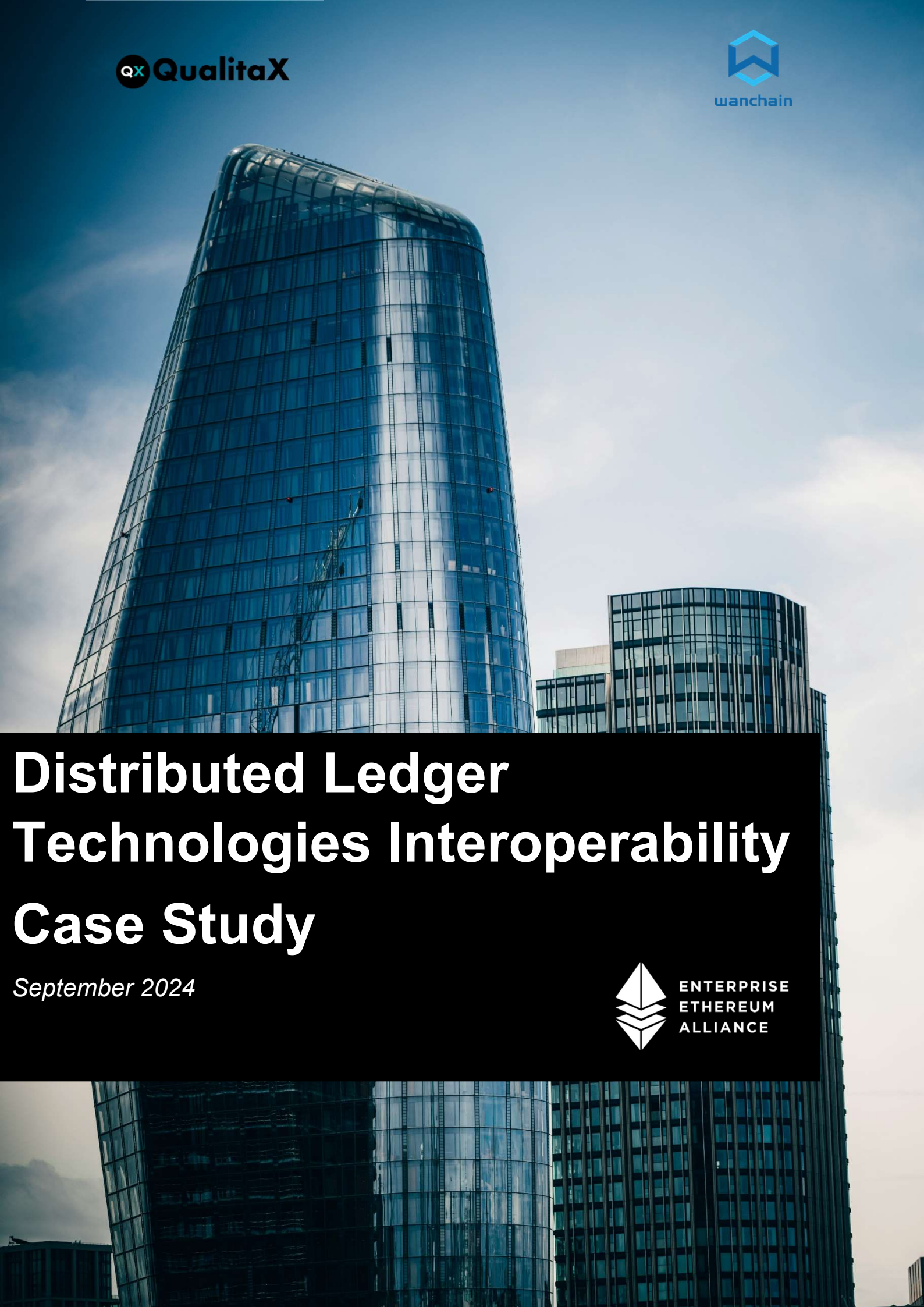


QualitaX

wanchain

Distributed Ledger Technologies Interoperability Case Study

September 2024

ENTERPRISE ETHEREUM ALLIANCE

AUTHORS

Anaïs Ofranc - Founder & CEO, QualitaX

Marelize Kriel - Cryptographer and Blockchain Engineer, Adhara

Weijia Zhang - Vice President Of Engineering, Wanchain

ABOUT

This document describes a case study implementation showcasing how using the Enterprise Ethereum Alliance (EEA) Distributed Ledger Technologies (DLT) Interoperability Specification can facilitate seamless communication and transaction capabilities between distinct DLT platforms. By adhering to this specification, organizations can overcome the interoperability challenges, allowing for a more integrated and efficient global financial system that leverages the full benefits of DLT.

