WORLD ECONOMIC FORUM

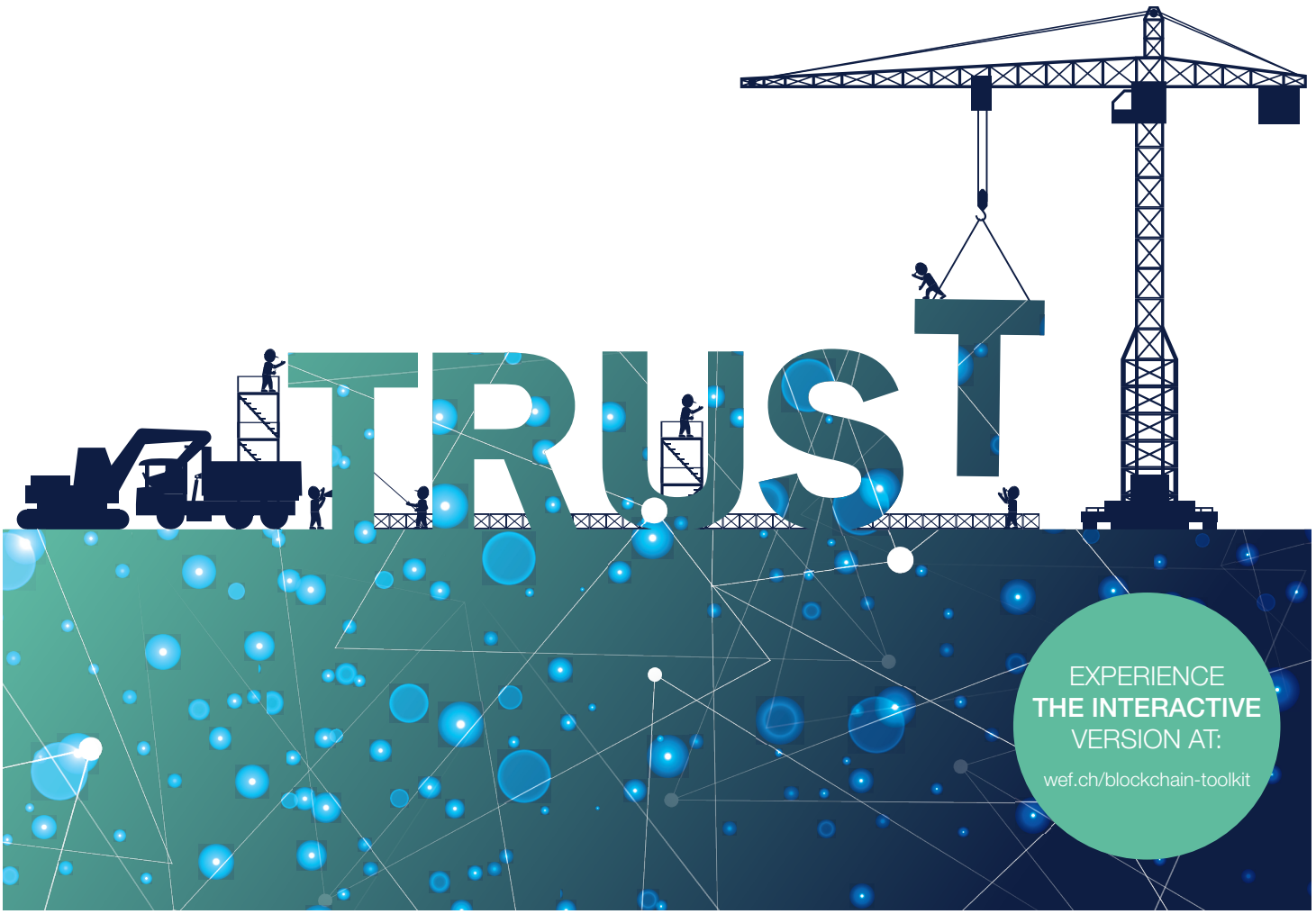
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Redesigning Trust:

Blockchain Deployment Toolkit

Supply Chain Focus

April 2020



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

Preface

Nadia Hewett
Project Lead – Blockchain and Digital Currency, World Economic Forum, USA

Sheila Warren
Platform Head – Blockchain, Digital Currency, and Data Policy, World Economic Forum, USA

Murat Sönmez
Managing Director, World Economic Forum, USA

The emergence of blockchain technology holds great promise for supply-chain organisations, perhaps as much as any new development in the industry's infrastructure since it switched to standardised containers decades ago. The case for blockchain is stronger as the COVID-19 pandemic underscores the need for more resilient global supply chains, trusted data and an economic recovery enabled through trade digitization. At the same time, blockchain may engender a fair share of puzzlement and anxiety among supply-chain leaders unfamiliar with it as a new and unfamiliar digitisation tool.

This toolkit is designed to help with the deployment journey, whether your organisation is seeking to gain increased efficiency, greater trust with counterparties, or other potential benefits offered by blockchain technology. Your organisation can use the toolkit to support more responsible blockchain deployments, de-risk early adoption, and ensure careful consideration of unintended consequences.

Unlocking opportunities means necessary consideration must be given to key technical and non-technical factors of success and the potential pitfalls in areas including consortium governance, interoperability, digital identity, cybersecurity, and regulatory – all included in this toolkit.

The toolkit is the culmination of more than a year of World Economic Forum efforts to document tested-and-tried deployment best practices, insights and lessons from a community of 100+ organisations – and to address related issues that may arise in implementation projects. In addition to learning from their use cases, the toolkit draws from a series of seven white papers[1] that delved deeply intokey topics such as digital identity, security, and interoperability. Delivered through the Forum's Centre for the Fourth Industrial Revolution, this work aims to shape the development and deployment of blockchain solutions and to provide a space for global cooperation to create understanding and policies that accelerate these technologies' positive impact.

To accelerate the proliferation of responsible solutions and to level the playing field for partners upstream and downstream, we encourage sharing of the toolkit within your professional network.

Sincere thanks to the generous commitment of the community who contributed their unique insights and expertise to this toolkit.

TABLE OF CONTENTS

Preface	3
Table of Contents	4
Introduction	6
Executive Summary	14
Ecosystem	19
Consortium Formation	32
Consortium Governance	52
Digital Identity	73
Interoperability	97
Structure: Public/Private	110
Data Protection	121
Data Integrity	131
Personal Data Handling	151
Cybersecurity	163
Legal and Regulatory Compliance	177
Tax Implications	197
Financial Reporting and Controls	206
Risk Factors	214
Navigate Key Questions	225
Glossary	230
Contributors	236
Endnotes	240

This toolkit combines best practices from dozens of experts across relevant domains

80+ Companies

- Technology and supply chain
- Fortune Global 500 and start-ups
- Civic and International Organizations
- Academia
- Professional services firms

40+ Blockchain use cases

- Product provenance and traceability
- Streamlining global supply-chain operations
- Automation and smart contracts
- Trade finance and many others

20+ Governments

- Customs and border protection
- Ministries of transportation
- Ministries related to technology and digitisation
- Trade single window ecosystems

50+ Countries

- Spans 6 continents

> Industries are increasingly forming consortia to explore the transformative potential of blockchain technology. Drawn from an unparalleled community of business and technology experts, this toolkit will guide business executives and deployment teams through essential processes and resources to make informed, practical, and timely decisions for a successful blockchain solution.

Nabil Alnuaim,
Chief Digital Officer, Saudi Aramco

> With the proliferation of blockchain-based solutions in our industry, this toolkit serves as a resource for those becoming familiar with blockchain solutions. Developed by a community of industry and technology experts, the toolkit offers a wealth of expertise and a practical guide for supply chain leaders.

Gene Seroka,
Executive Director, Port of Los Angeles

> Blockchain offers supply chain functions a full range of benefits, including a reimagination of the trust that is so vital to the supply chain ecosystem. But for supply chain leaders to derive the benefits that blockchain technologies offer, they have to navigate a thorny set of issues and trade-offs. This toolkit is a comprehensive array of principles and best practices to guide supply chain practitioners through a broad set of considerations to shape strategies, enhance processes, and deploy truly transformative solutions throughout the global supply chain ecosystem.

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

Introduction

Welcome to the Redesigning Trust toolkit, designed to guide you and your organisation through the development and deployment of a new blockchain solution. Before you get started, a few things you should know:

Who is the toolkit for? While anyone can use the toolkit, the content assumes that your team or organisation has identified a good blockchain use case via an honest evaluation of the technology as compared to other options. While useful for blockchain deployments generally, this toolkit focuses on supply-chain deployments.

What's in the toolkit? There are 14 modules in this toolkit with specific tools and resources throughout to help make the included information more readily useful to your project. It draws upon lessons from more than 40+ global supply chain use cases.[10]

Figure 1.1 – All 14 modules available in this toolkit

What's not in the toolkit? This toolkit does not include resources for determining whether blockchain technology is the right fit for your use case or for evaluating your organisation's digital maturity. More information about the scope of the document can be found in the Assumptions section.

How should the toolkit be used? The content is modular, not linear. The aim is that you will use the toolkit as a handy reference for your project, reviewing different modules as needed, whenever needed, depending on your particular project's needs.

More details are included in the Using the toolkit section at the end of the Introduction module.

Supplementary reading -

This toolkit builds upon previous publications released by the World Economic Forum. The following whitepapers were published as a series on Inclusive Deployment of Blockchain for Supply Chains:[2]

- Part 1 – Introduction[3]
- Part 2 – Trustworthy Verification of Digital Identities[4]
- Part 3 – Public or Private Blockchains – Which One Is Right for You?[5]
- Part 4 – Protecting Your Data[6]
- Part 5 – A Framework for Blockchain Cybersecurity[7]
- Case studies and learnings from the United Arab Emirates[8]
- Part 6 – A Framework for Blockchain Interoperability[9]

Interactive version

An interactive version of this toolkit is available online and it offers a digital spreadsheet consolidating the main tools and key questions of the toolkit for you to download and tailor.

The foundations: How to think about blockchain deployments

Before you dive into the modules, there is some important context to keep in mind. Remember that blockchain is simply one tool in an organisation's digitisation journey. As such, here are a few foundational themes:

The enterprise environment: meeting enterprise rigor and requirements

While the technology is still nascent, blockchain requires the same features and rigor that one would find in almost any government or corporate technology implementation. Figure 1.2 shows nine essential considerations that organisations typically need to address to ensure the success of any new enterprise solution. The items on this list are grounded in IT best practices and project management principles that are likely already familiar to the reader. This toolkit is intended to help your organisation think through and meet these typical enterprise requirements in the context of blockchain technology.

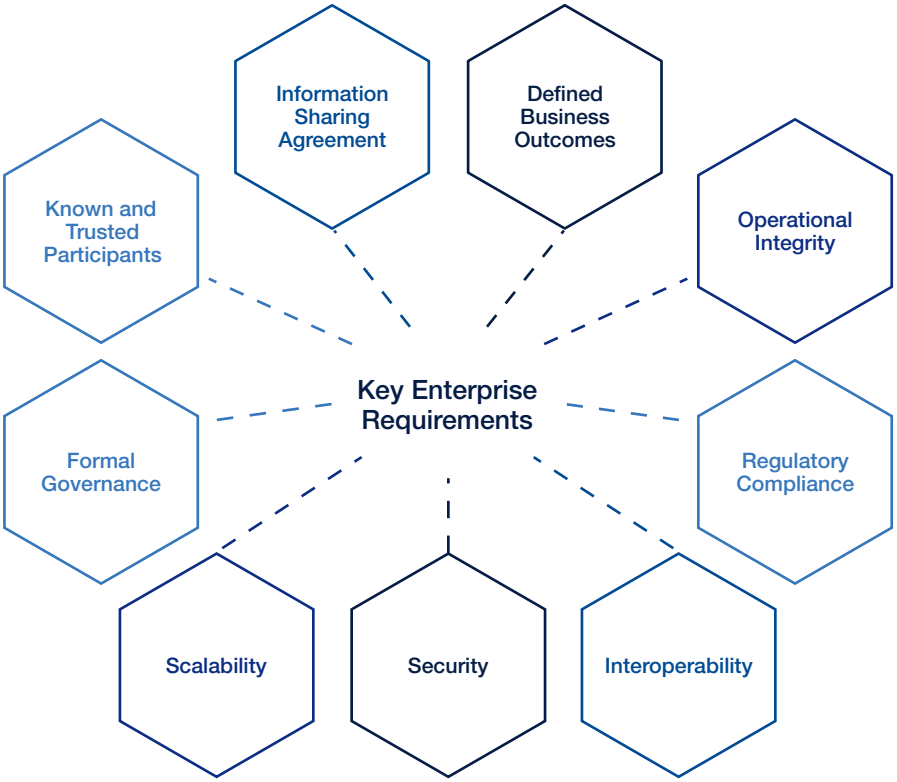


Figure 1.2 – Essential considerations typical for enterprise technology solutions

These considerations – and their relevance to compliance, corporate governance, and personal privacy laws and regulations – will affect how organisations structure their blockchain solutions. For most supply-chain use cases, the requirements mean organisations are likely to prefer permissioned solutions, where participation is subjected to identification of all parties, sensitive data confidentiality, and adhering to the system rules. As such, the toolkit focuses mainly on permissioned blockchain solutions – a common approach for enterprises – rather than permissionless blockchain solutions like Bitcoin, though many of the learnings can be applied to both. The Structure: Public/Private module explores the trade-offs between permissionless and permissioned systems in more detail.

Making decentralisation work for organisations

Decentralised processes will benefit from blockchain technology that is designed for automating decentralised process. The current challenge is that many supply-chain processes today use technologies that are designed for siloed centralised processes. Hence, a rigorous review on both process and technology is needed when evaluating blockchain as a fit to ensure that the given processes and use case will benefit from decentralisation. Governments and businesses must recognise that a business process that is inherently centralised or designed based on centralised trust controls may not be effectively automated using blockchain.

Decentralisation should not be an all-or-nothing objective but rather a balanced objective that requires consideration of trade-offs. There are practical reasons why a system may require both centralised and decentralised components.

However, decentralisation benefits degrade quickly when centralised components are added. Thus, if centralisation of a component is required as a transitional stopgap measure, then the organisation must recognise what decentralisation benefits will be lost during that phase of operations and must have a concrete plan for migrating to decentralised components when doing so becomes feasible.

> *Blockchain technology provides a base-level foundation — not a complete business solution. It is analogous to a concrete foundation in building construction upon which a 30-story building needs to be constructed. A lot of extra work has to be done before the blockchain-based decentralised business solution is ready for use by customers, partners, or employees.*
>
> **Henrik Hvid Jensen,** Senior Blockchain Adviser, Trustworks

Distinguish applications from underlying layers

Blockchain technology has its own nomenclature to navigate. Terms like "blockchain solutions," "smart contracts," and "decentralised applications" (Dapps) can overwhelm many newcomers. A development or project can, for example, be referred to as a "blockchain solution" or "blockchain technology" for simplicity sake.

Nonetheless, understanding what your project entails is important. Are you selecting underlying layers – for example infrastructure such as Blockchain-as-a-Service, network, and protocols – or realising a decentralised application? It is important to distinguish and understand the difference between Dapps and the underlying blockchain platform. For example, when you assess the security of your solution, the implications at the application layer will be different than at the underlying layer.

For a more detailed and technical overview of different layers within a blockchain reference architect or blockchain technology stack, overviews are available from Enterprise Ethereum Alliance[11], International Organization for Standardization (ISO)[12] or Deloitte,[13] among others.

The findings in the toolkit are undertaken in simple terms to bring understanding of some key considerations. For these reasons, the tools do not delve into the multitude of technical layers, complexities and exceptions that exist with blockchain technology, though the authors recognise their existence and importance.

Prepare for change – future proof your solution

Blockchain technology is developing rapidly. Your organisation or industry cannot sit on the sidelines for 3-5 years waiting for the technology to mature. If the blockchain solutions are relevant to your business, you should start preparing a non-technical and technical foundation progressively for the eventual mainstream operations.

- Existing differences will become configurable or interoperable features of future solutions.
- The current need for technology variety within the ecosystem will be rationalised to make the planning process more predictable and repeatable, similar to the world wide web's evolution in the 1990s.
- There will be a provider cycle where some initial vendors fail to become sustainable and are replaced by next-generation successors.
- Standardisation of blockchain protocols may lead to convergence. In fact, some expect the emergence of a handful of prominent platforms to comprise the backbone of a global network of blockchains that overlay today's internet.
- As the maturity of blockchain protocols grows over the next decade, the focus of many projects will gradually shift toward new layers of technologies. The future of the technology will likely include purpose-built protocols and platforms for decentralised off-chain computing, messaging, oracle, integration, storage, data management, and identity to complement blockchain and build solutions for the future decentralised web (a.k.a. Web 3.0). This would fundamentally alter the way supply-chain actors are interested in and able to engage with blockchain technology.

What does this mean for planning a project at present?

Given that current platforms could become obsolete over time, it is prudent to consider decoupling current decentralised applications from their underlying blockchain protocols as much as possible.

This can help any future migration to a new platform with less pain and rework. Whatever blockchain technology that you are using today, plan for upgrading or replacing it within 3–5 years.[14]

In the short term, there are obstacles and challenges with the adoption of blockchain technology. Today, the technology simply is not fully mature. But that does not mean you shouldn't participate at this early stage.

Executing on the following activities can and should be done in parallel with the maturation of blockchain technology:[15]

Ecosystem collaboration: Incumbent participants, many of whom may be fierce competitors within the industry's ecosystem, need to agree to collaborate using blockchain. This is like radio-frequency identification (RFID) in its early days; before blockchain can reach its potential, business processes and standards must be resolved.

Data interoperability: After industry participants agree to collaborate, there is significant effort to define what data will be shared by whom. Industries will need to go through the laborious process of agreeing upon what data belongs on blockchain and what processes should be handled by autonomous software agents, as well as the structure, format, and meaning of the data they share.

When organisations have solved the above two challenges, the industry will be ready to build a blockchain-based platform or solution. It will require effort to construct the system, test and deploy it across a diverse set of participants. New terminology, concepts, and technology usage all mean adoption will take time and patience but holds great promise for supply-chain organisations where the technology is a fit.

Toolkit Design Principles

A hyper-focus on efficiency gains and a culture where players create barriers to others, can reinforce existing mistrust or competition and undermine or even block the transformation that blockchain technology has the potential to bring about for the supply chain ecosystem.

For those reasons, this toolkit was designed with a set of main principles in mind:

- **Inclusivity:** Everyone can capture some value from blockchain technology. That said, organisations undertaking new blockchain projects need to consider potential unintended consequences as well. It is also important to design solutions that level the playing field for small and medium-sized enterprises and global access.
- **Interoperability:** This toolkit should help to enhance standardisation and end-to-end supply chain integration of new blockchain solutions with other mission-critical tools within organisations. A new blockchain solution may have to share information with other components across different blockchain networks or, more commonly, with legacy enterprise systems that will remain in use throughout the course of a deployment. Being mindful of such compatibility issues will help future-proof the blockchain part of the system at the technical, business, governance, and process levels.
- **Integrity:** Blockchain solutions should provide solid integrity in data, security, authentication, and other important pillars of successful solutions. Given the increased focus on privacy and data compliance, these needs are greater than ever within supply-chain organisations.
- **Fit for purpose:** Users can use the guidelines to pick the best approach and solution for their requirements. The tools and resources in the toolkit were created keeping in mind that users still need to look at the context of their selected use case and distinct requirements.
- **Variability:** The guidelines were designed to be applicable to diverse supply chains that consist of many stakeholders with differing relationships and incentives.

Assumptions

- While blockchain is one type of distributed ledger technology (DLT), for simplicity, the terms are used interchangeably in this toolkit to cover all types of distributed ledger technologies.
- Truly innovative deployments of blockchain require a match between blockchain's specific benefits and use cases that enable realisation of these benefits, followed by dedicated hard work to get it right and embedded in organisations and industries. DLT is not a workaround for business processes, nor is its use a guarantee of stakeholder alignment. This toolkit depends on sound business decision making up-front.
- This toolkit is designed to be accessible to those with varying degrees of blockchain knowledge, including those who are just getting started with the technology. The findings in the toolkit are undertaken in simple terms to bring understanding of some key considerations. For these reasons, the tools do not delve into the multitude of technical layers, complexities and exceptions that exist with blockchain technology, though the authors recognise their existence and importance.
- The toolkit does not present answers to all questions and considerations. Instead, decisionmakers can use the considerations, questions and guidelines to pick the best approach and solution for their specific requirements. As the toolkit outlines typical criteria, it is done such that users of the toolkit can apply it to the context of their selected use case and distinct requirements.
- The tools list key considerations, questions, risks and other. These are not an exhaustive list. Furthermore, they should not be equally weighted, but be weighted appropriately in response to the company specific use case, stakeholder complexities and other assessment, e.g. a certain blockchain solution may put more priority on data integrity than confidentiality and availability while others may do differently.
- This toolkit does not constitute legal advice.

Using the toolkit

Who will be using the toolkit?

Organisational Profile

The selection of modules, with resources and tools within, caters to the nuances of cross-border and international supply chain, logistics and trade-related use cases. The resources are designed so that it can be applicable to diverse supply chains that consist of many stakeholders with differing relationships and incentives.

Organisations should have already evaluated whether blockchain is fit for purpose and matching their digital maturity. More information in "Toolkit value throughout blockchain solution lifecycle" section.

Individual User Profile

The toolkit is aimed primarily at individuals and teams involved in the development and deployment of a blockchain solution. Roles and responsibilities that benefit from the resources and tools span functions typically involved in building and scaling blockchain solutions, including project management, operations, IT, compliance, procurement, partner engagement and more. This holistic approach is intentional so that no part of the business is an afterthought. For instance, auditing considerations should not be an afterthought; rather, they should be considered right from the initial scoping and strategy phase of blockchain implementation.

How is the toolkit structured – and how can it be used?

The content of the toolkit is structured into 14 different modules. The modules represent key success and risk factors for the deployment of a blockchain solution within the supply chain context.

Individuals and teams should decide and select the module(s) most relevant to their business questions and needs. Each module is a self-standing read. At the same time, modules are integrated, and it is important to consider the toolkit in its entirety when business decisions are made, together with any new findings and industry-specific considerations not addressed by this toolkit.

How to get started

There are several options for navigating the toolkit:

1. Use the toolkit end-to-end for holistic deployment guidance.
2. Choose the specific topics of interest. Brief overviews of what each module covers are below.
3. Start with your business needs and questions. Navigate Key Questions contains a checklist of deployment needs with links to the related content within the toolkit.

Figure 1.3 – Toolkit modules overview

Toolkit value throughout blockchain solution lifecycle

While the toolkit can be used at any time in the blockchain solution journey, the tools and resources of the toolkit are focused on **the development and deployment phases.** This toolkit starts from the premise that your organisation thought honestly about whether using blockchain is a sound business decision (during phase ideation and use case selection in Figure 1.4).

For any organisation, blockchain adoption should not be a goal in itself but a means to achieve specific business benefits. Before using this toolkit for development and deployment of a new blockchain solution, you should have completed a rigorous business assessment in which the results showed that blockchain is the most appropriate tool to address a specific business need. With that in mind, it is anticipated that the value derived from the toolkit would look something like this through the phases of a typical project:

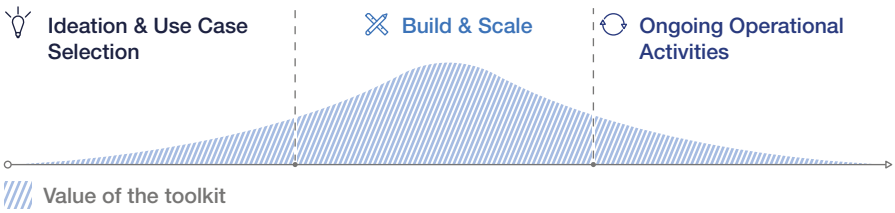


Figure 1.4 – Toolkit value through-out blockchain solution lifecycle

Table 1.1 shows a detailed listing of specific benefits the toolkit might provide at different stages of a project.

Table 1.1 – Toolkit value at different stages

Ideation & Use Case Selection	Build & Scale	Ongoing Operational Activities
• Right Mindset during business problem identification, use case validation, and technology assessment • Strategic Foresight to anticipate deployment risks and success factors • Structured Conversations with internal and external stakeholders • Recommended References from World Economic Forum[16] you can use at this phase	• Guidance to leaders to ensure deployment progresses with integrity, inclusivity and responsibility • Key Considerations across both technical and non-technical drivers of deployment • Structured frameworks to help organisations unlock value from their blockchain solutions • Proactive approach to recognise and manage new types of risks stemming from blockchain • Minimum Safety Check before product launch	• Foresight for deliberate ongoing ecosystem expansion • Resources for ongoing solution integrity • Principles that can be applied even as the blockchain landscape continues to change • Ability to revisit important solution design and development considerations and checks

Executive Summary

Blockchain has the potential to revolutionise how companies compete and stakeholders collaborate in the world of supply chains. As the technology is nascent, the World Economic Forum has published this toolkit to provide guidance for development and deployment of new blockchain solutions.

This summary provides the highlights of the toolkit but also serves as a brief to executives to familiarise them with deployment success factors and barriers. Additional detail is available in the toolkit modules, which provide deep dives into each topic.

Blockchain is a tool in the tech stack

Any implementation of blockchain technology should be approached just as any other new solution an organisation wishes to integrate into its overall operation. Blockchain is one piece of the information technology (IT) puzzle that, if deployed correctly, complements the other solutions used every day to carry out routine and mission-critical tasks.

Below are nine key requirements that organisations typically need to address for any new enterprise solution. The items on this list are grounded in IT best practices and project management principles that are likely already familiar to the reader. The toolkit helps your organisation think through and meet these typical enterprise requirements in the context of blockchain technology.

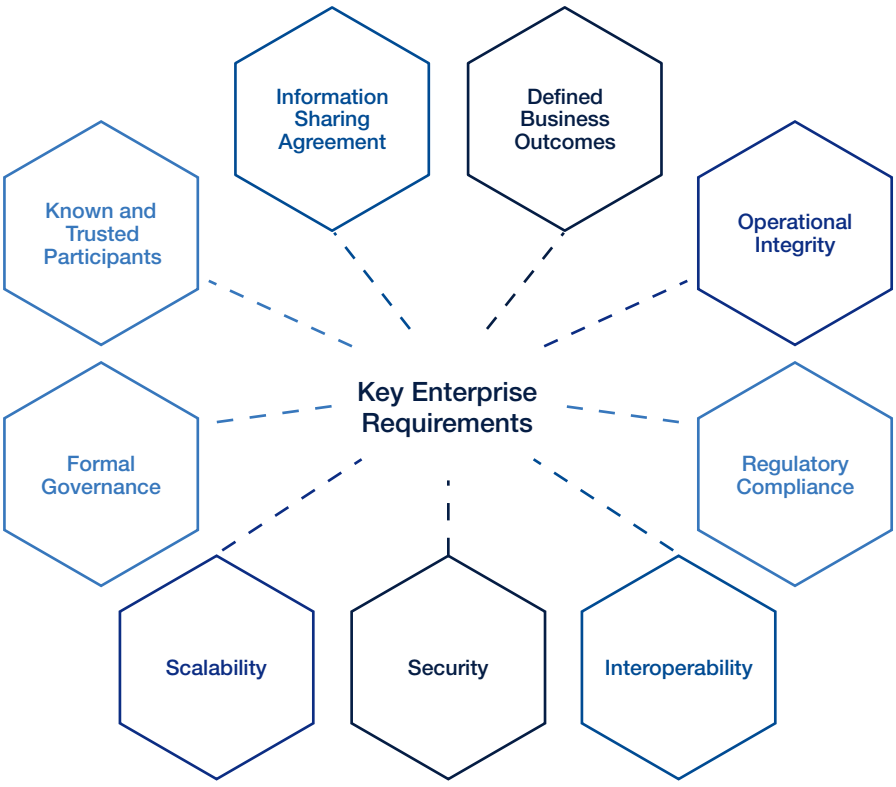


Figure 1 – Essential requirements typical for enterprise technology solutions

This toolkit builds on a series of earlier white papers on Inclusive Deployment of Blockchain for Supply Chains.[17] If of interest, as supplementary reading, it covers the following topics:

1. Introduction[18]
2. Trustworthy Verification of Digital Identities[19]
3. Public or Private Blockchains – Which One Is Right for You?[20]
4. Protecting Your Data[21]
5. A Framework for Blockchain Cybersecurity[22]
6. Case studies and learnings from the United Arab Emirates[23]
7. A Framework for Blockchain Interoperability[24]

For your organisation to ensure successful implementation of blockchain solutions, consider the following:

- **Defined Business Outcomes:** Like any other technology, blockchain is as much about careful attention to the economics and business models as it is about technology evangelism. Blockchain technology should not be a goal but a tool deployed to achieve specific purposes.

  Value brought by blockchain technology can best be understood through specific use cases. In general, the power of blockchain lies in its ability to enable peer-to-peer interactions and cross-enterprise automation – supported by smart contracts – typically as part of a broader solution. It offers the opportunity for greater trust and increased efficiency in supply chains.

  Today the typical operating model of most of the largest internet companies are platform-based. These centralised digital platforms can trend towards a "winner-takes-all" model that grows through quasi-monopolistic participant capture. Blockchain technology provides the tools for an alternative business model wherein the data and trust layer are collaboratively owned and managed by its participants. This provides an opportunity for incumbents to compete against the centrally driven platforms becoming the new market leader in their industry; to retain control of information collection and usage, the interface and trust-building.

Recommended reading from World Economic Forum publications on evaluating the business value of blockchain technology:[25]
- Blockchain Beyond the Hype
- Building Value with Blockchain Technology: How to Evaluate Blockchain's Benefits
- These 11 questions will help you decide if blockchain is right for your business

An introductory white paper[26] in this series outlines some of the most popular use cases in the supply-chain context to date.

- **Operational Integrity:** Blockchain solutions should provide solid integrity in data, security, authenticity, and other important pillars of operational integrity. Given the increased focus on privacy and data compliance in the general public and with governments, these needs are greater than ever within supply-chain organisations.

  There is much misunderstanding about data integrity as it relates to blockchain. Simply by its nature, blockchain technology does not necessarily ensure accuracy of data entered on-chain. However, it does specifically protect against manipulation of data, which is immutable once it goes on the shared ledger. Achieving data integrity within blockchain applications is broadly composed of three requirements covered in the toolkit: data origin integrity, oracle integrity, and digital twin integrity. Blockchain helps to establish a higher level of traceability and auditability to data as any data entered inaccurately prior to consensus can be traced back to its origin.

Interested? Learn more:
Data Integrity
Cybersecurity
Personal Data Handling
Data Protection
Structure: Public / Private
Financial Reporting and Controls
Digital Identity

- **Regulatory Compliance:** Compliance requirements can dissuade the deployment of blockchain in supply chains if not properly understood. This is in part because of the cost of non-compliance, but also because regulations are seldom made with distributed data exchange or self-executing contracts in mind.

  Key legal and regulatory risks include uncertainty around cross-jurisdictional regulations, antitrust violations, smart contract legal enforceability, Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements, and intellectual property (IP) protection. Personal data protection should also be considered within the blockchain design, including emerging rules like the European Union's (EU) General Data Protection Regulation (GDPR) and the recent California Consumer Privacy Act (CCPA). Blockchain platforms also create multiple tax implications, from the potentially transformative impact on tax processing systems to the rise of new tax complexities.

Interested? Learn more:
Legal and Regulatory Compliance
Risk Factors
Personal Data Handling
Data Protection
Tax Implications
Financial Reporting and Controls

It is also important to work with external auditors, along with relevant stakeholders, to determine what aspects of financial reporting may be impacted by blockchain deployment. These may include risks related to material misstatement, management's assertions, and internal controls, to cite just a few examples.

- **Interoperability:** The peer-to-peer interactions around shared distributed ledgers with blockchain technology make a transformation from a siloed and fragmented approach to end-to-end value chain integration more attainable. But this also means that integration with existing and future processes and systems is imperative – especially as there are more than 100 blockchain platforms in 2020.

  Interoperability is the ability for computer systems to exchange and make use of information in a collaborative way. But this otherwise straightforward concept can become complex in the context of blockchain due to its distributed nature.

  In a blockchain ecosystem, successful interoperability guarantees that the user can trust that "I know what I see is what you see" within a single platform as well as across platforms. The toolkit provides tools for dissecting the challenge of interoperability and for choosing the best workable interoperability approach. Being mindful of such compatibility issues will help future-proof the blockchain part of the system at the technical, business, governance and process levels.

Interested? Learn more:
Interoperability
Digital Identity

- **Security:** As any new software, blockchain-based solutions must include adequate safeguards against potential cybersecurity nightmare scenarios, like costly enterprise hacks, ransomware, and stolen user data.

  One of the main differentiators of blockchain is its decentralisation, which has profound impacts in security governance. While there is no security silver bullet in the world of cyber, ensuring a high degree of data segregation, control requirements, privacy, and clear custody of data is achievable. While various types of blockchains have varying degrees of fault-tolerance, most are considered better alternatives than traditional databases from an integrity perspective. Blockchain is no exception to the general rule of cybersecurity that sound risk management requires that security measures be baked in from the start. There are some fundamental security concepts that have emerged in the blockchain space, as well as a clear sense of what the risks are. The toolkit offers a risk management framework and a 10-step secure deployment plan that should be useful in a wide range of supply-chain projects.

Interested? Learn more:
Cybersecurity
Risk Factors
Structure: Public / Private
Data Protection
Personal Data Handling

- **Scalability:** Any new blockchain solution should be able to grow along with the enterprise. Also, as blockchain technology is developing rapidly, organisations should prepare for change over time. It is important to prepare for change and future-proof your solution.

  Given that current platforms could become obsolete someday, it is prudent to consider decoupling current decentralised applications from their underlying blockchain protocols as much as possible. This can help any future migration to a new platform with limited pain and rework. Whatever blockchain technology that you are using today, plan for upgrading or replacing it within 3–5 years.[27] But that does not mean your organisation shouldn't participate at this early stage. If the blockchain solutions are relevant to your business, you should start preparing non-technical and technical foundation progressively for the eventual mainstream operations. This is like RFID in its early days; before blockchain can reach its potential, business processes and standards need to be defined.

Interested? Learn more:
Interoperability
Digital Identity
Introduction

- **Formal Governance and Industry Collaboration:** With the advent of the digital age, companies and institutions have started to organise their activities and business architectures in the form of ecosystems. Good governance is key. Creating the framework for entities to effectively work together is just as important as building the related technology solution.

  Organisations are starting to understand the disruptive potential of blockchain to solve pain points and provide increased efficiency, automation and transparency across supply chains. CEOs are also starting to recognise that industry-wide collaboration around blockchain is necessary so that proof-of-concept, standards and solutions can be adopted at industry-scale. In fact, a lack of collaboration can undermine or even block the transformation that blockchain technology has the potential to bring about in a given ecosystem (blockchain is the ultimate networked technology). Joint ventures or blockchain consortia have been popular approaches in the industry to-date. While the rewards from collaboration can be high, agreeing on what constitutes a fair and well-designed governance system, let alone a joint blockchain platform, can be difficult. This is where many industry collaboration efforts have fallen apart. The toolkit provides guidance to help new consortia reach consensus on what constitutes fair, compliant and robust governance.

  Interested? Learn more:
  Ecosystem
  Consortium Formation
  Consortium Governance

- **Known and Trusted Participants:** For most supply-chain solutions, there needs to be a way to identify who or what entity was responsible for any specific part of a blockchain transaction. For this reason, trust-worthy verification of digital identity is needed, and it is important that there are clear rules and procedures for adding new participants to the network.

  A trusted digital identity is critical on a blockchain network as there is no face-to-face interaction during a transaction, and autonomous software agents and "things" might transact on behalf of legal entities in the future. A digital identity system in a blockchain deployment for supply-chain should be able to support digital identities for the various actors involved. The toolkit includes considerations and questions to guide the design and implementation of a responsible digital identity system.

  Interested? Learn more:
  Digital Identity

- **Information Sharing Agreement:** Parties should have agreed on data rights and intellectual property (IP) ownership before conducting transactions on a blockchain network.

  Realising blockchain in supply-chain use cases and taking advantage of the distributed nature of the technology, requires sharing of data that is usually generated in-house within individual member companies in a broader ecosystem. Thus, there is a risk of data being shared or used inappropriately by third parties. Data sharing also needs to comply with data protection legislation. European Union's General Data Protection Resolution (GDPR) is also at the forefront of a new wave of data protection legislation globally which places strict obligations on organisations handling personal data or personally identifiable information, such as the recent California Consumer Privacy Act (CCPA).

  Blockchain technology never requires an organisation to reveal more data than it is comfortable with. On-chain data can also be encrypted so that it is only usable by permissioned parties. Thus, in the course of selecting and deploying a blockchain solution, a supply-chain organisation has real flexibility to ensure it addresses both their data protection and privacy concerns and obligations and those of other supply-chain partners.

  Interested? Learn more:
  Data Protection
  Personal Data Handling
  Legal and Regulatory Compliance
  Consortium Governance

Final comments

The essence of blockchain is to offer a new way of collaboration through decentralisation. At the same time, it is important to keep in mind that decentralisation is not an all-or-nothing objective but a balanced one that can require trade-offs for practical reasons. Thus, a system may require both centralised and decentralised elements. Historically, the supply-chain industry's IT solutions have been a patchwork of centralised modules, some of which may have compatibility issues or create other challenges for organisations. The emergence of blockchain technology offers the opportunity to alleviate some of these headaches.

A hyper-focus on efficiency gains and a culture where players create barriers to others, can reinforce existing mistrust or competition and undermine or even block the transformation that blockchain technology has the potential to bring about for the supply-chain ecosystem. Strong players may push blockchain-based solutions to resolve pending industry issues. The industry is still in the infrastructure-building phase of the technology, in which it can be largely cost-prohibitive for small players to innovate or to build comprehensive solutions. Even though there are more open-source components to blockchain (than is the case for many other technologies), which could lead to a faster diffusion and adoption cycle, smaller incumbents may not have access to resources required to unlock the value of blockchain technology. For these reasons, the toolkit can be a valuable resource that level the playing field for small and medium-sized enterprises. It was designed to help organisations undertaking new blockchain projects to consider potential unintended consequences and to encourage integrity, interoperability and inclusivity.

This toolkit is designed to help organisations with the hard work that comes in blockchain implementation. The 14 modules are meant to be used on an as-needed basis, in whatever sequence is best suited to an organisation's practice. Your organisation can use the modules to support more responsible blockchain deployments, de-risk early adoption, and ensure careful consideration of unintended consequences.

As the Forum prepared this toolkit, an unparalleled community of leaders shared their expertise to benefit everybody. By bringing together competitors, this toolkit cuts through marketing hype and helps those new and overwhelmed by the proliferation of blockchain-based solutions.

MODULE

Ecosystem

Overview

Focus Areas

1. Proving the ecosystem value
2. The need for ecosystem collaboration with blockchain
3. Potential blockchain collaboration models
4. Typical roles in a blockchain ecosystem
5. Ecosystem governance
6. Short-term versus long-term value drivers

Tools and Resources

7. Essential steps and questions when forming an ecosystem

Overview

Blockchain is most effective when used to automate cross-enterprise workflows, thereby enabling business processes and the sharing of data across enterprise boundaries. However, doing so effectively requires an ecosystem with an agreed-upon governance structure defining the roles and behaviours of participants, how and what information will be shared amongst participants, data ownership, entrance and exit criteria and funding.

A distributed ledger carries some notable advantages, including decentralisation, greater flexibility, greater transparency, audit trail, independence, and more. But, like any new technology deployed in an organisation's day-to-day operation, blockchain carries additional considerations as well, such as managing what information is appropriate to put on the network and who gets to write that information to the shared chain. Thinking through such issues early on, and planning accordingly to manage them, is vital to a project's success.

1. Proving the ecosystem value

How does an organisation adapt its planning and development practices to suit the unique characteristics of this emerging technology?

Distributed ledger technology enables cross-enterprise collaboration and is the ultimate in networked technology, designed from the ground up to be decentralised. This opens exciting new possibilities in terms of delivering functionality to customers and employees, but for most organisations, it also means adopting new workflows and ways of thinking through development projects from the earliest planning stage.

The first crucial step is to identify an appropriate use case for blockchain – something that it can do better than an existing solution to improve an organisation's operation. For some use cases – for instance, a database that is infrequently updated and only used by one or two staffers in their work – it may make sense to stick with a traditional solution. But for other cases – for instance, data shared among dozens of stakeholders who could benefit from real-time information sharing – a blockchain might work better.

Following identification of a viable use case, it is vital to prove the business value that will be realised from a new project for **all stakeholders,** including both in-house employees and external partners.

Figure 2.1 – This module focuses on steps 2 and 3

Blockchain applications are premised on peer-to-peer engagement using shared ledgers that enable exchange of information and management of business processes across an ecosystem. Blockchain technology supports collaboration while maintaining independence. Using blockchain, one can automate a business process and select what information can be made available to specific participants in an ecosystem. For example, an organisation may not wish for a customer to see improvements made in safety stock levels or cycle time as that would give them negotiating leverage and reduce the ability to reprioritise work based on demand. While blockchain can provide that visibility, an organisation decides what information to share and with whom.

Because of these characteristics, the deployment of blockchain solutions requires a shift to thinking in terms of the ecosystem of these stakeholders, some within an organisation and some without, in order to take advantage of blockchain's trust and transparency features.

In order to deploy responsibly, it is necessary to analyse the ecosystem and clearly understand incentives and dynamics.

Recommended References from World Economic Forum before your start with the toolkit:

- Blockchain Beyond the Hype[28]
- Building Value with Blockchain Technology: How to Evaluate Blockchain's Benefits[29]
- These 11 questions will help you decide if blockchain is right for your business[30]

Example

Finboot[31] technologies delivered a solution involving airport logistics group, in which an ecosystem of airlines, fuellers and in-to-planes (logistics operators) participated. This implementation optimised the reconciliation of refuelling services. However, the solution focused on selective disclosure of the data registered on blockchain to make sure efficiencies gained don't compromise competing interests.

2. The need for ecosystem collaboration with blockchain

Why is an ecosystem both an essential component for a blockchain solution and the reason most solutions fail to scale?

An organisation has selected the right use case and proved through a rigorous business value assessment that a blockchain solution will provide unique and sustainable business value. Now it is time to scale that solution across multiple supply-chain partners.

