ITU Workshop

on Distributed Ledger Technology Scalability and Interoperability

2 August 2019
Geneva, Switzerland

JELURIDA

Building blockchain solutions since 2013

SECTION 0/4

Description:
Integrating with Hyperledger Quilt and the Interledger Protocol - Ardor's Experience

Sections

1. Why interoperability?
2. Options to achieve interoperability
    a. Atomic Swaps
    b. Oracles integration
    c. Side chains vs child chains
    d. Blockchain integration bus
3. Hyperledger quilt - Interledger Protocol
4. Demo

Who I am?

Alberto Fernández

Software Engineer, business development and consultancy

BACKGROUND

- Consultant and IT instructor
- Middleware expert
- Blockchain specialist.
- Co-founder of the Blockchain for Business Madrid and Barcelona meetup group (+1K members)
- Founder of Sistek Solutions Ltd

alberto.fernandez@jelurida.com

SECTION 1/4

Why interoperability?

SECTION 1/4

Why interoperability?

The problem

What is interoperability?

The End-to-End principle

Implications

SECTION 1/4

Why interoperability?

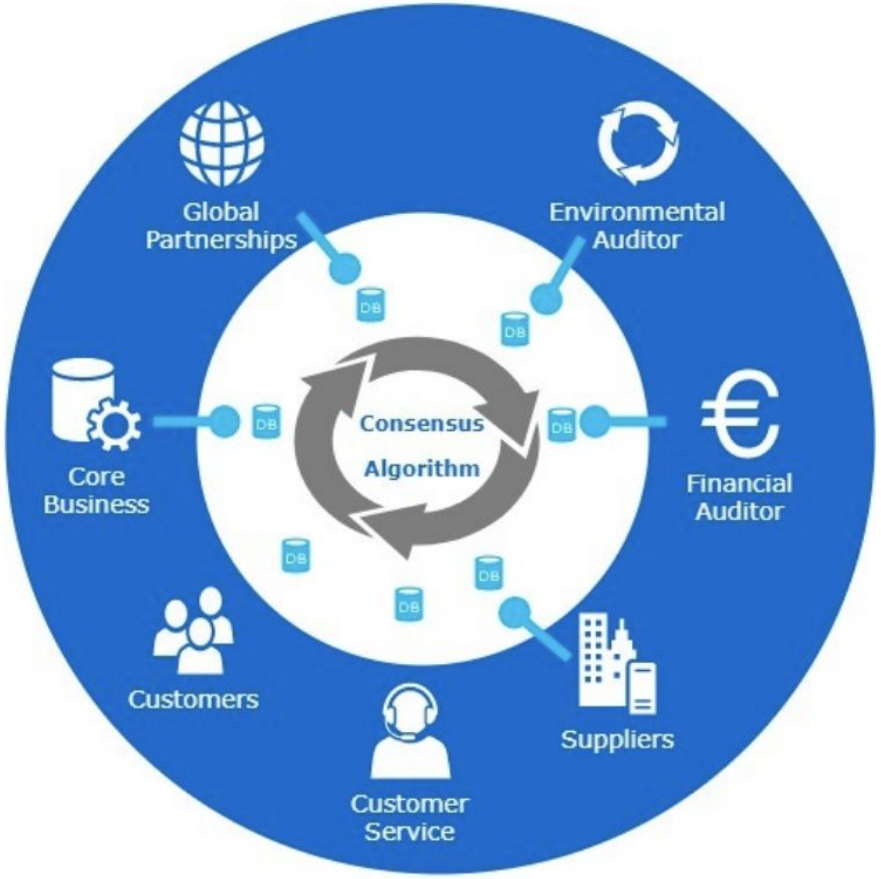
The problem

What is interoperability?

