MODULE

Interoperability

Overview

Focus Areas

1. Fundamental concepts
2. Top requirements of interoperability
3. Approaches to interoperability
4. Picking the right approach

Tools and Resources

5. Structure blockchain interoperability requirements

Overview

Blockchain technology by its very nature are premised on peer-to-peer interactions around shared distributed ledgers. This makes a transformation from a siloed and fragmented approach to end-to-end value chain integration more attainable, but it also means that the importance of interoperability is imperative.

In the simplest terms, successful interoperability allows the user to trust that "I know what I see is what you see". This module provides tools for dissecting the challenge of making blockchain solutions work seamlessly in that regard, and for choosing the right interoperability approach.

Recommended reading – Inclusive Deployment of Blockchain for Supply Chains Part 6 – A framework for blockchain interoperability[75]

FOCUS AREAS

1. Fundamental concepts

What are the basics of blockchain interoperability, considering the technology's potential, the use cases that have been applied to so far, and characteristics of non-blockchain systems commonly used in the supply-chain industry?

Context

Blockchain technology offers promising results, but overcoming obstacles to widespread adoption remains a challenge, with the technology yet to reach enterprise maturity. Moreover, many existing solutions within supply chain are using blockchain for relatively simple use cases, while realising there are numerous other possible opportunities both within and adjacent to supply chain. Other industries where blockchain could be relevant include finance, food safety, and insurance, among others.

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

Consequently, inter-blockchain communication has become a hot topic to ensure various supply-chain stakeholders are less dependent on sound design choices over technology stacks. In short, this expresses the need for solving the challenge of interoperability – a characteristic that allows a user to trust that "I know what I see is what you see" both within a single system and across systems.

This module will address the challenges of achieving blockchain-to-blockchain interoperability as well as between "regular applications" and blockchains. As the prior is more challenging than the latter, the primary weight of the module is towards addressing blockchain-to-blockchain interoperability. As such, this module on interoperability is one of the more technical of the toolkit, but it will highlight both technical and non-technical requirements for interoperability.

Non-technical readers should take from the module that blockchain interoperability is indeed possible, that it depends just as much on inputs such as governance, compliance, and data standards as it does on technical requirements, and that it is easiest to achieve if you are willing to compromise on decentralisation and speed of technological development.

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

The incentive challenge

Executives regularly ask, "What would incentivise solution 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 prioritise short-term incentives like building something to prove the use case for long-term initiatives like building something that will work with new or existing use cases on other complementing platforms.

Interpretations of interoperability

Put simply, interoperability is: (a) the ability for computer systems to exchange and make use of information and (b) entailing the ability to transfer an asset between two or more systems while keeping state and uniqueness 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 or compromising fairness in the ordering of transactions and accessibility to data. There should also be codification of common rules to the point where compliance becomes a non-issue.

Types of interoperability

Blockchain-to-blockchain interoperability comes in two types, each of which carries considerations distinct from ones that organisations must typically address with traditional, non-distributed systems.

For blockchain, the two types are:

- **Digital asset exchange:** This is the ability to transfer and exchange assets originating from different blockchains without trusted intermediaries such as centralised exchanges. An example for this would be making bitcoin spendable in distributed applications (Dapps) built on Ethereum. Digital assets exchange is the ability to transfer and exchange assets originating from different blockchains without trusted intermediaries such as centralised exchanges. An example for this would be making Bitcoin spendable in Ethereum decentralised applications (Dapp).

Figure 6.1 – Illustration of a digital asset exchange, where a Bitcoin is spent through Dapp

- **Exchanging arbitrary data:** This is the ability to do something on one blockchain that affects another blockchain. What is tracked is not necessarily an item of value but could be an event. 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.

