

Introduction on Interoperability of DLT systems

- Focus on Technological Developments and Standardization Trends -

'23. 9. 11

Dreamsecurity Co., Ltd.

- Contents -

- 1) DLT Interoperability Overview
- 2) DLT Interoperability Concept
- 3) DLT Interoperability Solution
- 4) DLT Interoperability Infrastructure
- 5) Conclusion

1) DLT Interoperability Overview

- DLT System
 - 1) Source DLT System
 - 2) Destination DLT System

- DLT Interoperability Mode
 - 1) Data Transfer
 - 2) Asset Transfer
 - 3) Asset Exchange

- DLT Interoperability Solution
 - 1) DLT Oracles
 - 2) Cross Authentication






- DLT Interoperability Infrastructure
 - 1) Direct Blockchain Interconnection
 - 2) Interconnected Blockchain-Based Approaches
 - 3) Application-Layer Interconnected Approaches

1) DLT Interoperability Overview

■ Constraints of Blockchain Platforms

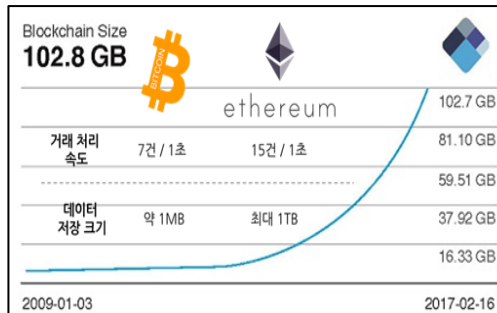
1) Blockchain Processing Performance

- ▶ Public blockchains (e.g., Bitcoin, Ethereum) offer 7-30 TPS,
- ▶ While consortium and private ones utilize PBFT for 1000-1500 TPS.
- ▶ Enhancing blockchain performance is crucial for stable service delivery with substantial data handling demands.

| |  Bitcoin |  Ethereum |  Bitcoin Cash |  Litecoin |  Dash |
|--|---|--|--|--|--|
| Median Confirmation Time | ~10 minutes | ~2 minutes | ~15 minutes | ~3 minutes | ~2 minutes |
| Number of Transactions Per Second | 14 | 10-20 | 56 | 56 | 28 |
| Maximum Number of Transactions Per Day | 1.2 million | 1.73 million | 4.8 million | 4.8 million | 2.4 million |
| Cost Per Transaction | \$2.34 | \$0.36 | \$0.07 | \$0.74 | \$0.15 |
| Blockchain Usage (# of operations in one day) | 370k MAY-14-2017 | 496k SEP-09-2017 | 137k AUG-16-2017 | 44k SEP-01-2017 | 9.5k AUG-19-2017 |
| Blockchain Length (# of blocks produced to date) | 490k | 4.4 million | 495k | 1.3 million | 752k |

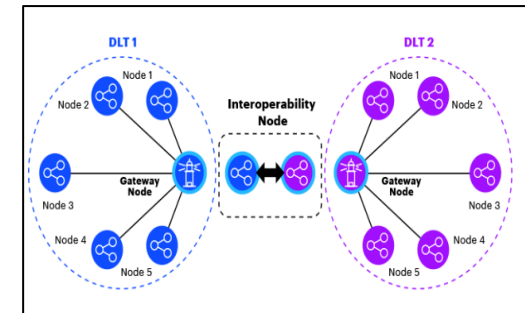
2) Ledger Data Growth

- ▶ Blockchain, as a distributed shared ledger, faces increasing data size, leading to higher costs for processing.
- ▶ Approaches like Ethereum's sharding and using off-chain storage solutions like IPFS are utilized to handle this growth.
- ▶ Solving blockchain storage capacity issues is essential to store and provide stable services for large-scale/large-volume data.



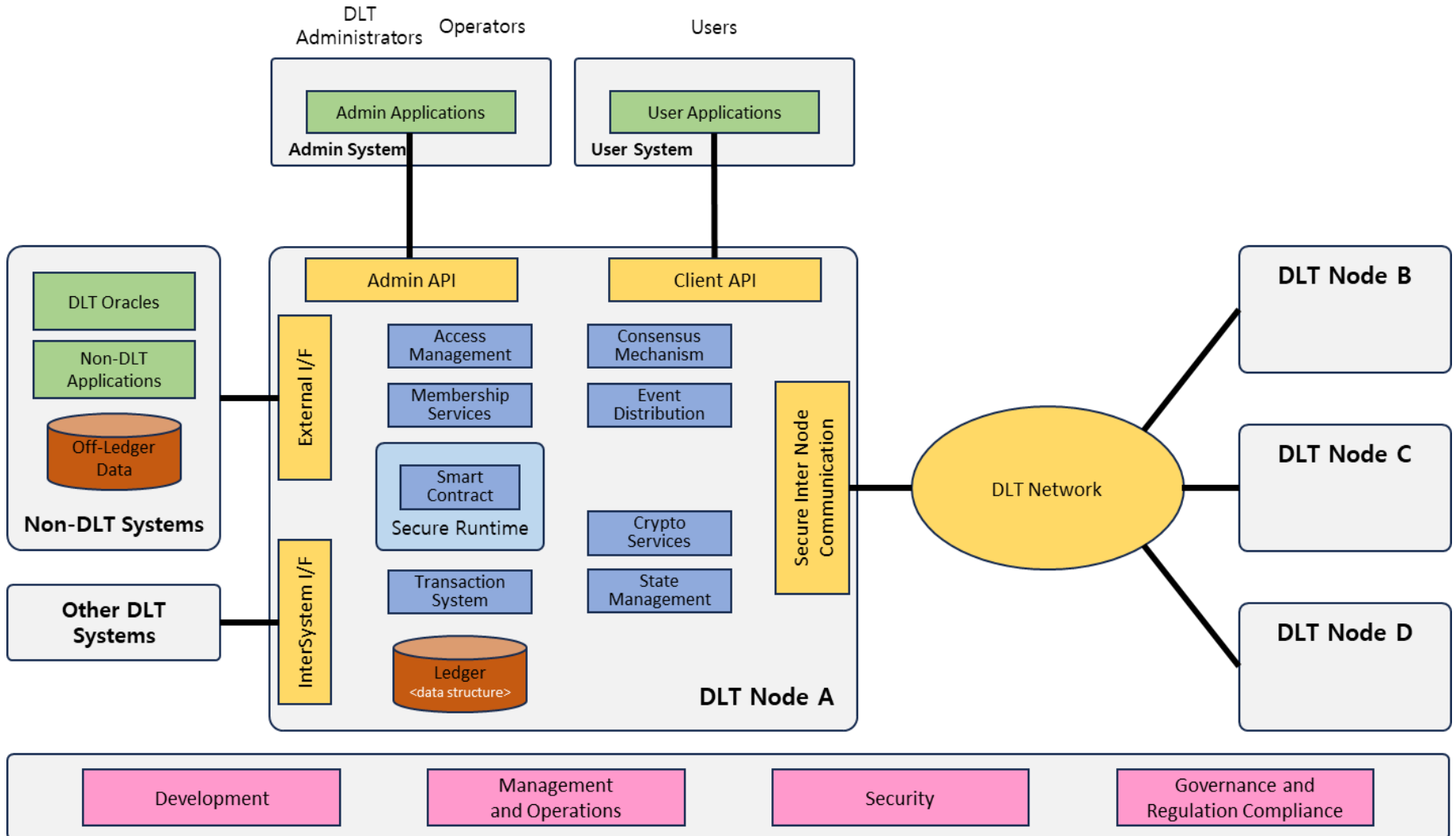
3) Blockchain Interoperability

- ▶ As various blockchain ecosystems grow, industrial use rises, demanding more system interoperability.
- ▶ Techniques like sidechains and notary schemes facilitate asset transfers, smart contracts, and scalability improvements.
- ▶ Standardizing blockchain interoperability is nascent, requiring national strategies via local tech development and standardization.