The End-to-End principle

Implications

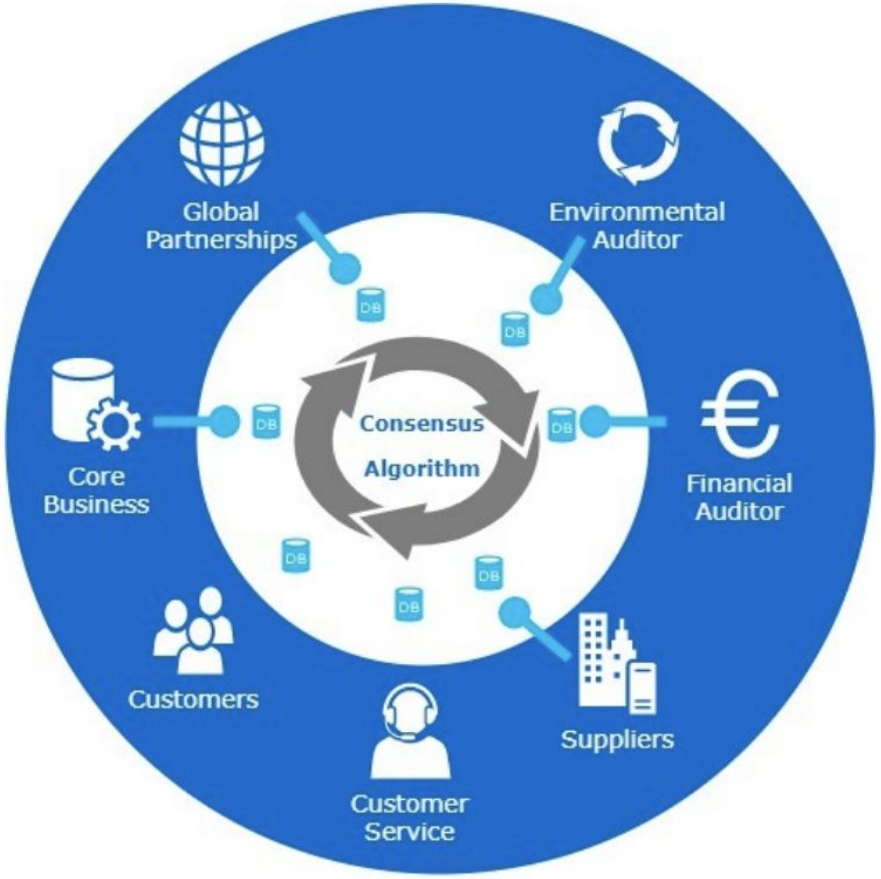
The problem



Current scenario

Companies has started to share data thanks to distributed ledgers

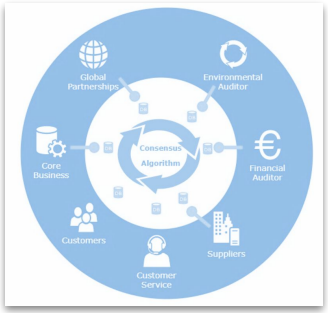
The problem

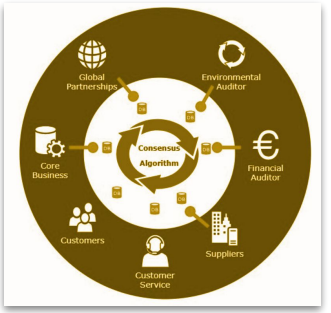


Current scenario

Companies has started to shared data thanks to distributed ledgers

But different ledgers:



