WORLD ECONOMIC FORUM

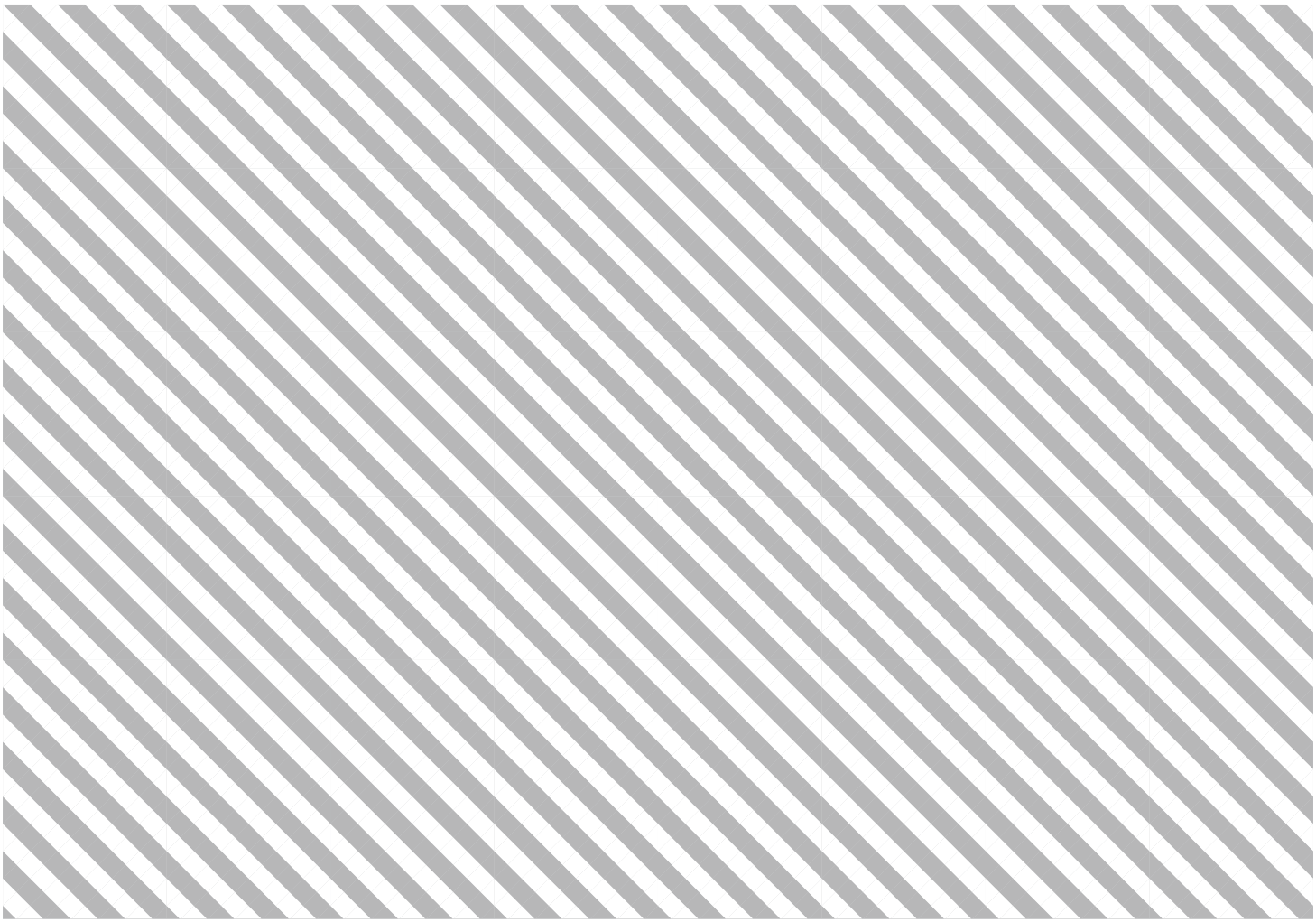
COMMITTED TO IMPROVING THE STATE OF THE WORLD

White Paper

Inclusive Deployment of Blockchain for Supply Chains: Part 6 – A Framework for Blockchain Interoperability

In Collaboration with Deloitte

April 2020



World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

Contents

Preface

Nadia Hewett, Project Lead, Blockchain and Digital Currency, World Economic Forum (Centre for the Fourth Industrial Revolution), United States

Margi van Gogh, Head of Supply Chain and Transport, Shaping the Future of Mobility, World Economic Forum, Switzerland

Linda Pawczuk, Global Consulting Blockchain and Digital Assets Leader, Deloitte, United States

Public and permissioned blockchains are now widely used for consumer-to-consumer (C2C) and business-to-business (B2B) data exchanges. In public blockchains, interoperability has been in development for many years – for instance, cross-chain, sidechains, proxy tokens, etc. However, a bigger challenge and, at the same time, a much bigger opportunity exists given interoperability among enterprise-grade permissioned blockchains. While still evolving, some solutions, such as trade finance platforms built under one jurisdiction, fail to realize the expected value, because trade and supply chains are global by nature. The value will come once different trade finance platforms in different countries can interoperate. Similarly, a traceability network is useless if data cannot be exchanged across industries, including manufacturers, logistics, wholesalers and retailers. Contrary to common belief, this specific challenge is not only a technology problem, but also a problem in terms of governance, data ownership and commercial business models that incentivize ecosystem stakeholders to collaborate with each other.

The 2020 coronavirus pandemic exposed weaknesses in supply-chain systems. Organizations globally (in both the public and private sectors) showed varying degrees of ability to respond. This revealed a breakdown in the collaboration required to track, trace, authenticate, finance and clear medical goods, supplies, etc. through trade channels in a trusted, verifiable and efficient manner. Such global events highlight the need for an interconnected and interoperable supply chain in a world after COVID-19. Contrary to common belief, this specific challenge is not only a technology problem, but also a problem in governance, data ownership and commercial business models in terms of how they incentivize ecosystem stakeholders to collaborate with each other.

Interoperability is the capacity of computer systems to exchange and make use of information. It is the capacity of systems to collaborate with each other, where collaborating in this sense entails the ability to transfer information or an asset between two or more systems while keeping the state and uniqueness of that entity consistent. The distributed nature of blockchain makes this ordinarily straightforward concept quite complex. In addition, interoperability for blockchain platforms implies that transactions involving parties or assets that belong to different blockchain platforms can be executed as if they belonged to the same blockchain platform. Successful interoperability enables the user to trust that "I know what I see is what you see" within a single platform as well as across platforms.

Blockchain interoperability emerged as a topic of much debate at World Economic Forum events and meetings. Typical questions included:

- Can blockchains speak to each other?
- Will the industry get to one global blockchain to rule them all?
- What blockchain platform should we use?
- Why don't we simply enhance our communication protocols to application programming interfaces?

> **"Interoperability enables the user to trust that 'I know what I see is what you see' within a single platform as well as across platforms."**

Continuing the series,[1] this white paper looks at one of the critical success factors of deployment: interoperability.

This is the seventh white paper in a series and part of a broader project focused on the co-creation of a toolkit to shape the deployment of distributed ledger technology in supply chains towards interoperability, integrity and inclusivity.[2] This paper aims to articulate, in simple terms, important blockchain and distributed ledger technology concepts as they relate to interoperability considerations.

Executive summary

In Section 1, the paper introduces the reader to blockchain interoperability and puts it in context: Blockchain solutions have been formed around existing smaller ecosystems, but global trade supply chains intersect with multiple ecosystems. However, the time is not yet right for convergence on a single platform due to, for example, commercial sensitivities, distinct views on technology choices, different perspectives on governance and as-yet still-developing nature of the blockchains, which is ultimately what makes interoperability critical.

In section 2, the paper elaborates on three blockchain interoperability layers (business model, platform, infrastructure) to structure how the reader thinks about interoperability requirements when analysing compatibility between blockchain platforms.

In section 3, the paper outlines three approaches to achieving interoperability to help the reader conceptually understand what needs to be done to proceed.

In section 4, the paper introduces a framework for selecting the right approach for blockchain interoperability. It combines the tools introduced in earlier sections and guides choice of approach depending on the context of the consortium and the level of compatibility between the platforms in question.

In section 5, the paper portrays the current state of interoperability solutions and their ability to connect the most common blockchain platforms.

In section 6, the paper presents two real-world use cases to give the reader an idea about where to learn more and to illustrate how the tools presented in the white paper can be applied in choosing an approach for blockchain interoperability.

In section 7, the paper lists several vital questions structured according to the interoperability layers from section 2 to give the reader a starting point and accelerate the collection of interoperability requirements.

While this paper can be read alone, blockchain concepts and features are covered in the first World Economic Forum white paper in this series – for further reference see *Inclusive Deployment of Blockchain for Supply Chains: Part 1 – Introduction* (April 2019).[3] The very nature of the topic requires some level of technical proficiency.

This paper does not examine the multitude of technical layers, complexities, hypotheticals and exceptions that exist within the blockchain space, especially related to significant differences between public and private chains, though the authors recognize their existence and importance.

