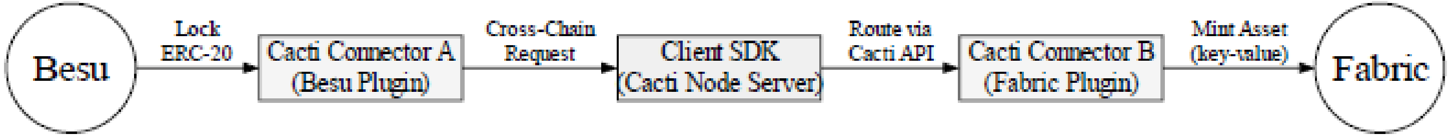
MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

State of the Art

Current Interoperability Solutions

Hyperledger Cacti for private-to-private interoperability


Besu
Lock ERC-20
Cacti Connector A (Besu Plugin)
Cross-Chain Request
Client SDK (Cacti Node Server)
Route via Cacti API
Cacti Connector B (Fabric Plugin)
Mint Asset (key-value)
Fabric

Key cross-chain mechanisms

- A **bridge** relies on a verifier to validate messages from a smart contract on Blockchain A (origin) and relay them to Blockchain B (target).
- **Atomic swaps** allow direct peer-to-peer exchanges of tokens across blockchains without trust in intermediaries.
- **HTLCs** (Hashed Timelock Contracts) enforce conditional transactions using cryptographic hash functions. Funds remain locked until all participants meet the predefined conditions.
- **Relay chains** act as intermediaries, monitoring multiple blockchains and validating cross-chain transactions.
- **Sidechains** are independent blockchains connected to a primary blockchain. They allow asset transfers between chains while reducing congestion on the main network.

Key cross-chain mechanisms

- A **bridge** relies on a verifier to validate messages from a smart contract on Blockchain A (origin) and relay them to Blockchain B (target). → **Third parties are involved.**
- **Atomic swaps** allow direct peer-to-peer exchanges of tokens across blockchains without trust in intermediaries. → **Simple but with limited flexibility.**
- **HTLCs** (Hashed Timelock Contracts) enforce conditional transactions using cryptographic hash functions. Funds remain locked until all participants meet the predefined conditions → **trustless and lightweight solution**
- **Relay chains** act as intermediaries, monitoring multiple blockchains and validating cross-chain transactions. → **Third parties are involved.**
- **Sidechains** are independent blockchains connected to a primary blockchain. They allow asset transfers between chains while reducing congestion on the main network. → **Complex infrastructure**

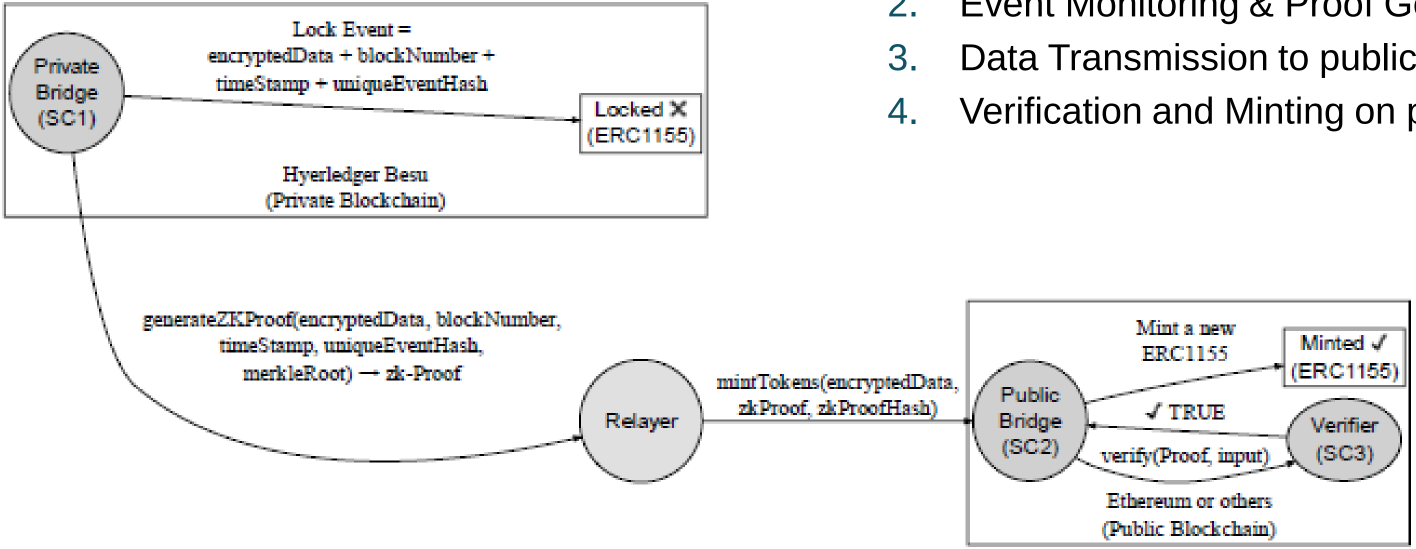
tecnalia
MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

tecnalia
MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

MINE.IO

Proposal

Architecture and Workflow



Private Bridge (SC1)
Lock Event = encryptedData + blockNumber + timeStamp + uniqueEventHash
Locked ✗ (ERC1155)
Hyerledger Besu (Private Blockchain)
generateZKProof(encryptedData, blockNumber, timeStamp, uniqueEventHash, merkleRoot) → zk-Proof
Relayer
mintTokens(encryptedData, zkProof, zkProofHash)
Public Bridge (SC2)
Mint a new ERC1155
Minted ✓ (ERC1155)
✓ TRUE
verify(Proof, input)
Verifier (SC3)
Ethereum or others (Public Blockchain)