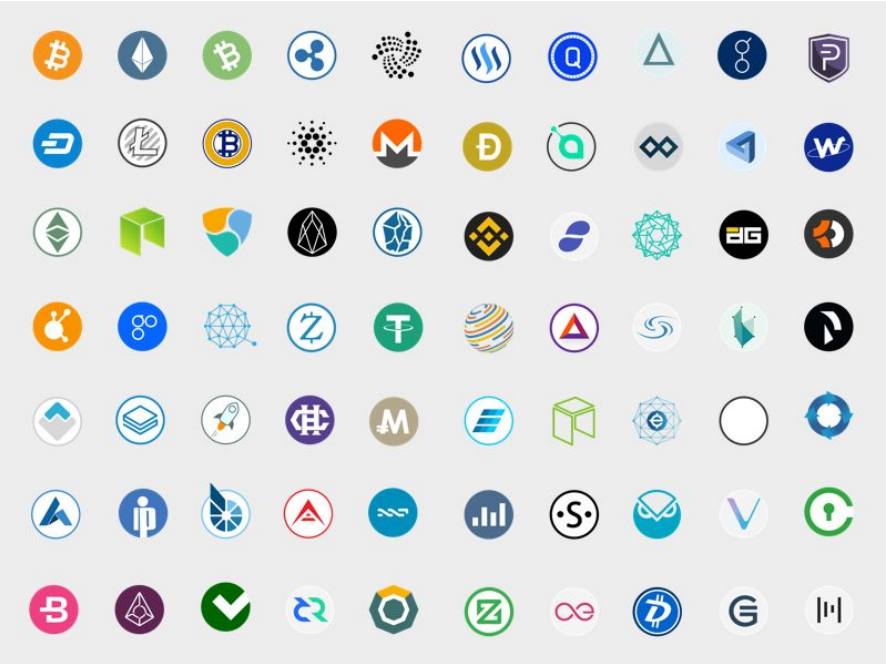


The problem

The number of **digital assets** and **blockchains** are growing at a rapid pace

The problem

The number of **digital assets** and **blockchains** are growing at a rapid pace



The problem

- There is **no one-size-fits-all solution** when it comes to different requirements of security, privacy, flexibility and political values
- These different blockchains remain **isolated**
- **Private** blockchains are hard to integrate with **Public** blockchains

The problem

- There is **no one-size-fits-all solution** when it comes to different requirements of security, privacy, flexibility and political values
- These different blockchains remain **isolated**
- **Private** blockchains are hard to integrate with **Public** blockchains

Does it sound familiar?

The problem

- There is **no one-size-fits-all solution** when it comes to different requirements of security, privacy, flexibility and political values
- These different blockchains remain **isolated**
- **Private** blockchains are hard to integrate with **Public** blockchains

Does it sound familiar?

Lessons learned from the **development of the internet:**

1. **Survivability**, **Variety** of services types and networks
2. **End-to-End** principle
3. **Routing**: scale-up capabilities

SECTION 1/4

Why interoperability?

The problem

What is interoperability?

The End-to-End principle

Implications

What is interoperability

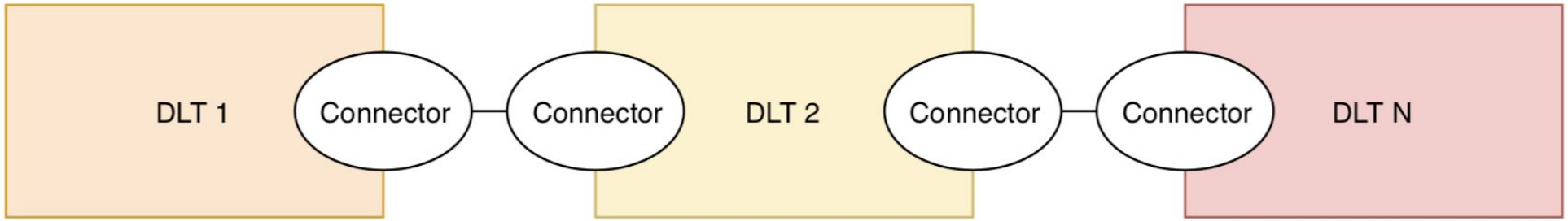
Distributed Ledger interoperability is the ability of spanning the transaction execution across multiple DLT systems. It implies the following

- The data recorded is reachable and verifiable by any other DLT.