CONTACT

To learn more about the EEA DLT Interoperability Specification and how it can support your DLT interoperability infrastructure, contact:

Weijia Zhang (weijia@wanchain.org), Co-Chair EEA DLT Interoperability WG

Anaïs Ofranc (aofranc@qualitax.io), Co-Chair EEA DLT Interoperability WG

Table of Contents

Introduction

The growing adoption of distributed ledger technology (DLT) and digital assets in global financial markets has made the need for interoperability standards clear to market participants.

The Enterprise Ethereum Alliance (EEA) recognizes the need for collaboration among stakeholders, including financial institutions, technology providers, and regulatory bodies, to drive standards development. This collaborative approach is essential for creating a seamless, secure, and efficient ecosystem that can support the diverse needs of the global financial system. The development and adoption of these standards will facilitate greater innovation, reduce operational risks, and enhance the scalability of blockchain-based solutions, ultimately contributing to the broader acceptance and integration of digital assets in traditional financial infrastructures.

The EEA Cross-chain Interoperability Working Group is dedicated to standardising interoperability, one of the most important areas in blockchain and distributed ledger technologies (DLT).

It defines DLT interoperability as the ability to transfer digital assets from one DLT network to another, send and receive messages across DLT networks, and initiate actions across DLT networks. This group's primary goal is to develop specifications, guidelines, and best practices frameworks that support interoperability between EVM-compatible networks (including Ethereum Mainnet, consortium blockchains, optimistic rollups, and zk-rollups) and non-EVM blockchain networks.

About the EEA DLT Interoperability Specification

The Enterprise Ethereum Alliance (EEA) Distributed Ledger Technology Interoperability Specification aims to establish a secure and efficient framework for interoperability between different blockchain networks, focusing on enterprise applications. This specification addresses the need for various blockchain platforms to interact and transact seamlessly, especially in complex and regulated sectors like financial services and supply chain management. The specification includes architectural guidelines, protocol stack, and interface definitions, crucial for asset and data exchange across different blockchain systems, enhancing their functionality and utility.

It is designed to support enterprise blockchain networks using diverse underlying technologies (for example, EVM and non-EVM networks), facilitating complex multi-chain ecosystem deployments involving assets, payments, and securities transactions. The open standard prevents fragmentation across different vendor implementations. Use cases include currency exchanges between blockchains with different tokens, coordinating securities transfers with payment transfers on different chains, and atomic swaps/transfers of assets. The specification aims to support regulated enterprise use cases that require interoperability between multiple blockchains with secure guarantees.

Primary stakeholder groups:

This specification is relevant to three primary stakeholder groups:

Developers, Architects, and Integrators: The specification provides interfaces to accelerate the development of interchangeable components for connecting heterogeneous distributed ledger technologies and blockchain networks. It is relevant to professionals seeking to implement interoperability solutions across various DLT platforms, building or incorporating them into their solutions and applications.

Decision-makers and IT executives: Executives and decision-makers in regulated industries such as finance, healthcare, and supply chain will find this specification crucial for unlocking new business models and value streams through interoperable blockchain solutions. Executive in corporations exploring or already using DLT technologies in their operations are key beneficiaries of this specification.

Regulators and Standards Development Organizations (SDOs): By setting a precedent for interoperability standards, this document aids regulators and SDOs in understanding the technical complexities and potential regulatory considerations of crosschain communications. It aims to foster a collaborative environment where regulatory frameworks can evolve with technological advancements, ensuring a balanced approach to innovation and regulations.

How to access the EEA DLT Interoperability Specification

The Enterprise Ethereum Alliance Distributed Ledger Technologies Specification is available here: https://entethalliance.org/technical-specifications/.