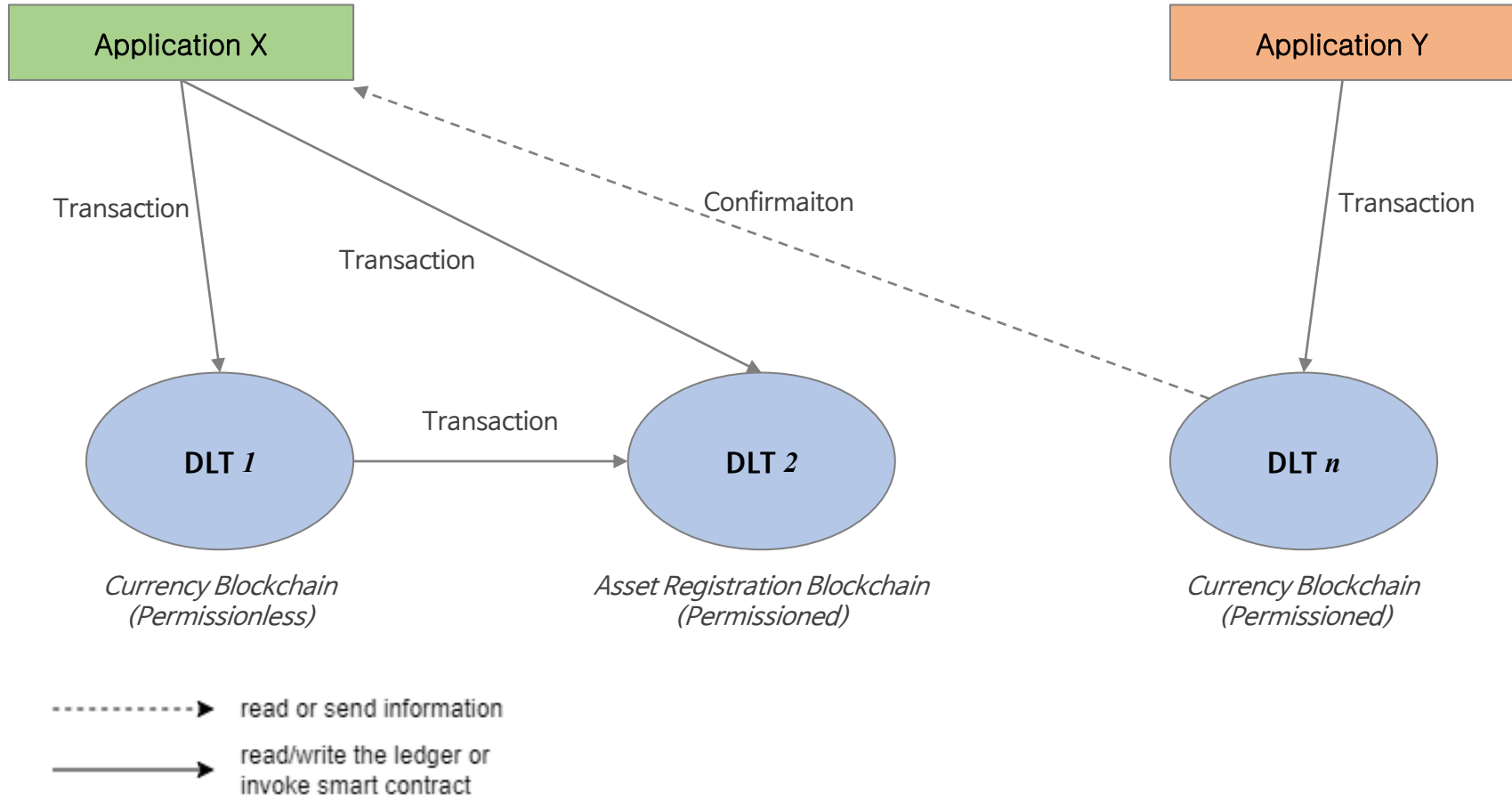
2) DLT Interoperability Concept

- Functional elements of a DLT system



2) DLT Interoperability Concept

- Interoperability Types

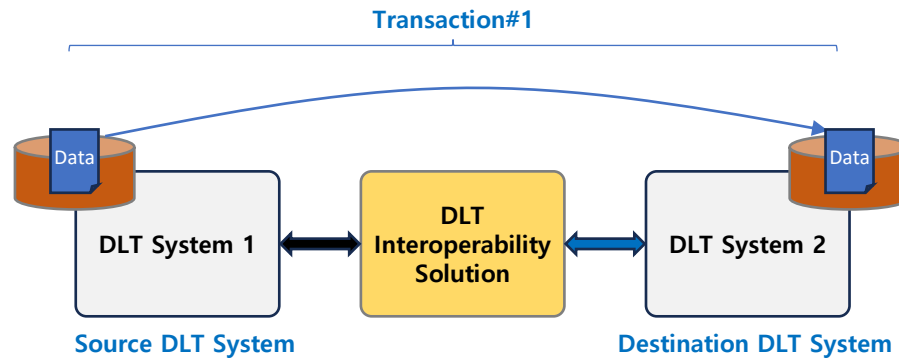


Source : Llambias, Guzman; Bradach, Bruno; Nogueira, Juan; González, Laura; Ruggia, Raúl: Gateway-based Interoperability for DLT. TechRxiv. 2023

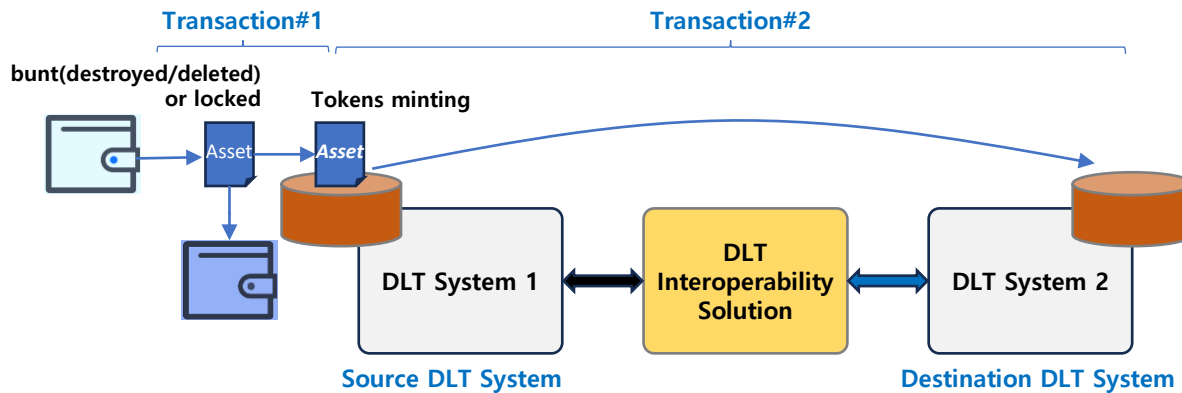
2) DLT Interoperability Concept

- DLT Interoperability Modes - The scope and content of interoperability processing

1) Data Transfer



2) Asset Transfer

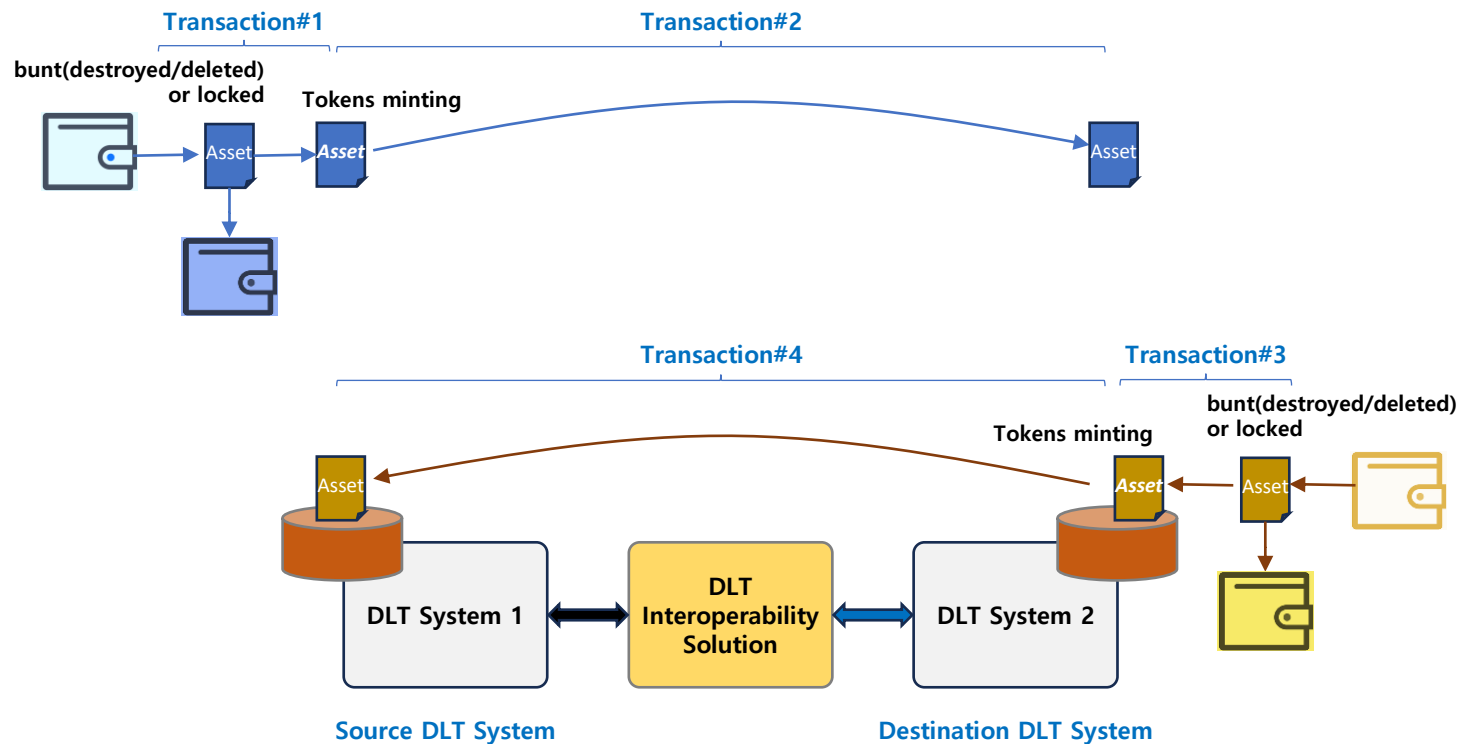


2) DLT Interoperability Concept

- DLT Interoperability Modes - The scope and content of interoperability processing

3) Asset Exchange

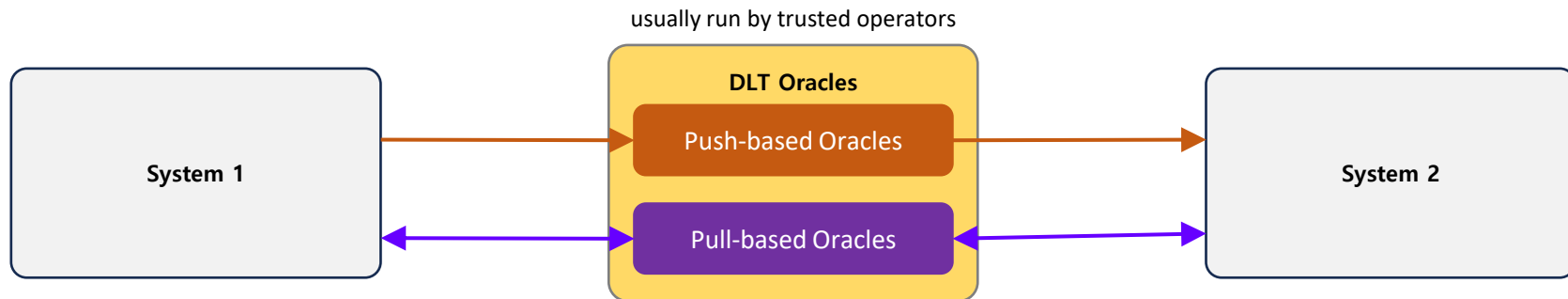
- Assets are exchanged between accounts in their respective distributed ledgers, i.e., no transfers across DLT networks occur.



3) DLT Interoperability Solution

- DLT Oracle

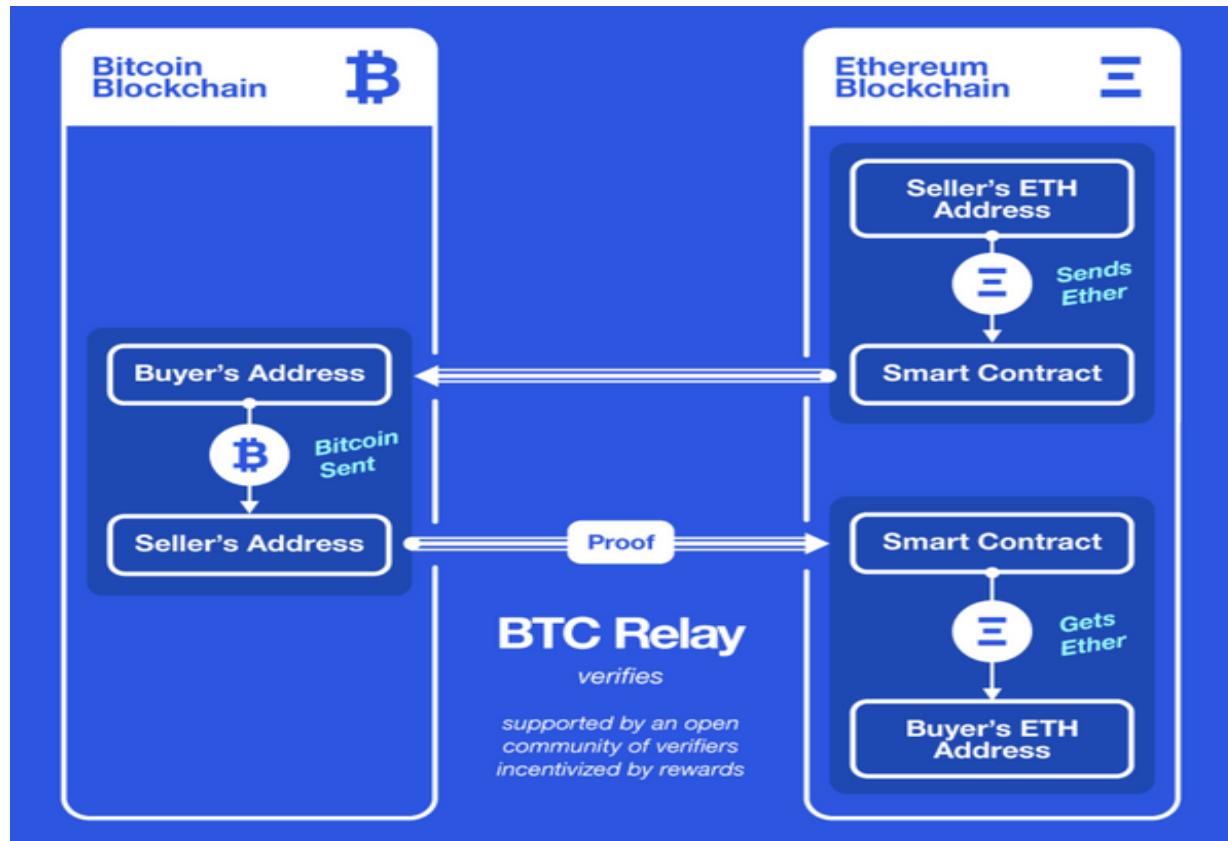
- DLT oracle solutions are used for both the data transfer and asset transfer interoperability modes.
- A DLT oracle is a service that updates a distributed ledger using data from outside of a DLT system. DLT oracles therefore allow data (including assets) to move from a source external system into a destination DLT system.



