# Blockchain Interoperability

Technology & Innovation Lab

WORLD BANK GROUP
Information and Technology Solutions

# Abstract

This paper summarizes the initial exploration and findings of the World Bank Group Technology & Innovation Lab, in partnership with the IMF's Digital Advisory Unit, on blockchain interoperability and some of the related approaches and efforts being carried out by blockchain innovators and other institutions. It covers the use cases and technical approaches of the different blockchain platforms used to exchange information and assets, as well as the experimentation the group conducted in the area of interoperability. The paper further identifies interoperability issues which needs more attention and provides guidance to practitioners.

Blockchain Interoperability Working Group: A Team of Technology Practitioners from the World Bank Group Information and Technology Solutions and IMF's Digital Advisory Unit. Since 2017, the World Bank Group Technology & Innovation Lab has partnered with the IMF's Digital Advisory Unit to explore blockchain and distributed ledger technology (DLT), including through the Learning Coin Project.[1]

1 https://www.ft.com/content/1cfb6d46-5d5a-11e9-939a-341f5ada9d40

# Acknowledgements

**WBG, Information Technology Solutions Technology and Innovation Lab (ITSTI)**
Yusuf Karacaoglu, Stela Mocan, Emmanuel Ayanfe Crown, Rachel Alexandra Halsema, Mahesh Chandrahas Karajgi, Han Wang, Raunak Mittal, Mert Ozdag, Ani Popiashvili

**WBG Information Technology Solutions, Treasury (ITSTR)**
Peter Z.Y. Zhou

**WBG Information Technology Solutions, Risk and Compliance (ITSSR)**
Zhijun William Zhang

**IBRD Legal**
Patricia Miranda, Menaka Kalaskar

**IMF Digital Advisory**
Herve Tourpe, Soheib Nunhuck, Chitranjan Zaroo

# Contents

# Executive Summary

Blockchain technology has been a core element of the so-called “digital revolution” for the last 10 years. As the COVID-19 crisis accelerates the digitalization of finance, commerce and trade, it is likely that blockchain-related projects will continue to grow in number. The technology is often praised for providing distinct advantages over traditional centralized databases, notably due to blockchain’s distributed architecture, involving many public or private participants (or nodes), which is thought to offer superior resilience, as well its security-by-design, tamper-proof protocol, which its supporters believe guarantees the protection of its users’ personal data and other hosted assets. As more solutions are beginning to rely on blockchain technology, it is becoming increasingly evident that the evolution of this technology is being held back by the lack of interoperability across blockchain solutions, other systems such as traditional IT solutions, or other emerging technology.

This paper reviews blockchain interoperability through the lenses of business, technology, security and risk, as well as legal considerations, and can be used as a reference to support further work on blockchain interoperability. We summarize our exploration agenda to date, along with key lessons learned from experimenting with interoperability across several blockchain platforms, e.g. Ethereum, Hyperledger Fabric, Corda and Quorum. Our intent is to share knowledge and promote awareness of blockchain interoperability. We identify areas where further technical development, standards and architecture patterns are needed, and provide guidance to practitioners in building open and sustainable blockchain solutions.

ONE

# The Case for Blockchain Interoperability

# The Case for Blockchain Interoperability

**There is no common definition of interoperability. For the purpose of this paper, the following definition of interoperatibility serves as a guide for the reader:**

> *The ability to exchange data with other platforms, including those running different types of blockchains, as well as with the off-chain world (EU Blockchain Observatory and Forum, 2019).*

This definition has to be understood not only at the application and technology levels, but also with respect to its business, security, and legal considerations (see Part III). Realizing the potential of Distributed Ledger Technologies (DLT) will require focusing on interoperability. Breaking siloes and walled gardens of data and applications are some of the many benefits presented by this emerging technology. However, these benefits will not materialize in the absence of interoperability among different blockchain protocols, blockchain and other emerging and legacy technologies, which may well leave us with the same original problems.

Blockchain or distributed ledger interoperability is a complex and complicated challenge to tackle. As we move towards the operationalization of this emerging technology, interoperability will come to the fore as issue of pressing importance. The different types and designs of the core shared distributed ledger can be broadly classified as being either permissioned and permissionless blockchain networks. Institutions and organizations have been exploring DLT technology protocols on the basis of their respective needs and the requirements of the challenge statement at hand. And since multiple blockchain networks are evolving, it is now critical for these different systems not just be able to interoperate with legacy systems but also be able to communicate across different distributed ledgers. This could be more easily understood through the presentation of a few examples:

**Central Banking and Digital Payments**: Several central banks have begun to trial blockchain for practical interoperability experiments. In 2019, the Monetary Authority of Singapore and Bank of Canada collaborated on a project to demonstrate the interoperability of two major blockchain networks – Corda and Quorum – using Hashed Time-Locked Contracts (HTLC).[2] Project Stella (more information on the project is available in the Annex), conducted by the European Central Bank (ECB) and Bank of Japan (BoJ), explored how cross-ledger Delivery versus Payment (DvP) can work between two individual ledgers without a direct connection. Thailand's central bank also worked with the Hong Kong Monetary

2 "Jasper–Ubin Design Paper Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies," May 2, 2019.

Authority (HKMA) on cross-border funds transfers using blockchain.[3] With the launch of the Libra project in 2019, the conversation around stablecoins – and Central Bank Digital Currency (CBDC) – has accelerated. In addition, the COVID-19 pandemic, which required social isolation and limited face-to-face commerce, has reinforced the importance of digital payment schemes. However, various existing data standards and communication protocols in payment networks, often proprietary networks, are leading to payment processing delays. Rapid change and innovation is taking place in payment technologies, which are enabling faster, cheaper, efficient domestic and cross-border payments – one of the key paradigms will be interoperability between these different channels. In the same spirit of collaborative learning, this White Paper seeks to build a better understanding on interoperability.

**Digital Identity:** Blockchain technology has become the driving force of the so-called "decentralized Internet Web 3.0", which requires interoperability and scalability to enable end-users to control and share data, or settle agreements with other parties, through the Internet in a trustworthy manner.[4] Digital identity cannot be locked in one platform –it needs interoperability across multiple platforms, and provide more choice to the end-user. This need has led to a concerted effort by various private sector and not-for-profit entities to work towards creating open standards for digital identity. The verifiable credential framework developed by the W3C Working Group is an approach aimed at ensuring that the sharing and verification of digital credentials can operate smoothly across different underlying technology protocols. This will be critical for the openness that is needed in digital identity systems.

**Supply Chains:** Interoperability is also expected to benefit the supply chain environment. One of the key challenges in supply chain systems is the lack of interoperability between the different data systems of supply chain actors. While blockchain-based supply chains could bring various advantages to fragmented supply chain systems, its implementation will face various challenges. One of these challenges is the interoperability between distributed ledgers and the existing high volume of legacy software systems, e.g. the Enterprise Resource Planning (ERP) software system.[5]



**Healthcare:** In the healthcare space, interoperability has been a challenge as a complex ecosystem of vendors, providers, regulators and patients seek to exchange and manage access to healthcare data across different systems and organizations. Healthcare Information and Management Systems Society (HIMSS) has examined how blockchain technology can be leveraged to achieve on-chain and off-chain helath data interoperability.[6]

3 Shen, Alice. 2019. "Thai Central Bank to Work with HKMA on Cross-Border Blockchain." Central Banking, August 6. Available at: https://www.centralbanking.com/central-banks/financial-market-infrastructure/4359381/thai-central-bank-to-work-with-hkma-on-cross-border-blockchain.

4 "Web3 - The Decentralized Web." BlockchainHub, August 29, 2019. http://blockchainhub.net/web3-decentralized-web/.

5 https://mneguidelines.oecd.org/Is-there-a-role-for-blockchain-in-responsible-supply-chains.pdf

6 "Interoperability: Why and How Providers Should Pursue It." CGAP, September 2019. https://www.cgap.org/research/publication/interoperability-why-and-how-providers-should-pursue-it.

In recent years, multilateral institutions and national governments have taken concrete actions to further the development of blockchain networks. The Innovation Lab of the Inter-American Development Bank (IDB Lab) developed a blockchain ecosystem – LACChain – as a global blockchain alliance. Among LACChain's main objectives are the development, promotion and adoption of standards that allow interoperability of networks, and the scalability of blockchain technology and its applications. [7]Along with LACChain, the International Association for Trusted Blockchain Applications (INATBA) has organized a series of online discussions to highlight the value of blockchain interoperability and other interoperability issues.[8] These sessions were attended by representatives of multilateral, governmental and private sector organizations.

China is about to launch its own national blockchain platform, which forms part of the country's strategy to digitally transform its economy. The platform will have important implications for its trading partners. The protocol at launch will be interoperable with major blockchain platforms and frameworks.[9] A number of other national governments have developed national strategies for blockchain adoption as well, including India[10] and Germany.[11] Finally, the World Economic Forum has issued a number of guidance notes and toolkits to assist public and private players in furthering their work in this area, including the Blockchain Deployment Toolkit for Supply Chains.[12]



7 LACChain Alliance. "What Is the LACChain Global Alliance?" Medium. Medium, March 5, 2020. https://medium.com/@lacchain.official/what-is-the-lacchain-global-alliance-and-what-does-it-consist-of-861cb76257b1.

8 INATBA Convenes Global Conversation on Standards, Governance and Interoperability (2020, May 30). Retrieved July 01, 2020, from https://medium.com/@INATBA/inatba-convenes-global-conversation-on-standards-governance-and-interoperability-cacd898a60e1.

9 Sung, Michael. "Michael Sung: China's National Blockchain Will Change the World." CoinDesk, April 27, 2020. https://www.coindesk.com/chinas-national-blockchain-will-change-the-world.

10 "Blockchain: The India Strategy Towards Enabling Ease of Business, Ease of Living, and Ease of Governance." NITI Aayog, January 2020.

11 "German Government Adopts Blockchain Strategy - Federal Ministry of Finance - Issues." Bundesministerium der Finanzen, September 18, 2019. http://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Financial_markets/Articles/2019-09-18-Blockchain.html.

12 World Economic Forum (WEF). 2020. "Redesigning Trust: Blockchain Deployment Toolkit." Available at: https://widgets.weforum.org/blockchain-toolkit/.

TWO

# The Current State of Blockchain Interoperability

# The Current State of Blockchain Interoperability

## Existing Standards

The problem of blockchain standards–relevant and necessary for interoperability–extends beyond the technical perspective and involves standardization in the business and legal spheres.

Blockchain technology has been used to develop various proofs of concepts and pilots, and is now being increasingly explored to deploy its applications in live production environments. International development agencies are actively pursuing this novel technology to address some complex and sticky problems pertaining to developing and emerging markets. However, the industry recognizes that this technology is still in the early stages of adoption, and that it is continuously evolving through new experiments and improvements. In this context, it is not surprising that blockchain standards are, as of today, fragmented, with uneven representation from emerging economies. In a 2019 analysis of ISO/TC 307 (blockchain and distributed ledger technologies), only three African countries were members, with only one country – South Africa – serving in a participating role.[13] In the past year, that number has risen to two, with the addition of Nigeria as a participating country. Given the active work being conducted in several African countries to explore and understand the potential of blockchain, the inconsistent participation in standards groups at the national level could have implications for enterprise adoption and institutional change.

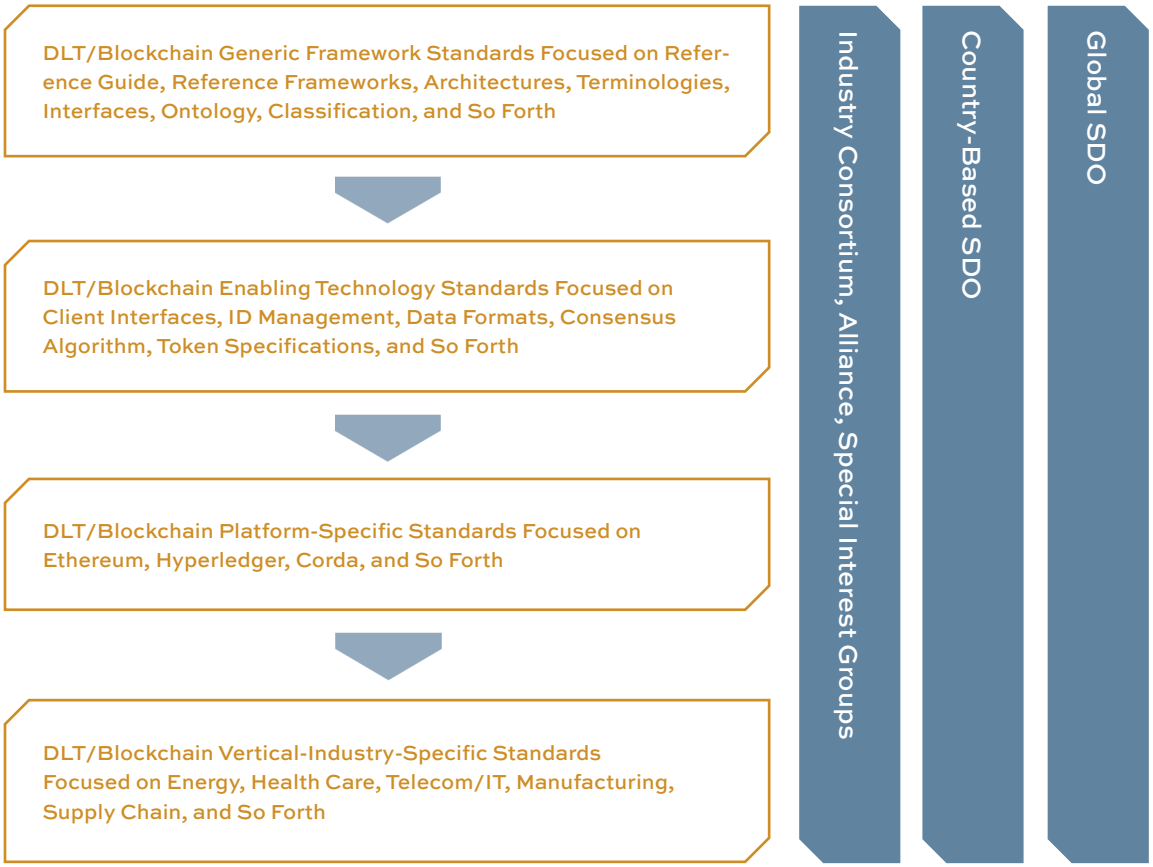


As more complex applications are being explored in the blockchain space, and also within the context of interoperability, cross-chain interoperability standards are increasingly needed. The standards could also be looked according to the different layers of technical architecture, e.g. platforms, applications or industry-specific data exchange, wallets and key management. The following framework[14] highlights these different layers, which addresses various initiatives and efforts by standards development organizations (SDO) in DLT standards:

13 "ISO/TC 307 Participation." ISO. Accessed June 23, 2020. https://www.iso.org/committee/6266604.html?view=participation.