1. Blockchain interoperability – context and definition

Context

Blockchain technology offers promising results, but overcoming the obstacles to widespread adoption remains a challenge, with the technology yet to reach enterprise maturity. Moreover, many existing solutions within supply chains are using blockchain for relatively simple use cases, while realizing that there are numerous possible opportunities both within and adjacent to the supply chain, as blockchain is relevant in finance, food safety, insurance and multiple other industries.

Industry analysts expect at least a handful of blockchain platforms to exist in the market, on top of which entire ecosystems of applications may flourish. The time is not yet right for a single platform due to, for example, commercial sensitivities, distinct views on technology choices, different perspectives on governance of blockchain networks and the still-developing nature of the technologies.

Consequently, "inter-blockchain communication", "an internet of blockchains" and "a blockchain of blockchains" (e.g. blockchain interoperability) have become hot topics to help ensure that various supply-chain stakeholders are less locked in to the design choices made. In short, this expresses the need to solve the challenge of interoperability, enabling the user to trust that "I know what I see is what you see" both within a single platform as well as across platforms.

> "To take the next leaps with blockchain technology, the interoperability between the chains and the integrity of data should be a top priority."
>
> **Jan Scheele**, Chief Executive Officer, BitCanna

Essentially, with multiple ecosystems within and adjacent to supply chains developing competing blockchain-based solutions, the potential benefits of shared ledgers and tokenization could be diluted if interoperability between the solutions or the underlying blockchain platforms is not ensured.

This white paper addresses the challenges of achieving blockchain-to-blockchain interoperability as well as between "regular applications" and blockchains. As the former is more challenging than the latter, the primary weight of this white paper is towards addressing blockchain-to-blockchain interoperability. As such, this white paper is of a technical character in order to shed light on the above-mentioned challenges. However, it will highlight both technical and non-technical requirements for interoperability.

What would incentivize vendors and users to work more intensely towards finding ways to enable interoperability?

The challenge is that one consortium designs and implements what is best for them given the use cases they are looking to address. Any incentives to ensure interoperability will always be secondary to that. Essentially, you prioritize short-term incentives (build something to prove the use case) for long-term initiatives (build something that will work with new or existing use cases on other complementing platforms).

Non-technical readers should take from the white paper that: blockchain interoperability currently is possible; that it depends just as much on governance, legal and data standards as it does on, for example, technical requirements; that it is easiest to achieve if you are willing to compromise on decentralization; and that technological development continues at breakneck speed.

Definition of interoperability

Put simply, interoperability is: a) the capacity of computer systems to exchange and make use of information; and b) the capacity to transfer an asset between two or more systems while keeping the state and uniqueness of the asset consistent. The latter part is what makes an otherwise straightforward concept complex in the context of blockchain. Ideally, blockchain interoperability should allow knowledge to be shared without sending copies of data, and provide fairness in the ordering of transactions and accessibility to data and codification of and adherence to common rules.

Figure 1: Blockchain solutions have been formed around existing smaller ecosystems…

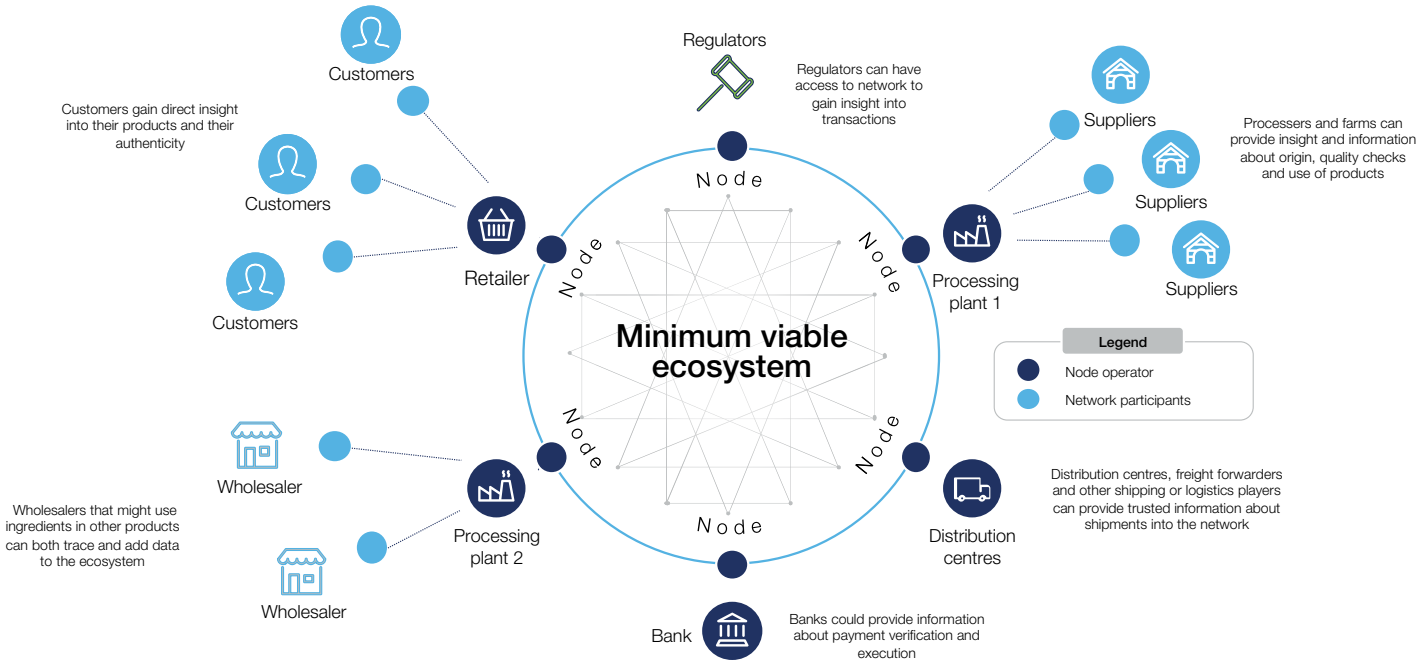
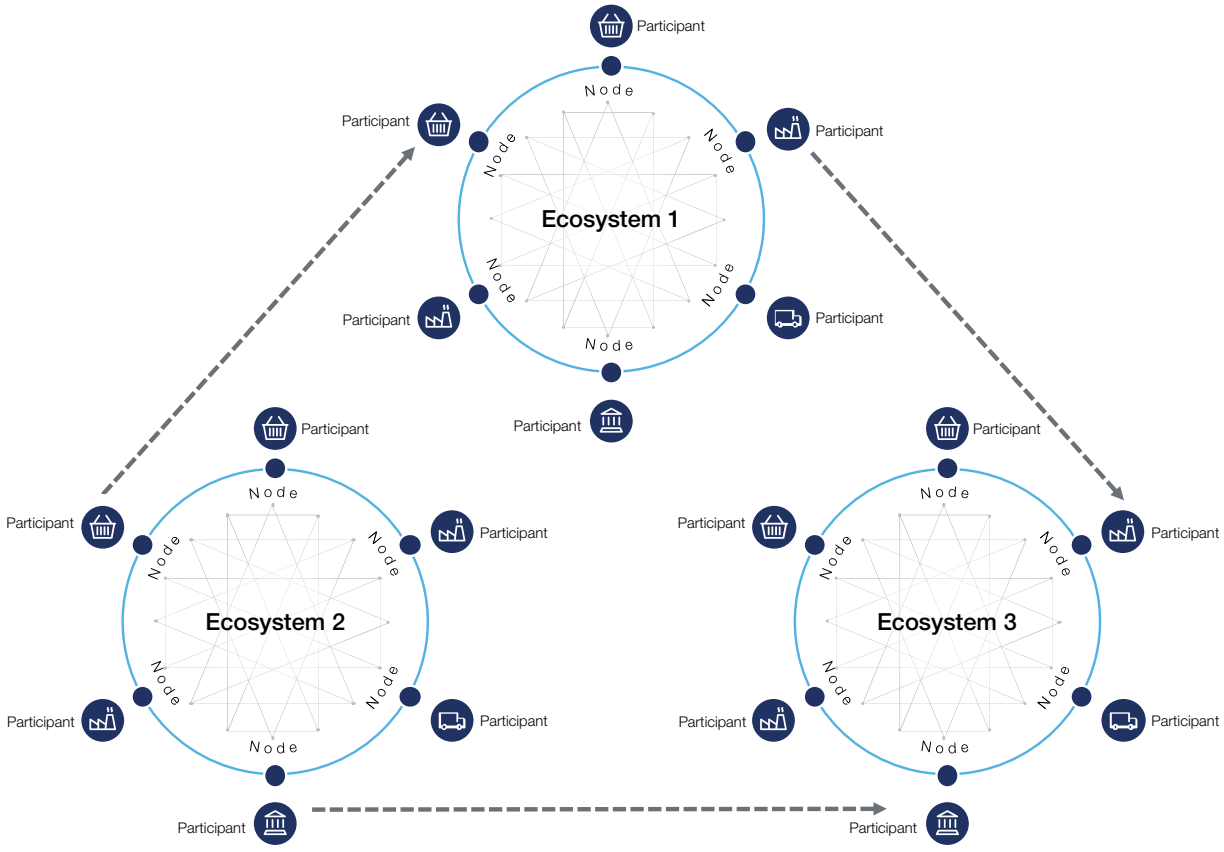


Figure 2: … but global trade supply chains intersect multiple ecosystems



Two types of interoperability

Blockchain-to-blockchain interoperability comes in two types beyond that of regular, non-distributed systems: digital asset exchange and arbitrary data exchange. Most supply-chain use cases will likely require arbitrary data exchange.