- **Push-based data transfer oracles:** These services add data from an external system onto a destination DLT system without an explicit request from a transaction on the destination DLT system.
(An example is the [BTC relay](#).)
- **Push-based asset transfer oracles:** These services add data (representing fungible or nonfungible value) onto a destination DLT system without an explicit request from a transaction on the destination DLT system.
(An example is the [Bitcoin to Ethereum wBTC bridge](#).)
- **Pull-based data transfer oracles:** upon request from a transaction on the destination DLT system, these services fetch data from a source system and add the data to a destination DLT system (via transactions).
- **Pull-based asset transfer oracles:** upon request from a transaction on the destination DLT system, these services fetch data (representing representing fungible or non fungible value) from source system and add the data to a destination DLT system (via a transaction).
(An example is a transaction to a [Rollup smart contract on Ethereum](#), causing token withdrawals from the Rollup network onto the Ethereum network. Another example is a Bitcoin transaction causing a withdrawal of tokens from a Bitcoin payment channel back onto the Bitcoin main network.)

3) DLT Interoperability Solution

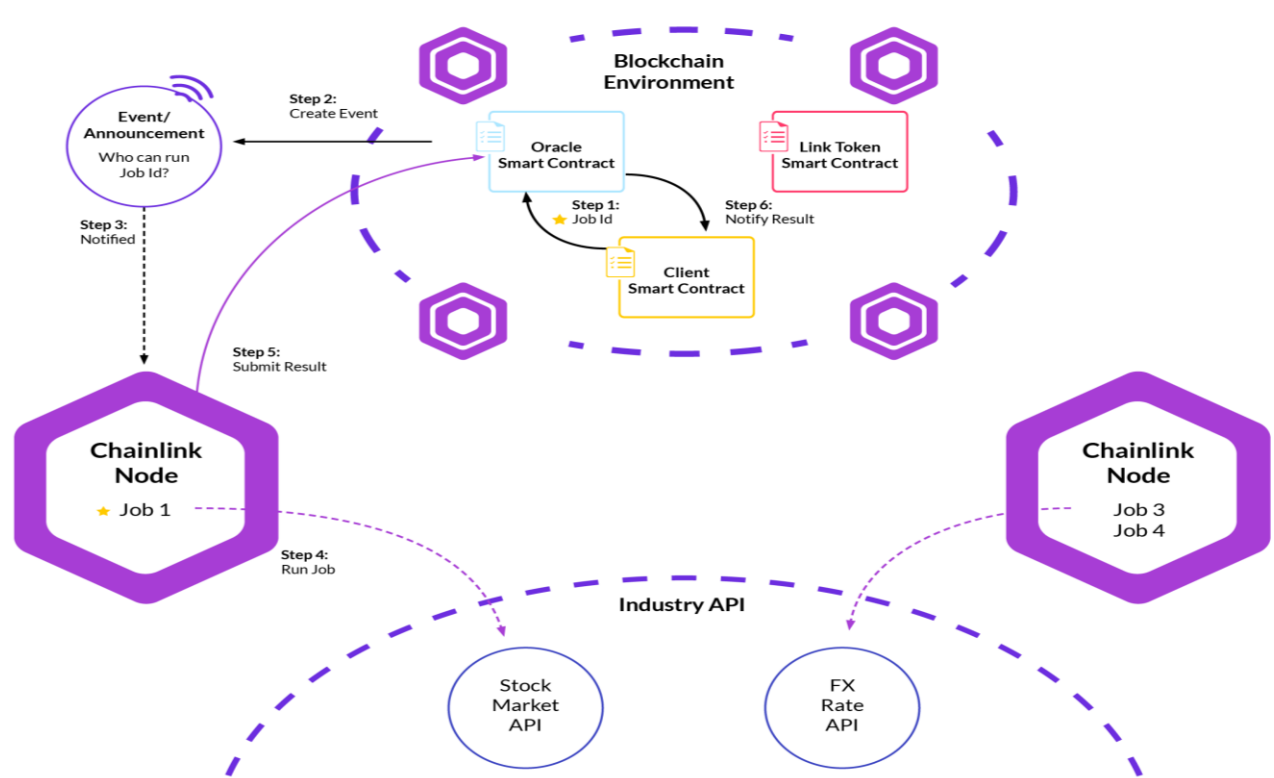
- DLT Oracle
 - (Push-based data transfer oracles) Still, like all oracles, they will add the fetched data into the destination DLT system via a transaction. An example is the BTC relay.



3) DLT Interoperability Solution

- DLT Oracle

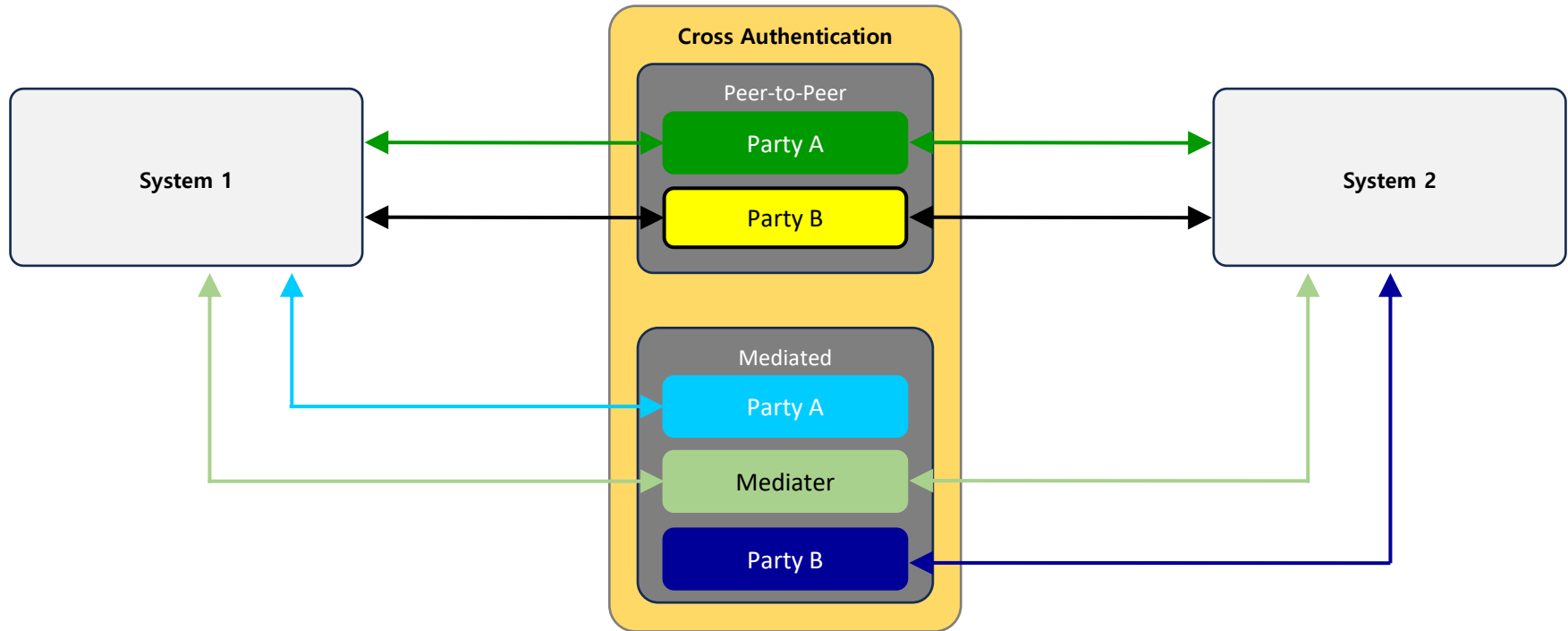
- (Pull-based data transfer oracles) Pull-based data transfer oracles on these DLT systems only require one transaction to complete the data request process as the data is fetched from the source system by nodes, before the transaction requesting this data, is signed and finalised in the ledger.



3) DLT Interoperability Solution

- **Cross Authentication**

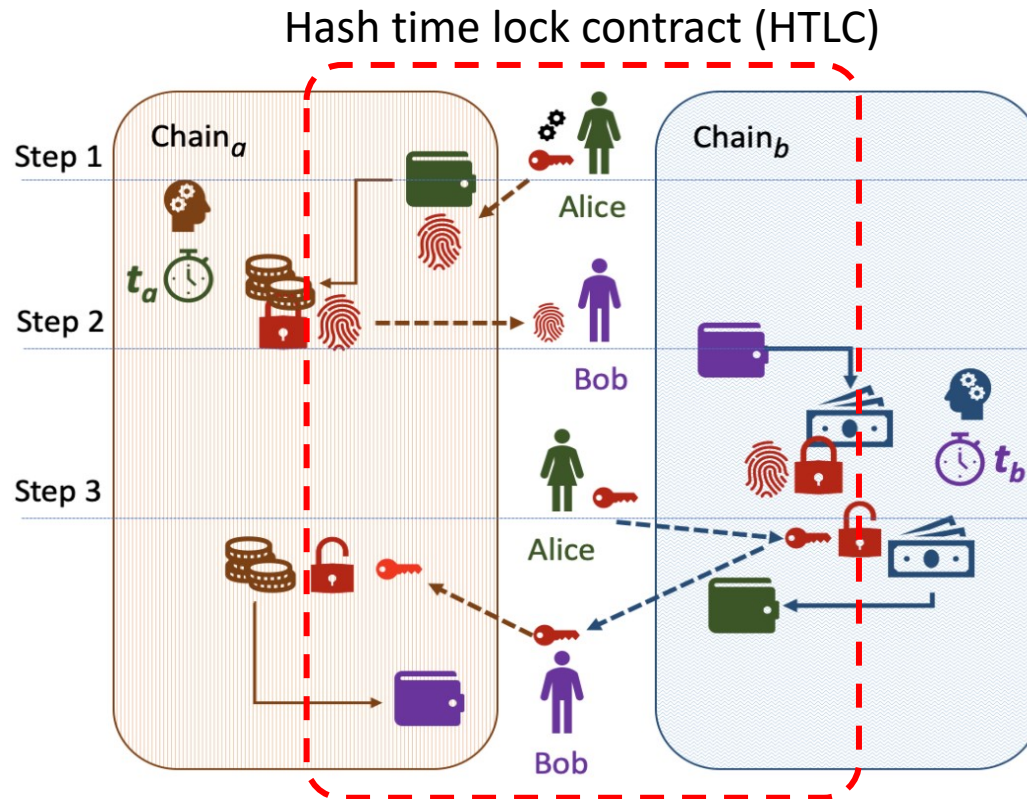
- Cross-authentication interoperability solutions allow parties to exchange assets across DLT systems, where each party adds a transaction on each DLT system. To this end, parties need to authenticate on both chains to perform the transfers.
- Peer-2-peer asset exchanges corresponds to one asset exchange with non-mediated communication.
- On the other hand, mediated asset exchanges are cross-authentication solutions with an additional party/parties.