14 Lima, Claudio. "Developing Open and Interoperable DLT\/Blockchain Standards [Standards]." CSDL | IEEE Computer Society, November 2018. https://www.computer.org/csdl/magazine/co/2018/11/08625908/17D45XfSEUx.

**FIGURE 1:** THE CLASSIFICATION OF BLOCKCHAIN STANDARDS




**Source:** Developing Open and Interoperable Blockchain Standards [Standards]

## Classification of blockchain standards and other related/like-minded efforts

The World Economic Forum, in collaboration with other members of the Global Blockchain Council recently released a paper[15], "Overview of Blockchain Technical Standards", highlighting the need for blockchain technology standards and providing an overview of its current landscape. The paper maps the existing standardization efforts, and identify corresponding gaps and overlaps on blockchain standardization.

Below is a non-exhaustive excerpt of the list of standard setting initiatives by formal standard setting bodies and blockchain specific industry groups, as highlighted in the WEF paper on:

15 https://www.weforum.org/whitepapers/global-standards-mapping-initiative-an-overview-of-blockchain-technical-standards

## MAJOR STANDARD-SETTING EFFORTS - FORMAL ORGANIZATIONS

| ENTITY | GEOGRAPHY | PURPOSE | TOPIC |
|---|---|---|---|
| IEEE | USA | The purpose of the Institute of Electrical and Electronics Engineers (IEEE) is promoting the development and application of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession, and the well-being of its members | Internet of things (IoT); cryptocurrency exchange and payment; tokens; energy; digital assets |
| ISO | Switzerland | The International Organization for Standardization (ISO) is an independent, non-governmental, international organization that develops standard to ensure the quality, safety and efficiency of products, services, and systems | Security; identity |
| W3C | USA | The Worldwide Web Consortium (W3C) is developing protocols and guidelines that ensure long-term growth for the web | Identity |
| IRTF | USA | The Internet Research Task Force (IRTF) aims to promote research for the evolution of the internet | Identity; digital assets |
| IEC | Switzerland | The International Electrotechnical Commission (IEC) promotes standardization of electrical technology, electronic, and related matters | Internet of things (IoT) |
| IETF | USA | The purpose of the Internet Engineering Task Force (IETF) is creating voluntary standards to maintain and improve the usability and interoperability of the internet | Cryptocurrency payment |
| ITU-T | Switzerland | The International Telecommunication Union Telecommunications (ITU-T) sector ensures the efficient and timely production of standards covering all fields of telecommunications and information communication technology (ICTs) on a worldwide basis, and defines tariff and accounting principles for international telecommunication services | Security; IoT; indentity; DLT requirements |

**Source:** World Economic Forum Global Blockchain Council – Overview of Blockchain Technical Standards

## MAJOR STANDARD-SETTING EFFORTS - INDUSTRY GROUPS

| ENTITY | GEOGRAPHY | PURPOSE | TOPIC |
|---|---|---|---|
| EEA | USA | The Enterprise Ethereum Alliance (EEA) builds, promotes and broadly supports Ethereum-based technology methodologies, standards, and a reference architecture | Interoperability; tokens |
| Hyperledger | USA | Hyperledger is an open-source community focused on developing a suite of stable frameworks, tools, and libraries for enterprise-grade blockchain deployments<br>It serves as a neutral home for various distributed ledger frameworks including Hyperledger Fabric, Sawtooth, Indy, as well as tools such as Hyperledger Caliper and libraries such as Hyperledger Ursa | Interoperability; tokens |
| IWA | USA | The InterWork Alliance (IWA) is working to: develop standards-based interworking specifications; address market requirements and performance metrics; support advances across all platform technologies; and enable multi-party interchanges | Tokens; analytics |
| JWG | USA and UK | The Joint Working Group on interVASP Messaging Standards (JWG) identified the need for VASPs to adopt uniform approaches and establish common standards to enable them to meet their obligations resulting from the FATF recommendations as they apply to affected entities<br>To tackle this, a cross-industry, cross-sectoral joint working group of technical experts was formed in December 2019 and a new technical standard developed by the group | Tokens |
| National Blockchain and Distributed Accounting Technology Standardization Technical Committee | China | This is a group of organizations that have joined a national committee focused on creating standards for blockchain technology | DLT requirements<br>DLT terminology |

**Source:** World Economic Forum Global Blockchain Council – Overview of Blockchain Technical Standards

The approach standard-setting bodies will take will also be critical. Bringing together various sectoral and technology experts and having a diverse representation among those responsible for developing and maintaining 'open standards'[16] could be important for interoperability and adoption.

## Past projects and implementations in the financial sector

In recent years, several central banks have embarked on experimental projects and pilots to explore the use of blockchain to enable cross-border interbank payments and settlements.

Although these projects are spearheaded by central banks, it is important to note the participation of financial institutions and consulting companies in providing technological solutions and prototypes at every stage of the development process, as well as rigorously documenting each project's technical aspects.

Project Ubin is a collaborative project and aims to help the Monetary Authority of Singapore (MAS) and the financial industry to better understand the technology and the potential benefits it may bring through practical experimentation.[17] The project explored the different phases of blockchain interoperability:[18]

- Led by MAS, Singapore Exchange, and Deloitte, Ubin Phase III considered utilizing DLT to develop Delivery versus Payment (DvP) for the settlement of tokenized assets to achieve interledger interoperability and finality of DvP.
- In Ubin phase IV (also known as Jasper-Ubin), MAS and Bank of Canada (BoC) explored cross-border and cross-currency payments using CBDC in domestic payment networks. They used HTLC, which connects two payment networks and allows Payment versus Payment (PvP).
- In collaboration with J.P. Morgan and Temasek, MAS developed a prototype which exchanges different currency on the same blockchain network. This network will allow other blockchain networks to integrate and offer some functions to support certain payment transactions, e.g. DvP with private exchanges. Phase V is still under testing.

Project Stella – a joint research project undertaken by the ECB and the BOJ – aims to contribute to the experimentation of blockchain technology, and evaluate the opportunities and challenges for financial market infrastructure to support payments and securities settlement. Reports on Phase II indicate that cross-ledger DvP could function, even without connections between individual ledgers. HTLCs and digital signature "would be used to achieve interoperability between ledgers." [19]



16 https://www.itu.int/en/ITU-T/ipr/Pages/open.aspx

17 "Project Ubin: Central Bank Digital Money Using Distributed Ledger Technology." Monetary Authority of Singapore, November 20, 2019. https://www.mas.gov.sg/schemes-and-initiatives/Project-Ubin.

18 See Annex for an overview of the context in which the other phases took place.

19 Kishi, Michinobu. 2019. "Project Stella and the Impacts of Fintech on Financial Infrastructures in Japan." Asian Development Bank, October 24. Available at: https://www.adb.org/publications/project-stella-impacts-fintech-financial-infrastructures-japan.

THREE

# A Framework for Blockchain Interoperability

# A Framework for Blockchain Interoperability

## The Business Perspective

Interoperability is increasingly becoming one of the most critical core concerns as governments seek to deliver seamless public services and develop the digital strategies to do so. Public administration could become inefficient, costly and fragmented if cross-system communication is not achieved in the digital ecosystem. The European Interoperability Framework highlights that a key aspect of the European 'Digital Single Market' is to "guarantee the secure and free flow of data, develop standards and ensure interoperability".[20] Among the reasons for this heightened focus on achieving ICT interoperability are its potential benefits, e.g. increased competition, higher innovation, and more autonomy and flexibility of choice.[21]

Blockchain technology has demonstrated its benefits and potential over the years. However, many organizations are still hesitant about its value for their operations and businesses. The lack of interoperability contributes to some of these uncertainties. It is clear that the transfer of information from one blockchain to another is a big challenge; it is also clear that organizations are cautious about relying on one vendor, and later finding that they are unable to transfer data if they decide to switch vendors. However, in addition to technology interoperability, the organizations will also have to focus on business processes that would require to align with cross-organizational trust on respective governance and business ecosystems. An example to illustrate this challenge could be blockchain-enabled and shared "Know your Customer" (KYC) utility models.[22] While interoperable blockchain systems could lower the high costs associated with KYC, it would nonetheless require new commercial and governance models to emerge for sharing KYC across different financial institutions.



The core underlying infrastructure of the digital economy is experiencing changes and shifts due to blockchain technology, as well as other emerging technologies. However, there are challenges around standardization and interoperability, which are critical for the successful scaling of these potential alternative market structures. Exchanging data assets and exchange of value in the form of digital instruments between two counterparts is relatively easy if they use the same blockchain platform. However, this is rarely the case: most businesses operate different types of blockchain technologies, making the transfer of digital assets an insurmountable challenge. The value of blockchain interoperability to industry and enterprise networks is rapidly becoming evident in the context of a growing digital economy, accelerated by the COVID-19 crisis.

20 https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf

21 https://cyber.harvard.edu/interop/pdfs/interop-breaking-barriers.pdf

22 https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/03/kpmg-blockchain-kyc-utility.pdf

An interoperable digital architecture is now imperative for the exchange of data and digital assets in the digitalization of trade, e-commerce, or e-government services. Interoperability also has direct implications on an organization's business model and its strategic positioning to deliver value. Some technology providers initially might be less focused on interoperability issues, as each one would like to grab a larger part of the market, especially those reliant on network effects. The emergence of multiple new alternatives, in addition to legacy instruments, could result in further fragmentation rather than solving the challenges if the issues around standards and interoperability are not addressed through multi-stakeholder coordination. Interoperability cannot result from the efforts of a single entity, rather it requires a governance group made up of all stakeholders active in this field. This governance group will administer and make decisions on business agreements, legal terms and technical feasibility. This group will also manage the data standard of interoperability, such as smart contract, entities and digital assets.[23] This governance model could help to establish a business partnership, which is not constricted by technological limitations.

## The Technology Perspective

> *So far, the notion of chain interoperability has seen much theory and little practice, primarily because a live example of successful chain interoperability requires not one, but two, already existing, stable and sufficiently powerful blockchains to build off, but this is slowly starting to change. -Vitalik Buterin (2016).*



### Technology Approaches

Technically, blockchain interoperability seeks to achieve one fundamental goal, namely ensuring the integrity of both information exchanges (data exchange among business systems) and value transfers (digital assets exchange, e.g. crypto, tokens). Internet protocols, such as TCP/IP and APIs, have set good examples of achieving data interoperability. However, value transfer has been an application-layer concern, and not a protocol-level concern in the traditional Internet context. With blockchain becoming the "Internet of Value",[24] ensuring the integrity of value transfer across different blockchains has become a problem to address at the foundation layer, and also needs to be considered at the blockchain network protocol level as well. In addition, there are attempts to create interoperability among different blockchains at the middleware level, e.g., blockchain-agnostic smart contracts, e.g. DAML by Digital Asset Holdings, or Quant Network's multi-blockchain DApps (MApps).

23 Inclusive Deployment of Blockchain for Supply Chains: Part 6 – A Framework for Blockchain Interoperability: http://www3.weforum.org/docs/WEF_A_Framework_for_Blockchain_Interoperability_2020.pdf

24 Ripple. 2019. "The Internet of Value: What It Means and How It Benefits Everyone." October 25. Available at : https://ripple.com/insights/the-internet-of-value-what-it-means-and-how-it-benefits-everyone/.

**Below are some popular technical means for achieving blockchain interoperability:**

**1. Oracles and Notaries**

Oracles and notaries are trusted agents between different blockchains, or between a blockchain and the off-chain world. To achieve better resiliency and to increase trust, oracles can adopt a decentralized architecture in the same manner as Chainlink.

In a notary scheme, one or more trusted nodes agree to carry out an action on chain B when some event on chain A happens (Buterin, 2016). Trusted nodes are the key to notary schemes. One important feature of the notary scheme is its atomicity, meaning that a transaction needs to be all or nothing for all participants. The notary scheme has been implemented in the Atomic mode of the Interledger Protocol[25] , whereby an ad hoc group of notaries are selected to support the execution of each payment by confirming the success or failure of the payment.

**2. Time-bound Asset Locking and Release**

To support the exchange of value across different blockchains in a trustless mode, assets can be locked on a blockchain ledger and released upon confirmation that the recipient is ready to receive the asset. This has been implemented in the Universal Mode of the Interledger Protocol and HTLC.

In the Universal Mode of the Interledger Protocol, after a chain of participants has been selected for the value transfer, assets are locked on the corresponding ledger of each participant. Following confirmation by the final recipient of the value, the locked value is released and transferred to the recipient by the operator on the last ledger. The last ledger will then provide a payment confirmation to the previous ledger, which will unlock the asset and send it on, etc., until the ledger for the sender also receives the confirmation, unlocks the asset, and finalizes the deduction of this asset from the sender's account. To prevent a liquidity starvation attack on any participant, all transactions are time-bound, with upstream ledgers allocating more time than the downstream ones.



25 Stefa Thomas & Evan Schwartz. A protocol for Interledger Payments. http://interledger.org/interledger.pdf

In HTLC, hash locking between blockchain A and blockchain B can be achieved in three steps (Buterin, 2016):

1. Blockchain A generates a random secret s, and computes the hash of the secret, hash(s) = h. Blockchain A sends h to B.

2. Blockchains A and B both lock their asset into a smart contract with the following rules (A locks first, B locks after seeing A's asset successfully locked).

   a. On A's side, if the secret is provided by B within 2X seconds, then the asset is transferred to B; otherwise, it is sent back to A.

   b. On B's side, if the correct secret (i.e., the value whose hash is h) is provided within X seconds, then the asset is transferred to A; otherwise, it is sent back to B.

3. Blockchain A reveals the secret within X seconds to claim the asset from B's contract. However, this also ensures that B learns the secret allowing B to claim the asset from A's contract.

Unlike in the notary scheme, hash locking does not require a pre-existing trust relationship between the two blockchains or with a third party.

**3. Sidechains/Relays**

Another approach to allow different blockchains to interoperate is to have an "integration" blockchain to support the exchange of value and information between different participating blockchains.



In the sidechains-relay model, the relay chain is the integration layer. It can issue a token to be used for value exchange by all sidechains. The relay chain can offer smart contracts for different sidechains to interact with and exchange information. In addition, it generally provides a larger number of validation nodes than any of the sidechains, thereby providing more robust security as it ensures that no double-spend is made on value exchanges. The information integrity is preserved as long as that information is part of the overall "block header" that is: (i) generated in some cryptographically authenticated way, most likely using Merkle trees; and (ii) recorded on the relay chain.