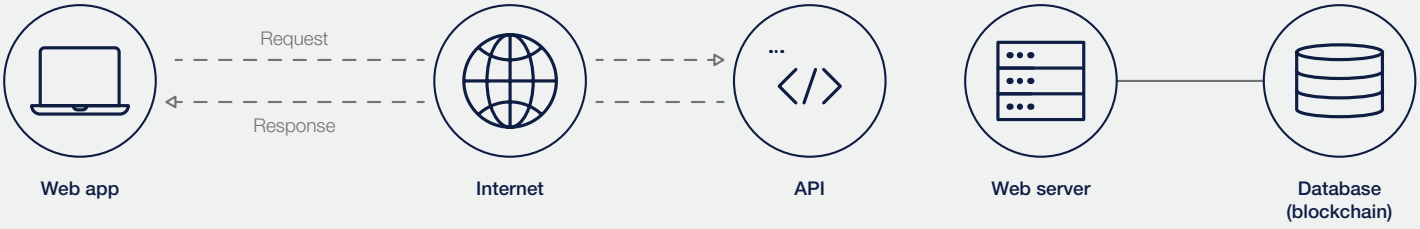
Digital asset exchange:
Put simply, digital asset exchange is the ability to transfer and exchange assets originating from different blockchains, such as cryptocurrencies, without trusted intermediaries (e.g. centralized exchanges). From a technical perspective, this functionality can be constructed atop blockchains that have fairly simple programming capabilities, as users on both sides can easily produce publicly verifiable signatures for actions that enable atomic swaps or transfers that complete only if both sides do their part.

An example is making bitcoin spendable in Ethereum decentralized applications (dApps) (see Figure 3).

> Atomic swaps are smart contracts that give you the ability to exchange digital assets on-chain or off-chain seamlessly and securely without the involvement of a third-party).

Figure 3: Illustration of a digital asset exchange, where a Bitcoin is spent through dApp on Ethereum

Figure 4: API is a piece of code that governs the access point to a server and the rules developers must follow to interact with a database, library, a software tool or a programming language



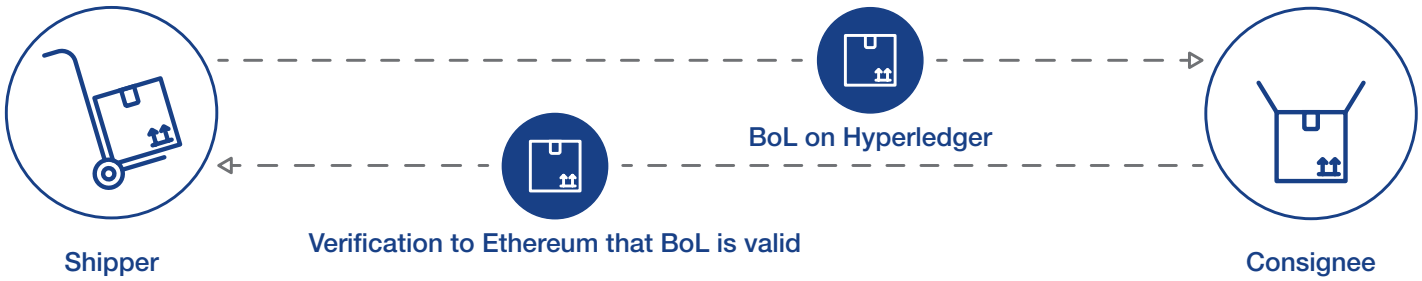
Arbitrary data exchange:
Put simply, exchanging arbitrary data is the capacity to do something on one blockchain platform that affects another blockchain platform. What is tracked is not necessarily an item of value but could be an event. From a technical perspective, this means making blockchain-to-blockchain application programming interface (API) calls, which can go as far as having smart contract code on one blockchain platform verify the consensus finality of events on other blockchain platforms directly.

This capacity allows the use data on one blockchain platform to affect state changes on another. It also lets us create synthetic versions on one chain of an asset that is home to another chain, making that asset usable on a state machine that occupies a different part of the trade space.

As most blockchains are passive systems unable to produce a verifiable-by-others signature, arbitrary data exchange is the more difficult type of interoperability to achieve. However, the use cases enabled by arbitrary data exchange can be more advanced than what digital asset exchange makes possible.

An example of arbitrary data exchange is the changing ownership of a bill of lading (BoL) from a shipper on Ethereum to a consignee on Hyperledger. The BoL is a document of title. Currently, the BoL is typically issued from the ocean carrier to the shipper/seller as proof of receipt of the container and contains data on, for example, the shipper, the consignee, the notified party, the vessel voyage, the vessel name, the container ID, goods description, trade terms, signatures, stamps and BoL number. The document is typically kept with the shipper/seller until payment for the shipment has been received from the buyer. The document can be changed multiple times if, for example, the shipment misses its route, if the notified party changes, if the buyer changes and the consignee needs updating. Moreover, banks typically hold a copy of the document as security for loans in relation to trade finance.

Figure 5: Illustration of how ownership of the bill of lading (BoL), which is arbitrary data, can be transferred from a shipper on Ethereum to a consignee on Hyperledger



2. Three layers of the blockchain interoperability model

Interoperability is a top concern for decision-makers interested in building blockchain solutions. Organizations do not want to find themselves on a blockchain platform that may limit their options for external collaboration in the future. They want to build scalable solutions that can grow with both the enterprise and the extended ecosystem if needed. Many organizations also want to remain flexible in changing or connecting to different solutions. Meanwhile, others are preoccupied with how to make their existing systems interoperable with blockchain platforms, typically to submit to or use data from a blockchain solution. This section focuses primarily on blockchain-to-blockchain interoperability while the coming sections also cover the former type of interoperability.

The interoperability model for blockchain solutions below consists of three layers addressing this challenge for the full stack for the blockchain solution, including the underlying blockchain platform on which it is built. It corresponds with typical blockchain architecture[4,5] and is intended for organizations to structure their efforts to: clarify interoperability requirements; enable blockchain solutions to exchange and make use of their data; and select one of three approaches to interoperability.

Figure 6: Blockchain interoperability framework breaking down the challenges in three layers: business, platform, infrastructure

Layer	Aspect
Business model	Governance model
	Data standardization
	Commercial model
	Legal framework
Platform	Consensus mechanism
	Smart contract
	Authentication and authorization
Infrastructure	Hybrid cloud
	Managed blockchain
	Proprietary components

In all three layers, a holistic question of trust must be posed: Do participants on blockchain platform A fundamentally trust the set-up of blockchain platform A? If the answer is yes, interoperability will help futureproof the solution in question. However, if the answer is no, interoperability can be a destructive force, eroding the incentive for participants to participate in the blockchain platform.

> **Remember that interoperability is not an individual decision, but a decision taken by at least two parties and probably more.**

Henrik Jensen, Senior Blockchain Adviser, Trustworks

Business model layer

When two ecosystems exchange data with each other, the governance models behind these two ecosystems should be comparable with each other, together with well-defined legal framework and commercial arrangements; technical feasibility alone cannot enable interoperability.

- **Governance**: To help ensure the trustworthiness of the participants, a prudent governance model has to be designed and agreed between the different blockchain ecosystems. For instance, if a bank in a know-your-customer (KYC) network opened an account for a blacklisted manufacturer, the second bank would then finance the blacklisted manufacturer by trusting the first bank. To potentially avoid these kinds of situations, a very stringent onboarding process for the blockchain platform will have to be in place, so that only qualified financial institutes can contribute KYC information to the platform, because they are essentially conducting KYC on behalf of the whole ecosystem.