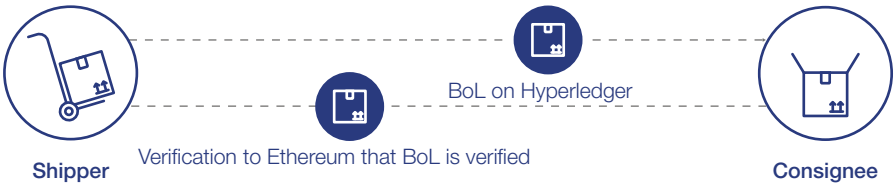

Figure 6.2 – Illustration of how ownership of the Bill of Lading (BoL), which is arbitrary data, can be transferred from a shipper on Ethereum to a consignee on Hyperledger

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

2. Top requirements of interoperability

What are the specific needs of a blockchain solution in terms of governance, data standardisation, and other characteristics for it to successfully operate alongside other systems?

Interoperability is a top concern for decision-makers interested in building blockchain solutions. Organisations 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.

Meanwhile, others may be preoccupied with how to make their existing systems interoperable with blockchain platforms, typically to submit to or use data from a blockchain solution within their existing enterprise applications.

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 is corresponding to typical blockchain architecture[76] [77] and intended for organisations 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.

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

Figure 6.3 – Blockchain interoperability model breaking down the challenges in three layers: business, platform, infrastructure

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

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 frameworks and commercial arrangements; technical feasibility alone cannot enable interoperability.

Governance: To ensure the trustworthiness of the participants, a prudent governance model has to be designed. 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 out of the trust of the first bank. To 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 onto the platform, because they are essentially conducting KYC on behalf of the whole ecosystem.

Data Standardisation: 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 standardisation to ensure it can be understood by all parties.

Table 6.1: Overview of selected organisations with focus on creating standards to drive business model interoperability

Organisation	Focus on creating standards to drive business model interoperability
BIA[78]	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.
BiTA[79]	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.
BRIBA[80]	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 technology.
BSI[81]	The British Standards Institution (BSI), the national standards body of the United Kingdom producing technical standards, is working on blockchain standards for supply chains.
CESI[82]	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.
DCSA[83]	The Digital Container Shipping Association (DCSA) seeks to pave the way for interoperability in the container shipping industry through digitalization and standardization.
EBP[84]	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.
EEA[85]	The Enterprise Ethereum Alliance (EEA) is a member-driven standards organisation whose charter is to develop open blockchain specifications that drive harmonization and interoperability for businesses and consumers worldwide.
GS1[86]	GS1 develops and maintains global standards for business communications. The best known of these standards is the barcode.
IEEE[87]	The Institute of Electrical and Electronics Engineers (IEEE) has created a blockchain initiative to mature the technology.
ISO[88]	The International Organization for Standardization (ISO) is facilitating a global collaboration to create standardization of blockchain technologies and distributed ledger technologies.
MOBI[89]	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.

> *The game is changing for container shipping. Customers are demanding a better experience across many areas, including digitalisation, regulatory complexity, cybersecurity, and environmental impact. To stay competitive, we have to evolve to meet these challenges head-on. 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 paving the way for interoperability in the container shipping industry through digitalization and standardisation.*
>
> **Thomas Bagge,** Chief Executive Officer, Digital Container Shipping Association

Legal Framework: It can be difficult to ascertain who "owns" the network and its data due to the decentralised characteristics of blockchain platforms. In a decentralised environment, it may be challenging to know who has processed what data, where, and when, and 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, like data privacy or consumer protection.[90] These challenges are only further complicated in the context of interoperability, as it is now two or multiple blockchain platforms 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.

Platform Layer

For two blockchain platforms to be interoperable, it must be considered if the platform layers are technically compatible with the following in mind:

Consensus mechanism: Different consensus mechanisms that are inherently different – for example, Proof of Work (PoW) and Proof of Stake (PoS) – 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 synchronise 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, persisted 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 prose. As a result, sharing codified logic for automated contract executions is usually infeasible across heterogeneous blockchain platforms.

Authentication & authorisation: Blockchains can support multi-signature transactions, allowing multiple participants to digitally sign on the same transaction. Yet this is not designed similarly across all blockchain platforms.

For instance, Hyperledger generally allows signing at user level, while Corda does so at node level. The authentication and authorisation 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.