Regarding information exchange, a smart contract on the relay chain can function as a light client for a specific sidechain, thus leveraging the sidechain's standard verification procedure to verify any block headers that have been fed into the contract. Relays are very powerful as they can be used for asset portability, atomic swaps, and many other more complex uses.

For example, Polkadot uses a relay chain to connect multiple sidechains known as parachains, with each parachain being a blockchain. The Polkadot architecture is described in detail in the latter part of this paper.

**4. Application Layer Adaptors**

In order to facilitate the development of applications that may run on multiple blockchains, an abstraction layer can be created so that the business functions of the underlying blockchains can be exposed as common APIs.

A blockchain-agnostic smart contract language can be another alternative to code the business logic and map the different underlying blockchain platforms. DAML is a smart contract language that enables distributed application development without having to decide what blockchain or distributed ledger platform to use. The creator of DAML, Digital Asset, is working with partners to have DAML-based applications run on Corda, HyperLedger Fabric or Sawtooth, VMware Blockchain, and other platforms.

Vottun's technology exposes blockchain-specific smart contracts as common APIs, making it possible for applications to be built without having to target any particular blockchain network. Each API is mapped to an underlying blockchain smart contract function, which will execute on the specific blockchain. Vottun currently supports Hyperledger Fabric, Alastria, Quorum, and Ethereum.

The Overledger platform by Quant Network, connects various blockchain networks, as well as legacy systems. The platform provides a blockchain-agnostic operating system for business applications to run. It currently supports Hyperledger Fabric, Corda, Ethereum, Bitcoin, IOTA, EOS, and Ripple, either permissioned or permissionless, and provides Java and JavaScript SDKs for developers to develop applications to run on the platform. Quant Networks uses its own Dapps technology (Multi-blockchain Dapps or MDapps).

LiquidApps provides a run-time middleware and developer SDK to enable the development of decentralized applications that can run across multiple blockchain networks. It currently supports EOS, Ethereum, Telos, and sother blockchain networks.



**Technical framework**

The technical methods for interoperability can be categorized across two dimensions: just-in-time vs. on-going interoperability, and direct vs. third-party interoperability. In the second dimension, third-party can be an independent entity, e.g. a notary or oracle service provider, or a blockchain network to which the interoperating parties must belong, such as a sidechain or relay chain.

| | JUST-IN-TIME | ON-GOING |
|---|---|---|
| Direct | Protocols, e.g. time-bound asset locking and release | Application layer adapters |
| Via a third party | Oracles, notaries | Sidechain, relay-chain |

When the team has this interoperability initiative, both value exchange and information exchange were explored technically. Blockchain is touted to be the foundation for "The Internet of Value" (or digital assets). In this exploration the exchange of value is singled out as a particularly important problem for blockchain interoperability. When it comes to exchange of information, it is referring to the scenarios where no digital assets changes hands as part of the cross-chain operation.

Table 1 illustrates how two blockchains using the respective ledger technologies can exchange value or information based on current technologies.

**TABLE 1:** VALUE EXCHANGE AND INFORMATION EXCHANGE USABILITY BETWEEN DIFFERENT BLOCKCHAIN PLATFORMS

| | ETHEREUM/ QUORUM | CORDA | INTERLEDGER | POLKADOT | HYPERLEDGER FABRIC |
|---|---|---|---|---|---|
| Ethereum/ Quorum | Value: HTLC Infor.: Oracle | Value: HTLC Infor.: oracle[26] | Value: Application layer adapter | Value & Information: Application layer adapter | Value & Information: Application layer adaptor[27] |
| Corda | | Value & Information: Corda Network as the relay chain. | N/A | Value & Information: Application layer adapter (to be developed) | Value & Information: Application layer adaptor |
| Interledger | | | | N/A | Value: Application Layer Adapter |
| Polkadot | | | | (There is only one Polkadot network) | Value & Information: Application layer adapter (to be developed) |
| Hyperledger Fabric | | | | | Value: HTLC Infor.: oracles, Events API, Joint network or channels |

**Note:** The shaded cells repeat the same information as in the right side of the diagonal line of the matrix(table).



26 Wan, Clemens. 2019. "Unlocking Corda Ethereum Interoperability Pt 3." Medium. March 15. Available at: https://medium.com/@clemens_wan/unlocking-corda-ethereum-interoperability-pt-3-15aa4de97e40.

27 Ledger Insights. 2019. "Hyperledger Fabric Integrates Ethereum Smart Contracts." October 29. Available at : https://www.ledgerinsights.com/hyperledger-fabric-integrates-ethereum-smart-contracts-evm-blockchain/.

Table 2 summarizes past projects and our explorations based on our technical framework.

**TABLE 2:** TECHNICAL APPROACHES USABILITY BETWEEN DIFFERENT BLOCKCHAIN PLATFORMS AND PROJECTS

| | ETHEREUM/ QUORUM | CORDA | INTERLEDGER | POLKADOT | HYPER-LEDGER FABRIC | LEGACY SYSTEMS |
|---|---|---|---|---|---|---|
| Ethereum/ Quorum | HTLC: Working Group Explorations | HTLC: Ubin (Phase IV) Jasper | Working Group Explorations | Application layer adapter | EVM user chaincode and Web3 provider support in Fabric[28] | Oracles as implemented by Chainlink[29]: |
| Corda | | Corda Network is live | N/A | N/A | DAML by Digital Asst Holdings | Corda Settler for payments |
| Interledger | | | | N/A | Hyperledger Quilt (being developed) | Stronghold Platform[30], Gates Foundation Mojaloop, Project Stella Phase III |
| Polkadot | | | | There is only one Polkadot network | N/A | Adapter using Substrate: Working Group Exploration |
| Hyper-ledger Fabric | | | | | Information: oracles or Events APIs[31]. | It is being explored.[32] |

**Note:** The shaded cells repeat the same information as in the right side of the diagonal line of the matrix (table).

28 "Hyperledger Fabric Now Supports Ethereum" Hyperledgger, October 26,2018. Available at: https ://www.hyperledger.org/blog/2018/10/26/hyperledger-fabric-now-supports-ethereum/.

29 American Crypto Association. 2020. "Kadena Collaborates with Chainlink in Hybrid Blockchain Oracle Integration.", May 19. https://www.americancryptoassociation.com/2020/05/19/kadena-chainlink-blockchain-oracle/.

30 Medium. 2019. "Stronghold Platform Integrates with Interledger Payments Protocol." Medium. Stronghold, May 16. https://medium.com/strongholdpay/stronghold-platform-integrates-with-interledger-payments-protocol-cbdd5477e0f0.

31 "Fabric@Lists.hyperledger.org: Multiple Fabric Networks." fabric@lists.hyperledger.org | Multiple fabric networks. Accessed June 23, 2020. https://lists.hyperledger.org/g/fabric/topic/17549956.

32 Desrosiers, Luc, and Ricardo Olivieri. 2019. "Oracles: Common Architectural Patterns for Hyperledger Fabric." IBM Developer. IBM, March 11. Available at : https://developer.ibm.com/technologies/blockchain/articles/oracles-common-architectural-patterns-for-fabric/.

It should be noted that these technical solutions may need to be augmented with a semantic layer. In cases of information exchange, i.e. how each blockchain interprets the data, this may need to be coordinated off-chain. Similarly, when tokens are exchanged between blockchains, the "exchange rate" between two different tokens may need to be determined off-chain, unless there is an oracle for that exchange rate.

## The Security and Risk Perspective

Blockchain projects employ different trust models. Public blockchains build trust based on cryptography, consensus algorithms and incentive models, e.g. proof-of-work and the considerable costs associated with attacking a network's data integrity. Their security strength typically correlates to the number of nodes on the network. Blockchains rely heavily on membership management and traditional Public Key Infrastructure (PKI) to provide trust on the network. Their security mostly hinges on the established business relationship among the participants.

When two blockchains interoperate, it is important to analyze the difference in their security models and introduce necessary compensating controls so that the integrity of information or value exchange would not be compromised for the two interoperating blockchains. This requires careful design of the interoperability interface. A good example is the way parachains leverage the strength of the relay chain in Polkadot.

For information exchange, the critical security issue is the integrity and trustworthiness of the information from another chain or system. The 2019 Oracle attack on the crypto-asset platform Synthetic resulted in the loss of 37 million digital tokens within several hours, exemplifies this issue.[33]



For value exchange, the key issues include: **(i)** the integrity of the information; **(ii)** the asset ownership and its intended action; and **(iii)** the value exchange's execution being fair and atomic. The fairness ensures that both parties would get their part of the exchange, and no party should have an advantage in backing out of the transaction based on external events.

A condition for interoperability resides in the ability for two systems to recognize each other's identity schemes. Aiming for a common identity management is unrealistic, as they are intrinsically linked to each chains' cryptographic choices. On the other hand, one precondition for establishing trust is to establish some sort of mapping across identity schemes.

From a risk perspective, a party may take on additional risks if it interoperates with another party from a platform with a lower security and risk profile. Such additional risk must be carefully assessed and be deemed appropriate for the business benefit that would be achieved.

33 Todd, Ryan. 2019. "Synthetix Suffers Oracle Attack, More than 37 Million Synthetic Ether Exposed." Yahoo! Finance. Yahoo!, June 25. Available at : https://finance.yahoo.com/news/synthetix-suffers-oracle-attack-potentially-224737187.html.

Table 3 summarizes the security factors to consider when two blockchains interoperate:

**TABLE 3:** SUMMARY OF SECURITY FACTORS

| COMPATIBILITY FACTORS | CONSIDERATIONS | MEANS OF RECONCILIATION |
|---|---|---|
| Identity | Some entity may have different identities on different blockchain. | DIDs, proof of identity ownership. |
| Cryptography | Different blockchains may use different hash and digital signature algorithms. | Validation via a third party. |
| Level of decentralization | Number of nodes and consensus algorithms often vary between different blockchains. | Risk/reward analysis; make adjustment to participating blockchains when feasible. |
| Semantics layer | Interpretation of time, unit of measurement and unit of value could be different across different blockchains. | Combination of decentralized oracles and offline agreements. |

## Legal Considerations

This report highlights selected legal considerations of our exploration on blockchain interoperability. Current legal frameworks for blockchain cover both the inputs and the outcomes of the technology but not the technology itself. Blockchain interoperability could yield additional layers of regulatory scrutiny as it will inevitably involve different jurisdictions; explorations will assist regulators better understand the technology.



**Interoperability describes the ability of computer systems or software to exchange and make use of information.**

The two main aspects to take into account in blockchain interoperability are the technologies involved and the legal dimensions. The technological aspects may be easier to overcome. This can be illustrated by how emails evolved from once being limited to exchanging messages within the same email network to now being able to exchange messages across different email networks. Overcoming the technological gap to bridge interoperability is inevitable. It is already moving forward in the realm of cryptocurrencies.[34] The legal aspects might be more challenging as the many existing legal frameworks regulating the same or similar purposes are already giving rise to conflicts, without adding technology in the mix. It is not necessarily the medium of technology but its purpose and implications which has surfaced the tensions with existing frameworks.

34 See Magas, Julia, "Crypto interoperability evolves: From blockchain bridges to DeFi transfers", at https://cointelegraph.com/news/crypto-interoperability-evolves-from-blockchain-bridges-to-defi-transfers

If two or more systems are exchanging information, the purpose of that exchange will drive which laws may apply. For example, the Securities Exchange Act of 1934 in the United States regulated investments, "in whatever form they are made and by whatever name they are called". Thus, as the Act points out ***the name of the instrument doesn't matter, what matters is its nature***. This was emphasized by panelists[35] at the first panel on "Virtual Currencies" at the CFTC TAC Meeting of 3 October 2019. Below are some of those key points:

1. it is important to **focus on the functions and features of the digital asset/stablecoin;**
2. as with any investment, there is a need to **understand the nature of the instrument,** so one can assess the value, how to use it, and how to regulate it;
3. it is important to look at the different types of stablecoins and identify **what their nature really is, regardless of what they are called/named;** and
4. the value of FINMA's principle of **"same risks, same rules"** set forth on its recent guidance on stablecoin.

None of this, however, minimizes the complexities of trying to identify an instrument under the current regulatory environment. Such identification remains a challenge as it is impacted by, for example: (i) small permutations on the instrument; (ii) by the jurisdiction where the instrument is to be considered; and/or (iii) how the instrument is marketed since its issuance may have different purposes in different places, and therefore classifying it as a different instrument at different times. And this is just one example in one industry and in one country.

26 Thus, the main legal question to ask before even considering the technical interoperability of a proposed blockchain application is the exact purpose of the proposed blockchain application. Teams need to look beyond mere labels and:

A. analyze the essential characteristics of the proposed application to determine what it really is and, thus, what industry it relates to and what laws, regulations and/or compliance requirements may apply;
B. consider how it may impact market competitiveness as it may raise anti-trust issues depending on what it is going to do.

Depending on the purpose of the blockchain application and the jurisdictions involved, there may be as many commonalities as there are divergences in laws and regulations. These may impose different requirements that may need to be implemented through technological controls, and which may subsequently impact the technical aspect of interoperability.

The wide range of possible blockchain applications remain largely unregulated. In the meantime, relevant industry laws and regulations apply, regardless of the technology being used. For example: **(i)** financial laws will apply to blockchain applications for financial services; **(ii)** health and drug regulations will apply to blockchain applications used for health and drugs; **(iii)** consumer protection laws may also apply depending on the issue that arise

35 The panelists included Gary DeWaal, Special Counsel, Chair, Financial Markets and Regulator; Katten Muchin Rosenman LLP; and Lee Schneider, General Counsel, block.one.

from the use of a blockchain application, etc. Current laws on cybersecurity, financial services, privacy and data protection, money transfers or transmission licensing, to name but a few, can and should, certainly apply to any technology.