As blockchain projects almost always involve cross-enterprise workflows, collaboration is a critical success factor that needs to be considered at proof-of-value (PoV) time. Since information in a blockchain project will usually be shared across multiple supply-chain participants, it is important to consider how the ecosystem will operate and be governed.

Conversely, a lack of ecosystem thinking, and up-front planning have already hampered several blockchain projects in the supply-chain space. This is why there have been many PoVs for blockchain solutions in the space, but few deployed into production.

Ecosystems enable integration across enterprise boundaries, allowing organisations to deliver products or services that they would otherwise not have the technological capabilities to deliver on their own, nor the end-customer understanding to imagine. An ecosystem mindset allows organisations to move beyond what's traditionally possible for them within the confines of their own vertically integrated operations, as well as the dynamic limitations of a particular supply-chain network.

It is worth noting that ecosystems exist for a variety of reasons. Typically, there are a couple primary drivers emerging. The first is a closed ecosystem where all participants are involved in the production of a good or service. For example, a prominent apparel manufacturing company, invited all its suppliers (from Tier 1 to Tier 3) onto a blockchain system for tracking the lifecycle of a t-shirt from yarn to consumer. At the other end of the spectrum are industry-wide consortia to for example drive better visibility to provenance of fair-trade items such as coffee or palm-oil might. These ecosystems have very different requirements and governance. Services are ever more valuable as additional buyers and sellers participate in the ecosystem.

Most successful ecosystems start out small and expand. Starting big has proven difficult and produced few successes. The most effective model seems to be one in which a leader establishes the workflow and governance to produce quick benefits while enabling the future buildout of the ecosystem. As the network matures, network governance and operations adapt to the evolving needs of participants, often including new entrants.

Notably, technology providers have begun to document different generalised models for managing an ecosystem, including the concept of a minimum viable ecosystem (MVE) and the prime tenant model. While it will be interesting to keep an eye on the development of these models over the next few years, the important thing for now is that these models all seem to share the premise of starting out small with an ecosystem an organisation can control, then build from there.

At the early stages, this might entail starting with a supply chain for just one product line that expands as the organisation gains experience and can clearly

> *Ecosystems require managers to think about business challenges in a new way. The traditional focus on maximising profits within the boundaries of the company may be the very thing that keeps companies from engaging and succeeding with participation in an ecosystem.*
>
> **Jesper Mathias Nielsen,** Manager, Deloitte

Example

SAP's Blockchain powered industry alliance, SUSTAIN,[32] brings together palm growers, palm oil processors, consumer goods manufacturers, non-profit organisations, and other relevant stakeholders.

Example

OneAgrix,[33] a Singapore-based online marketplace for halal products, has implemented a blockchain system powered by Origin Trail that enables consumers to check the provenance of any products, including its halal certifications.

Example

Repsol,[34] the Spanish oil and energy giant, started out with a PoV in one business unit, which then turned into an industrial pilot and then, as of July 2019 has scaled to a digital solution used in 4 industrial complexes and 2 business units.

quantify the advantages of using blockchain. The solution can then grow to encompass multiple product lines and potentially establish industry standards.

Figure 2.2 shows a blockchain network for a food traceability use case. Blockchain solutions have been formed around existing smaller ecosystems. Participating in an ecosystem is becoming increasingly in vogue as doing so allows companies to move beyond what's traditionally possible for them within the capability confines of a vertically integrated organisation and the dynamic limitations of a supply network. Ecosystems allow organisations to deliver products or services that they would otherwise not have the technological capabilities to deliver nor the end-customer understanding to imagine. Figure 2.3 illustrates how global supply chains are increasingly intersecting multiple ecosystems.

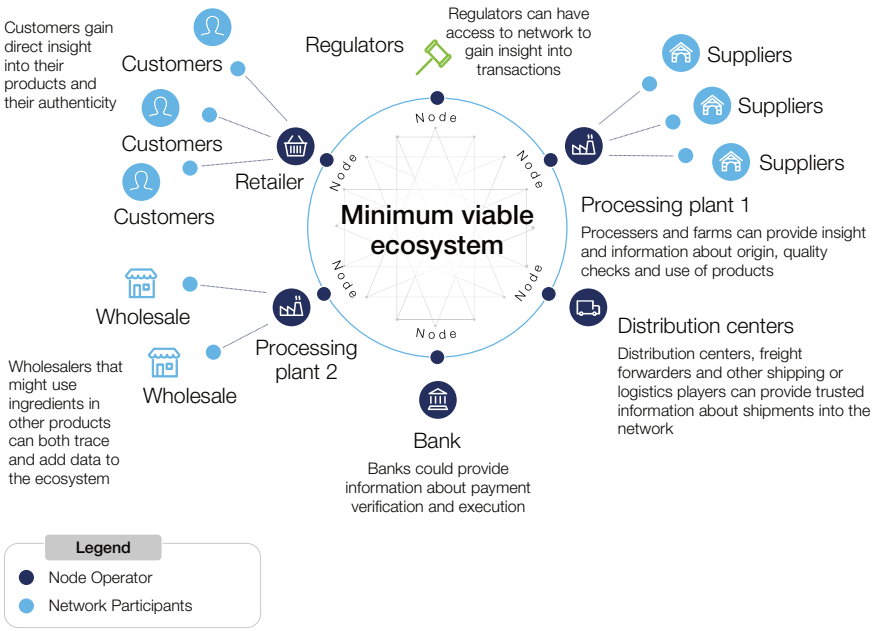


Figure 2.2 – Illustrative example of a network of participants for a supply-chain traceability use case[35]

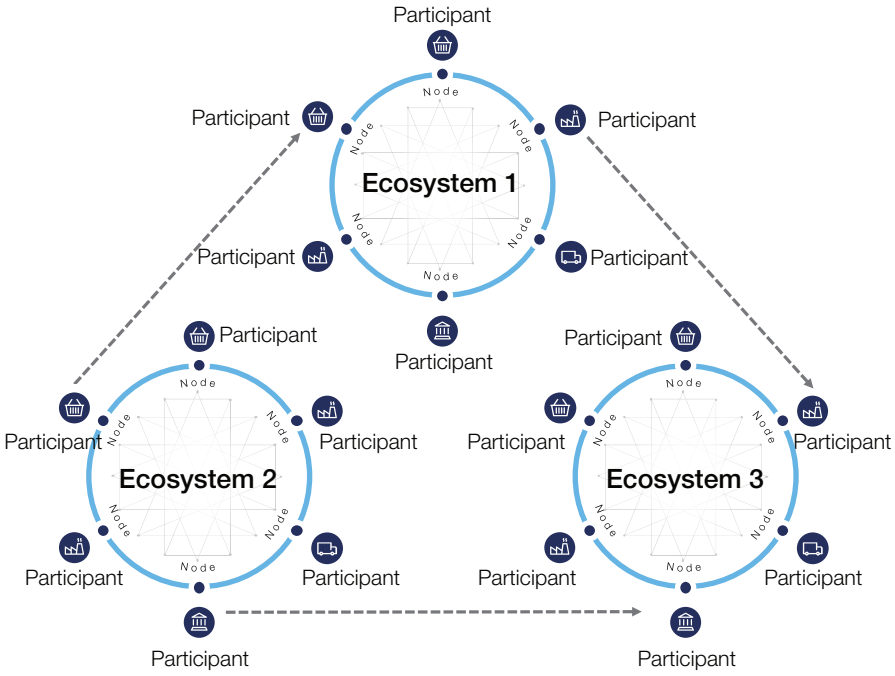


Figure 2.3 – Global supply chains intersect multiple ecosystems[36]

3. Potential blockchain collaboration models

What are the various partnership models through which a blockchain ecosystem organises today?

As shown in Figure 2.2, a blockchain ecosystem can be thought of as **a network of participants** with shared business processes and relationships that create and allocate business value. A blockchain is a complex alliance that will generally involve several to many actors with shared objectives, but unique points of view on how to achieve those objectives.[37]

The individual participants may have different business models, different roles in the ecosystem, or even be competitors. What binds them together and enables the ecosystem is the business value it provides for each participant.

In that context, selecting a model for a shared blockchain project depends on who needs to participate to enable the network to be most effective. The initial model can also evolve into other models as more participants join the network as previously discussed.

A brief overview of some of the collaboration models that have been used in the supply-chain space so far:

- **One-party led:** Single-party blockchain projects enable cross-enterprise workflow for mutual benefit. For example, Bumble Bee Foods[38] has united several stakeholders of the fishing industry, leading an effort to track-and-trace of yellowfin tuna from the Indonesian ocean to the dinner table.

  More on Bumble Bee solution:[39] All the various stakeholders of the fishing ecosystem, who take the fish from the sea to the packagers, transporters, distributors and retailers will be able to record details of yellowfin tuna on blockchain technology. This information will be available on the customer front QR code which would boost customer's confidence about the food they eat. Bumble Bee operates in a complex ecosystem with multiple stakeholders with highly focused businesses. As an external big player with bird's eye view – it makes strategic sense for Bumble Bee to lead this as a one-party initiative and revolutionise the food supply chain.

- **Strategic business associations like a joint venture (JV) or consortium:** These are examples of associations with two or more organisations or governments with the objective of participating in a common activity or pooling their resources for achieving a common goal.[40] A looser consortium model is increasingly prevalent in the blockchain space, even in lieu of a more formal JV, because in many instances the latter is just too complicated.

  A key question to ask when forming a strategic business association, is whether the group should form a new legal entity, or simply enter into a formal contractual arrangement among the consortium members. This decision will be driven by many considerations, including tax, financing and regulatory requirements.

  See the module Consortium Formation on more details for developing a consortium.

Example

BunkerTrace[41] is a JV between Forecast Technology Limited and BLOC (Blockchain Labs for Open Collaboration), a solution used to track marine fuel.

Examples

OneAgrix,[42] a B2B marketplace that enables consumers to check the provenance and halal certifications of food items.

The Institutes RiskBlock Alliance, which helps bring together risk-management professionals, insurers, and blockchain developers to work on industry-specific use cases.

- **Regulatory:** This category includes shared projects among government agencies or parties that have to report to themselves to help ensure compliance verification. A good example here would be the shared project between Marine Transport International and the Recycling Association to use a blockchain-based tool to capture data and satisfy compliance requirements concerning shipments of recyclable waste from Britain.

Within all three above-mentioned business models, one of the most critical considerations is how the ecosystem will be funded. Business model funding is somewhat independent of the ecosystem model and can include for-profit versus non-profit, annual contribution, fee for service, transactional fees or some mixture. There is a clear cost to connect to the ecosystem and deliver on the organisation's individual responsibilities as a member, but there are also resource considerations and funding for the governance and operations that will be required. All must be identified and taken into account as the ecosystem is established.

These matters are explored in further detail in the subsequent modules Consortium Formation and Consortium Governance.

> *Benefits from a blockchain solution are not homogenous across the value chain. The success of the implementation lies in the capturing the varied benefits across the network and turning them into a strategic advantage.*
>
> **George Bailey,** Managing Director, Digital Supply Chain Institute

4. Typical roles in a blockchain ecosystem

What are the roles and responsibilities of each participant in an ecosystem?

Who brings what to the table?

In an ecosystem, the participants are those who are involved in the workflow that is being automated. Typically, those entities make up the supply chain and collectively participate in the production of goods or services. For a blockchain project to succeed, each participant in the ecosystem will need to contribute data and resources that are beneficial to the others.

There may also be users of the information that do not actively contribute to the production of the goods or services at hand. For instance, a user might be a consumer who wants to verify that the product they are purchasing was sustainably produced, while other participants in the ecosystem might be parties involved in the production or handling of the product who need to update data about its shipment, related payments, and compliance.

When planning for the ecosystem, it is critical to identify the actors to be included and identify how they interact from a business perspective. Below identify key participant relationships:

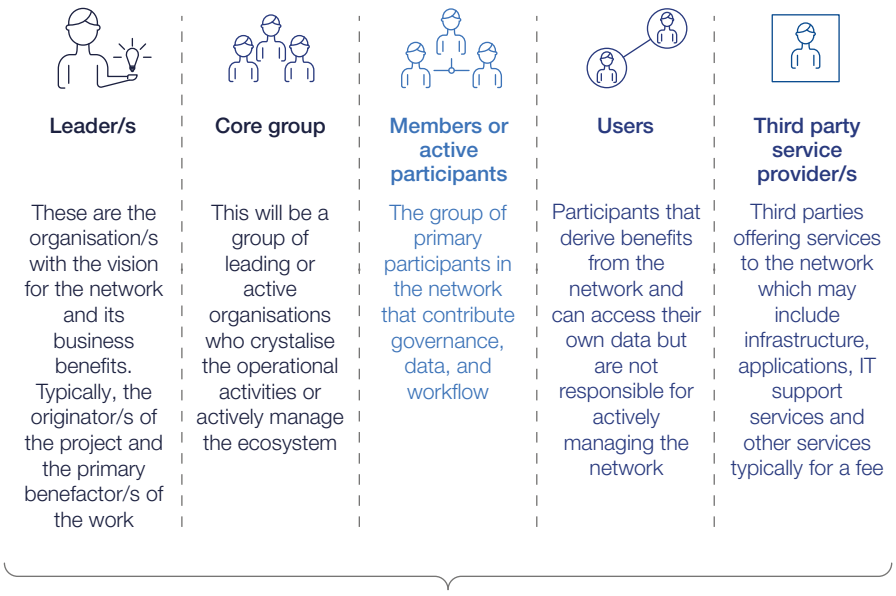


Figure 2.4 – Participants in a typical ecosystem

Participants will at least need to take one of the above roles. However, in most cases, they will take up or participate in multiple roles.

Every participant must commit to a shared network that provides benefits for others, because each participant's success is, at the core, based on the success of the group.

For a tool to assist with the mapping of actors and their different interactions, see the module Digital Identity and more specifically the tool Table: Mapping out actors and interactions.

A blockchain network - roles and responsibilities

Hyperledger explains a **blockchain network** as follows: A blockchain network is a technical infrastructure that provides ledger and smart contract services to applications. Primarily, smart contracts are used to generate transactions which are subsequently distributed to every peer node in the network where they are immutably recorded on their copy of the ledger. The users of applications might be end users using client applications or blockchain network administrators. In most cases, multiple organisations come together as a consortium to form the network and their permissions are determined by a set of policies that are agreed by the consortium when the network is originally configured (more on consortium formation in the module Consortium Formation).

Context matters

The perspective of the user of this toolkit might differ depending on the user's role within their organisation. A businessperson, such as a supply-chain leader, will view the ecosystem from a perspective of good and services that move across the network including purchase orders and invoices along with the automation of associated business process. A systems person will be more interested in the technical architecture of the network, connection of the nodes and how data moves across the network and how processes or smart contracts are triggered.

Understanding the different roles at both a business and system level, requires an understanding of the variants and awareness of the context. In any discussion on the topic, it is hence important to align on the verbiage and terminology used. Take for instance the term 'network participant'. A businessperson might use 'network participant' to refer to a group of people/organisations working together on a common goal with blockchain technology (many times the same connotation as with 'ecosystem') whether through a consortium, JV or other collaboration model. A more technical perspective will possibly refer to 'network' as one layer in the technology stack and basically comprising of the 'network nodes' (so which organisations are node operators where the type of protocol, consensus mechanism etc is relevant). In this context, widely used, network participants are users of the blockchain network that are involved in operational governance.

Following are blockchain-related roles that an organisation is likely to come across.

Different types of permissions are granted to participants of a blockchain network:[43]

- Read: Who can access the ledger and see transactions
- Write: Who can generate transactions and send them to the network
- Commit: Who can update the state of ledger

Another way to look at roles on the network level:

- Data providers: Members of the network who write and commit data to the network
- Data users: Typically the readers of the network
- Some users may play both of the above roles
- Validators: a blockchain validator is responsible for verifying transactions within a blockchain

The naming and specifics of these roles may vary depending on the protocol and other variables in question. For example, in Hyperledger Fabric, the roles are broken down as:[44] [45]

- **Peer nodes:** The blockchain network is comprised primarily of a set of peer nodes (or, simply, peers). Peers are a fundamental element of the network, form the basis for a blockchain network and host ledgers and smart contracts. Peers maintain the state of the network and a copy of the ledger.
- **Clients:** Clients are applications that act on behalf of a person to propose transactions on the network.
- **Orderers:** The mechanism by which applications and peers interact with each other to ensure that every peer's ledger is kept consistent with each other is mediated by special nodes called orderers. The ordering service accepts endorsed transactions, orders them into a block, and delivers the blocks to the committing peers.

Agreed roles and responsibilities are necessary

The table below uses the roles outlined above to illustrate how business relationships and systems-level relationships might intermingle. When designing an ecosystem, it will be helpful to identify the role for each participant at a business level and at the system level (Table 2.1 provides a simplified matrix which could be useful for this task):

Table 2.1 – Simplified overview and example of identifying roles and responsibilities

Roles	System level designations	Permissions
Leaders	Data owners/users	Readers
Core group	Data owners/providers/users/ validators	Readers/writers
Members	Data providers/users/validators	Writers/node operators
Users	Data providers/users	Readers/writers

5. Ecosystem governance

What are the key governance considerations when forming a blockchain ecosystem?

Establishing an ecosystem with the associated governance is a complex undertaking that needs to be driven by the business owner. It is important to note that one governance structure may enable the startup of the network while a different structure may enable scaling, such as when additional competitors begin to participate. So, the need for agility, as the ecosystem grow and develop, will be necessary. This gets into the complexity of scaling.

While the rewards from collaboration can be high, agreeing on what constitutes a fair and well-designed consortia governance system, let alone a joint blockchain platform, can be challenging. This is where many industry collaboration efforts have fallen apart. Ultimately, all parties must get benefits from participation in the network. It is unlikely that anyone will participate if such participation creates additional work for them without clear benefits.

In addition to establishing the network and defining business and technical governance, there are many legal considerations to starting a new project successfully. A more detailed discussion is taken up in the subsequent modules – see Consortium Formation, Consortium Governance and Legal and Regulatory Compliance.

6. Short-term versus long-term value drivers

Has one considered both the short-term and long-term value propositions for the ecosystem?

During formation of a business-focused ecosystem (or more formally a consortium) it is critical to reach agreement on not just the initial value levers to be pursued by the ecosystem but also the longer-term vision to be pursued. See the module Consortium Formation on more details for developing vision for a consortium. The value drivers will evolve over time as participants better understand the value of digitising their supply chains.

An example to illustrate this short-term versus long-term dilemma: The ecosystem will likely have to opt for a specific blockchain technology stack as part of pursuing its initial set of value levers. Typically, blockchain technology is only a part of an overall solution and will need to interface with Enterprise Resource Planning systems and other IT systems including, possibly, other blockchain architectures that may differ by participant.

Establishing the appropriate governance and management practice is essential to enabling the ecosystem to evolve to the dynamic needs of its participants.

TOOLS AND RESOURCES

7. Essential steps and questions when forming an ecosystem

Below is a list of five key steps and questions to ask when forming an ecosystem. When designing a blockchain ecosystem, it is important to address these key steps and questions to ensure that an organisation has a model that can provide the expected business benefits for the organisation and other ecosystem participants.

Navigating these considerations requires project managers to have in-depth understanding of the targeted ecosystem and the full-backing of C-suite executives.

It is also worth noting that proper consideration of an ecosystem design and dynamics will not guarantee success of the project. But an ill-conceived ecosystem will almost certainly result in failure. In fact, it is the most common reason for not achieving desired results.[46]

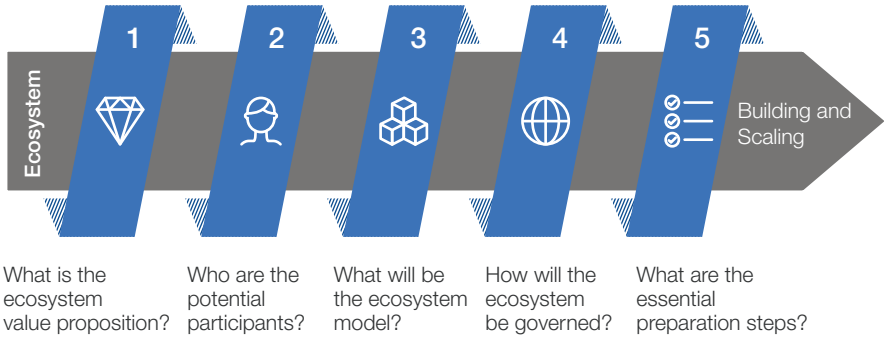


Figure 2.5 – Summary of key steps and questions in building and scaling the ecosystem

Step 1: Ecosystem value proposition

As always, the journey starts by defining why the organisations involved are pursuing a joint blockchain solution. This step includes defining the issues to tackle and fundamental purpose of the ecosystem's actions.

These are some questions to ask:

- What business problem does the proposed solution address for the ecosystem as a whole?
- How would the blockchain-enabled solution impact each of the currently involved participants and what value propositions will the participants in the ecosystem be able to reach consensus on pursuing?

Step 2: Expected participants

Now it is important to answer a big question from the perspective of those who are essential participants in the ecosystem: Will they want to invest in blockchain and view it as the essential technology?

This is where most organisations fall down. They go off and say, “Let me try blockchain.” But they don’t have a set of success objectives and overlook involving others. It is important during the PoV to involve potential ecosystem members. Safe to say that if not, then the organisation will likely miss some of the key design points that will incentivise them to participate in the future.

These are some questions to ask:

- Who are the target participants, and why would they want to join the ecosystem?
- Why would target participants find the new value proposition and solution desirable?
- What are the incentives for each of the required participants to engage in the ecosystem, and how does the blockchain solution form a viable business future for them?
- Will the ecosystem be open or closed?
- How does the currently available blockchain technology enable the envisioned value propositions?
- Who are the necessary participants to be successful? What is the MVE?

Step 3: Ecosystem model

An organisation will start to have an idea on which collaboration model will be a best fit for their purpose.

These are some questions to ask:

- Which of (a) one-party led, (b) strategic business association, or (c) regulatory is the best model? Any other arrangement makes most sense?
- How might the model need to change over time?

Step 4: Ecosystem governance

It is important to consider early on who will operate the network and how it will be governed. The characteristics of the network will help determine the desired structure. Governance specific for a consortium model is explored in more detail in the module Governance Consortium and early considerations in the module Consortium Formation.

More detailed questions to ask:

- For the value propositions agreed to under step 1, what consortium governance will be required to bring it to life?
- What governance model will constitute a fair, scalable and robust arrangement for all?
- How will value and cost from the blockchain solution be fairly allocated?

Step 5: Organisation's preparation

At this stage in the process, each organisation should have some idea about what benefit it might derive from joining the proposed ecosystem. It should, however, conduct more detailed due diligence at this point before proceeding further.

A few important questions to ask:

- What are resources and necessary capabilities for initial development of the ecosystem?
- Is the proposed solution lawful?
- What are key risks and possible missteps?

MODULE

Consortium Formation

Overview

Focus Areas

1. Prevalence of consortia in scaling blockchain solutions
2. To join or not to join a consortium
3. Blockchain consortia landscape
4. Different consortium elements and deliverables
5. Blockchain consortium business models
6. Navigating the pre-consortium agreement: key to-do's
7. Navigating the pre-consortium agreement: key considerations
8. Learning from others: key lessons

Tools and Resources

9. Main steps to take when forming a consortium
10. The pre-consortium agreement: issues to resolve

Overview

Among and across supply chains, one common approach to blockchain exploration and adoption that has emerged is to form a consortium among multiple stakeholders with the intent to create, deploy, accelerate, and scale industry-wide solutions. The consortium model allows participants to take advantage of blockchain technology by balancing the benefits, which often include allowing competitors to collaborate to create decentralised networked solutions to solve shared problems, while also protecting their competitive advantage individually, keeping sensitive data confidential.

As this technology continues to emerge, the consortium approach can take Research and Development (R&D) to the next level beyond what an enterprise may be able to achieve alone to develop new blockchain solutions that address specific supply-chain use cases. The consortium can evolve as the solutions are deployed to encourage adoption, create standards, and interoperate with other business organisations and additional consortia. For example, a proof-of-concept (PoC) may start out in-house at a single company or with a small group of participants within an industry, then grow over time in terms vertical and horizontal participation, technical sophistication, or both.

FOCUS AREAS

1. Prevalence of consortia in scaling blockchain solutions

Why do supply-chain organisations often form consortia as vehicles to explore the potential of blockchain? What about the technology lends itself to this collaboration model in particular?

The module Ecosystem emphasised the importance of proving the business value of blockchain for all stakeholders, not just an organisation. It also explained the key drivers with blockchain technology that encourage collaboration; in that blockchain is the ultimate distributed networked technology that offers the opportunity to re-allocate trust in a decentralised manner, and collaboration is required to reap the benefits. This module will focus on consortia - one prominent method and model that organisations are using today to organise collaboration and create network effects – and more specifically on the early stages of consortium formation.

Collaborative business structures are not new. Joint ventures (JVs) and consortia have operated for decades. So what is it about blockchain that particularly lends itself to consortium-based business arrangements?

One hint lies in the longstanding history and culture of open technical standards[47] – an area of technology that has largely operated on a consortium model dating back at least to the 1990s. These types of business arrangements have continuously and successfully operated for years.

As blockchain technology has emerged beginning with publication of Bitcoin whitepaper in 2009[48] and more recently started to gain traction, many of the popular distributed-ledger protocols have also been openly licensed. To support the development, use, and interoperability of these protocols, industry consortia have coalesced around them, extending the organisational structure and tradition of open-source software previously established in projects like the original development of the World Wide Web and Linux operating system.

Of course, JVs exist throughout many different industries. Yet a looser consortium model is increasingly prevalent in the blockchain space, even in lieu of a more formal JV, because in many instances the latter is just too complicated. In the 2019 Deloitte Global Blockchain survey,[49] 81% of the participants surveyed responded that they are already participating in a blockchain-related consortium or will join one in the next 12 months.

The consortium model is especially useful as a way for competitors to organise themselves[50] when approaching emerging decentralised software solutions as collaboration is needed to take advantage of the true benefits that blockchain technology has to offer. As the global business environment becomes more competitive due to emerging technologies and digital transformation, and understanding that blockchain is a team sport, “coopetition” is born.

Competitors and other participants within the same industry who are researching and experimenting with blockchain technology may form a variety of consortia to take their R&D to the next level or to develop joint blockchain digital platforms, even while remaining strategic rivals. For example, they may still compete by building rival applications on top of the blockchain platform they are jointly maintaining via a consortium.

The consortium arrangement often forms organically with a few companies or among participants in an ecosystem or even through an initiative of some

> *Blockchain-based collaboration cannot come from a single company. Industry collaboration has to proactively drive disruption, innovation, and transformation throughout the industry by identifying and modeling areas where distributed autonomous software agents can transact on behalf of people, businesses, and things.*
>
> **Henrik Hvid Jensen,** Senior Blockchain Adviser, Trustworks

participants within a single company who are interested in exploring blockchain technology further. They may start out with a PoC in-house or with a small group of participants within an industry or across a market vertical.

When such experiments succeed and begin to grow in usage, it may be necessary to work more formally with other industry competitors, suppliers, and participants to enable interoperability, set more stringent data and protocol standards, and to ensure industry-wide adoption. At this stage, the formation of a consortium is one approach.

At this point, careful thought about the consortium formation is required because the size of a consortium can grow quickly.

There are several key questions that one should consider before determining which type of consortium, new or existing, is right for the organisation. These questions include the following:

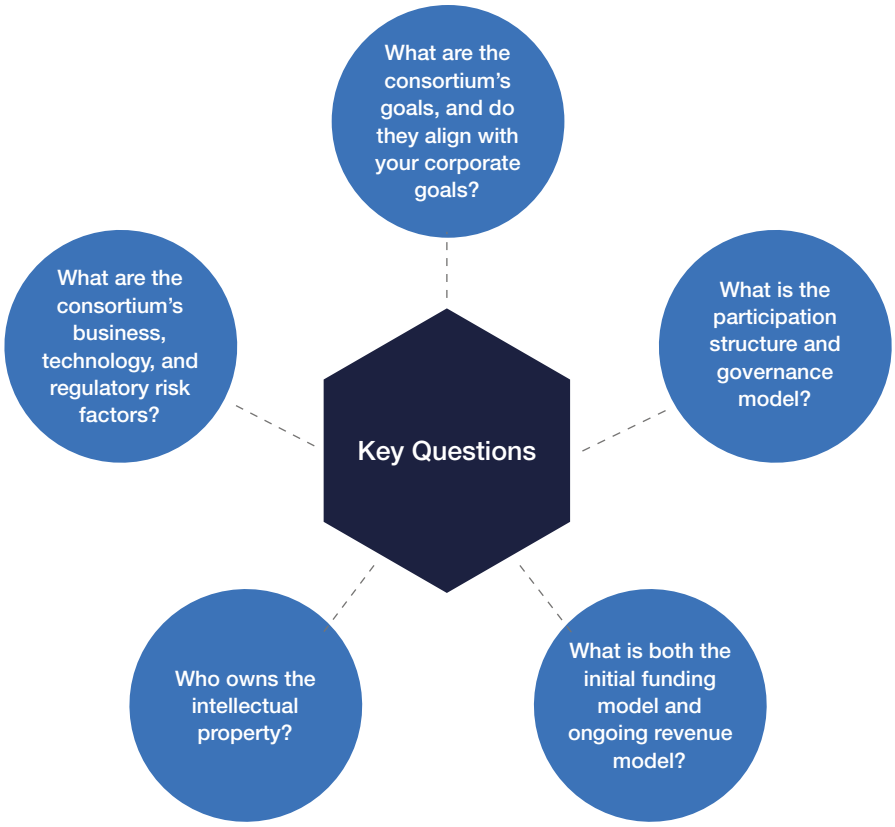


Figure 3.1 – A rapid analysis of whether a new or existing blockchain consortium is right for the use case and organisation

Example

The R3[51] consortium started in September 2015 with nine banks and have since evolved and grown. By December 2015 there were forty-two members. Such rapid growth can destabilise a consortium if the right rules that allow for the growth and evolution of the group are not in place from the beginning. Setting best practices for the consortium at the outset is critical. With the right structures in place, a consortium can thrive and build on its successes.

2. To join or not to join a consortium

Is there a blockchain consortium that is already active in the industry that can tackle a specific use case, or one already working on a similar problem?

If a consortium in the industry exists, what is its size in terms of market share? What is the progress of the consortium? These questions are essential to analyse whether it makes sense to join an already established group or form a new one. A cost-benefit analysis is therefore recommended when making such a choice.

Before pursuing a blockchain solution, decision-makers need to think hard about whether they wish to join a blockchain consortium or trade partnership that is already active in the respective industry or specific to their desired use case.

It is often substantially cheaper and less time-consuming to accept an imperfect solution over a custom one. After all, the latter tend to become useless in cases where a consortium solution eventually morphs into an industry standard.

Obviously, if organisations believe they can mount a credible challenge to existing solutions, gain critical mass to make them successful, and possibly become a dominant solution, designing and owning that solution is a viable strategic option.

To a lesser degree, the same question is true for initiatives within an organisation. If there are ongoing blockchain projects or deployments within the organisation, it is often easier and faster to leverage those existing resources before embarking on a second or third initiative that leverages a new platform or protocol. In this way, all previous investments can be leveraged.

> *Convince your organisation to accept a 'shared endeavour' mindset; Blockchain/DLT (distributed ledger technology) is a team sport! Be prepared to share development, share maintenance and share operations to truly take advantage of the network effects that will present themselves. Education of the decisionmaking organisational layers in the business as to the real value of DLT is key, thereby dispelling myths associated with the technology.*
>
> **Bob Crozier,** Head of Allianz Global Blockchain Center of Competence and B3i Board Member

What makes collaboration in a blockchain consortium appealing?

Much of this has to do with the very nature and architecture of the technology itself. It is often said that blockchain is a "team sport". This is because the technology is at once: a) nascent, b) distributed in nature, and c) there is necessary involvement of business people and technologists to work together to create and apply solutions. Including:

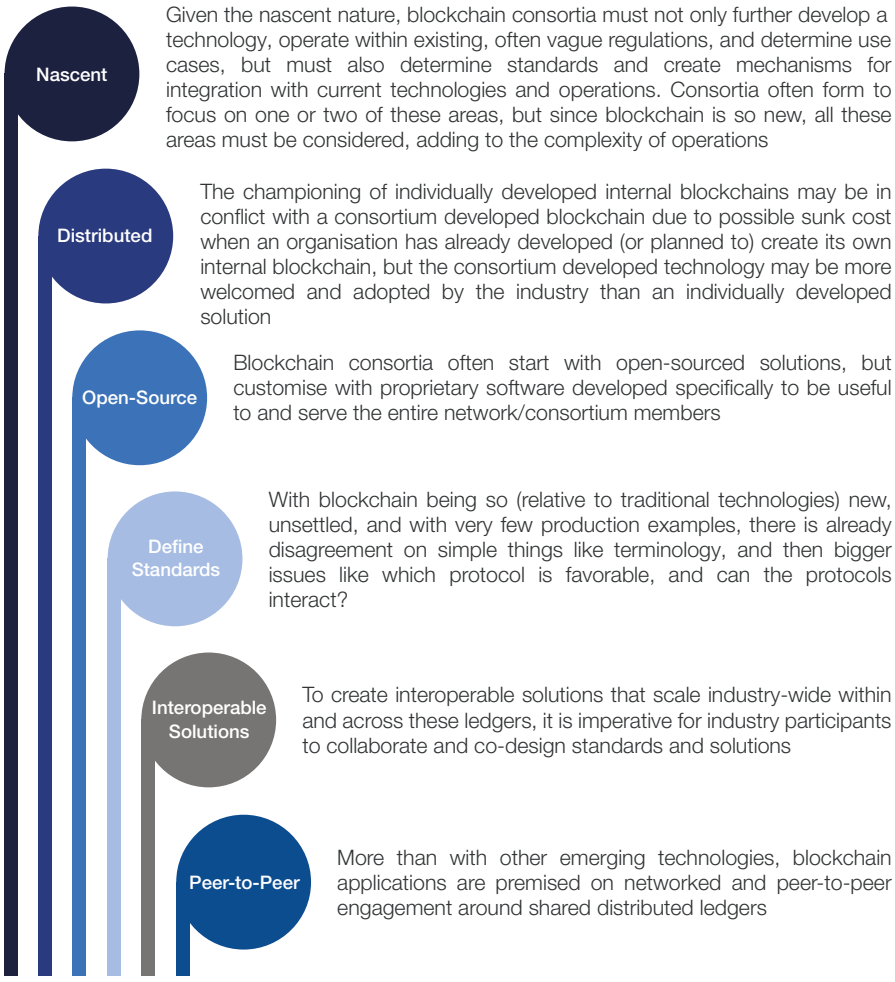


Figure 3.2 – Blockchain is a team sport – it requires collaboration to truly unlock the benefits of its features

3. Blockchain consortia landscape

Which types of blockchain consortia are prevalent today?

Today's blockchain consortia are organised in varying ways and can evolve over time to accommodate more than their initial purpose. One issue to resolve and a common question an enterprise asks is whether it should join more than one consortium. The best way to frame this inquiry is to ask what business problem the enterprise is trying to solve,[52] and which group or groups are addressing these issues. It may be that more than one group or technology protocol is being tested for a particular solution, and varying levels of interoperability may exist in different protocols. Since the real world is early on in the evolution of the technology, there may be several groups to join to test different solutions.

Common ways for groups to organise can be seen as a continuum ranging from those who form around protocols, standards, business verticals, business horizontals, or government-mandated groups. Increasingly, interoperability is becoming a focal point for these groups. Because there are so many ways in which consortia are organised and different groups offer different solutions, businesses may find it necessary to join more than one consortium.

Following is one way to think about how a consortium today can be organised.

Business-led and government mandated consortium: In this model, collaborating companies or regulated entities seek to solve a common business problem or facilitate improved processes among themselves. These groups can be organised by vertical or horizontal participants.

Protocol-led consortium: This model of a blockchain consortium is formed to develop and maintain a specific blockchain protocol, usually regardless of industry or use case. These types of consortia can evolve to add business groups that address specific use cases on top of the protocol so that there are consortia or groups hosted on top of an original consortium.

Standards-led consortium: This type of consortium typically convenes participants within the same industry or field to develop blockchain standards in order to unlock interoperability and new business models. This type of ecosystem may not develop a blockchain solution at all, or it may include a variety of tech providers to test several different possible solutions.

Figure 3.3 – One way to think about the different types of consortia out there

4. Different consortium elements and deliverables

Which type of blockchain consortium should be formed?

A consortium should understand its purpose and relationships both internally and externally. The planning for this type of business arrangement requires

analysis and agreement regarding different elements of the relationship, possibly including deliverables and business structure, among other things.

Collaborative deliverables for a blockchain consortium can take many forms. The following are typical deliverables prevalent in many blockchain consortia to date. In such groups, it has so far been common for members to:

- **Design and develop a common blockchain-based digital platform and/or application for a given industry or ecosystem.** This typically starts with a joint PoC for a shared digitised platform to reduce friction, cost and accelerate adoption to test collaboration among organisations. The blockchain platform will have an agreed-upon technical architecture, platforms neutrality, and no vendor lock-in, with a goal of shared processes to reduce friction, minimise cost, and accelerate adoption. Further, a decentralised infrastructure should be able to support legacy centralised apps on top of the blockchain framework. Backward integration tools to existing systems should also be provided.

Example

India[53] blockchain ecosystem to insulate telco subscribers from Unsolicited Commercial Calls and Text mandated by Telecom Regulatory Authority of India (TRAI). This consortium began as a PoC by Microsoft, Tech Mahindra and IBM and later on became mandated by regulators.

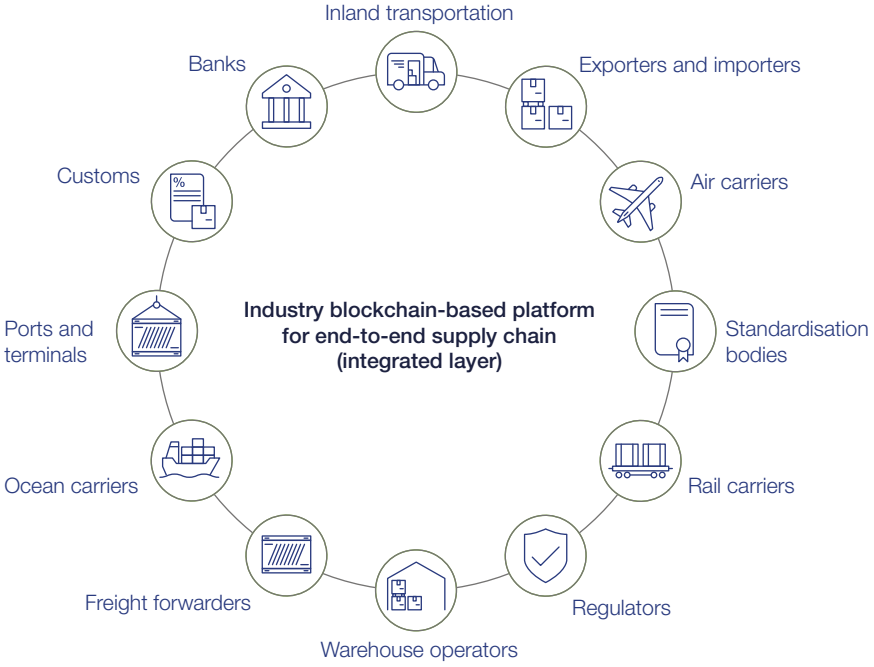


Figure 3.4 – Example of an industry blockchain-based platform for end-to-end supply chain (industry integrated layer).

- **Set industry standards.** Consortium partners often seek to complement and accelerate existing standardisation efforts on data and protocols. After a PoC is made in-house, perhaps at one partner company, it is critical for organisations to work with other industry competitors, suppliers and participants to set standards as the PoC is further developed into a production-ready solution.
- **Share research and development.** Consortia often serve as a handy tool to do industry-specific open innovation. This may take the form of an open-source working group dedicated to collaborative R&D around blockchain technology. Such working groups may also seek to identify desirable, feasible, and viable industry use cases. They also enable industry participants to learn from and build upon one another's work.

5. Blockchain consortium business models

What types of business structures are useful to consider for a blockchain consortium?

Two of the most common business models for consortium-led blockchain ventures are as:

- **Non-profit entities**
- **For-profit entities**

The non-profit approach may be focused on an industry challenge that has a significant social impact. These groups may operate as open-source projects and have public or third-sector involvement.

Increasingly, there are some enterprise businesses that prefer a non-profit model to protect against potential antitrust concerns. In the case of RiskStream,[54] certain of the insurance industry have organised as a non-profit to create a platform that is a utility for the industry. Enterprises employing this model may use a two-tier approach: create the underlying platform as a non-profit such as RiskStream or create a for-profit ecosystem that sits on top of the platform.

Alternatively, the platform could be created by a for-profit entity and then turned over to a non-profit – likely a foundation or similar entity – that will manage the platform thereafter.

The pure for-profit model is used where development is driven by the private sector and where there is the promise of an exceptional medium-term valuation as seen in many supply-chain ventures. Many blockchain consortia today follow this model. The actual commercial structure may ultimately be spun out as a JV as in the case of the eight banks that joined to form Contour,[55] or they may have a hybrid commercial model where the intellectual property (IP) is helped by just a few members and the technology is leased out by others. These types of spin-outs occur well after the initial pre-consortia steps are taken.

Antitrust issues are a perennial concern for consortia. Caution should be noted in the for-profit scenario regarding possible antitrust claims and checks against collusive behaviour should be strongly monitored and implemented. Regulatory permissions should be obtained when necessary. For instance, TradeLens, a blockchain shipping consortium originally developed by IBM and Maersk GTD, was recently granted an antitrust exemption[56] by the Federal Maritime Commission so that the five major container line shipping companies participating can effectively cooperate in providing data for use on the platform.

Further, providing integration tools are a critical offering. These types of tools might help to allow smaller, less technologically supported and sophisticated entities to join a network which can help neutralise antitrust concerns.

The traditional utility model: another business model

Another model exists that can encourage broad market participation, while also providing initial investors with a means for creating and recouping value around a new platform – the traditional utility model.

In this model, a consortium first provides basic capabilities – network consensus, transaction distribution and verification, basic smart-contract templates, tokenised assets, or digital documents, among other possibilities – as a kind of utility. Usage fees are established using a cost-based model, and any excess revenue is distributed back to all market participants based on some measure of use, such as volume or value channelled through the platform. IP rights are retained by initial investors, participants, or the platform's creators.

