The future of blockchain in supply and logistics

Blockchain Interoperability.

Wout Hofman, Erik de Graaf, Andrea d'Auria

TNO – Dutch National Institute of Applied Science

Societal and economic innovations emerge with new technologies like blockchain technology. Several cryptocurrencies and non-fungible tokens (NFTs) representing ownership of digital assets emerge and change our behavior. The technology is also applied by authorities and in supply chains, where it is expected to provide many advantages. Various public and private initiatives are taken to construct so-called blockchain networks or blockchain applications. Blockchain interoperability not only depends on inherent features of the technology, but initiatives also make different design choices that prevent their interoperability. Much research has been done to create interoperability between blockchains at technology level and solutions emerge. The main issue of these different solutions is the capability to share what are called 'assets' between different applications, including identity and authentication aspects. Solutions are under development like gateways and Self Sovereign Identity (SSI), but are not adopted by the market.

When blockchain technology is applied for data sharing in supply and logistics, not only the technology has to be interoperable, but also the data: its meaning (semantics) and action (process). Without addressing these aspects, blockchain interoperability requires additional functionality potentially leading to data loss. In case also design choices lead to different implementations (like all data is only stored off chain and only links are shared on-chain), this requires also changes to IT systems of blockchain users.

This document presents the state of the art of blockchain interoperability and proposes a step forward for organizations to apply blockchain technology in supply and logistics. We present a classification of types of blockchain applications and provide a way by which organizations can experiment with the technology, eventually creating an open and neutral data sharing infrastructure. In our view, blockchain technology can be considered as a component of an IT data sharing infrastructure in supply and logistics.

Table of Contents

1 BLOCKCHAIN

Blockchain is considered a key enabler for implementing data sharing amongst various stakeholders in the public and/or private domain. The basics of blockchains can be found in many publications, see for instance [1]; the most prominent features are given separately. Their applications address several issues like supply chain management and global trade [2] and business to government data sharing [3] [4]. The European Commission (EC) set up the European Blockchain Services Infrastructure (EBSI) to create what can be called a Decentralized Blockchain Internet [1] for non-repudiation, diplomas and credentials, digital identity, and trusted data sharing [5]. The Spanish SIMPLE Project creates a blockchain based infrastructure for supply chain visibility, trusted data sharing, and compliance in Spain [6]. A similar initiative is taken by the Baltic states for creating a distributed index registry of electronic transport (eCMR) documents in the DIGINNO project [7]. TradeLens, TradeTrust, CargoX, and Vinturas are examples of private sector initiatives supporting visibility and sharing of (links to) business documents. These initiatives are all private – or consortium blockchains (i.e. permissioned), meaning that there is some type of governance structure with respect to use of the application [8].

Many cryptocurrencies and Non-Fungible Token (NFT) are public blockchains, meaning that anyone can join and participate (i.e. permissionless). Both cryptocurrencies and NFT can be transferred between participants, where an NFT represents ownership of a (digital) asset and transferring ownership can require payment. Many cryptocurrencies are not (only) used for payment, but like NFT's as investment.

Yet other initiatives strive to create a so-called Decentralized Blockchain Internet, a trusted, fully distributed environment for sharing all kinds of assets. Governance of such a solution should also be fully distributed. The kinds of assets can be any like a cryptocurrency, NFT, or a business document (see 'features'), resulting in all types of distributed applications (or dApps in blockchain terms). These dApps themselves utilize the network and are also distributed via the network. Ethereum is an example of a Decentralized Blockchain Internet with over 600.000 nodes and a power consumption comparable with that of the Netherlands (https://digiconomist.net/ethereum-energy-consumption). Dfinity is another example of an initiative to create such an Internet. These types of solutions have an underlying business model, for instance transaction based with initial costs. Such a business model and data sharing environment is similar to the well-known appstores.

These initiatives will result in different usage of the concept 'asset'. On the one hand, the concept is open (like in the Decentralized Blockchain Internet), whereas dApps are developed that utilize the concept in a particular way and create a privately governed environment separate from the open environment. Furthermore, blockchain is not the only technology for sharing transactions on assets. Organizations will also have their internal IT applications. Thus, supply and logistics dApps must interface with existing IT back-office systems of participating stakeholders and all types of solutions for trusted data sharing [9]. Integration of a dApp with IT systems of individual stakeholders can be based on Application Programming Interfaces (APIs), where that stakeholder also must participate in the distributed ledger application.

BLOCKCHAIN FEATURES

The most prominent features of blockchain technology are **immutability** and **transparency**. Immutability is the feature that once data that is stored it is impossible to change. It provides the proof that for instance a transaction of an asset like a crypto currency took place and provides the proof of ownership of an asset. Immutability is reached by inserting a block to a chain and distributing these new blocks to a potential large number of nodes. Transparency makes all transactions publicly available.

These two features are not always required. Functionality can be implemented making transactions only transparent to a user group. This is a permissioned blockchain: one needs to get permission for using the blockchain. Another method for reducing transparency is called 'channeling': a peer-to-peer channel can be established between any two users. Another function is off chain data storage. An asset can be anything. A crypto currency and NFT are the well-known assets, but these can also be a data set. By storing for instance only a link to a data set on a blockchain and implementing access control to off chain data, a data holder always governs data access. This is called **data sovereignty**.

Another important feature of a blockchain application is **disintermediation** by replacing any relevant stakeholder with a consensus mechanism implemented by so-called **miners**. These miners act as intermediates. It resulted in for instance high energy consumption for crypto currencies like Bitcoin since a majority of miners needs to approve a transaction.

Mining also led to relative long delays before approval of a transaction and storing it in a 'block' (**latency**). Whereas traditional database systems implement a two-phase commit transaction protocol (the so-called ACID rules: Atomicity, Consistency, Isolation, and Durability) that immediately confirms a complete transaction (or aborts it), blockchain based technology introduced a delay since relevant miners need to approve a transaction first. Especially a method like Proof of Work requires a majority of all miners to approve a transaction before a commit can be given (which is also the cause of the high energy consumption). Other mining methods are faster (and require less energy consumption).

Latency not only depends on the mining method, but also the block size. Small blocks require more mining effort, since the same amount of data needs to be included in a blockchain in small blocks, but large blocks require more transactions (more data) to be able to construct a block and insert it to the blockchain.