Case Study

The context of this case study is a Stellar Soroban-Polygon Asset Bridge, a DLT interoperability solution designed to expand the potential buyer pool for Soroban-based assets by enabling digital asset sales to buyers on the Polygon PoS network. Soroban is the smart contracts platform on the Stellar network. The Stellar network reaches consensus using the Stellar Consensus Protocol (SCP), a construction of the Federated Byzantine Agreement (FBA).

This bridge aims to improve liquidity for Stellar and attract more participants to the Stellar ecosystem by leveraging Polygon's user base. Enhancing the interoperability of the Stellar network with other blockchain ecosystems, such as Polygon, in a way that is compliant with the EEA specification broadens the scope, utility and relevance of Stellar-based assets and applications for enterprises, financial institutions and regulators looking for and prioritizing standard-compliant implementations.

Exploring EEA-compliant interoperability between Stellar and the Ethereum ecosystem can further enhance trust among various Stellar' stakeholders, including financial institutions, users, partners and regulators, as well as demonstrate a commitment to address those stakeholders' needs.

Stellar Soroban-Polygon Asset Bridge

The Stellar network has grown to be one of the largest blockchains in terms of real-world assets, with over 430 million in tokenized market cap (excluding stablecoins) and 1.3 billion in transaction volume for assets tied to real-world value.

Stellar provides asset issuers with significant control over their assets, including the ability to approve users, freeze or claw back assets, and program-specific functionalities through smart contracts. This level of control is essential for banks and licensed financial institutions.

Issuers such as Franklin Templeton are now launching on-chain products such as the Franklin OnChain U.S. Government Money Fund. The project uniquely provides daily interest payments to Benji token holders, leveraging the Stellar blockchain for cost-effective settlement and

eliminating secondary ledgers. This project also recently expanded to include peer-to-peer payment functionality and support for the Polygon blockchain, Benji aims to become a versatile, interest-bearing instrument for various financial transactions.

The Stellar Soroban-Polygon Asset Bridge could complement such initiatives by enhancing liquidity, improving interoperability, and expanding market reach for issuers.

To demonstrate the bridge's capabilities, we began with a straightforward use case: enabling buyers to purchase Soroban-based digital assets on the Polygon PoS network. We deliberately chose a low-risk asset for this initial implementation, starting with NFTs. This approach allowed us to test the core functionalities of the bridge while minimizing potential risks. By successfully facilitating this simple transaction across networks, we established a solid foundation for more complex use cases and validated the bridge's fundamental interoperability features.

Overview

Summary	The Stellar Soroban-Polygon Asset Bridge is an EEA-compliant interoperability solution aiming to enhance liquidity and attract participants to Stellar. To demonstrate the bridge's capabilities, a simple use case was implemented: allowing Polygon PoS buyers to purchase Soroban-based digital assets, starting with a low-risk, custom NFT to showcase the concept.
Target Customers	Banks, Financial Institutions
Technology	Stellar Soroban, Polygon PoS, Wanchain
Product Type	DLT Interoperability solution
Notable Partnerships	Stellar Development Foundation Enterprise Ethereum Alliance (EEA) Wanchain QualitaX

Leveraging the EEA DLT Interoperability Specification

This section explores the adaptability of the EEA specification to Stellar Soroban architecture, focusing on block-based consensus mechanisms, messaging types, cryptographic support, and the implementation of the Wanchain Messaging Bridge.

- **Incompatibility considerations of Soroban and EVM blockchains**

Although the block-based structures provide clear points of reference for event emission, state updates, and transaction finality, which is crucial for implementing reliable bridges or interoperability solutions, there are still some incompatibilities between the two blockchains that are addressed below:

Stellar's SCP focuses on federated agreements with trusted validators, while Polygon employs a traditional PoS system with block production and validation by staked validators.

Stellar Soroban uses Rust as a smart contract programming language, while Polygon leverages Ethereum EVM architecture with smart contracts implemented in Solidity. For interoperability, the two sets of smart contracts will need to use compatible crosschain messaging functions and data types to enable the transfer of messages across the two blockchains.

Similar to EVM, Soroban implemented events to store custom data corresponding to a transaction. The storage of event data of Soroban is in env construct, while the event data for EVM is in transaction logs. The declaration and publication of events also follow different syntax. The message relayers will need to parse the events and package the event data to a format acceptable to the target chain.