What is interoperability

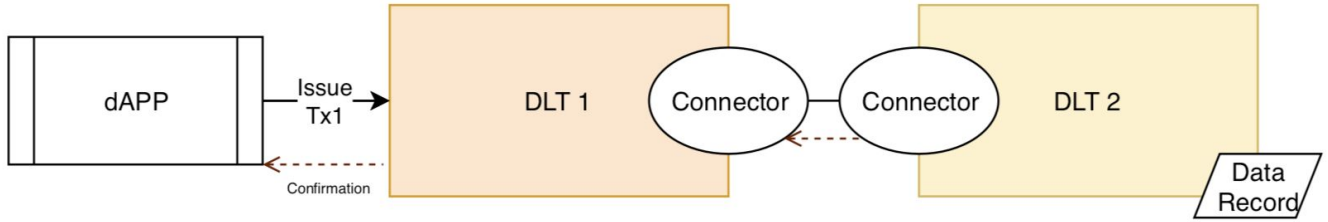
Distributed Ledger interoperability is the ability of spanning the transaction execution across multiple DLT systems. It implies the following:

- The data recorded is reachable and verifiable by any other DLT.

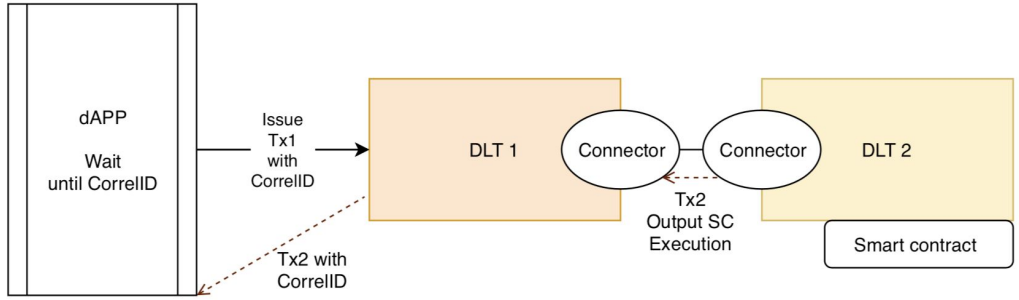


What is interoperability

Asynchronous transaction (most common use case)



Synchronous transaction



SECTION 1/4

Why interoperability?

The problem

What is interoperability?

The End-to-End principle

Implications

The End-to-End principle

In a network designed according to this principle, application-specific features reside in the communicating end nodes of the network, rather than in intermediary nodes, such as gateways and routers, that exist to establish the network.

- Message duplicate detection
- Non-repudiation
- Guaranteed message delivery
- Sequencing

SECTION 1/4

Why interoperability?

The problem

What is interoperability?

The End-to-End principle

Implications

Implications

New paradigm: Cryptography applied to the communications to determine sender and receiver

- Ideal scenario where the private keys from different DLTs can be derived bidirectional
- One single DLT entity or address can be represented in all DLTs

Interoperability should be outside political interests

SECTION 2/4

Options to achieve interoperability

SECTION 2/4

Options to achieve interoperability

Atomic swaps

Oracles integration

Side chains Vs child chains

Blockchain integration Bus

SECTION 2/4

Options to achieve interoperability

Atomic swaps

Oracles integration

Side chains vs child chains

Blockchain integration Bus

Atomic swaps

It is the ability to exchange transactions in two different distributed ledgers, without the need to trust a third-party