Another important feature of blockchain technology is what is called '**smart contracts**'. These are software components that are distributed via a blockchain network to all participants and implement agreed functionality. In the Ethereum network for instance, smart contracts are part of the blockchain and due to transparency available to all users. Whenever developers and miners agree on functionality and their implementation by smart contracts, they are available. Smart contracts are not portable between different technologies, they are

BLOCKCHAIN TECHNOLOGY

There are many technologies with blockchain features. Ethereum, Quorum, Hyperledger Fabric, IOTA, and Corda are examples of blockchain technology. There are also protocols like the Baseline Protocol that utilize a public network build with for instance Ethereum.

Each of the technologies has its own specific way of implementing features. For instance, Corda provides a peer-to-peer data sharing network with an underlying notary network providing immutability of for instance data that is shared. Hyperledger Fabric has a mechanism of channeling by which any two users can share data in a peer-to-peer manner.

When designing a blockchain based network, there is always a choice with respect to the **network structure**. We distinguish four types of networks: an open, transparent network, a meshed, peer-to-peer network, a star network with one central component, and a hub-spoke network which is a combination of meshed star networks. The public Ethereum network is for instance an open network. The channeling feature of Hyperledger Fabric can be applied to construct a star network with channels towards a central component. In the same way, this mechanism can be applied to construct a hub-spoke network.

2 DATA SHARING IN SUPPLY AND LOGISTICS

To create an overall view requires a good understanding of data sharing between organizations in general and in supply and logistics in particular. There are all types of cargo to be transported using different modalities. Each supplier or customer has organized its supply chain in a certain manner. This complexity is addressed by for instance the FEDeRATED project (federatedplatforms.eu) and the Digital Transport and Logistics Forum (DTLF). Reducing the complexity to a solution, data sharing is about creating a fully **distributed, immutable database** of business transactions between supply and logistics actors with the following features:

- **Data sovereignty** – each actors manage their own data and – access, compliant with (inter)national regulations.
- **Data at the source (pull)** – data always remains at the source where it has been created. Access to data is shared according to a data classification, where business relations and authorities received links to data (so-called 'Linked Data'). The one that owns the data is known as 'data holder', the one that accesses the data is a 'data user' (see the Data Governance Act).
- **Data semantics** – linked data and data at the source must be processable to a data user. It requires a common, shared semantics for data sharing in supply and logistics. DTLF has defined such a semantic model.
- **Transactions on data** – the links that are shared have a business context. They represent for instance the actual status of a physical activity like transport or ordering that activity. The allowed sequence and the minimal required content of each data transaction need to be specified. Data transactions like 'booking' and 'order' compose a business transaction. For instance, an order will follow a booking confirmation and lists the actual cargo to be transported including times and places.
- **Identity, authentication, and authorization** – the identity and credentials of each actor and an employee acting on behalf of that actor must be authenticated. Credentials are managed by each actor.
- **Data confidentiality** – any two actors that share data have the choice whether this data is transparent or can only accessed by them. Peer-to-peer encryption can provide data confidentiality. There are two levels of data confidentiality, namely that shared data is only accessible to those that share, and it is not transparent who share the data.
- **Reliable transfer** – whenever data is shared between any two actors, these actors should both have the same data representing the state of a physical activity (e.g. transport of a container).
- **Non-repudiation** – an immutable proof that data has been accessed or shared with someone else. Non-repudiation can be implemented by for instance an immutable log and audit trail of all data transactions between actors.

Secure - and reliable transfer and non-repudiation provide the immutability of a distributed database. The other features are required to create a distributed database. Each actor can implement its own database if it implements the features.

All types of **permits and certificates** are part of logistics operations. Not only must goods flows be compliant with (inter)national regulations, but there are also regulations governing capabilities of

individual actors. Goods flows can be inspected by authorities like customs and be blocked (or continued) and they can have a certificate provided by an authority like a certificate of origin. There are also restrictions to goods flows like the transport of bio-hazardous -/waste cargo, and cabotage. These should all be logged and made available to proper authorities. Capabilities of individual actors are represented by permits and certificates of those actors. There are all types of them, for instance on the level of a transport means, its operator (e.g. a driver's license of a truck driver or capabilities of a train operator), equipment, the administration of an actor (e.g. Authorized Economic Operator or AEO), and a license for handling dangerous cargo.

EXAMPLES - ELECTRONIC B/L BLOCKCHAIN NETWORKS

There are various examples of blockchain networks supporting supply and logistics. To illustrate the interoperability, we will present three examples supporting the same functionality, all three in a different way. The examples are about sharing business document data in sea transport, the so-called Bill of Lading (B/L). In short, a B/L is a document used in international trade that can serves as ownership (negotiable BL) and represents the contract of carriage and thereby liability and responsibility of transport of goods. It is used by an exporter to ensure payment of the goods carried and an importer to receive those goods. Cabrera Mosca (section 2, [10]) provides a good analysis of relevant exchanges in such global supply chains via sea.

Blockchain networks supporting an eB/L in global trade are for instance TradeLens [8] [4], Vinturas [11] [12], and TradeTrust (tradetrust.io). Besides supply chain visibility provided by TradeLens in international maritime transport and Vinturas in road transport of finished vehicle in Europa, both solutions provide an option for eB/L. TradeTrust also provides the same option. We will only access this part of the functionality of these solutions. They are implemented as follows:

- TradeLens. The blockchain network of TradeLens is implemented with Hyperledger Fabric. Each participant has a channel with a central TradeLens node. Participants share data via this trusted central node in the network. The actual eB/L data is stored in a central repository, managed by TradeLens. The blockchain network is used to share links to eB/L data, thus providing a recipient access to the data and implementing non-repudiation including a hash for data integrity.
- Vinturas. Vinturas also applies Hyperledger Fabric. However, eB/L data can be stored on the blockchain network, thus serving to share the data and to provide non-repudiation and data integrity. There is no central, trusted node in the network, each participant operates its own node. To ensure data confidentiality, the channel construct is applied. However, since channels cannot be initialized dynamically, one channel is applied for data sharing between all participants with end-to-end encryption over this channel between participants. Non-repudiation, data integrity, and data confidentiality are thus provided to all participants. Participants can view which parties share data, but not the data itself.
- TradeTrust. TradeTrust applies the Baseline Protocol [13] over a public blockchain network like the Ethereum network. The Baseline Protocol is an end-to-end data sharing protocol over a Consensus Controlled State Machine (CCSM), representing a blockchain network. The protocol considers various functions to support data sharing like workflow management and off-chain data storage. TradeTrust applies the Baseline Protocol for peer-to-peer sharing of links to eB/L data as Non-Fungible Tokens (NFT) via Ethereum. It assures data integrity (storing hashes and/or applying Zero Knowledge Proof (ZKP)), data confidentiality (e.g. links to off-chain data are shared or on-chain encrypted data storage), and non-repudiation (logging that a particular NFT is shared between two participants).