### Lessons from cryptocurrency

Cryptocurrencies have conferred celebrity status to blockchain technology. However, in some cases it challenges the sovereign control of the state in issuing currencies. Regulating cryptocurrency became a necessity due to its potential impact in banking and financial markets. A 2018 PWC survey of 600 executives in 15 countries reported that 48 percent of respondents considered that regulatory uncertainty is the most important barrier to blockchain adoption.[36]

About 130 countries and some regional organizations have issued laws or policies on cryptocurrencies.[37] Out of 130 countries, nine have an absolute ban on cryptocurrencies, while 16 countries have banned it an implicitly.[38] While China and Lithuania implicitly ban cryptocurrencies, they nonetheless are among 13 countries that have or are issuing national or regional cryptocurrencies.[39] While countries such as Belarus, the Cayman Islands, Luxembourg and Spain, do not recognize cryptocurrencies as legal tender, they see a potential in the technology behind it and are developing a cryptocurrency-friendly regulatory regime to attract investment in technology companies.[40] Yet others accept cryptocurrency as a means of payment, even by government agencies, as in the case of the Swiss Canton of Zug and a municipality in the Canton of Ticino.[41] The Isle of Man and Mexico also allow the use of cryptocurrencies as a means of payment alongside their national currency; Antigua and Barbuda allows the funding of projects and charities through government-supported ICOs.[42]



36 PWC, Blockchain is here. What's your next move?, available at https://www.pwc.com/blockchainsurvey?WT.mc_id=CT3-PL300-DM1-TR1-LS4-ND30-TTA5-CN_US-GX-xLoSBlockchain-ggl-nonbranded&eq=CT3-PL300-DM1-CN_US-GX-xLoSBlockchain-ggl-nonbranded

37 Library of Congress, Regulation of Cryptocurrency Around the World, June 2018, available at https://www.loc.gov/law/help/cryptocurrency/world-survey.php?loclr=ealrr

38 Library of Congress, Legal Status of Cryptocurrencies, available at https://www.loc.gov/law/help/cryptocurrency/map1.pdf. Countries with an absolute ban on cryptocurrency include Algeria, Bolivia, Egypt, Iraq, Morocco, Nepal, Pakistan, United Arab Emirates, and Vietnam. Countries with an implicit ban on cryptocurrencies include Bahrain, Bangladesh, China, Colombia, Dominican Republic, Indonesia, Iran, Kuwait, Lesotho, Lithuania, Macau, Oman, Qatar, Saudi Arabia, Taiwan (China), and Thailand.

39 Library of Congress, Countries that Have or Are Issuing National or Regional Cryptocurrencies, available at https://www.loc.gov/law/help/cryptocurrency/map3.pdf. These countries include: Anguilla, Antigua and Barbuda, China, Dominica, Grenada, Ireland, Lithuania, Marshall Islands, Montserrat, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, and Venezuela.

40 Library of Congress, Regulation of Cryptocurrency Around the World, June 2018, available at https://www.loc.gov/law/help/cryptocurrency/world-survey.php?loclr=ealrr

41 *Ibid.*

42 *Ibid.*

Malta is leading a new approach as the first country in the world to provide regulations for blockchain operators, cryptocurrency and DLT, and became a safe and welcoming environment for blockchain initiatives.[43,44] Understanding the need for legal certainty for companies to operate, Malta established: (i) an authority to certify DLT platforms and ensure credibility and legal certainty to users wishing to use DLT platforms; (ii) DLT arrangements and certifications of DLT platforms; and (iii) a regulatory regime for ICOs, cryptocurrency exchanges, and other related services.[45] Other jurisdictions, including Bermuda, Gibraltar and the small town of Zug in Switzerland, are developing laws and regulations to attract cryptocurrency businesses.[46]

Blockchain technology is actively used in Liechtenstein; on 16 November 2018, Liechtenstein completed consultations on a proposed Law on Transaction Systems Based on Trustworthy Technologies (TT) (Blockchain Act).[47] The Blockchain Act is Liechtenstein's response to a demand for greater legal certainty in connection with blockchain.[48] It intends to strengthen legal certainty for users and service providers to support the positive development of the token economy in Liechtenstein.[49,50]

### Liability and Disputes

While laws and regulations may diverge, parties engaging and developing blockchain applications could potentially address any conflict of laws and jurisdiction through contractual obligations. Parties could agree that a specific set of laws and jurisdiction will apply in solving disputes among the parties and users. In this scenario, the parties would be responsible for assessing the proposed legal system and jurisdiction to apply; users may need to read the agreements they are asked to adhere to before using a blockchain application. Without any such contractual agreement, parties would be left at the mercy of courts to decide which one would have jurisdiction. With blockchain's decentralized nature that could entail a long and arduous legal battle, just only to determine where the dispute should be settled.



43 *Ibid.*

44 Forbes. 2018. Maltese Parliament Passes Laws That Set Regulatory Framework For Blockchain, Cryptocurrency And DLT, July 5. Available at https://www.forbes.com/sites/rachelwolfson/2018/07/05/maltese-parliament-passes-laws-that-set-regulatory-framework-for-blockchain-cryptocurrency-and-dlt/#7540d0e049ed

45 *Ibid.*

46 The New York Times. 2018. Have a Cryptocurrency Company? Bermuda, Malta or Gibraltar Wants You, July 29. Available at https://www.nytimes.com/2018/07/29/technology/cryptocurrency-bermuda-malta-gibraltar.html, and Cointelegraph, Which Countries Are Best to Start Blockchain Projects?, August 9, 2018, available at https://cointelegraph.com/news/which-countries-are-best-to-start-blockchain-projects

47 *Consultation launched on Blockchain Act*, August 29, 2018, available at http://www.regierung.li/en/press-releases/212310

48 *Ibid.*

49 *Ibid.*

50 Reference to the status of legislation and regulation in some of these and other countries in Appendix 2.

### Key Questions

Determining what type of blockchain is desirable is crucial in identifying what other considerations need to be taken into account. Legal considerations on blockchain technology may be amplified depending on whether the blockchain is public or private, permissionless or permissioned. This is because on a public and permissionless blockchain environment the decentralized nature of blockchain raises prominent legal concerns relating to the liability, jurisdiction, applicable law, rights and obligations of its different actors, to name but a few. In such an environment, actions and decision-making are likely to be spread out geographically among numerous nodes located in different locations, as well as among parties that may not be readily identifiable, if even possible to identify them in the first instance. The inability to control illicit activities and malicicous actors, and identify responsibility of the network poses a challenge. For instance, the WannaCry ransomware attack in May 2017 demanded payment in Bitcoins. By receiving Bitcoin payments it is not possible to know who owns those Bitcoins, even if the transaction has been executed in a public and permissionless blockchain.[51]

**The legal issues in a public and permissionless blockchain are clear:**

**a.** Who is responsible for harm in a blockchain environment? Should it be the node operators who are running the network, or the software developer, i.e. the one who codified the blockchain rules and/or protocols; or some other party?

**b.** Who has legal personality in a blockchain?

**c.** Which law applies since the "decision-makers" are in different locations?

**d.** Which jurisdiction has authority to hear and consider disputes in light of the different locations of all involved in a blockchain?



For now, these questions remain mostly unanswered. Courts will have to decide these issues when they come before them at some future date and challenges are mounted against the blockchain technology itself.

Broadly speaking, identifying the actors is easier in a private and permissioned blockchain as it is privately owned and those on the blockchain are participating thanks to someone's permission to do so. There is control in a private and permissioned blockchain, which makes it less problematic from a legal point of view. As private and permissioned, one easily knows who controls the blockchain, who has access, where it is located (even if in different locations), who acts and makes decisions on the blockchain. Being able to identify who has control of a blockchain makes it possible to determine which jurisdiction would have authority over a dispute, which law applies, and who may be responsible. This is not to say that some of the broader questions disappear if the blockchain is private and permissioned, rather it may make it easier to identify the actors in a public and permissionless blockchain. Knowing the nature of the blockchain thus helps narrow down the legal questions one should consider when working with blockchain technology.

51 "As with all such wallets, their transactions and balances are publicly accessible even though the cryptocurrency wallet owners remain unknown", at https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

**Any business considering a blockchain application must have clarity on:**

1. What type of blockchain is desirable? Should it be public network or private network?
2. What industry does the proposed solution apply?
3. What are the local laws that apply to the industry concerned?
4. What are mandatory requirements that need to be included in the design of the blockchain application?
5. How are such requirements going to be implemented on the blockchain? Are they different in different places? Will this impact the development of the application?
6. What information will be captured and exchanged? Who will access the information?
7. What is the desired privacy and data security for the solution?
8. What is the data/information flow?
9. Is it possible for the application to have one full node in one location that will determined and/or reiterate the choice of jurisdiction among the parties to solve disputes?
10. If a blockchain application is chosen, what governance structure is best for governing the technology as it needs to adapt over time to remain relevant?

FOUR

# Working Group Explorations and Lessons Learned

# Working Group Explorations and Lessons Learned

To obtain a deeper understanding of blockchain interoperability among different blockchain platforms from a technical perspective, we explored three of the four technical approaches described in Part II. The team implemented a token swap using HTLC between two different Ethereum networks, and value transfer using Interledger protocol between Ethereum testnet and XRP Ledger testnet. The team also looked at the Polkadot's interoperability capability between blockchain networks and legacy systems, as well as Corda's example of integrating with financial systems on issuing obligation and settlement. Additionally, the team tried and implemented two interoperability methods for a project involving sovereign/national governments.

A technical perspective of the explorations and lessons learned is presented below:

**1. Hashed Time-Locked Contracts (HTLC)**

An HTLC is a conditional transfer of value from a "depositor" to a "recipient" in which two distinct conditions prevent immediate execution. The hashlock requires the proper "secret" to be presented to the blockchain before the timelock expiration; if this does not occur, the value automatically returns to the "depositor."

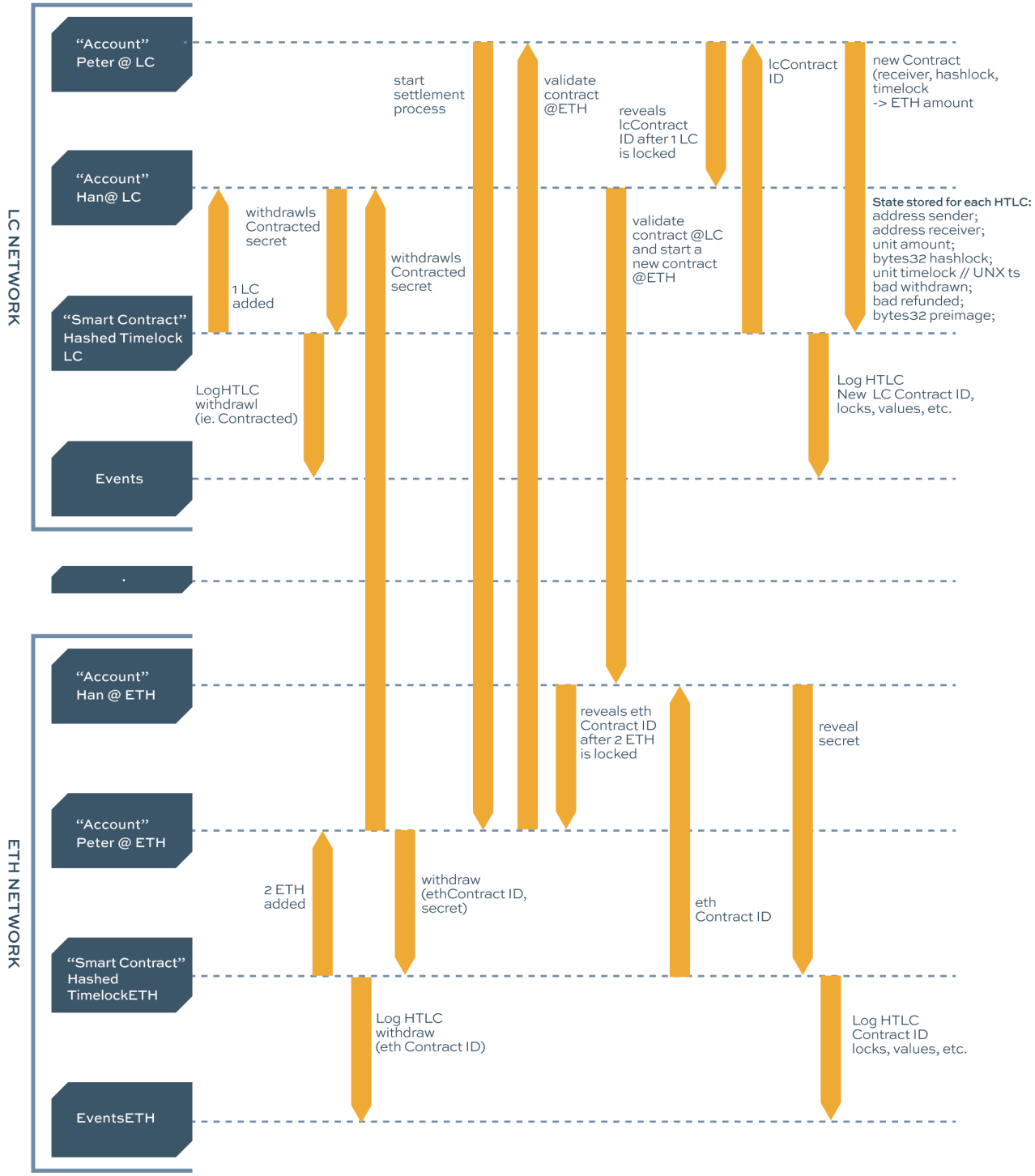
This allows two parties to exchange assets on independent platforms without a trusted intermediary and securely, and thus enables Atomic Cross-Chain Swaps (ACCS), among other useful functionalities.

During hands-on exploration, HTLCs for Ethereum native tokens swapping was explored between two Ethereum networks. Firstly, the team tried this effort between Ganache and public Ethereum testnet Ropsten. The HTLC was deployed to both networks and conduct the token swap (see Figure 4).

For detail of this exploration, please refer to this link: https://github.com/GOOGZHOU/htlc-lc-eth

## **FIGURE 4:** HTLC EXPLORATION PROCESS FLOW

**HASHED TIMELOCK CONTRACT:** normal flow - receiver withdraws with preimage before the timelock expires



Additionally, the team explored the token swap on a Blockchain-as-a-service platform. This service supports atomic swap, HTLC, and cross-token swapping. During the exploration, two kinds of native tokens were generated in a private Ethereum network, and swapped within the locked time.

From these hands-on explorations on HTLCs, we learned that there is no need for a third party to accomplish the transaction. This aligns with the requirement to interoperate without the need of a trusted intermediary. However, there are some assumptions and conditions to accomplish HTLCs. One is that this relies on the two parties verifying the smart contracts independently on both networks. Another one is that it still needs offline communication on the timelocks set in the smart contract. The second party must set the timelock and conclude the transaction ahead of the timelock set by the first party. During this time, the assets or payments are locked and no party is able to move the assets or payments. If the transation is a large one, it will generate a low-liquidity issue in reality, and would thus require an efficient communication between two parties for transactions to exchange digital assets.

A key recommendation going forward would be to develop a new technique, or method to support messaging across different blockchain networks.