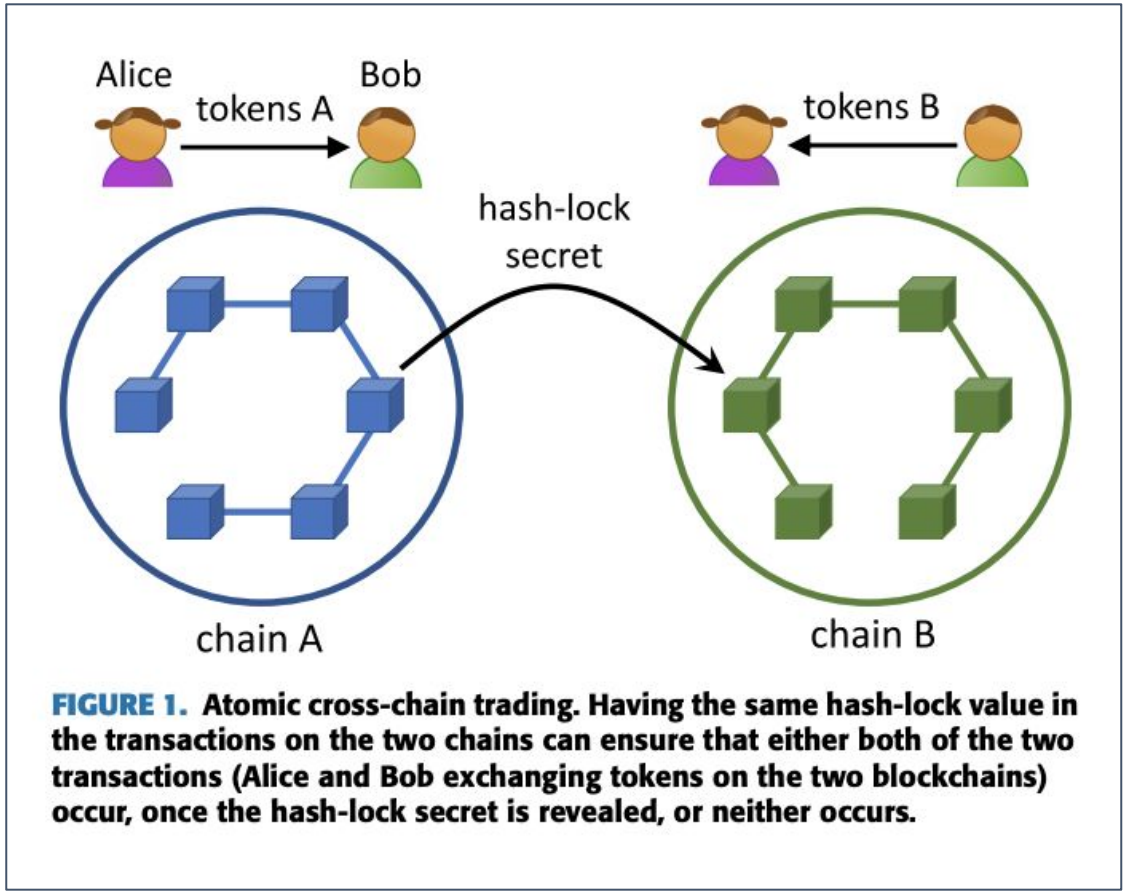


FIGURE 1. Atomic cross-chain trading. Having the same hash-lock value in the transactions on the two chains can ensure that either both of the two transactions (Alice and Bob exchanging tokens on the two blockchains) occur, once the hash-lock secret is revealed, or neither occurs.