BLOCKCHAIN DESIGN CHOICES

When developing a blockchain based application, various design choices must be made. A choice of technology should be based on clearly specified requirements. In general, design choices can be given independent of requirements, they are based on technology features (see 'Blockchain features'). These design choices are:

- On-chain versus off-chain data: a basic choice is what data is stored on a blockchain. Literature shows three basic configurations, namely integrity of data set representing an asset, reference to data set of an asset, potentially also including the ownership of that asset, and all data on-chain (asset and its ownership). An example of the latter is for instance a blockchain based Cadastre.
- Data sovereignty: who has access to the on-chain data. It relates to transparency. Data can be commercial -/ economic sensitivity and prone to cyber-attacks (passive attacks like accessing the data and active attacks like changing or inserting data to adjust the physical flows and goods ownership). Technology provides solutions with for instance a type of channeling (.e.g Hyperledger Fabric and Quorum) or like fully peer-to-peer implementation over a private (Corda) or public, permissionless network (Baseline protocol using the Ethereum network [13].
- Asset specification – this refers to the semantics and structure of the data stored not only on-chain, but also the off-chain data. Most often, private networks and dApps using public, permissionless networks have a proprietary data structure. However, they may also use a data structure specified by an Industry Association, for instance one that represents a business document.
- Transactions or smart contracts – these specify the operations on the assets like the transfer of ownership of an asset like a cryptocurrency. These transactions are implemented as so-called smart contracts.
- Identity – permissionless or permissioned – each blockchain network requires a public/private key pair representing one's identity. These key pairs can be provided to anyone (permissionless) or is governed by a body (permissioned). In a permissionless blockchain, key pairs are difficult to relate to an identity.

3 BLOCKCHAIN INTEROPERABILITY – TWO CHALLENGES

Besides design choices that lead to different implementations of the same functionality, technology features lead to inherent interoperability issues. In supply and logistics, we consider so-called permissioned blockchain networks. Users of the network are known to be trusted. For permissionless networks, interoperability solutions are available, but these might be prone to security attacks.

Differences in design choices made by different blockchain networks can be easily addressed. For instance, if a blockchain network only shares links to data whereas the other shares the data on-chain, the first network one might have a (temporary) data store for off-chain data that can be made available like on-chain data to the other and vice versa. Also differences in data structures, whether they are on-chain or off-chain, can be handled via data transformation functionality. With respect to blockchain interoperability, there are two basic challenges, namely:

- **Latency – ensuring asset transfer** – whenever an asset is transferred between any two users, there is a latency before a transaction is stored on the chain. When these two users are member of two different blockchain networks, the initiating user cannot access whether the asset is stored on the blockchain network of the receiving user.
- **Identification and Authentication of users** – whereas there is a choice between permissioned and permissionless blockchain networks, the assumption is that all blockchain networks applied by organizations will be permissioned. Now, the users and their keys (identities) are not shared between blockchain networks, so mechanisms must be developed by which a user of one chain can access the identity of a user of another chain.

Solutions to these two challenges are still in a research phase, as explained separately. They may require the inclusion of other functionality like Self Sovereign Identities (SSI) combined with Decentralized Identities (DIDs), using wallets. The latter technologies address **identities** and their verifiable credentials, making it feasible to authenticate a user of one blockchain network in any other.

From a practical perspective, blockchain networks where assets like (links to) data sets (e.g. Bills of Lading) are made available to authorities, where these authorities have their permissioned blockchain network, can be deployed. The assumption is that an enterprise pushing data to this trusted public sector environment is sure that the data set is received by the proper authority. Zero Knowledge Proof (ZKP) could provide more details in this respect to an enterprise.

Blockchain networks that are applied for data sharing, i.e. a user of one blockchain network shares data with another user of a different network, can be made interoperable by means of a gateway with so-called atomic swaps implementing the ACID rules. Blockchain networks need to implement such a gateway. Any latency with respect to fulfilling the asset rules, which is currently some 15 minutes for atomic swaps of for instance crypto currencies, does not seem an issue for data sharing. Of course, identity has to be solved and design choices need to be compatible (e.g. data semantics and off chain versus on-chain data storage). Achieving blockchain interoperability for supply and logistics is thus still not yet deployable.

STATE OF THE ART IN BLOCKCHAIN INTEROPERABILITY

Solutions to blockchain interoperability are still in a research phase. We present some research lines hereafter. First, a layering is presented. Secondly the so-called atomic swaps and finally some research on identity.

Layering

The challenges can be approached in a layered manner, like for instance by Jin et al [14]. They distinguish a data -, network -, consensus -, contract -, and application layer that clarifies all functionality of a blockchain network:

- **Data layer** – it consists of 'transactions' composed to a 'block' that can be added to the blockchain. The complete blockchain is stored by all nodes in the network. A transaction is on a so-called asset, which can be anything like a cryptocurrency or information. Assets structured can be standardized; those of cryptocurrencies are simple as they contain a value of a currency. Like said, the block size versus the transaction size and – frequency is of impact to the latency.
- **Network layer** – the protocol between the various nodes of the network to share transactions, blocks, and the blockchain. The challenge here is whether two blockchain networks share blocks of each other.
- **Consensus layer** – the mechanism by which a transaction is included in a block. There are various consensus mechanisms like Proof of Work, Proof of Stake, and Proof of Elapsed Time. The consensus layer applies the network protocol for operating on the data layer. It is part of the latency of a blockchain network.
- **Contract layer** – this layer specifies the structure of the assets and its allowed operations. These operations can be triggered by transactions on the ledger, i.e. a transaction may trigger another transaction. A contract, also known as smart contract, can be real-time updated. It is called 'contract' since its functionality will be used by a (potentially) large number of participants and is stored as a transaction on the ledger.
- **Application layer** – the set of APIs provided to a participant based on the contract layer functionality. This would in fact be a dApp, where Bitcoin could also be considered a dApp.