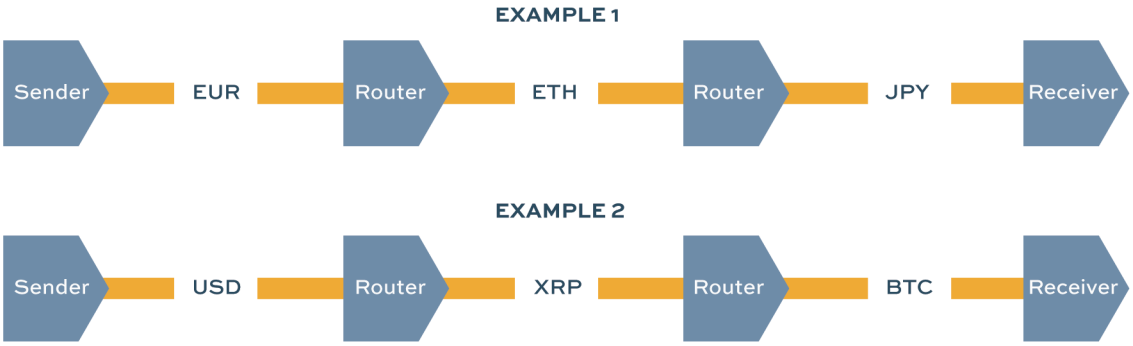
### 2. Interledger

Interledger is an open protocol, originally inspired by the Internet Protocol, for sending payments across various blockchain networks. It enables the exchange of value across different payment networks. Using Interledger, the XRP can be sent to someone who wants to receive ETH or USD can be sent to someone who wants to receive EUR. [52]



Interledger routes packets of value in the same way as the Internet routes packets of information. Computers on the Interledger network are called nodes. Nodes can take one or more of the following roles: sender, router, and receiver (see Figure 5).

**FIGURE 5:** INTERLEDGER NODES EXAMPLES



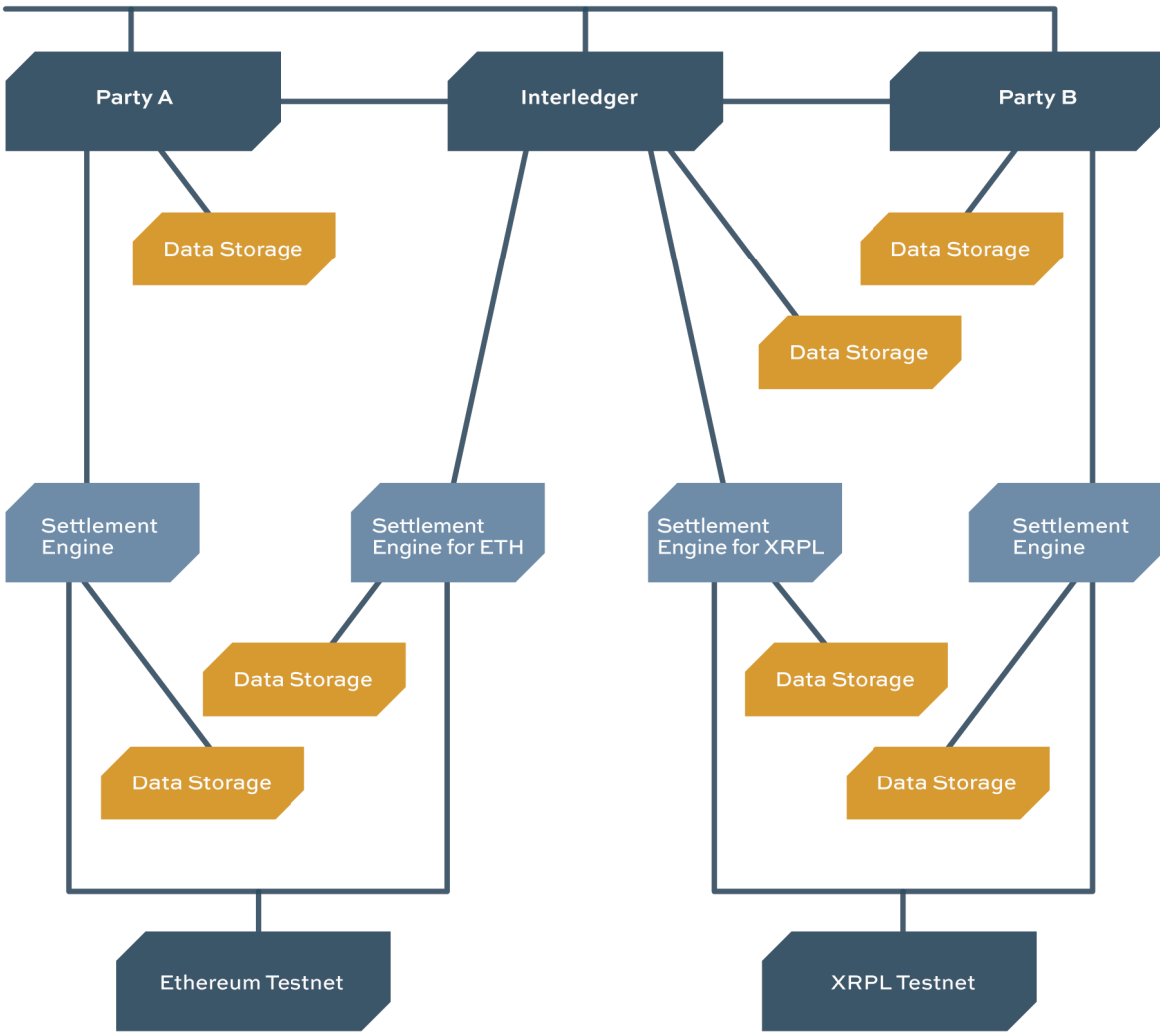

**Source:** Interledger Overview

52 Interledger. 2020. "Interledger Overview." Accessed June 23, 2020. Available at: https://interledger.org/overview.html.

The settlement engine plays a crucial role in the Interleger network to support sending and receiving settlements between ledgers. One engine can manage several accounts and settle with many ledgers.

The team tried to run three Interledger nodes connected to two blockchain testnets (Ethereum and Ripple XRPL: Party A, Interledger (acting as an intermediary node), and Party B. Party A sent Ether and Party B's node received XRP, while a the third node acted as intermediary during the token exchange. To accomplish this, Party A with Ether needs to install a settlement engine to transfer Ether from Ethereum testnet to the intermediary node through settlement engine for ETH (see Figure 6).

**FIGURE 6:** INTERLEDGER EXPLORATION PROCESS FLOW




**Source:** the working group

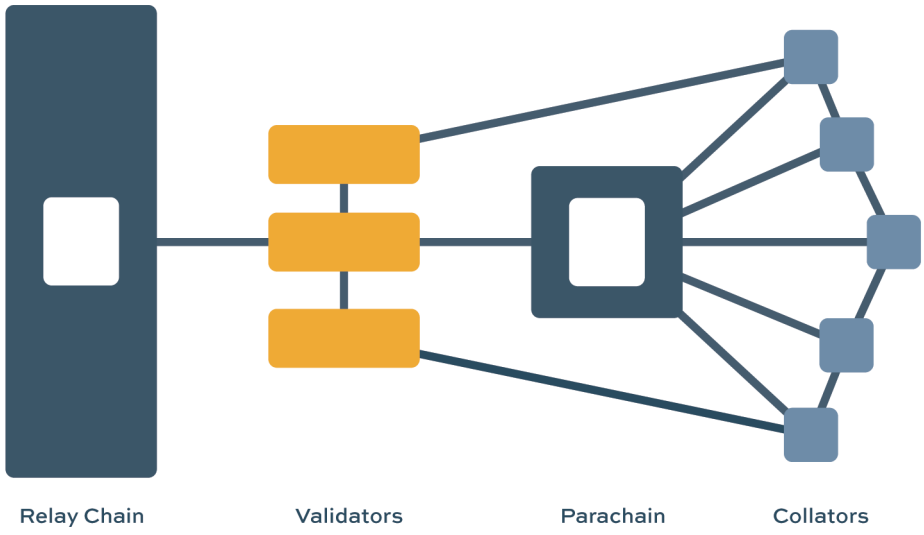
The Interledger project working team claims to create an "Internet of Value". This is a very promising for the payment domain. The Interledger team already developed several settlement engines for different types of non-crypto payment, such as PayPal and mobile money.

**3. Polkadot**

Polkadot is built for a scalable, interoperable and secure blockchain network. It allows particular blockchains to interact with each other in a secure way. Polkadot uses the Relay Chain to send message between blockchains in its ecosystem and host a group of parachains which run their own applications. Below are the high-level architectures,[53] which demonstrate the basic concept of relay chain and parachain (see Figure 7).

Relay Chain is the main chain of the system. Parachains generate blocks for validators on the Relay Chain before the blocks are validated and added to the finalized chain. Thus, the Relay Chain provides security guarantees. Different parachains can run parallel transactions without interference, resulting in Polkadot being potentially more scalable than a current PoS system (see Figure 8).

**FIGURE 7:** PIECES OF POLKADOT

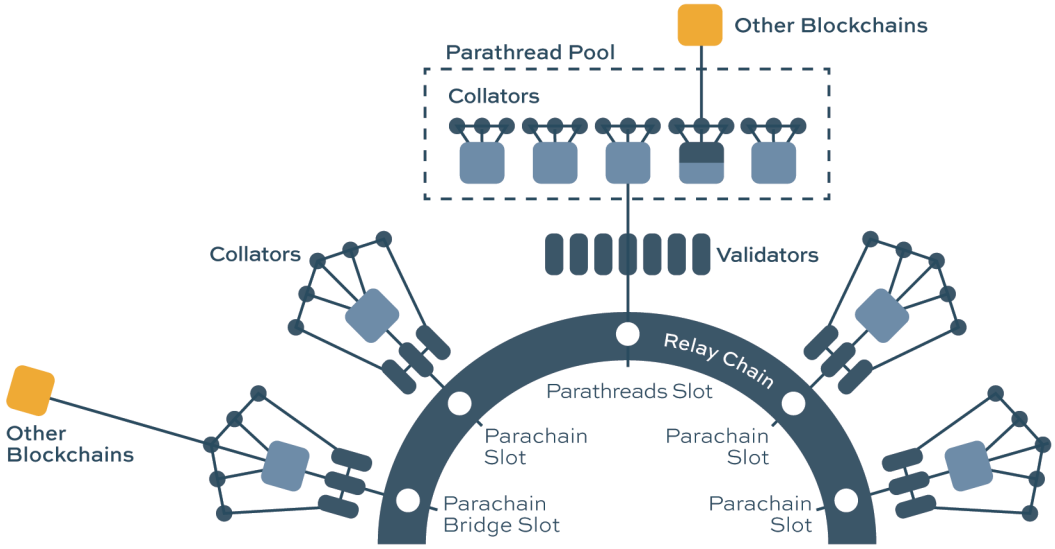



**Source:** An Introduction to Polkadot



53 Polkadot. 2020. "An Introduction to Polkadot." April. Available at: https://polkadot.network/Polkadot-lightpaper.pdf

**FIGURE 8:** POLKADOT HIGH-LEVEL ARCHITECTURE




**Source:** An Introduction to Polkadot



Polkadot's parent company, Parity, plans to release the production version in 2020. We plan to test Polkadot after its release. During the exploration, the team tested Substrate (a framework to efficiently build different blockchains by Parity) within a four-hour hackathon. Substrate was developed to build blockchains which can easily connect to Polkadot. The lessons learnt in this exploration are that Polkadot:

- Gives developers flexible options to do the implementation in a modular way.
- Provides plenty of tools that help develop the blockchains fast.
- In its current status, even though it makes the development easy, it is still difficult to compare it with Ethereum which already has gained substantial momentum. Substrate requires developers to have specific skills, such as Ink!, smart contract language programming applications, such as the rust programming language.

Substrate provides an interesting option known as "off-chain workers," which integrates a blockchain node with existing systems. This option is similar to using oracles, but the off-chain workers provide a better alternative, especially with respect to security, scalability and infrastructure efficiency. Off-chain workers allow execution of long-running and possibly non-deterministic tasks, e.g. Web requests, that would require longer than the block execution time. Off-chain workers have their own Wasm execution environment outside of the substrate runtime and they can also be initiated from the substrate runtime.

Some examples of off-chain workers can be found at https://github.com/tomusdrw/sub0-offchain-workshop and https://github.com/jimmychu0807/substrate-off-chain-pricefetch

**4. Corda Network Issuing Obligations and Settling with Cash**

The Corda platform can be used to issue, transfer and settle obligations through its defined contracts and API integrations. To settle an obligation with cash, the issuer of the obligation would require having Bank APIs integration for the issuer itself, and have a mapping of bank accounts where the obligations will be settled. The idea for this exploration was to understand how this process would work, and develop some foundational knowledge to potentially further explore the Corda Token SDK. This exploration does not demonstrate cross-chain interoperability as this is not settling obligations across two different blockchains. However, it demonstrates potential integration with legacy financial institutions, or legacy payment rails through APIs and settling on-chain obligations. The APIs were not used in the demonstration, but cash and obligations were issued and settled on the Corda network. The team believes that there is a potential of further explorations on Corda Asset encumbrance, Corda token SDK, and Corda Settler.