Another incompatibility is the wallet used by the two blockchains. Soroban and EVM blockchains use different account public and private keys mechanisms, making their wallets incompatible. The source chain and target chain will need to connect to different wallets. For this implementation, we use Metamask for the EVM chain and Freighter wallet for the Soroban blockchain.

- **Messaging Type Supported**

For bridging Stellar Soroban and Polygon PoS, event-based messaging is the most appropriate approach, as it can react to the finalization of ledgers (in Stellar) or blocks (in Polygon) to trigger cross-chain actions. Soroban' smart contract platform can emit events when certain conditions

are met, or actions are performed. These events are used to trigger corresponding actions on the Polygon network. And vice versa.

- **Cryptographic support**

The ED25519, SECP256K1 curves are used for ECDSA (Elliptic Curve Digital Signature Algorithm) EDDSA (Edwards-curve Digital Signature Algorithm) signing. Keccak256 hash functions have been implemented in the Stellar Soroban smart contract platform. Both signature schemes are supported by the EEA DLT Interoperability specification. The Keccak256 implementation can be considered part of the broader cryptographic toolkit and is used in hashing operations within the specification. The SECP256K1 curve is commonly used in blockchain systems, including Bitcoin and Ethereum, for public key cryptography and digital signatures. This curve is supported by the specification.