3) DLT Interoperability Solution

- Cross Authentication

- Peer-2-peer asset exchanges corresponds to one asset exchange with non-mediated communication.
- The de-facto method for implementing this scheme are Hash Lock Time Contracts (HTLCs), where both parties deploy (or utilise) a smart contract in each chain that transfers the right number of coins to the other party.



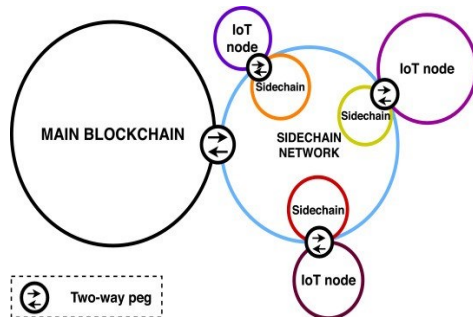
Source : Hash Lock Time Contracts (HTLCs) [Hash Time Locked Contracts \(HTLCs\) Explained | by Liquidity | Liquidity | Medium](#)

4) DLT Interoperability Infrastructure

▪ Trends in DLT Interoperability Research and Developments

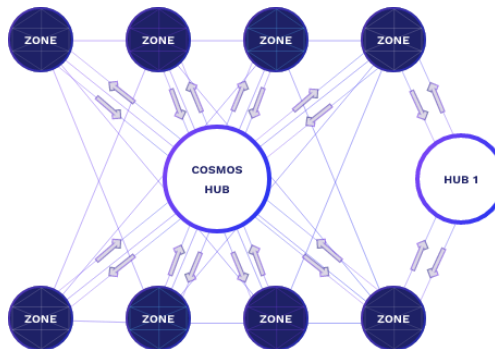
1) Public Connectors

- ▶ The following methods are utilized:
 - Sidechain & Relay
 - Notary Scheme
 - Hash-locking
- ▶ These approaches are actively researched and widely used for inter-chain asset exchanges between public blockchains
- ▶ They have limitations in supporting diverse transaction types.



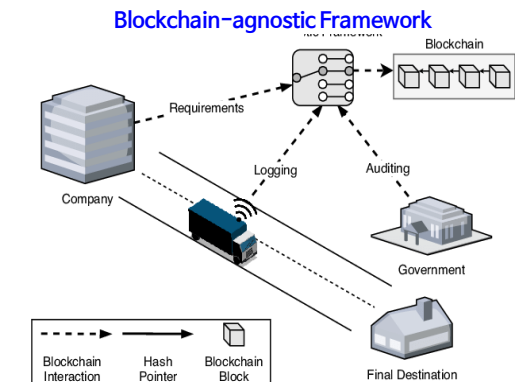
2) Blockchain of Blockchains

- ▶ The following approaches have been developed:
 - Polkadot
 - Cosmos
- ▶ Utilizing the BOB framework, separate blockchains are created to encompass various other blockchains.
- ▶ However, lack of interoperability between BOBs leads to operational limitations based on user choices.



3) Hybrid Connectors

- ▶ The following methods have been developed:
 - Blockchain-agnostic protocols
 - Blockchain migration
- ▶ These approaches focus on providing interoperability between public and private blockchains
- ▶ These are deemed suitable for future considerations of blockchain interoperability across diverse domains.



[출처] Toward a Policy-based Blockchain Agnostic Framework, 2019 IFIP/IEEE International Symposium on Integrated Network Management (IM2019)

Source : RAFAEL BELCHIOR, ANDRÉ VASCONCELOS, SÉRGIO GUERREIRO, and MIGUEL CORREIA, "A Survey on Blockchain Interoperability: Past, Present, and Future Trends", 2021

4) DLT Interoperability Infrastructure

- Overview of DLT Interoperability Infrastructure of ISO TC307

- The operational approaches for technical elements supporting interactions between different systems are as follows:

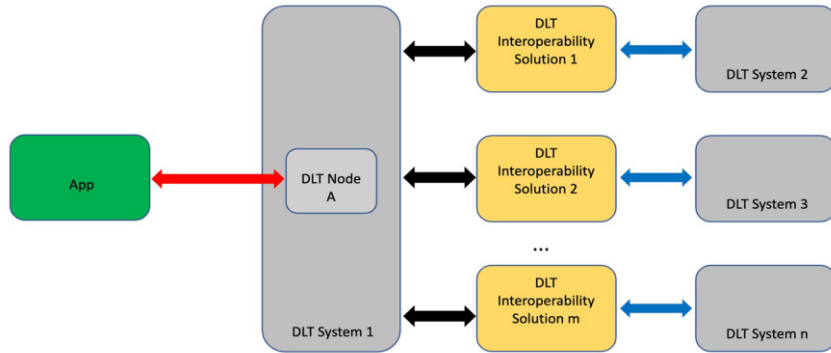


Figure 1: An App connecting directly to one DLT node of one DLT system to interact with multiple DLT systems

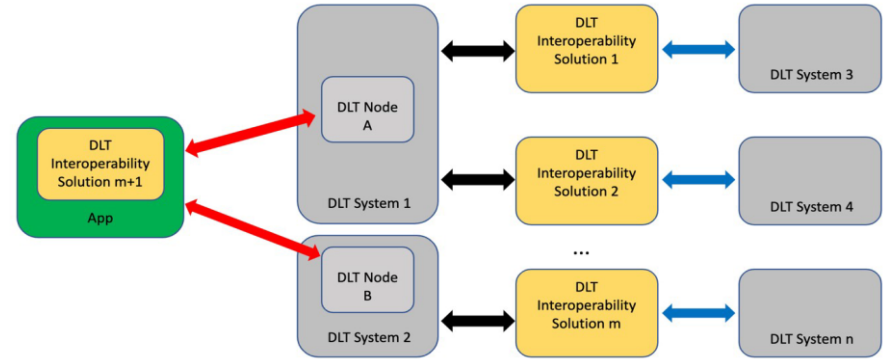


Figure 2: An App interacting with multiple DLT systems via connecting directly to one DLT node of multiple DLT systems

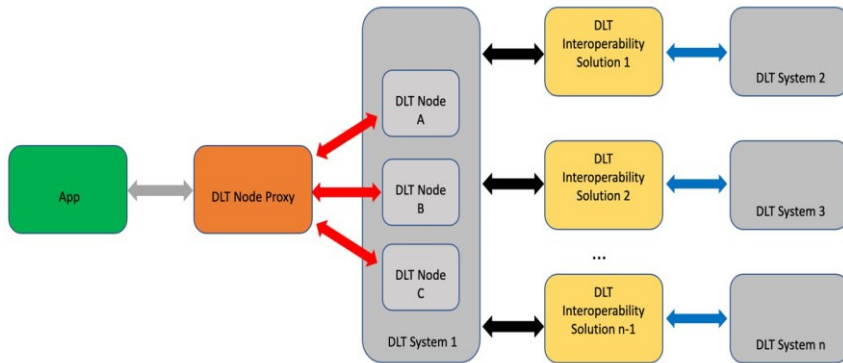


Figure 3: An App connecting directly to a DLT node proxy of one DLT system to interact with multiple DLT systems

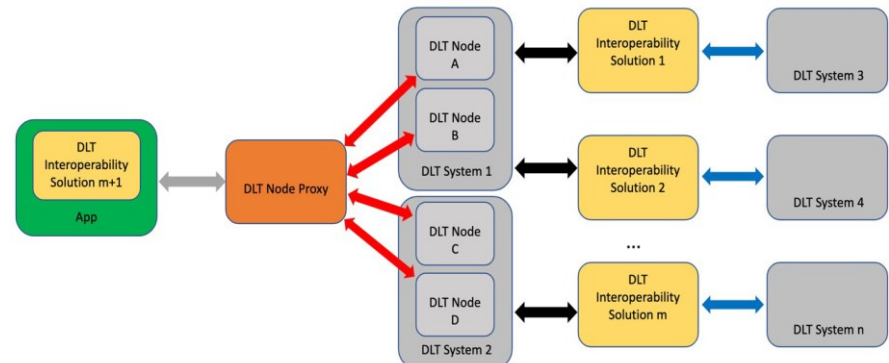


Figure 4: An App interacting with multiple DLT systems via connecting directly to a DLT node proxy of multiple DLT systems

4) DLT Interoperability Infrastructure

- Overview of DLT Interoperability Infrastructure of ISO TC307

- The operational approaches for technical elements supporting interactions between different systems are as follows:

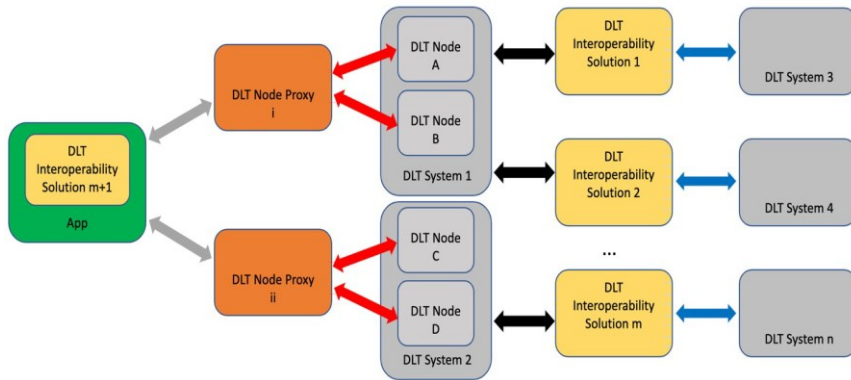


Figure 5: An App interacting with multiple DLT systems via connecting directly to multiple DLT node proxies of different DLT systems