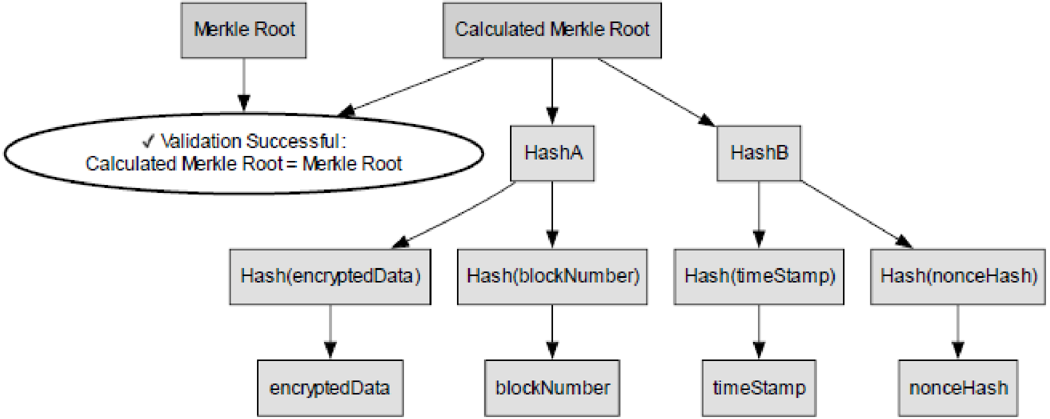
1. Locking on Besu.
2. Event Monitoring & Proof Generation
3. Data Transmission to public network
4. Verification and Minting on public network

Security by ZoKrates: verifier

It validates that the data received by the relayer in the locked event → If positive, the token is minted.

It generates the merkle root without publicly exposing these sensitive values.

It automatically generates the verifier smart contract with the described logic.



tecnalia

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

MINE.IO

Results

Validation: MINE.IO

Trace mining waste assets inside a pyrometallurgical process

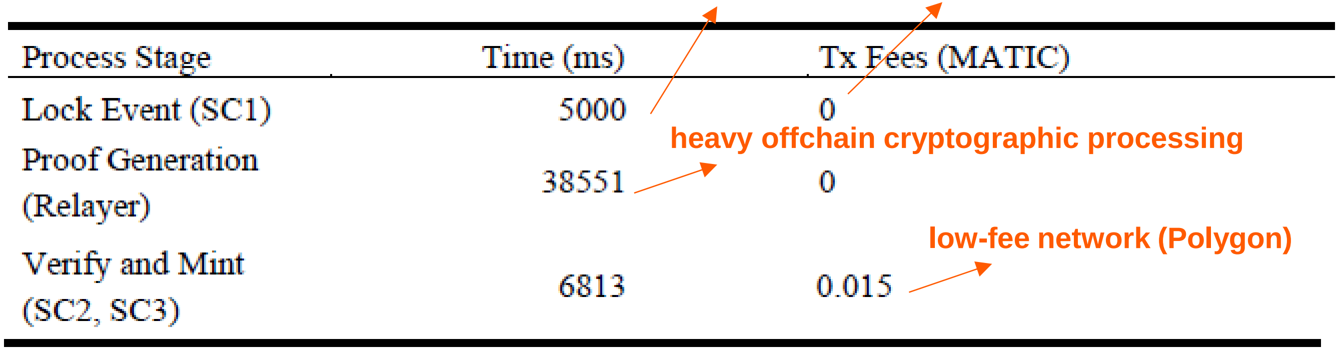
Novel **circular economy** approaches as well as the current **strict regulations** on the management of mining waste in the European Union highlight the need for the tokens representing waste assets (i.e., tailings, slag, etc.) to be managed in public networks where **transparency is greater**.

New value strings in **DeFi ecosystems**.

MINE.IO

Validation: MINE.IO

Considered technologies: Besu, Amoy (Polygon testnet), hardhat, Node.js Relayer, ZoKrates.



Process Stage	Time (ms)	Tx Fees (MATIC)
Lock Event (SC1)	5000	0
Proof Generation (Relayer)	38551	0
Verify and Mint (SC2, SC3)	6813	0.015

Block time

Zero Base Fee

heavy offchain cryptographic processing

low-fee network (Polygon)

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

Conclusions

Conclusions & Future Work

Secure and scalable token migration between private (Hyperledger Besu) and public (Amoy) blockchain networks

- Secure ERC-1155 bridging is feasible
    - Public/private bridges enable transparency & value.
    - zkSNARKs bring privacy to interoperability

- Domain agnostic
    - Applied to MINE.IO traceability solution

- **Future work:**
    - Explore zkSNARK batching for higher efficiency
    - Analyze more complex ZKP solutions.(e.g., Circom).
    - Extend comparative studies with other alternatives.

MINE.IO

tecnalia

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

MINE.IO

Cristina Regueiro
cristina.regueiro@tecnalia.com

tecnalia.com

This study was funded by Horizon project MINE.IO: A Holistic Digital Mine 4.0 Ecosystem (Grant agreement ID: 101091885).