This arrangement addresses the issue of founding members having too preferential a position relative to other participants. The consortium can then focus, through a second legal entity, on establishing second-order benefits unlocked through wider adoption and effective use of the base layer.

The graph below shows the range of some blockchain consortia that exist today. Most are organised around a for-profit model, but that does not mean the non-profit model is not viable. In fact, a non-profit environment might lend itself to defusing antitrust challenges. The technology led consortium focuses on standards and tend to offer open-source solutions.

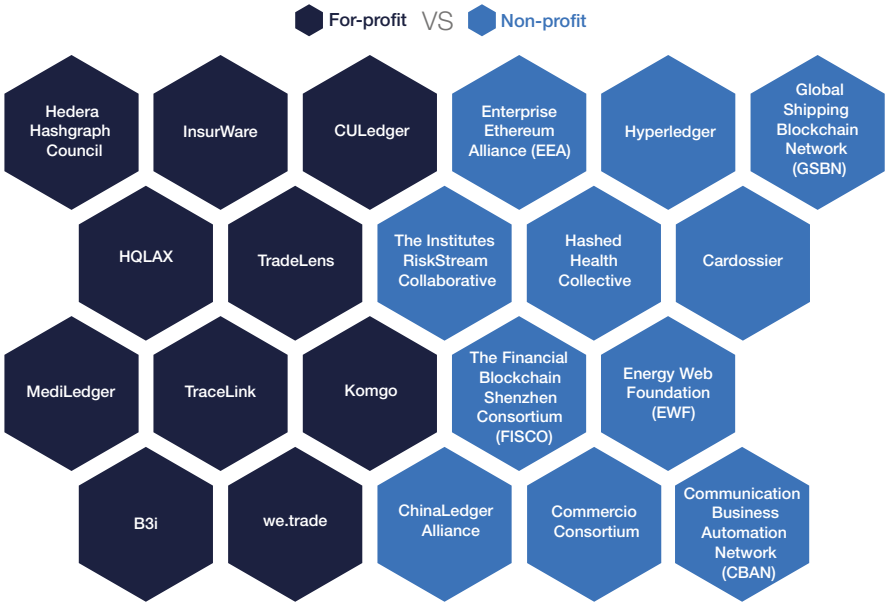


Figure 3.5 – Examples of consortia organised by for-profit versus non-profit (as of January 2020)

6. Navigating the pre-consortium agreement: key to-do's

What are the important steps in creating and setting up the pre-consortium agreement?

A pre-consortium agreement is often used to define the expectations that all parties bring to the table of a new collaboration. Properly done, the pre-consortium negotiation and agreement can act as a road test for the participants to see how they might work together in a more formal relationship in the future.

At the outset, four challenges must be met which collectively can be referred to as the Code of Practice. They include 1) agreement on the set-up of the organisation, 2) enumeration of shared goals, 3) the operating rules and responsibilities, and 4) the memorandum of understanding (MOU) committing the agreement to writing.

1. Define the organisation's business case and structure

Potential consortium members should convene to workshop ideas for use cases, business justification, viability and related factors. They should receive a detailed business value or use case outline with potential return on investment (ROI) suggested. ROI can be more than financial return and may include the assurance that their peers will not outpace them in technology development. There should also be a short-term and long-term version to address areas of concern and garner buy-in. Participants should be provided with information outlining the minimum number of members required to establish a viable ecosystem to support and drive future success. Remember, however, to set realistic expectations. The technology, regulatory, and cooperative platforms for blockchain are all still nascent, and software takes time to collaboratively develop and deploy.

2. Define shared goals and key success factors

Members and potential members should discuss their individual and shared goals for the consortium and establish agreement on key factors related to its purpose, vision, and definition of "success". Members may also want to agree on a pilot use case or PoC. It is important to break the big ideas and vision of a consortium into something that can be implemented.

3. Define operating rules and responsibilities

Once the ecosystem has been defined and analysed, stakeholders have been identified, and a group has come together to engage in common activities, the group should understand and explore how it will set out governing and operating rules. This can be done and documented with a clear delineation of rights and responsibilities. An operating model should be selected and adhered to. Care should be given to antitrust concerns, and plans should be discussed if regulatory permissions are required.

> Consortia always benefit from early alignment and buy-in among potential members.

Members should design and agree upon a governance structure acceptable to all participants including selecting the party who is in charge of facilitating the organisation and coordinating the other members. Members should also agree on how much input or control each participant will have in the consortium, and agree on a regular meeting schedule to address issues relating to the consortium's overall performance and growth potential, and establish appropriate committees and boards to execute on such governance like Board of Directors, Board of Advisors, Business and/or Technical Steering Committees, IP and/or legal committees. Exit and entry procedures should also be agreed upon at the outset.

4. Draft the Memorandum of Understanding

If the group is not yet committed to forming a consortium but wants to try out the group relationship in the context of blockchain activities, the group should consider drafting and entering into pre-consortium agreements in the form of a Memorandum of Understanding (MOU). This document will set out clear rules and responsibilities for participants, as well as the role of the group itself. Even if the group has already decided to create a consortium, C-level buy in, receipt of funding, as well as gathering a large enough participation base can take a long time. MOUs can be used to launch the activities to complete these

steps.

Again, attention should be paid to creating an agreement that does not create antitrust issues.

It is best to document the scope and arrangement in writing so there is a clear allocation of responsibility, risk and liability. MOUs can either be binding or non-binding, and their form is highly flexible and not uniform because their content is determined by the pre-consortium objectives. There are no standard forms or templates. Typically, the MOU addresses goals and priorities, sets out services offered, enforces mutual respect of individual and group organisational practices, provides indemnity and liability, sets out contributions, operations, governance (the module Consortium Governance covers detailed governance considerations), offers amendment/modification processes and rules for exits and new member admission. It is always a good idea to "time" the MOUs and establish a timeframe goals of turning such agreements into official participation contracts.

7. Navigating the pre-consortium agreement: key considerations

What are important pre-consortium agreement considerations?

Consideration 1: Agreement should match group objectives

A blockchain consortium usually involves complex relationships among established industry players working alongside competitors and the start-ups who may be trying to displace them by offering solutions that re-configure existing business relationships or offer new types of technology solutions.

In the midst of these complicated relationships, they are all trying to understand, explore, and create industry solutions using an emerging technology that while increasingly understood, has not yet had its value proven at scale.

In other words, consortia aren't easy by any stretch.

With that in mind, a consortium agreement can provide stability as it spells out formal and detailed rules and responsibilities. Consequently, the consortium agreement may take many months to negotiate. Each member will contribute funds, and/or know-how, equity or some combination of the three, while retaining their separate individual legal status. If the consortium is not a separate legal entity, rights and responsibilities should be set out in the more informal draft documents as mentioned in the previous focus area. Later on, if/when the group is formed separate legal entity, the consortium, takes on the risk, perhaps owns or jointly owns the IP, and governs the activities, including how profits are divided and distributed.

A consortium does not form out of thin air. Usually a few industry players get together in a working group to explore blockchain technology within and across an industry. This working group can be regarded as a "seed group" that precedes the formation of a formal consortium. Not all working groups lead to consortium formation. But those who do can benefit from having a pre-consortium agreement in existence as a roadmap.

Pre-consortium agreements, by contrast, are more flexible than consortium agreements, and are created for the short term or for a very limited purpose.

They are negotiated relatively quickly, and they tend to support a single use case or short-duration research and exploration. Thus entities seeking to build use cases or test concepts often enter into pre-consortium agreements to set expectations, distribute responsibilities, and manage IP. The pre-consortium agreement can represent the "toe in the water" approach to working with others as a group heads toward forming a formal consortium.

Consideration 2: Groups are start-ups by nature

Pre-consortium groups and nascent consortia tend to be leanly staffed and share certain characteristics of start-up companies.[57] Many of these start-up characteristics can be harnessed to enable the group to work effectively to reach its goal.

A blockchain group's agreements are typically created at the initial stage when the group forms to build a solution or set up testing among several parties. Attention should be paid to developing the group's culture which will evolve over time. Often participants may be, in part, competitors, and agreements should be put into place at the outset to avoid uncertainty, misunderstandings, and fallout if the group dissolves or one party leaves. Likewise, provisions should be made to create the ability to add additional members on an ongoing basis or to work with other consortia.

Pre-consortium agreements are generally intended to govern over a short term, but terms from the agreement can carry over to more complicated formal arrangements entered into at a later time as the group evolves. Many of the agreed-upon items – for example, the rights and responsibilities attached to the continuing use of pre-consortium IP – can be later negotiated and folded into a more formal consortium agreement.

This later agreement will include understanding of how contractors will be paid and setting up the requisite bank accounts and tax reporting and designating one or more of the consortium members to act on behalf of the group to handle issues like payments. The pre-consortium group will in all likelihood have to hire independent contractors and vendors. Formal structure should be put in place regarding bank accounts, tax records, and supplier payments. If necessary and agreed to, a separate legal entity can be created to handle those functions. However, jurisdiction and operations will have to be sorted out if a new entity is formed.

Consideration 3: Educate the organisation

When assembling a new MOU that can lead to the formation of a consortium, there is a strong educational component necessary to sell the value of the narrative to the potential stakeholders. Remember, leaders within many potential partner organisations may be unfamiliar with the basics of blockchain technology. Thus, it is paramount to communicate clearly and consistently why a proposed business arrangement leading to a consortium is important and what business value it will bring.

In fact, this educational piece should continue even once the consortium is formed, since software takes time to develop, and members will need to maintain industry support for the long haul. In addition, new partners may enter the consortium over time and need to familiarise themselves with basic information as they enter.

> *Education is a big part of forming any new blockchain consortium. Especially for the sake of new comers to the blockchain space, be clear and consistent in explaining the importance and business value of a potential new consortium.*
>
> **Ashley Lannquist,** Co-Founder, Mobility Open Blockchain Initiative

8. Learning from others: key lessons

What are the key lessons learnt from others who have participated in blockchain consortia?

Figure 3.6 – Lessons and best practices from tested-and-tried consortia and projects

The following is an overview of vital insights and lessons captured by the Forum through research, meetings and interviews with 25+ blockchain consortia in 2019 and 2020.

Appoint an independent executive director who is either a respected industry or experienced consortium leader

When possible and applicable, this leader should ideally leave his or her current job in the industry to work exclusively on the consortium. This establishes a level of industry neutrality that would not be possible if he or she remains affiliated with one particular organisation. This practice also affords the following possibilities, which are invaluable to a new consortium:

- Provides credibility to the venture, both within the industry and with the blockchain ecosystem broadly
- Leverages the director's network to bring in fellow industry participants
- Provides expertise and guidance on initial use cases

Role of an impartial party (nexus / glue / convener)

Many blockchain consortia had an impartial "nexus" organisation involved at the early stages to act as the glue to mobilise collaboration among additional competing organisations. For example, the MOBI consortium worked with the Media Lab at Massachusetts Institute of Technology to play this nexus role, and Energy Web partnered with the Rocky Mountain Institute. This may be especially important during the early days of a consortium, when antitrust policies are still being worked through. Having a "nexus" also provides the new consortium with neutral meeting space early on. The "nexus" also provides an experience level familiar with group formation otherwise unobtainable. However, it is not a prerequisite.

Inclusion of regulators and academics

In order to ensure the activities of the consortium are compliant and using best practices, it is recommended that consortium members involve representatives from regulatory, civil, and academic bodies, particularly if a regulated industry is forming the group. Regulators should be consulted, however need not be a direct part of the operating group.

> *Have a "break-the-ice" kick-off session and get to meet all the participants in person: too many stakeholders not knowing each other's roles and functions good enough can quickly create a project management mess. We advise to have only one key point of contact representing the company that will dispatch the information to their respective internal stakeholders.*
>
> **Nicolas Verschelden,** Managing Partner Dream Tech Alliance, AB InBev

Vertical versus horizonal participation and inclusion

A consortium can be formed either vertically among similar entities within an ecosystem or horizontally across an ecosystem. The consortium should have representation from across the industry. One key question is do members reflect a similar mix of the size and geography to their industry. Care must be taken to be inclusive including gender inclusion of representatives. This is especially imperative to foster true collaborative innovation and technology design, which sets the stage for industry adoption. A new consortium should seek top-tier industry players as well as newer, more specialised technology players. Further, dialogue stemming from an inclusive group garners greater resourcing and richer perspectives, and builds buy-in and validity to technology standards.

Technology and firm agnosticism

It is paramount that the consortium be flexible and capable of technological interoperability. While many consortia may align around and work well with one particular technology, the consortium should be flexible and fluent enough to be able to entertain other technologies. The blockchain space is still in its infancy, and its tools are rapidly evolving even as they are being deployed. Hence, maintaining some flexibility and capability for growth from a technical standpoint is important.

The consortium's management team and board of directors should not be employed full-time at an industry competitive organisation once the consortium has formed as a legal entity. If the group is operating under an MOU, care must be taken so that "seconded" employee loyalties fall to the group goals first, and then to their supporting company. Consortium participants should also be diverse and represent various blockchain protocols and technologies, as well as various industry competitors and participants and not be driven by the interests of one or a few dominant companies.

Further, technology vendor lock-in without interoperability, and potential stack integration issues where solutions are designed to operate only with one technology platform or vendor at the cost of platform flexibility, is a serious risk. Technology silos are to be avoided. Ensuring representation and participation from across platforms alongside interoperability measures and universally applicable data standards is imperative to reduce this risk.

> *Based on our experience, the following are some best practices with blockchain consortia:*
> - *Take an iterative approach to test conceptual assumptions early on.*
> - *Identify the critical stakeholders early on and map their incentives and concerns.*
> - *Incrementally build out the software, including a validation loop after every increment*
> - *Don't commit to protocols or platforms too early in the process.*
>
> **Tobias Disse,** Chief Executive Officer and Co-Founder, Kryha.io

Notably, when working groups for blockchain innovation are founded and led by a single major industry player, trust can be easily eroded, and cohesion lost if that major industry player dominates the group. Historically, a single major company leader could pressure adoption of its technology preferences across a supply chain which leads to the very siloed behaviour blockchain technology solutions want to alleviate. With blockchain and software solutions in general, one has to start somewhere. So, it is likely a group will organise around a dominant protocol, and may even a dominant vendor. These protocols are not yet generally scaled or interoperable. When structured this way, groups are thus far struggling to gain adoption and industry buy-in. Care must be given to anticipate how interoperability and standards will work to create resilient solutions and groups.

Craft an MOU and any initial participation documents as non-binding

If the consortium intends to become a formal entity, including a partnership agreement with fees and other aspects, it is valuable to first craft an MOU as an initial document upon which future members agree. The MOU serves multiple practical purposes, in addition to setting an initial intent for participation and understanding. See more details on this in the previous focus areas which outline the pre-consortium agreement.

Show critical mass before launch

Before the consortium is publicly and officially launched, it is valuable to gather a strong group of industry and blockchain leaders. If the group is too big, it will not be viewed as workable. However, there is a fine line, and establishing critical mass, accompanied with a well-organised promotional campaign to announce the launch, is critical for rapidly establishing the credibility of the ecosystem. This will attract future participants and help build real momentum for the project community.

Attracting a strong board of advisors can also help with brining other industry players along.

> *Agree on a locked number of participants for each round: you can increase after phase1 but avoid adding extra participants in the middle of the project.*
>
> **Nicolas Verschelden,** Managing Partner Dream Tech Alliance, AB InBev

Develop strong antitrust and governance policies

Policies should be devised by legal experts and advisors and include buy-in from the participants to ensure they meet all needs. Additionally, a review should be undertaken to understand whether there are regulatory barriers that may be overcome through government permissions. If so, be prepared to move forward on that front.

> Very quickly, any meeting that includes multiple competitive organisations in one place will push against antitrust laws unless clear policies and procedures are in place to mitigate such concerns.

See the module Consortium Governance for a detailed overview of governance considerations.

Company representatives evangelise in-house

Typically, one or two individuals from each organisation in the consortium or open innovation group will represent that organisation in consortium meetings and working groups. This individual is a leader and interlocutor on behalf of that organisation, representing its interests and providing value from that organisation to the working group.

The responsibility also falls on this individual to advocate for and represent the consortium within his or her organisation. For better or worse, this individual is charged with building internal support for the consortium's vision, securing sponsorship, drafting organisation documents, obtaining approvals, and funding for the efforts. This places the embryonic consortium "brand" on the representative's head. Strong internal communication structures should be put in place as soon as possible. This responsibility is key to continuing external support, and the consortium should help support individuals for this purpose.

The consortium can provide support by creating documentation articulating the value of blockchain for the industry, potential use cases, and ideas as to how to communicate these concepts and the strategic value of R&D to management. The company representative is then responsible for sharing these documents with managers internally and establishing buy-in.

Establish a foundational use case

If possible, the consortium or working group can anchor its efforts and vision on developing a PoC, pilot, research report, or standards document for an initial use case whose value is universally acknowledged. This serves to test the value and success of the initial collaborative format and working group, to provide a clear example externally and internally, and to guide initial focus. This use case may be identified as one that several organisations have already created PoCs or conducted research about, where innovation and implementation stalled without establishing a broader network for adoption or addressing industry-wide technology or implementation concerns.

9. Main steps to take when forming a consortium

Building on the important areas covered in previous focus areas, here is a summary of issues in priority order that must be resolved when forming a consortium. The process review below is intended to serve as a useful starting point of key steps to consider.

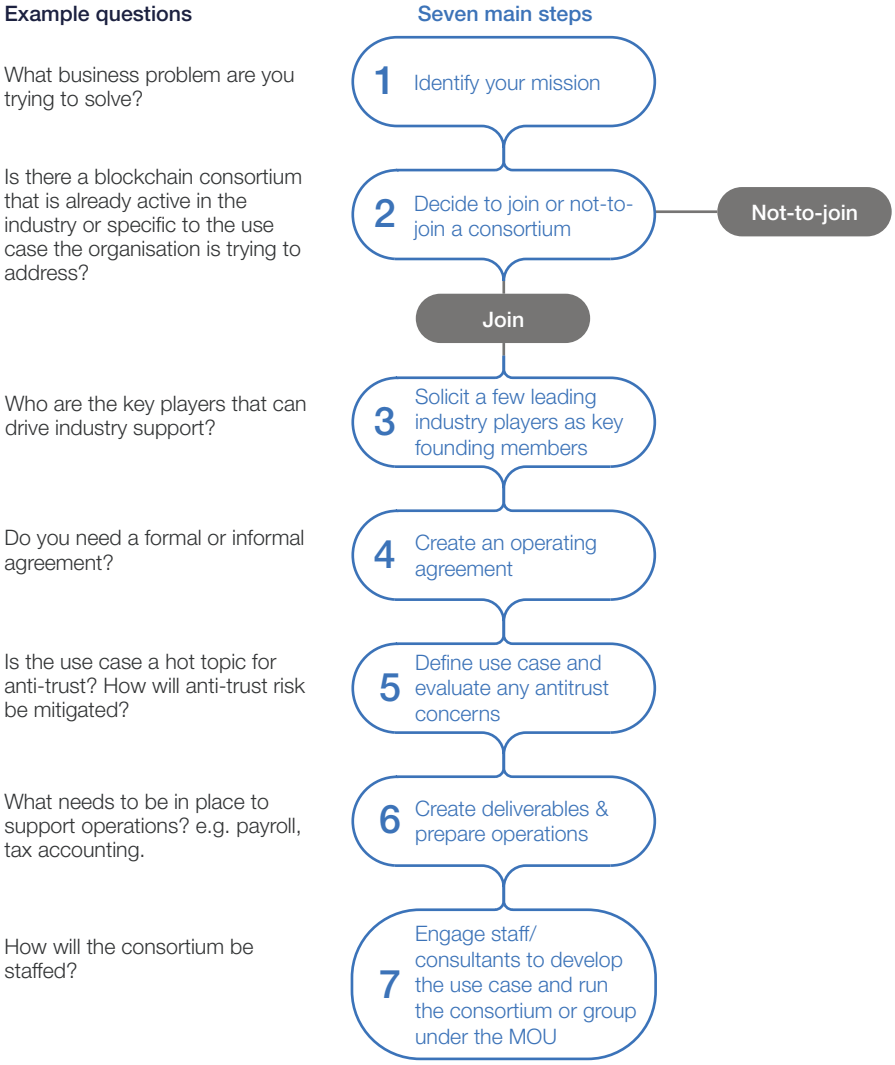


Figure 3.7 – Seven main steps and example questions when forming a blockchain consortium

Seven main steps to form a consortium

1. **Identify your mission:** Identify a real problem and make a sound business decision that blockchain is appropriate technology. What business problem is one trying to solve?
2. **Start a new one or join an existing one:** Decide whether to start a consortium or join an existing one. It is often easier and faster to leverage such underlying tech than to embark on a new project. Is there a blockchain consortium that is already active in the industry or specific to the use case the organisation is trying to address?
3. **Solicit leading players:** If one decides to form a new consortium, solicit some leading industry players as key founding members to act as a seed group. Who are the key players that can drive industry support?
4. **Create an operating agreement:** As a minimum, an agreement should be a Memorandum of Understanding. Do you need a formal or informal agreement?
5. **Define your use case and evaluate any antitrust concerns:** Define a use case that the consortium will try to develop. When use cases are selected, the consortium should also evaluate any antitrust concerns. Is the use case a hot topic for antitrust? How will antitrust risk be mitigated?
6. **Create deliverables and prepare operations.** Set-up actual operations and processes. What needs to be in place to support operations such as payroll and tax accounting?
7. **Engage staff or consultants to develop the use case and run the consortium or group under the MOU.** Consortium resources can consist of dedicated employees, member organisation volunteers/ workstreams, and others. How will the consortium be staffed?

10. The pre-consortium contract: items to resolve

If the group is not yet committed to forming a separate legal entity, but wants to try out the group, they should consider drafting and entering into pre-consortium agreement (a Memorandum of Understanding (MOU) Agreement is the most likely vehicle that will be used).

Below is an expanded list of common concerns a consortium might face in its initial formation stage. Of course, each group that forms in real life may have unique considerations of its own, in which case it will make sense to customise from this general overview of concerns. Any issues from prior working groups now transitioning toward a consortium arrangement need to be identified and resolved when entering into pre-consortium agreements. But, with that caveat, this list should be a good starting point for formulating a pre-consortium agreement.

Mission and goals

- ☐ Align on the business problem this initiative is aiming to solve
- ☐ Decide on the key drivers of the group: standards, organise around a protocol, organise around a vertical, organise around interoperability, government authorised group or other

Legal agreement

- ☐ Set out operating rules and responsibilities as a detailed MOU or in a separately drafted operating agreement
- ☐ Set out rules for IP
- ☐ Set out proper committees like steering committees (both business and technical or hybrid), legal and IP committees, board of governors/ directors, board of advisors
- ☐ Set out rules and terms for additional members to join and for exits
- ☐ Set up operating bank accounts and tax processing
- ☐ Decide on use cases. This may require a workshop
- ☐ Staffs either internally or outsource to design, code and deploy use cases

Structure

- ☐ Legal entity structures
- ☐ Operating Agreement - how the business is to be paid for and operated, including communication and responsibilities, both internally and externally. Also, how technology decisions including interoperability concerns are to be made (initial and ongoing choices, development, reviews, testing, changes, and updates)
- ☐ Data management and ownership
- ☐ Voting structure to operate the agreement
- ☐ Committees required for the consortium
- ☐ Funding & contributions set out (monies, in-kind, combination of monies and in-kind and how those funds are to be used)
- ☐ Covenant to enforce mutual respect of individual entity practices
- ☐ Covenant to enforce mutual respect group organisational practices
- ☐ Provision of indemnity
- ☐ Allocation of liability (joint, several, etc.)
- ☐ Dispute resolution
- ☐ Regulatory interface if necessary
- ☐ Amendment and modification processes

- ☐ Rules for exits including voluntary resignation and removal of participants and any pay-outs
- ☐ Rules of new member admission and requirements
- ☐ Antitrust analysis and applications for exemptions if relevant
- ☐ Smart contract legality
- ☐ IP obligations and rights – decide who owns different types of IP generated and how are the IP rights licensed and administered
  - The consortium is sole owner
  - The business network designer is sole owner
  - IP ownership is shared among different parties
  - IP arrangements defined upon exit
  - Initial IP rights and prior art considerations

Operations

- ☐ Define initial consortium duties, roles and responsibilities of each member, including secondment rules
- ☐ Use case development (and anti-competitive implications, if any)
- ☐ Enumeration of services offered
- ☐ How are payments to service providers made? In a pre-consortium fashion, for these companies to work together and have a means (bank account) to pay the technology or other partners, the consortium will either have to 1) establish a legal entity 2) appoint one of the companies to act on behalf of the group to handle payments
- ☐ Brand creation of group, marketing strategy and support by the pre-consortium group
- ☐ Marketing duties and obligations or pre-consortium members and corporate marketing support supplied by members
- ☐ Hiring and managing vendors and consultants as well as creating staffing plans
- ☐ Define the main consortium deliverables – some typical deliverables include:
  - Standard setting
  - Sharing of research and development
  - Design and develop a joint blockchain-based platform
  - Hybrid settings involving multiple options of the above

MODULE

Consortium Governance

Overview

Focus Areas

1. Business versus operational governance
2. Purpose and stage impacts governance
3. Organisational structure
4. Intellectual property
5. Competition and inclusivity
6. Liability and risk management
7. Business strategy and economics
8. Participant on-boarding and off-boarding
9. Dispute resolution and errors
10. System change management
11. Data sharing and storing

Tools and Resources

12. Business governance considerations
13. Operational governance considerations

Overview

Good governance is a key indicator of a well-functioning consortium. Creating the framework for entities to effectively work together is just as important as building the related technology solution. Inevitably, members of a consortium will have different priorities and interests that need to be reconciled. Thus, before forming a consortium, it is important to plan in advance how decisions will be made and how differences of opinion will be resolved. While there is no single solution that will enable every disparate interest to be accommodated, establishing rules of the road early on can greatly help to smooth disagreements, or even prevent them altogether.

Deciding on a governance model is important at the very formation of a consortium, as the governance model is key for all other decision making. Important initial decisions include who will fund operations, who will be responsible for the development of new technology, and who will own this technology. However, note that it is also possible – and even likely – that a consortium's governance model will change over time as the blockchain solution becomes more sophisticated, adding new participants and functionalities.

FOCUS AREAS

1. Business versus operational governance

Has the consortium defined governance at both a business and operational level?

The Ecosystem module covers the importance of proving the business value that will be realised from a new project for all stakeholders. If an ecosystem decides to organise as a consortium, the module Consortium Formation explains the important early steps and considerations for joining or forming a consortium. Building on that, this module focuses on the establishment of governance within a consortium. Well-designed, inclusive, and fair governance of a consortium is a requirement to operate and maintain a distributed ledger solution.

Governance for a blockchain consortium can typically be thought of in two separate components:

1. **Business governance:** Includes forming a legal entity, establishing the governance model for the new legal entity, setting a budget, creating commercial models, allocating profits, selecting new lines of business, setting marketing strategy, and standards for adding new consortium members.
2. **Operational governance:** Includes setting information security and other standards for accessing the blockchain solution, giving permissions to new network participants when they meet applicable standards, determining when participants must upgrade to a new version of the blockchain software, and dispute resolution.

While the governance process and model for each of these governance components can be exactly the same, it may also diverge in some respects. For instance, in a blockchain consortium where a new legal entity is formed to own related technology, that legal entity's governing body will be responsible for business governance, and that legal entity will play a significant role in operational governance. But non-profits, industry standards bodies, and trade associations who are not members of the legal entity's governing body may also be involved in operational governance.

Operational governance deserves particular attention given the nature of distributed ledger networks. The multiple layers of distributed ledger networks necessitate changes to more traditional operational governance models. For example, because each network participant operates an independent node that communicates with other nodes on a peer-to-peer basis, they must all be running up-to-date or compatible versions of the relevant software. In addition, to ensure all participants on the network trust one another, each participant should be able to certify that it meets relevant information security and data protection standards.

The multiple layers of distributed ledger networks necessitate changes to more traditional operational governance models.

Although each consortium is unique, there are still guidelines related to governance worth considering as foundational best practices. This module will review these important considerations to be taken into account when selecting a governance mechanism. The focus is on enterprise blockchain solutions rather than permissionless solutions.

This module also reviews certain business considerations for early-stage consortia, such as how to treat new intellectual property (IP), funding,

budgeting, and competition and inclusivity issues. (For more details on important steps to take pre-consortium, see the module Consortium Formation). Finally, this module also covers some ongoing operational decisions that a consortium must make.

This module distinguishes between **"consortium members"** – members of the corporate entity or parties to the contractual arrangement that are involved in its business governance – and **"network participants"** – users of the blockchain network that are involved in operational governance. For example, consortium members will be interested in business aspects of governance such as budget and financials, ownership of IP, and management of the network as a whole. Network participants will be interested in dispute resolution, requirements for participation, and information security standards.

2. Purpose and stage impacts governance

How does the purpose of the consortium impact governance? How does the consortium's lifecycle stage impact governance?

As outlined in the module Consortium Formation, deliverables for a consortium can take many forms. Joining a consortium to study the potential use cases of blockchain technologies is very different from joining a consortium whose purpose is to develop, deploy, and monetise current blockchain solutions to drive revenue. As such, the amount of input an organisation may want to exert on a consortium can vary greatly, depending upon what each member is hoping to achieve through membership in the consortium. A consortium may even start out as a research based non-profit organisation, and then evolve into a revenue-driven business consortium – a change requiring a significant shift in governance models.

In a more "research-oriented" consortium, participating organisations may prefer to take something of a laissez-faire approach to management, weighing in only on issues related to their specific needs or interests. In a consortium that is more focused on bringing a solution to production, organisations may consider taking a more hands-on approach on issues related to funding, membership, leadership, and overall governance. This more active role may require additional resources and closer, day-to-day involvement between the business personnel of the members and the consortium.

Blockchain consortia should also consider whether changes to governance are appropriate as the consortium's solution goes into production and becomes more widely adopted, especially for operational governance matters. While a consortium may be established by a small number of initial partners, it may be appropriate to open operational governance to a broader group of constituents such as network participants, standards bodies, and regulators.

One example of how this can play out: It is often easier to design a prototype among a limited number of consortium members. These members can remain responsible for business governance, but as the blockchain solution becomes operational, they should consider opening operational governance to additional network participants.

However, parties should be aware that larger governing groups can become unwieldy. When moving to the operational stage, it is often helpful to delegate significant authority to a board of directors or to employees of a new

consortium entity, while leaving key strategic decisions to a vote of all consortium members. Or, if no new legal entity has been formed, day-to-day management may instead be delegated to a small working group with authority delegated by all members.

For example, many consortia begin as loose associations of member organisations before the formation of a legal entity or the entry into a formal agreement. In such a case, consortium members may work by consensus, requiring unanimity on all decisions.

A key decision to take is whether your consortium should form a new legal entity, or simply enter into a formal contractual arrangement among the consortium members. Will the consortium form a new legal entity or will it simply enter into a formal contractual agreement? This decision will be driven by many considerations, including tax, financing, and regulatory requirements. Once parties are ready to commit to forming a new entity or entering into a formal contractual arrangement, the governance requirements can become more complex.

This module does not attempt to define all of the considerations applicable to the formation of a new entity or the creation of a formal contractual arrangement. For consortia where a legal entity is formed, the jurisdiction in which the entity will be formed affects many of the considerations discussed in this module.

Different jurisdictions have different rules about how a board should be structured, funding opportunities available and other considerations discussed here.

> *The main success factor to get a consortium off the ground is to have collaboration-minded people at the outset who are willing to work with their peers to solve common pain points for the industry's customers. Once a real business case is identified, moving quickly to a legal entity with a profit motive will certainly help focus minds on the delivery of a product the community will pay for. Participants must keep an agile mindset and be open to change.*
>
> **Bob Crozier,** Head of Allianz Global Blockchain Center of Competence and B3i Board Member

Choosing the jurisdiction in which the legal entity will be formed is critical, as different jurisdictions have different rules that can significantly impact the various aspects of the consortium.

3. Organisational structure

What are the key roles and responsibilities and who will fill those positions?

It is first important to consider who from each member organisation is involved. While it is up to individual organisations to determine which individuals internally will be responsible for day-to-day management of the business' relationship with the consortium, a consortium may wish to establish the level of seniority of such individuals. Although it may be ideal to have overall responsibility for the relationship ultimately reside in the C-suite, for large organisations this will be impractical. Thus, relationship management will need to be delegated.

The key is for each individual responsible for a member's relationship with the consortium to have decision-making authority, or a clear line to decision-making authority for matters that are not day-to-day operations, as governance will prove overly cumbersome otherwise.

Depending on each member's goals – and those of the consortium – management of each member's relationship with the consortium will often fall under the auspices of the chief technology officer, chief information officer, chief financial officer, or legal counsel. In some cases, management responsibilities may fall across multiple functions in a member organisation, requiring the formation of an internal working group to advise the relationship manager on key decisions and issues. It is recommended that this internal working group include representation from business/strategy, technical, and legal views.

The governing body of a blockchain consortium will typically have final responsibility for all aspects of the consortium's business governance, including how funds will be raised and used, the selection of service providers and key software components (such as the blockchain protocol to be used), and commercialisation and marketing.

The governing body of a blockchain consortium, as part of business governance, will typically select a turnkey services provider – sometimes referred to as a "network operator" – to provide technical services such as support, monitoring, and technical onboarding. The network operator may also provide the blockchain software as a third party, or the consortium itself may function as the network operator.

If the network operator is a third-party service provider, it will need to enter into a contract with the consortium entity, if one has been formed, or the consortium members to clearly set out the duties and responsibilities on all sides.

The governing body of the consortium may also have authority over more operational policies, such as information security requirements, that all network participants must adhere to, and the operating procedures for actually interacting with the network. Alternatively, operational policies may be the responsibility of a separate governing body for the blockchain network.

Operational governance also includes giving permissions to participants to join the network once such potential participants have established that they meet the standards established by the governing body, and for ongoing monitoring to ensure those standards are met. A governing body can have subcommittees for business and technical operations, setting up and monitoring service level agreements (SLAs), and reviewing legal and operational requirements for all the participants in the network, as well as separate dispute resolution bodies for transactions on the network. In addition, some or all of these functions can be delegated to employees of a consortium entity, if one has been formed. Figure 4.1 shows examples of how responsibilities might be divided among different levels of governance.

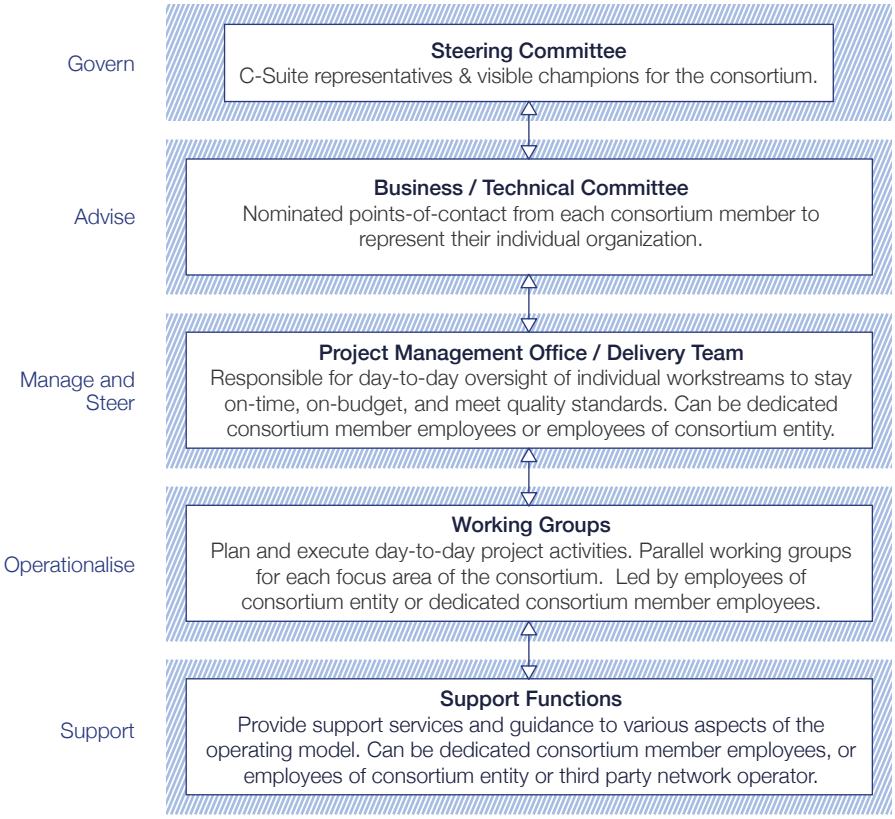


Figure 4.1 – Example set of roles for a consortium

The remainder of this module is divided into business governance considerations and operational governance considerations (Figure 4.2):

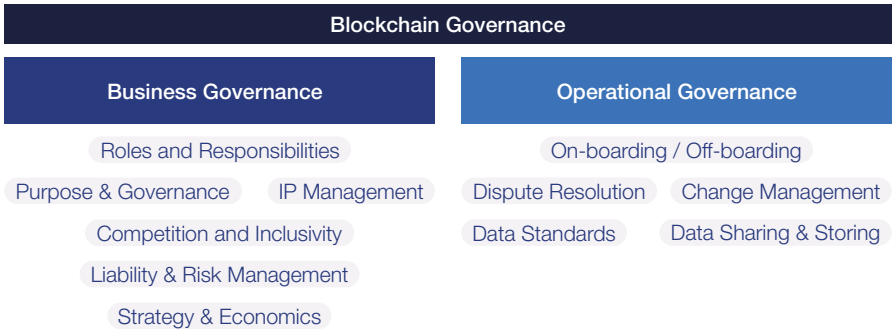


Figure 4.2 – Two types of governance in a blockchain ecosystem and their key considerations

4. Intellectual property

What intellectual property ownership models should be considered?

Intellectual property (IP) considerations should be addressed at the very beginning of consortium members' discussions. IP is created before coding even begins, when the parties are discussing functional requirements, and it is important for each consortium member to know how it can and cannot use that IP within its own organisation.

Even if consortium members initially believe that the IP being created will hold little value outside the consortium context, members should consider and document what their rights are to use any such IP as it may prove valuable later. In addition, consortium members should review their IP assets and consider whether any can be leveraged in the consortium, and how this IP can be protected and shared.

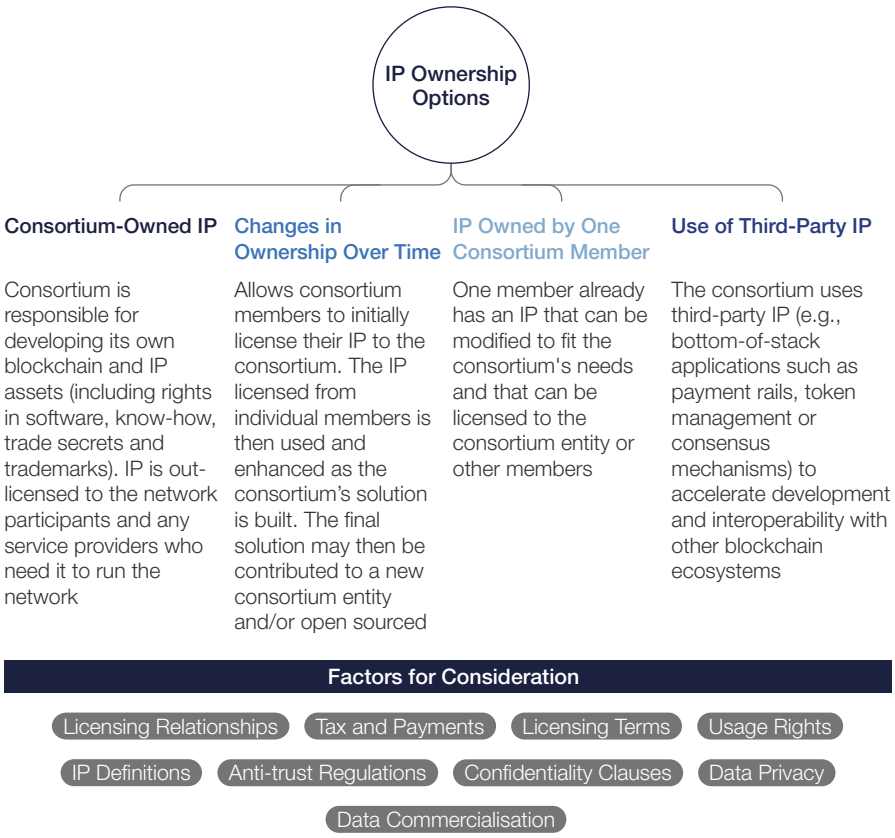


Figure 4.3 – Overview of intellectual property ownership options

Blockchain consortia can use several types of IP ownership structure (Figure 4.3):

- **Consortium-Owned IP:** If a consortium is developing its own blockchain technology, IP assets including rights in software, know-how, trade secrets, and trademarks will be the core assets created. Typically, if new IP is being developed to be licensed to third parties, the consortium members will want to assign these rights to a newly created entity. This is because consortium members themselves are unlikely to want to have direct licensing relationships with network participants, with the associated support, maintenance, and liability considerations. Joint ownership among the consortium members is also a possibility but has many disadvantages. For example, it becomes much more difficult to pursue infringement claims if all owners must be involved in the claim, as is the case in some jurisdictions. Members will also need to consider whether the exploitation rights to jointly owned IP should be limited or divided amongst themselves in any way. Finally, consortium members may also determine to allocate ownership of certain inventions among themselves and enter into cross-licensing arrangements. But unless all IP is being allocated to a single consortium member, this may prove overly complex in practice as the parties will then need to enter into assignment arrangements. Tax and payments issues will also need to be taken into account.
- **IP Owned by One Consortium Member:** If one member of the consortium already has fit-for-purpose IP, or IP that can be modified to fit the consortium's needs, a standard licence can be used. In such a case, however, issues of consideration will become important and must be negotiated among the members. If one or more members have IP that can be used to further develop the consortium's product, this IP can be licensed to the consortium entity or to the other members as background IP. In each case, consortium members should consider the ownership structure of any modifications to in-licensed IP and newly created IP. Consideration should also be given to appropriate restrictions on the use of any one consortium member's IP, keeping in mind potential expansion of the network but also giving consideration to protecting the consortium member that owns such IP.
- **Changes in Ownership Over Time:** The consortium members may also elect to undertake a "timeframe to own IP" clause. In any legal situation, it may be optimal for the members to own IP for a predetermined period of time, then transfer rights to a new consortium entity or for a consortium entity to own rights and then transfer those rights to individual members. This approach might make it more appealing for members to bring their IP to the table under a licensing agreement, but as the assets are enhanced and developed by other parties in the consortium, a transfer process is then enacted. Alternatively, consortium members could determine to open source related IP once it has matured sufficiently. The open source framework is becoming more popular as its benefits – a community of developers working to build integrated applications and provide corrections – are established.