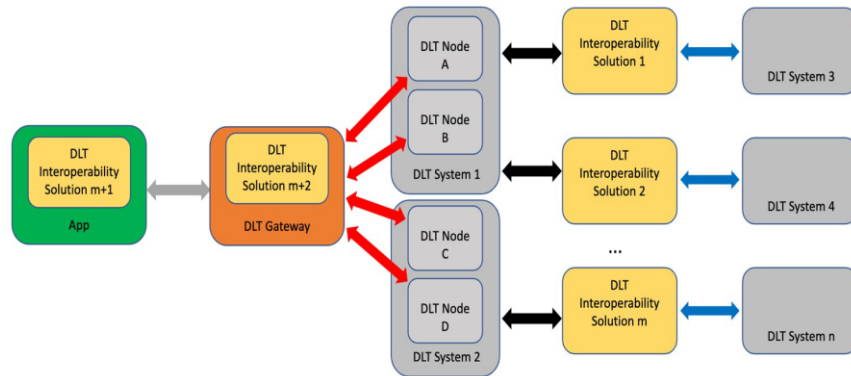


Figure 6: An App interacting with multiple DLT systems via connecting directly to a DLT gateway of multiple DLT systems

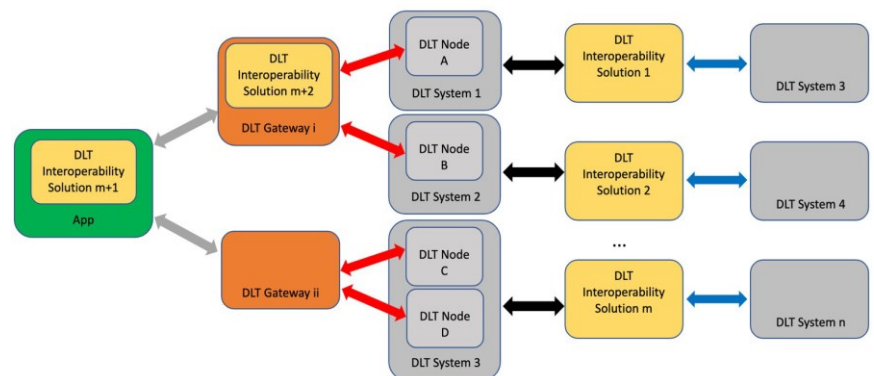
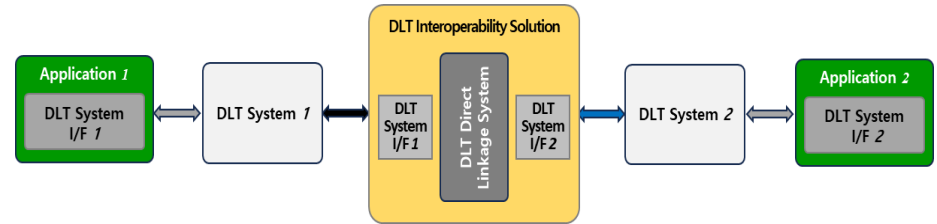
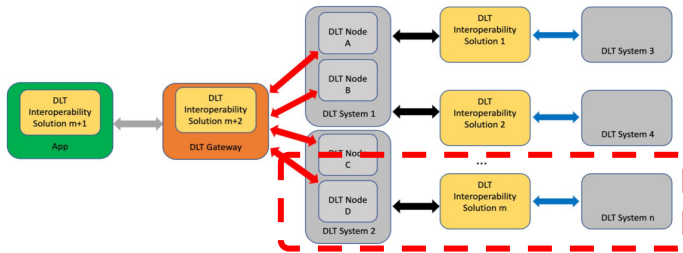


Figure 7: An App interacting with multiple DLT systems via connecting directly to multiple DLT gateways of different DLT systems

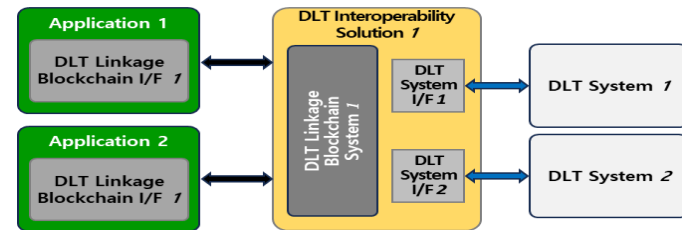
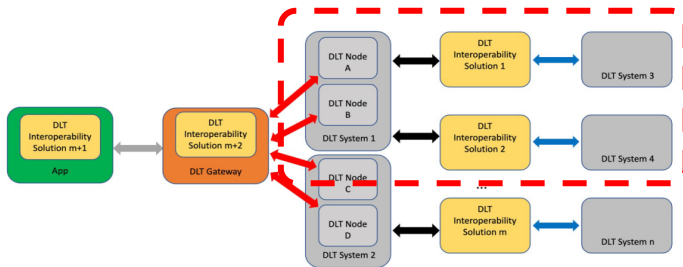
4) DLT Interoperability Infrastructure

- Analysis of DLT Interoperability Infrastructure of ISO TC307

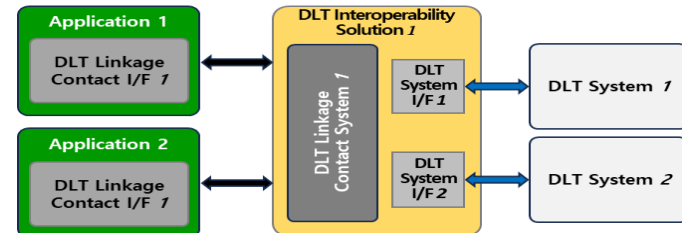
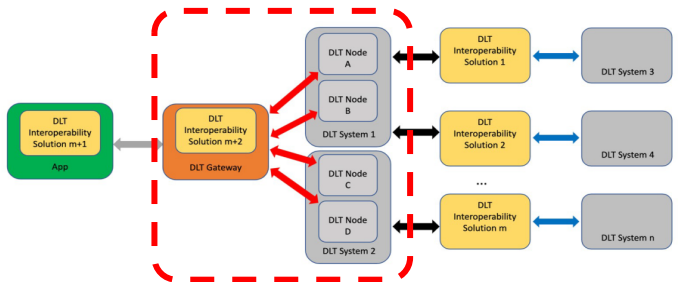
1) Interoperability through Direct Blockchain Interconnection (so-called "Public Connectors")



2) Interoperability through Interconnected Blockchain-Based Approaches (so-called "Blockchain of Blockchains")



3) Interoperability through Application-Layer Interconnected Approaches (so-called "Hybrid Connectors")



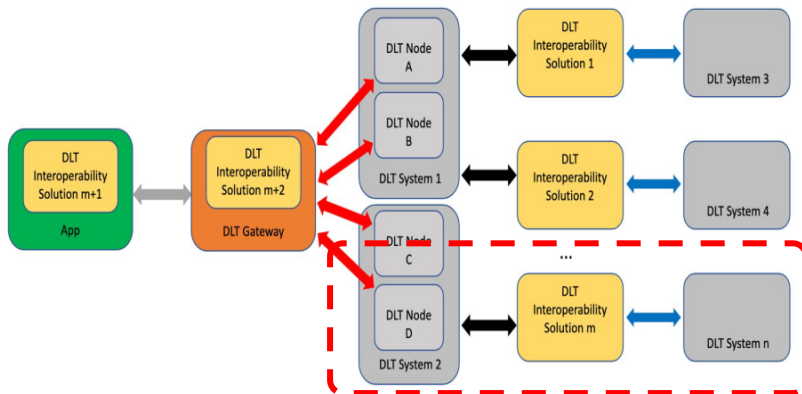
4) DLT Interoperability Infrastructure

▪ Analysis of DLT Interoperability Infrastructure of ISO TC307

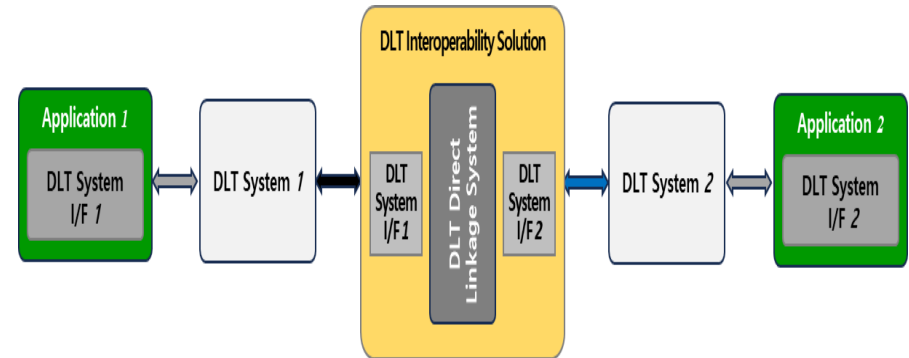
1) Interoperability through Direct Blockchain Interconnection

- As a method to provide interoperability through direct linkage within the blockchain layer, various approaches are employed. These include protocols enabling connectivity with different blockchains, smart contracts for interchain communication, and interoperability between sidechains and mainchains.
- For instance, techniques like Atomic Swaps to exchange cryptocurrencies across different blockchains, or propagating events from one blockchain to another for interaction, are encompassed in this category.

[Infrastructure of ISO TC307]



[Infrastructure of Direct Blockchain Integration]