> **The game is changing for container shipping: digitalization, regulatory complexity, cybersecurity, environmental impact. Customers are demanding a better experience. To stay competitive, we have to meet these challenges head on, to evolve. No one company can move the industry forward on its own. Collaboration is the key to greater efficiency and agility to meet new demands. Today, fragmented systems are holding us back. Without a foundation for the seamless, end-to-end exchange of information, these challenges will go unmet. At Digital Container Shipping Association (DCSA), we're establishing standards for a common technology foundation […] and pav[ing] the way for interoperability in the container shipping industry through digitalization and standardization.**

Thomas Bagge, Chief Executive Officer, Digital Container Shipping Association

Figure 7: Overview of selected organizations with a focus on creating standards to drive business model interoperability

BIA	The Blockchain Industrial Alliance (BIA) seeks to promote cross-blockchain transactions and interconnectivity. The goal of this alliance is to create a globally accepted standard for connecting blockchains and to bring innovations together.[6]
BiTA	The Blockchain in Transport Alliance (BiTA) is seeking to develop and embrace a common framework and standards from which transportation/logistics/supply-chain participants can build blockchain applications.[7]
BRIBA	The Belt and Road Initiative (BRI) has established the Belt and Road Initiative Blockchain Alliance ("BRIBA") to spur the development of the BRI by leveraging blockchain technologies.[8]
BSI	The British Standards Institution (BSI), the national standards body of the United Kingdom producing technical standards, is working on blockchain standards for supply chains.[9]
CESI	The China Electronic Standardization Institute (CESI) works with standardization, conformity assessment and measurement activities in the field of electronic information technologies. In the past couple of years, CESI has come out with a vision to introduce three blockchain standards on smart contracts, privacy and deposits in a bid to better guide the development of blockchain industry in the country.[10]
DCSA	The Digital Container Shipping Association (DCSA) seeks to pave the way for interoperability in the container shipping industry through digitalization and standardization.[11]
EBP	The European Blockchain Partnership (EBP) connects countries to cooperate in the establishment of a European Blockchain Services Infrastructure (EBSI) that will support the delivery of cross-border digital public services.[12]
EEA	The Enterprise Ethereum Alliance (EEA) is a member-driven standards organization whose charter is to develop open blockchain specifications that drive harmonization and interoperability for businesses and consumers worldwide.[13]
GS1	GS1 develops and maintains global standards for business communications. The best known of these standards is the barcode.[14]
IEEE	The Institute of Electrical and Electronics Engineers (IEEE) has created a blockchain initiative to mature the technology.[15]
ISO	The International Organization for Standardization (ISO) is facilitating a global collaboration to create standardization of blockchain technologies and distributed ledger technologies.[16]
MOBI	The Mobility Open Blockchain Initiative, also known as MOBI, is a non-profit consortium funded by its members and created to define open standards for the automotive industry to develop and adopt blockchain at scale.[17]

- **Data standardization**: In many blockchain platforms, the value lies in the exchange of validated data among participants in the ecosystem. As a result, the trustworthiness of the records in a blockchain platform depends on the trustworthiness of the participants. For participants to share information, all data must follow a form of data standardization to ensure it can be understood by all parties. Consequently, every blockchain ecosystem necessarily standardizes the data representation of its entities (contracts, parties, etc.). When we want to make blockchain platforms interoperable, different standards may collide with missing attributes, for example.
- **Legal framework**: It can be difficult to ascertain who "owns" the network and its data due to the decentralized characteristics of blockchain platforms, which makes it hard to place who is legally responsible for it. In a decentralized environment, it may be challenging to know who has processed what data, where and when, and thus to ascertain who is "responsible" for it, what jurisdiction applies in disputes or who controls the information and is liable for its security or responsible for its integrity. Moreover, blockchain ledgers are generally append-only and cannot be changed after the fact, which can raise issues in a number of regulatory spheres, such as data privacy or consumer protection.[18]

These challenges are only further complicated in the context of interoperability, as it is now two or multiple blockchain platforms that are in question.

– **Commercial**: The commercial model will be critical for success. If a bank initially takes two hours to conduct KYC and, based on that record, a second bank can then open an account for the same customer in a few minutes, the second would have to pay the first bank back, otherwise the first bank would never contribute the KYC record.

However, commercial models will inevitably be different in different blockchain ecosystems. Making blockchains interoperable could introduce arbitrage opportunities, for example. This may not be bad, but some participants might not like it.

Platform layer

For two blockchain platforms to be interoperable, it must be considered whether their platform layers are technically compatible, while keeping the following in mind:

– **Consensus mechanism**: Different consensus mechanisms that are inherently different (e.g. proof-of-work (PoW), proof-of-stake (PoS) and Raft) are not interoperable by default. Blockchain platforms that use the same consensus mechanism can be interoperable. However, even if two platforms use the same consensus mechanism, it can be difficult to synchronize data across platforms with consensus about the order of those data transactions. For example, Hyperledger Fabric and Corda may both use Raft as the consensus mechanism, but they use different models for how data is stored, how it persists and who participates in the consensus.

– **Smart contracts**: Different blockchain platforms may use different languages for smart contracts, from Turing incomplete Bitcoin script to Turing complete Java code with legal proses. As a result, sharing codified logics for automated contract executions is usually infeasible across heterogeneous blockchain platforms.

– **Authentication and authorization**: Blockchains can support multisignature transactions, allowing multiple participants to digitally sign on the same transaction. Yet this is designed differently across blockchain platforms. For instance, Hyperledger generally allows signing at user level while Corda does so at node level. The authentication and authorization are hence not interoperable across some blockchains despite their similar consensus mechanisms. Consequently, interoperability methods must rely on cross-authentication mechanisms. These mechanisms could range from simple storage of encrypted passwords to an overlaying user authentication on top of the blockchain platforms.

Infrastructure layer

The infrastructure layer deals with sets of components, enabling the services of the blockchain platform; these typically include, without being limited to: compute, storage, network and virtualization. While the interoperability challenge generally lies in having compatible infrastructures, it is often complicated due to propriety components offered by cloud providers.

– **Hybrid cloud**: Theoretically, an ecosystem can deploy a blockchain platform on hybrid infrastructures, because blockchain is a distributed system. For public blockchains, machines – from home computers to large server farms with hypercomputing power (HPC) – can become a data node and participate in a blockchain ecosystem. However, these networks are usually not sufficiently high performing for enterprise-grade solutions, and their lack of governance models creates vulnerabilities, which can be exploited for, for example, money laundering and breach of currency controls, etc. These challenges are exacerbated when attempting to make two solutions interoperable. Therefore, most enterprises opt out of hybrid clouds for their blockchain infrastructures.

– **Managed blockchains (BaaS)**: for managed blockchain as a service (BaaS) solutions, the challenge lies in the hidden control cloud providers have over the solution, limiting the options for interoperability. While most cloud providers claim that the blockchain services they are offering are open-sourced, there are always some components in the services that are propriety based. This implies a certain dependency on the vendor for part of the blockchain architecture. It could be an orderer hosted centrally by the cloud provider, a membership onboarding tool, a special access management method or an innovative security-management design.

– **Proprietary components in private blockchains**: Private blockchains are always permissioned and differ greatly from public blockchains – especially in terms of infrastructure requirements. They are not demanding on computing power and electricity consumption and can achieve high performance in transaction processing. As a result, they can be deployed in traditional data centres or, more often, on virtual private clouds. Blockchain data nodes deployed in different geographical locations on different network segments can effectively exchange data through the internet, especially because network latency or intermittent disruptions will not affect eventual data consistency. The interoperability challenge for private blockchains lies in finding private blockchains that have sufficiently similar characteristics.

3. Interoperability approaches

Three approaches unique to blockchain interoperability exist. Each approach comes with pros and cons, and their usability depends on the types of systems between which one wishes to achieve interoperability; this requires organizations to be aware of all three approaches before choosing one.

Figure 8: Three approaches to blockchain interoperability

Approach 1: Cross-authentication

Three technical methods for interoperability exist within the cross-authentication approach:

Pros: Only approach that can enable blockchain interoperability without using a central trusted party (notary schemes not included).

Cons: Only relays and notary schemes support the arbitrary data exchange type of interoperability, typically needed for more advanced use cases within a supply chain. Also, relays in particular are yet to see widespread adoption for enterprise use.

Notary schemes: Executed by trusted parties (notaries) that help participants on blockchain A confirm that some event occurred on blockchain B and vice versa. The notaries will come to agreement through some form of consensus algorithm and will then issue a signature that can be used to finalize a transaction on chain A, conditional on this consensus.

Notary schemes are one of the simplest ways to achieve the full suite of cross-chain interoperability. However, they centralize trust, which goes against the main paradigm of blockchain, namely decentralization. This consequence might be acceptable in situations where blockchain consortia members can agree on a central party to operate the notary scheme. Ultimately, if the use case relies solely on the immutability of the distributed ledger and does not need to replace institutional trust in a central party with a systemic trust through decentralization, a notary scheme should be considered as a viable option. Multiple enterprise use cases on permissioned networks would fall in this category.

Relays: Systems inside one blockchain platform that can validate and read events and/or states in other blockchain platforms. More specifically, a relay is a contract on blockchain platform A that functions as a light client of blockchain platform B, using blockchain platform B's standard verification procedure to verify block headers fed into the contract. This gives blockchain platform A the capacity to understand event changes on blockchain platform B, without using a trusted party. As the relay would allow a secure message to pass between the two blockchain platforms in question, it can allow each blockchain platform to execute transactions on its own state machine using the synthetic versions of assets from the other blockchain platform.

The downside is that it is very difficult to connect blockchain platforms that don't have the desired or similar characteristics. For relays to work best, the blockchain platforms should share certain characteristics, including flexible multisignature capability and fast consensus finality.

Hash-locking: Setting up operations on blockchain platform A and blockchain platform A that have the same trigger, usually the revelation of the preimage of a particular hash. This is the most practical technical method to interoperability in cross-authentication but is also the most limiting in terms of functionality, supporting only digital asset exchange.