- **Use of Third-Party IP:** Finally, a consortium may elect to use third-party IP – especially bottom-of-stack applications such as payment rails, token management or consensus mechanisms. Third party bottom-of-stack protocols can be used to create interoperability with other blockchain networks and are thus an important tool for consortia to consider. However, consortium members will also need to consider and evaluate the stability of the third-party software, the availability of support services and the ease in which the consortium's application – and the consortium members' other systems – can be integrated with it. See the module Interoperability for more details. Finally, since in a distributed network each consortium member will need to run its own version of the blockchain software, licensing fees will need to be considered.

The ability to use and commercialise data resulting from operation of a new blockchain network is also an issue that should be addressed before the network becomes operational. For example, data regarding the cost-of-goods on a blockchain platform can be valuable to other players in the chain such as customs brokers. That said, each party to a transaction will want to keep their individual transactions private. Ownership of this IP can, and likely should, be allocated differently from the ownership of the base IP on which the network operates.

Network participants will likely want to maintain ownership and control over the use of data they generate or bring to the network. However, the network operator may want to use or commercialise such data on an aggregated and anonymised basis, as well as use data such as overall transaction and message volume for marketing purposes. Any data that relates to individuals' use of a network will also be subject to privacy considerations which are beyond the scope of this module, but more information available in the module Personal Data Handling.

Confidentiality clauses determining information protection obligations and their limits also should be considered as a part of IP management. Such clauses regulate what information is deemed to be confidential and what is not, confidential labelling of documents, the procedures agreed upon for the transfer of confidential materials, to whom confidential information may be divulged and under which conditions, and the time-lapse during which the confidentiality obligations will be in force. This is especially important in the initial stages of the consortium formation when final legal documents have not been executed but conversations are well underway.

Finally, certain information and data should not be shared amongst consortium members. Sharing data regarding customers or individual member commercial arrangements, for example, will be seen as anti-competitive in nature. Antitrust policy should be followed regardless of what type of IP management choice is made.

> It is important to ensure that deliberations do not interfere with the competitive relations of companies. Clear guidelines and protocols based on competition and antitrust laws must be developed.

For IP legal and regulatory concerns related to the development of a blockchain technology solution, refer to the module Legal and Regulatory Compliance.

5. Competition and inclusivity considerations

How will you ensure that governance is not viewed as overly exclusive while also creating a functional system?

Consortium members should ensure that participation in the blockchain network itself is not exclusive to a single group, although they may establish objective criteria for participation, such as regulatory qualifications, insurance requirements, or security certifications.

Consortium members should also take care not to suggest or imply that they intend to coordinate to use one service or platform to the detriment of other services or platforms, or that they intend to stop using a certain service or platforms, or that they intend to stop using a certain service or platform. This does not mean that a consortium cannot select a single blockchain platform to base its service on or select a set of providers to the exclusion of other providers. But consortia must avoid requirements that members should only use the services provided by the consortium.

Competition counsel should be consulted to ensure that the consortium's activities are not perceived as exclusionary.

Ownership of the legal entity that manages the solution – or, if there is no legal entity, participation in the contractual arrangement that governs the consortium can be limited. However, consortium members should take care that the system is not seen as catering just to the interests of large participants or a particular industry segment. The key is to ensure that the system remains usable by all industry participants that can benefit.

A consortium project may not attain critical mass until industry leaders join or back the effort. However, there is always the risk of an actual or perceived conflict of interests. Industry leaders by nature will be among the largest participants on any blockchain network. Conflicts of interests can be perceived when these industry leaders are also the only members of governing bodies and marginalise the considerations of other participants.

In short, inclusivity considerations are important. The core group involved in creation of a consortium should take a broad-based view and include business partners from varied industry sectors, potential participant constituencies and jurisdictions in governance, whether through participation in advisory or technical committees for the network, or even through an opportunity to invest in the consortium entity itself. This increases the number of value chains that can be unlocked.

Ways to create inclusivity in governance include rotating seats on committees among participants and having separate working groups to address different issues based on member interests, expertise and industry roles.

A major goal of consortium governance should be to ensure broad representation without creating governing bodies so large that they are ineffective.

6. Liability and risk management

What type of legal liabilities are consortium members exposed to, if any? What mitigating actions can be taken?

Consortia are organisations composed of individual members, many of which will be large corporations. The consortium itself is most likely to be a separate legal entity similar to a startup in nature. It will take on its own risk and liability, which the consortium members will likely desire to limit.

Still, the question remains: Do members of the consortium take on any potential liability?

Liability can be imposed under law, and it may also be imposed – or limited – by contract. Generally, consortium members should consider liability among network participants and also potential third-party liability, including regulatory issues and situations where third-party interests are impacted.

Liability in general can be sensitive and intimidating to deployment owners, executives, and influencers to varying degrees and for different reasons. The aim of this section is to summarise insights that can help frame your thinking (and as illustrated in Figure 4.4). As with other consortium-related considerations, it is important to proactively seek legal advice from those on the leading edge of this topic.

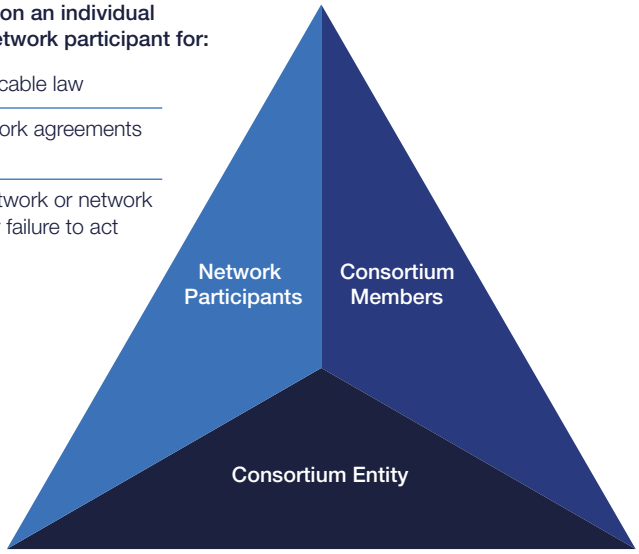
- **Liability of Network Participants:** Liability may be imposed on a blockchain network participant for its failure to comply with applicable law, network agreements or policies, or other damages caused to the network or network participants by its bad acts or failure to act. This type of liability is created through network participant agreements and is typically one of the most heavily negotiated provisions of any participant agreement. Participants will typically want to limit their liability as much as possible, but the consortium entity will need to consider what level of limitation it can accept. In addition, given the point-to-point nature of distributed networks, participants should take into consideration the fact that they will be receiving direct transmissions from all network participants with whom they do business. Thus, they should consider whether to impose liability on a participant-to-participant basis. Also note that a single network participant's egregious behaviour will have an impact on the consortium itself around branding, reputation, and future business opportunities. Network participants will of course be liable to their end customers and regulators, regardless of which functions are outsourced to the blockchain network.
- **Liability of Consortium Members:** Consortium members should also consider whether they are taking on additional liability as part of their participation in a consortium, and how to mitigate this liability, if any. A third party may make a claim against one or more consortium members who are perceived to have the resources necessary to satisfy a claim or to be likely to regard the claim as trivial enough to settle without litigating. Thus, members might find themselves defending against acts they did not commit. If the legal arrangement of the group is still in an informal stage such as a memorandum of understanding (MOU) or pre-consortium agreement when the blockchain network goes into production, it is possible that the entities in the working group will be individually responsible for any liabilities incurred as there is no separate legal entity to act as a shield and absorb the liability. See the module Consortium Formation for pre-consortium agreement details.
- **Liability of the Consortium Entity:** In most cases, it is likely that a blockchain consortium will form a legal entity to hold related IP and enter into contractual arrangements with network participants. The contractual counterparty will be taking responsibility for network operations and will be liable for a breach of its covenants to participants. (While it is possible that a third-party network operator could accept this responsibility, it is unlikely as a practical matter.) The counterparty entity formed by the consortium may seek to limit its liability through contract, but some liabilities cannot be excluded by contract, and fines and other liabilities imposed by regulators cannot be waived. Owners of the consortium entity can be shielded from this liability through appropriate corporate governance – however, if the consortium entity needs funding to resolve liabilities, it is to these members it will most likely turn.

Liability may be imposed on an individual consortium member or network participant for:

Failure to comply with applicable law

Failure to comply with network agreements or policies

Damages caused to the network or network members by its bad acts or failure to act



Responsible for network operations and will be liable for a breach of its covenants to participants

Figure 4.4 – Typical liabilities faced by various types of blockchain participants

Mutual indemnity clauses covering breaches and damages may be included in consortium agreements to provide liability protection. Insurance might be available as well. Consortium members should confirm whether their individual corporate insurance policies cover consortium work, whether a consortium secured insurance policy covers this work, and what the gaps in protection may be.

7. Business strategy and economics

How will the consortium be funded, both initially and on an ongoing basis? What drives decisions related to product development?

Funding a consortium project does not need to be a contentious issue. However, it is important to consider the true costs of a consortium project and how those costs will be funded before devoting significant resources and time. Consortia should take into account the costs of developing necessary technology and the cost of any third-party technology, compliance and licensure costs, and any related headcount. If the consortium is not forming a new legal entity, consider whether each member will commit to spending required amounts and fulfilling other requirements to accomplish the consortium's goals. If the consortium is forming a new entity, funding will likely be required to hire staff dedicated to the project.

The cost of taking a blockchain use case from inception to commercialisation can be significant, and the timeframe can be long. Building a system that will scale takes significant time and up-front cost, but it is preferable to attempting to scale with a system that is built for smaller use.

It is possible that consortium members would prefer to not fund the entire cost upfront. In that case, consortium members should consider what milestones shall be set for obtaining and releasing additional funding and what will happen when additional funding is needed. Should the members be required to

> *The setup of a permissioned blockchain consortium in many aspects resembles the setup of an internet-enabled supply chain collaborative network. Early examples include Covisint in automotive, Elemica in chemical. If the investment is heavily skewed towards a particular group of supply chain actors and benefits are not distributed fairly, there is a great danger that the consortium network would collapse.*
>
> **Yingli Wang,** Professor, Cardiff Business School

contribute additional amounts? Should the consortium entity have the ability to seek outside funding, which is likely to result in expanding the consortium and in sharing ownership with the new funders?

Of course, a consortium should consider the revenue side of the financials as well. Before fees can be set, the consortium should consider a philosophical question: Will the consortium be run as a not-for-profit entity, with members paying dues but providing services free of charge? Will the consortium operate as a market utility, with fees set based on the goal of recouping expenses but not making significant profit? Or will the consortium set its fees with the intention of making a profit to be invested in future expansion or to be returned to its owners? If the consortium does achieve a profit and those profits are to be distributed among the owners, how will those profits be allocated? It is only after these initial questions have been answered that the consortium begins to consider how rates for its services can be set.

In the event members pay some sort of fee to join and retain membership in the consortium, the governance may dictate that members pay different fees based on their organisation size or structure. For instance, in a research or industry consortia, large industry participants may pay the most, smaller industry participants like startups may pay a lesser amount, and academia, governments, and non-profits may not be required to pay a fee at all.

In order to prevent contention from other members, criteria for this should be clearly outlined from the beginning. Otherwise, members who are paying more for access to the consortium and its resources may feel that their peers are benefiting disproportionally, or even free riding.

Another important question is what will drive product development decisions in the future. Although decisions will generally be made according to the governance model chosen, it is helpful for a consortium to consider up front whether product development will be based on a pre-agreed roadmap. If there is no pre-agreed development roadmap – or once the roadmap is completed – is the goal of the consortium to further the members' interests even when this may not be in the best interest of the industry as a whole? Or is the goal of the consortium to pursue projects that will bring the most profit or the most industry benefit, even if those projects are not of the greatest use to the consortium members themselves?

8. Participant on-boarding and off-boarding

What criteria should blockchain network participants have to meet? How can ex-participants be transitioned from the network?

As discussed above under the focus area Competition and inclusivity considerations, it is important for any blockchain network to have objective criteria that determine which parties can and cannot become participants. However, these objective criteria can take many forms.

For example, a consortium should consider whether participants should be required to have certain licenses or meet certain regulatory qualifications, whether participants must meet specified financial thresholds in order to ensure they can stand behind their transactional liabilities on the network, and

Example

In a supply chain consortium for organic milk, participants that are milk producers should have to demonstrate their organic credentials and certifications.

whether participation should be limited to specific jurisdictions. The latter consideration is especially important as adding participants in new jurisdictions may subject the consortium entity itself to new regulatory requirements.

Determining whether a potential new participant meets these criteria can be a function of the consortium's governing body or a network governing body. However, where the number of network participants and potential participants is large, it will more likely be delegated to employees of the consortium entity or outsourced to a network operator. Any new network participant should of course be required to prove its identity and should be checked for sanctions and otherwise provide appropriate proof that it meets the required qualifications. New participants may also be required to provide proof of insurance and certify compliance with required information security standards – especially important where data is shared across network participants.

Participants can leave blockchain networks voluntarily or involuntarily. In the case of a voluntary exit, a transition plan could be developed, but for involuntary leavers who have breached relevant agreements or become subject to sanctions, a consortium will want to have exit plans in place. These exit plans should ensure that after a participant's network access has been restricted, assets and transactions can be accessed elsewhere. An exiting participant should already have access to its data as each participant theoretically manages its own blockchain node, but transferring assets and transactions will be more difficult. This transfer may take the form of requiring transactional counterparties of the exiting participant to open new accounts outside the blockchain network or to cash out accounts or transactions, subject in each case to any rules (such as sanctions regimes) that may block the exiting participant's assets or prevent counterparties from further dealings. Consortia should also consider any regimes (such as insolvency) which would prevent a participant from being forced out.

Consortia should clearly define the circumstances in which a participant will be required to exit (for example, regulatory sanctions or failure to continue to meet entry criteria) with a view to avoiding disputes over access and should consider who has the authority to make the decision to terminate a participant. While affirming entry criteria could be seen as more administrative, consider whether forcing an exit should require involvement of a higher level of decisionmaker.

While a participant may be free to leave the network, the data they have entered on the blockchain will remain on the blockchain after their departure, as is inherent with blockchain technology. While dispute resolution options may be available as outlined below, removing this data may affect the integrity and auditability of the blockchain history. Network participants should be made aware of this, both upon entering and exiting the network. See the focus area Intellectual property considerations for more context on the implications of this data remaining available to other network participants.

9. Dispute resolution and errors

Does the blockchain network need an internal dispute resolution mechanism? When should rollback or cancellation of transactions occur?

Depending on the use case of the blockchain network, an internal dispute resolution mechanism may be necessary. On some networks, disputes about on-chain transactions are unlikely to occur – for example, the disputes arising in connection with a network for the sharing of medical records may be more likely to relate to off-chain use of information and/or compliance with data protection policies. Disputes about whether a participant on such a network has complied with applicable rules or whether it has breached its obligations to other network participants could be resolved through the courts or through arbitration, and this may save the consortium the complexity of setting up an internal system of resolution.

However, some solutions, such as trading applications for financial instruments that process transactions on-network, may prefer to have an internal dispute resolution mechanism so that disputes can be fully and finally resolved on a rapid basis by parties with industry expertise and with incentives and experience to produce consistent outcomes.

When determining the composition of any internal dispute resolution body, consider whether independent experts can be retained, whether the members of the dispute resolution body should be voted on by network participants or selected based on some objective criteria, and how to ensure that decisions are viewed as impartial. For example, a transaction dispute resolution committee, similar to that for securities exchanges, could be implemented for financial transactions within a blockchain network.

Regardless of how disputes will be resolved, network governing documents should clearly state what law will govern the transactions entered into over the network and any disputes, and all blockchain network participants should consent to the exclusive jurisdiction of the selected dispute resolution body. In addition, to the extent that an off-chain judgment needs to be enforced on-chain, consider how this can be enforced from a technological perspective.

Given the immutable nature of blockchains, consideration should also be given to whether there are any circumstances in which participants should be required to reverse a transaction or refrain from completing a partial transaction.

Example

Given flexibility that R3 (an enterprise blockchain technology company) provides on contractual arrangements on Corda business networks, it could be possible to create an agreement between the participants that empowers the notary to implement a court order obtained from a court of the contractually agreed jurisdiction on Corda, potentially avoiding the need for the relevant judgment to be enforced against the judgment debtor in its home courts.[58]

10. System change management

What processes and procedures need to be in place in order to ensure continuity and compatibility? What procedures are in place to manage code?

In a collaborative environment, agreeing upon system upgrades and maintenance can become a complicated task among stakeholders. Maintenance and upgrades of blockchain systems are vital to any successful

effort. One reason for this is that as blockchain and distributed networks are emerging technologies, best practices in security and data sharing are still in development, and in order to employ these best practices, organisations need to remain flexible. However, given that blockchain networks are by their very nature operated by the individual participants in a network, each participant must be sure to be running a compatible version of the blockchain software. Blockchain developers should ensure that their software is backwards-compatible so that transactions and data implemented in previous versions are not lost after software upgrades.

Participants in a blockchain consortium may have different processes for how upgrades and maintenance internally occur, leading to a lack of agreement among stakeholders as a whole. In order to prevent gridlock or delays in development of the technology, a strong technical committee with representation from relevant stakeholder groups should oversee the decisions as to when changes should be implemented.

Given that blockchain software is likely to be integrated with participants' own internal systems, enough lead time must be given to ensure internal testing and any necessary internal changes can be completed before a new version goes into production. However, the technical committee should also consider in what circumstances emergency updates may be required – such as for information security emergencies.

If the consortium is developing its own blockchain protocol or applications, members will need to consider how code is managed. Who has control of the official codebase? Who has the right to request changes? Who decides what changes to make? How are changes propagated across the network?

Versioning should be defined and maintained separately from any member organisation's specific IT components. This will be important as upgrades are introduced across the network.

11. Data sharing and storing

What data storage and sharing approach is optimal? What data standards should be followed?

If the consortium has elected to use a third-party protocol – either a public permissionless blockchain or an existing permissioned protocol – the consortium will have little influence over the type of data storage mechanism used unless the consortium is one of the largest applications running on the blockchain protocol. However, the type of data storage mechanism is one of the factors the consortium should consider when determining which third-party protocol to use.

One of the key decisions any developer of a blockchain protocol must make is whether data will be broadcast to all users of the solution or shared only between parties to a transaction. Business users may desire the second model to preserve transaction privacy as well as to comply with regulatory requirements such as data privacy laws. See the module Data Protection for more details on how to protect sensitive data.

In addition, it may be impractical to store all data related to a transaction on the blockchain even when that data is only shared between the parties to the transaction. If that approach were taken, large files combined with large numbers of transactions could result in unwieldy chains.

Finally, for blockchains that are focused on information sharing, such as in medical records implementations, storing data on-chain creates issues around who controls and who can edit that data.

Members in a consortium should align and decide where and how to store data, considering the following options:

- **Centralised storage.** Results in fewer endpoints to protect but introduces resiliency concerns.
- **Storage by the data owner with retrieval on demand.** Protects data autonomy but introduces resiliency concerns.
- **Decentralised storage.** Solves resiliency concerns but introduces additional endpoints and also the possibility of control issues.

There are also data standards considerations. In order to ensure the value of the information is being derived, the consortium members must firstly agree on standardised data requirements. There needs to be alignment on the format the data will be presented in and the shared criteria for what constitutes as a valid transaction. Without a clean and standardised dataset, the true value in information sharing across network participants cannot be realised.

Example

In a supply chain blockchain, data standards must be followed throughout the supply chain to ensure that goods can be traced from production to consumer.

TOOLS AND RESOURCES

12. Business governance considerations

The checklist below may be useful to act as a conversation starter for the discussions your consortium will need to have regarding business governance. However, this is not an exhaustive list, and additional considerations are likely to come up in discussions of your particular use case.

Purpose impacts governance

- ☐ What is the purpose of the consortium?
  a. What value will we deliver to consortium members and network participants?
  b. How does the purpose of the consortium impact governance?
  c. Is anything needed to align incentives of various stakeholder groups?
- ☐ What are the deliverables of the consortium? Collaborative deliverables can take many forms. The following are the most typical deliverables prevalent in a blockchain consortium:
  a. Designing and developing a blockchain solution for a given industry or ecosystem. This typically starts with a joint proof-of-concept to test organisation collaboration. This can lead to building blockchain infrastructure that can include the following:
     - Blockchain software which forms the base for top-of-stack applications
     - Top-of-stack applications for industry use cases
  b. Standard-setting. Complement and accelerate existing data and protocol standardisation efforts. After a proof-of-concept is created, it is critical for organisations to work with other industry competitors, supply chain partners and ecosystem participants to set data and software standards.

c. Sharing research and development. Consortia can become industry-specific open innovation working groups dedicated to collaborative R&D around blockchain technology. Industry participants must be able to learn from and build upon one another's work.

- ☐ Short-term versus long-term drivers of success.
  a. What do we want to accomplish in the short-term? What will be the first use case? Who is critical to involve now versus later?
  b. What do we want to accomplish in the long-term?

Organisational structure

- ☐ What are the key roles and responsibilities and who will fill those positions?
  a. What representatives from each consortium member will be involved?
  b. Who do you work with in the pre-consortium phase and post-establishment? When do you engage with whom?
  c. How many consortium members is appropriate?
  d. What is the minimum number of blockchain network participants necessary for a viable solution?
  e. Who are the legal partners of the consortium?
  f. Who are the technology partners of the consortium?
  g. Who are the business partners of the consortium?
  h. Should the consortium seek out independent experts, non-profits or industry standards bodies at the initial stage or a later stage?
  i. How do you engage with regulators?

Intellectual property

- ☐ Agree up front on, and document, ownership of IP assets created in collaboration.
- ☐ Review existing IP assets and consider whether those relevant to the specific consortium should be licensed. Agree who will own the improvements to this IP.
- ☐ Clearly define IP rights in the case of code that interacts with the blockchain, such as smart contracts or other applications deployed in connection with the solution.
- ☐ Put in place appropriate confidentiality, data transfer and data sharing agreements.

Competition and inclusivity

- ☐ At the outset of discussions among competitors, put in place policies and procedures to keep competition law compliance top-of-mind.
- ☐ Consult with competition counsel to ensure that the consortium's activities are not perceived as exclusionary.

Liability and risk management

- ☐ Consortium members should confirm whether their individual insurance policies cover consortium-related work.
- ☐ Consider what levels of insurance are appropriate at the consortium entity level.

Business strategy and economics

- ☐ What is a realistic budget for bringing the consortium's product to production, if that is the goal?
- ☐ How is the consortium initially funded? What happens if additional funding is needed? What commitments will consortium members make?
- ☐ What is the ideal revenue model – non-profit, market utility or for-profit?
- ☐ What is the fee structure? Is it a licence, a subscription, a usage-based fee, or something else?

13. Operational governance considerations

The checklist below may be useful to act as a conversation starter for the discussions your consortium will need to have regarding operational governance. However, this is not an exhaustive list, and additional considerations are likely to come up in discussions of your particular use case.

Participant on-boarding and off-boarding

- ☐ How do new participants join the blockchain network?
  a. Note that the network itself should be inclusive, subject to meeting objective criteria such as regulatory qualifications, insurance requirements, or security certifications, to avoid antitrust/competition law concerns.
  b. Who is responsible for approving new participants?
  c. Need to conduct know your customer (KYC) and ensure any technical requirements are met before allowing a new participant to connect.
- ☐ How do exits work?
  a. Under what circumstances is a participant required to exit?
  b. How are assets and transactions transitioned?

Dispute resolution and errors

- ☐ Consider whether a network-specific dispute resolution forum is needed.
- ☐ Consider whether a transaction rollback/cancellation/error policy is needed.

Systems change management

- ☐ Determine who makes decisions regarding upgrades at the strategic and operational level.
- ☐ What are the procedures for upgrades? How long do blockchain network participants have to test or integrate before an upgrade must be put into production?

Data standards, sharing and storage

- ☐ What data goes on-chain versus off-chain?
- ☐ Should storage be centralised, decentralised or stored by the data owner with retrieval on-demand?
- ☐ What data can be stored and transmitted using the blockchain solution? What data is prohibited?
- ☐ Should any third-party data standards be implemented?

MODULE

Digital Identity

Overview

Focus Areas

1. Building trusted digital identities
2. Identifying actors and defining roles
3. Making technology decisions
4. Future-proven digital identity system
5. Defining and securing identity data
6. Process and governance
7. Decentralised identity considerations

Tools and Resources

8. Mapping out actors and interactions
9. Processes and governance questions to resolve

Overview

With the growing complexity of supply chains, trusted identities of peers in the supply network are critical to efficient operations. A trusted identity can span across different contexts, including both physical and digital. This module focuses on the latter form of identity – an online presence that represents and acts on behalf of an external actor.

This module covers considerations and questions to guide the design of a responsible digital identity system as it relates to blockchain for supply chain. The information in this module assumes that blockchain is the key capability enabling transformation in a supply-chain use case.

This module should be leveraged by the blockchain network's designers, owners, and operators to focus digital identity as one of the key components of the blockchain capability. It contains general considerations around the design of a digital identity system, including who the actors are, technology decisions, business models, securing identity data, process and governance. It also includes a specific focus area intended to inform the design of a decentralised identity system.

Recommended reading – Inclusive Deployment of Blockchain for Supply Chains Part 2 – Trustworthy verification of digital identities[59]

FOCUS AREAS

1. Building trusted digital identities

What is digital identity, and why is digital identity important?

Online interactions in supply-chain use cases are growing in volume and complexity. Such growth introduces more potential for value creation, and contrarily, more potential for inefficiencies and risk. When blockchain technology is leveraged for a supply-chain use case, a trusted digital identity can facilitate complex online interactions, mitigate risk, and enable the full potential of the system.

As a foundation to every transaction, a trusted digital identity unlocks the potential business value of distributed ledger technologies, allowing for greater confidence in the growing digital world, and ultimately making best use of blockchain to streamline, simplify, and reduce cost in supply-chain applications.

In developing and deploying blockchain for a supply chain, digital identity must be embedded into the design, to facilitate and maintain trust. With increasingly complex supply chains, it is critical to ensure each contributing delegate is really "who" they claimed to be. Consider who should control digital identity verification in global supply chains – for example, a federated national stakeholder versus a private company versus individual stakeholders. How will this selection impact the ability of the blockchain to scale and maintain trust? Digital identity, when done correctly, will enable trust for every participant in the supply chain.

In developing and deploying blockchain for a supply chain, digital identity must be embedded into the design, to facilitate and maintain trust.

What is a digital identity?

A digital identity is an online presence that represents and acts on behalf of an external actor in an ecosystem. An identity could belong to a legal entity, a financial intermediary, or a physical object, for example. Ideally, a digital identity is verified by a trust anchor, or something confirming the legitimacy of an actor, so that those interacting with that actor's digital identity have confidence the actor is who and what it claims to be.

Why is a digital identity important? When is it necessary?

A digital identity is important to establish trust and understanding among stakeholders in an ecosystem. If stakeholders do not trust the identity of their peers, the data held in the blockchain solution will be deemed unreliable, and the overall ecosystem will lose its effectiveness.

A supply-chain solution needs strong digital identities for all stakeholders involved because it brings together partners that may not have strong existing working relationships. For example, consider a global supply chain for luxury designer leather bags. Each stakeholder must work directly with those who represent the "links" in the supply chain immediately before and after, but not necessarily others throughout the chain. The raw material provider (first link) works directly with the leather treatment facilities (second link). Following the treatment, the leather is shipped to the manufacturing facility where it is sewn into handbags. Lastly, bags are sent to the final retailer (last link), who checks for authenticity of the bags with the manufacturer.

Now, imagine an "Internet of things" (IoT) tracking device is attached to the bags during production. The blockchain and IoT tracking device unites and informs all supply-chain participants, giving each visibility into a larger portion of the supply chain. The supply chain becomes a web of interconnected businesses, rather than a linked chain. Identity is crucial to this example, as

trust in each of the actors will affect the trust in the handbag and its authenticity. One needs to know that each actor, from devices, to legal entities, to employees and things, is trustworthy and really who they claim to be.

This is especially important and complex in the digital world, where physical interaction with people and things, like the handbags, is replaced with digital transactions and data about goods, products, and entities.

Digital identity is necessary to support the growth and change in the Fourth Industrial Revolution. As supply chains and global trade become digital, trust is critical in order to transact in the digital world. For instance, millions of connected devices are set to be deployed in supply chains. To trust the digital information that is collected from them, an entity needs to know that it is the correct device – that it is still the same device and has not been spoofed or tampered with.

Digital twins, or replicas in the digital world of actual assets or objects, can only be leveraged and trusted if certainty of identity can be established. For coffee to make its way from farmer to exporter, roaster, retailer, consumer, and everything in between, there is an interconnected web of organisations that rely on data to be shared and trusted to facilitate a multitude of interactions – such as certifications, payments, and proper movement of goods. Thus, the importance of trust and trust in data underpins companies' ability to conduct trade, from authenticity of products to financing letters of credit to facilitating exports.

Today, systems across the supply chain are built and operated in a siloed manner. To bring these together and to benefit from the transformation that blockchain can bring, a digital identity system for supply chain and trade needs to be thoughtfully designed to bring together these silos, enabling more efficient, accurate, and trustworthy digital interactions.

This module can be used as a standalone resource, but is a complement to the prior publication, Inclusive Deployment of Blockchain for Supply Chains, Part 2: Trustworthy Verification of Digital Identities.[60]

> *Implementing blockchain technology in supply chains should not just be focussed on increasing efficiency, but merely on redesigning trust for all its stakeholders, including consumers.*
>
> **Jan Scheele,** Chief Executive Officer, Bitcanna

Digital twins, or replicas in the digital world of actual assets or objects, can only be leveraged and trusted if certainty of identity can be established.

2. Identifying actors and defining roles

What actors are involved in the blockchain use case, and how does identity affect them?

Actors

A digital identity system should be able to support digital identities for the various actors involved in a blockchain ecosystem, directly or indirectly through other mechanisms such as legacy or third-party systems the blockchain solution is integrated with. The word "actor" refers to any of the entities listed in the following illustration, which defines a broader view of supply-chain interactions using blockchain:

Figure 5.1 – Potential acting entities in supply-chain interactions

Why are actors important?

Defining actors is a critical first step to take; who is involved will ultimately determine what the digital identity system looks like: how it functions, what technology is used, how data is handled, and so on. Digital identity determines the trustworthiness of an actor in the digital world, and digital identity must be thoughtfully designed to work effectively for, and with, each actor.

Why look at each of these types of actors?

Each of these types of actors is important to consider in designing a digital identity system for a blockchain solution in supply chain. While legal entities and public authorities may be the central actors involved, people and objects are acting on behalf of those entities in many transactions. Therefore, looking at the actors holistically is critical for getting the design of a digital identity system right.

To hold each party accountable in a transaction, there needs to be a method to identify who/what was responsible for any specific part of the transaction. A trusted identity enables these transactions in the digital world and can even facilitate binding legal agreements digitally (through digital signatures) – a piece of enabling supply chains' entrance into the digital world. Further, this trusted identity becomes more critical in a digital environment with no face-to-face interaction. (It should also be noted that many transactions happen directly between systems talking to other systems, without human involvement).

A buyer might never meet a seller in person; instead the buyer must trust that the seller is real, and the goods are authentic. The value of blockchain is to enable trust in data such that parties who do not necessarily trust one another can more efficiently conduct business. Building mechanisms to support trusted digital identities for actors in a supply chain is foundational to a successful supply-chain solution.

It is imperative to first consider the universe of potential actors in the ecosystem or use case. Each participating actor will need a trustworthy digital identity (of themselves) in order to interact in the digital world and need to trust the digital identity of others with whom they interact. Each actor may have different needs. Once the potential actors have been identified, consider some of the following questions:

- **Who (or what) is this actor in the use case and ecosystem?**

  Starting with the "who" and illustrating it with examples will help to concretely define the types of actors and the digital identity needs for each. Remember to also include things, software agents that act on behalf of legal entities, and other roles in the ecosystem. Some of these actors may not even be present in the early days of the project, but the design must prepare for their addition later.

- **With what or whom does the actor need to interact?**

  Determining the scope of transactions that each actor in a supply chain is involved in will help to define who should be part of the ecosystem. It is important to consider the lifecycle of each entity in the supply-chain transaction and how each component is created. This will inform how the identity of the component should be created, issued, and changed throughout the supply chain. Considering the lifecycle from creation of an entity will help to identify actors that might not have been previously considered. Understanding the lifecycle of these entities on the supply chain will help identify requirements for how its digital identity will be confirmed. For instance, what information is required for the identity to be trusted across the entire supply chain? Who needs what data for authenticating the entity? What other systems is the identity used for? What does it need to interact with? What technical and legal requirements,

as well as critical processes, need to be fulfilled to support each of the interactions in which the actor is involved? Addressing these considerations in advance of building an ecosystem will provide a "big picture" understanding of the operations to come, allowing the team to build and proactively address considerations that could otherwise be overlooked.

- **What identity information and methods for identification and authentication are accepted, where, and in what contexts?**

  Is the digital identity verifiable and auditable? Who owns the liability for identity proofing? Who are the trust anchors (authoritative sources for identity proofing)[61] for each actor?

  Trust anchors are authoritative entities that are accountable for maintaining the integrity of identity information, can attest to its accuracy, and can provide trust in the digital identity. Within their span of responsibilities, is the requirement to identity proof each actor under its jurisdiction. In many cases, a government agency or financial institution grants an actor – for instance, a legal entity – its proof of existence (PoE).[62] The trustworthiness of the institution granting the PoE impacts how trustworthy the digital identity of the actor is perceived to be; how strong and reliable is the vetting of the digital identity? Trust anchors are thus nominated because of how they are perceived by other actors in the ecosystem. Consider why and on what qualifications these trust anchors have been given these roles and the strength of the blockchain network's governance and rules.

Trust anchors are authoritative entities that are accountable for maintaining the integrity of identity information, can attest to its accuracy, and can provide trust in the digital identity. Within their span of responsibilities, is the requirement to identity proof each actor under its jurisdiction.

- **How do elements of proof differ across an ecosystem based on levels of risk, business-specific considerations, and external factors?**

  When a private-sector actor requests identity documents to validate an identity claim – for example, to prove legitimacy before opening a company bank account – the bank typically leverages a government-issued identity document. Hence, the government plays an important role in enabling initial trust for future transactions. While in most cases relating to human identities, trust anchors are typically regulated industries like banks, governments, or utilities, in a supply-chain use case, these trust anchors could include device manufacturers, freighters, custom forwarders, and cargo carriers.

  Different levels of assurance in the identity may be required depending on the level of risks associated with the transaction. Further, consider how these credentials are maintained on an ongoing basis. Should credentials need to be revoked, how can the ecosystem address this before a critical issue arises? The ecosystem should agree on a digital identity maintenance plan and a critical course of action in the event of corruption before operating. Ultimately, whether digital identities are trusted is at the discretion of each member in the ecosystem, and a decision that considers many different business-specific and external factors. For this reason, confidence in trust anchors is critical to the successful supply chain blockchain solution.

- **Who is responsible for the final interpretation of trust?**

  In global supply chains, the level of trust will vary based on the governance of the digital identity and the standards to which it is held – and ultimately, individual entities will interpret how much to trust an identity based on a number of factors. An entity will adjust trust levels for each PoE based on previous business transactions, industry expertise, geography, political climate, and other factors. For example, one may attribute high trust in identities with a PoE issued by a neighbouring country because of the similar political and economic environments, yet it may reduce how much

it trusts identities from another country that has different business norms or increased instability.

- **What identity information of the actor is considered private or should not be shared? How are privacy and control maintained? What identity and related data are required for audit and compliance, security policies, and what data can be shared? What are the unintended consequences given the permanence of blockchain and changing data protection regulatory environment?**

  What is considered private and confidential to one actor is not always for another. What is considered confidential data today might not be tomorrow. Conversely, what is not considered confidential data today, might be confidential and private tomorrow. It is critical to consider what data should be shared on-chain and what shouldn't be shared, because once the data is on-chain, it is there permanently. Moreover, with better computing capability, any encryption capabilities have a lifespan. What is considered "unhackable" today, might not be true in a few years to come. All organisations considering blockchain in their supply-chain environment must consider the unintended consequences of sharing data. For example, business intelligence can derive meaning from patterns in available data and use analytics to advance their future transactions. Most organisations today do not have information security policies that define what data should be shared and how to share these in a blockchain environment. In most cases, organisations' policies are unlikely to allow for data to be shared with parties that are not "trusted" or have no established relationships with. As legal systems shift, organisations can leverage evolving technologies to provide options in addressing these legal barriers. Consider how to manage different levels of privacy and transparency, especially in the context of establishing a blockchain system, where information is stored in a non-traditional, shared data construct. For efficiency, privacy, and performance reasons, consider how to put as little data as possible on chain.

For more information on personal data protection and the EU's General Data Protection Regulation (GDPR), see the module Personal Data Handling.

Roles and lifecycle

When is an actor "created"? What are the different stages an actor can have? Understanding this aspect of the actors can help define what digital identity means for each, and the nuances that exist even within a category. For instance, how does an entity define the "birth" of an IoT device or a physical object? What can be used to reliably identify that object throughout its lifecycle as it gets software updates and patches, as it transforms, or as it changes custody? How do the trust anchors and their roles change as that object transforms? How does a change to its status affect any data about it or collected from it – and how can an entity define the "end of life" for an object? Or, how is the consensual exit of any actor from the network handled? Finally, how does one build a foundational process that empowers an entity to address these identity decisions, understanding that the traditional view of government-issued identity isn't transferable in global trade networks?

Legal entities

Legal entities are always a primary party involved in a transaction. Therefore, it is key that they have reliable, trustworthy digital identities. They may also be a source of trust for other actors – such as those actors' employees or autonomous software agents (ASAs) they run. Ultimately, the legal entity will decide what trust to place on a digital identity – legitimising other actors in the ecosystem.

Public authorities

Public authorities often provide PoE for legal entities. In addition, they are heavily involved in ensuring compliance with certifications, licenses, tax collection, laws, and other regulations – such as in the import and export of goods and services. Therefore, public authorities may play the role of, both an identity provider and a consumer. They will need a trustworthy digital identity to participate in digital transactions.

Autonomous software agents

Software will increasingly be used to make decisions or take actions autonomously on behalf of an actor. An ASA will need the appropriate proof to show its association with that actor, and the authority under which it can transact. Especially as an ASA may make decisions, it is important to clearly outline accountability of a given transaction and ensure the ASA itself remains secure.

Physical objects

The link between the physical and digital world is highlighted when defining digital identity for physical objects. Identification and authentication methods must be flexible to implement and continue to be effective even when characteristics of those objects change – especially when considering the use of digital twins that heavily rely on adaptable and accurate methods of identifying and maintaining the state of real assets. For instance, as an object or its use transforms through the supply chain, the method must adapt to the change without compromising integrity. Identities for these objects can range from simple to very complex due to how often those characteristics change and how often that object changes custody/ownership. Industry standards will be important so that different parties may effectively communicate about complex physical objects and their digital twins.

People

Employees and contractors that act on behalf of another actor – such as a legal entity or public authority – need to be able to prove their authority to transact on behalf of that actor in a reliable and trustworthy manner. For instance, how can an entity prove the individual who digitally signed a document is who they say they are, and is authorised to act on behalf of their employer in that context?

Delegates of legal entities

Custodianship is an official role whereby an individual may be granted specific rights over a digital identity. For instance, a person may have custody of a car's digital twin once they have bought, and own, the physical car. This topic can be complex in and of itself, but it is important to consider how people may be custodians of identity information on behalf of legal entities, things, or even other people.

People have many different personas, an "employee" or "contractor" being just a couple of examples. People may be delegated specific access or control of a digital identity based on their different personas or the different roles they play in an ecosystem; it is therefore critical to consider how to build a good digital identity that real humans can establish, use, and maintain in a way that works for them. There are many additional considerations when building good digital identity for people, such as ease of use and inclusivity.[63]

Connecting the dots

The actors, their associated lifecycles, and roles defined in the ecosystem are highly interconnected and interdependent on one another. For instance, a person's authority to transact on behalf of a legal entity is conferred on them by that legal entity; the legal entity's legal status and PoE is often given by another legal entity (such as a financial institution or a public authority). This interconnectedness means that digital identity needs to be carefully considered for each actor. If digital identities of just one type are not trusted, then that distrust can propagate and undermine the trust that is foundational to online transactions, including in a supply chain blockchain solution.

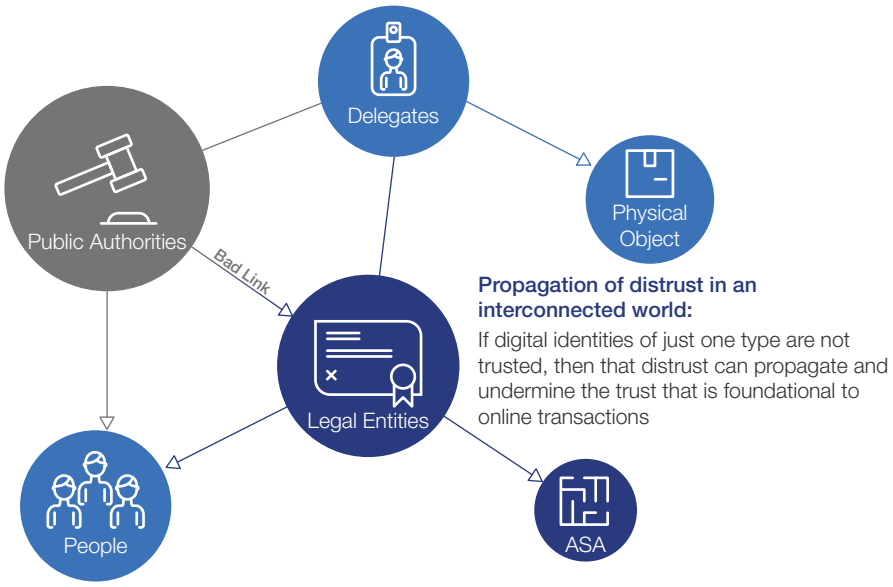


Figure 5.2 – Propagation of distrust in an interconnected world

A supply chain blockchain solution is often the work of multiple contributing groups, so digital identity will need to be designed collaboratively. Trusted digital identities are therefore a collective effort by many parties, and require collaboration across industries, sectors, and borders to be effectively maintained and managed.