A proposal is made to create a so-called **Open Asset Protocol** for standardized operations (APIs) on an asset [15]. This protocol specifies how to construct tokens and operations on these tokens that can be applied in smart contracts. In case information is the asset, it can have a complex structure. The structure itself is defined by the contract – and application layer. Those layers specify the operations on the information that composes an asset. A transaction on an asset is the transfer of that asset by one participant to another. There is thus always a single owner of an asset, although the contract layer can also implement operations where one asset can have multiple owners. The blockchain contains all operations on that asset and provides a trace, what is called the ledger.

Atomic Swaps

To address latency between different blockchain networks, a so-called called '**atomic swap**' based on for instance so-called Hashed Time-Lock Contracts (HTLC) can be implemented. This

mechanism is also supported by the **Interledger Protocol** version 4 (ILPv4, [16]). Where atomic swaps with HTLC are unconditional, ILPv4 also supports an end-to-end two-phase commit protocol, thus providing ACID capabilities. It enables assets to be shared from a network with one technology to another network utilizing another technology. The consensus mechanism of each network involved will have to include a transaction based on an atomic swap to a block.

There are some issues with respect to atomic swaps, namely the difference in latency [1], [17]. Operations on assets implemented by smart contracts may lead to changes of an asset, e.g. information that is stored by an asset is updated. The 'state' of an asset is based on its trace of all state transactions that took place and all changes of the asset itself. This type of application will require additional functionality, thus enabling a network to function as a distributed, immutable database. Avrilionis and Hardjono [17] give a proposal for the required functionality. The proposal considers smart contracts to be stateless and representing business logics, an asset representing a Digital Twin of a real-world object, and additional code linked to an asset implementing invariants and pre-/post-conditions. An asset and its related software code are implemented by a Digital Twin Container (DT-Container). Their proposed implementation is by constructing gateways between blockchain networks that implement what is called a Logical Unit of Work (LUW) supported by the ACID rules. They further propose to implement an orchestrator for smart contracts, identity management, and access control.

There are many proposals for implementing atomic swaps. Other solutions are bridges between networks that enable atomic swaps (with or without hash-locks or notary schemes), side-chains, and a ledger-of-ledgers that governs transactions in all other ledgers [10]. There are also prototypes that support these solutions [16], [1].

Identity in permissioned blockchains

Wang [1] does not further discuss the issue of '**identity**' in permissioned networks. As stated, each participant will have a public/secret key pair and has access to public keys of all participants on the same network. These key pairs are provided according to the governance structure of the network (permissioned or permissionless). Each participant can store its key pair in a so-called wallet [18] [19]. These wallets are applied for storing credentials that can be verified. A participant will not have access to public keys of participants of other networks. However, a participant that receives an asset should be able to verify the identity of the sender of that asset, even if they are using different networks. Cabrera Mosca [10] addresses this issue by creating a separate credentials management layer. His proposed solution is based on Self-Sovereign Identities [20] [21]. These allow for so-called attestation [19] over different networks.

4 SUPPLY AND LOGISTICS DAPP'S

In many publications, 'lack of trust' is indicated as an issue in supply and logistics that can be addressed by a blockchain based infrastructure. Let us start with that one. Lack of trust is governed by commercial relationships. In those relationships, enterprises are willing and able to share data. The lack of trust is mainly with unknown trading relations (e.g. will they deliver, will they pay) and third party platform service providers used for data sharing. The lack of trust in unknown trading relations is currently addressed via permits and certifications issued by competent authorities and various intermediates providing services with respect to for instance payment behaviour and creditworthiness of enterprises. A question would be whether disintermediation is applicable to this. A platform provider will be out of business if it misuses data of its customers. Furthermore, such a platform must comply with EU Regulations like GDPR, Cyber-Security Act, Data Governance Act, Data Service Act, and Data Act. In case such a platform is an open blockchain network like Ethereum, there will not be a single stakeholder that is liable for data misuse.

Furthermore, compliance to regulations requires data sharing, although an enterprise is not that willing to share all type of data. There is always the concept of 'goal binding': an authority can only access data of an enterprise according to a legal basis.

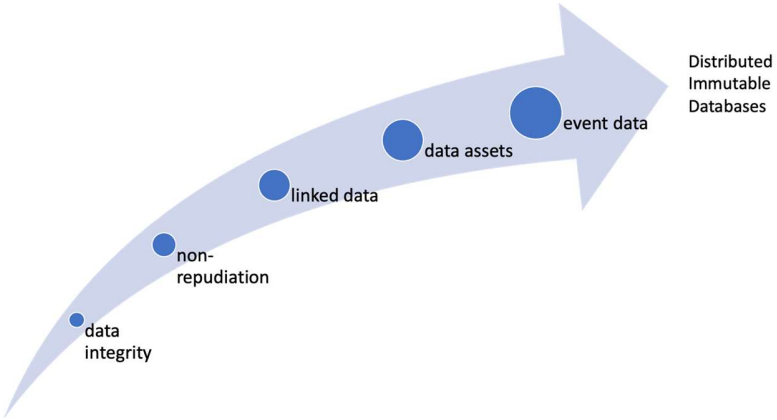


Figure 1: classification of data sharing applications of a blockchain infrastructure

Blockchain technology can be applied to provide functionality in the context of the features. We propose the following classification of potential applications, see also the figure (we introduce the term '**blockchain infrastructure**' as an infrastructure of more than two interoperable blockchain networks):

1. **Data integrity** – a blockchain infrastructure only stores a hash with a unique identification of the data set, e.g. the eB/L of the examples in the beginning of this paper. Potentially, only one blockchain network needs to store the hash accessible to everyone (permissionless, transparent and immutable), so this functionality does not require blockchain interoperability. In this case, a dApp is implemented outside a blockchain network. The data is stored off chain and can be

deleted, thus not available anymore. Solutions like the Interplanetary File System (IFPS) and Arweave try to solve deletion of data and of a hash stored at a blockchain.