Two general types of hash-locking exist: on-chain hashed time-lock contracts (HTLC) and off-chain hashed time-lock agreements (HTLA). An HTLC is on-chain and is a class of blockchain-based payment that uses hash locks and time locks to require the receiver of a payment to either acknowledge receipt prior to a deadline or forfeit the ability to claim the payment, returning it to the payer. HTLCs allow for cross-chain atomic swaps and fully funded bidirectional payment channels between assets on certain types of blockchain platforms. An alternative solution is HTLA over a peer-to-peer network that is used for cryptocurrency payments across different blockchain platforms. Unlike HTLCs, this solution is not built as a smart contract on the blockchain platform but an off-chain solution. Hence, it does not provide the same inbuilt decentralized characteristic as HTLC.

Overview of industry solutions in cross-authentication

Several companies have released interoperability solutions that are at varying levels of maturity. These have been mapped according to the technical methods presented above. Most solutions focus on digital asset exchange and thus offer limited functionality for arbitrary data exchange. The relay method is most popular among start-ups, while enterprise solutions have focused on hash-locking.

Figure 9: Interoperability solutions released by multiple companies and mapped out according to the three technical methods presented above

Notary schemes	Relay		Hashed time-lock contract
Multisignature Liquid by blockstream	Quant AION ICON ARK BLOCKNET Polkadot	Wanchain POA Cosmos Block Collider Metronome	**Contracts on-chain** BTC Relay Bitcoin Lightning network **Agreements off-chain** Interledger Hyperledger Quilt R3 Corda Settler

Approach 2: API Gateway

An application programming interface (API) is a piece of code that governs the access point to a server and the rules developers must follow to interact with a database, library, software tool or programming language.

Pros: Tried and tested technology – easy to implement.

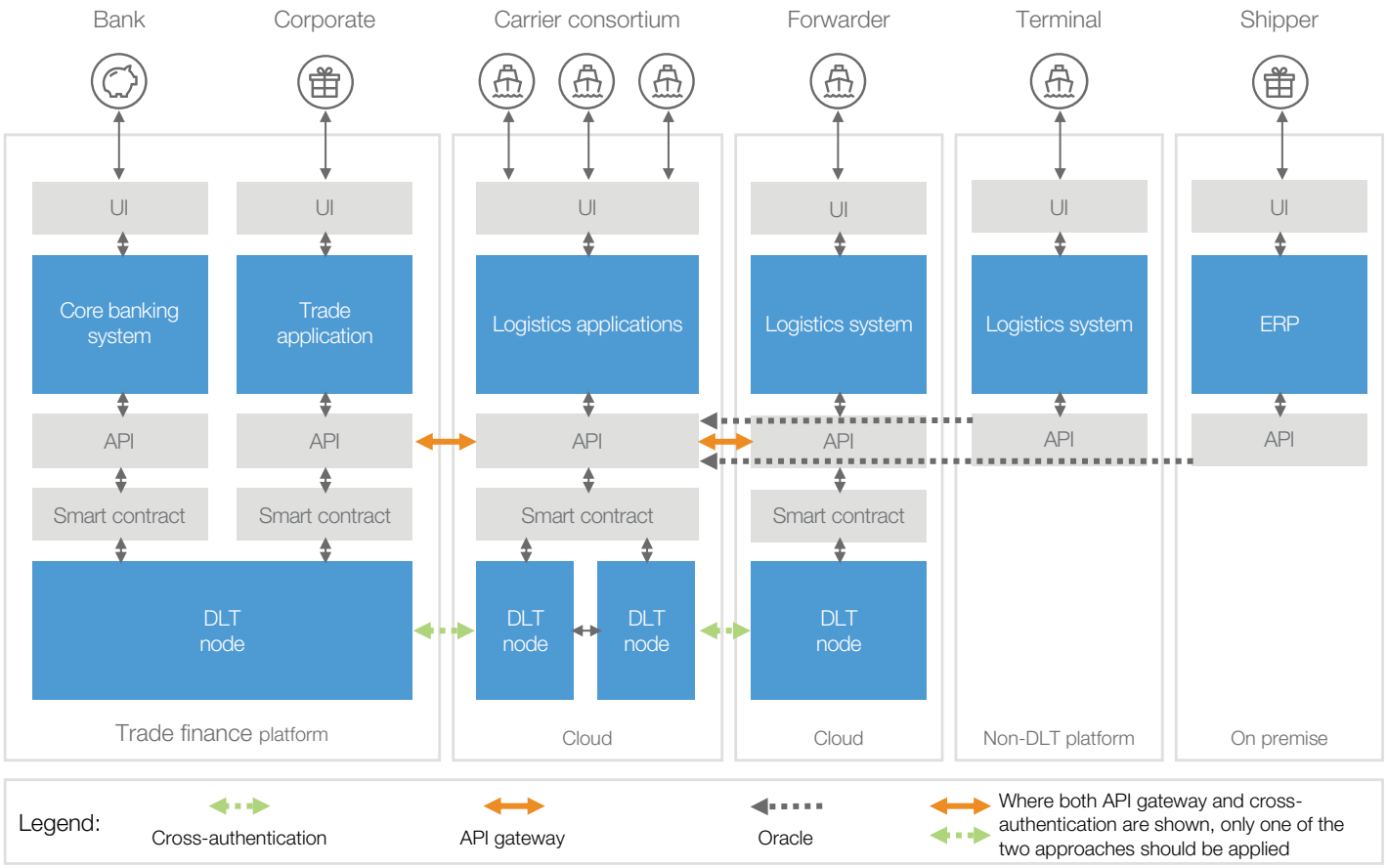
Cons: May not guarantee eventual data consistency and centralizes trust to whoever operates the APIs.

An API gateway organizes several APIs. It is the conductor that organizes the requests being processed by the underlying architecture to simplify the experience for the user or the process of requesting for a client. It is a translator, taking a client's many requests and turning them into just one, to reduce the number of round trips between the client and application.

Given the challenges introduced in the cross-authentication approach, interoperability solutions are hard to achieve through smart contracts in relay and hash-lock solutions. Also, given the challenges introduced in the platform layer, few blockchain platforms are fit for interoperability solutions. Therefore, organizations may opt to use an API approach, where APIs are used in an additional external layer on top of the blockchain platform. Yet, the challenge here can be that the APIs tend to be drastically different, not sufficiently high level and speak the language of the underlying blockchain not the language of the business.

Another problem when using the API approach is that it may not be able to guarantee eventual data consistency across the two blockchain platforms, meaning that it may not be possible to guarantee that no new updates are made to a given data item. Moreover, it centralizes trust to whoever operates the APIs.

Figure 10: Overview of an API interoperability solution. There is a tendency for blockchain platform integrations to use an external API layer for data exchange and event-triggered logic execution as opposed to using a smart contract (see Approach 1: cross-authentication)



Approach 3: Oracles

An oracle is an agent that enables the transfer of external data to the blockchain for on-chain use. This is done using smart contracts that add information about real-world events to the blockchain. Simple examples of data that are useful to import include temperatures, prices or information about flight delays. Once entered on the blockchain, this data can be used to automate processes based on real-world events (e.g. if a train is delayed, an insurance contract automatically and autonomously delivers the indemnification).

Technically speaking, oracles are no different from other smart contracts. However, in order to be useful, oracles need to be trusted, either because they are operated by a trusted third party or thanks to cryptographic attestations.

Pros: Proven and easy-to-implement systems. Oracles provide a data feed about external events.

Cons: Do not create actual blockchain-to-blockchain interoperability; they make blockchains interoperable only with non-blockchain systems. Applications are only as reliable and trusted as their oracles are.