3. Making technology decisions

What models for digital identity should be considered? How can one ensure digital identities are secure and interoperable?

The distributed and shared nature of blockchain means there are several different technical considerations for digital identity in supply chain. In setting technical requirements, it is also crucial to take into account the great variety of actors, needs, and use cases that may be covered in a blockchain solution. With that in mind, digital identity and access control must be scalable to support a growing and varied ecosystem.

Supply-chain implementations of blockchain mean there is a breadth of different actors, from legal entities to connected devices. The decentralised nature of the blockchain shifts the responsibility of ecosystem building, which has traditionally been placed on a centralised point of control, to many stakeholders in the ecosystem.

Overall, blockchain enables real-time data sharing among parties that may not have traditionally worked together, essentially removing the middleman from these connections. Additionally, the transparency that blockchain can provide introduces new considerations around privacy and auditability. How can this breadth of technical requirements and limitations be properly dealt with to ensure a successful blockchain deployment?

Archetypes for digital identities

For detailed information on each archetype and comparisons among them, refer to a previous publication on digital identity. Included in that publication[64] are several considerations when choosing amongst different identity archetypes. Keep in mind, however, that most identity systems today are built for people and not the scale of, for instance, millions of connected devices or complex legal entities. In a more complex world where people, things, legal entities, and processes all interact, moving from the current centralised, siloed systems (some still paper-based) to even a federated model will require strong collaboration and may be a large lift.

Centralised digital identity system

Overview:

- Traditional model for most identity systems.
- Usually owned and managed by a single organisation for users to access services provided by that organisation.

In practice:

- In the supply chains space, this shows up with an employee in a procurement department having a set of credentials to authenticate with an online supplier's ordering system.

Key considerations:

- Centralised identity systems are, by nature, siloed. Amid a growing crisis of identity fragmentation, organisations are moving toward including federated identity models in their identity systems and exploring decentralised identities.
- If working from a centralised identity system and looking to incorporate that into a blockchain solution for supply chain as the primary form of digital identity, scalability and extensibility may be a concern if neither federation nor decentralisation for identity is available.

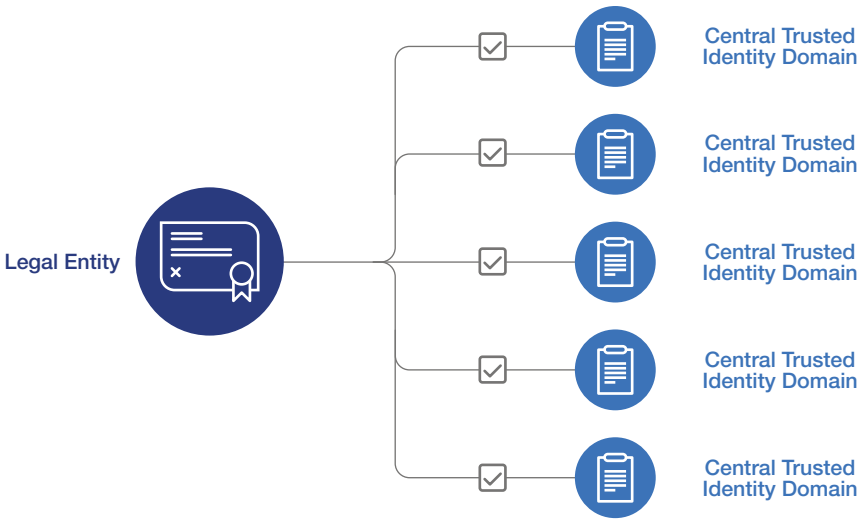


Figure 5.3 – A centralised identity system

Federated digital identity system

Overview:

- Enable a one-to-one trust relationship between entities.
- An Identity Provider (IdP) and the Service Provider (SP) establish a relationship and the SP decides to trust and accept digital identities from an IdP. The SP accepts a standardised and agreed-upon set of identity information from the IdP, and trusts that the IdP has done the necessary identity validation and sufficient authentication to prove that the entity really is who they say they are.

In practice:

- In the consumer space, this often shows up as the ability to log into, say, a retailer's website using social media credentials.

Key considerations:

- While some standards, such as the federation standards SAML2.0 and OIDC/ OAuth2.0, provide a means for a basic level of interoperability, each organisation must still establish relationships with each other organisation (in a one-to-one model).
- When considering using a federated model for the identity system, ensure it is standards-based and scalable for the purposes – especially in a large blockchain solution where establishing trust in each individual entity involved may be a challenge. Given that federated models are mostly built around use cases for people (and sometimes legal entities), identity of devices needs to be investigated further in federated models for support and scalability.

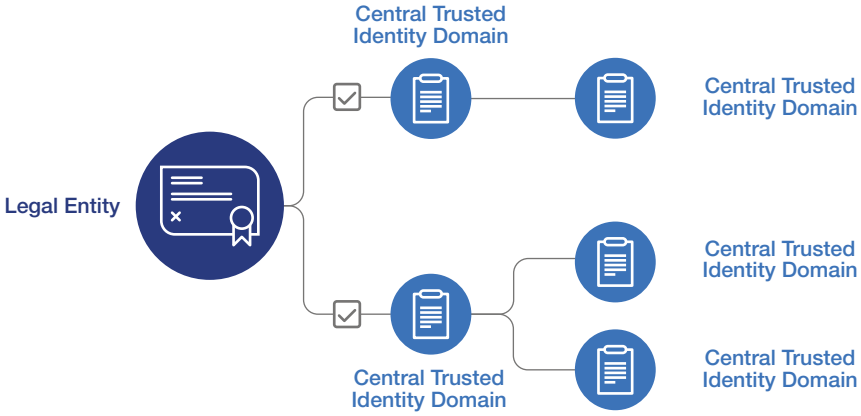


Figure 5.4 – A federated identity system

Decentralised digital identity system

Overview:

- Decentralised identity models are emerging and starting to gain traction.
- An identity holder, verifier, and issuer all work to establish verifiable and authentic digital identity for entities involved.
    - The holder (in the cases of consumers, an end-user, or a delegate of a company responsible for maintenance of the company's digital identity) receives verifiable pieces of identity information from an issuer.
    - A verifier receives pieces of the entity's digital identity by that entity sharing it with them, where the verifier can check that the information is correct and authentic with the ledger.

Example

British Colombia and Ontario's Verifiable Organizations Network. The Canadian provinces of British Colombia and Ontario designed the Verifiable Organizations Network (VON) to enable a trusted digital environment for their businesses. Using the decentralised identity system Sovrin Network, where they have placed their credential definitions and verification keys, it aims to furnish businesses with a trusted digital identity issued by their local government with which they can conduct their affairs globally. Shortly after their launch in early 2019, VON had already more than 7 million verifiable credentials for Canadian companies issued.[65]

Key considerations:

- While this model has enormous potential, it is still in an emerging state. Many organisations are not yet poised to accept a decentralised identity model for production use cases, though that is changing.
- When considering this model, ensure that organisations are well-prepared for the changes that this new model for identity will necessitate – such as the changes to governance models for digital identity requiring cross-organisation support and the associated technology changes.
- To future-proof a decentralised identity model, ensure it follows the emerging standards, such as those by the World Wide Web Consortium. However, because of the potential of a decentralised identity model and several important differences in how digital identity is managed and constructed in this model, an additional focus area with specific considerations for decentralised identity is invited.

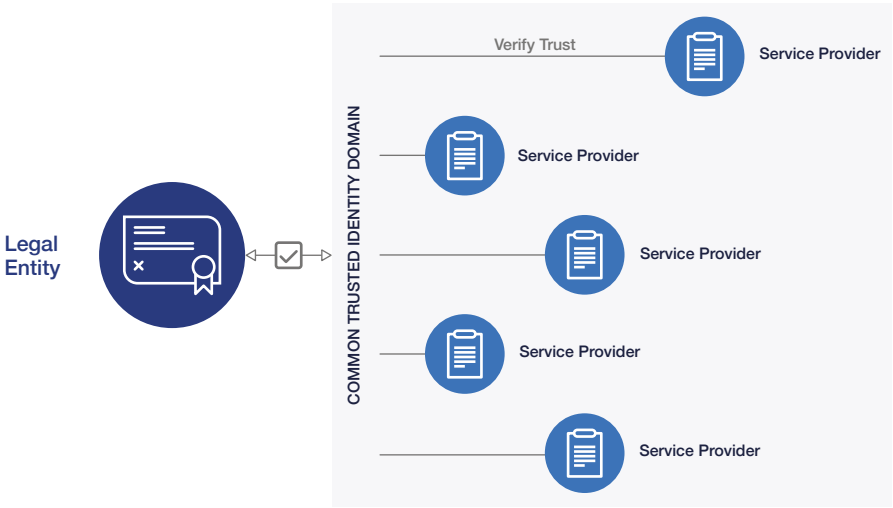


Figure 5.5 – A decentralised identity system

> *Blockchain has allowed us to take a completely different approach to digital identities that ranges from better protecting private information and giving users higher control over their data to the consideration of very interesting ideas about user authentication and peer-to-peer validation.*
>
> **Hanns-Christian Hanebeck,**
> Founder and Chief Executive Officer, Truckl.io

A hybrid model for digital identity

These three different archetypes each have their benefits and challenges and provide unique solutions to the digital identity space. Consider the possibility that an identity system is unlikely to maintain just one, or even only two, of these models; all three may coexist and therefore interoperate.

For instance, one such model could be a centralised-decentralised hybrid model, whereby proofing and de-duplication (ensuring uniqueness and singularity of a digital identity) is done centrally, and authentication occurs in a decentralised model.

A hybrid model supports the role of critically important centralised systems and enables the trusted sharing of data across systems and entities – building capabilities on top of what exists and bringing a wider ecosystem of actors together. This takes the collaborative effort and work of parties across an ecosystem, from building governance models to collaborating on standards and working with new technology to enable transformation in trade and supply chains.

Standards, integration and interoperability

The pace and ease at which an organisation's digital identity system can be adopted depends on the ease of integration and its wide acceptance. Greater acceptance and interoperability of digital identity can support the wider

> Like barcodes, the digital identity of any entity on the supply chain must be widely accepted and recognised for it to be adopted.

adoption of cross-enterprise and cross-sector blockchains, since digital identity is foundational for every transaction – including those that are supported by blockchain. Also, identity systems and their interoperability are a vital part of overall system's interoperability.

General interoperability techniques and approaches are also valid when it comes to the integration and interoperability of identity management systems. For a broader look at the topic of interoperability and how different systems talk to each other, refer to the module Interoperability.

When an organisation tries to design a digital identity system for a blockchain solution, it is important to be able to support existing and common methods and technical requirements for digital identity. Any standards that are used or supported should also be considered especially for the interest of inclusivity. Such care for actors with limited access to technology will enable them to have a digital identity or otherwise use them.

As the blockchain deployment scales and the number and types of actors expand, interoperability of a digital identity system will play a crucial role.

When considering what technology standards to support in a digital identity system, understand what most of the actors in an ecosystem currently support or use. If a digital identity system for the supply-chain blockchain solution will support up-and-coming archetypes (e.g. decentralised identity) or technologies, one must consider how to bridge the gap that many of the actors in the ecosystem will inevitably face: how to interact with the blockchain solution based on different technologies than the deployment currently uses. Most identity systems in the real world operate based on centralised archetypes and support some federation protocols like SAML or OIDC/OAuth. In the meantime, some blockchain solutions want to move to a decentralised identity management model. Therefore, there must be a way to support interoperability between the two while actors are being onboarded to the new technology.

Critically, consider how to make the most of the transformation that comes with using a blockchain; while in the short term existing systems may need to be compatible with blockchain, a long-term strategy should more deeply consider the design of future systems and how to handle changes to technologies, standards, scale, and ways of doing business.

However, having standards does not guarantee acceptance. On an organisational level, it is critical that acceptance of the digital identity is established across the ecosystem well before any standards discussions take place. Acceptance of a digital identity is a matter of governance before it is a technical discussion.

Standards for identity management systems

Interoperability is what will enable scale for a digital identity system. Therefore, it is recommended that the supporting 'standards' that actors in an ecosystem already support, or that the market is moving towards, be a critical piece of the design of a digital identity system. If it is not standards-based, it will not be viable in the long-term.

For instance, National Institute of Standards and Technology (NIST) in the United States has defined Identity Assurance Levels (IALs) to define assurance levels for identity proofing, Authentication Assurance Levels (AALs) for authentication, and Federation Assurance Levels (FALs) for federation cases, in the context of identity for humans.[66] These governance rules help to unify the assurance in a digital identity – how stringent the procedures were for each identity proofing, authentication, and federation – across entities such that they can interpret and understand these aspects of a digital identity from other systems. And while often referenced with respect to human and consumer digital

identities, these standards on governance are defined such that they can be applied to any of the actors defined in this document.

Cybersecurity and digital identity

Integrity in a digital identity depends on the security of the technology that supports it. If the digital identity system is not secure, there is less assurance that the actors are really who they claim to be.

As digital identity is foundational to every transaction, it is critical that digital identities are managed by secure process and system.[67] This will not be a new effort but yet require endless efforts to manage systems security. See the module Cybersecurity, and more specifically for key considerations refer to focus areas Blockchain cybersecurity risk management and Blockchain secure deployment.

On the other hand, data protection in the sense such as data confidentiality and data integrity sometimes utilises digital identity system, such as role-based access controls or even private blockchains. These requirements, such as the security level, will influence to the design of a digital identity system. Requirements from the data-protection perspective are discussed in the modules such as Data Protection, Data Integrity, and Personal Data Handling. Also, the module Legal and Regulatory Compliance explains how laws and regulations may affect decisions – for instance, how personally identifiable information (PII) is regulated. The module Financial Reporting and Controls considers the auditing process of legal entity-related identity date and its use.

4. Future-proof your digital identity system

How can one ensure digital identities are sustainable and scalable to support ever-changing technology landscapes?

The initial building and implementation of a blockchain solution should be done with the future state in mind. While a digital identity system is enabled to support the blockchain solution, it must be sustainable in and of itself.

If the digital identity system cannot scale, or cannot be maintained long-term, then the blockchain solution is at risk of scaling to new use cases, products, industries, and jurisdictions. It is also important to consider how the blockchain solution can leverage existing tools and infrastructure to ease the burdens that come with the massive changes enabled by the blockchain solution and use case – and how any new models and identity systems interoperate with those existing systems. For members of the ecosystem, knowing the solution can grow with the ecosystem provides comfort that the technology will not be a limiting factor as they shift their business processes to accommodate it.

Scalability

Blockchain for supply chain will inherently involve numerous organisations and governments across sectors and borders. The number of people and devices involved will also grow. It's important to consider not just what will work now, or for the next 5 years, but what can be supported as the number and types of entities involved changes.

- **Cost and maintenance:** Looking at each type of actor and use case supported, understand how the digital identity system scales in terms of cost or complexity of maintenance. Analyse, also, how the technology that underlies the digital identity system scales, as well as any costs associated with scaling. For instance:
    - How much does the infrastructure cost to maintain, including both any existing identity systems being integrated with the blockchain solution and new pieces added to support digital identity?
    - How are upgrades to any digital identity components handled across the entire solution? Does each member of the network need to shut down all at once, for instance, or can upgrades be rolled incrementally? How are these upgrades tested?
- **Cross-sector interoperability:** Today, numerous sectors are conducting blockchain pilots using different platforms and different ways of managing identities. Some do not consider digital identities at all. As any supply chain crosses sectors, it is critical to consider how the data across blockchain platforms could be consumed and trusted, how blockchain platforms will need to interoperate across sectors, how blockchain platforms will adapt to innovative and scale for growth, and how identities will need to be verifiable and trusted across platforms and sectors.
- **Change management:** Consider if changes to a digital identity system would be prohibitive if the blockchain solution is scaled up. Understand how changes to requirements are evaluated, approved, and implemented, and if there is a governing body that plays a role in that process.
    - How is training of employees handled when a new digital identity system or processes are in place? How are legal entities informed of changes and enabled to make any corresponding changes in their processes? How are devices updated with any new identity requirements, software, etc.?
    - How are new features added? Who gets to decide what, if any, new capabilities are enabled? What is standardised across the ecosystem, and how does any governing body of the blockchain solution handle these decisions?
    - What happens if laws and regulations change, or if an authority changes identity issuance processes (for instance)? Who needs to be involved in understanding and implementing any corresponding changes to existing or new identities, and changes to processes in the identity system itself?

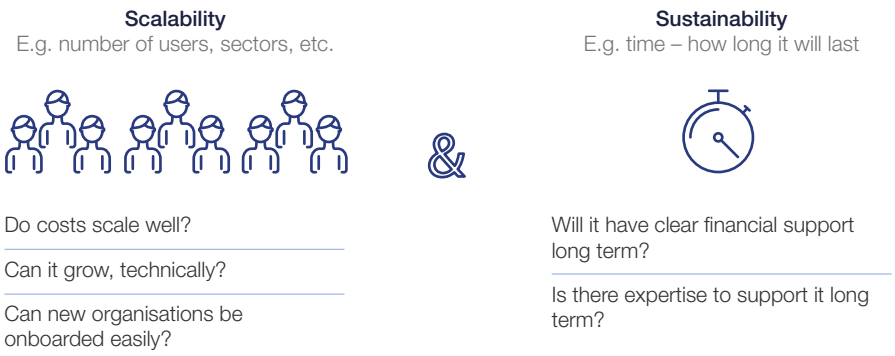


Figure 5.6 – A future-proven digital identity system must be scalable and sustainable

Sustainability

A digital identity system in any supply chain should have sustainable, long-term financial and maintenance plans to ensure its use and survival. Blockchain introduces new ways of working, which requires new cost models. To make a blockchain solution sustainable, it must provide a positive return on investment (ROI) for the organisations involved. This return may be achieved through lower costs or improved business efficiency, for example. Cost models must be shifted accordingly, to offer ways of sharing the burden of supporting and enhancing the systems that make it work – such as digital identity systems.

- **Financial model:** A digital identity system should have clear financial support, whether brand new or integrating existing digital identity systems. As blockchain solutions are inherently shared among different legal entities (and even different departments within those), it is important to understand how digital identity will be supported financially in this new way of working.
- **Maintenance & ongoing support:** Consider also how the technology that supports the digital identity system will be supported, maintained, operated and how changes can be implemented. To avoid a backlog of upgrades and maintenance that differ across actors, it is important to determine operating model and effective operations of the blockchain network in order to keep all relevant parties synchronised and secured. The digital identity parts require operations and support with the right skills and expertise, just like any other system.

Example

The Bitcoin blockchain compensates its miners for verifying transactions on the chain by rewarding them with bitcoins, thus providing a financial incentive to encourage its upkeep.

Example

The host of a blockchain will charge a fee for external stakeholders to cover cost of maintenance and provide the business a return on investment. The value the ecosystem adds to the stakeholders, through greater transparency and data availability, must justify the fee. If this is the case, a cyclical value chain makes the solution sustainable.

5. Defining and securing identity data

What data will be created and associated with particular people or entities in a blockchain solution, and what specific steps should be taken to ensure adequate protection of that information?

Data associated with a digital identity, commonly referred to as “identity data”, is a vital component in establishing trust among different stakeholders in a supply-chain ecosystem. You are what your attributes (or in other words your identity data) say you are. For instance, a logistics provider may ask a factory to provide it with identity data – like the entity’s legal incorporated name or a legal address – before doing any business with that factory.

You are what your attributes (or in other words your identity data) say you are.[68]

Digital identities are useful insofar as the identity data are accurate, up-to-date, verifiable, and securely managed.

This benefit also plays a critical role in linking the physical and digital worlds. This is accomplished by creating a digital twin, or virtual representation that clones a physical object. For example, a physical handbag moving through the supply chain has a digital record of movement assigned to its digital replica. In such use cases, what information is used for identity data, and how to create these links is an important component of a good digital identity for supply chain. (See the module Data Integrity for more information on digital twin integrity).

Key topics for consideration as part of a well-managed identity data process include:

Accuracy and verifiability

A trusted digital identity requires that critical pieces of identity data – for instance, the tax identification code of a legal entity – remain accurate, up-to-date, and verifiable. Consider how often that data changes and how a digital identity can remain fresh, and therefore trusted and relevant.

Feasibility and maintenance

For a digital identity to be sustainable, the data associated with it needs to be feasible to collect, to verify and maintain, or to otherwise reconcile. There are several factors to balance when deciding what information to include in a digital identity and how, including costs, time, accuracy, and liability. For instance, consider the following questions:

- **How often should identity data be verified for accuracy and updated?** What happens to a digital identity after an actor has been successfully onboarded? If, for instance, an ASA's software package has been updated, should that be recorded? Who is responsible for updating the digital identities of devices, and how? How much will it cost – versus the benefit received – to update and verify identity data? Is it sufficient to rely on annual audits, or should more regular verifications take place? It can be time and resource intensive to conduct deep assessments of the accuracy of identity data, but inaccurate data can render the digital identity less credible, if not useless.
- **What is the minimum amount of data necessary?** In this age of Big Data, it may be difficult to imagine not collecting every piece of identity-related data available – not just for people, but also for legal entities and things. Data minimalism,[69] in fact, is a rising trend due to the complexity and liability associated with holding identity records of many actors – where the data stores then become a huge risk for attacks and breaches. Consider collecting only the minimum amount of data necessary, to reduce complexity and liability.
- **Where possible, implement standards-based identity data and identifiers.** For instance, the Legal Entity Identifier (LEI) has enabled and standardised this identification process for financial transactions by providing each legal entity a unique identifier code based on a defined standard (ISO 17442). This will enable participants across the ecosystem able to render and understand critical pieces of identity data that enable digital interactions.

Confidentiality and privacy

A blockchain solution is only as valuable as the data the stakeholders choose to share on it – and how much other stakeholders can be trusted. To reach its fullest potential, a blockchain's architecture should ensure confidentiality and privacy protection of identity data – or risk losing trust in the other actors in the digital world and, therefore, any information they provide or transactions they perform.

Digital identities are composed of different data points that help to identify and authenticate an entity in different contexts. It's critical that the data – especially that which is private or a trade secret – remain confidential. Such data should only be accessed, modified, and controlled by authorised parties.[70]

More details on protecting commercially sensitive data and privacy data are found in the modules Data Protection and Personal Data Handling.

Data exchange in a blockchain world: on-chain vs. off-chain

While there are identity-specific blockchain platforms that have emerged, other types of identity data or sensitive data are not always considered with the

same scrutiny. With proliferation of blockchain solutions and the permanent nature of blockchain, it is critical that any sensitive data and different types of identity data are considered in their treatment – including what types of identity data may need to be off-chain – as part of the blockchain solution. It is recommended that if there is data that is considered private or sensitive – for instance PII of an employee or sensitive trade information – that data should not be stored on the blockchain. For more information on protecting personal data, see the module Personal Data Handling.

6. Process and governance

What are the important non-technical processes and governance points to consider when designing and building the digital identity system?

In a supply chain blockchain ecosystem where actors have different goals and incentives, and where laws and regulations lag technology, below is a list of important non-technical processes and governance points to consider when designing and building the digital identity system.

- **Identity and identity data ownership and stewardship:** It's important to establish who or what party is responsible for (and has the rights to establish, read, use, or update) an identity and related data. Consider the different roles, rights, and responsibilities that data owners, custodians, maintainers, etc. might have, and how they differ. It may not be entirely clear in some cases, and therefore it is important to establish upfront what these roles might look like. For instance, if a physical object is transferred from one party to another, or if custody changes, what responsibilities do each of the parties involved have? Federated Identity Management (FIM) has begun to explore this ambiguity. To address differences in security requirements among involved parties, participating members are required to implement policies that address the security requirements of all the members.
- **Liability, risk management and role of insurance:** If identity data turns out to be fake or wrong, who is liable? Is there a role for insurers to be part of the ecosystem to underwrite the risks? Standards and procedures should be defined and enforced in order to achieve a common baseline to reduce risks in the network e.g. level of due diligence required for identity proofing and for validating and accepting an identity. Define procedures and liability terms with levels of assurance that are universally understood and accepted for when something goes wrong. E.g. if one entity has a breach, how are identities revoked? How do other parties reduce risks and exposure? Understand who is liable and responsible for what and outline a plan for remediating any costs and disputes. Plan for these situations so it's clear who is responsible in the aftermath and beyond to create a resilient system.
- **Digital identity system governance & maintenance:** Maintaining an identity system is more than ensuring the technology is functioning correctly. As ecosystems and use cases change, the processes that support and structure a digital identity system may also need to change. Consider how to evaluate the overall health and functionality of the system.

- **Starting out:** Building a digital identity system for an ecosystem effort in blockchain will require collaboration and agreement in the very beginning. For instance, digital identities and identifiers will need to be established from the very beginning of the supply-chain use case – how can this be efficiently and effectively done, especially where not all the actors in supply chain are known? Or how is proper "use" of identity defined? Understand what problems need to be solved from the beginning and work out where collaboration is required.
- **Maintenance:** An actor may participate in many different supply chains or ecosystems; look for opportunities to collaborate or establish interoperability. Especially in the case of omnipresent organisations, for example, large scale shipping companies, a verified digital identity can be leveraged across multiple supply chains. Additionally, map out theresponsibilities in terms of cost and maintenance.
- **Monitoring and oversight:** Establish metrics that could be used to view and understand the overall health and success of the digital identity system and how it could be improved to better support the blockchain solution for supply chain. Additionally, consider establishing independent oversight of the digital identity system; especially in an ecosystem where many different entities are involved, it is important to have a neutral body, entity or procedure that can help ensure the trustworthiness and integrity of digital identity.

- **Regulatory considerations:** Identity often is regulated and can involve highly sensitive information. Given that many supply chains span multiple countries or jurisdictions, complying with these regulations or ensuring privacy can get complex. The International Traffic in Arms Regulation (ITAR), for example, controls the movement of defence-related materials. A blockchain operating in this environment would be limited to publishing only ITAR-compliant data on the chain – and therefore any identity-related data must ensure compliance with that regulation. It is important to design a new blockchain for supply chain use case with these considerations in mind.

7. Decentralised identity considerations

How is decentralised identity a different model, and what additional governance and technology decisions need to be made?

As adoption of a decentralised model for identity is emerging, technology and standards are evolving. While ideal case is a single solution to work for all global supply chains, the reality is that most supply chains are incredibly different from one another, so different solutions may emerge on a case by case basis. For example, consider how a milk supply chain differs from a coffee supply chain. A milk supply chain may operate entirely within one country versus a standard coffee supply chain will operate in a few – so the regulations that each may adhere to with regards to identity information will be different. The actors in these environments may be entirely different – where milk, for instance, may involve strict refrigeration requirements and therefore requires monitoring at every step, whereas coffee may be a more robust product and involve very different transportation methods, companies, etc. And, of course, the types of data and information that both may need to

handle will be extremely different. Where a single solution could add value is within a narrow and very homogenous industry, for example, the airline industry. Across the industry, companies face similar issues, supply chains include similar (if not the same) stakeholders, etc. This similarity across the industry invites the potential for a more universal solution across the industry.

It is critical to understand what recurring considerations need to be addressed when creating a decentralised identity ecosystem – including operational considerations (e.g. who operates nodes, and the responsibilities of each node or actor involved), technological considerations (e.g. technology design and support), and governance of the decentralised identity system. Decentralised identity is still very much an evolving space and will require ongoing evaluation.

Decentralised identity may be a great archetype to use to help preserve the benefits of decentralisation in a blockchain solution for supply chain. However, it is again important to consider interoperability and even a hybrid model for identity; organisations, especially in a supply chain world where changing the procedures of many organisations, people, and thing is necessary for moving to a new technology, may not be able to move to a fully decentralised model for identity for reasons such as cost, time, change management complexities, and others.

Decentralised identity standards

As identity is often considered more sensitive and requires different security architecture and privacy considerations, specific models and platforms have emerged in blockchain for identity e.g. Hyperledger Indy, DIF. Standards that are specific to decentralised identity are also emerging, such as ISO TC307 (Working Group 2). Additionally, a working group under the W3C began to define a standard on Decentralised Digital Identities in September of 2019.

Common data standards and technical standards are critically important for decentralised identity to be adopted in supply chain. Emerging standards exist today for decentralised identity but most of these relate to people (e.g. ERC 725, DIDs). These will need to be adapted and considered specifically for legal entities, connected devices, things, and ASAs. For organisations adopting decentralised identity for blockchain in supply chain, it is essential to keep abreast of these changing standards, as this will greatly influence future success of the solution and its adoption. Standards will help to drive interoperability across industries and supply chains for blockchain to deliver business value.

Example

ERC 725 is one example of a proposed industry standard. This standard allows users to manage their identity across all platforms that support it, instead of forcing the user to forego ownership of their identity to a centralised organisation.

Organisations need to consider these as some blockchain platforms are not well suited for the identity use cases. It is recommended to use built-for-purpose blockchain platforms: those that have been designed with identity as the central use case, though the platform should be evaluated on a case-by-case basis.

Technical design

Consider up front which blockchain should be used, and what model will be supported (e.g. public or private, permissioned, etc.), and how identity data should be stored – for instance, if sidechains or other archetypes are necessary to support privacy considerations. Given the evolving nature of blockchain as a relatively new archetype, consider if or how a hybrid model could be supported and how current architectures and technologies used for digital identity might be integrated to support a smoother and quicker transition.

Ecosystem technology support

Understand who will support the technology in the ecosystem – for instance, who will run nodes, and what changes in technology or policies will be required throughout the ecosystem to support the new model. It is important to note

that blockchains with fewer nodes (such as new platforms or those that have been abandoned by most of their nodes) are more susceptible to being compromised by malicious actors, because it is easier to achieve a majority.[71] For this reason, a well-defined ecosystem of technology support will make a blockchain more secure.

Businesses and international standards organisations such as Digital Bazaar and GS1[72] and IBM[73] are building decentralised identity systems that will verify identity of stakeholder in a global supply chain, enabling a global interoperable system of identity management. These systems, in the future, can be used by a newly established ecosystem to verify legitimacy of each stakeholder. While these types of identity systems are still emerging, it is important to keep close watch on how they evolve.

Examples

Digital Bazaar and GS1 Proof of Concept (PoC) to build verifiable identities for stakeholders, with an emphasis on supply chain and shipping.

IBM Trust Your Supplier: The blockchain addresses issues in supplier management, including validating supplier credentials, supplier onboarding, and lifecycle management.

Data storage and validation

The way identity data has been traditionally stored, maintained, and used changes in a decentralised model.

- **Data storage:** What identity data is considered private? This data should not go on chain, rather, it should be stored and accessed by a different model that ensures the privacy of data in the long term. Consider a model like Decentralised identifier (DID)[5] - identity data that is deemed private is stored off the blockchain; and in its place on chain, is reference information that indicates where that data exists. Conversely, data that is not considered private can be stored on chain. Creating environments with specific entitlement requirements based on privacy, reinforces the access security across users and ensures the security of data that is considered private is not compromised.
- **Validation:** While in the long term, a centralised PoE issuing authority may develop, in the short term there is no universal centralised solution. Thus, a decentralised identity model introduces a new way of working, which is characterised by a non-centralised responsibility for identity data validation, to ensure actors involved are legitimate. How is identity data validated in this new decentralised model? Understand any additional actors or processes that need to be included, or what changes are necessary, to support this new way of working and maintain an acceptable level of accuracy and authenticity of identity data in the ecosystem.

Governance

Adopting a decentralised archetype for digital identity introduces new ways of working and thinking about digital identity – where regulations may lag and traditional polices on identity are not effective means of governing and securing decentralised digital identities. Decentralised identity, operated by a consortium model typically built on top of distributed ledger, has specific considerations to tease out.

While enabled by technology, successful implementation requires thorough governance considerations including:

- **Operating models:** How are decisions made when there is no central authority governing the digital identity system, and what roles do ecosystem participants play? The concept of digital identity ownership changes from a traditional model when moving to a decentralised model. For instance, in a centralised identity model, the system owner owns, and is responsible and liable for, all the identities it contains. What policies and operating models need to change?

  The Depository Trust & Clearing Corporation (DTCC) is building a blockchain-based solution for reporting of credit default swaps (CDS). This solution unites many different stakeholders within the ecosystem, so DTCC and Accenture teamed up to define governance and the operating

model for the solution. In defining these terms, DTCC hopes to instil confidence in the safety of information in the network, so stakeholders engage fully.

The DTCC,[74] for instance, has defined a governance and operating model for a blockchain platform.

- **Policies and regulations:** How are policies enforced across a decentralised identity ecosystem – especially where laws and regulations have not yet caught up to a decentralised identity model? Having independent oversight and collaborating with public authorities on developing regulations can ensure development of policies that positively affect a decentralised model – such as ensuring its longevity or promoting collaboration between parties. Consider also how auditing and reporting requirements can be met, and how a regulator or auditing role and a corresponding audit node can be supported. Refer to module Legal and Regulatory Compliance, for several legal issues that arise when making use of decentralised digital identity systems.
- **Wide, cross-cutting impacts:** Look beyond the walls of a single use case and single network – what roles to other ecosystems or networks play, and how can digital identity enable new or different operating models across different use cases, ecosystems, and networks? For instance, how does the digital identity of a legal entity in the context of a single handbag supply chain interact with a digital identity system built for consumers of those handbags? Digital identity is most useful when it operates beyond silos, but given the complexity, significant work is needed to establish a cross-cutting governance model and understand the impact beyond the interactions of a single network or single type of actor or entity.

> *And you might ask, what's the benefit of digitalising the supply chain. Simple. A country that can't have or lacks seamless e-trade capabilities - can't have strong economic ties, because having an economic relationship is a form of trading itself. This toolkit will help everyone to understand more about digital identity and to make it accessible as possible.*
>
> **Jana Krimpe,** Co-Chair, Global Alliance for National Mobile Identities

TOOLS AND RESOURCES

8. Mapping out actors and interactions

The below table may be useful in starting to define the actors involved in an ecosystem. The rows include potential actors contributing in an ecosystem. The columns depict different considerations and interactions within the ecosystem.

For example, different actors will have different privacy and compliance considerations. Fill in the table to help outline those actors and define how their considerations and interactions differ from one another.

A description of each column and its meaning follows:

- **Examples:** It may be daunting to list all the actors involved, but listing out a few examples of, say, the important legal entities a blockchain use case deals with can help to understand the scope and nuances of actors.
- **Trust Anchors:** Who are the primary trust anchors involved in providing the underlying trust in who an actor says they are? For instance, legal entities and public authorities are generally the trust anchors for people.
- **Interactions:** With whom or what does an entity directly interact with for a given scope of transactions for a blockchain? For instance, a person may interact with passive physical objects to scan a barcode and may interact with a public authority to submit compliance reports.
- **Privacy and Compliance:** What major rules dictate any privacy considerations for this actor? Legal entities won't want to reveal trade secrets, for instance, but how does that affect, say, ASAs acting on behalf of that legal entity? And what information is required to be reported that may be related to an actor's digital identity?

- **Lifecycle:** Give a brief description of what a lifecycle for this actor looks like for a use case. How are ASAs updated, for example? Or how are new physical objects (active ID) commissioned or de-commissioned? This will help understand the lifecycle of the digital identity of the actor.
- **Geography considerations:** For this particular actor and a use case, what additional rules or regulations apply for any specific geography? This will mainly affect privacy and compliance, but may also dictate, for instance, which trust anchors apply to an actor or a specific way lifecycles must be managed.

Table 5.1 – Mapping table to organise digital identities and related considerations

	Examples	Trust Anchors	Interactions	Privacy & Compliance	Lifecycle	Geography Consideration
Legal Entities						
Public Authorities						
Autonomous Software Agents						
Physical Objects (Passive ID)						
Physical Objects (Active ID)						
People						

9. Processes and governance questions to resolve

This tool is not intended to be fully comprehensive but rather to provide a starting point for the types of processes and governance questions to understand and solve. Working through this checklist will provide a strong foundation for such considerations in developing a digital identity system. Users are encouraged to think beyond this list and understand what unique considerations need to be included in a particular project.

Identity data ownership and stewardship:

- ☐ Define clearly what roles exist for identity data ownership and stewardship, for instance:
  - Data owners
  - Custodians
  - Maintainers
  - Auditors
- ☐ Establish clear policies and procedures on:
  - Assignment and transfer of roles
  - Education on rights and responsibilities to role holders
  - Security policies and access rights for each role
  - Mediating ambiguity in role definitions

Liability, risk management, and insurance:

- ☐ Understand threat models and what risks there are regarding digital identities and identity data. For instance:
  - Data inaccuracy
  - Identity proofing or authentication errors, or other procedural errors
  - System breaches
- ☐ Define procedures and liability terms with levels of assurance that are universally accepted.
- ☐ Outline a plan for remediating costs and disputes.
- ☐ Explore and understand where cyber insurance may be applicable.

Digital identity system governance and maintenance:

- ☐ Establish a clear group responsible for the governance, maintenance, and design of digital identity for a blockchain solution.
- ☐ Establish a way to collaborate across the ecosystem and within the governance group to define policies, roles, procedures, etc.
- ☐ Define standards on digital identity data and processes across the ecosystem from the very beginning.
- ☐ Understand maintenance activities and costs, and assign them to specific owners.
- ☐ Define and continuously evaluate metrics that could be used to view and understand the overall health and success of the digital identity system.

Regulatory compliance and oversight:

- ☐ Work with legal and compliance teams to map out any regulations that an identity system must comply with across jurisdictions – including privacy regulations.
- ☐ Consider and implement independent oversight of the digital identity system.
- ☐ If not already required, establish procedures for regular audits and compliance checks.

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]

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.

> *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

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.

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.

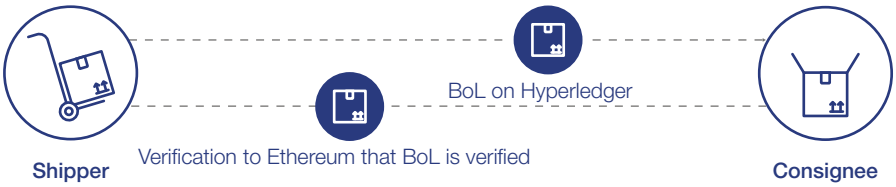


Figure 6.2 – Illustration of how ownership of the Bill of Lading (BoL), which is arbitrary data, can be transferred from a shipper on Ethereum to a consignee on Hyperledger

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?

> *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

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]

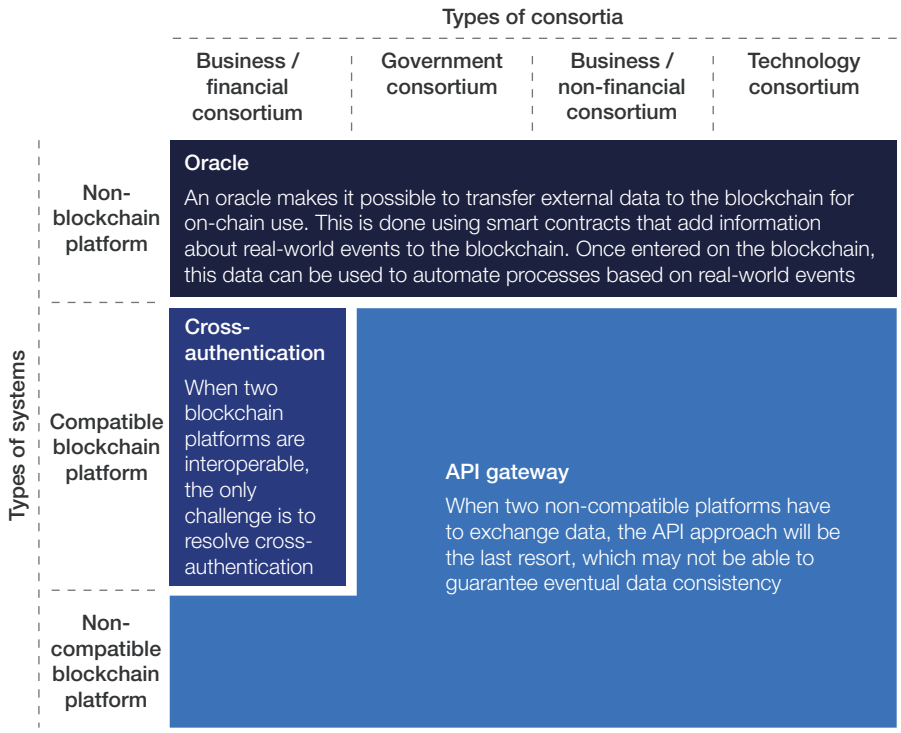


Figure 6.5 – Four context-dependent approaches to blockchain interoperability

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?

MODULE

Structure: Public / Private

Overview

Focus Areas

1. Points to keep in mind when choosing a blockchain structure
2. Navigating the blockchain structure decision

Tools and Resources

3. Navigate requirements gathering

Overview

For supply-chain organisations launching new blockchain projects, one of the most fraught considerations typically is whether to use a public or private ledger, and with what permission models. A public blockchain like Bitcoin's allows anyone on the Internet to read or write to the shared ledger, while a consortium-run blockchain might restrict access to partner organisations, for example.

Ultimately, the "public-versus-private" decision will affect functionality, security, compatibility with other partners' systems, and, perhaps most important, competitive positioning for organisations in their supply-chain projects. To be sure, there is no one "correct" answer. Rather, it is vital to first understand the unique benefits and drawbacks to each type of chain, then choose the one best suited to your particular project's requirements.

Recommended reading – Inclusive Deployment of Blockchain for Supply Chains: Part 3 – Public or Private Blockchains – Which One Is Right for You?[93]

FOCUS AREAS

1. Points to keep in mind when choosing a chain structure

What are the specific factors related to the needs of a particular project and its participants that affect the decision whether to utilise a public or private blockchain?