**5. Multilateral Sovereign and Trade Blockchain Project (WBG)**

The multilateral sovereign and trade blockchain project at the WBG is an effort to explore the potential of Blockchain and qualify it as the go-to technology to address and circumvent challenges associated with multilateral agreements. We demonstrated the management of multilateral agreements by leveraging two separate Blockchain platforms, namely the core chain and the service chain. These are described as under-

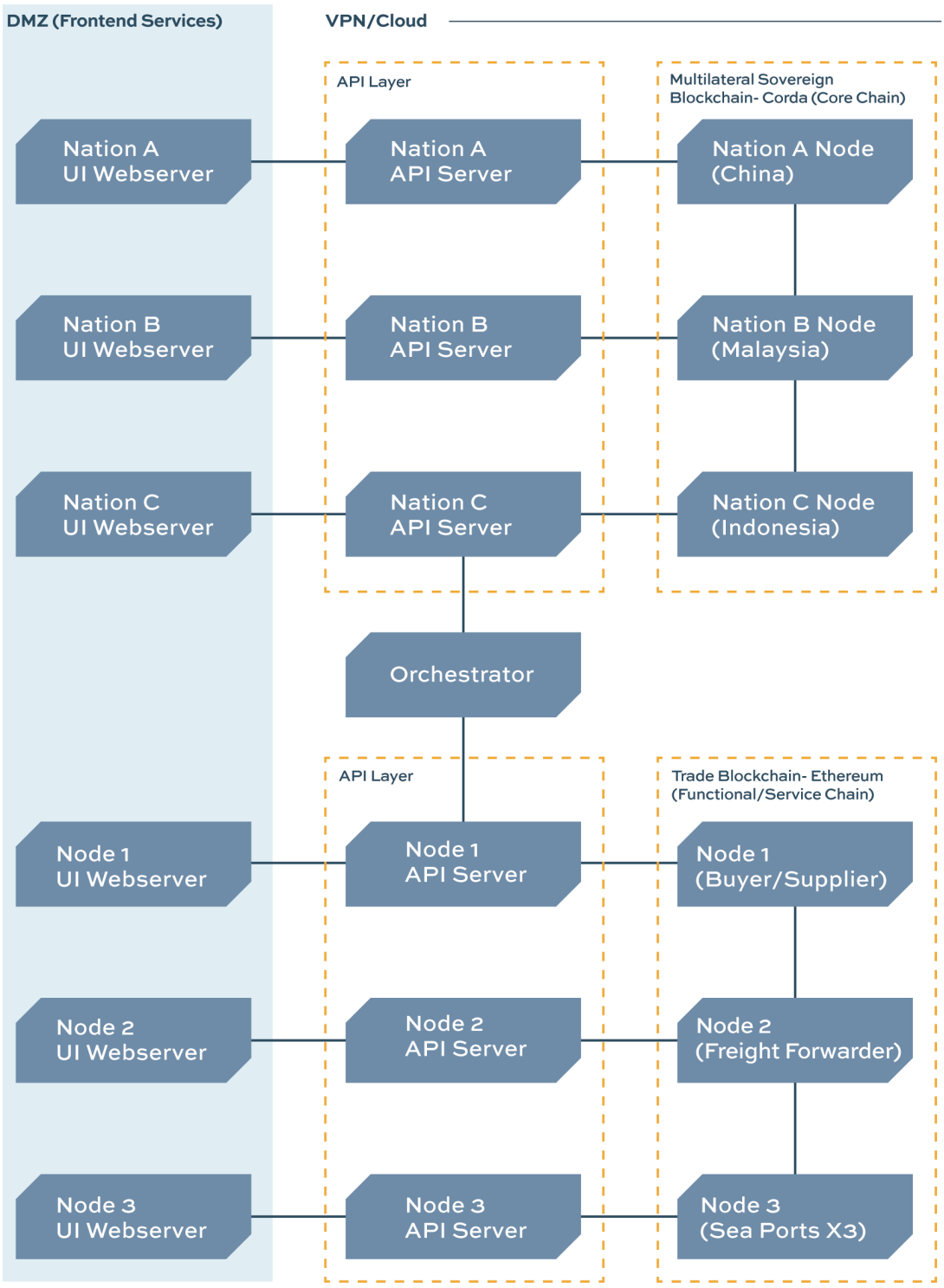


**Multilateral Sovereign Blockchain (Core Chain)** This network includes national or sovereign entities. For the purpose of this project, we have simulated the participation of China, Indonesia and Malaysia in the wider context of an FTA between ASEAN countries and China. These countries are represented by a node each and leverage the network to record multilateral agreements. The platform of choice in this case is Corda.

**Trade Blockchain (Service Chain)** Here, we have simulated participation from the buyer (in Indonesia), the supplier (in China), the transit hub (Malaysia), the respective seaports and the freight forwarder. For the sake of simplicity, both the buyer and supplier operate from two separate member accounts on the first node, the freight forwarder operates via a member account on the second node and the seaports operate via member accounts on the third node. The Blockchain platform used here is Ethereum (private instance).

**The reference architecture for these Blockchain networks is as illustrated below:**

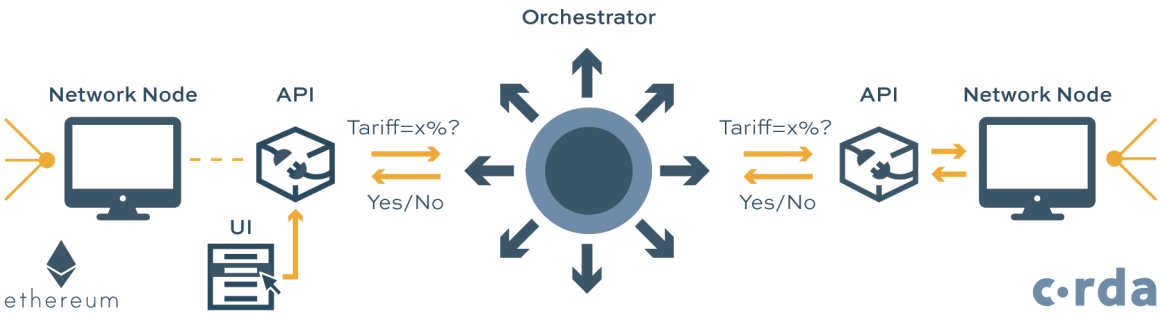
**FIGURE 9:** REFERENCE ARCHITECTURE



In Phase 1, the main purpose of the core chain was to track trade and transit agreements between participating nations (China, Indonesia and Malaysia). The trade agreements specified preferential tariff rates for certain goods over a given period of time, and a limit on the quantity. Similarly, a multilateral agreement covering, among others, transit arrangements allows for goods to be transported via the ports of a given country. Although multiple nations can be part of this network, only the ones involved in a given trade or transit agreement are privy to the details of an agreement.

As the name suggests, the service chain is intended to implement services, such as the supply chain, trade finance and payments, while also governed by multilateral agreements. For this project, we have taken an end-to-end procure to pay flow between the buyer and supplier to demonstrate the service layer application. One of the key features that allows for such governance and adherence to multilateral agreements is the interoperability between the two platforms. This was achieved that using Orchestrator service at the API layer, as explained below.

**FIGURE 10:** ORCHESTRATOR AS AN APPLICATION ADAPTER

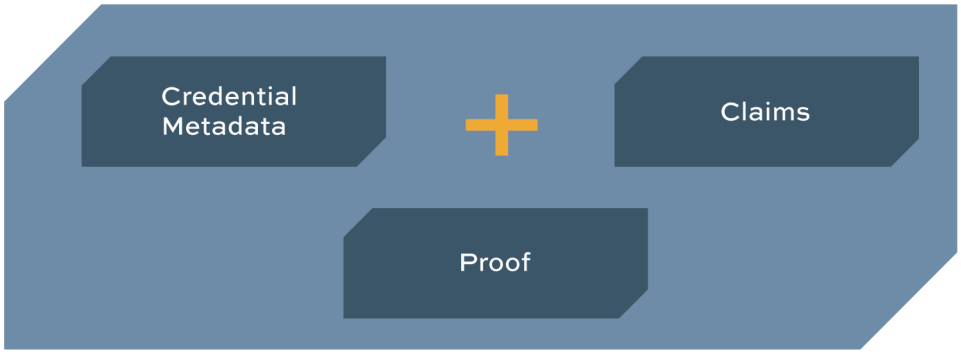



The architecture deployed to achieve this can be divided into three logical components: **(i)** Corda nodes and API in the core chain; **(ii)** the Ethereum nodes and API of the service chain; and **(iii)** the Orchestrator, which is a Java application. The trigger for validation is initiated by the supplier on the UI screen, this event makes an API call to the node service on Ethereum with the relevant PO details. The node service, in turn, makes a call to the Orchestrator application. Upon receiving the data, the Orchestrator will make an API call to the web server corresponding to the Corda node that represents China. Next, the Web server makes an internal RPC (Remote Procedure Calls) to the node's vault to retrieve trade and transit agreement for a two-way match with the PO data. The response is carried back via the web server to the Orchestrator, and subsequently to the node service on the Ethereum chain. Depending upon the response received, the smart contract for the given PO updates its state to either 'Accepted' or 'Invalid'.

In Phase 2, we employed Verifiable Credentials (VC) to demonstrate direct integration amongst two different blockchain platforms (see Figure 11). In this context, the client blockchain platform requests data from the counterpart blockchain platform and re-

ceives it in form of a VC, thereby ensuring the correctness and authenticity of data without any dependency on external entities and systems, such an orchestrator. A VC is a data structure that contains credential metadata made up of information on the credential itself, e.g. issuer information, issuance date, etc. A set of claims are issued by the issuer with regards to a subject. This information is combined with the proof identifying the issuer, and ensures that the verifier of the credential can verify the authenticity of the credential.

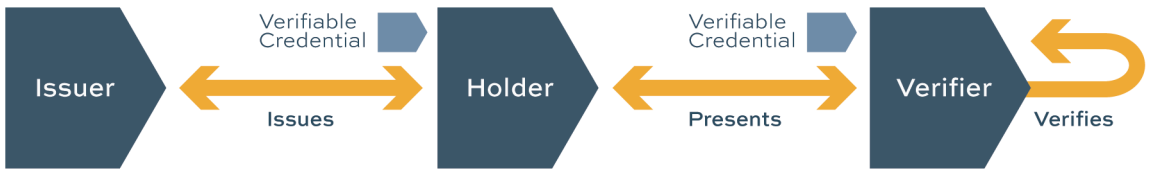
**FIGURE 11:** VERIFIABLE CREDENTIAL






To use a VC, an issuer issues a verifiable claim to the holder. The holder presents the verifiable claim to the verifier. The verifier then checks the verifiable claim (see Figure 12).

**FIGURE 12:** VERIFIABLE CLAIMS




The issuer issues a VC to the holder. The holder can then present the VC to any verifier who needs to verify the claim(s) being made by the holder pertaining to the subject of the VC. The verifier can independently verify the VC.

**To use VCs, each network node should have the following capabilities:**

1. Accept data in the form of VC;
2. VCs issued by trusted issuers; and
3. Provide output in the form of a VC;

The usage of verifiable claims is demonstrated through the interaction between the Malaysian Port on the service chain with the Malaysian node on the core chain. The goods pass through the Malaysian port which acts as a transit hub, before it reaches the buyer based out of Indonesia. To ensure that the goods being transported are in line with the agreed upon transit agreement between the three nations, the Malaysian Port issues a request for transit agreement data in the form of a VC to the Malaysian sovereign node, and then verifies the validity of the transit agreement residing on the Malaysian sovereign node. Upon receiving a positive response on parameters, such as tariffs, product code, validity, etc., the goods are forwarded to the shipping line for further transportation.

Table 4 summarizes the technical explorations of blockchain interoperability by this working group.

**TABLE 4:** SUMMARY OF WBG'S TECHNICAL EXPLORATION OF BLOCKCHAIN INTEROPERABILITY

| APPROACH | PROJECT | BLOCKCHAINS INVOLVED | GOAL |
|---|---|---|---|
| Oracle/Notary | Interledger PoC | Ethereum and Ripple | Value Exchange |
| | Multilateral Blockchain Phase 2 | Corda and Ethereum | Information Exchange |
| Sidechain/Relay | Polkadot PoC | Polkadot | Information Exchange |
| Time-bound Asset Locking and Release | HTLC PoC – 1 | Private Ethereum and public Ethereum | Value Exchange |
| | HTLC PoC – 2 | Two private Ethereum networks | Value Exchange |
| Application Layer Adapter | Corda Settler | Corda & Legacy | Value Exchange |
| | Multilateral Blockchain Phase 1 | Corda and Ethereum | Information Exchange |

FIVE

# Concluding Thoughts and Implications for International Development

# Concluding Thoughts and Implications for International Development

This White Paper has shown that blockchain interoperability is about sharing data (value and information) across different blockchain networks and legacy systems. Blockchain interoperability is seeing some important experimentation by central banks and technology providers in cross-border payment areas. However, there are many other use cases that will depend on having interoperability. For instance, with support from the Ministry of Foreign Affairs of the Netherlands and the Bill and Melinda Gates Foundation, the WBG has explored the role of Fintech in economic development, especially with respect to financial inclusion. They looked at how smart contracts (one of the highly important blockchain capabilities) can be leveraged in a wide range of microfinance transactions covering supply chain finance, insurance and consumer credit.[54] In the exploration, one of the key takeaways in effective smart contract deployment is the need for large-scale connectivity with an external data source; the blockchain based smart contracts need to interoperate with legacy systems for getting its data inputs in a reliable and secure way. This case reveals the need of interoperability across different organizational infrastructures and data sources. The framework highlighted in this White Paper makes it clear that a governance group is needed to oversee data sharing, monitor interoperability standards from standard-setting bodies, refer to the technical framework to find an appropriate approach, and examine security and legal framework to check the design and implementation.

The global supply chain is said to have a lot of potential in leveraging emerging technologies, such as AI, Blockchain and the Internet of Things (IoT). The COVID-19 pandemic has also brought the issue of cross-supply chain communications into focus. However, the lack of connectivity of IoT devices and Blockchain systems have become barriers because of the absence of common standards and interoperability. [55] These challenges relating to standards will need to be resolved by standard-setting bodies.



54 World Bank. 2020. "Smart Contract Technology and Financial Inclusion." Open Knowledge Repository. World Bank, Washington, DC. Accessed June 23, 2020. Available at: https://openknowledge.worldbank.org/handle/10986/33723.

55 Niforos, Marina. 2019. "Bridging the Trust Gap: Blockchain's Potential to Restore Trust in Artificial Intelligence in Support of New Business Models." International Finance Corporation (IFC), October.

Among various explorations by the World Bank teams, the e-Procurement and disbursement traceability use case exploration is very relevant in the interoperability discussion. In the disbursement traceability use case, the team is exploring blockchain-enabled grants and loan disbursements to client countries for WB funded projects. The success would depend on how these could be operationalized by the country government either to complement their financial management systems or become an alternative to fragile and lease developed countries for their financial management and procurement systems. Concerned stakeholders include donors, the World Bank, governments, project intermediaries, suppliers and contractors, and ultimately the beneficiaries. In addition to this, there is another exploration of blockchain-enabled e-procurement systems which is looking into modernizing and making the procurement systems more efficient. Going forward, there might be a need for these two different systems to be able to have data exchanged across chains and be able to interact with each other.

Interoperability can be a complex issue because it is needed between different instances of the same blockchain platform, between different blockchain platforms, and then, of course, between those blockchain platforms and remaining systems with legacy interfaces. With blockchain systems, interoperability is more difficult, as it is significantly different than existing isolated data environments where you can agree on the transfer of data. Blockchain entails more than this as it involves transfering state and provenance, which is much more complex than simply the data fields. Is it about data provenance or about control flow? In fact, it covers all of these. The idea of a heterogonous future state with more than one tech platform is inevitable. Ensuring they can work together is key. How to validate something from one blockchain to another blockchain is important.