Source: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8755830

SECTION 2/4

Options to achieve interoperability

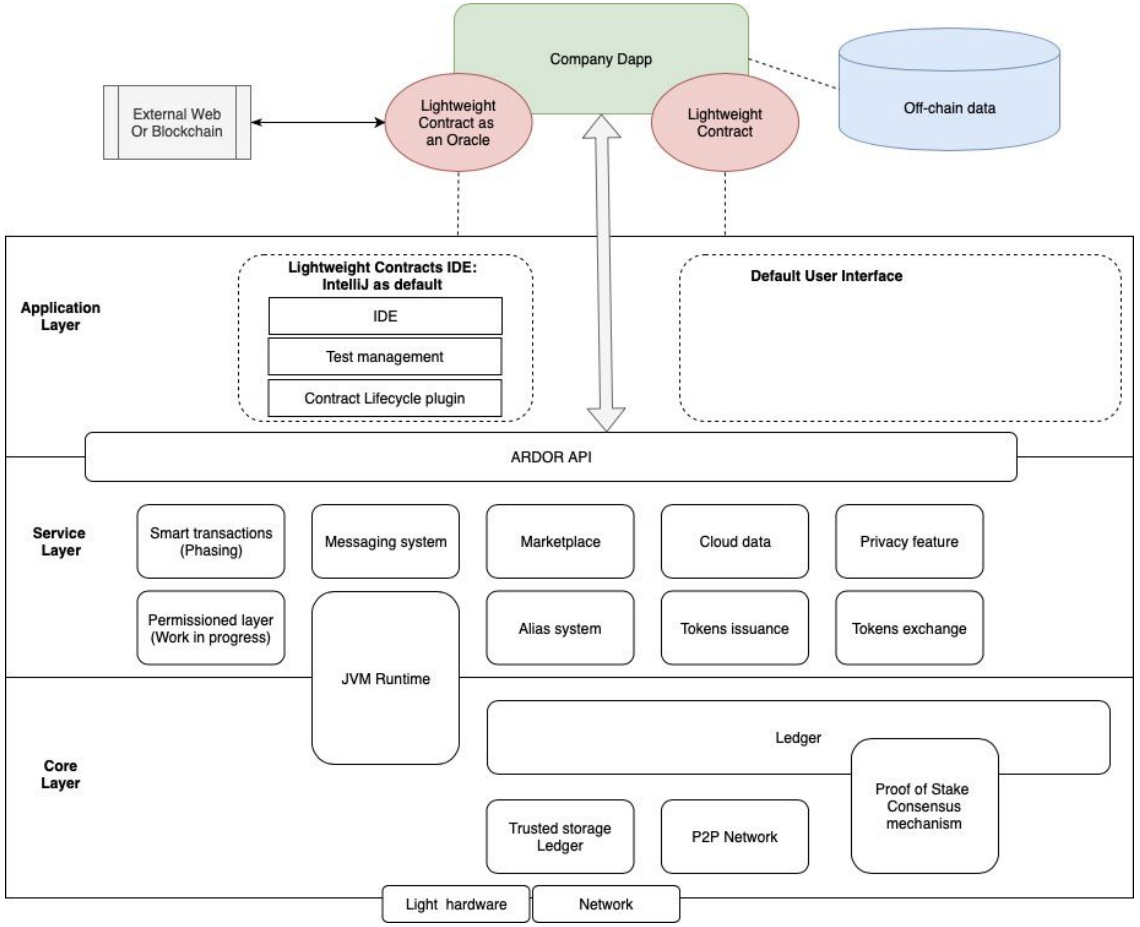
Atomic swaps

Oracles integration

Side chains vs child chains

Blockchain integration Bus

Oracles integration



SECTION 2/4

Options to achieve interoperability

Atomic swaps

Oracles integration

Side chains vs child chains

Blockchain integration Bus

Side chains vs child chains

	Side Chains	Ardor Child Chains
Structure	Side chains are independent blockchains that have a kind of "pegging mechanism", where at least one of the chains (main chain and side chain) is "aware" of the other chain and both tokens are pegged at a set ratio. Side chains need their own network security and block processing.	"Child Chains" of the Ardor platform are tightly integrated into the main Ardor parent chain. All transactions are processed and secured by the parent chain forgers. This makes cross-chain transactions possible. Pruning will be enabled on child chain transactions in order to significantly reduce blockchain bloat by pruning the transactions on regular basis from the blockchain.
Function	Transactions executed between the locks and unlocks of the main chain tokens don't bloat the main chain. As the technology of a side chain is connected to its main chain, it can be used to build on the developments of the main chain and introduce new features to the market.	Child chains serve as the transactional chains of the parent-child architecture, as the parent chain retains minimal features.