Example

Recent developments in platform layer, on February 13, 2020, Hedera Hashgraph launched Hedera Consensus Service, affording developers an option to create verifiable timestamps and ordering of events for any application.[91] Utilising this solution, developers can build their own application networks, consisting of a set of computers which enable privacy but utilise the trust of Hedera's public ledger as their consensus engine. As the solution can be used standalone or as a decentralised ordering service with other ledgers, such as Hyperledger Fabric, Corda, or Ethereum, it creates new opportunities for blockchain interoperability.

Infrastructure Layer

The infrastructure layer deals with sets of components enabling the services of the blockchain platform. These typically include, but are not limited to, compute, storage, network, and virtualisation. 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 data nodes 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 also renders legal vulnerability of the network to money laundering, breach of currency controls, and other pitfalls.

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 that cloud providers have on the solution, limiting 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. This instils a certain dependency on the vendor for part of the blockchain architecture. It could be an ordering feature 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 of 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. Approaches to interoperability

What approaches exist for achieving blockchain interoperability?

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

Figure 6.4 – Three approaches to blockchain interoperability

Cross-authentication

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

- **Notary schemes** are executed by trusted parties that help participants on blockchain platform A confirm that some event occurred on blockchain platform B, and vice versa. Notary schemes are one of the simplest ways to achieve the full suite of cross-chain interoperability. However, it centralises trust which goes against the main paradigm of blockchain, namely decentralisation. This consequence might be acceptable in situations where blockchain consortia members can agree on a central party to operate the notary scheme.
- **Relays** are systems inside of one blockchain that can validate and read events and/or states in other blockchains. This gives chain A the ability to understand event changes on blockchain platform B without leveraging a trusted party. The downside is that it is very difficult to connect existing blockchains that don't share similar characteristics.
- **Hash-locking** means setting up operations on blockchain platform A and blockchain platform B that have the same trigger, usually the revelation of the pre-image of a particular hash. This is the most practical technical method to interoperability but is also the most limiting in terms of functionality, only supporting digital asset exchange.

Cross-authentication

Pros: Only approach that can enable blockchain interoperability without leveraging 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 supply chain. Also, relays in particular are yet to see widespread adoption for enterprise use.

Oracle

An oracle is an agent that transfers external data to the blockchain platform for on-chain use. This is done using smart contracts that add information about real-world events to the blockchain platform. Simple examples of data that are useful to import 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. (For example, if a train is delayed, an insurance contract can 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. This might be either because they are operated by a trusted third party or because of cryptographic attestations.

Oracle

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 only make blockchains interoperable with non-blockchain systems. Applications are only as reliable and trusted as their oracles are.

API Gateway

An Application Program 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, a software tool or a programming language.

An API gateway organises several APIs. It is the conductor that organises the requests being processed by the underlying architecture to simplify the experience for the user or the process of requesting for a client. It's 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.

API Gateway

Pros: Tried and tested technology – easy to implement.

Cons: May not be possible 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 centralises trust to whoever operates the APIs.

4. Picking the right approach

How does an organisation pick the right approach for its use case?

When organisations need to decide on an interoperability approach, they should first understand two dimensions. One is 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, organisations should use the three interoperability layers to understand whether the system is a compatible blockchain, a non-compatible blockchain or a non-blockchain platform. When this is clear, organisations should then know which of the three interoperability approaches to pick.

For instance, say an organisation is utilising a blockchain platform solely dealing with financial transactions, as in a digital asset exchange. It wishes to become interoperable with another blockchain platform, which through analysis of the three layers in the blockchain interoperability model turns out to be fundamentally different (non-compatible blockchain platform). In this case, the right approach will be the API gateway approach.