# Glossary

**BITCOIN**
Blockchain protocol developed by Satoshi Nakamoto

**BLOCKCHAIN**
A ledger where data is organized into blocks linked by a cryptographic hash

**CONSENSUS MECHANISM**
A mechanism that verifies that the information that is placed in a blockchain is valid

**CRYPTOGRAPHY**
Technique for secure communication

**DIGITAL SIGNATURES**
Mathematical scheme to verify the authenticity of digital messages or documents

**ENCRYPTION**
Encoding message in such a way that only authorized parties can access it



**ETHEREUM**
Decentralized platform for application that are expected to run exactly as programmed

**FORK**
A split in a blockchain that results in the formation of a new chain

**HASH**
Cryptographic hash function used in the verification of the authenticity of data

**HYPERLEDGER**
A multi-project open source collaborative effort hosted by The Linux Foundation, created to advance cross-industry blockchain technologies

**MINING**
Process of adding a record to a blockchain ledger

**NODES**
A device on a blockchain network

**PEER-TO-PEER NETWORK**
A network made of computers that are connected to each other whole being equally privileged

**PROOF-OF-WORK**
A technique for combatting e-mail spam by requiring proof of computational effort

**SMART CONTRACT**
Autonomous agent that live within the Ethereum execution environment of virtual machine. Other platforms do also make use of smart contracts e.g. Hyperledger

**HASH TIME-LOCKED CONTRACT (HTLC)**
A smart contract that enables the implementation of time-time bound transactions



**NOTARY NODE**
A notary is a service that provides transaction ordering and timestamping

**TOKENS**
A token is a symbol whose value does not depend on mining. A token is not a coin.

**STANDARDS DEVELOPING ORGANIZATION**
An organization whose primary activities are developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise producing technical standards that are intended to address the needs of a group of affected adopters

# Endnotes

**TABLE 5:** BLOCKCHAIN INTEROPERABILITY DEFINITIONS

| AUTHORS (YEAR) | DEFINITION |
|---|---|
| Hardjono, Lipton, and Pentland. MIT (2018) | Interoperable blockchain architecture is a composition of distinguishable blockchain systems, each representing a distributed data ledger, where transaction execution may span multiple blockchain systems, and where data recorded in one blockchain is reachable and verifiable by another possibly foreign transaction in a semantically compatible manner. https://arxiv.org/pdf/1805.05934.pdf |
| Lima. IEEE (2019) | "Transfer[ing] value, assets, and tokens between…multiple platforms" https://www.standardsuniversity.org/e-magazine/may-2019-volume-9-issue-1-blockchain-standards/distributed-ledger-technology-dlt-blockchain-interoperability-standards/ |
| Buterin. R3, (2016) | [The capability to] move assets from one platform to another, or payment- versus-payment and payment-versus-delivery schemes, or access information from one chain inside another (e.g. "identity chains" and payment systems may be a plausible link)… without any additional effort required from the operators of the base blockchain protocols. https://www.r3.com/wp-content/uploads/2017/06/chain_interoperability_r3.pdf |
| GS1, IBM (2018) | Leveraging common standards for identification and for data sharing.<br>**1.** Globally unique, persistent identification for organisations, locations, and things<br>**2.** A standardised language for supply chain events<br>**3.** A scalable network governance model that crosses ecosystems.<br>https://www.gs1.org/sites/default/files/bridging_blockchains_-_interoperability_is_essential_to_the_future_of_da.pdf |
| EU Blockchain Observatory and Forum (2019) | The ability to exchange data with other platforms, including those running different types of blockchains, as well as with the off-chain world. https://www.eublockchainforum.eu/sites/default/files/reports/report_scalaibility_06_03_2019.pdf |

# Appendices

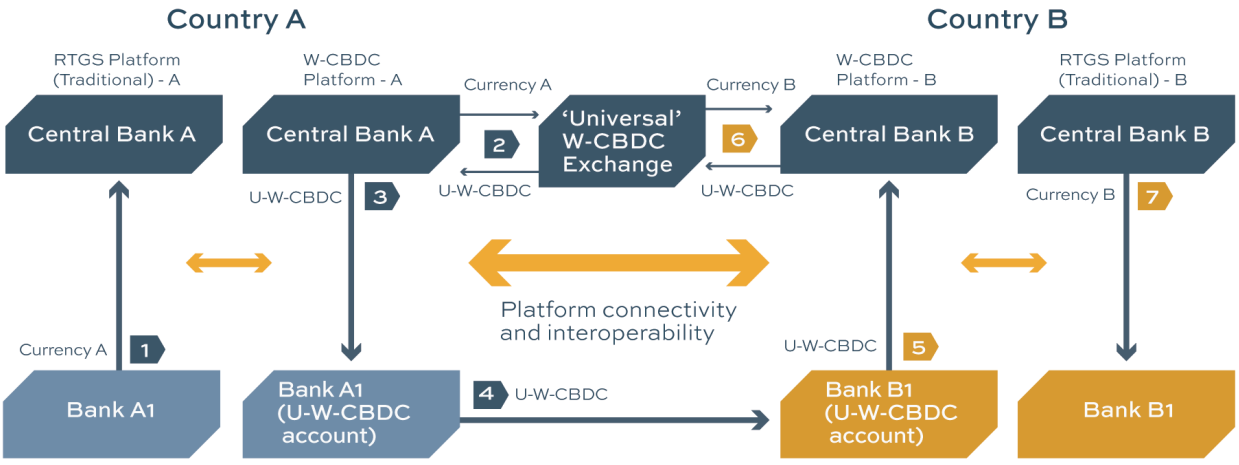
# Appendix One: Cross-Border Payments & Settlement and Current Interoperability Initiatives

This appendix reviews the increasingly discussed use case of cross-border payments involving blockchain technology. Addressing the cost and slow execution of cross-border payments and settlement has been a major motivation for projects, such as Bitcoin, Ripple or Libra, as well as some central bank-led projects on wholesale CBDC interoperability, e.g. Ubin, Jasper or Stella. From a technology perspective, the main issues with the current systems include the lack of standardized payment status capability, incompatible real-time gross settlement (RTGS) systems that don't operate 24/7, and reliance on too many intermediaries operating with their legacy systems. Central banks have started to study both retail and wholesale Central Bank Digital Currencies (CBDC), and other rapid payment and settlement systems (e.g. TIPS in Europe).

Central banks have also collaborated across their various wholesale CBDC projects to study the question of interoperability. In the paper "Cross-Border Interbank Payments and Settlements paper"[1] and Jasper-Ubin (2019)[2], the authors explained how wholesale CBDC coupled with the use of blockchain could address most of the cross-border payments pain points.



## MODEL 3C: A SINGLE, UNIVERSAL W-CBDC BACKED BY A BASKET OF CURRENCIES




**Source:** Cross-Border Interbank Payments and Settlements

## Project Jasper (Bank of Canada)

Project Jasper started as an initiative in March 2016 between the Bank of Canada, R3 Lab and Research, Payments Canada, and other domestic financial institutions. All parties sought together as an industry to study DLT for interbank payments in Canada. Since the initiation of Project Jasper, there have been three phases of experimentation contributing to the development of a proof of concept leveraging wholesale central bank digital currency (W-CBDC) and DLT for interbank payment settlements.

### Jasper Phase I: Project Jasper Primer (March 2016 to June 2016)

This collaborative public-private research initiative aimed to understand how DLT could transform the wholesome payments system. An Ethereum-based interbank transfer prototype was developed at this phase. The goals were described as follows[3]:

> "Build a proposal for a central bank-issued digital currency, including issuance, transfer, settlement, and destruction.
>
> Leverage rapid prototyping to test and validate the business, operational and technical hypotheses."

The Bank of Canada has also tested digital depository receipts (DDR) as a digital representation of Canadian currency in 2016 and 2017. In the context of Project Jasper, DDRs took the form of "CADcoin" issued by the Bank of Canada to better understand the potential impacts of blockchain technology on financial market infrastructure (FMI).

### Jasper Phase II (December 2016 to April 2017)

Building on the learning outcomes of Phase I, Phase II focused on rebuilding the platform using an alternative form of DLT to test further the efficiency of this technology for the clearing and settlements of high-value interbank systems.[4] Jasper, therefore, transitioned to a Corda DLT platform, which consequently introduced the "notary node" concept at the core of its consensus protocol. This platform was exclusively built in a test environment only, and there was no integration with external systems.

The Phase II platform was built to accommodate multiple settlement options. The two settlement options by the platform are the "atomic" option and the liquidity-saving mechanism (LSM) option. This mechanism allows participants to coordinate their payments to reduce liquidity needs, through batches of queues payments.[5] Netting promotes funding efficiency and enables a smoother intraday flow of payments.

A key conclusion of Jasper Phase II was that the material benefits of a DLT-based financial system might be realizable if the scope of the DLT system included the settlement of multiple assets.

### Jasper Phase III: Securities Settlement using DLT

Jasper Phase III explored the potential benefits of integrating this "cash on ledger" with other assets, such as foreign exchange and securities. By extending Phase II's proof of concept, it now allowed for immediate cleaning and delivery-versus-payment settlements, demonstrating the possibility of completing post-trade settlement on a DLT platform. The ability to settle transactions immediately significantly reduces counterparty risk and frees up collateral.

## Project Ubin. Monetary Authority of Singapore (MAS)

Project Ubin aimed to help MAS and the industry better understand the technology and the potential benefits it may bring through practical experimentation.

### Ubin Phases I, II and III

In partnership with R3 and a consortium of financial institutions, MAS started Project Ubin to support "the creation of open Intellectual Property and foster collaboration between industry players, creating a vibrant, collaborative, and innovative ecosystem of financial institutions and FinTech companies."[6]

Phase I served as the foundation to assess the feasibility and implications of DLT and to identify the elements required for future, and phase II focused on solving transactional privacy and deterministic finality, and most critically, the ability to perform multilateral netting capabilities in a decentralized manner.

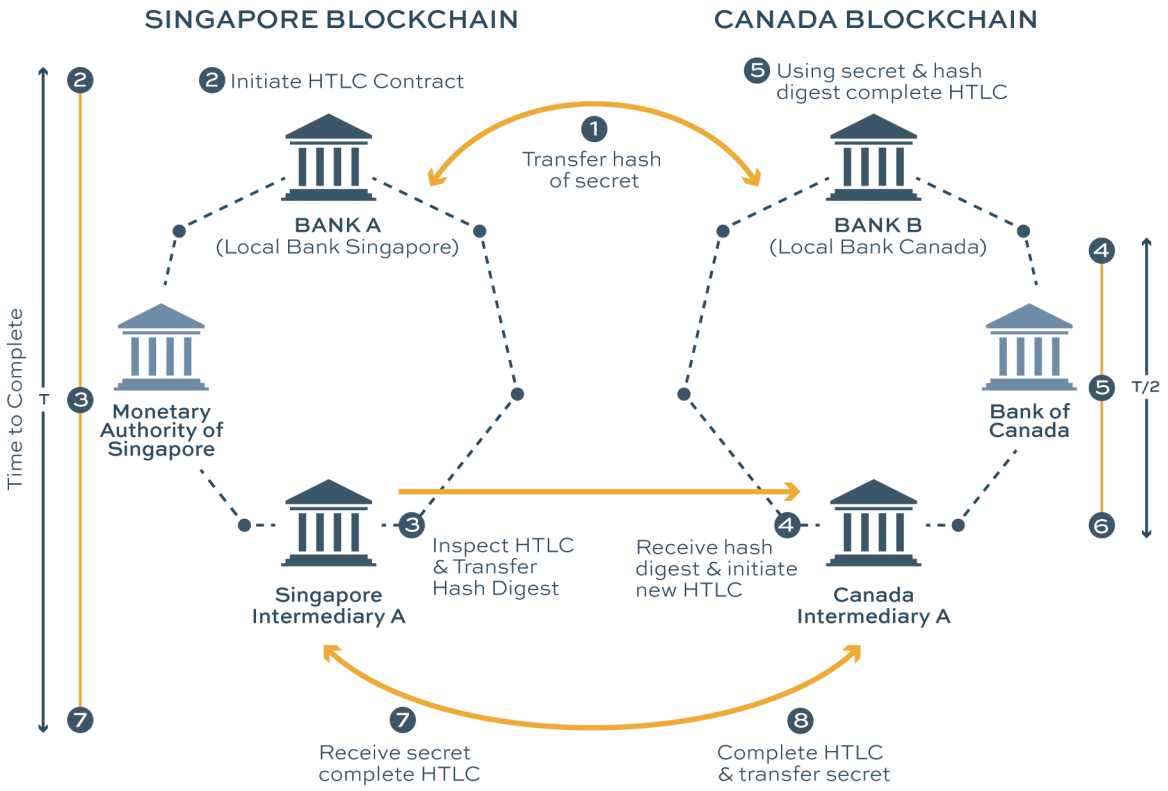
Led by MAS, Singapore Exchange and Deloitte, Phase III considered utilizing DLT to develop Delivery versus Payment (DvP) for the settlement of tokenized assets to achieve interledger interoperability and finality of DvP.

### Ubin Phase IV: Cross-border payment-versus-payment (PvP)

In Phase IV, MAS and BoC linked their respective experimental domestic payment networks by the announcement of Project Jasper-Ubin in May 2019. This experience was deemed successful on cross-border and cross-currency payments using CBDC.

### Ubin Phase V: Enabling Broad Ecosystem Collaboration

Project Ubin is currently determining the commercial viability and value of the blockchain-based payments network and is undergoing industry testing to determine its ability to integrate with commercial blockchain applications.




**Source:** Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies

## Project Stella

The Bank of Japan (BOJ) and the European Central Bank (ECB) together launched Project Stella in December 2016, which studies the possible use of DLT for financial market infrastructures. Like Jasper and Ubin, Project Stella was developed through development phases.

### Stella Phase I and II

In Project Stella's Phase I, the BOJ and the ECB conducted experiments to determine "whether specific existing functionalities of their respective payment systems could be run in a DLT environment in an efficient and safe manner". In Phase II, project Stella sought to gain practical understanding of DvP functioning on DLT thanks to prototypes developed on three different DLT platforms: Corda, Elements and Hyperledger Fabric. Reports indicate that "DvP can run in a DLT environment subject to the specificities of the different DLT platforms". Depending on the use case, the design of DvP can be influenced by a number of factors, including "the interaction of the DvP arrangement with other post-trade infrastructures.[7]

They concluded that DLT offers a new approach for achieving DvP between ledgers, which does not require any connection between ledgers thanks to "cross-chain atomic swaps," which can help ensure interoperability between ledgers. Cross-ledger DvP arrangements on DLT can be complex and can give rise to additional challenges that would need to be addressed. Legal aspects, which have not been part of this study, would need to be further explored.

### Stella Phase III: Synchronizing cross-border payments (June 2019)

Following the two previous phases, Project Stella examined how cross-border payments could be improved. "Cross-border payments are payments between currency areas that involve various entities across multiple jurisdictions. Compared with domestic payments, they are often characterized as slow and costly".