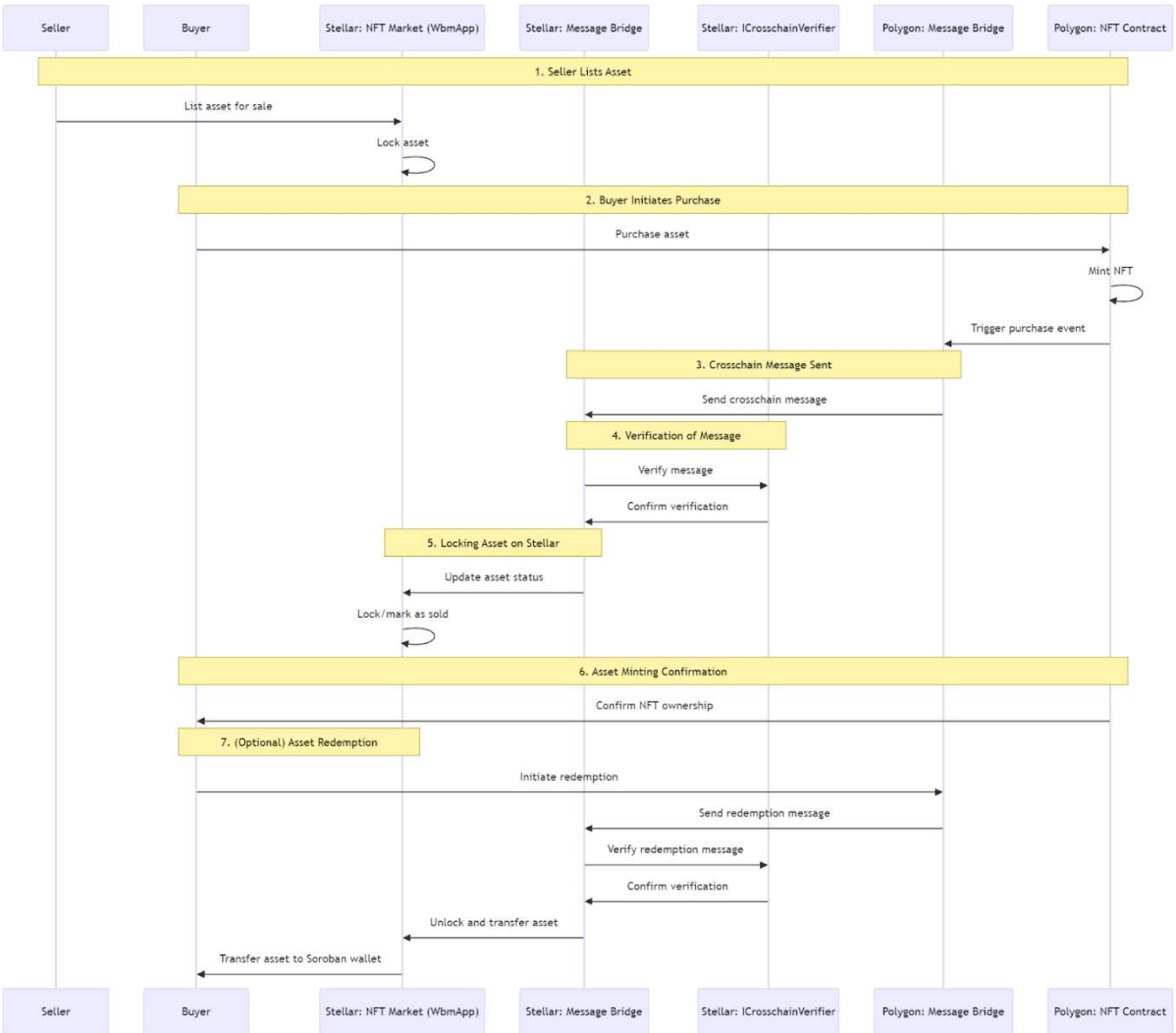
- **Wanchain Messaging Bridge**

The Wanchain Message Bridge is a decentralized messaging system that allows users to send messages across different blockchains. Message Bridge is designed to comply with EEA DLT Interoperability Specification.

The WmbGateway smart contract is the main entry point of the Wanchain message bridge system. It facilitates cross-chain messages between different blockchain networks by serving as a gateway. This contract leverages the functionalities of the OpenZeppelin library for security and utility purposes.

Process Flow

A user submits a request to sell an asset on a target chain with a specific price; the asset can be locked on the source chain, and a wrapped asset can be minted on a target chain. A buyer can then purchase the asset on the target chain and become the owner of the wrapped asset. The buyer can then unwrap the asset on the source chain to gain ownership of the original asset on the source chain.



The flow of the use case is as follows:

1. **Seller Lists Asset on Stellar Soroban:** The seller lists the asset on the NFT marketplace by interacting with WbmApp contract. The contract locks the asset on the Stellar Soroban network, and a

crosschain sell message is sent to the smart contract on the Polygon chain, marking the asset as listed for sale

2. **Buyer Initiates Purchase on Polygon:** A buyer on the Polygon network sees the listed asset and decides to purchase it. The minting process triggers an event indicating the buyer's intent to purchase the asset.
3. **Crosschain Message Sent from Polygon to Stellar:** The Polygon network needs to inform the Stellar network about the purchase. The event triggered by the minting on Polygon is captured by the Message Bridge contract on Polygon. The Message Bridge contract packages this event data, including purchase details, into a crosschain message. This message is then sent to the Stellar network via the Wanchain Message Bridge (WMB) infrastructure, using the IWmbGateway interface.
4. **Verification of Crosschain Message on Stellar:** The Stellar network receives the crosschain message. The Message Bridge contract on Stellar receives the message. The ICrosschainVerifier contract is invoked to verify the authenticity and integrity of the message. This process ensures that the message is genuine and that the purchase on Polygon was indeed completed by the buyer.
5. **Locking the Asset on Stellar:** After successful verification, the asset is locked or marked as sold on the Stellar network. The Message Bridge contract communicates with the NFT Market (WbmApp) contract on Stellar Soroban to lock the asset. The asset's status is updated, preventing any further sale or transfer within the Stellar network.
6. **Asset Minting Confirmation on Polygon:** The process finalizes with the confirmation of the minted asset on the Polygon network. The buyer now owns a newly minted NFT on Polygon, which represents the asset originally listed on Stellar. The NFT on Polygon is fully linked to the original asset on Stellar, ensuring interoperability between the two networks.
7. (**Optional) Asset Redemption on Stellar by the Buyer:** The buyer can choose to redeem the asset back to Stellar if they have a Soroban wallet. The buyer initiates a redemption process by triggering a message from Polygon to Stellar, requesting to transfer the asset back. The crosschain message follows a similar verification process. Upon successful verification, the asset on Stellar Soroban is unlocked and transferred to the buyer's Soroban wallet.

Key Takeaways

- **Interoperability between DLT Networks**

Successful Implementation: The case study demonstrates a successful implementation of an asset bridge between two distinct DLT networks: Stellar Soroban for asset management and Polygon PoS for facilitating transactions within the Ethereum ecosystem.