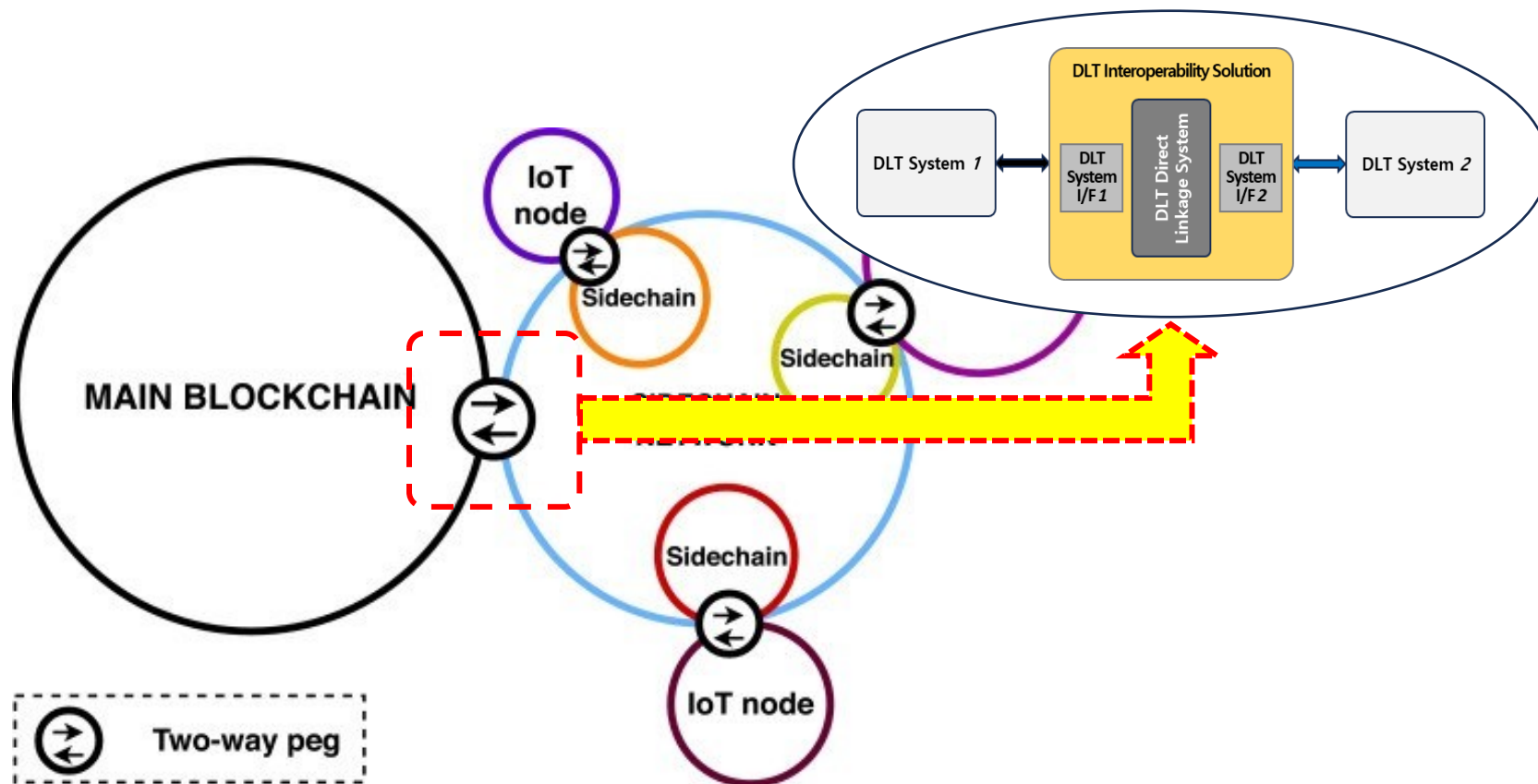


4) DLT Interoperability Infrastructure

- Analysis of DLT Interoperability Infrastructure of ISO TC307

1) Interoperability through Direct Blockchain Interconnection

[Sidechains based on Two-way Peg]



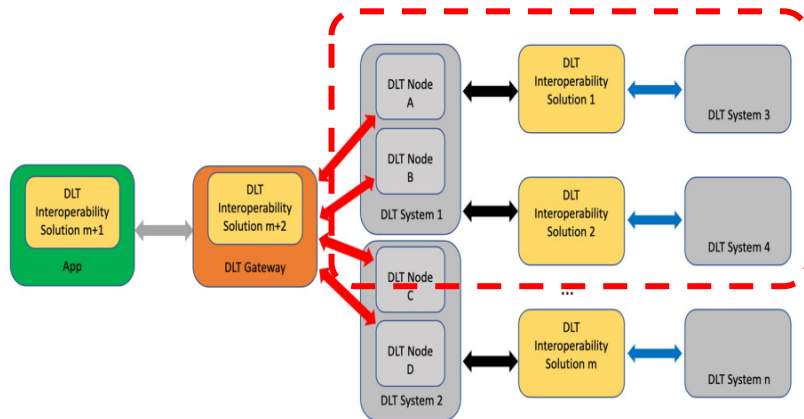
4) DLT Interoperability Infrastructure

- Analysis of DLT Interoperability Infrastructure of ISO TC307

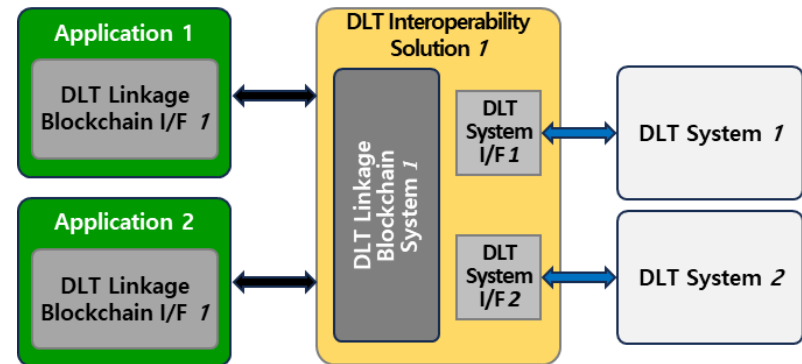
2) Interoperability through Interconnected Blockchain-Based Approaches

- Various technologies and protocols are being developed to facilitate interconnectivity between different blockchains through the utilization of interlinked blockchains.
- For example, methods like employing Polkadot's Substrate framework to connect and enable interactions among diverse blockchains, or utilizing Cosmos' Inter-Blockchain Communication (IBC) protocol to establish secure and reliable communication between blockchains, fall under this category

[Infrastructure of ISO TC307]



[Infrastructure of Connected Blockchain-Based Approaches]

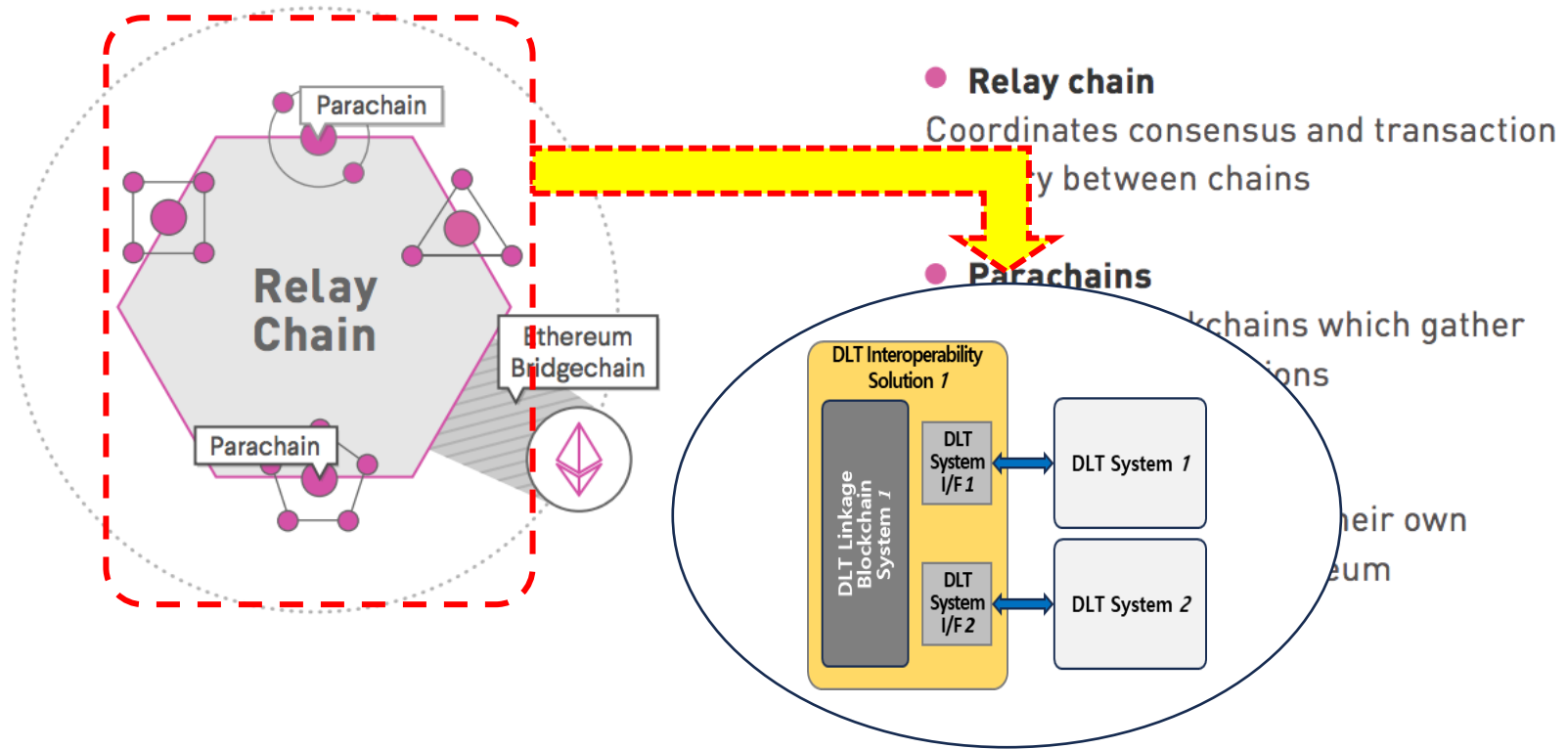


4) DLT Interoperability Infrastructure

- Analysis of DLT Interoperability Infrastructure of ISO TC307

2) Interoperability through Interconnected Blockchain-Based Approaches

[Relay chain, parachains, and bridges in the Polkadot network]



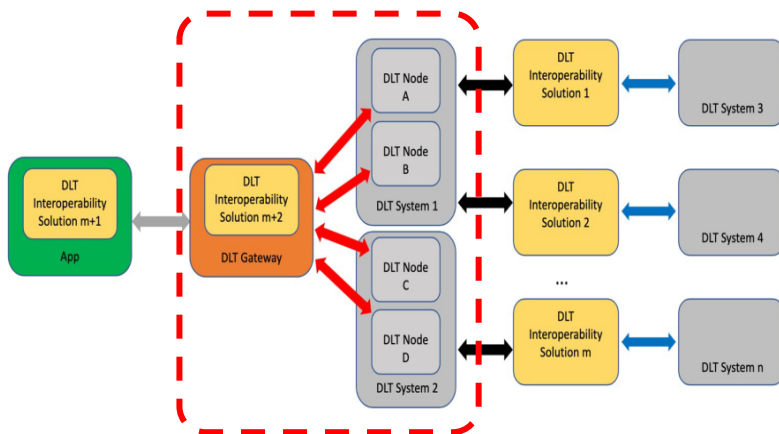
4) DLT Interoperability Infrastructure

- Analysis of DLT Interoperability Infrastructure of ISO TC307

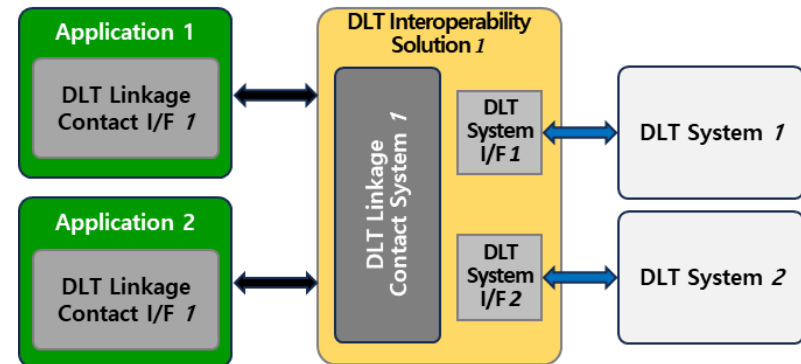
3) Interoperability through Application-Layer Interconnected Approaches

- As a method of providing interoperability at the application layer, standardized data formats, API interfaces, and protocols can be utilized.
- For instance, using standardized data formats for exchanging data between different blockchains or employing API interfaces to facilitate interactions with other blockchains are among the strategies in this category.