To assist organisations in making decisions in interoperability approaches, the following introduces three types of systems to connect to, and four types of consortia as business context for interoperability needs.[92]

> *It is easy to wish interoperability to connect ecosystems to each other, but like security it is hard to find the best approach. The most effective way is to conduct this study in a systematic manner by investigating the interoperability layer model and specifying interoperability requirements at each layer.*
>
> **Yusuke Jin,** Research and Development Division, Hitachi

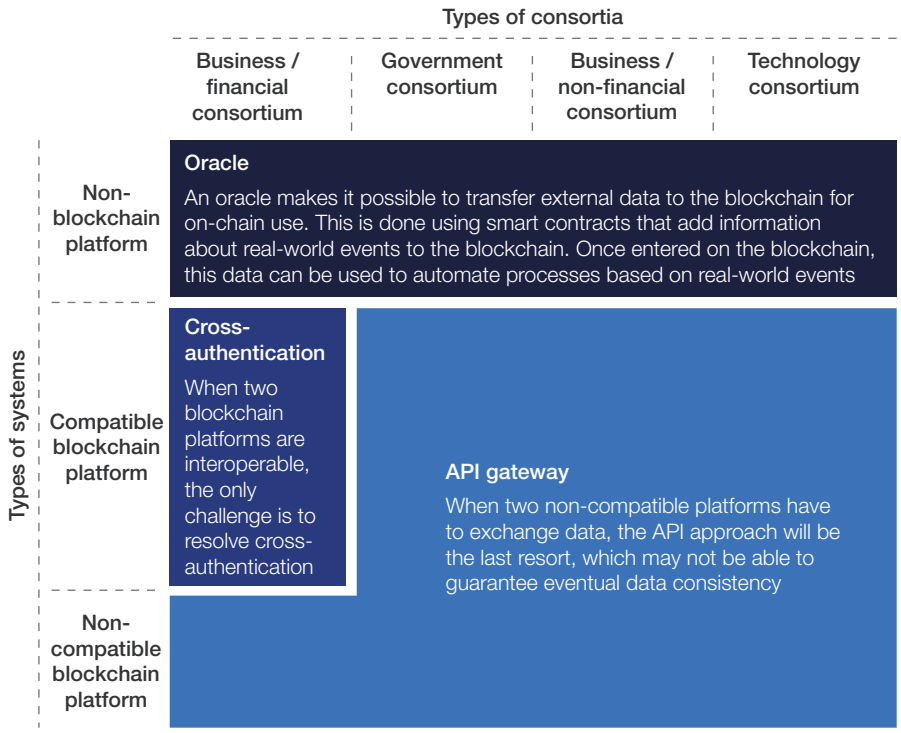

Figure 6.5 – Four context-dependent approaches to blockchain interoperability

Types of systems

Non-blockchain platform: Systems which do not utilise blockchain technologies and therefore have inherently different infrastructure setups than blockchain platforms.

Compatible blockchain platform: Blockchain platforms which are technically compatible for all three interoperability layers.

Non-compatible blockchain platform: Blockchain platforms that share some features to the blockchain platform in question but without sufficiently similar characteristics when analysed using the three interoperability layers.

Types of consortia

Business/financial consortium: Focuses 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 both have the need for 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: Acts as a provider of the technologies enabling a blockchain platform. Therefore, the technology produced by such a consortium is rarely technically compatible with blockchain platforms from other consortia regardless of any requirements to exchange data.

5. Structure blockchain interoperability requirements

Below is a checklist meant for assisting organisations to structure their efforts in clarifying blockchain interoperability requirements. The checklist is structured 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? If so, what data standards are being used?
- ☐ How should participants discover, exchange, and make use of relevant distributed data across different ecosystems?
- ☐ Does the desired use case rely on features supported by adjacent ecosystems? For instance, does the supply chain use case require payments or trade finance features?
- ☐ How can inherent interoperability risks such as exposure of information to distrusted third parties and loss of access to information on secondary chains be avoided or mitigated?

Platform Interoperability

- ☐ Do any of the participants participate in an existing blockchain ecosystem? If so, what blockchain platform is it built on, and which consensus mechanism does the ecosystem rely on?
- ☐ Do the blockchain platforms have support for similar multi-signature transactions for authentication and authorisation? For example, 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 decentralisation 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 differences in their consensus mechanisms and governance models?
- ☐ 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 data storage location or other matters?
- ☐ Does the use case allow the solution owner to deploy the solution on a virtual private cloud?
- ☐ Does the use case allow the solution owner to leverage BaaS offerings?
- ☐ Is the IT organisation mature enough to depart on a journey of hosting nodes, wallets, secure keys, or even to manage tokens?