2. **Non-repudiation** – the immutability aspect of a blockchain is applied to construct a log and audit trail. A sender and recipient can both use different blockchain networks to store their own log and audit trails, if they both are identical with respect to the data they shared and if they can only access their own log and audit trail. If one does not require transparency, a Zero Knowledge Proof mechanism could be developed. Such a functionality can be provided by an open infrastructure with permissioned users.
3. **Linked data** – the blockchain infrastructure is used to share references to off-chain data, so-called 'linked data'. By including a hash, this application can also support data integrity and non-repudiation. This type of blockchain infrastructure requires **data confidentiality** as part of data sovereignty: a link provided by a sender is only available to one recipient and/or the recipient and sender cannot be detected.
   The link is basically a URI (Uniform Resource Identifier) to a document data set with an indication of its document type. The following requirements need to be met:
   a. **Data semantics**. All blockchain networks in the infrastructure require implementation of the same asset structure by.
   b. **Non-repudiation**. All blockchain network requirements are the same as for non-repudiation.
   c. **Identity, Authentication, Authorisation, and Access Control**. An off-chain data repository needs to implement an attestation process and access control, and the persistency of the link needs to be specified, including archiving requirements of the linked data set.
4. **Data assets** – all data that is shared between a sender and recipient is stored on-chain. An example is the implementation of an eB/L by Vinturas. It could also concern assets representing Digital Twins like a vessel or a product. The same rules apply as before, but in case the data asset can change over time, pre-/post-conditions and invariants must be formulated. This is the type of application that can be supported by the mechanisms identified by [17].
5. **Event data** – the blockchain infrastructure is used to share references to off-chain data (linked data), where the link is complemented with additional data representing real-world activities and Digital Twins. This is about sharing links between Digital Twins, where we will call these links '**event**'. In supply and logistics, this type of application is called **supply chain visibility**. It can be used by a recipient to search applicable data, like a vessel call sign or a truck license plate and an arrival data at a location like a port or terminal. This is the approach taken by FEDeRATED [22] and DTLF (Digital Transport and Logistics Forum, dtlf.eu). The same requirements as the previous applications must be met, where 'event' is considered as Digital Twin asset (meaning pre-/post-conditions and invariants need to be specified for event).
6. **Distributed, immutable database** – this is the ultimate blockchain infrastructure which contains all data that is shared between supply chain stakeholders. Each participant has operations and access rights to (properties of) Digital Twins, including 'events' that provide

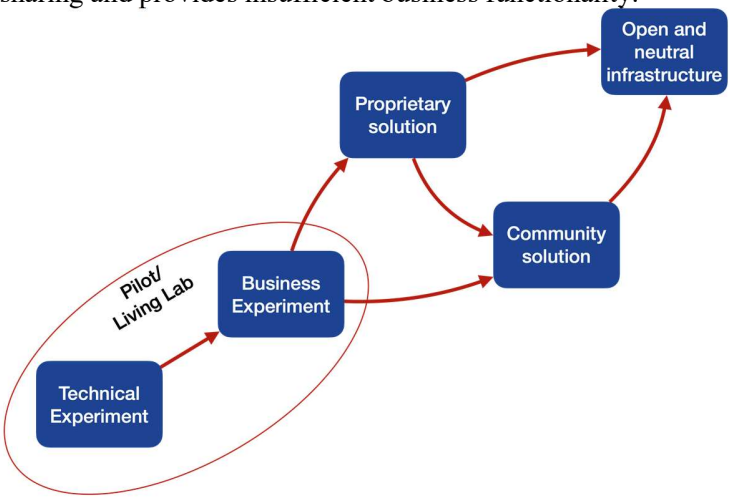
the links between Digital Twins. Consensus mechanisms relate to public and/or private trade legislations like the Incoterms and the eCMR convention. There can be sub-infrastructures of the blockchain infrastructure, where such a sub-infrastructure can consist of various blockchain networks. Each sub-infrastructure can be organized for Digital Twins and their operations like container transport or commodity goods trade and transport. These sub-infrastructures can be interoperable at for instance production level, where commodities and products are combined into new ones. The infrastructure can be seen as a distributed, immutable data base. Semantics of all Digital Twins needs to be agreed upon by all relevant stakeholders.

This application has many advantages, since all relevant stakeholders always have controlled access to the same data set. We have constructed an example of such an application for commodity trade of palm oil. One of the main barriers to such an application is that supply chain stakeholders do not trust such an infrastructure (see before).

One could specify that data integrity and non-repudiation require a common data format that is an asset, including the operations that are allowed on that asset, although the asset is stored off-chain. The off-chain asset can still change over time, e.g. an eB/L data set can change. The linked data solution also requires off-chain assets that can change over time, which requires data integrity and non-repudiation.

5 FROM EXPERIMENT TO INFRASTRUCTURE

Since blockchain technology is a fairly new technology, most enterprises start with a technical exploration of its applicability. Such a technical experiment may evolve into an open and neutral infrastructure, providing all features and selecting functionality like the supply and logistics dApps. Such an infrastructure that could be based on blockchain technology should at least support linked data and at most event data. Support of data integrity and non-repudiation is considered a requirement for data sharing and provides insufficient business functionality.



The various experiments can be organized as a pilot or Living Lab with user involvement. These experiments can result in a proprietary – or a community solution, whereby the latter involves other stakeholders with respect to governance. The various experiments can be described as follows:

- **Technical experiment** – experimenting to assess the functionality provided by the technology. The technical experiment is in fact prototyping the proposed solution by means of a demonstrator. Such a demonstrator can be used for validation in practice [23].
- **Business experiment** – the objective of a business experiment would ideally be involvement of employees requiring business functionality. After a business experiment is completed, two approaches can be taken that will be described hereafter. These approaches are not mutual exclusive.

  The success of a business experiment can be measured in many ways. One would be that a solution fits with business processes and another is realization of a business case. A (multi-stakeholder) business case is expressed by changes in Key Performance Indicators (KPIs) that can be measured at the start and end of the experiment. A business case can also be expressed financial (savings and benefits) and more subjective measures (e.g. improvement of the competitive position). The experiment should also provide an indication whether the business case is positive for all participants, or how to distribute any positive results to stakeholders involved.