[Infrastructure of ISO TC307]



[Infrastructure of Application-Layer Connected Approaches]



4) DLT Interoperability Infrastructure

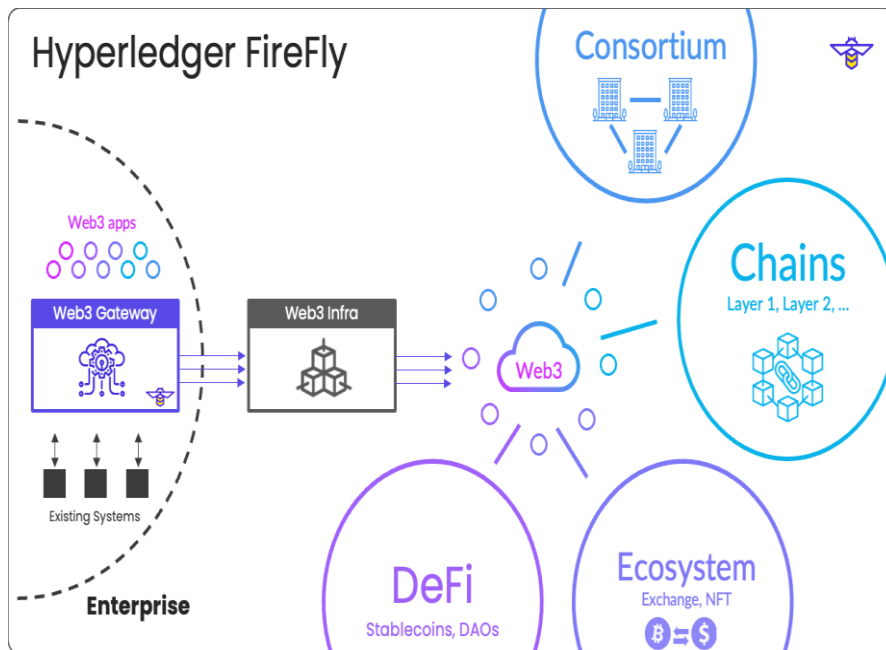
- Analysis of DLT Interoperability Infrastructure of ISO TC307

3) Interoperability through Application-Layer Interconnected Approaches

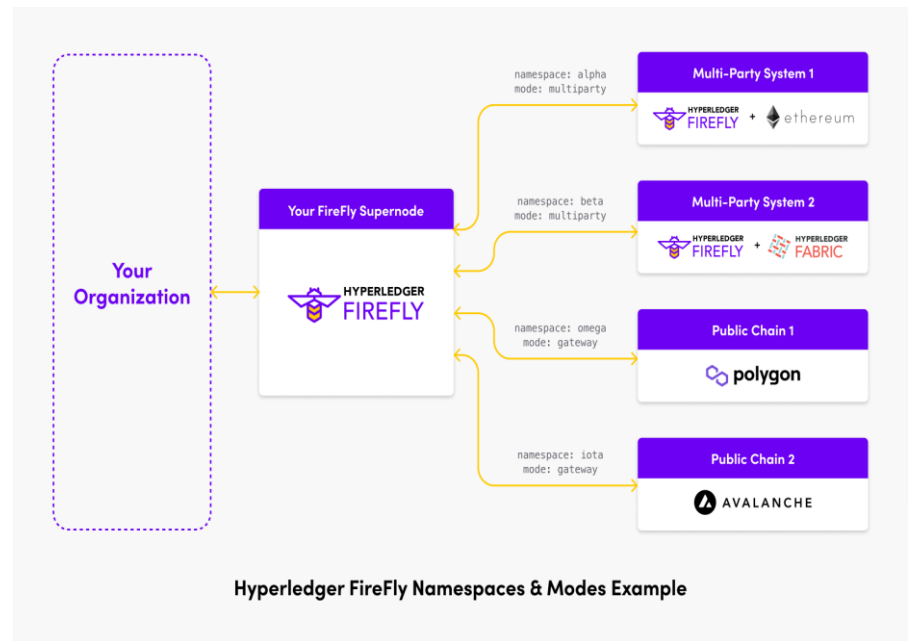
[Hyperledger FireFly]

FireFly is an organization's gateway to Web3, including all the blockchain ecosystems that they participate in and integrating into all of the different types of decentralized technologies that exist in Web3.

Operational Concept



Operational Structure



4) DLT Interoperability Infrastructure

- Analysis of DLT Interoperability Infrastructure of ISO TC307

3) Interoperability through Application-Layer Interconnected Approaches

[QUANT's Overledger]

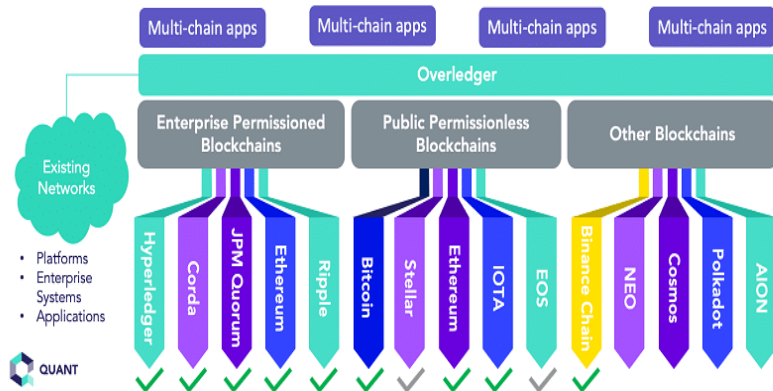
Overledger enables you to deploy your use case on multiple chains, issue chain-agnostic digital assets, connect them to other networks, and develop multi-chain applications quickly without compromising on security.

Operational Concept

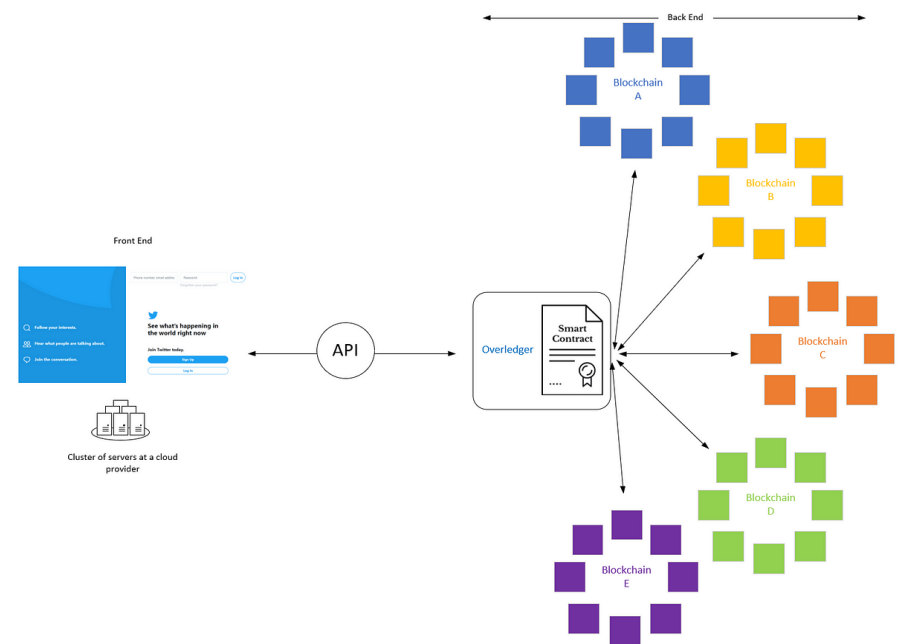


An Enterprise Operating System that interconnects blockchains, enterprise platforms and networks

- **Interoperable** - Connect **any** network to **any** network without overhead or limits
- **Hyper-decentralized** applications that run and store data on multiple blockchains



Operational Structure



5) Conclusion

- **Key Content Summary**

- 1) DLT Interoperability Solution**

- Oracle
- Cross Authentication

- 2) DLT Interoperability Infrastructure**

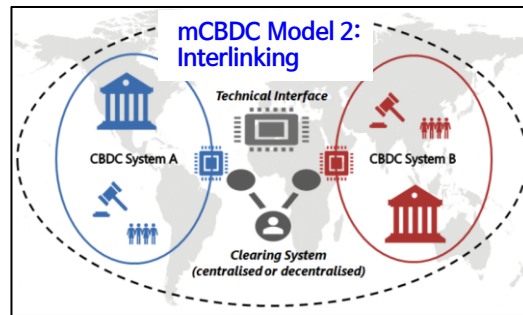
- Direct Blockchain Interconnection (so-called "Public Connectors")
- Interconnected Blockchain-Based Approaches (so-called "Blockchain of Blockchains")
- Application-Layer Interconnected Approaches (so-called "Hybrid Connectors")

5) Conclusion

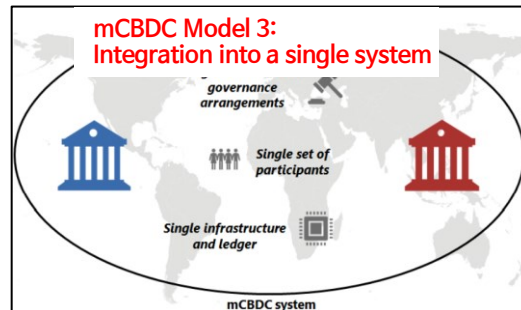
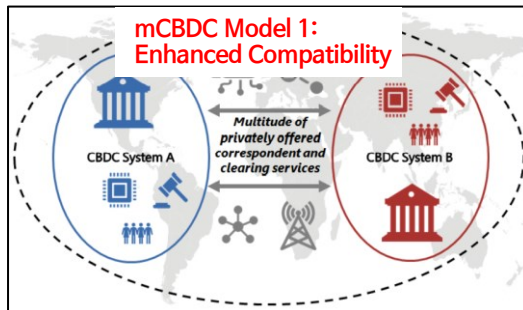
- Key Content Summary

- The use cases for the hybrid connector approach will also increase.