Source: https://www.jelurida.com/sites/default/files/JeluridaWhitepaper.pdf

SECTION 2/4

Options to achieve interoperability

Atomic swaps

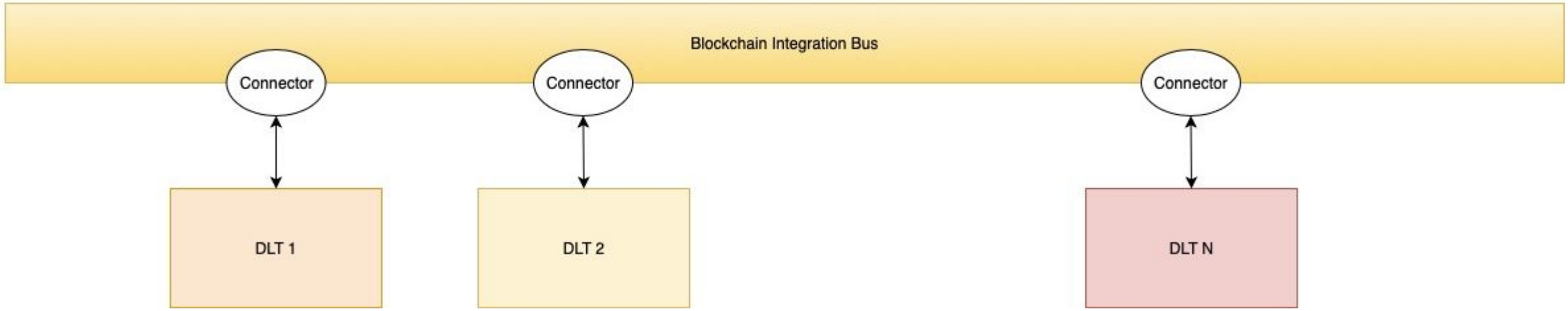
Oracles integration

Side chains vs child chains

Blockchain integration Bus

Blockchain Integration Bus

Hardware of Software Integration Bus able to interconnect the different connectors of an interledger protocol, aiming to achieve smart contract agreement in different ledgers



SECTION 3/4

Hyperledger quilt - Interledger Protocol

SECTION 3/4

Hyperledger quilt - Interledger Protocol

Architecture

ILP

Ardor integration

SECTION 3/4

Hyperledger quilt - Interledger Protocol

Architecture

ILP

Ardor integration

Architecture

Java implementation of the Interledger Protocol

- Easy to integrate in the Ardor stack
- Set of rules for enabling ledger interoperability
- Standard for a ledger-independent address format and data packet
- Framework for designing higher-level use-case-specific protocols

Source: https://interledger.org/rfcs/0001-interledger-architecture/

Architecture

README.md

Hyperledger Quilt

Discuss Interledger Forum | Follow @interledger 18k

circleci passing | codecov 73% | code quality A | issues 16 open

Quilt is an implementation of the Interledger protocol in Java.

Modules

The quilt project is organised as a Maven multi-module project. Each module exists in a subdirectory and has its own POM and README.

Dependency and plugin versions are managed in the parent project.

Issues are labelled and prefixed to make it easy to identify which project they relate to.

ilp-core

The ilp-core module is the base library for any Interledger projects providing service interfaces, event descriptions, exceptions and data models. It also includes an encoding framework and codecs for encoding and decoding ILP objects using the Octet Encoding Rules (OER).