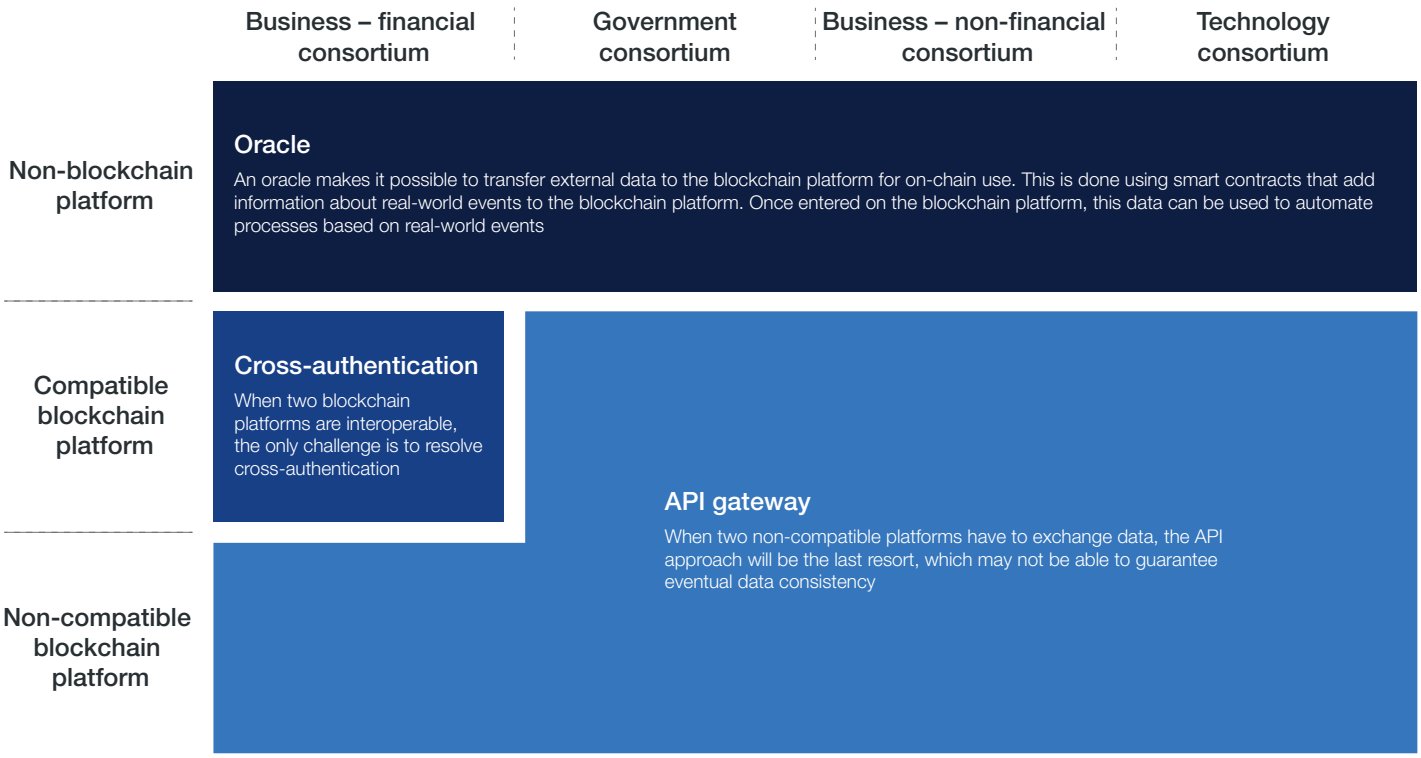
4. Picking the right approach

When organizations need to decide on an interoperability approach to go by, they need to understand two dimensions. First, they need to understand the business context they are coming from, which can be split into four types of consortia. Second, they need to understand the system they wish to become interoperable with, split into three types. To understand this system, organizations should use the three layers in the blockchain interoperability model to understand whether the system is a compatible blockchain, a non-compatible blockchain or a non-blockchain platform. When this is clear, organizations should now know which of the three interoperability approaches to pick.

If, for instance, an organization is trying to make a blockchain platform solely dealing with financial transactions (digital asset exchange) and wishes to become interoperable with a blockchain platform, which through analysis of the three layers in the blockchain interoperability model turns out to be fundamentally different (non-compatible blockchain platform), then the right approach will be the API gateway approach.

To assist organizations in making decisions in interoperability approaches, the following introduces three types of systems to connect to, and four types of consortia as the business context for interoperability needs:[19]

Figure 11: Four context-dependent approaches to blockchain interoperability



Types of systems

The following three types of systems exist:

- **Non-blockchain platform**: Systems that do not use blockchain technologies and therefore have inherently different infrastructure set-ups from blockchain platforms.
- **Compatible blockchain platform**: Blockchain platforms that are technically compatible for all three interoperability layers.
- **Non-compatible blockchain platform**: Blockchain platforms that share some features with the blockchain platform in question but without sufficiently similar characteristics when analysed using the three interoperability layers.

Types of consortium

The following four types of consortia exist:

- **Business – financial consortium**: Focusing primarily on digital asset exchanges, which may limit the need for arbitrary data exchanges.
- **Government-driven**: Contexts where government bodies need to control the blockchain platform in question, which puts additional requirements for all layers of interoperability, limiting the options for interoperability choices. This type of consortium may have the need for both digital asset exchange and arbitrary data exchange.
- **Business – non-financial consortium**: Typically has the need to exchange arbitrary data for more advanced use cases. This category often includes supply chain consortia.
- **Technology consortium**: These are also providers of the technologies enabling blockchain platforms. Therefore, they are rarely technically compatible with blockchain platforms from other consortia regardless of the required data exchanged.

5. Current state of interoperability solutions

Landscape for blockchain-to-blockchain solutions

The interoperability landscape for blockchain-to-blockchain solutions remains immature for enterprise use. Most solutions focus on Bitcoin and Ethereum, and little activity has been observed on the permissioned blockchain platforms. Moreover, the interoperability challenges stemming from the business-model layer discussed above mean it is a challenge that is difficult for technology providers to solve alone.

In terms of the three technical methods in the cross-authentication approach, some working solutions do exist, but enterprise adoption remains limited. Notary schemes have seen limited use and have so far been observed only for crypto exchange settlement. The hashed time-lock agreements (especially for token swaps) used between permissionless blockchains such as Ethereum and Bitcoin have been used for interoperability between the Corda and Ripple ledgers. Relays have thus far been used only for permissionless blockchain platforms and none has succeeded in creating interoperability for blockchain platforms other than Bitcoin and Ethereum.

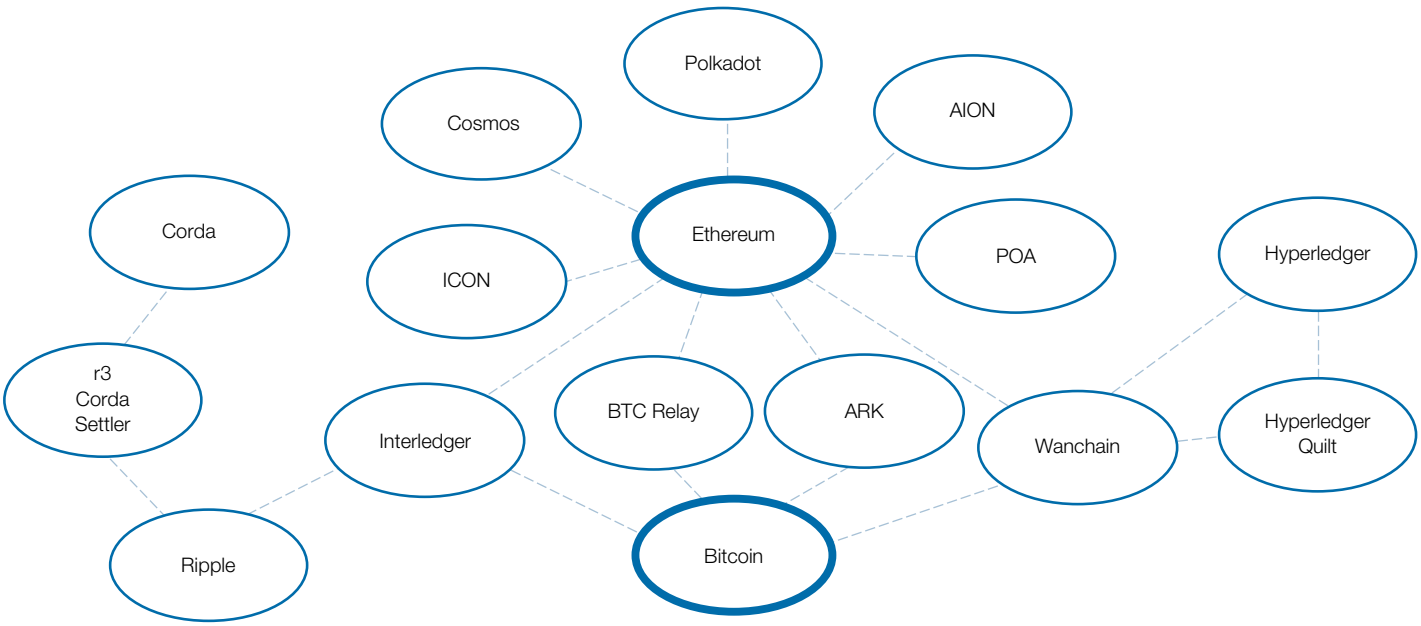
Hedera Hashgraph recently announced the Hedera Consensus Service, which appears promising for blockchain-to-blockchain interoperability and details how a global, fault-tolerant and cost-effective ordering service can be made available to any Hyperledger Fabric network built today.[20]

In short, there is demand for a distributed and fast way to reach consensus without centralizing the consensus process and, while widespread adoption is yet to take off, a number of actors are working on making it a reality.

Landscape for API solutions

API is a technology type already seeing widespread use and is used both for blockchain-to-blockchain interoperability and for interoperability solutions between "regular applications" and blockchain platforms. Hence, API solutions generally have a high degree of maturity and are easy to implement for blockchain-to-blockchain interoperability, compared to cross-authentication. However, solutions are, in some cases, still relatively immature and come with the loss of decentralization along with other challenges, which are further addressed in the section on API gateways.

Figure 12: Documented interoperability between individual blockchain technologies or interoperability solutions. Parties that claim to be working on establishing interoperability but have not yet presented working solutions are not shown



API solutions are common in the market. All blockchain platforms in the market today have APIs for integration with non-blockchain applications and are working on solutions that allow for interoperability with other blockchain platforms. Though all of the platforms below have announced this functionality, only limited results have been published to prove any maturity. This indicates that blockchain platforms are generally aware of the interoperability need but are still in an immature state.