In 2018 and 2019, the World Economic Forum dove deeply into the evolving discussion on whether public or private blockchains are typically best suited for the supply chain industry. Key findings of this body of research include:

- To the extent that organisations in the industry have experimented with blockchain technology so far, both public and private versions have been useful in achieving different objectives and meeting project requirements.
- The supply-chain industry is generally cautious about adopting new technology tools such as blockchain. Collaboration and data sharing among organisations have traditionally not been the norm. Thus, new entrants aiming to encourage blockchain adoption are likely to face challenges, and many see private technologies in the near term as a path for the industry to begin using blockchain.
- As the industry explores private blockchain solutions, it is important to distinguish the benefits associated with public or private chains versus those of traditional solutions for sharing data. Being aware of the pros and cons of blockchain and understanding where its features really help to solve a problem will help to prevent the new technology from becoming merely an expensive version of a centralised database. In use cases where the unique advantages of blockchain aren't particularly helpful, solution providers may opt to stay with, for example, an SQL or NoSQL database or a similar traditional solution.
- The public-versus-private blockchain debate has received much media and industry attention in the supply chain industry over the past two years, perhaps to a degree that it can distract from what is really important. Many experts point out that for supply-chain solutions, it is also important that the industry move past the public-versus-private debate to one focused on deploying solutions where organisation- and enterprise-specific requirements can be met. Blockchain solution requirements should be tailored for all potential considerations and safeguards. Figure 1.2 (Essential considerations typical for enterprise technology solutions) outlines typical requirements that organisations need to address to ensure the success of any new enterprise solution. These are the same characteristics that your IT team would identify as essential for any technology implementation.

Being aware of the pros and cons of blockchain and understanding where its features really help to solve a problem will help to prevent the new technology from becoming merely an expensive version of a centralised database.

2. Navigating the blockchain structure decision

What questions must be addressed when making a rapid initial analysis of whether a public or private blockchain is appropriate solution for the use case?

These seven questions are typically important in deciding which blockchain structure to use for a particular project. Note, this list is not intended to provide a final authoritative answer, but to assist in a rapid initial analysis. These questions can be used in conjunction with the public-versus-private decision-making worksheet (Table 7.1 – A worksheet to navigate requirements gathering and public-versus-private decision-making).

It is important to remember that structure is only one aspect of the technical solution – decision-makers must always take into account the context of their selected use case and distinct requirements (Figure 7.1 – Seven questions to enable a rapid analysis of whether public or private blockchain is most suited).

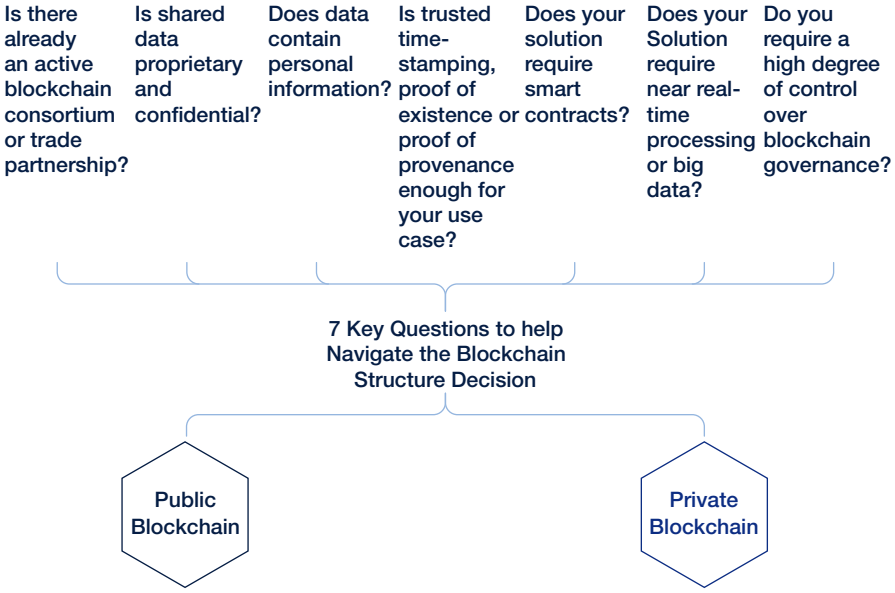


Figure 7.1 – Seven questions to enable a rapid analysis of whether public or private blockchain is most suited

1. **Is there a blockchain consortium or trade partnership that is already active in the industry or specific to the use case?**

   If so, decision-makers need to think hard about whether they wish to deviate from it. It is often substantially cheaper and less time-consuming to accept an imperfect solution over a custom one. After all, the latter tend to become useless in cases where a consortium solution eventually morphs into an industry standard. Obviously, if organisations believe they can mount a credible challenge to existing solutions, gain critical mass to make them successful, and possibly become dominant in the marketplace, a custom build is a viable strategic option. To a lesser degree, the same is true for projects within organisations. If there are ongoing blockchain projects or deployments within an organisation, it is often easier, faster, and more cost-effective to leverage the underlying technology before embarking on a second or third project that leverages

a new platform or protocol. Ideally, all previous investments ought to be leveraged.

2. **Is shared data proprietary and confidential?**

   If so, then the decision turns to how much and which data needs to be kept on-chain. As soon as shared confidential data is written to a blockchain, a private configuration or hash-based solution on a public blockchain can be one way to handle this situation. In cases where proprietary databases can keep shared and confidential data secure, a public configuration may be better positioned for an organisation. Public blockchains are also exploring innovative privacy measures, which means that their value proposition can develop over time as stakeholders prioritise data protection. Zero-knowledge proofs are one such example.

   If a project requires the handling of confidential and proprietary shared data, combined with public verifiability as well, a public permissioned system will likely be required.

3. **Does data contain personal information?**

   In cases where personal data is involved, data protection and data privacy laws like the European Union's General Data Protection Regulation (GDPR) need to be considered. Because anyone can join a public permissionless blockchain, it is difficult to ensure that blockchain network participants comply with necessary rules around the protection of personal data. As a result, if data must be kept on-chain, the permissioned blockchains are more likely to be designed towards a GDPR-compliant blockchain solution. However, using private chain, by design, will not alone guarantee a GDPR-compliant solution. For more details see the module Personal Data Handling.

4. **Is trusted time-stamping, proof of existence, or proof of provenance enough for the use case?**

   Time-stamping builds trust, fosters higher levels of accountability, and serves as a great way to resolve conflicts and disputes. If this suffices, a solution in which a hash is written to the blockchain and used to validate that documents have not been altered is suitable. In these situations, a public blockchain is typically faster to implement and the variable cost of writing data can be contained through the aggregation of entries. For example, you can take a contract and store its hash on blockchain. Then, if there is a dispute about which contract is real, you can do a hash match to the one stored on the ledger. That said, some warn that you can run into a lot of challenges standing up a new public blockchain for one-off use cases.

5. **Does the solution require smart contracts?**

   Use of smart contracts is not limited to private blockchains; however, some public configurations need to be augmented through an additional technology layer to add smart-contract capabilities where they do not exist. A good example is what Rootstock (RSK) does for the Bitcoin blockchain. There are also public blockchains that support smart contracts natively, without additional layers, as the Ethereum protocol.

   More importantly, given the nature of supply-chain use cases, it is likely that you will need to input sensitive business data into smart contracts, if your solution is using them. Since the data input to smart contracts are visible to all users, a public blockchain may not be a good solution when you want to limit visibility to a transaction but still reach consensus.

6. **Does the solution require near real-time processing or does it need to handle large datasets?**

   In either case, private configurations are likely a much better solution. Public blockchains – at least as they exist today – are severely constrained when it comes to file size, processing speed, number of transactions, and the cost of processing each transaction.

7. **Is it necessary to have a high degree of control over blockchain governance?**

   Blockchain governance refers to the mechanisms by which decentralised node networks adapt and change over time. This includes decisions like changes in block sizes, data storage formats, smart-contract execution protocol, consensus mechanism, and more. If you do not require control over such decisions, and the way a blockchain configuration works today is sufficient, then reputable public blockchains are often superior as they are less prone to drastic governance changes. Reputable public blockchains are more stable because of the large numbers of users need to agree to governance changes. In cases where your organisation requires more control over the network governance or requires control over business processes, data formats and transaction processing, a private chain is likely the better choice.

TOOLS AND RESOURCES

3. Navigate requirements gathering

What questions must be addressed when making a rapid initial analysis of whether a public or private blockchain is appropriate solution for the use case?

As decision-makers weigh the public-versus-private question, they must typically consider several requirements that the blockchain solution should meet. For each requirement, the performance and benefits of public versus private blockchain will differ. Collecting and understanding these requirements from your business for the specific use case is a first step in the decision-making process of choosing private versus public.

This outline provides the most common requirements in public-versus-private decision-making based on a survey conducted by the Forum of more than 40 organisations across many supply-chain use cases. The worksheet can be useful as organisations gather business requirements and understand whether a public or private blockchain will best serve those needs. This is not an exhaustive list but can serve as a starting point to collect key requirements from the organisation.

The importance and priority of each requirement may vary greatly and will have to be determined with the specifics of each use case in mind. Factors may include how many partners are included in the solution, what primary customers and partners are already doing (perhaps you are joining a consortium), what use case is being addressed, or what types of goods and materials are involved.

Table 7.1 – A worksheet to navigate requirements gathering and public-versus-private decision-making

Requirements	Essential, High / Low Importance	Potential Implications	
		Public Blockchain	Private Blockchain
Alignment with industry			
Alignment with internal			
Access to data			
Personal data protection			
Level of trust and accountability			
Smart contract			
System performance			
Control over governance			
Data integrity, availability, and security			
Interoperability and standards			
Total cost of ownership			
Need for payments integration			
System switching cost			
Alignment with other internal blockchain solutions			
Needs of public verification			
Use-case specific compliance			
Human resources and talent			
Add others of relevance			

Following is a description of each requirement to help in setting the priority and reflecting the implication on each blockchain scenario.

Alignment with industry: Considering what key customers, partners, standard bodies and the industry are already doing is important. Is there a blockchain consortium or trade partnership that is already active in your industry or specific to your use case? If so, decisionmakers need to think hard about whether they wish to deviate from it. It is often substantially cheaper and less time-consuming to accept an imperfect solution over a custom one.

As politics and trade wars loom over us more and more, consider whether a specific private blockchain technology provider will be acceptable across geographic region where you are active.

Example

When key business partners have already joined a blockchain consortium such as R3, Energy Web Foundation, or B3i, it may be made moot for individual organisations to ponder a solution that deviates from the consortium's collective action.

Alignment with other internal blockchain solutions: To a lesser degree, the same is true for projects within organisations. If there are ongoing blockchain projects or deployments within an organisation, it is often easier and faster to leverage the underlying technology before embarking on a second or third project that leverages a new platform or protocol. In this manner all previous investments can be leveraged.

Access to data: In a public blockchain, anyone can access and take part in the ledger, while in a private blockchain, only selected parties can access and make changes to the distributed ledger. In a public blockchain, transactions are broadcast to every single participant (node) and every node thus keeps a complete record of the entire transaction history. Private blockchains limit access to the blockchain to only those organisations that have been admitted into the blockchain network. Different types of permissions can be granted to participants of a network:

- Read: Who can access the ledger and see transactions
- Write: Who can generate transactions and send them to the network
- Commit: Who can update the state of ledger

Most data found in supply-chain transactions today is confidential. More commonly, data protection concerns have made organisations more willing to deploy private solutions in lieu of using public blockchains. (For a more detailed discussion of such concerns, refer to the design options explored in the toolkit module Data Protection).

Physical storage of data should also be kept in mind when using a private blockchain. Consider issues related to data ownership on physical storage media, potential size, and protective measures against unauthorised use and access of blockchain data.

Personal data protection: For supply-chain operators considering public blockchains, personal data protection is a critical concern. For more details and considerations around user privacy in blockchain solutions see module Personal Data Handling.

Level of trust and accountability: Refer to question number 4 in focus area Navigating the blockchain structure decision.

Smart contract: Refer to question number 5 in focus area Navigating the blockchain structure decision.

System performance: Performance, or the speed with which transactions are written to the blockchain, is another important consideration in that public blockchains in general tend to be slower than private versions. This can be due to a number of factors, including wider polling to achieve consensus and, in some cases, outright limits on transactions or block sizes. If users need to store large amounts of data on the blockchain, a public chain can thus be problematic.

Data integrity, availability, and security: Generally blockchain enhances the data-integrity posture. With that being said, a public and well-established blockchain could be more appropriate to achieve data integrity goals. Getting sufficient control to rewrite the ledger over a public blockchain is more difficult for an attacker than in a private chain with fewer nodes. In terms of information availability, the processing power of a private chain allocated to the business case can be fine-tuned to meet particular processing time constraints. By contrast, a public chain potentially incorporates a higher level of redundancy and may tend to be slower in verifying transactions.

Example

CargoX, a blockchain-backed platform that enables exchange of digital original documents worldwide builds on top of a public blockchain supporting smart contracts - Ethereum. Blockchain is used to store digital fingerprint of the documents (hash) and document ownership information. Documents are encrypted and stored off-chain - in a decentralised file storage Interplanetary File System (IPFS). Smart architecture guarantees that CargoX is GDPR compliant and censorship-resistant even by using a public blockchain which allows it to unlock features that public chains have to offer.

Interoperability and standards: Public blockchains are more interoperable today since they are based on widespread common understandings about how blockchain networks should operate. By contrast, private blockchains are always dependent on different parties within a system coming together to agree on their own shared standards from scratch. It remains to be seen whether private blockchain providers can garner enough support to cover broad industry requirements in this way.

In parallel, organisations such as the International Organization for Standardization (ISO) and industry groups such as the Blockchain in Transportation Alliance (BiTA), Digital Container Shipping Association (DCSA), The World Wide Web Consortium (W3C), EU's International Association for Trusted Blockchain Applications (INATBA), and the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) are driving standardisation and the development of quasi-standards as well. These efforts will help to proliferate not just technical standards but also effective methodologies for use in public and private blockchains. For more details, refer to focus area Business model layer in module Interoperability.

Total cost of ownership: The cost per transaction, often referred to as "gas" in public blockchains, is a fee paid to the creator of a block for writing data. This cost can vary substantially and can depend on traffic, so that users may pay more per transaction as volumes go up. With scalability solutions that public blockchains are developing, cost per transaction is expected to significantly drop. Private blockchains typically do not involve gas fees or limits on usage or block size; however, it takes resources to maintain and support the blockchain infrastructure.

With a private blockchain the upfront costs are typically several orders of magnitude higher. Public blockchains tend to require a substantially lower upfront investment to launch a new project or application, especially when organisations deploy hash-based solutions.

Cost considerations are usually easy to resolve with side-by-side comparisons that focus on the total cost of ownership over longer periods of time.

Operators should also be cognizant of system switching cost, or the total cost of moving from one blockchain solution to another. An industry consortium, for example, will likely be interested in maintaining stability and may deliberately select a private blockchain precisely because it bears an inherently higher switching cost. This creates an incentive not to exit the consortium, which in turn can keep participants aligned over the longer term. At the same time, it could also lead to a slower pace of evolution.

Need for payment integration: Some solutions for blockchain have integrated cryptocurrency payments, but it has been more typical to date to handle payments using fiat currency. Given the industry's general preference to date for private blockchains, this is perhaps to be expected.

Private chains often use tokens to represent a value that can be transferred to and from a fiat currency. This may yet change over time, however, depending in particular on how financial services providers implement blockchain in their operations. On public blockchains, use cases involving payments in cryptocurrency have already been well-established, thanks to Bitcoin's global popularity. This notably includes payments to block creators, though public chains are well-suited for other payment integrations as well if desired in a particular project.

Control over governance: Public blockchains are often governed by all, or a majority of, participants, which can lead to decisions that oppose the interests of supply-chain operators. In private chains, there tends to be closer alignment of objectives among participants to begin with, so ongoing governance is often

less of a concern. That said, private chains can also experience challenges in relation to governance when the interests of diverse supply chain nodes do not align – for example, between shippers and carriers or intermediaries. The owner of a private blockchain may also make decisions counter to the interests of other participants, such as raising prices or implementing new transaction fees.

Some of these conflicts can be avoided if the initial setup of a consortium for a private blockchain is handled properly. All parties need to have general alignment on objectives, benefits and processes. They need to agree on underlying technologies, and there needs to be a negotiation when trade-offs occur.

Needs of public verifiability: For some applications that require open distribution of records or where public verifiability is required – for instance government agencies that must respect public-records laws – a public chain would probably be a better fit.

Use-case specific compliance: The choice of a public or private blockchain also depends heavily on compliance requirements that the use case in question may mandate. Within heavily regulated industries, for instance, private chains will tend to be more prevalent, since data can be protected in a more tightly controlled way for compliance purposes.

Human resources and talent: Availability of coders in the specific language and blockchain developments. For example, when primary business partners have already joined a blockchain consortium such as R3, Energy Web or B3i, it may be made moot for individual companies to ponder a solution that deviates from the consortium's collective action.

> *Very few institutions have the requisite skills to run bleeding-edge decentralized architecture and applications.*
>
> **Souleïma Baddi,** Chief Executive Officer, Komgo

To reflect on the considerations outlined in this module, below is a list of real-life examples applied across various business scenarios:

Port of Valencia: Improving container management

The Port of Valencia solution, called GESPORT 4.0, aims to digitise documentation, increase process efficiency and ease communication. The port experimented with public and private chains and recently developed a private permissioned solution for container management that is based on Hyperledger Fabric.

The organisation selected a private permissioned blockchain solution for several reasons, including the existence of sensitive data, the need for governance via a community of stakeholders, the ability to store data and the avoidance of convoluted consensus mechanisms. In addition, decisionmakers looked into performance, transaction volume, system scalability and security prior to their commitment to Hyperledger Fabric.

Key considerations: Access to data, control over governance, personal data protection, system performance

Everledger: Making a private chain a diamond's best friend

Everledger, a private blockchain solution focused on diamond traceability, uses high-resolution imagery at every touchpoint along the supply chain to uniquely identify each stone and record its characteristics, serial number, chain of possession, location and condition, along with certificates of authenticity and payment documents. The solution requires privacy, not least because the whereabouts of high-value items needs to remain concealed.

Key considerations: Access to data, system performance, data integrity, availability, and security

Truckl: eliminating costly mistakes along the supply chain

In Truckl's solution, all participants in a transaction share the required documents while carriers collect data before, during and after a load is delivered. Information updates are made available on a dashboard and when exceptions occur, they are documented, and all parties receive instant alerts and notifications. Every aspect of a transaction ranging from documents to photos, signatures or location data is recorded in a transaction file, which is then hashed and written to the blockchain. This provides visibility focusing on eliminating errors, miscommunication and exceptions in transport transactions.

Users capture several benefits from the use of blockchain, amongst other that participants are encouraged to act honestly and openly, there is a single source of truth for documents, and transaction files are valuable as soon as disputes or insurance claims occur. Each authorized party has access to the documents and can audit transactions using Truckl's blockchain features.

The company determined early on that its users do not need to share information directly on the blockchain and subsequently implemented a hash-based solution so that customers and business partners can validate documents (proof of existence) on the public Ethereum blockchain. The solution is censorship-resistant, and the public nature of blockchain means that Truckl has no power to interfere.

Key considerations: Access to data, data integrity, availability, security, and system performance

Tradewind Markets: Provenance management for precious metals

Tradewind Origins is a provenance application that unlocks the latent value of precious metals by delivering data on how, when, and where assets were sourced. It links detailed information about the provenance of precious metals to digital records of ownership to distinguish sellers and buyers based on their unique characteristics. Tradewind selected R3's Corda due to its ability to isolate data, offer privacy, and provide a developer-friendly technology. The organisation decided on a private permissioned blockchain to meet the strict data privacy requirements of the platforms' users, and the ability to share information on a need to know basis amongst different supply chain participants. The desire for confidence around data confidentiality and ensuring no reputational risk for clients was a key driver. In addition, the ability to use a private platform to create enterprise tokens to represent precious metals as digital assets was key. The organisation also considered cloud deployment options, performance, and security prior to their commitment to Corda.

Key considerations: Access to data, control over governance, system performance

MODULE

Data Protection

Overview

Focus Areas

1. Protecting commercially sensitive data
2. Technology solutions for data protection
3. Case study: a manufacturing conglomerate

Tools and Resources

4. Data protection strategies

Overview

The perceived loss of control over data is one of the biggest obstacles to blockchain adoption that many supply-chain organisations face. With good project planning and communication, however, this issue can be greatly mitigated.

Blockchain technology never requires an organisation to reveal more data than it is comfortable with. On-chain data can also be encrypted so that it is only usable by permissioned parties. Thus, in the course of selecting and deploying a blockchain solution, a supply-chain organisation has real flexibility to ensure it addresses both its data protection and privacy concerns and those of other supply-chain partners.

Recommended reading - Inclusive Deployment of Blockchain for Supply Chains: Part 4 – Protecting Your Data[94]

1. Protecting commercially sensitive data

What are the top action items to consider for protecting the confidentiality of sensitive data shared on a blockchain network?

There are two fundamental questions to answer when building a data protection structure for a blockchain network:

- Which supply chain partners need to have access to which pieces of information?
- Who, external to the system, should have access to what information?

The typical requirements baseline among supply-chain organisations for sharing data include the following four dimensions as shown in Figure 8.1.

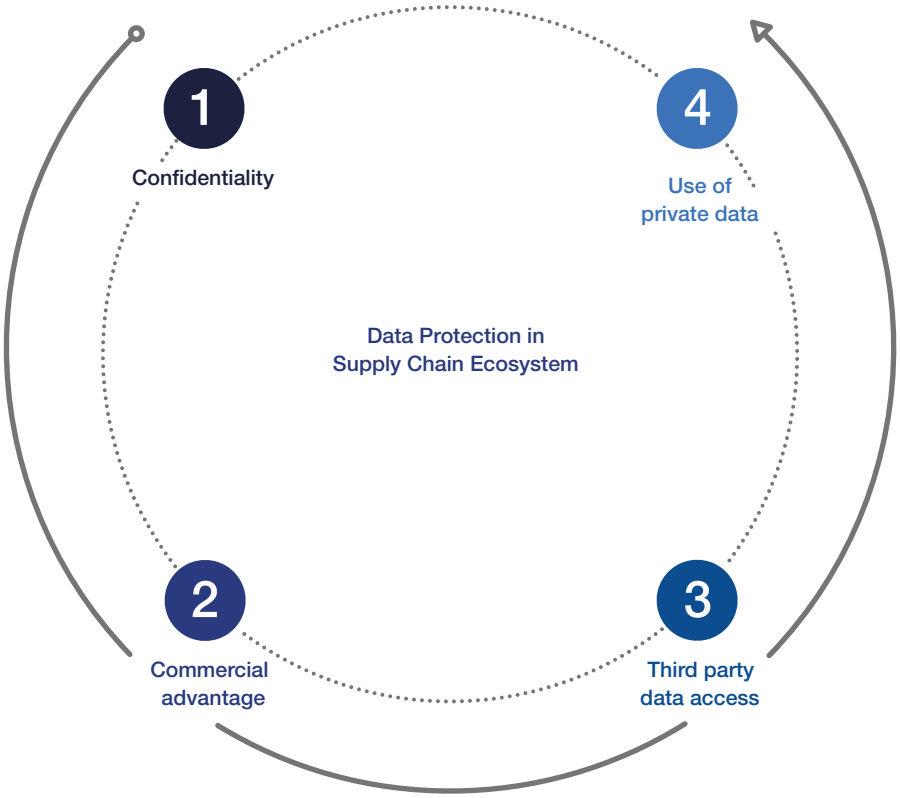


Figure 8.1 – Key points to investigate in protecting data

Confidentiality

At a fundamental level, transactions in a supply chain cannot be transparent to all participants in a blockchain network. Confidentiality requirements for some information must be maintained regardless of which permitted parties it is shared with.

To put it another way, supply-chain partners transacting with one another may be logging information onto the blockchain, but still need to keep the information from each other. Two reasons why that happens:

- They believe there is value to having the blockchain serve as a single source of truth for authenticated supply-chain data so that participants can extract the particular data they need.

- The practical challenges of understanding what should be obfuscated and what can be revealed during a one-to-one integration process are too immense.

Example: An electronics contract manufacturer (CM) provides vendor-managed inventory services to its buyer, a large electronics original equipment manufacturer (OEM). The CM would now like to obtain supply-chain finance on the blockchain, which will entail revealing to the OEM some of the CM's current financing costs without revealing other operating costs such as storage and insurance. The financier providing the capital will want to know all of this information and is willing to offer more competitive financing precisely because of this visibility. Thus the CM needs to be able to share information on a secure, need-to-know, and one-to-many basis with any counterparty – a good use case for blockchain. No traditional solution presents a practical way of meeting the CM's requirements.

Commercial advantage

Organisations want to use supply-chain data in forecasting and planning. At the same time, however, there may be a number of reasons why supply-chain partners are naturally resistant to providing the raw datapoints needed to conduct such analysis. For instance, they may feel they're not adequately compensated for the information, that it reveals strategically sensitive information about their own business, or that raw data they provide might be cross-referenced with other information to generate insights that could be used by competitors.

Example: When forecasting demand, buyers are incentivised to either inflate expected demand to ensure adequate supply or secure a volume discount. In anticipation of this, a supplier will therefore underproduce and "adjust" its reported inventory depending on whether it needs to create scarcity or meet outsized demand. This cat-and-mouse game creates inefficiency in the supply chain as a whole. A blockchain solution could allow suppliers and buyers to take a more collaborative approach, reporting data more truthfully without giving away control entirely or compromising competitive advantage.

Third party data access

To illustrate the challenges in this area, let's say an organisation needs to use a critical piece of pricing information in a blockchain transaction, but that information cannot be known to certain parties with access to the chain.

This is an instance where value can be unlocked by hiding certain information from parties even when those parties need to use that information in a transaction. This case is slightly different from the one in which parties acknowledge that information treated as confidential in the status quo must preserve the same level of confidentiality after a blockchain network is put in place.

In this example, the information was not confidential when only two parties were involved. However, by bringing it into a blockchain solution, that data must now stay hidden to certain participants on the blockchain, even where such information might be integral to the activities of the blockchain.

Example: A commodities producer would like to get its inventory off its balance sheet as soon as possible and recognise revenue. It can sell this inventory to a trading company or third-party financier on the blockchain, who can then sell to the end buyer at the appropriate time. However, the sensitivity of commodities prices is such that, while all parties would benefit from this financing structure, it would be commercially unacceptable to the producers for the financier in the middle to know the actual price.

Use of private data

Organisations only need to verify information authenticated on the blockchain, but they have to do so without seeing the data itself.

This situation is similar to the one described above. Whereas that case can be solved with blockchain-enabled computation, this particular problem requires matching and verification of large volumes of data without ever revealing the information itself. Once hashed or encrypted, data must remain in this state even when functions are performed on it. Zero-knowledge proofs (ZKP), although still in research and development phases, can be a useful tool in this endeavour for certain computationally intensive cases. (Zero-knowledge proofs are covered at greater length in the module Personal Data Handling and focus area Technology approaches to GDPR compliance).

For further details on this subject, see focus area Intellectual property considerations in the module Consortium Governance, focus area Legal and regulatory risks in the module Risk Factors, and the module Legal and Regulatory Compliance.

> *For audit purposes, it is important when planning a new blockchain solution not to put requirements solely on the technology being used. Instead, it's better to co-design technology and business processes together to ensure sound audit results. For example, handling confidential data on a public blockchain may be technically resolved by encryption, but that is not sufficient from an audit perspective. There must also be a design for the audit process itself for things such as security level of encryption and healthy key management.*
>
> **Takayuki Suzuki,** Financial Information Systems Sales Management Division, Hitachi

2. Technology solutions for data protection

What are some of the current technologies that establish data protection on a blockchain supply chain?

Design options available for data protection

There is no single blockchain solution or set of solutions to solve for data protection needs. The solutions adopted depend on the technological capabilities of a particular blockchain platform and the specific privacy and performance factors that a supply chain is trying to optimise. There may also be contractual relationships to consider between the blockchain's users and network participants.

In most cases, a blockchain solution is built to be a core component within a larger system in which it works in conjunction with other technologies. For example, tools like application logic to implement access controls may be employed to supplement the capabilities of the blockchain itself. These additional technologies are required components of the technology stack in a blockchain solution to achieve the data protection or integrity often incorrectly assumed to be a core feature of blockchain.

Once an organisation determines there is confidential information that must be protected in a blockchain solution, there are several security design options.

Keep in mind that these technologies are best-in-class as of the writing of this toolkit. However, blockchain is a fast-developing space that may offer new technology options within a span of months.

On-chain/off-chain configurations and hashing	Role-based access controls (RBAC)	Zero-knowledge proof (ZKP)	Homomorphic encryption
Basic protections, such as on-chain/off- chain configurations, and only storing hashed data on the blockchain	Enable selective obfuscation of data depending upon the identity of a particular participant	Allows users to prove their knowledge of a value without revealing the value itself	An approach in which data is encrypted before being shared on-chain. It can then be analysed without decryption

Figure 8.2 – Major design options for data confidentiality of a blockchain solution

Each of these approaches has trade-offs with respect to sophistication, complexity, cost, and technology readiness.

The more complex the technology becomes, the more potential drawbacks in usability, including:

- Limited transaction speed
- Necessity of a trusted blockchain operator
- Higher transaction costs (in terms of computing power)
- Risk of irrelevant data being included in the payload, or any supplemental data area

The methods outlined above must be understood in the context of a broader blockchain solution architecture in order to effectively put them into practice. These architectures can include additional databases or storage mechanisms that communicate with the blockchain. See Figure 8.3 for different blockchain configurations for data confidentiality. Data may still be kept entirely on-chain or stored in an off-chain database. In the latter case, data is stored as a hash on the blockchain, and the raw information is securely placed in an off-chain database.

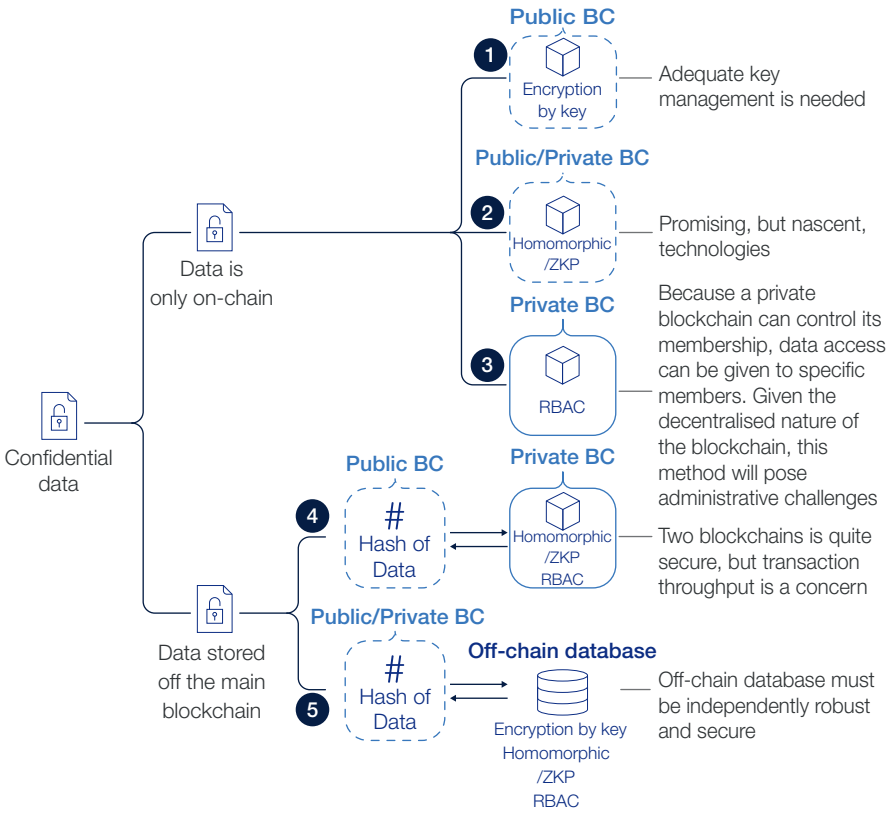


Figure 8.3 – Blockchain configurations for data confidentiality

- **Option 1:** Public or private blockchain with encryption. When confidential information is stored in raw form on the blockchain, it should be encrypted. Decryption keys are then shared through another secure channel.
- **Option 2:** Public blockchain with information cryptographically hidden, but mathematically usable by itself via methods like ZKP and homomorphic encryption.
- **Option 3:** Private blockchain with necessary permissions and role-based access controls are sufficient to provide required confidentiality. Data can be recorded as raw data.
- **Option 4:** Private blockchain is paired with a public blockchain to store the raw data or documents while the public blockchain only stores hashes. The private blockchain is configured to provide required confidentiality.
- **Option 5:** An ordinary database is paired with a public or private blockchain to store the raw data or documents while the public blockchain only stores hashes. The database and microservices that publish from the blockchain to the database are configured to provide required confidentiality.

Considerations for each design option

- **Option 1:** Functionally realises both confidentiality and data utility. Its drawback is that the basic key generation function of a blockchain is insufficient to implement meaningful access controls. Rather, a solution must also consider secure key storage, status monitoring of key confidentiality, key revocation, and key deletion. To determine which keys can decrypt information shared on the blockchain over multiple types of data payloads, a network needs sophisticated key management and coordination among data policies that are often dictated by contract at the data field level. Group key management can remove some of the

complexity of this task, but the overall process of key management simply requires investment and clear communication among participants prior to network membership, as well as constant monitoring and upkeep once participation is established.

- **Option 2:** Leverages promising technologies that are not yet easily scalable. Zero-knowledge proofs add several seconds of latency to each transaction it is applied to. Fully Homomorphic Encryption (FHE) is turning into the most powerful and useful encryption technology for blockchain and supply chain, but other technologies may be better equipped to provide value today.
- **Option 3 and 4:** Control the admittance of membership in a blockchain network more closely. These options therefore have greater ability to manage identities. If not coordinated through key management, then access to data will have to be run against a list of permissions before that access is granted. That list, in turns needs to be maintained across blockchain nodes and freely auditable by the owners of the nodes to ensure trust. The administrative effort involved may make these approaches cost-prohibitive.
- **Option 5:** Pairs a public or private blockchain with an off-chain database that is part of a member's node. The blockchain will only save the hash of the data. The system needs to be architected such that when the hashed data is queried, it can be pulled from the off-chain database and verified against a key management system that is part of the blockchain. Those who are meant to have access to the data will then be able to take actions upon it.

> *When implementing any data protection measures, it is important that the participants in a blockchain network be able to audit and control access rights to their data, regardless of the overall network governance structure. For those reasons, Role Based Access Controls and key management are far more trustable than FHE and Zero Knowledge Proofs, which still require faith in algorithms.*
>
> **Rebecca Liao,** Co-Founder and Executive Vice President, Skuchain

3. Case study: a manufacturing conglomerate

How should data protection technologies be applied in a real-world use case?

Challenges

To see how technologies may be adopted on a curve or combined to achieve optimal results, let's consider through a hypothetical use case in collaborative planning. This is one of the most fertile grounds for efficiency gains in supply chain and one of the hardest to achieve due to privacy reasons.

Let's say a major heavy manufacturing company has historically overstated its forecast to its plastics supplier to account for potential emergency orders. The supplier has become aware of this practice after years of building up excess inventory because the manufacturing company ultimately does not buy anywhere near the levels of its forecast.

One year, the supplier decides to significantly cut the procurement of resin from its supplier, a Tier 2 supplier to the manufacturing company. The supplier cut too much and could not meet demand for the manufacturing company that year.

In an effort to avoid supply outages, the manufacturing company would like to access data about the plastic supplier's, even the resin supplier's, inventory on hand and production rate on a more frequent basis. The plastic supplier would like to know the manufacturing company's inventory level, consumption rate

and demand forecast as often as possible. None of the parties have any incentive to share this information with one another given how it will affect pricing and negotiation leverage. The question therefore arises of what can be done.

If the manufacturing company simply knew the schedule of delivery, in real time, of resin to the plastic supplier and of the plastic supplier to them, there can be an incremental improvement in planning. Perhaps the resin supplier is not ready to share other information at this time, so the logistics information goes onto the blockchain, but other data stays off-chain.

Applying the toolkit

On the other hand, another solution may be one in which all parties are comfortable placing just-in-time (JIT) inventory data on the blockchain, but only their immediate counterparty has access to the information. In addition, the counterparty may have access for purposes of executing smart contracts or algorithms with the data, but the counterparty may not see the underlying data itself. Employing encryption together with a key management is one of the solutions. This native approach is scrutinised and achieves good maturity.

Otherwise, with role-based access controls (RBAC) on the blockchain, the parties are able to accomplish this. They can then engage in collaborative planning with data that is obfuscated but usable for valuable data analysis. With both of these technologies, sensitive data can stay hidden, but it is not exactly encrypted.

If the companies are unsatisfied with RBAC and key management but still want to use the cryptographic technique, then more sophisticated means will have to come into play. If the manufacturing company wants to control the level of resin inventory at the plastic supplier, then when the level falls below 5,000 litres, the manufacturing company will ask the plastic supplier to order more.

A zero-knowledge proof can certify to the manufacturing company that this threshold has indeed been crossed without revealing exactly how much resin remains at the plastic supplier. Otherwise, fully homomorphic encryption allows all parties to place their data on the blockchain, keep it encrypted, and simply run any planning algorithms on the encrypted data.

As is noted as a drawback, zero-knowledge proof or fully homomorphic encryption will incorporate complex software which requires further engineering for maturity. Also, these techniques may consume more computational power, and this can be a bottleneck if the system is expected to handle a large amount of data.

TOOLS AND RESOURCES

4. Data protection strategies

The following checklist is an overview of high-level considerations your organisation will need to address to approach data protection concerns. It collects together the key points presented in this module and the more detailed overviews in the focus areas can be referenced while going through this checklist.

Since data protection considerations will have a pervasive impact on the final implementation of the project, these questions should be considered early in the timeline of a blockchain deployment, in the later portions of the design phase, after the core value proposition and mechanics of the use case have

been determined but before the use case begins code development. Data protection considerations should be revisited ongoing in an organisation as external and internal requirements, rules and regulations change.

- ☐ Which supply-chain partners need access to certain information to execute their roles on the network?
  - Who has write permissions? Who has read permissions? How are these permissions established (who would determine who has access to the blockchain)? What level of access are users granted?
- ☐ How will the protocol, framework or platform protect data privacy and confidentiality?
- ☐ Which approaches for data protection are best fit?
- ☐ When the approach for confidentiality is taken, what are potential drawbacks, barriers, and risks?
  - Is encryption-based protection adequate for safeguarding data, or is there sensitivity around even sharing encrypted data with unauthorised parties?
  - How do you overcome such drawbacks, barriers, and risks?
- ☐ How is identity managed to meet data protection needs?
- ☐ What sets of policies are needed for governance and control of the blockchain network?
  - How would these policies interact with individual contractual arrangements among the network participants for distribution and use of data?
- ☐ How frequently do data standards change, and what level of flux does it cause for the data stored on-chain?
- ☐ How long does data need to be available for, and how does this affect any archival and obsolescence processes?
- ☐ What data access audit requirements need to be built into the system?
- ☐ Protocols are rarely deployed without middleware or an application layer sitting on top of them, each of which will likely have its own data privacy functionality. Where will the data privacy features sit?
- ☐ Is overall system security engineering designed to achieve data confidentiality? Many, if not most, of the purported features and capabilities of blockchain are design- and implementation-specific. Assumptions should not be made that because one design implementation includes a particular feature, that others will share that feature as well.

MODULE

Data Integrity

Overview

Focus Areas

1. The importance of data integrity and key requirements
2. The data pipeline – from creation to confirmation
3. Faults in the data pipeline
4. Solutions for data integrity in a blockchain context
5. Ensuring digital-twin integrity
6. Cyber-physical correspondence

Tools and Resources

7. Key questions to approach blockchain data integrity

Overview

Data integrity is the property that the data used in a solution is correct, reliable, and useful for all participants. The term “data integrity” is used here in the broader sense ubiquitous in the supply-chain world, referring not only to a resistance to unintended data modification, but also to the completeness, timeliness, and accuracy of the data over its entire lifetime.

This module covers typical considerations around ensuring that the data used in a blockchain solution is correct, reliable, timely for all participants, and preserved from the point of data creation to the point of usage on the blockchain. This module emphasises that blockchain technology does not necessarily ensure accuracy of data entered on-chain. It highlights that there are indeed multiple stages and steps where data integrity can be compromised.

FOCUS AREAS

1. The importance of data integrity and key requirements

What are the key requirements for achieving data integrity in a blockchain context?

Data integrity is not new to the supply-chain industry – capturing relevant data with integrity has been a priority for a long time. Using a blockchain, however, does not ensure data accuracy of the entered data on-chain, by design. Nevertheless, blockchain specifically protect against manipulation of data, which is immutable once it goes on the shared ledger. Once data is entered and confirmed through the consensus process, blockchain technology provides strong protection from further changes, since those changes would be easily noticed by other participants on the network. Thus, blockchain helps to establish a higher level of traceability and auditability to data so that any data that was entered inaccurately prior to consensus can be traced back to its origin.[95]

Like any supply-chain solution, blockchains, too, must be designed for data integrity; otherwise the solution will be fragile at best and completely non-functional at worst. This module discusses the challenges to data integrity that arise in a blockchain and supply-chain deployment, and offers nuanced answers and thought frameworks to guide decision-makers along this process.

Because the purpose of using a blockchain is to collect and manage data in a way that is useful to participants, it is a given that the data used must be accurate, reliable, and timely. Achieving data integrity within blockchain applications is broadly composed of three requirements: data origin integrity, oracle integrity, and digital-twin integrity (Figure 9.1 – Data integrity requirements).

Achieving data integrity within blockchain applications is broadly composed of three pillars: data origin integrity, oracle integrity, and digital-twin integrity.