open ilp-core issues 9

Source: https://github.com/hyperledger/quilt

SECTION 3/4

Hyperledger quilt - Interledger Protocol

Architecture

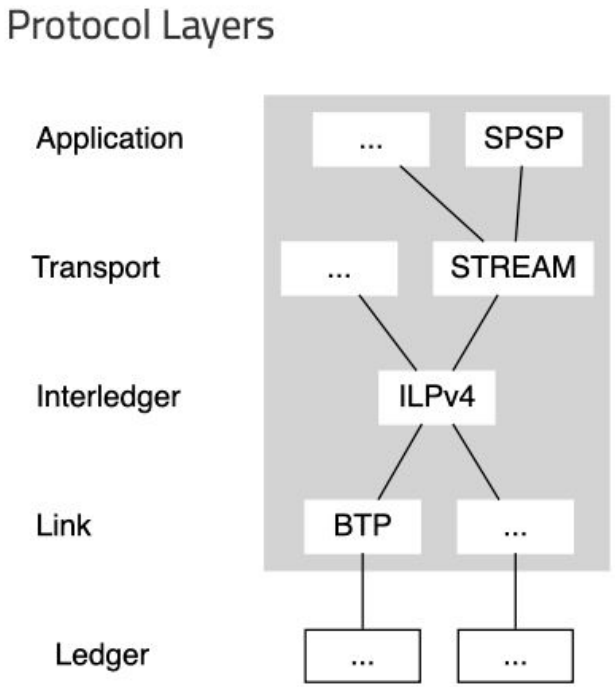
ILP

Ardor integration

Interledger protocol (ILP)

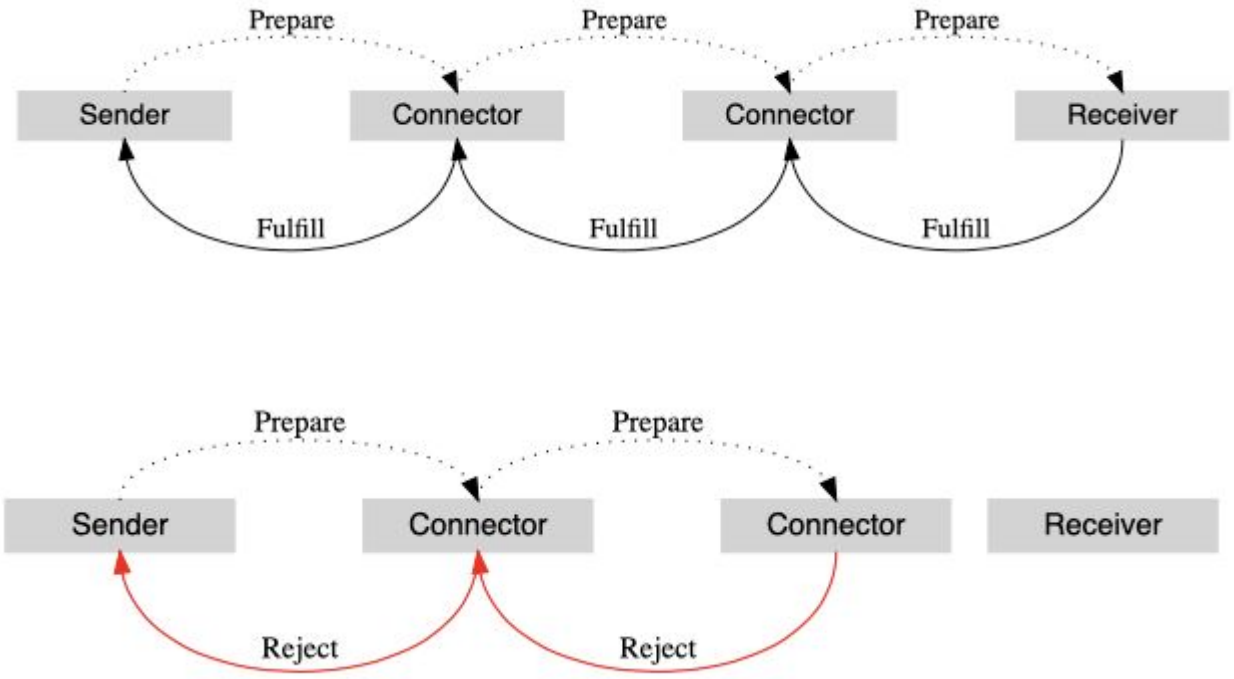
Interledger is a standard way of bridging financial systems. The Interledger architecture is heavily inspired by the Internet architecture described in RFC 1122, RFC 1123 and RFC 1009.

Interledger protocol (ILP)



Interledger protocol (ILP)

Flow:



SECTION 3/4

Hyperledger quilt - Interledger Protocol

Architecture

ILP

Ardor integration

Ardor integration

- Address generation
- Token transfer

SECTION 4/4

Demo