Figure 13: Example of three platforms and their APIs used for legacy integration

Blockchain	Ethereum	Hyperledger	Corda
Blockchain to non-blockchain	JSON.RPC API	Hyperledger Composer API	JSON API
Blockchain to Blockchain	Open standards-based framework	Hyperledger Quilt	Corda Settler

None of the large technology vendors supporting blockchain has launched interoperability solutions except for Microsoft, which is currently working on a project with Nasdaq to create a ledger-agnostic solution.

Figure 14: Overview of large technology vendors' support for blockchain interoperability

Vendor	Supported blockchains	Interoperability with non-blockchain	Interoperability with other blockchain
IBM	Hyperledger Fabric	IBM® MQ for z/OS® for hybrid cloud transformation	Mentions smart contracts and relies on the partnership between Hyperledger and EEA. Expect a "mashup" application to solve the isolated networks, giving organizations one consistent API covering all networks. Also claims interoperability can be met through vendor offerings. Partially uses GS1 standards. The adoption of the Hedera Consensus Service could be a viable path towards interoperability with other blockchains.
Microsoft	Hyperledger Fabric, Corda, Ethereum and more	Azure Blockchain Workbench REST API	Is working with Nasdaq to create a ledger-agnostic solution for the Nasdaq Financial Framework, enabling Nasdaq customers to use different blockchains through one common interface. Intends to use GS1 standards.[21]
SAP	Hyperledger Fabric, MultiChain and Quorum	Integrates SAP solutions to blockchains via a SAP cloud service and a blockchain adapter	SAP is constantly evaluating which protocols to support, based on customer needs. For example, SAP has developed interoperability with R3 Corda to demonstrate real-time gross settlement in banks for central bankers. In addition, in order to achieve interoperability between blockchain protocols and use cases, SAP is working on standardization on the technical layer, such as the Token-Taxonomy-Framework and semantical standardizations like GS1.
ORACLE	Hyperledger Fabric	Accessible from cloud and on-prem applications via REST APIs and Hyperledger SDKs	Interoperable with non-Oracle versions of Fabric using compatible releases.

6. Interoperability case studies

The following section provides details on how blockchain interoperability has been achieved in two specific cases. The first case applies a combination of elements from the oracle approach and the API gateway approach, as it is achieving interoperability between two blockchain platforms that are non-compatible (Ethereum and Hyperledger Fabric) and a non-blockchain platform (Singapore Exchange). The second case focuses on data typically being supply-chain events. Hence, the primary need is arbitrary data exchange. As the solution is not exclusive to certain blockchain platforms, it is not possible to assure the compatibility of the blockchain platforms in question. However, the solution is well suited to potentially incompatible blockchain platforms and relates to the API gateway approach.

Deloitte[22] connecting Hyperledger Fabric and Ethereum with Singapore Exchange (SGX) and Monetary Authority of Singapore (MAS) via node integration

Deloitte has connected Hyperledger Fabric and Ethereum with Singapore Exchange (SGX) and Monetary Authority of Singapore (MAS), the central bank of Singapore.[23]

The objective was to reduce the turnaround time of the delivery-versus-payment (DvP) process from T+2 to T+0, lower the risk of counterparties and reduce the liquidity required in the ecosystem. The delivery leg – i.e. the transfer of title of the securities – was executed on the permissioned Hyperledger Fabric, while the payment leg using the central bank digital currency named Ubin, each coin backed with one SGD, was running on crypto-enabled Ethereum. Both Fabric and Ethereum are open-sourced and widely adopted, and are most suitable for delivery and payment respectively. The challenge was how to integrate these two blockchain technologies together.

Deloitte used the smart contract (chaincode) of Hyperledger Fabric to trigger payment at the Ethereum network upon the change of title of the securities. The seller first receives a secret from the SGX server to lock the securities on Hyperledger Fabric, which in turn validates the ownership of the securities against the seller. The SGX server then issues another secret to the buyer to lock their payment on Ethereum, and the event-triggered smart contract will exchange these two secrets between seller and buyer simultaneously, so they can unlock and receive the payment and securities respectively. This eliminates the need for intermediates such as custodians, traditionally required to mitigate counterparty risk.

The design requires interoperability between the two most widely adopted permissioned and permissionless blockchain platforms, and Deloitte has proven that they can be tightly integrated through smart contracts. In fact, Ethereum Pantheon Client has already become part of the Hyperledger solution named Besu, supporting several consensus algorithms.

EVRYTHNG connecting multiple chains via API to digitize products

The EVRYTHNG Product Cloud gives products a digital identity. Put simply, it transforms a physical item into a digital object that exists and interacts on the web. A unique product is given a serialized digital identity, or twin, in the cloud, which is linked to an identifier embedded in the smart packaging or smart code. This enables the physical object to be scannable and interactive, and given software intelligence to participate in new applications.

This process helps to resolve supply-chain integrity issues (e.g. backdoor goods, counterfeit goods, parallel imports, etc.) and enables new direct-to-consumer applications triggered by end customers scanning products with their smartphones.

EVRYTHNG offers an API gateway called the Blockchain Integration Hub (decentralized platform). The service enables data about products to be replicated to, or collected from, different blockchains. This data typically consists of events (e.g. supply-chain history, live tracking data, consumer scans, etc.) and metadata about a product to be updated (e.g. temperature, humidity, current owner, etc.).

It is comprised of packaged open-source connectors for each blockchain running EVRYTHNG's rules engine, called Reactor. These custom scripts run securely and at scale for any events sent to the EVRYTHNG Product Cloud, translating these transactions from the EVRYTHNG model (based on the W3C Web of Things model and the GS1 EPCIS, Digital Link and identifiers standards) to the models used by EVRYTHNG's blockchain partners. Transactions are then pushed to the selected blockchain(s) via blockchain nodes hosted by EVRYTHNG, which act as part of the decentralized network of each platform. EVRYTHNG usually manages, secures and scales these nodes for its customers, but they may also choose to operate their own nodes. The script receives back a transaction hash that it stores on the EVRYTHNG Product Cloud. The transaction can now be leveraged by apps using both the EVRYTHNG platform API and the APIs of the blockchain platforms.

While the approach does introduce a centralized component (an API gateway), it allows brands to use a number of the benefits of blockchains in a straightforward manner. In particular, it is used to allow:

- Decentralized data sharing, ensuring that no single actor has full control, as data and rules are shared
- Verifiable and immutable provenance and authenticity events
- Token-based loyalty, where consumer rewards are attached to specific transactions, such as purchasing or recycling

7. Checklist for interoperability requirements

Below is a checklist intended to assist organizations in structuring their efforts to clarify blockchain interoperability requirements. The checklist is structured according to the blockchain interoperability model presented earlier, which splits interoperability into three layers. The checklist may be used to clarify requirements for each of the three layers and brings up questions to consider before engaging in developing a blockchain solution for interoperability purposes.

Business interoperability

- ☐ Which industries and associated data standards do these participants conform to?
- ☐ Do any of these participants participate in an existing blockchain ecosystem and, if so, what data standards are being used?
- ☐ How should participants discover, exchange and make use of relevant distributed data across different ecosystems: e.g. supply chain and trade finance?
- ☐ Does the desirable use case rely on features supported by adjacent ecosystems: e.g. Does the supply-chain use case require payments or trade finance features to be desirable?
- ☐ How can the inherent interoperability risks (exposure of information to distrusted third parties, loss of access to information on secondary chain, etc.) be avoided or mitigated?

Platform interoperability

- ☐ Do any of these participants participate in an existing blockchain ecosystem and if so what blockchain platform are they built on and which consensus mechanism does the ecosystem rely on?
- ☐ Do the blockchain platforms have support for similar multisignature transactions for authentication and authorization: e.g. Does one blockchain platform sign at user level while the other signs at node level?
- ☐ Is it possible to create a cross-authentication mechanism?
- ☐ Assuming a notary-scheme-based interoperability solution, is it a viable option to trust a third party to run a notary scheme to facilitate cross-chain interoperability, or does it run counter to the decentralization agenda being pursued in the first place?
- ☐ Assuming a relay-based interoperability solution, why were the two ecosystems built on distinct blockchain technologies in the first place? Subsequently, how can the participants in the application layers of two different blockchains trust one another given that the first chain uses one consensus mechanism and one governance model that was chosen instead of the alternative consensus mechanism and governance model employed by the second chain?
- ☐ Is it possible to create an API gateway?

Infrastructure interoperability

- ☐ Will the use case expose the solution owner to regional legal constraints with regards to e.g. data storage location?
- ☐ Does the use case allow the solution owner to deploy your solution on a virtual private cloud?
- ☐ Does the use case allow the solution owner to use blockchain-as-a-service offerings?
- ☐ Is the IT organization mature enough to depart on a journey of hosting nodes, wallets and secure keys, or even to manage tokens?

Glossary

Application programming interface (API)
An application programming interface (API) is a piece of code that governs the access point to a server and the rules developers must follow to interact with a database, library, software tool or programming language.

Consensus mechanism
Consensus mechanisms ensure convergence towards a single, immutable version of the ledger. They enable actors on the network to agree on the content recorded on the blockchain, taking into consideration the fact that some actors can be faulty or malicious. This can be achieved by various means, depending on the specific needs. The most famous consensus algorithms include proof-of-work, proof-of-stake and proof-of-authority.