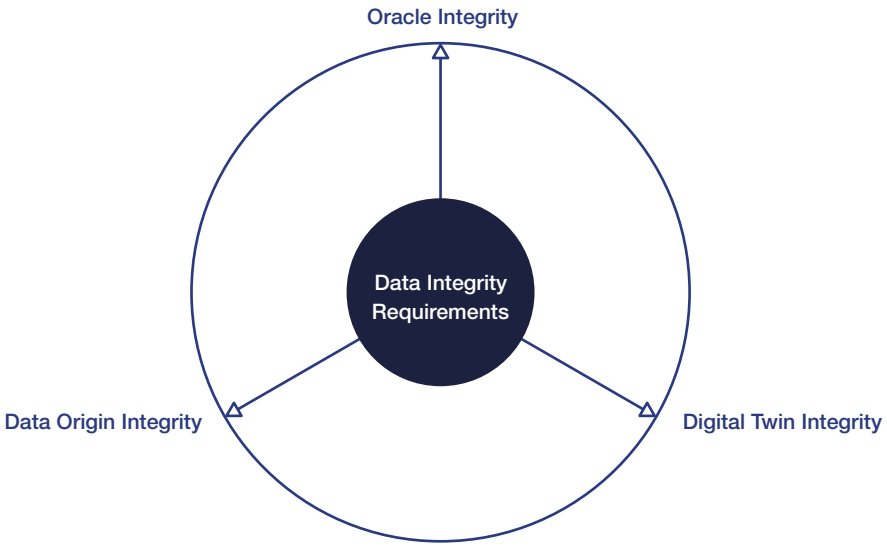


Figure 9.1 – Data integrity requirements

Data origin integrity: A common misconception is that the use of a blockchain alone can ensure data integrity. However, even though blockchains can reliably prevent the undetected modification of data once it is confirmed on-chain, blockchains will enforce this only on the data it is given. If the data is not accurate to begin with, then making it immutable by storing it on a blockchain does not provide any benefit - "garbage in, garbage out."

Thus, it is clear that in order to guarantee data integrity in a blockchain and supply chain solution, the accuracy and reliability of data must be preserved from the point of creation to the point of usage on the blockchain. This is referred to as data origin integrity. A lack of data origin integrity will prevent blockchain participants from drawing useful insights from the data on the blockchain, since the data itself is faulty.

Oracle integrity: A common step where problems can occur is at the point of submission to the blockchain. Since blockchains themselves cannot directly access information about the real world such as the status of a shipment, weather conditions, and commodity prices, blockchains must rely on third parties to submit this information, commonly referred to as oracles. The entity submitting the information (the oracle) is often the same entity as the one that provides the data (the data provider or data origin). In either case, these oracles are trusted. Depending on the environment the blockchain solution operates in, a degree of care must be taken to ensure that oracles have not modified or omitted data before submission to the blockchain. This is referred to as oracle integrity. A failure to achieve oracle integrity leaves a blockchain system susceptible to manipulation and exploitation by malicious actors.

These concepts sound similar to the "Oracle Problem". What's the difference?

This problem of ensuring the accuracy and correctness of data at the time it is submitted to the blockchain is widely referred to in the blockchain industry as the "Oracle Problem". This is simply a different naming convention. The terms "data origin integrity" and "oracle integrity" are used to reflect the fact that the security of the oracle is only one component of the overall solution, that achieving the broader goal of data integrity requires thinking back to where the data was created in the first place.

Digital-twin integrity: Lastly, it is common for blockchain and supply-chain solutions to represent real-world objects such as materials and products on the blockchain in a digital form such as a token. This digital representation is referred to as the real-world object's 'digital twin'. The idea is that useful real-world data about the object, such as its identity, current location, and other metrics, can be attached to this digital twin in order to yield useful insights about the condition of this objects in the real world, and updated as conditions change. The obvious concerns with this design are whether the data attached to the digital twin presents an accurate and timely view of the physical object and whether the link between the physical object and digital twin may have been compromised. These considerations altogether constitute the property of digital-twin integrity. A lack of digital-twin integrity will cause the digital twins to no longer be an accurate representation of reality, which can prevent the detection of lost, stolen, and counterfeit goods.

What about off-chain data?

It is common practice in blockchain deployments to only store the hash digest of data on-chain instead of the data itself when the dataset is particularly large, perhaps including documents, images, videos, long strings of text, or other elements. Storing all of this on the blockchain can lead to blockchain bloat.

To address this issue, the larger dataset may be stored somewhere off-chain, whether in a shared database, another blockchain, or a peer-to-peer network like InterPlanetary File System (IPFS). The on-chain hashes of the data can then help a blockchain refer to the off-chain data as needed.

> *Blockchain technology can't solve for the human factor. If someone inputs garbage data onto a blockchain, that garbage is recorded forever and can inadvertently become a flawed source of truth. Thus, an analysis of data hygiene is a critical precursor to any blockchain deployment.*
>
> **Sheila Warren,** Platform Head – Blockchain, Digital Currency, and Data Policy, World Economic Forum

In order to guarantee data integrity in a blockchain and supply chain solution, the accuracy and reliability of data must be preserved from the point of creation to the point of usage on the blockchain.

This arrangement guarantees that unwanted modifications to the data will not go undetected, but the same problems, considerations, and solutions relevant to data integrity still apply. The data must still be validated in some way, but since the smart contracts on the blockchain cannot do this directly, the validation needs to be completed by a different architectural component such as by the clients of participating users or even by a trusted execution.

Since a relatively straightforward change in configuration is sufficient to address this concern, data integrity for on-chain vs off-chain data will not be discussed further. The module Data Protection covers additional information on the off-chain approach to protect data.

The rest of this module discusses these requirements in more detail and presents solutions for each, with an emphasis on techniques and solutions specific to blockchain-based supply chain deployments.

2. The data pipeline, from creation to confirmation

How exactly does data move from the point of origin to a blockchain network? Where should one look for potential data integrity violations?

In every blockchain solution that relies on external data, data is originated, submitted to the blockchain by an oracle, and finally confirmed and made usable for blockchain applications. In order to clarify the thinking around this process and raise an awareness of common threats to data integrity, it is helpful to conceptualise data as flowing along a pipeline that includes various stages of processing (Figure 9.2 – Different stages in the lifecycle of data).

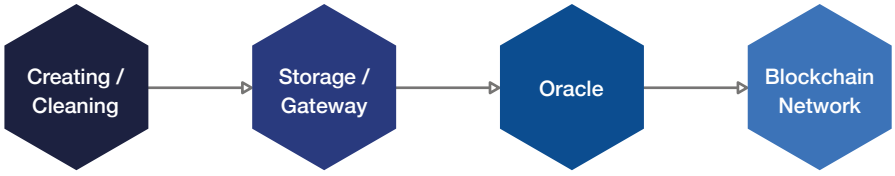


Figure 9.2 – Different stages in the lifecycle of data

Stages in the data pipeline:

- **Creation/Cleaning:** Measurements are made, and raw data is produced. It may come in the form of numbers, text, images, videos, or other structured and unstructured formats. It may be inputted manually by humans or collected automatically by computers and devices, or both. The data is cleaned, enhancing its usefulness, which may include quality assurance, standardisation, analysis, and conversion to usable formats. There is always a human or organisation involved in collecting the data, with varying motivations for doing so.
- **Storage/Gateway:** The data is stored somewhere. The data may or may not be stored by the same entity that produced it. If necessary, it is made accessible to relevant parties, through some gateway, whether it is a website, a database download, an application programming interface (API), or simply just physical access to paper records. Usually, a request for data through this gateway simply returns a set of existing data, but in some cases, other operations may be performed as well.

- **Oracle:** The oracle connects the data gateway to the blockchain. This may be the same or different entity as the creator of the data or the entity that stored it and made it accessible. The oracle takes data from the data gateway, encapsulates the data in a blockchain transaction, signs it, and broadcasts the transaction to the blockchain's node network, using a blockchain client. An oracle will often also listen for data requests from the blockchain network and relay these requests to the data gateway. For example, a shipping carrier system may serve an active role as an oracle in a blockchain solution, listening for requests for shipping updates and responding accordingly. However, it is far more likely that some specialised blockchain service provider will provide oracle services by interfacing with the API of the shipping carrier system and submitting results to the blockchain, as it doesn't require any action on the part of the shipping carrier system.
- **Blockchain node network:** The transaction undergoes the consensus process, gets stored in a block, and is eventually confirmed on the blockchain network. The data is stored in a variable in some smart contract on the blockchain and can be usefully consumed or referenced by other smart contracts and users.

For example, even if a trustworthy, well-secured, and uncompromised computer serves as an oracle, the integrity of the data it provides would still be violated if it were reliant on measurements made by a broken or tampered-with sensor at the point of data creation. Thus, in order to guarantee data integrity, the accuracy and reliability of the data must be maintained from the point of origin all the way to its point of usage on the blockchain.

> Since each stage in the data pipeline relies upon what was given by the previous stage, data integrity requires that every stage in the pipeline is secure, reliable, and resistant to malfunction or abuse.

Since security of every stage in the pipeline is a prerequisite, it is also important to deploy good practices of cybersecurity. Refer to the module Cybersecurity for further discussions and approaches to enhance cybersecurity throughout a solution.

3. Faults in the data pipeline

What could cause data submitted to the blockchain to be inaccurate? What could go wrong at each stage in the data pipeline?

The lists below aim to exemplify the kinds of data integrity risks decision-makers should consider when architecting their own use cases. Data integrity faults are highly use case-specific, so these lists should be used as inspiration to help identify potential challenges unique to the organisation's own use case, rather than as exhaustive categorisations of all possible faults.

Benign faults

Most problems in the data pipeline tend to be benign faults, meaning that they are unintentional and not motivated by malicious intent.

Table 9.1 – Examples of benign faults in the data pipeline

Data Pipeline Stage	Example
Creation / Cleaning	• A flawed measurement process results in biased data or fails to capture important information. • Hardware sensors are poorly calibrated or cannot connect to mobile networks in remote areas. • Lack of quality authentication fails to catch human input errors.
Storage / Gateway	• A data provider is not willing to share their data due to privacy concerns. • A database is not backed up and gets corrupted during a power surge. • An API is updated, causing data requests to fail. • A gateway has lost connection to a hardware sensor and fails to fulfil requests.
Oracle	• An oracle service is down for maintenance or goes out of business, and there is no mechanism for the blockchain smart contract to switch to a different oracle. • The data returned by the data source contains a new file format which the oracle does not know how to handle correctly.
Blockchain Node Network	• There are insufficient funds to pay transaction fees for a public blockchain network. • A blockchain client is unstable and prone to crashing. • Transaction throughput is insufficient to support the needs of participants.

Malicious faults

Malicious faults occur much less frequently but are important to consider if the blockchain deployment operates in a highly adversarial, low-trust environment, or if the stakes are high. For example, if one is using a blockchain for real-time data sharing among long-trusted business partners, then protections against malicious behaviour are likely of lower priority, since it is assumed that a highly trusted business partner would not intentionally submit misleading data.

Malicious faults occur much less frequently but are important to consider if the blockchain deployment operates in a highly adversarial, low-trust environment, or if the stakes are high.

On the other end of the spectrum, if a blockchain deployment programmatically determines which company will win a multi-million dollar procurement contract based on quantitative measures of vendor performance supplied by oracles, protecting oracle integrity is much more important. In this scenario, the procurement contract provides a substantial incentive for the vendors to collude with an oracle in order to submit false performance metrics at the expense of other stakeholders in the system.

While most violations of data origin integrity are benign, violations of oracle integrity tend to be malicious, since manipulating data to be false or fraudulent generally does not happen by accident.

Additionally, changing business conditions, shifts in incentives, and takeovers by new management are all commonplace occurrences in the long run that can cause trustful relationships to break down or turn competitive. If the circumstances allow it, former business partners may turn adversarial as well. That is why it is important for serious blockchain deployments designed to operate over a long period of time to take measures against malicious behaviour.

Changing business conditions, shifts in incentives, and takeovers by new management are all commonplace occurrences in the long run that can cause trustful relationships to break down or turn competitive.

Table 9.2 – Examples of malicious faults in the data pipeline

Data Pipeline Stage	Example
Creation / Cleaning	• There is physical tampering with sensor hardware or with the subject or environment being measured. For example, the intake of a pollution sensor may be covered by a malicious actor when inspectors are not present. • Critical resources such as power or internet are cut off for unwanted sensors. • Data collected corresponds to the wrong object. For instance, a location tracker is separated from the object it is supposed to track. • Internet of Things (IoT) sensors are taken over by hackers. • Measurement software is modified to report values different from those measured, to make systematic adjustments favourable to the fraudulent party, or to generate data that doesn't exist.
Storage / Gateway	• The values in a database are modified or deleted prior to transmission to the oracle, due to outside hackers or privilege abuse by insiders. • There is a denial-of-service attack in which the server hosting the data gateway is flooded with internet traffic and thus unable to answer requests. • There is a man-in-the-middle attack in which an attacker intercepts real data from the legitimate data source and replaces it with modified data before sending it to the oracle.
Oracle	• In another variety of man-in-the-middle attack, the oracle intercepts real data from the legitimate data source and replaces it with modified data before submitting it to the blockchain. • There is a one-off manipulation in which the oracle submits false data to impact single decisions or outcomes. • As part of a systematic manipulation, the oracle continually submits false data crafted to portray a desired narrative.
Blockchain Node Network	• Legitimate oracle input transactions are unable to finalise due to a large number of bogus "spam" transactions. • Participants in the blockchain consensus mechanism collude to do a "rollback" in which they censor transactions or rewrite the blockchain history to reflect a different outcome.

4. Solutions for data integrity in a blockchain context

What techniques and solutions are available to support data integrity in a blockchain deployment?

Preventing benign faults

Data integrity problems, especially non-adversarial ones, are not new to the supply-chain world. Thus, the solutions relevant to preventing benign data-integrity faults in a blockchain context don't differ much from the solutions applied to data-integrity concerns in a more traditional supply-chain context.

It is relatively straightforward to prevent benign faults, since doing so doesn't require anticipating the potential actions of intelligent and resourceful attackers. The same traditional principles and techniques apply – employing

proper system design, maintenance, management, and business practice will prevent the vast majority of benign faults. This module will place a greater emphasis on the techniques and solutions relevant for protecting against malicious faults, an area that blockchain technology excels at.

The same traditional principles and techniques around data integrity for other technologies apply to blockchain as well. Employing proper system design, maintenance, management, and business practice will prevent the vast majority of benign faults.

Protecting against malicious faults

All malicious faults stem from the abilities and privileges given to participants in the blockchain, whether they are data providers, oracles, organisations, or users. While under ordinary circumstances these powers are constructive and supportive of key functionalities in a blockchain deployment, they can also be abused when conditions worsen.

Protecting against malicious faults is thus a matter of limiting privileges to only those which are necessary, minimising the potential negative impact of privilege abuse, detecting malicious behaviour and holding responsible parties accountable if it occurs. It is also important to minimise the number of trusted actors the system depends upon.

In the specific context of ensuring data integrity, solutions aim to maintain a high confidence in the reliability of some data while minimising the trust placed in the parties supplying it. This usually comes in the form of protocols and additional processes that help validate data inputs in some way before being finalised.

Protecting against malicious faults is a matter of limiting privileges to only those which are necessary, minimising the potential negative impact of privilege abuse, detecting malicious behaviour and holding responsible parties accountable if it occurs, and minimising the number of trusted actors the system depends upon.

These approaches are all guided by the principle of trust-minimisation, which, as the name suggests, seeks to minimise the trust and reliance placed on any parties involved in transactions. Applying this principle helps to produce a system that remains robust, resilient, and functional in the face of malicious behaviour as well as additional classes of benign faults.

Trust minimisation is relevant even when some parties are necessarily relied upon by the blockchain system. For example, even if an oracle is the only entity to have access to some information needed by the blockchain, all of their data inputs should be transparently recorded somewhere so that any suspected misbehaviour can be examined at a later time if needed.

Solutions for protecting against malicious faults are more costly than solutions for preventing benign faults, due to the additional complexity and overhead involved. Naturally, it is up to the designer of the blockchain deployment to determine to what extent these protections are necessary and how to balance these requirements against associated trade-offs, such as cost, technical difficulty, and integration challenges. In general, it is best to employ as many of the following techniques as possible within reasonable constraints.

Traditional techniques for data integrity

These comparatively simple techniques for data integrity are well-known, effective, and already widely applied across the supply-chain industry in general, not just blockchain deployments.

- **Vetting trusted actors:** Strictly vet any humans or organisations that must be trusted to perform certain duties. The same filtering and qualification procedures that apply to choosing a new employee or new contracting company generally apply also to choosing which humans and organisations get to play privileged roles in blockchain systems. For example, individuals could be asked to provide “know your customer” (KYC) information when necessary, or to undergo a certification process. One could select individuals who are legally obligated to act according to certain rules, such as adapting public notaries to blockchain functions. For organisations, one could look at their performance track record, at their company values and management, and at their overall capabilities.

- **Contractual obligations:** Another strategy is to introduce punitive measures through traditional legal contracts, such as a fine defined for certain bad conduct on a network. Such a measure would inherit the known advantages and disadvantages of legal contracts, raising questions such as if the contract is practically enforceable, whether the value of what is at stake is great enough to warrant legal settlement, and so on. If arbitration is sufficiently streamlined and cost-effective, legal contracts could be an effective way to create a strong obligation to uphold data integrity.

Advanced techniques for data integrity

These comparatively advanced techniques are newer and more difficult to apply but are highly relevant to, and compatible with, the data integrity requirements of a blockchain deployment.

- **Reputation system:** Over time, the actions and inputs produced by privileged actors generate information that can help gauge the expected continuing trustworthiness and reliability of these actors. For example, an oracle that has never submitted a value differing substantially from those submitted by other oracles (for the same request) can be said to have a strong track record of good performance that may justify assigning their future inputs a slightly higher weight or paying them a higher rate for their services. The track records that form the basis of the reputation system can themselves be used to audit prior behaviour if any foul play is suspected. Performance track records and manual ratings of trusted actors can be incorporated into a reputation system that serves as the basis for increased privileges and rewards in the future.

  However, financial rewards or enhanced privileges awarded to highly-reputable actors should be introduced only with great caution, as they increase the incentive for potential adversaries to try to unfairly take advantage of the system. This can be done by reputation farming, colluding, destroying the reputation of competitors, abusing power for unfair financial gain, or exit scamming, for instance. Difficulty in aligning incentives properly is a large part of why reputation systems are so notoriously hard to make robust.

- **Automation:** Another approach is to try to minimise reliance on potentially malicious human actors through automation. Trucks used for shipments could automatically report their location at all times, so that drivers don't have any opportunity to lie about packages arriving on time. Payments for goods and shipments could be triggered by smart contracts upon the satisfying pre-specified conditions, instead of waiting on human and bureaucratic processes that may stall payments, intentionally or not. The legal filings required for international shipments could be digitised on a blockchain in order to circumvent those who benefit from the inefficiency and opaqueness of the current process.A major determinant of whether automation is useful to data integrity is whether the automatic process is robust enough to produce objective results even in the face of reasonable attempts to cheat the system. In addition to process efficiencies and cost reductions, increased levels of automation usually come with the added benefit that human input errors are more easily corrected or prevented, helping to prevent more types of benign faults. However, this technique is limited to the extent that many types of work still require humans to complete.

- **Fraud detection and accountability:** Ideally, false or fraudulent data inputs can be detected in some way. This is valuable even if data integrity violations can only be detected after the data has already been used, because offending parties can still be held accountable after the fact.

Depending on the severity of the faults, whether it was accidental or maliciously motivated, and other factors, offending parties can be reprimanded accordingly, such as by marking down their reputation, suspending or revoking their power to submit data inputs, or even by confiscating the whole or a part of some financial collateral they have deposited for the purpose of attesting to their current and future good behaviour. Other possibilities include the integration of machine learning models to detect anomalous data submissions and raise red flags or reject submissions automatically. There are many possible variations, but the underlying motivation is the same – to detect incorrect data inputs and hold trusted parties accountable to them.

Example

The decentralised prediction market platform Augur utilises tokens which represent reputation, have monetary value, and which must be owned in order to earn fees as an oracle. If an oracle reports an incorrect value (voting against the majority of what all the other oracles independently reported), a portion of their reputation tokens are confiscated.

- **Aggregation across redundant inputs:** In some cases, a single data request can be redundantly answered by multiple oracles, where the final result is taken as the aggregate of the inputs supplied by the oracles, usually with outlier results thrown out. The core idea is that by aggregating across redundant inputs, the maximum negative impact of any individual oracle is reduced, and in some cases, the accuracy of the final result is improved as well. Inputs can be aggregated by taking the median, mode, mean or a hybrid of these approaches, but other aggregates could be used, especially for more complicated types of data - it all depends on the use case (Figure: 9.3 – Aggregation across redundant inputs).

  The primary drawback to this technique is that a large portion of data relevant in a supply-chain context is only accessible to a single party, and thus cannot be reported redundantly. For example, the current location of a package is only known by the entity that is currently custodial of it, and an accurate list of its contents can only be supplied by the entity that originally shipped the package. However, for any data that is publicly available or that can be made available to multiple parties, this technique is effective in improving its reliability, accuracy, and robustness to manipulation.

  For example, regional weather conditions, commodity prices, foreign exchange rates, figures inside a U.S. Securities and Exchange Commission filing, and practically everything that can be downloaded from the internet are all suitable candidates for redundancy and aggregation. If the data can be drawn from the API of an organisation, then it is likely that multiple oracles could integrate with the API.

By aggregating across redundant inputs, it minimises the the potential risk/impact of any individual oracle.

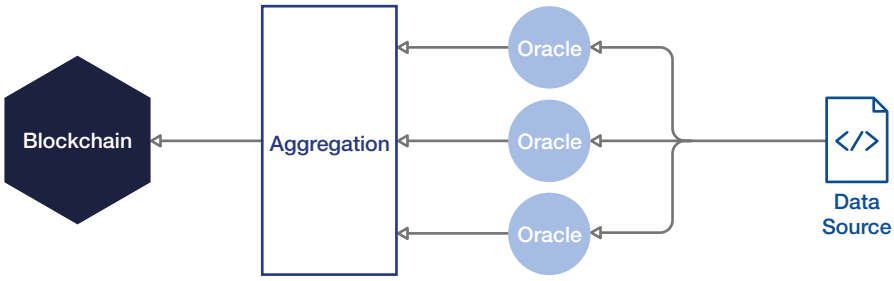


Figure: 9.3 – Aggregation across redundant inputs

The pros and cons of common aggregation methods:

Here are the most common aggregation methods along with associated benefits and drawbacks.

1. **Mean:** Best if each additional oracle input improves the accuracy of the final result, such as in sampling the credit score of a group in a poll. However, since a single oracle could greatly skew the end result by submitting outlier entries, a naive usage of the mean aggregate is not resilient to manipulation by even one of the oracles, which implies that using multiple oracles is even riskier than using a single one. A more intelligent approach could throw out the greatest and least entries as a rule, only averaging the entries that remain.
2. **Median:** Best when variance between values is expected to be moderate or high. Since only the 'middle' entry is taken, even extreme outliers will have negligible effects on the result. A median is resilient to a small proportion of false data arising from malfunctioning or adversarial manipulation.
3. **Mode:** Best when it is expected that every oracle will return the same value. This includes objective, discrete values or when the variance between results is expected to be low or zero. For example, a request for "the number of non-faulty phones manufactured in this batch" is expected to return the same whole number from all oracles queried. Mode also works well for nominal data, which is composed of categories or labels, and ordinal data, which is composed of ordered, non-numeric options, since the values are discrete.

   Note that if the data is numerical, the numbers must be sufficiently coarse-grained in order for the mode to consistently converge on the "right" value. For example, since the price of Bitcoin in USD ranges in the tens of thousands and fluctuates quickly, applying the mode aggregate to converge on a Bitcoin price may require that prices are rounded to the nearest multiple of 10 or even 25 or 100.
4. **Hybrid approaches:** For instance, an approach that entails taking an average of the middle two quartiles would inherit traits from all of the median, mode, and mean approaches, including tolerance to accidentally or intentionally false data. This approach also has the potential to increase accuracy as more data entries are submitted without having to round numbers down as is sometimes necessary with mode. However, gaining all of these advantages may increase the number of oracles required to the point of being cost-prohibitive. The best scheme will vary case-by-case.

- **Cross-validation:** Another approach is to "cross-validate" inputs, meaning that each input submitted is corroborated with nearby inputs. For example, if all of the temperature sensors deployed in a grid-like fashion across a large food storage facility report that the current temperature is around 5℃, with the exception of a single sensor reporting that the temperature is 30℃, it is plausible that the single sensor is malfunctioning, and its input can be automatically thrown out.

  Another example could be applied to the Global Positioning System (GPS) locations of vehicles on the road owned by a large shipping company. A vehicle would not only report its own location, but also the locations of company vehicles nearby, making it more difficult to tamper with a single vehicle's GPS system without detection. Successfully faking a location would require compromising the GPS systems of all the company vehicles nearby, as opposed to just a single vehicle.

> *In many blockchain projects, oracles don't have much input in the development process. Therefore it may be difficult to implement additional security mechanisms for additional integrity of oracles later. In such cases, one possible solution might be to introduce a human-oriented approach to data integrity, such as use of a trusted third party to verify the correctness of oracle data.*
>
> **Nishio Yamada,** Research and Development Group, Hitachi

Input aggregation and cross-validation yield significant data-integrity improvements to the use of oracles. However, since every additional sensor or oracle used incurs fixed and ongoing costs, the key consideration is whether the level of security possible with the chosen quantity and quality of these components is sufficient for the needs of one's use case.

- **More data, more evidence:** In general, more data allows for higher confidence in the events and conditions implied by the data. For example, the simple policy that a courier should record a short video while placing a valuable package in a deposit-only receptacle gives a much stronger assurance that the package was actually delivered. While it is still possible for the courier to record a video of the delivery and then fish out the package afterwards, getting away with it becomes more difficult as more data is required, since the data must not only be self-consistent but must also be comparable to data produced by similar events. Recording this evidence in an immutable tamper-evident data store such as a blockchain allows events to be audited in the future should a dispute arise, although it's likely that only a hash of the data would be stored on-chain.

  Determining what additional data and evidence is helpful to data integrity is highly specific to each use case, and requires creative thinking by blockchain architects and supply-chain decision-makers. However, the main idea is constant – while evidence can be faked and preventing fraud entirely is difficult, increasing the amount of data and evidence collected makes it more expensive and time-consuming for an attacker to submit false data, especially when used in tandem with other data-integrity solutions.

- **'Provably Honest' Protocols:** Another option is to integrate cryptographic protocols and special hardware that allow oracles supplying data inputs to include a corresponding "proof" that the data they are submitting is exactly the data they received from the data source. When the data and proof are received by the blockchain, they are checked against each other, and the data is thrown out if the proof is invalid. The protocols are designed such that it is impossible to generate a proof for some data if it has been modified after receipt from the data source. Hence, oracles that have provided data in this way are "provably honest" and do not have to be trusted except in the sense that they will continue to provide oracle services. However, even if an oracle becomes non-cooperative or discontinues its service, that oracle is fully replaceable. From the perspective of the blockchain, it doesn't matter which oracle submits the data as long as the associated proof is valid.

- **Hypertext Transfer Protocol Secure (HTTPS):** For requests made over the internet, one of the best options is TLSNotary, which modifies the internet HTTPS protocol to allow any computer to produce a proof that a particular web page appeared in its browser. For example, an oracle that connects to the UPS API could use TLSNotary to prove that the tracking info and timestamps it received from UPS were not modified before submission to the blockchain, and a smart contract on the blockchain could verify this proof that the data came from ups.com. Unlike the prior techniques that use redundancy to reduce the amount of trust placed in oracles, TLSNotary incurs very low costs, since the only requirements on the oracle are to integrate TLSNotary and maintain a server. TLSNotary can be used for any data source that uses the secure HTTPS protocol, which includes the vast majority of websites today.

- **Trusted Execution Environment (TEE):** For requests that primarily require some computation to be completed off-chain, one of the leading technologies that can produce a similar proof of correctness are TEEs

such as Intel Software Guard Extensions. Essentially, Intel chips that support this protocol include a special component completely isolated from other components in the computer called the Trusted Execution Environment. Other components in the computer can't read the memory inside the TEE, nor can they see the inputs or outputs of the TEE's computations, since all of that data in encrypted while in transit. This TEE can then be used to run highly sensitive code that computes over highly sensitive data, with a strong guarantee that the code ran correctly and without leakage of confidential information to any third party or even the computer that this TEE resides on. TEEs excel at providing strong data integrity guarantees in highly adversarial environments.

For instance, even if a computer, all of the software on it, and the internet connection the computer uses are all under the control of a hacker, any computations sent to the TEE would still be executed correctly due to the hardware and cryptographic security properties of the TEE. Any blockchain project that requires an oracle input that can be obtained as the output of some code could theoretically integrate a TEE, enabling a wide range of use cases and possibilities. However, it is worth noting that TEEs today are still a developing technology with a substantive number of unresolved issues.

> *The design choice over smart contract and TEE forms a trade-off between security and accountability, and this choice must be done with consideration of use case specifics. While TEE will bring greater security benefit, it will also pose limitation on process's transparency. In such case, alternative code verification process that is trusted by stakeholders will complement.*
>
> **Takayuki Suzuki,** Financial Information Systems Sales Management Division, Hitachi

5. Ensuring digital-twin integrity

How do I ensure that digital twins are synchronised with the physical objects they represent? What are the major components of digital-twin integrity?

Digital-twin integrity is a more specific type of data integrity that arises whenever physical objects are represented on a blockchain in a digital format. This usually applies to products, parts, and materials, but can apply to virtually any physical component in the supply chain that is useful to track in real-time.

For example, a luxury handbag tracked on a blockchain may be represented by a blockchain token, with the latest information about its location, current custodian, and stage of manufacturing attached. The digital representation is the 'digital twin' of the real, physical object, and the physical object itself may be considered the 'physical twin'. In order for the digital twin to provide useful insights about the physical object as it is being shipped, it must satisfy three primary conditions:

1. **Accuracy:** The data associated with the digital twin is correct and reliable.
2. **Timeliness:** The data is recent enough to be useful.
3. **(Cyber-physical) Correspondence:** The digital twin represents the physical object it is intended to represent, and the associated data describes the physical object it is intended to describe; the identities of the cyber (digital) and physical twins correspond.

For example, a luxury handbag tracked on a blockchain may be represented by a blockchain token, with the latest information about its location, current custodian, and stage of manufacturing attached.

These three components are the core essence of digital-twin integrity. Digital-twin integrity is important to consider whenever a violation of the accuracy, timeliness, or correspondence of data associated with the digital twin can unacceptably distort one's view of the supply chain. This in turn may result in

item mix-ups, missing items, counterfeit items, or simply just not insightful data. The accuracy and timeliness of the data associated with the digital twin can be ensured using the same techniques applied to data origin integrity and oracle integrity – robust system design, competent management, and minimisation of trust. It is in ensuring the correspondence between physical and digital twins that requires thinking in a different way.

Digital-twin integrity is important to consider whenever a violation of the accuracy, timeliness, or correspondence of data associated with the digital twin can unacceptably distort one's view of the supply chain.

6. Cyber-physical correspondence

What are the different realms of correspondence between physical and digital twins? What are the solutions for common cyber-physical correspondence issues?

Ensuring the correspondence between physical and digital twins usually only requires that there is a valid identification method for the physical object being tracked. This is usually done by attaching an identifier (ID) directly to the object or recording identifying information about the object.

The concept of cyber-physical correspondence may also extend to any systematic process that can uniquely identify and consistently differentiate objects from one another.

In a system with sound data integrity, an object will be assigned a unique ID such as a serial number, and the digital twin on the blockchain records this unique ID, allowing all data collected about the physical object to be associated with this ID. Such a setup enables a blockchain observer to look up information about a physical object by searching for its ID on the blockchain and is sufficient to ensure cyber-physical correspondence in most cases. However, if the physical objects being tracked have a non-trivial risk of loss, theft, or counterfeit, more stringent requirements must be imposed on the method of identification. This idea is best illustrated with an example.

Example of cyber-physical correspondence

In order to provide faster shipping for its customers, a luxury handbag company stores some of its inventory at third party fulfilment centres around the world, where its handbags are personalised with custom engravings, placed in their final packaging, and shipped directly to the customer. However, the company has discovered that counterfeit products are frequently swapped in for real ones at these fulfilment centres, where the company no longer has direct oversight over the bags.

The company attempts to solve this problem by tracking the handbags on a blockchain. When a bag is manufactured, it is assigned a serial number that uniquely identifies the bag. This serial number is etched onto a tag attached to the inside of the bag and recorded into a newly created blockchain token that represents the bag. Whenever the bag is transported to a different location and changes hands, its associated token is passed along, recording the location of the bag, the identity of the newly responsible party, and other details.

Altogether, this establishes a full history of the bag from completion of manufacturing to arrival at the fulfilment centre to final delivery to the end customer. The company believes that keeping this data on the blockchain will prevent counterfeiting, citing the transparent, immutable nature of the blockchain maintaining a verifiable, tamper-proof record of information that will supposedly prevent the introduction of counterfeit products.

However, their blockchain solution may not have resolved the counterfeiting problem if either of the two following conditions was not met:

1. First, the means of identification on the bag must be hard to forge. If the identification does not have sufficient anti-forgery protections, then a fraudster could create a fake identification tag that appears legitimate, attach it to a counterfeit bag, and swap the counterfeit bag with the real one at the fulfilment centre or any other point in the supply chain. The forged product would continue unnoticed by the following parties in the supply chain.
2. Second, the identification must be tamper-evident or tamper-resistant, such that modifying or substituting an identifier will be difficult or at least leave traces of tampering. This is necessary because even if the company used a hard-to-forge identifier, a fraudster could still detach a real identifier from a real bag, reattach it onto a fake bag, and pass the fake bag along with the real identifier to the rest of the supply chain - all without leaving a trace.

In either case, the addition of a blockchain for recordkeeping does not alone prevent counterfeiting. A lack of anti-forgery or tamper-evidence / tamper-resistance protections allows a fraudster to profit by obtaining real bags at the cost of fake bags. On the other hand, if the company has adopted a means of identification that is both hard-to-forge and tamper-evident / tamper-resistant, any party in the remainder of the supply chain can notice attempted counterfeiting and report the fraud.

For more information on the digital identity of “things” and identifiers, refer to the module Digital Identity.

Solutions for cyber-physical correspondence

In use cases where the cyber-physical correspondence of an object is substantively threatened by a risk of loss, theft, or counterfeit, two requirements on the identification method for the physical object must be met:

1. **Hard to forge:** It is difficult to falsify an identification that passes as legitimate.
2. **Tamper-resistant or tamper-evident:** The method of identification is sturdy enough to prevent tampering or tampering leaves behind detectable evidence.

Both of these requirements are related to physical security. Considerations of physical security, theft, and counterfeiting are not new to the supply-chain industry, so they are not necessary to discuss in full detail here. Just like the approaches to data origin integrity and oracle integrity, solutions for digital-twin integrity and cyber-physical correspondence are very use case-specific and must be balanced against costs, integration difficulty, and other trade-offs.

The rest of this section provides more information about hard-to-forge and tamper-resistant / tamper-evident identification methods.

Something that is **tamper-proof** is supposedly impossible to tamper with. However, nothing is tamper-proof in the same way that nothing is absolutely secure – it depends on the extent to which risks have been mitigated and the resources of a potential adversary.

It is thus more accurate to use the term **tamper-resistant** to describe an item considered to be difficult to tamper with, allowing its security against meddling to be evaluated along a spectrum. Examples of tamper-resistant items include steel safes and vaults, padlocks and bolts, or other sturdily constructed objects, locks, and containers. Note that all of these protections could be broken by an attacker with sufficient time, motivation, and resources.

On the other hand, a **tamper-evident** item might not be hard to tamper with but will leave evidence of any meddling that will be apparent to a recipient of the item. Numerous examples are in common use today, such as the lids on pharmaceuticals or jarred foods that pop up when opened, hologram stickers, labels, and seals that leave traces that are difficult to prevent when peeled or broken. Something that is **hard-to-forge** is hard to reproduce fraudulently without also leaving apparent evidence of forgery. Intuitively, anti-forgery techniques are thus similar to techniques designed to provide tamper-evidence. Examples include the many protections we apply to our paper bills, coins, stamps, and coupons, such as holograms, embedded strips, differing bill sizes, colour shifting and UV-reflective inks, watermarks, and grooves on coins.

For some examples of identification methods, and their relative effectiveness in satisfying the physical security constraints required for cyber-physical correspondence, see (Table 9.3 – Examples of identification methods and their associated effectiveness levels).

Table 9.3 – Examples of identification methods and their associated effectiveness levels

Data Pipeline Stage	Not tamper-resistant or evident	Somewhat tamper-resistant or evident	Very tamper-resistant or evident
Not hard-to-forge	Bar codes QR codes	Taping a lid closed + ID RFID chips Sewn serial numbers	Etched serial numbers
Somewhat hard-to-forge		Pictures or video of the item Info such as dimensions, shape, weight	Tamper-evident seals + ID Specialised high-security RFID Chips
Very hard-to-forge			Hologram stickers + ID Embedded strips + ID UV-reflective inks + ID Chronicled strips, inlays, seals

7. Key questions to approach blockchain data integrity

The following checklist is a series of guiding questions you can use with your organisation or consortium to approach data integrity concerns. It collects most of the key considerations presented in this module, but the more detailed discussions above should be referenced while going through this checklist. After reading this module, working through this checklist is an ideal starting point for supply chain decision-makers, product managers, solution architects, lead engineers, security experts, corresponding representatives from partner organisations, supply-chain domain experts, and practically anybody who plays a major role in the design and implementation of the blockchain and supply-chain deployment.

Since data-integrity considerations will have a pervasive impact on the final implementation of the project, these questions should be considered early in the timeline of a blockchain deployment, in the later portions of the design phase, after the core value proposition and mechanics of the use case have been determined but before the use case begins code development.

Data origin integrity and oracle integrity

- ☐ Has every stage in the data pipeline been examined to determine the faults that may occur?
- ☐ Have proper design, maintenance, and management of this deployment been ensured?
- ☐ Are there measures in place to identify faults unique to the intended use case?
- ☐ Are there malicious faults worth considering in addition to any benign ones?
- ☐ Approximately how much protection against malicious behaviour is required for the intended use case?
- ☐ Have there been measures to protect the integrity of data for every unacceptable fault that has been identified?
- ☐ Has the organisation considered all the techniques and solutions available to address data integrity faults?
- ☐ Is the quantity and quality of protections achievable under any resource constraints for the solution? Have protections been maximised?
- ☐ Does the proposed solution minimise the trust and reliance placed on any and all participating entities?

Digital-twin integrity

- How has the accuracy of data associated with the digital twins in the system been ensured?
- How will data in the system always be kept up-to-date?
- To what degree does the use case require assurances of cyber-physical correspondence? If there is a significant requirement, does the solution's design include an identification method that can uniquely identify the objects I'm tracking? Does the identification method consistently differentiate the objects in question from one another?
- Is loss, theft, and counterfeiting non-trivial risks to the intended use case? If so, has the proposed solution integrated adequate physical security measures to protect against these risks? Is its method of identification hard-to-forge and tamper-evident or tamper-resistant?
- Are objects sufficiently secured against anti-theft and anti-counterfeit according to the organisation's needs and cost preference?

Techniques and solutions

- Have strict vetting procedures been applied to all humans or organisations relied upon in the blockchain system? Has the organisation checked participants' credentials, or have they been certified by a reputable entity? Can the solution rely more heavily on actors who have a legal obligation to act honestly?
- Has the organisation considered applying legal measures to keep privileged parties contractually obligated to perform their duties as expected? Are these legal measures practically enforceable given the amount of value at stake and time required for arbitration in case of a dispute?
- Are the actions taken by privileged entities in the system immutably recorded somewhere in order to establish track records of performance? Could these track records serve as the basis for a reputation system? How exactly will bad behaviour be punished? Is it possible to reward good behaviour without creating an incentive misalignment?
- What parts of the data pipeline can be automated to reduce the number of human errors? Where can systematic validations of data inputs be applied? Can any of the mechanics in the use case be handled programmatically? Is an automated process robust enough to produce objective results even in the presence of adversaries?
- Can false or fraudulent data inputs be detected in some way? How can offending parties be held accountable for their actions? Are there opportunities to apply machine learning models to detect data anomalies programmatically?
- Can any of the requests for data in the proposed system be answered redundantly by multiple oracles or sensors? If so, how might redundancy help mitigate systemic risks? Which of the aggregation functions is most suitable for the types of data in the intended use case? How does the organisation determine and throw out outliers? How do outlier data feed into the system of reputation or accountability? Are there any opportunities to introduce cross-validation of data inputs instead of pure redundancy? Does this redundancy meet the system's security needs for a reasonable cost?

- How can more data be collected to increase confidence in the conditions reported by the data? What data would be useful for this aim? Where can the solution store this data so that it can help resolve potential disputes in the future?
- Does the system rely on data accessible over the internet or an API via HTTPS? If so, how can the system uses TLSNotary to avoid having to place any trust in oracles? Is a replacement mechanism for the oracles included in the system?
- Does the system require any computations to be completed off-chain, or do the computational inputs and outputs need to remain confidential? If so, is it possible to conduct these computations with a trusted execution environment? Could the system use a TEE to provide strong data integrity guarantees without having to incur the large overhead costs of redundant sensors and oracles?
- How do all the system's data integrity techniques and solutions work together? Is the combination of solutions coherent? Do they altogether form a comprehensive plan to ensure data integrity in the blockchain and supply-chain deployment?

MODULE

Personal Data Handling

Overview

Focus Areas

1. Applicability of the GDPR
2. Meeting GDPR obligations
3. Technical approaches to GDPR compliance
4. Principles for building GDPR-compliant solutions

Tools and Resources

5. Rapid initial analysis for GDPR compliance

Overview

When it went into effect in 2018, the European Union's General Data Protection Regulation (GDPR) offered ground-breaking protections for personal data. But it also raised questions for blockchain networks as to their new compliance obligations both within and beyond the EU.

The GDPR places obligations on what/whom it terms data controllers and processors. However, when there is no centralised service provider as on a blockchain network, who is responsible for overseeing the treatment of personal data, or paying penalties when obligations are breached? And if a chain is recording data immutably, what does that mean for erasure obligations if that data cannot be taken down? While such considerations need not be prohibitive to beginning a new blockchain project, they should be addressed early on – even, in some circumstances, by supply-chain organisations not based in the EU.

Recommended reading - Inclusive Deployment of Blockchain for Supply Chains: Part 4 – Protecting Your Data.[96]

FOCUS AREAS

1. Applicability of the GDPR

Is there a general understanding that personal data regulation will apply to your blockchain solution? What factors do organisations need to consider when determining the applicability of data protection and privacy obligations?

Personal data protection compliance requirements can dissuade the deployment of blockchain in supply chains if not properly understood, in part because the cost of non-compliance is so high. In addition, such regulations are seldom made with blockchain in mind and thus do not consider the particular nuances associated with blockchain.

While it is not possible to present a comprehensive treatment of all personal data protection regulations that might apply to an international blockchain solution, this module focuses on the European Union's General Data Protection Regulation (GDPR) as a proxy for all data protection and privacy obligations due to its broad scope and detail. The GDPR is also at the forefront of a new wave of data protection legislation globally which places strict obligations on organisations handling personal data or personally identifiable information, such as the recent California Consumer Privacy Act (CCPA).