- **Proprietary solution** – a proprietary solution for data sharing with first – and potential second tier business partners can be implemented. By making the functionality of the solution publicly available, others will accept it and implement the same solution or use the original one, depending on possibilities of the provider. In this respect, proprietary refers to the governance structure of the solution with a single – or a closed group of owners that make decisions on rights of others with respect to the solution. A single owner is for instance enforcing its suppliers to use a particular solution or a service provider to provide an interface to its customers, for instance for supply chain visibility. A single owner solution acts in fact like a gateway for an enterprise with its environment.
- **Community solution** – creation of a community with the objective of on-boarding all relevant stakeholders. Community solutions can be found in (large) logistics hubs like ports, airports, and inland ports, and in supply and logistics chains involving competitors like the chains for vehicles ('cars') as implemented by Vinturas. A hub functions as a dynamic organizational network with many stakeholders involved.
- **Open and neutral infrastructure** – to develop an open and neutral data sharing solutions with interoperability between all platforms and blockchain networks providing functionality to supply and logistics stakeholders. It is about developing a protocol stack for supply and logistics to support many others in deploying their solutions. A blockchain network can develop its implementation with its own governance structure (community, proprietary). The stack and many different (blockchain) implementations must be available to all stakeholders. It requires an independent governance structure like the one for the Internet and regulation. In our view, such an infrastructure can only be developed by an independent organization, operating internationally with the potential power (or soft measures) for adoption. The EC DG Move has taken the initiative for this infrastructure via an expert group, the Digital Transport and Logistics Forum (DTLF), supported by public funded EU projects. Support of (inter)national supply and logistics (sectorial) perspectives is required for agile, resilient, multimodal supply and logistics chains compliant with regulations.

Whether or not an open and neutral data sharing infrastructure with for instance blockchain technology can be achieved depends on the level of commitment of stakeholders. Participating stakeholders need to commit to the challenge and/or have a positive business case. The challenge can be on various levels, for instance a global or European Union level, e.g. sustainability and geopolitical concerns, or a community level, e.g. improved competition of a hub. In case a challenge does not have a positive business case for all stakeholders hard – and soft measures might be taken like a regulation and financial stimulation.

6 IT IS ALL ABOUT GOVERNANCE

Governance distinguishes the different options to come to deployment. It is about rights: who has the right to make changes, etc. Literature distinguishes three types of rights[1]: (a) **constitutional** rights: who may or may not participate in making collective choices; (b) **collective choice** rights: rights concerning users and components within the information system; and (c) **operational** rights: rights related to access to the information system and to reading and adding data. There are solutions where constitutional rights are by those that paid for development and deployment. These latter stakeholders manage the collective choice rights and thus define how and by whom the solution can be used and further evolve. In case of an open, neutral infrastructure, the constitutional and collective choice rights for the protocol stack can be made by a public body; a blockchain implementation by for instance a community has its own governance structure.

The way forward would be to separate the functionality, i.e. the protocol stack, provided by a blockchain from its implementation. Literature on blockchain has produced a model for governance [24], which is not only applicable to blockchain applications, but also to other types of applications supporting (inter)national trade. The model consists of two dimensions, namely:

- **Mechanism** – the mechanism for implementing the governance. Two types of mechanisms are identified:
  - **Legal code** – these are extrinsic and can be broken. However, a breach of the legal code leads to an action. Compliance to legal code is monitored.
  - **Technical code** – these is intrinsic. The technical code is the implementation of (part of) the protocol stack. In case of a breach of the technical code, an error is detected, and no further action is taken. Standards, software, and smart contracts are examples of technical code.
- **Governance** – the way the mechanism is formulated. Governance can lead to ad hoc private rules, for example those implemented by Bitcoin as technical code. Governance can be either in a private or a public environment.
  - **Private** – rulemaking by the owners or participants of a system with the purpose of safeguarding their private interests
  - **Public** - rulemaking by an outside authority tasked with representing the interests of the public.

The following table lists examples of mechanisms and governance along these two dimensions.

	Legal code	**Standards (Technical code)**
Private	Visa Core Rules Faster Payment Service Rules FOSFA (commodity trading)	Financial Information eXchange (FIX) protocol Bitcoin
Public	European Market Infrastructure Regulation	Internet (TCP/IP) World Wide Web (HTTP/HTML)

[1] Constantinides, P. (2012): Perspectives and implications for the development of information infrastructures. IGI Global. https://doi.org/10.4018/978-1-4666-1622-6.

	BitLicense GDPR (General Data Protection Regulation)	

The Internet and its protocols are an example of public developed technical code. The protocols and a sample implementation have been developed by the US Department of Defense and the World Wide Web by the public organization CERN. Public legal code has been included at a later stage. Bitcoin and other crypto currencies are examples of privately developed technical code, without any legal code (yet).

When deciding on a governance structure, one could either look at the structure of its sector. Is there for instance a body like FOSFA (commodity trading) that could serve as a basis to establish the legal code? Is there a body already focusing on data sharing in your industry like CEFIC for the chemical industry? How is the integration between the legal – and the technical code? How is the technical code documented, implemented, and deployed?

Especially when the technical code is independent of its implementation (i.e. a protocol stack), an open and neutral ledger-based infrastructure can be created. Communities can even deploy their blockchain, as long as they comply with the technical code. One might argue technical code needs to be produced public, since it is cross-sectoral of nature. Collaboration amongst organizations mostly takes a lot of time. Innovation diffusion like blockchain also takes a lot of time. Bitcoin protocols have been developed in 2008 and took more than five years for a take up. These are the timelines for setting up new initiatives. Like said, the issue of interoperability of supply and logistics blockchains also requires more time.

7 TOWARDS A DECISION

The previous pages have provided several ingredients for applying blockchain technology. These all comprise choices that an organization can make. There is always a choice to apply blockchain or conventional technology like so-called 'connector'- or 'integration broker'-based data sharing or a platform of a third-party provider. This choice depends on whether data needs to be stored in a data sharing infrastructure and the capability of that infrastructure to meet the features. For instance data sovereignty supported by access control, Identity, Authentication, and Authorization (IAA), and the capability to share linked event data as a means to provide limited data access.