Hash
A hash is the result of a function that transforms data into a unique, fixed-length digest that cannot be reversed to produce the input. It can be viewed as the digital version of a fingerprint, for any type of data.

Know your customer (KYC)
KYC is the process of a business or a network verifying the identity of its clients and assessing their suitability, along with the potential risks of illegal intentions towards the business relationship.

Node
A node is a computer running specific software that enables that computer to process and communicate pieces of information to other nodes. In blockchains, each node stores a copy of the ledger, and information is relayed from peer node to peer node until transmitted to all nodes in the network.

Raft
Raft is a consensus algorithm designed as an alternative to Paxos (claimed to be easier to understand) and an algorithm for implementing a fault-tolerant distributed system.[24]

Signature
Signing a message or a transaction consists in encrypting data using a pair of asymmetric keys. Asymmetric cryptography enables someone to interchangeably use one key for encrypting and the other key for decrypting. Data is encrypted using the private key and can be decrypted by third-party actors using the public key to verify the message was sent by the holder of the private key.

Smart contract
Smart contracts are pieces of code stored on the blockchain that will self-execute once deployed, thus using the trust and security of the blockchain network. They enable users to automate business logic and therefore enhance or completely redesign business processes and services.

Transaction
Transactions are the most granular pieces of information that can be shared among a blockchain network. They are generated by users and include information such as the value of the transfer, address of the receiver and data payload. Before sending a transaction to the network, a user signs its contents by using a cryptographic private key. By controlling the validity of signatures, nodes can figure out who is the sender of a transaction and ensure that the transaction content has not been manipulated while being transmitted over the network.

Contributors

The World Economic Forum's Centre for the Fourth Industrial Revolution "Redesigning Trust: Blockchain for Supply Chain" project is a global, multi-industry, multistakeholder endeavour aimed at co-designing and co-creating frameworks to encourage inclusive and well-thought-through deployment of blockchain technology. The project engages stakeholders across multiple industries and governments from around the world. This white paper is based on numerous discussions, workshops and research and the combined effort of all involved; the opinions expressed herein may not necessarily correspond with those of every person involved with the project.

Sincere thanks are extended to those who contributed their unique insights to this report. We are also very grateful for the generous commitment and support of Deloitte and their fellow at the Centre dedicated to the project.

Lead authors

Linda Pawczuk, Global Consulting Blockchain and Digital Assets Leader, Deloitte, USA
Jesper Mathias Nielsen, Manager, Deloitte, Denmark
Paul Kwan Hang Sin, Consulting Partner, Deloitte, China
Nadia Hewett, Project Lead, Blockchain and Digital Currency, World Economic Forum, USA

Contributors

Abdulhakim Al-Habib, Systems Consultant, Saudi Aramco (and World Economic Forum Fellow), USA
Mikkel Boding Kildetoft, Consultant, Deloitte, Denmark
Shelby Botula, Project Coordinator, World Economic Forum, USA
Sigrid Lucie Effersøe Sømod, Senior Consultant, Deloitte, Denmark
Soichi Furuya, Senior Researcher, Hitachi (and World Economic Forum Fellow), USA
Dominique Guinard, Co-Founder and Chief Technology Officer, EVRYTHNG, Switzerland
Lucy Hakobyan, Head of Program, Mobility Open Blockchain Initiative, USA
Henrik Hvid Jensen, Senior Blockchain Adviser, Trustworks, Denmark
Francis Jee, World Economic Forum Fellow, USA
Yusuke Jin, Senior Researcher, Hitachi, USA
Anastasia Kuskova, Transformation and Sustainability Director, Eurasian Resources Group, The Netherlands
Wolfgang Lehmacher, Supply Chain and Technology Strategist, Independent, Hong Kong
Nakul Lele, Consulting Managing Director, Deloitte, USA
Moritz Petersen, Senior Researcher, Kühne Logistics University, Germany
Dirk Siegel, Partner, Deloitte, Germany
Jason Spasovski, Senior Consultant, Deloitte, Denmark
Sergey Tyan, Strategy Director, Eurasian Resources Group, The Netherlands
Sheila Warren, Head of Blockchain, Digital Currency and Data Policy, World Economic Forum, USA
Rasmus Winther Mølbjerg, Director, Deloitte, Denmark

Endnotes

1. As of March 2020, six white papers in the series have been published:
   - *Inclusive Deployment of Blockchain for Supply Chains: Part 1 – Introduction* (April 2019): https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-for-supply-chains-part-1-introduction.
   - *Inclusive Deployment of Blockchain for Supply Chains: Part 2 – Trustworthy Verification of Digital Identities* (April 2019): https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-for-supply-chains-part-2-trustworthy-verification-of-digital-identities.
   - *Inclusive Deployment of Blockchain for Supply Chains: Part 3 – Public or Private Blockchains – Which One Is Right for You?* (August 2019): https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-for-supply-chains-part-3-public-or-private-blockchains-which-one-is-right-for-you.
   - *Inclusive Deployment of Blockchain for Supply Chains: Part 4 – Protecting Your Data* (September 2019): https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-for-supply-chains-part-4-protecting-your-data.
   - *Inclusive Deployment of Blockchain for Supply Chains: Part 5 – A Framework for Blockchain Cybersecurity* (December 2019): https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-for-supply-chains-part-5-a-framework-for-blockchain-cybersecurity.
   - *Inclusive Deployment of Blockchain for Supply Chains: Case Studies and Learnings from the United Arab Emirates* (January 2020): https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-case-studies-and-learnings-from-the-united-arab-emirates.
2. Contact Nadia.Hewett@weforum.org to learn more about the toolkit and how to get involved.
3. World Economic Forum, *Inclusive Deployment of Blockchain for Supply Chains: Part 1 – Introduction* (April 2019): https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-for-supply-chains-part-1-introduction.
4. ISO, 2020. ISO/CD 23257.2 *Blockchain and Distributed Ledger Technologies – Reference Architecture*. [Online] Available at: https://www.iso.org/standard/75093.html?browse=tc [Accessed 09 01 2020].
5. Deloitte, 2017. *Figure 2: Blockchain in Banking*. [Online] Available at: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/strategy/in-strategy-innovationblockchain-in-banking-noexp.pdf [Accessed 09 01 2020].
6. BIA, 2019. *BIA*. [Online] Available at: https://bialliance.io/ [Accessed 09 01 2020].
7. BiTA, 2019. *BiTA*. [Online] Available at: https://www.bita.studio/standards [Accessed 09 01 2020].
8. BRI, 2018. *BRI*. [Online] Available at: https://www.beltroad-initiative.com/ [Accessed 09 01 2020].
9. BSI, 2019. *BSI*. [Online] Available at: https://www.bsigroup.com/en-MY/About-BSI/Media-Centre/press-releases/2019-press-releases/january-2019/bsi-partners-with-origintrail-to-developblockchain-enabled-solutions/ [Accessed 09 01 2020].
10. CESI, 2019. *CESI*. [Online] Available at: http://www.cc.cesi.cn/english.aspx [Accessed 09 01 2020].
11. DCSA, 2019. *DCSA*. [Online] Available at: https://www.dcsa.org/ [Accessed 09 01 2020].
12. EBP, 2019. *EBP*. [Online] Available at: https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership [Accessed 09 01 2020].
13. EEA, 2019. *EEA*. [Online] Available at: https://entethalliance.org/ [Accessed 09 01 2020].
14. GS1, 2019. *GSI. Blockchain Standards*. [Online] Available at: https://www.gs1.org/standards/blockchain [Accessed 09 01 2020].

15. IEEE, 2019. *IEEE*. [Online] Available at: https://blockchain.ieee.org/ [Accessed 09 01 2020].

16. ISO/TC307, 2019. *ISO*. [Online] Available at: https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0 [Accessed 09 01 2020].

17. MOBI, 2020. *MOBI*. [Online] Available at: https://dlt.mobi/ [Accessed 17 02 2020].

18. EU Blockchain Observatory and Forum, 2019. *www.eublockchainforum.eu*. [Online] Available at: https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf [accessed 09 01 2020].

19. Deloitte, 2019. So, You've Decided to Join a Blockchain Consortium, s.l.: s.n. Available at https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-definingthe-benefits-of-coopetition.pdf [Accessed 04 03 2020].

20. Hedera, 2019. *Hedera: A Public Hashgraph Network & Governing Council*. [Online] Available at: https://www.hedera.com/hh-whitepaper-v2.0-17Sep19.pdf [Accessed 09 01 2020].

21. GS1, 2019. *GS1 Blockchain Standards*. [Online] Available at: https://www.gs1.org/standards/blockchain [Accessed 09 01 2020].

22. Deloitte is a co-author of this report.

23. MAS, D., 2018. *Monetary Authority of Singapore*. [Online] Available at: https://www.mas.gov.sg/news/mediareleases/2018/mas-and-sgx-successfully-leverageblockchain-technology-for-settlement-of-tokenised-assets [Accessed 09 01 2020].

24. Raft, 2019. *The Raft Consensus Algorithm*. [Online] Available at: https://raft.github.io [Accessed February 2020].

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org