[Blockchain Interoperability Service Model of Bank for International Settlements (BIS)]



CBDC : Central Bank Digital Currency
mCBDC : multi-CBDC



Considering Interoperability Support Ensuring Independent Operation of Blockchains

mCBDC Model 1

- ▶ Utilization of Technology, Legal, Regulatory, and Supervisory Standards including Message Formats, Data Requirements, and User Interfaces
- ▶ Challenges Exist in Establishing Common Standards

mCBDC Model 2

- ▶ Connecting Systems from Different Shared Technology Environments (Centralized or Decentralized)

mCBDC Model 3

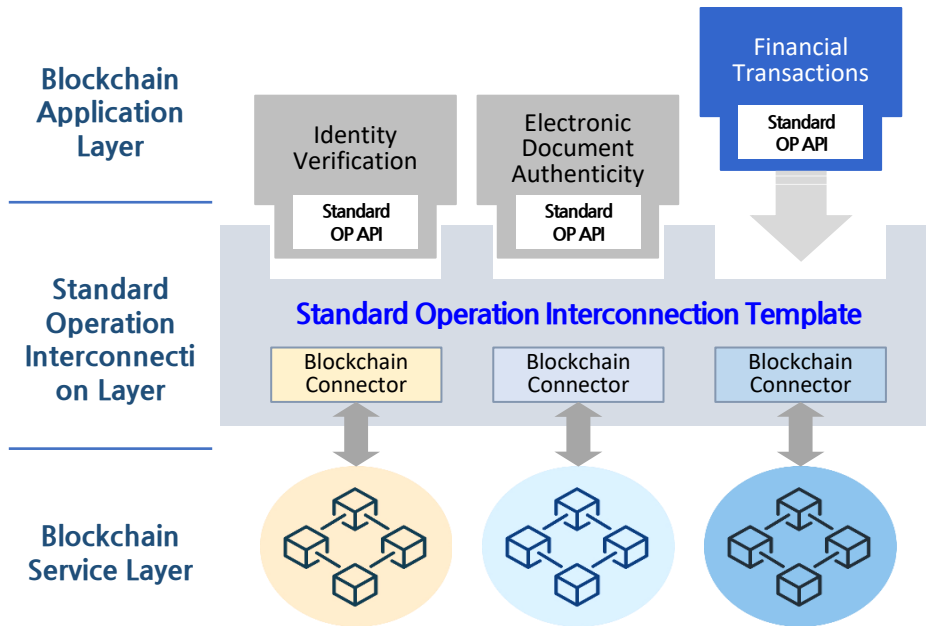
- ▶ Operationalizing through a Single Platform with Unified Technology and Regulations

5) Conclusion

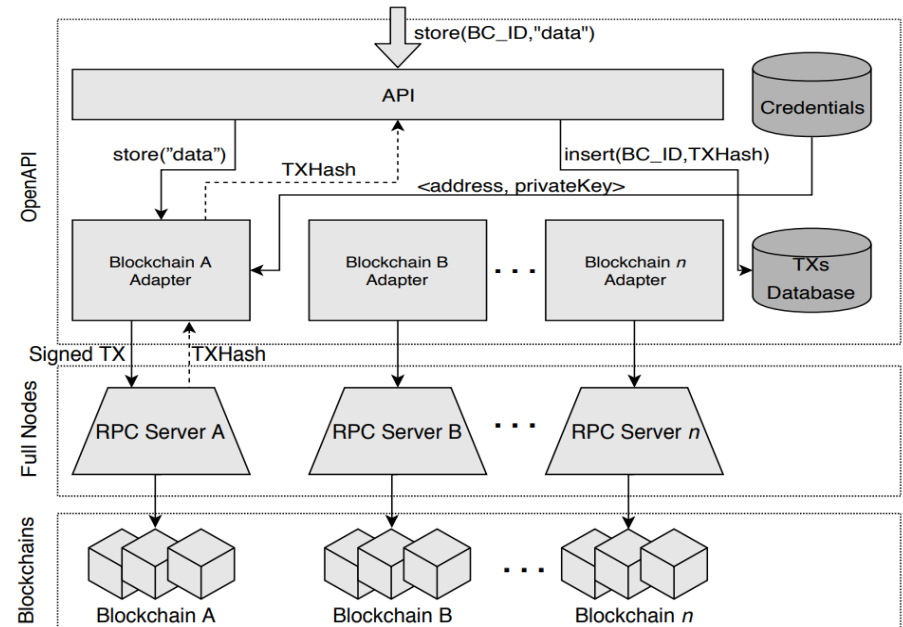
- Future Action Plans

- Implementation and Validation of Application-Layer Interconnected Interoperability Service

[Standard Operation Interconnection Architecture]



[Architecture Implementation Cases]



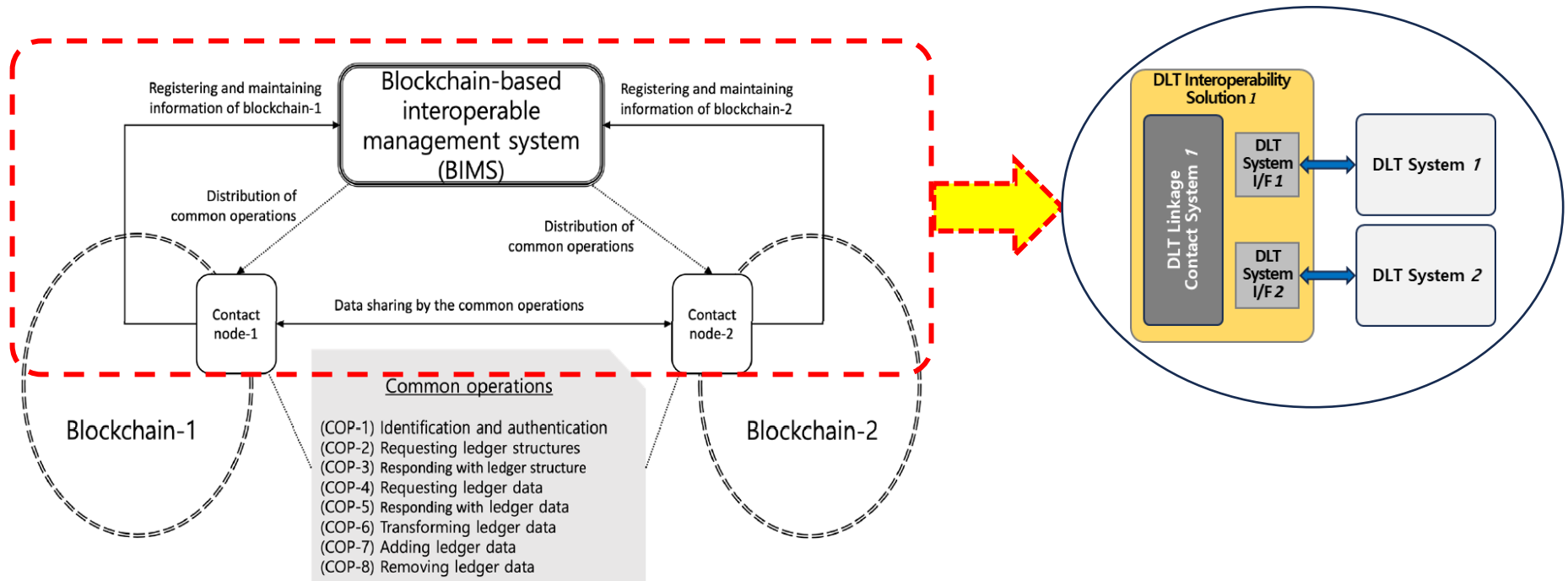
[Source] Toward a Policy-based Blockchain Agnostic Framework, 2019 IFIP/IEEE International Symposium on Integrated Network Management(IM2019)

5) Conclusion

- Future Action Plans

- Standardization of Application-Layer Interconnected Interoperability Service

[Standard Operation-Based Interoperability Service of Application-Layer]



Source : Proposal of Decentralized P2P Service Model for Transfer between Blockchain-Based Heterogeneous Cryptocurrencies and CBDCs, Keundug Park and Heung-Youl Youm, 2022


5) Conclusion

- Future Action Plans

2) Standardization of Application-Layer Interconnected Interoperability Service

[ITU-T SG17 Standardization Contribution Report]

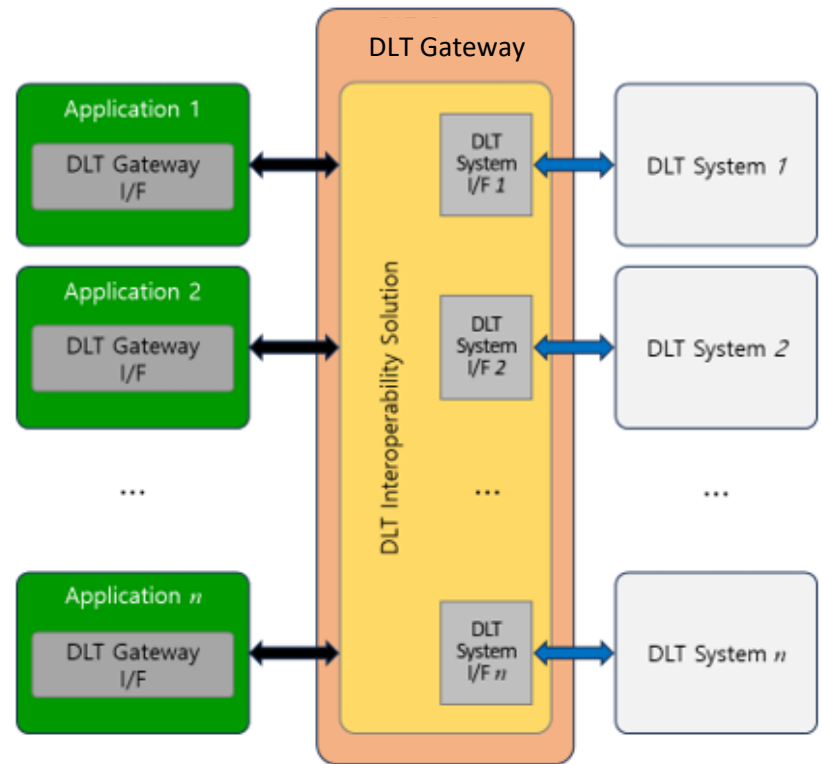
[Overview of the DLT gateway system for heterogeneous DLT system interoperability]

| | | |
|---|---|---|
|  | INTERNATIONAL TELECOMMUNICATION UNION | SG17-Cxxx |
| | TELECOMMUNICATION STANDARDIZATION SECTOR | STUDY GROUP 17 |
| | STUDY PERIOD 2023-2025 | Original: English |
| Question(s): 14/17 | Goyang, 29 August - 8 September 2023 | |
| CONTRIBUTION | | |
| Source: | Korea (Republic of) | |
| Title: | Proposal for new work item: Security requirements for interoperability of heterogeneous DLT systems on DLT gateway system | |
| Contact: | Youngjin Kim Dream Security Co., Ltd. Korea (Republic of) | Tel: +82 2 22335533 E-mail: yjkim@dreamsecurity.com |
| Contact: | Mikyong Kim Dream Security Co., Ltd. Korea (Republic of) | Tel: +82 2 22335533 E-mail: mg.kim@dreamsecurity.com |
| Contact: | Wonchan Kim Dream Security Co., Ltd. Korea (Republic of) | Tel: +82 2 22335533 E-mail: wonchan.kim@dreamsecurity.com |
| Contact: | Kyoungchul Park K4 Security Co., Ltd. Korea (Republic of) | Tel: +82 2 16448384 E-mail: kucst@k4-security.com |
| Contact: | Jung Yeon Hwang Sungshin Women's University Korea (Republic of) | Tel: +82 2 9207911 E-mail: jyhwang@sungshin.ac.kr |

Abstract: This contribution proposes to establish a new work item on study of "Security requirements for interoperability of heterogeneous DLT systems on DLT gateway system" at Q14/17

1. Background

With the rapid advancement and widespread adoption of blockchain technology, it has become clear that a single blockchain system alone cannot effectively cater to the diverse needs of various distributed applications. As a result, the demand for blockchain interoperability solutions has become increasingly apparent. As blockchain-based services continue to emerge across different industries and sectors, the need for seamless interaction and interoperability between disparate blockchain networks becomes crucial.



The END