The following aspects need to be considered:

- Business decision – these are considerations that must be addressed at business level. They are the responsibility of management. It includes aspects like:
    - Sufficient stakeholders involved. This refers to creation of a coalition of the willing, with one or more individuals accepted as a type of leaders/opinion makers that can act as ambassadors. This aspect is rather subjective: it could include most of the market share provided by a limited number of stakeholders, the majority of potential stakeholders involved, or both.
    - Challenges and drivers – these can be external (new regulations, pandemics like Corona, sustainability, digitization stimulation programs of for instance governments, digital product passports for consumers), technology (availability of solutions, standards, and technology), jointly (clear multi-party business case), individually (e.g. Corporate Social Responsibility relating to work conditions and sustainable growth and transport of materials), stakeholders, individual business case). These drivers define the functionality of an application.
    - Legal aspects – this is about considering regulations for applying data sharing, like GDPR, competition laws, any acts like the Data Governance – and Data Act of the EC, specific regulations (private and public applicable to supply and logistics like the Hague-Visby rules, CMR treaty, etc.) and acceptance by authorities in case of scaling.
    - Trust – various aspects should be covered by a solution, for instance data sovereignty, liability, cyber-security, identification and authentication, and non-repudiation.
    - Cost estimation – this is of course part of a business case and will also depend on market assessment. A choice can be to join an existing solution or develop a new one, each will have different costs.
- Market assessment. This needs to provide input for a business decision. Part of it should be performed by IT persons, others by businesspersons. The following aspects are considered:
    - Technology – technology matureness of what are called blockchain protocols. It should also give an indication about the implementation of trust.
    - Available solutions – overview of available solutions addressing drivers and learnings of how these solutions addressed trust.
    - Standards – is there an open standard (or a protocol stack as mentioned for an open and neutral data sharing infrastructure) addressing implemented by an existing solution or a solution based on any other technology. An assessment also needs to be

made with respect to market acceptance of (open or defacto) standards: what do major stakeholders use, who developed such a standard, is there a transparent maintenance body, is it open, etc.?

- Development – this about developing the solution. Still several detailed decisions needs to be made and various aspects need to be clearly considered.
    - Technology choice – a choice of a blockchain protocol used for implementation the selected application
    - Separation of concerns – a solution should only support data sharing functionality that is shared by (preferably) all participants. Any value-added functionality, like (predictive) data analytics of for instance asset maintenance utilizing the solution can be developed by a one or more participants. This should all be in line with competition regulations.
    - Implementation of trust – mechanisms for implementing trust issues identified before.
    - Network – creation of a new or use of an existing blockchain network of nodes.
    - Smart contract development – development of software code to support the application, based on the separation of concerns.
    - Mining structure – development or use of a mining mechanism provided by the technology or an underlying network.
    - Governance structure – clear procedures and conflict resolution mechanisms with roles and responsibilities addressing the following aspects (amongst others):
        - Scalability and extendibility – inclusion of new participants as users and/or node operators/miners. In this context, trust in terms of identification and authentication needs to be addressed (permissioned versus permissionless network, linked to for instance existing (federated) identity providers).
        - Openness - integration with other solutions where these solutions have their own governance structure. Openness is improved by applying standards.
- Implementation and deployment – this is about operation, maintenance and evolution of the solution with new functionality. Implementation can be in phases:
    - Piloting – start with a limited group of participants, using for instance a stand alone solution (no integration with existing IT systems yet). The objective is to validate and improve the solution.
    - Migration – participants integrate the solution with their existing business processes and IT solutions.
    - Roll out – implementation of the solution by all participants.

Considering all these aspects, especially SMEs in supply and logistics will never develop their own blockchain solution. They lack the knowledge and funding. Consortium building is required, driven by for instance industry or the necessity to implement a regulation. Although its solution is not yet fully mature, we recommend to start developing a solution sharing event data via a blockchain in a peer-to-peer manner with reference to off-chain data, based on the common semantics developed by the FEDeRATED project and adopted by the DTLF.

8 CONCLUDING REMARKS

This white paper addresses blockchain interoperability in the context of supply and logistics and proposes different ways to deploy the technology, within the context of a **challenge** or **driver**. Supply chain visibility and predictability or a regulation can be such a challenge for individual business stakeholders; sustainability with reduction of transport movements based on improved capacity utilization can be a challenge from an EU perspective. A challenge results in a **governance** structure, either with only technology or also supported by private or public regulations.

In terms of functionality, blockchain can either support data sharing by storing a hash on chain (data integrity) or acting as log and audit trail (non-repudiation), or can actually be applied to share the data on-chain or links to off-chain data. In the latter case, features like data sovereignty and security need to be implemented, depending on stakeholder requirements. **Generic features** can be considered to construct interoperable blockchain applications, whereas it is also shown that an infrastructure based on **interoperable blockchain networks** must address two features: latency due to for instance mining and identity in permissioned blockchain networks. Mainly those blockchain networks can be constructed that store assets like hashes (data integrity) and are not used to transfer assets between users can be applied without any restrictions. Thus, **data integrity** and **non-repudiation** can easily be implemented. Others, where assets are transferred between users of different blockchain network, are not yet considered feasible for operational deployment and required further technical (and business) experiments.

There are also **public blockchain networks** available to deploy any application, for instance the Ethereum network. A peer-to-peer protocol like the Baseline protocol can be applied over Ethereum, where Ethereum provides data integrity and non-repudiation. The Ethereum network is however still too expensive to share (links to) data sets like electronic documents. The reason is that each transaction over the network requires Ether, the crypto currency used for mining. Others like Dfinity operate as a type of Appstore with probably a similar business model. This may reduce transactions costs compared to those of for instance Ethereum. The question there is: what do they disintermediate?

Adoption of these various solutions still needs further research. We assume that the last type of application in a blockchain infrastructure where all data is stored and shared via an infrastructure will not (yet) be adopted by stakeholders. Stakeholders still require control over their data in their environment and not in a public infrastructure. Instead, stakeholders will choose a particular cloud provider for off-chain data storage, based on their own data semantics and structure. Stakeholders might agree on adopting blockchain for data integrity and non-repudiation, whilst they are still in full control of their data (data sovereignty). Furthermore, visibility data and sharing complex assets like eB/L data via a blockchain will also be acceptable to them in a blockchain network, where they can be in control (governance with the operational choice – and operational rights). Deployment of Self-Sovereign Identities is also to be expected to take time, since identities can be verified by public infrastructures and are maintained in wallets interfacing with issuers of credentials.

We are still in the **early stages** for developing blockchain based infrastructures, although different operational applications are already deployed. The technology still must evolve to support meaningful dApps to private and public sector organizations that are fully interoperable. Organizations can still experiment with the technology, but they must be aware that future alignment is required at dApp level to realize interoperability, assuming that interoperability at technical level will be achieved. In case any participants in an ecosystem are not able or willing to implement a participant node, they can easily integrate via the APIs of a blockchain network. Such a network needs to implement an API gateway to be able to perform the proper routing in the network and from the network to a participant using the API.