EEA-Compliant Interoperability: Crosschain interoperability is achieved via an EEA-compliant crosschain messaging protocol, including cryptographic proofs and multi-signature verification, enabling secure asset transfers and interactions across the two networks.

Importance of Standards: This underscores the critical role of open interoperability standards like those from the EEA in unlocking the full potential of DLTs in various industries, especially in ensuring secure and standardized crosschain operations.

- **Benefits of DLT in Asset Liquidity and Market Expansion**

Enhanced Liquidity: By bridging Stellar-based assets to the Polygon network, the case study showcases how DLT can significantly enhance liquidity by tapping into Polygon's larger user base, thereby broadening the market for Stellar assets.

Expanded Market Access: The implementation allows Stellar assets to be easily accessed and traded by users in the Ethereum ecosystem, opening up new investment opportunities and driving broader adoption of the Stellar network.

Efficiency and Cost Reduction: The use of DLT for crosschain asset transactions demonstrates improvements in operational efficiency, lower transaction costs, and a reduction in the need for intermediaries.

- **Security and Trust in Crosschain Transactions**

Robust Verification Mechanisms: The implementation employs cryptographic proofs and signature verification mechanisms to ensure that only authenticated and authorized crosschain transactions are executed, thereby enhancing the security and integrity of the asset bridge.

Compliance and Trust: Adhering to EEA standards not only strengthens security but also builds trust among institutional stakeholders, regulators, and end users, making the solution more attractive to regulated industries.

- **Enhancement of Atomic Settlement**

Ensuring Atomicity: The bridge implementation currently uses multisignature to ensure decentralised trust of the relayers. The messaging relayer can be extended to include atomic transactions in which a hash time lock contract (HTLC) is added and only wallet users who have the secret key can unlock the transaction on the target chain. The HTLC mechanism ensures atomic settlement of transactions across the Stellar and Polygon networks, thereby eliminating counterparty risk and guaranteeing settlement finality.

Reliable and Consistent Settlements: This atomicity is crucial for maintaining consistency and reliability in crosschain transactions, particularly in financial and asset management scenarios where trust and finality are paramount.

- **Ownership Transfer without Crosschain Asset Movement**

Efficient Asset Ownership Updates: Instead of physically moving assets between the Stellar and Polygon networks, the implementation updates asset ownership records on the respective networks. This allows for seamless and efficient transfer of asset ownership without the need for complex asset transfers.

Demonstrating DLT Potential: This approach highlights how DLT can enable the efficient transfer of ownership rights across different blockchain ecosystems, minimizing the need for direct crosschain asset movement while still ensuring security and regulatory compliance.

Conclusion

In conclusion, this case study demonstrates how Distributed Ledger Technology (DLT) interoperability can enhance asset liquidity and market access. The Stellar-Polygon Asset Bridge showcases how different DLT networks can be leveraged to create efficient, secure, and scalable cross-chain asset transactions.

The bridge combines Stellar Soroban's robust asset management capabilities with Polygon PoS's access to the Ethereum ecosystem, illustrating the synergies possible between diverse blockchain networks. The successful testing deployment, adherent to the EEA DLT Interoperability Specification, underscores open standards' adaptability and practical applicability across different blockchain ecosystems. This interoperability solution broadens utility and relevance for Stellar-based assets and applications, particularly for enterprises, financial institutions, and regulators prioritizing standard-compliant implementations.

This case study exemplifies how adherence to open standards like the EEA DLT Interoperability Specification can provide a robust framework for enterprises to build and deploy interoperable DLT solutions, ultimately driving innovation and efficiency in the blockchain space in regulated settings.

Wanchain, in collaboration with QualitaX, developed the implementation of the DLT specification for Stellar Soroban and Polygon blockchains through its cross-chain messaging framework. Wanchain intends to release this technology as an open-source project to contribute to blockchain interoperability. Third-party developers can leverage the messaging framework to develop advanced decentralised applications across various heterogeneous blockchain architectures.

CREDITS

Report prepared by QualitaX on behalf of the Enterprise Ethereum Alliance DLT Interoperability Working Group.

MEDIA CREDITS

Frontpage:

Photo by Kevin Lang on Unsplash

Source: https://unsplash.com/photos/black-and-white-glass-building-PJB7pOiMMr0

Description: Black and white glass building.

https://entethalliance.org/