Phase III identified a new approach for settlement across ledgers through HTLC, which would potentially "allow the mitigation of credit risks through the synchronization of settlements". The BOJ and ECB conducted experiments involving synchronizing payments between DLT ledgers, between centralized ledgers, and between DLT and centralized ledgers.[8]

The findings indicate that "only payment methods with an enforcement mechanism [through a smart contract], either through the ledger itself or through a third party, can ensure that the transacting parties that completely satisfy their responsibilities in the transaction process are not exposed to the risk of incurring a loss on the principal amount being transferred". Although experiments applying a payment method with HTLC proved the technical feasibility of synchronized settlement between different types of ledgers, further reflections on legal and compliance issues have been raised.

### Stella Phase IV: Balancing confidentiality and auditability in a DLT environment

Phase IV focused itself on privacy-enhancing technologies/techniques (PETs) as challenges arise when auditing transactions in DLT-based financial market infrastructures, while also limiting access to information by third parties to ensure the confidentiality of the payment system.

# Appendix Two: Regulatory Environment

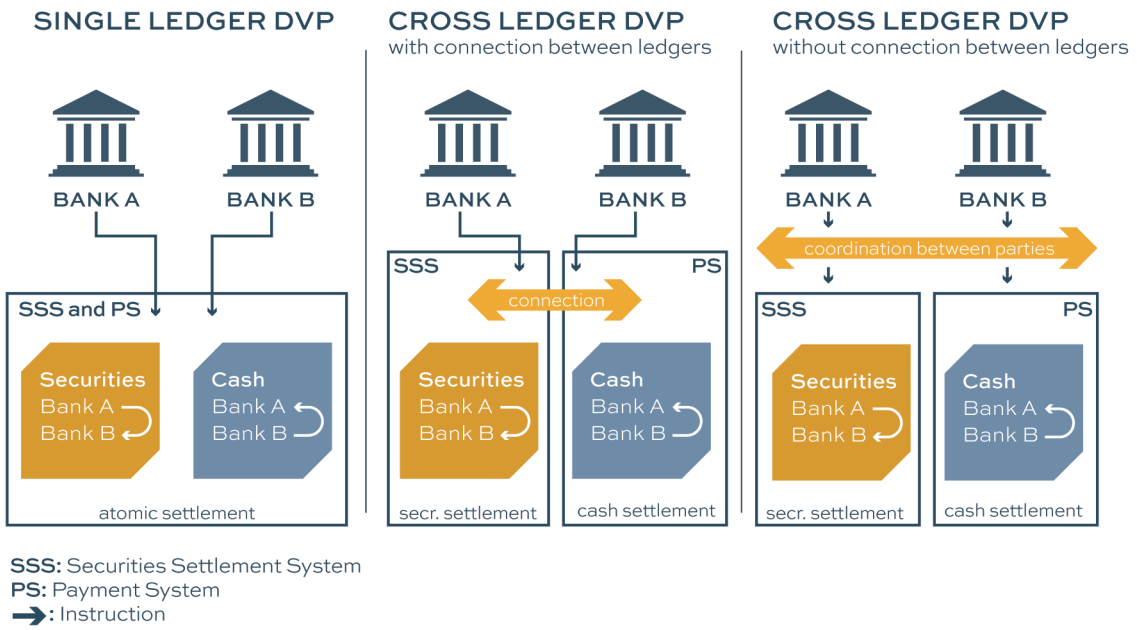
**This appendix reviews in detail some of the regulatory environment related to blockchain in the United States and around the world.**

## Regulatory Environment

Blockchain technology has been subject to regulatory scrutiny, part of which seems to result from what the blockchain application offers as a product and the risks that it may circumvent applicable laws. Lack of familiarity with the blockchain technology will certainly lead to heightened scrutiny as we do not know whether the technology fulfills relevant legal and regulatory requirements. Still, it has also gained enough support to prompt regulators to either pass new laws, or attempt to fit blockchain technology developments within existing legal frameworks.

The clearest example of the latter is the way government authorities treat digital assets, e.g. Bitcoin, under their existing laws. In the United States, early initial coin offerings (ICOs), which offered retail investors the opportunity to invest in the development of new blockchain projects, raised the question of whether these fundraising projects could be regulated by established securities laws. The United States Securities and Exchange Commission (SEC) was slow to act on this question, but eventually took a step toward answering the question in the affirmative by bringing enforcement actions under existing securities laws against startup companies offering ICOs.

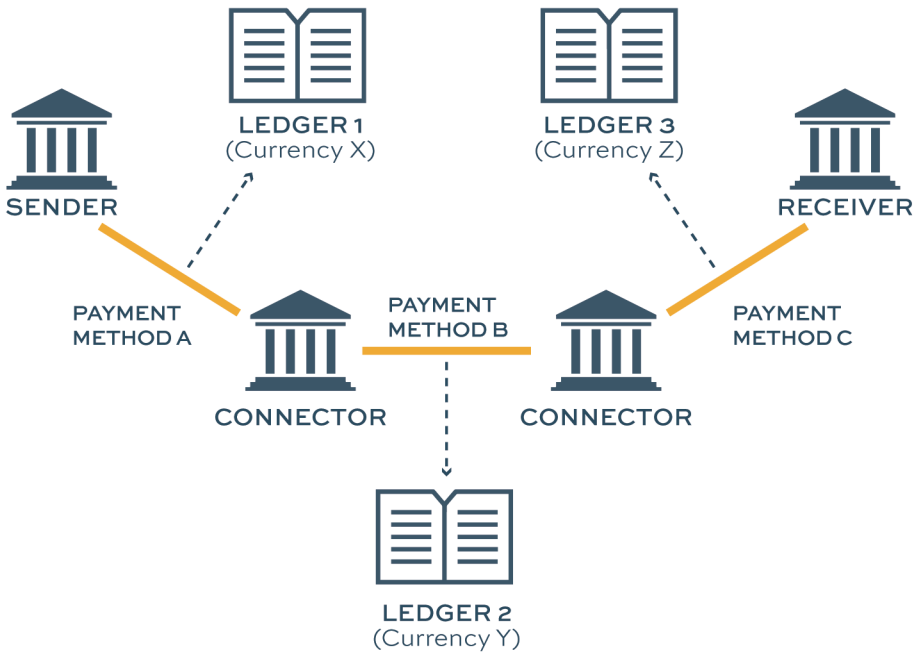





**SSS:** Securities Settlement System
**PS:** Payment System
→: Instruction

It is illegal to sell a security in the United States unless the security is registered with the SEC or is exempt from registration. The definition of "security" is set forth in the Securities Act of 1933 and the Securities Exchange Act of 1934. Generally, the courts have applied a four-part test to determine whether investment contracts are securities: whether the arrangement involves: **(i)** an investment of money; **(ii)** a common enterprise; **(iii)** the expectation of profits; and **(iv)** the expectation of profits is to be derived from the efforts of others. If these elements are present, the arrangement is a security and must either be registered with the SEC or be exempt from registration.

The SEC has applied this established test to digital assets. It proceeded to bring enforcement actions against Airfox and Paragon, two start-up companies, for failing to register their ICOs as securities under federal law. The companies settled the charges and agreed to register the securities, pay a fine and return money to investors. The SEC settled another enforcement action with EtherDelta, a token trading platform, soon thereafter. It was the SEC's first action "based on findings that [the] platform operated as an unregistered national securities exchange."




These examples show that regulators will apply existing legal frameworks to regulate Blockchain based on the nature of the product being offered. Accordingly, developers and practitioners must consult existing laws in the relevant industry before adopting blockchain technology solutions.

On the other hand, and apart from being subject to existing legal frameworks, Blockchain technology also has the potential to enhance an industry's ability to comply with applicable regulations. In the area of healthcare, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulates the United States healthcare industry. Among other provisions, the law codified the Privacy Rule, which governs the use and disclosure of patient health information (known as "protected health information" or PHI), and sets standards for patients to understand and control how their PHI is used. Blockchain technology can be used to great effect to enhance compliance with the Privacy Rule. As others have noted, a patient's identity and records could be stored on a private, permissioned blockchain and private keys could be used to transfer data or information in a secure manner.

In addition to fitting blockchain technology applications in existing legal frameworks, a number of United States jurisdictions have passed blockchain-specific laws that aim to encourage the adoption and use of blockchain within their borders. The following is a summary of laws that are at the forefront of this rapidly developing area:

**ARIZONA:** In 2017, Arizona passed HB 2417, which allows the use of smart contracts in commerce and prohibited contracts from being denied legal validity because the contract contains a smart contract term. The bill recognizes records secured using blockchain as valid records under state law. Tennessee passed similar legislation in 2018.

**DELAWARE:** Thanks to its business-friendly laws, more than half of publicly traded companies in the United States are incorporated in Delaware. Accordingly, Delaware took an early interest in incorporating blockchain developments into its existing corporate laws. In 2017, it amended its general corporation law to allow companies to maintain their corporate records, including stock ledgers, using blockchain technology.



**VERMONT:** In 2018, Vermont was the first in the country to allow blockchain-based limited liability companies (BBLLC). The idea, similar to traditional limited liability companies, is to allow companies that use blockchain technology as a material part of their business activities to protect its members from legal liability. A BBLLC may customize its governance structure using blockchain technology and validate and store records on a blockchain. The Act also directed Vermont's Department of Financial Regulation to explore the use of blockchain technology in different industries and to identify regulatory changes that would allow blockchain to be adopted in those industries.

**WYOMING:** In 2019, Wyoming was one of the first states to adopt a series of blockchain-friendly measures aimed at bringing blockchain business to the nation's least populous state. Wyoming laws: **(i)** create an exception from state securities laws for blockchain tokens; **(ii)** make virtual currency exempt from money transmitter rules; **(iii)** recognize distributed-ledger-based corporate recordkeeping; **(iv)** exempt virtual currency from property taxes; and **(v)** recognize a form of limited liability company (the "series" LLC) conducive to blockchain businesses.

In addition, various United States jurisdictions have launched their own projects to explore the use of blockchain, rather than simply regulate its usage by private actors. The states of Delaware, Illinois, and Colorado, among others, have launched initiatives to shift state records to distributed ledgers. More broadly, in 2019, nearly every state in the US had a blockchain-related bill sponsored and introduced to the legislature, proving that this rapidly evolving area needs continuous monitoring to keep pace with changing regulations.

Globally, a number of countries have raced to court blockchain business by creating or amending regulatory frameworks:

**MALTA:** Also known as "Blockchain Island," this small island nation in the Mediterranean adopted a "complete regulatory framework" in 2018, which was "designed to make Malta one of the most desirable locations to set up shop in the blockchain space."The laws established the Malta Digital Innovation Authority, certified DLT platforms, set up exchanges and other companies in the cryptocurrency market, and established a regulatory regime governing cryptocurrency and ICOs.

**SWITZERLAND:** This European nation known for its banking and finance industries recently amended several existing laws to accommodate blockchain technology developments. Among other things, the amendments establish a legal basis for exchanging digital securities and for recovering digital assets from bankrupt companies.

**LICHTENSTEIN:** Lichtenstein passed new laws and amended existing laws in order to allow rights and assets to become tokenized, thereby allowing the development of the so-called token economy.

**UNITED ARAB EMIRATES (UAE):** In 2018, the UAE announced the Emirate Blockchain Strategy 2021, a plan to shift at least 50 percent of government-related transactions to DLT platforms by 2021. The country's ambitious effort, expected to greatly increase efficiencies through reduced transaction costs, work hours and resource use, is a novel approach to incorporating blockchain-based solutions into everyday life. Specific projects include using blockchain technology for logistics and to record land ownership. The country was an early leader in regulating businesses operating using Blockchain technology, issuing guidelines for ICOs in 2017 and establishing an authority to regulate digital assets.

**JAPAN:** Despite high-profile hacks in Japanese cryptocurrency exchanges, Japan encourages blockchain technology through constantly evolving laws and regulations. Since 2016, Japan has officially recognized cryptocurrency as legal tender and thereby regulates cryptocurrency under its financial regulatory authority. The generally friendly blockchain environment has encouraged Japanese exchanges to self-regulate, which allows them to quickly respond to evolving security threats such as hacks. Following perhaps inevitable conflict between exchanges and anti-money laundering policies, however, Japan recently banned privacy coin trading.

**SINGAPORE:** The Monetary Authority of Singapore (MAS) was an early regulator of cryptocurrency. MAS's approach is to "regulate the space to prevent stifling innovation, while simultaneously protecting investors and the public at large." MAS is participating in Project Ubin, which creates a digital token for the Singapore dollar on Ethereum. Singapore recently passed the Payment Services Act, which streamlines regulations for payment services, including cryptocurrency and exchange services. Payment service providers required to obtain licenses must meet anti-money laundering and countering the financing of terrorism (AML/CFT) requirements. MAS has issued AML/CFT guidelines specific to digital payment token services.

The opportunities behind digital inclusion have also created a need for development organizations with a focus on economic development and trade to establish agile technology-specialist teams. These teams have become privy to deliver concise advice on technology matters in various disciplines: business, economics, legal, and technical. Examples of these teams include the World Bank Group Technology & Innovation Lab, the IMF's Digital Advisory Unit, IDB (IDB Lab). Other intergovernmental organizations working to promote economic cooperation, such as OECD (Blockchain Policy Forum), WEF (Center for the Fourth Industrial Revolution), as well as the European Commission (Blockchain Observatory), have dedicated many working groups to research how growth can flourish through future technological developments. Many of these working groups strive to produce knowledge pieces for the public to evaluate and inspire the activities of these innovation teams. In addition, international conferences are regularly to capture the various learnings being carried out in various institutions. Nevertheless, there is no universal standard for Blockchain applications that could potentially facilitate interoperability at the moment. Such a space is open for exploration, development, and in need of leadership to pave the way.



## ENDNOTES

1 Authored by the Bank of Canada, the Bank of England, the Monetary Authority of Singapore, HSBC and a group of other commercial banks in the United Kingdom, Canada, and Singapore https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Cross-Border-Interbank-Payments-and-Settlements.pdf

2 https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Jasper-Ubin-Design-Paper.pdf?la=en&hash=437222C94FD39314FB4C685EA31FC3AAA5CA5DA1

3 https://www.payments.ca/sites/default/files/29-Sep-17/jasper_report_eng.pdf

4 Payments Canada (2017) "A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement"

5 International Monetary Fund (2019) "FinTech in Sub-Saharan African Countries: A Game Changer?"

6 https://www.deloitte.com/content/dam/Deloitte/sg/Documents/financial-services/sg-fsi-project-ubin-report.pdf

7 https://www.boj.or.jp/en/announcements/release_2018/data/rel180327a1.pdf

8 https://www.boj.or.jp/en/announcements/release_2019/data/rel190604a1.pdf