9 RECOMMENDATIONS

It seems that blockchain technology is not yet mature enough for deployment by organizations. This is certainly true for creation of a blockchain infrastructure consisting of interoperable blockchain networks. However, one can already start: we recommend developing a solution sharing event data via a blockchain in a peer-to-peer manner with reference to off-chain data, based on the common semantics developed by the FEDeRATED project and adopted by the DTLF. This approach is stable enough for further implementation.

More general, we recommend the separation of technology into a protocol stack as defined by [25] and its software implementation: a **protocol stack** can be implemented by many blockchain networks (and conventional data sharing solutions) that have their own (private) governance structure and can be made interoperable. Public governance and regulation can be given for the protocol stack.

ACKNOWLEDGMENTS

The content is made possible by the SPARK! Living Lab project granted by the Dutch Topsector Logistics, the H2020 PROFILE Project (grant agreement No 786748), the CEF FEDeRATED Action, and the technical support provided on behalf of EC DG Move to the Digital Transport and Logistics Forum.

REFERENCES

[1] G. Wang, "SoK: Exploring Blockchains Interoperability," IACR Cryptology ePrint Archive, 2021. [Online]. Available: https://eprint.iacr.org/2021/537.prdf. [Accessed January 2022].

[2] Y. Chang, E. Iakovou and W. Shi, "Blockchain in Global Supply Chains and cross border trade: a critical synthesis of the state-of-the-art, challenges and opportunities," *International Journal of Production Research, Volume 58 - issue 7,* pp. 2082-2099, 2020.

[3] S. van Engelenburg, Designing context-aware architectures for business-to-government information sharing, Delft: https://doi.org/10.4233/uuid:d25fd4fd-02d7-4811-b675-615badbb3c05, 2019.

[4] L. Segers, J. Ubacht, B. Rukanove and Y. Tan, "The use of a blockchain-based smat import declaration to reduce the need for manual cross-validation by customs authorities," in *ACM Int. Conf. Proceedings, 196-203*, 2019.

[5] European Commission, "European Blockchain Services Infrastruture," [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure. [Accessed 4 January 2022].

[6] Puerto del Estado, "FEDeRATED network of platforms - Living Labs," December 2021. [Online]. Available: http://www.federatedplatforms.eu/index.php/living-labs. [Accessed 4 January 2022].

[7] DIGINNO Project for digital collaboration in the Baltic Sea Region, "DIGINNO-Proto," 2020. [Online]. Available: https://www.diginnobsr.eu/diginno-proto. [Accessed 4 January 2022].

[8] S. van Engelenburg, B. Rukanova, W. Hofman, J. Ubacht and Y.-h. J. M. Tan, "Aligning stakeholder interests, governance requirements and blockchain design in information sharing," in *eGov2020*, online, 2020.

[9] The Digital Transport and Logistics Forum (DTLF), "An outline for a generic concept for an innovative approach to interoperability in supply and logistics chains," Brussels, 2017.

[10] A. Cabrera Mosca, "Connecting Commercial Blockchain Platforms and European Customs: an Interoperable and Self-Sovereign Data Exchange Architecture," TUDelft, Delft, September 2021.

[11] E. Vels, "Digital Blockchain-platform of Vinturas makes spreadsheets obsolete for transport and tracking of vehicles (in Dutch)," September 2021. [Online]. Available: https://innovationorigins.com/nl/digitaal-blockchain-platform-van-vinturas-maakt-spreadsheets-overbodig-bij-vervoeren-en-traceren-van-voertuigen/. [Accessed 5 January 2022].

[12] J. Kuiper, "Blockchain brings visibility to the finished vehicle supply chain," November 2019. [Online]. Available: https://www.ibm.com/blogs/client-voices/blockchain-brings-visibility-to-finished-vehicle-supply-chain/. [Accessed 5 January 2022].

[13] OASIS, "Baseline Protocol: Architecture," 2021. [Online]. Available: https://docs.baseline-protocol.org/baseline-basics/architecture. [Accessed 5 January 2022].

[14] H. Jin, D. Xiaohai and J. Xiao, "Towards a novel architecture for enabling interoperability amongst multiple blockchains," in *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDS)*, Aug. 2018.

[15] X. Li, X. Wu, X. Pei and Z. Yao, "Tokenization: Open Asset Protocol on Blockchain," in *IEEE*, DOI: 10.1109/INFOCT.2019.8711021, 2019.

[16] V. A. Siris, P. Nikander, S. Voulgaris, N. Fotiou, D. Lagutin and G. C. Polyzos, "Interledger Approaches," *IEEE Access,* vol. 7, pp. 89948-89966, 2019.

[17] D. Avrilionis and T. Hardjono, "Towards Blockchain-enabled Open Architectures for Scalable Digital Asset Platforms," 24 October 2021. [Online]. Available: arXiv:2110.12553v1. [Accessed 5 January 2022].

[18] D. Karakostas, A. Kiayias and M. Larangeira, "Account management in Proof of Stake Ledgers," in *Security and Cryptography for Networks*, Amalfi,Italy, September 14-16 2020.

[19] T. Hardjono, "Attestation Infrastructures for Private Wallets," 2021. [Online]. Available: https://arxiv.org/pdf/2102.12473.pdf. [Accessed 5 January 2022].

[20] A. Preukschat and D. Reed, Self-Sovereign Identity: Decentralized digital identity and verifiable credentials, Manning, ISBN 9781617296598, 2021.

[21] M. Sporny, D. Longly and D. Chadwick, "Verifiable Credentials Data Model v1.1," 09 November 2021. [Online]. Available: https://www.w3.org/TR/vc-data-model/. [Accessed 5 January 2022].

[22] FEDeRATED, "Milestone 2 FEDeRATED Interim Master Plan," 15 12 2021. [Online]. Available: http://federatedplatforms.eu/index.php/library/category/2-masterplan.

[23] A. Hevner, S. March, J. Park and S. Ram, "Design Science in information systems research," *MIS Quarterly: Management Information Systems,* pp. 75-105, 2004.

[24] V. Lehdonvirta and R. Ali, "Governance and regulation," in *Distributed Ledger Technology: beyond blockchain technology*, Government Office for Science, UK, 2016, pp. 40-45.

[25] A. S. Tanenbaum, Computer Networks (Third Edition), Prentice Hall, 1996.