Many non-EU entities mistakenly believe that the GDPR is not applicable to their solutions. It is important for non-EU-based supply-chain partners to consider that they may still find themselves being subject to GDPR requirements in specific circumstances.

In light of the substantial fines levied for non-compliance and the GDPR's requirement to consider data protection implications from the ground up – a concept known as "privacy by design" – review of this module and professional legal advice is strongly recommended. In addition, professional legal advice is recommended to determine if any other country-specific data protection legislation should be taken into consideration, including legislation surrounding international data transfers.

Using the GDPR as a proxy for data protection and privacy regulations, we can assume that the GDPR may apply to a blockchain solution or transaction. There is nothing about a blockchain context that exempts such things from data protection regulation.

Whether the GDPR applies will rest on the answers to two main questions:

- **Personal Data under the GDPR: Does the data in the supply chain meet the definition of "personal data" under the GDPR?**

  Personal data may include the name, identification number, location data, online identifier, or other information relating to a person. There are therefore various data points within a supply chain that could reasonably be considered to meet the definition of personal data. The GDPR's definition of personal data can also include pseudonymised data if such data can be indirectly associated with a person whether by cross-referencing with other datasets or by other means.

  For the purposes of the GDPR, transactional data stored in the blocks and public keys may be deemed to meet the definition of personal data, although again this list is non-exhaustive. Note that special categories of personal data such as data that would reveal a data subject's racial origin, religious beliefs, or sexual orientation, are defined as special category data and thus are subject to even greater protections under the GDPR.

- **Territorial Scope of the GDPR: Does the processing of such data by the blockchain solution in question fall within the territorial scope of the GDPR?**

  The question of territorial scope requires a consideration of (1) whether the controllers or processors are established within the EU (the "establishment test"); or (2) if the controller or processor is established outside the EU, whether it: (a) offers goods and services to data subjects (people) within the EU (the "targeting test"); or (b) monitors the behaviour of data subjects in the EU, where that behaviour occurs in the EU (the "monitoring test").

  The GDPR applies only when both the personal data definition and territorial scope conditions are met. If the GDPR applies, then all collection, storage and processing of personal data must be done in accordance with the GDPR's requirements, and this includes that data on the blockchain.

The GDPR applies only when both the personal data definition and territorial scope conditions are met. If the GDPR applies, then all collection, storage and processing of personal data must be done in accordance with the GDPR's requirements, and this includes that data on the blockchain.

See the World Economic Forum's white paper Inclusive Deployment of Blockchain for Supply Chains: Part 4 – Protecting Your Data[97] for a detailed description of these two issues. The correct application of these tests depends on the specific facts of the case, and professional legal advice is recommended beyond the initial assessment exercise. In addition, professional legal advice is recommended to determine if any other country-specific data protection and privacy legislation, as well as the rules governing international data transfers, should be taken into consideration.

In this toolkit, the module Digital Identity offers insights on various considerations for Personally Identifiable Information (PII) and a deeper understanding of digital identity.

2. Meeting GDPR obligations

Can a blockchain solution be GDPR-compliant given its characteristics of immutability and distributed nature?

The European Union Blockchain Observatory and Forum stated in its thematic report on Blockchain and the GDPR: "There is no such thing as a GDPR-compliant blockchain technology. There are only GDPR-compliant use cases and applications."

When the GDPR applies, obligations regarding the handling of personal data will apply to processing operations.

Achieving GDPR compliance may require a detailed legal and technical analysis. The following are important steps to take in order to approach compliance under the GDPR for a blockchain solution:

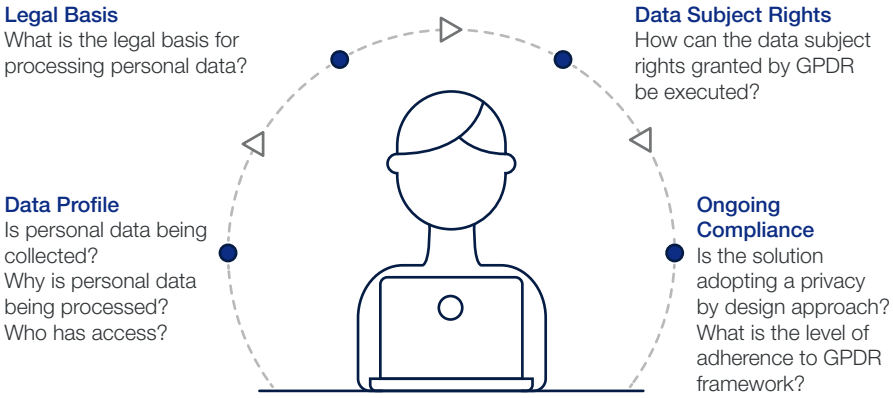


Figure 10.1 – Important steps to take in order to build a GDPR-compliant solution

- **Understand the organisation's data profile.** Engage in a detailed fact-finding exercise in relation to the organisation's data profile. This includes understanding the roles and responsibilities regarding data processing activities in order determine whether you are a data controller, joint controller, or processor. It also includes understanding what personal data is collected, who it relates to, how it is processed and for what reasons, where it is processed, to whom it is provided, who has access to it, and how long it is retained. Further guidance on these and other considerations is available from EU Member States' national data protection authorities' websites.

Example

The UK Information Commissioner's Office and the Irish Data Protection Commission provide some helpful English-language resources, which are designed to be accessible to non-specialists such as citizens and small business owners.

- **Consider the legal basis for processing.** Determining the legal basis for processing personal data on the blockchain. It is a core principle of the GDPR that lawful data processing can only take place on one of six lawful grounds – for instance, as part of a contract, legal obligation, or legitimate interest, amongst others. This is not a straightforward consideration for blockchain due to the nature of blockchain, such as the fact that, in many cases, there will not be a straightforward relationship between a given blockchain actor and the party whose data is being processed. The obligations around data controllers and data processors should be taken into account here also.
- **Consider how to uphold data subject rights.** Consider how data subject rights granted by the GDPR - including data access, correction, and erasure - can be satisfied when a data subject makes such a request. Depending on the blockchain solution used – for example, a public permissionless or private permissioned blockchain. or any other blockchain type. Whilst accessing personal data on a blockchain should be technically feasible, it may prove challenging to rectify or delete personal data on a blockchain as blockchains are generally designed to offer immutability. It is important to note that these rights can be exercised at any time by a data subject, and it is therefore important to put in place systems that allow the controller of the personal data to comply with the request within one month of the request. In this regard, consideration of accessibility at the point of engineering the data stack can make such requests easier to comply with later on if and when they occur. This is otherwise known as a "privacy by design" approach to engineering the data stack.
- **Consider the ongoing compliance process.** GDPR compliance is an ongoing process rather than a one-off exercise. Ongoing activities may include:

- Applying a “privacy by design” approach whereby data protection is made an essential part of the core functionality of the blockchain solution, and data protection requirements are considered throughout the design and implementation process
- Creating a GDPR framework and internal compliance program that includes essential policies covering data security, data breaches, and notification obligations, privacy by design, third-party vendor management, and data subject rights
- Implementing GDPR-compliant transparency notices including a website privacy policy, employee privacy policy, etc.
- Ongoing employee training to ensure that the GDPR framework and compliance program are appropriately operationalised and implemented
- Ongoing maintenance of the organisation’s security obligations
- Ongoing maintenance of processes for and adherence to data-subject rights obligations
- Ongoing review of guidance issued by the European Data Protection Board (EDPB), an independent European body, which works to ensure the consistent application of the GDPR among European Union member states, and EU member state regulators such as the UK Information Commissioner’s Office or the Irish Data Protection Commission. This function will realistically be outsourced to a legal advisor
- Good data hygiene and mapping, including at the data stack engineering level, to ensure data-subject rights obligations can be met with ease
- Incentivising a privacy-first company culture
- Staying abreast of changes in data protection laws that will affect legal obligations
- Familiarisation with and legal advice regarding the GDPR’s obligations around data transfers outside the EU

There is no single blockchain solution or set of solutions to solve the issues described above.

The most straightforward GDPR-compliant solution will always be to exclude the storage and processing of personal data on the blockchain at the outset, but where this is not possible or practical, careful consideration will need to be given to the requirements summarised above, the technical practicalities of the blockchain solution, and the specific performance factors that the blockchain solution aims to optimise. If off-chain data storage is chosen as an appropriate method of reducing risk on the blockchain itself so as to take the blockchain out of scope of the GDPR, then the GDPR obligations will still apply to the data stored off-chain if the two conditions of definition of personal data and territorial scope are met.

The following describes technology approaches which may be used as a starting point to achieve GDPR compliance.

3. Technical approaches to GDPR compliance

What features can be built into a blockchain solution to make GDPR compliance possible?

The data protection authorities of the EU Member States, the European Data Protection Board (EDPB), and the respective courts, including the European Court of Justice (CJEU) have not yet concluded which technology approaches ensure a GDPR-compliant blockchain solution. However, the following represent some technologies and common strategies that may be used to meet certain GDPR requirements when processing personal data while maintaining the desired functionality of the blockchain.

These possible solutions have been recognised by the European Union Blockchain Observatory and Forum,[98] the European Parliamentary Research Service's Panel for the Future of Science and Technology,[99] as well as the French Data Protection Authority (CNIL).[100] However, it is important to note that of the above three entities, only CNIL has legal authority to determine with a relative degree of certainty the legality of a solution, and its ruling could in theory be overturned by the EDPB and CJEU at a future point in time. Legal advice on a case-by-case basis is still recommended when in doubt.

On-chain/off-chain configurations and hashing	Role-based access controls (RBAC)	Zero-knowledge proof (ZKP)	Homomorphic encryption
Basic protections, such as on-chain/off- chain configurations, and only storing hashed data on the blockchain	Enable selective obfuscation of data depending upon the identity of a particular participant	Allows users to prove their knowledge of a value without revealing the value itself	An approach in which data is encrypted before being shared on-chain. It can then be analysed without decryption

Figure 10.2 – Major design options for data confidentiality in a blockchain solution

For a broader overview of some of the current technologies that establish data protection on a blockchain, see the module Data Protection.

The following is an explanation of each technology and its relevance to GDPR compliance.

On-chain/off-chain, obfuscating personal data and GDPR compliance

Under the GDPR, personal data must only be kept for as long as is necessary to achieve the aims for which it was collected. Being unable to delete or effectively delete such personal data from a blockchain, due to the principle of immutability, could constitute a breach of the GDPR because the "data controller" would be unable to protect the data subject's right to erasure.

Where personal data is being processed for a supply-chain solution, a potential approach would be to store only a hash of the relevant personal data on the blockchain, instead of storing the personal data itself on the blockchain. The personal data could be stored off-chain.

The hashing or obfuscation of personal data can increase the control and security of the original personal data maintained by the data controller and

allow the data controller to continue to protect and fulfill data subjects' rights requests. For example, if a data subject were to request erasure of their personal data, the data controller would be able to make such deletion by deleting the personal data stored off-chain, leaving what would then become a meaningless hash on-chain.

This solution also presumes that (a) the hash makes the original personal data inaccessible – e.g. the hash cannot be somehow processed to reveal the original personal data; (b) deleting the original personal data is enough to render the hash meaningless even when combined with any other information – e.g. any relevant keys, information stored on other parts of the distributed ledger; and (c) that regulators are satisfied by this strategy.

This approach could permit meaningful analysis to be conducted (on usage patterns, for example), while having the potential to achieve GDPR compliance if applied comprehensively across the entire blockchain – and the presumptions in (a), (b) and (c) are true.

Role-based access controls and GDPR compliance

Data integrity problems, especially non-adversarial ones, are not new to the supply-chain world. Thus, the solutions relevant to preventing benign data-integrity faults in a blockchain context don't differ much from the solutions applied to data-integrity concerns in a more traditional supply-chain context.

It is relatively straightforward to prevent benign faults, since doing so doesn't require anticipating the potential actions of intelligent and resourceful attackers. The same traditional principles and techniques apply – employing From a GDPR perspective, role-based access controls (RBAC) may be an effective tool to address compliance challenges. Ultimately, GDPR obligations largely apply to the treatment of the personal data regardless of whether the data handler is defined as a controller (who determines the purposes and means of processing personal data) or processor (who processes personal data on behalf of and at the instruction of a controller).

In the GDPR framework, the controller in a blockchain is anyone who determines the purposes and means of processing personal data by writing or adding personal data to the blockchain in a professional or commercial capacity, and a processor is anyone who processes that personal data on the controller's behalf or at the controller's instruction.

Anyone who accesses the blockchain to read the personal data needs to ensure that they have a lawful basis on which to process the data they access. In a blockchain, this lawful basis is unlikely to exist without some sort of contractual relationship between the blockchain actors.

An open-access blockchain solution without role-based access controls or other access restrictions (such as a public blockchain) does not fit neatly into this framework, primarily because it is difficult to identify any one entity who can be held liable, or be compelled to uphold data protection regulations that would apply to the personal data on that public blockchain solution. While it may be clear who the controller is before the personal data is uploaded to the blockchain and in a traditional client-provider model, it is less clear what happens after upload. On upload, the personal data will be collectively processed via a shared protocol leaving no way for the controller to ensure that any blockchain recipient maintained GDPR requirements.

Because of this shared protocol if the blockchain participant is a processor, the problem in such cases is to determine how the original controller can compel the processor to meet GDPR requirements (such as enforcing data-subject rights) and abide by the original terms of disclosure from the data subject to the controller.

If the blockchain participant is a new controller, they have no defined relationship with the data subject, so it is unclear on what legal basis the new controller would process that personal data. It is clear, then, that the disclosure of personal data to the blockchain would present significant GDPR compliance problems for the original controller and create an enforcement nightmare for the data subject.

Note that legal uncertainty remains around the status of actors who act as validating nodes in public permissionless blockchains as the GDPR was not designed with this particular scenario in mind.

Potential approaches. It may be possible to address this problem architecturally by designing a private permissioned blockchain solution, whereby all participants must agree to abide by certain GDPR-compliant terms as a condition to being granted permission: e.g. permitted uses, rules on retention periods, deletion, security and data export to foreign jurisdictions.

Moreover, as CNIL has recommended, the private consortia of the permissioned blockchain networks should also identify the controller, or joint controllers as soon as possible.[101] No public or unauthorised access to the blockchain data would be permitted, or such access should be considered carefully. However, it is unlikely that this would address concerns regarding how liability for errors would be apportioned, if at all.

Data subjects maintain a right to have inaccurate personal data rectified, and so while blockchain maintains good security over data tampering, once that data has been added, any solution will still have to deal with the problem of faulty or fraudulent data being added in the first place.

A possible countermeasure may be to cut off a "bad" participant who consistently shares faulty or fraudulent data. However, where such errors have financial consequences, the matter of enforcement among the blockchain participants – for example, who can bring a claim, what would be the quantum of such a claim, and how will liability be apportioned - becomes important and should be considered at the blockchain-solution design stage.

Zero-knowledge proof

Zero-knowledge proof allows one party to assert the validity of a statement without revealing the underlying facts that make the statement true or false. The algorithm that accomplishes this runs a statement through a true/false test repeatedly until the probability that that statement is false becomes incredibly low. At this point, one is able to confidently assert that the statement is true. One of the key advancements in zero-knowledge proof is s zero-knowledge succinct non-interactive argument of knowledge (zk-SNARK). This technology significantly reduces the time it takes a zero-knowledge proof algorithm to return a result and is one of the most powerful and promising features of blockchain. The obfuscation of the underlying data, including any personal information, may render the obfuscated personal data fully anonymised.

Fully homomorphic encryption

Fully homomorphic encryption (FHE) is a way by which mathematical calculations can be performed off-chain on encrypted data and return an encrypted result. However, the latency of a system that uses this method of computation is even slower than one that uses zero-knowledge proof. While supply-chain partners would be able to run data analytics on artificial-intelligence algorithms on fully encrypted data, and only those who should have access to the result would be provided with a key to decrypt it –and therefore the data may be fully anonymised. The slowness of FHE, however, means that it may not generally beworth the undertaking unless a supply chain

> *With an emerging technology like blockchain, the readiness or maturity of the technology is important to note when designing a solution. Regarding data protection in particular, fully homomorphic encryption (FHE) might seem ideal from a technical perspective for securing information. But from a practical standpoint, it may be slow and thus should be applied only to a limited type of data processing. Given the current state of FHE, it is more realistic to use ordinary encryption or an off-chain database as the use cases likely to benefit from FHE would be limited.*
>
> **Takayuki Suzuki,** Financial Information Systems Sales Management Division, Hitachi, Japan

has a computation for which it does not need real-time, or close to real-time, transmission.

Other methods to approaching GDPR compliance

Storing personal data off-chain with an on-chain hash and adopting role-based access controls are two of the most commonly used approaches to strive for in order to achieve GDPR compliance in a blockchain deployment. However, it is important to note that other approaches also exist. Although uncommon, editable blockchains permit data-subject rights to be respected by allowing a private permissioned blockchain administrator to delete and edit incorrect or outdated information; the trade-off is that it also sacrifices the immutable nature of blockchain. Other solutions allow for deletion by encryption, whereby a blockchain administrator makes certain data inaccessible by increasing the permission needed to access a pre-existing block on the blockchain. It is currently unclear whether this solution would be considered GDPR-compliant by data protection regulators.

4. Principles for building GDPR-compliant solutions

What are four key principles for GDPR-compliant blockchain solutions to follow?

In 2019, a report by several supply-chain industry groups and law firms identified four guiding principles for GDPR-compliant blockchain solutions.[102]

The principles as outlined in the report are:

1. **Use a private, permissioned blockchain when you collect and process personal data.** While the most common vision of blockchain is of a fully public, permissionless network, there are many private networks that are in fact private and require permission to join. Because anyone can join a public permissionless blockchain, it is impossible to ensure participants agree to necessary rules around the protection of personal data. As a result, the private, permissioned blockchains can be employed to work towards a GDPR-compliant blockchain solution. Additionally, proper mechanisms should be put in place when connecting private and public blockchains.
2. **Avoid, if possible, the storing of personal data on the blockchain.** The most obvious way to avoid GDPR compliance issues is to use a blockchain solution that does not process any personal data and minimises free-form data storage. While keeping a blockchain completely free of personal data will be very difficult to achieve, this may be done by deploying advanced cryptographic techniques such as data obfuscations, hashing and aggregation. For example, a blockchain solution can store a hashed representation of the personal data on the blockchain, with the underlying and identifiable personal data kept off-chain. Middleware can then be used to combine off-chain and on-chain data to provide a complete view that includes the off-chain personal data for authorised users only.
3. **Establish a detailed governance framework.** Given: (a) the need to adequately protect personal data; (b) the requirement to establish

contractual relationships governing the processing of personal data between parties; and (c) the legal obligations on data controllers to provide individuals with the means to uphold their personal data rights, a GDPR-compliant commercial blockchain solution will require a governance framework and data lifecycle management that is contractually binding on all participants and clearly sets out each party's rights and responsibilities.

4. **Employ innovative solutions to data protection problems.** The immutable nature of blockchain data is the one element of the technology which clashes most obviously with data subjects' rights under the GDPR. However, through use of innovative solutions such as advanced irreversible encryption as a means of deletion, it may be possible to comply with the spirit and the policy of the legislation, if not yet fully the word. While there are good arguments for irreversible encryption being adequate for GDPR compliance, definitive guidance from regulatory authorities is necessary in this area. One of the key challenges faced by regulators in this space is balancing legislation and technological advancements as, without doubt, technology is moving at a pace which lawmakers struggle to keep up with.

TOOLS AND RESOURCES

5. Rapid initial analysis for GDPR compliance

Because of the great variety of blockchain solutions and configurations, each needs to be analysed on its own distinct merits for GDPR compliance. The following decision tree (see Figure 10.3) provides a simplified summary of common approaches to approaching GDPR compliance in a blockchain context.

This tree is not intended to provide a final authoritative answer, but to assist with a simplified overview of the choices needed to be made during the design and development of a blockchain solution. A solution which is less likely to be GDPR-compliant requires further evaluation and a data protection impact assessment.

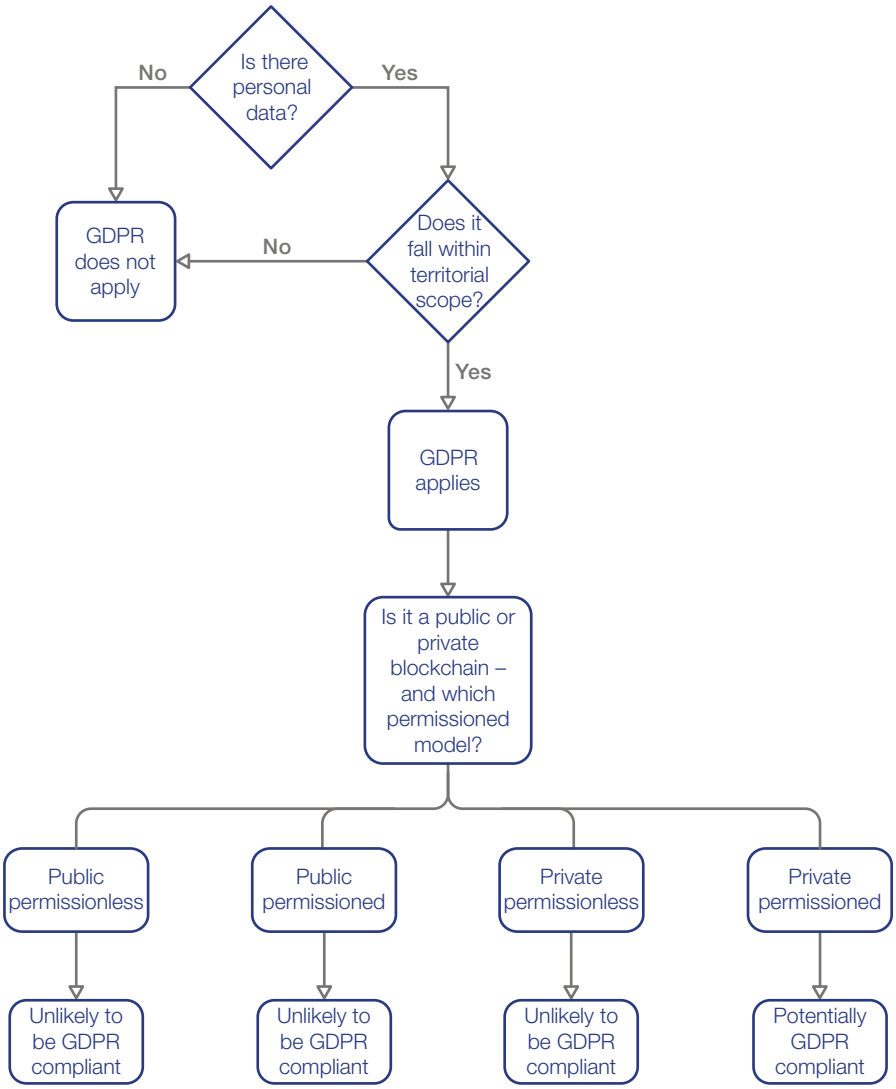


Figure 10.3 – Decision tree with a simplified summary of common approaches for GDPR compliance in a blockchain context. A solution unlikely to be GDPR compliant requires further evaluation and a data protection impact assessment

In conclusion, whilst there is inherent tension between a technology-neutral data protection law such as the GDPR and a specific technology such as blockchain, it is not impossible to become compliant. Legal advice should be sought to ensure that proposed solutions are compliant on a case-by-case basis. Demonstrating compliance where a prescription is not obvious requires a willingness to adhere to both the law (where clear) and the spirit of the law (where the letter of it is unclear) by conducting a data protection impact assessment to satisfy regulatory authorities.

MODULE

Cybersecurity

Overview

Focus Areas

1. Fundamental concepts
2. Top blockchain security risks
3. Blockchain cybersecurity risk management
4. Blockchain secure deployment

Tools and Resources

5. Risk management template
6. Secure deployment process
7. Key questions in securing a blockchain solution

Overview

As they make technology decisions, leaders these days are bombarded with constant headlines about costly enterprise hacks, ransomware, and stolen user data. Thus, any new technology implementation must include adequate safeguards against such nightmare scenarios.

Although blockchain technology is rapidly evolving, there are some fundamental security concepts that can be applied to the blockchain space effectively. After covering these focus areas, this module offers a risk management framework and a 10-step secure deployment plan that should be useful in a wide range of supply-chain projects.

Recommended reading - Inclusive Deployment of Blockchain for Supply Chains Part 5 – A Framework for Blockchain Cybersecurity[103]

1. Fundamental concepts

What are the basics of blockchain security, including factors unique to this new technology and concepts that apply to other areas of IT as well?

It is important to keep in mind that a blockchain solution is part of wider technological, business and human systems. Blockchain solutions do not stand on their own; for instance, they require connectivity, users, and sound business processes. Thus the security of a blockchain is directly related to the security of other systems it is integrated with.

The hype around blockchain technology has also led to a polarised debate concerning security. On one end of the spectrum are those who view a blockchain as inherently insecure and unfit for use cases that would require robust privacy protections for individual users. On the opposite end are those who view blockchain as a cryptography-native, "unhackable" computational module, or even an unhackable solution overall.

The truth lies somewhere in the middle.

A blockchain requires proactive security management, like any other technology. There are information security considerations that cut across technologies that impact blockchain; there are also blockchain-specific security issues.

To better appreciate both the general needs and blockchain-specific considerations, it is necessary to understand a few cybersecurity basics. Once you get the basics of cybersecurity right, a team will be in a much better position to address the nuances related to blockchain. (Figure 11.1 – Cybersecurity basics and blockchain nuances).

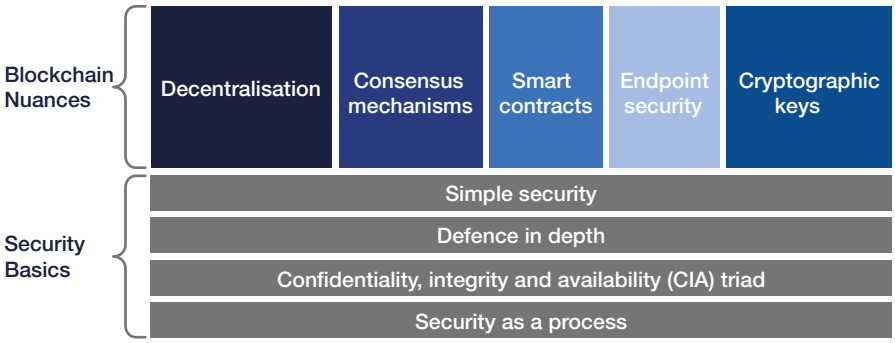


Figure 11.1 – Cybersecurity basics and blockchain nuances

Security basics:

- Security as a process: There is no security silver bullet. Instead, it is a cat-and-mouse game in which attackers and defenders continuously attempt to outsmart each other. No software solution, including any based on blockchain, is ever "secured" with finality. Security is consistently improved, not achieved.

> *Often, I am in situations where I need to educate the client on security, since they would not have brought it up. Interestingly enough, investors also often ask about our approach to security.*
>
> **Hanns-Christian Hanebeck,**
> Founder and Chief Executive Officer, Truckl.io

- **The CIA (confidentiality, integrity, and availability) triad:** Security goals are defined by three properties - confidentiality, data integrity, and availability. However, it's worth noting that pursuing all three properties at once is usually not possible. Blockchain is designed to achieve data integrity in particular. But the confidentiality and availability objectives will conflict with each other, for example. While security controls can help, those deploying blockchain solutions will usually need to make trade-offs on one of the two other goals.

Data integrity and immutability:

In computer security, the terminology "data integrity" is preferred to convey the idea that data has not been altered or destroyed in an unauthorised manner. "Immutability" means perfection of data integrity in some professional context.

In a more commercial context, these terms may be used in a somewhat different way. But in this module we use the terminology as is customary among cybersecurity experts, for the sake of consistency.

- **Defence in depth:** A system design principle that revolves around the idea of introducing multiple layers of defence so that attackers can be detected before they reach critical cores. For blockchain, this suggests security controls at multiple checkpoints, for example, using virtualised private clouds to secure blockchain nodes, opening only the required ports and using access control lists to restrict access to smart contracts.
- **Simple security:** The best security measures are transparent and simple. The idea that hiding something or making it complex will make it secure has been proven wrong time and time again. In blockchain, that means to use tested-and-tried hash algorithms or consensus mechanisms rather than to try to innovate.

> *There is a trend emerging throughout the cybersecurity profession to treat all networks, users and endpoints as zero-trust. In that framework any information technology security work is analogous to the painting of San Francisco's Golden Gate Bridge — the work is always ongoing in multiple areas, using multiple techniques, and with never-ending innovation. Blockchain developers need to think and act that way too.*
>
> **Andrew Borene,** JD, CISSP, Chief Executive Officer, Cipherloc Corporation and Fellow at Georgetown University's Center for Security Studies

Blockchain nuances:

Traditional information security is required to secure the development stack supporting blockchain, from cable to communication network and software security. Beyond this, there are five key blockchain characteristics that require specific security measures:

- **Decentralisation:** Whatever the blockchain type, the essence of the technology is to offer a certain degree of decentralisation. This has profound impacts in security governance, a discipline that has been mostly centralised in the past.
- **Consensus mechanisms:** A blockchain's data integrity is directly linked to the security of consensus mechanisms. For public blockchains, while Proof-of-Work and Proof-of-Stake are the most established consensus mechanisms to date, there are multiple ways in which these are implemented, with various degrees of security and different prerequisites for implementation. For private blockchains, a team can select the consensus mechanism that best aligns with the nature of the desired solution. In either case. it is critical to select the right consensus mechanism and implement it securely.
- **Smart contracts:** A double-edged sword, in light of their data integrity. While the integrity aspect is a good thing to provide hardness to modify something that is agreed upon by multiple parties, it is also important to note that patching smart contracts is not trivial. This will be risky especially where there is transparency to all users of the blockchain in which smart contracts are created. Thus smart code auditing will be fundamental to include as well.

Example

Following the logic that blockchain builds upon traditional information technology, TradeLens, an industry platform developed by Maersk and IBM, obtained information security certification against the ISO/IEC 27000 standards, maintained by a joint technical committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

- **Endpoint security:** While this is not strictly limited to blockchain, the absence of central entities pushes many security responsibilities to solution developers and users. Because it is very difficult to protect digital access points, solution providers must not just raise awareness among users. They must also clarify individual user responsibilities at the endpoints early on.
- **Cryptographic keys:** These are the foundation of security in blockchains. It is of utmost importance to securely generate, use and store these cryptographic keys.

For broader scope of discussion on decentralisation and its challenges, refer to the modules Ecosystem, Consortium Governance, and focus area Risk identification checklist in the module Risk Factors. More generally, those matters are also covered at length in the designated white paper about blockchain cybersecurity that the Forum has published.[104]

2. Top blockchain security risks

What are the top blockchain security risks, how can they be mitigated, and how do they compare to traditional databases or other familiar technologies?

As mentioned previously, one of the goals of blockchain design is to achieve data integrity. While various types of blockchains have varying degrees of fault tolerance, most are considered better alternatives than traditional databases, from a data integrity perspective. As a result of the clear strength of data integrity inherent to public blockchains, the top cybersecurity risks related to public blockchains tend to be related to the confidentiality and availability goals. (See the CIA triad introduced earlier). In private blockchains, however, confidentiality will be a less challenging risk while the level of data integrity may be less than that of a public blockchain. It is important for non-technical expert leaders and policymakers to know that different settings and configurations can change the risk landscape in the deployed blockchain solution; there is not a “one size fits all” answer. In addition, data integrity can have its own risks related to the source and quality of the data that is registered.

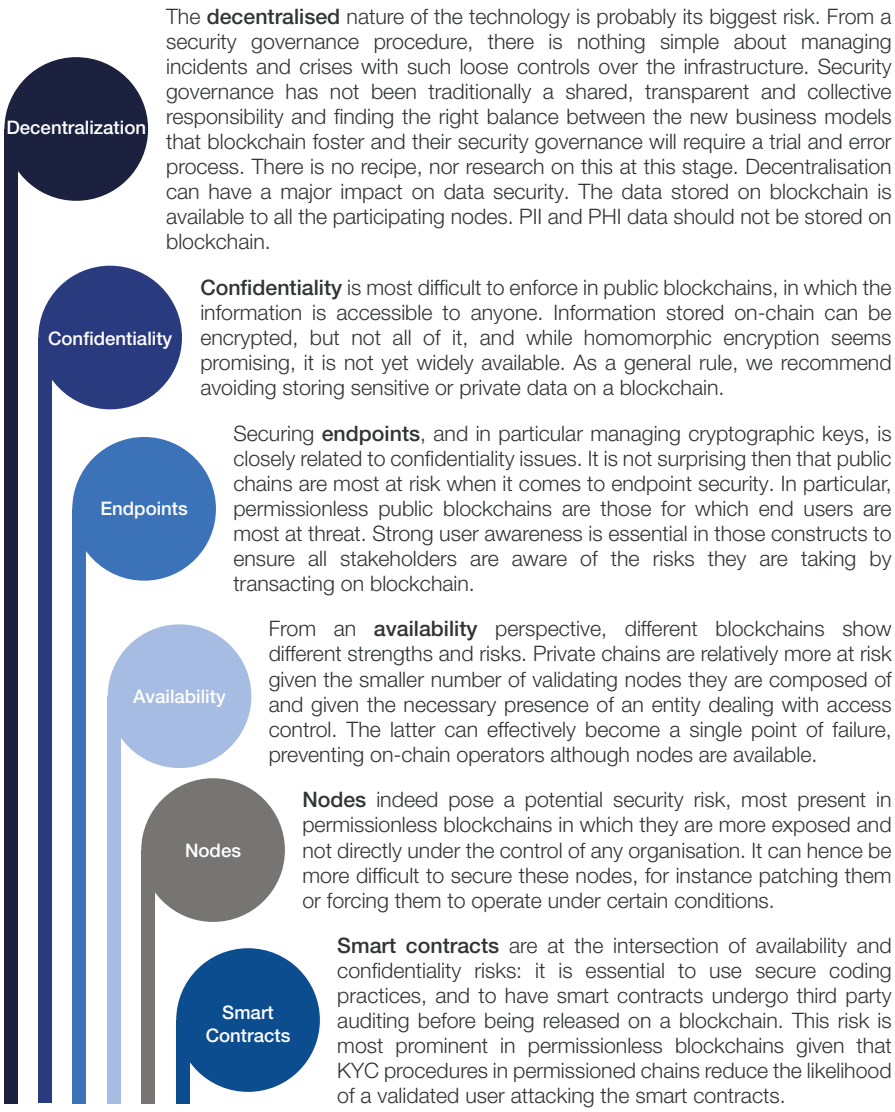


Figure 11.2 – Top blockchain security risks

For further references in the toolkit, there are suggestions at the end of the previous section on Fundamental concepts. Confidentiality is the main topic discussed in the toolkit module Data Protection. And availability, which carries some performance-related risks, is discussed in the module Risk Factors.

3. Blockchain cybersecurity risk management

What specific steps can project teams take to manage blockchain security risks, including initial assessment of potential pitfalls and ongoing management?

A risk is defined as the probability that a threat uses a vulnerability and that this results in a given impact. In light of the risks presented in focus area Top blockchain security risks in this module, organisations deploying a blockchain solution must perform a risk assessment. This is an essential step in the blockchain secure deployment process presented below in focus area Blockchain secure deployment of this module. For further reading, blockchain project teams are recommended to follow the same framework used by organisations for other information technology deployments, such as the US National Institute of Standards and Technology, "Guide for Conducting Risk Assessments, 2012" (NIST SP 800-30).[105]

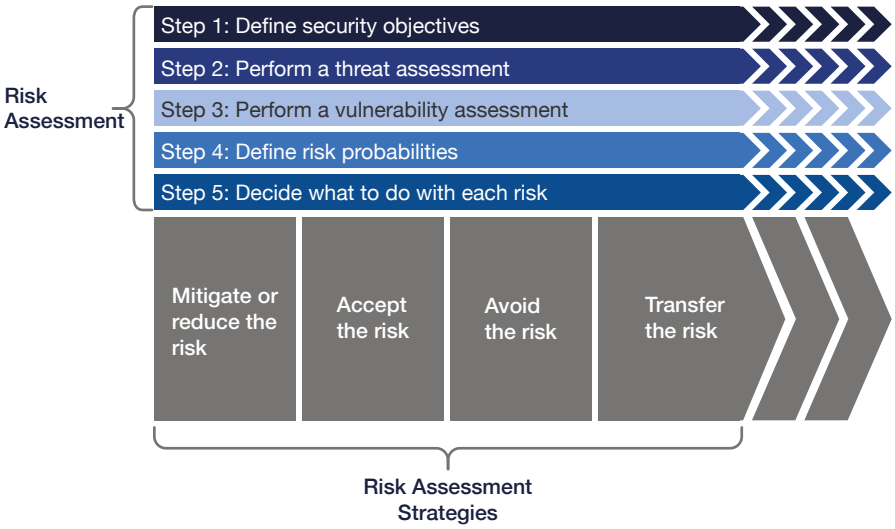


Figure 11.3 – Five-step approach blockchain cybersecurity risk management

Risk assessment generally follows a five-step approach (Figure 11.3 – Five-step approach for blockchain cybersecurity risk management):

Step 1: Define security objectives

This is the foundation of the risk assessment as such, it informs all following steps. In light of the business model that will be supported by blockchain, what are the key security objectives to foster? Would confidentiality be more or less important than availability? Should anonymity be guaranteed? Also, such security features must be upheld by a holistic solution. Which parts of the system must preserve data integrity other than a blockchain platform?

Step 2: Perform a threat assessment

A threat assessment helps the organisation understand what the blockchain solution will need to be protected from, ranging from human accidents to natural catastrophes and deliberate cyberattacks. Differentiating among threats by categorising them according to capabilities and intent is a good way to measure the potential for disruption. For instance, a government agency may have capabilities but no intent to attack a particular blockchain.

Hacktivists, by contrast, may be interested in harming the reputation of a particular organisation but lack the ability to overcome certain security barriers.

Step 3: Perform a vulnerability assessment

A vulnerability assessment helps the project team better appreciate the part of the blockchain solution that will be disclosed to attackers and what weak spots could lead to adverse outcomes down the line. Identifying vulnerabilities is difficult, and all organisations should regularly perform penetration testing on all aspects of the blockchain solutions they deploy. In particular, attention needs to be paid to testing smart contracts. Defining a process early on to secure smart contract code is critical to reduce the vulnerabilities.

Step 4: Define risk probabilities

Defining risk probabilities allows for their prioritisation. Risks emerge from the intersection of vulnerabilities and threats as defined in the previous steps. Prioritise risks by determining the likelihood of particular vulnerabilities intersecting with particular threats, and if that happens, determine the criticality of the impact. A highly impactful risk that is very unlikely to occur will be managed differently from a somewhat impactful risk that is likely to occur regularly. The matrix depicted in Figure 11.4 can be used to define priorities of risks associated with blockchain implementation solutions.

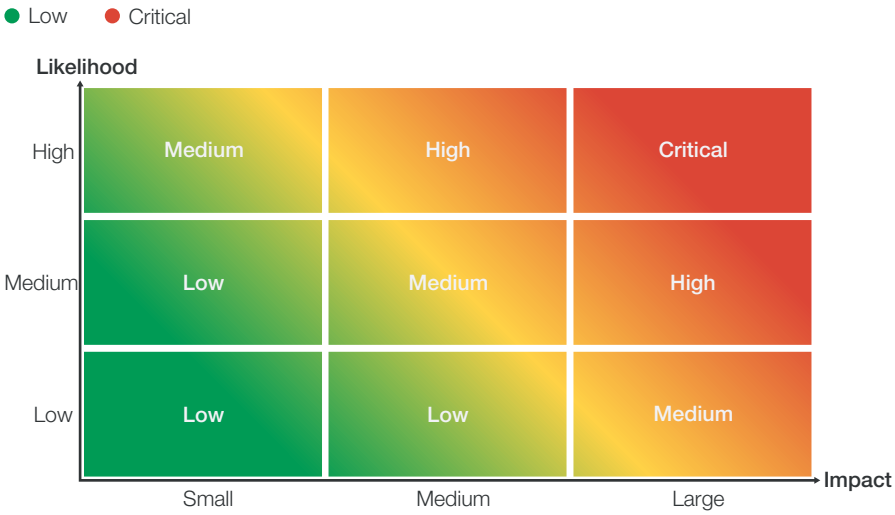


Figure 11.4 – Criticality estimates by likelihood and impact

Step 5: Decide what to do with each risk

Once you have identified specific risks that may arise in your project, it is time to address each one individually. There are four strategies for managing any particular risk. (See Figure 11.5 – Strategies to manage specific security risks to a project):

- **Mitigate or reduce the risk.** Tackle the threat and/or the vulnerability directly to contain its impact. In blockchain, containing impact is perhaps more challenging than with other technologies, and emphasis should probably be placed on reducing vulnerabilities and deterring threats. This strategy offers the best risk control but is generally costly. It is best advised for high and critical risks.
- **Accept the risk.** Acknowledge its existence and budget for it should it materialise. This approach is best advised for low to medium risks.
- **Avoid the risk.** Re-work the systems approach in order to eliminate the specific security challenge entirely. Doing this generally involves trade-offs and accepting the removal of certain functionalities or solution users.

- **Transfer the risk.** Involve a third party, such as an insurance company or an external service provider, to address the risk.

Due to the complexity of blockchain, using external expertise to develop a solution, and another entity to review and audit its results, is highly recommended.

Figure 11.5 – Strategies to manage specific security risks to a project

Depending on the level of engagement in security engineering, it is recommended that the reader refer to topics in other modules, such as Data Protection, Data Integrity, and Personal Data Handling. Also, cybersecurity risk management should be treated as part of overall risk management, as explained in the module Risk Factors.

4. Blockchain secure deployment

What are the key steps to maintaining the security of a new blockchain solution as it moves from planning and development into everyday use by end users?

This focus area introduces a ten-step blockchain secure deployment process (Figure 11.6 – Ten-step blockchain secure deployment process). It is important to integrate these steps into a system's design and implementation for a blockchain solution. This is a complex process, so it is highly recommended to use and refer to more complete documents on integrating security engineering into software development lifecycles, such as one in the US National Institute of Standards and Technology, Special Publication.[106]

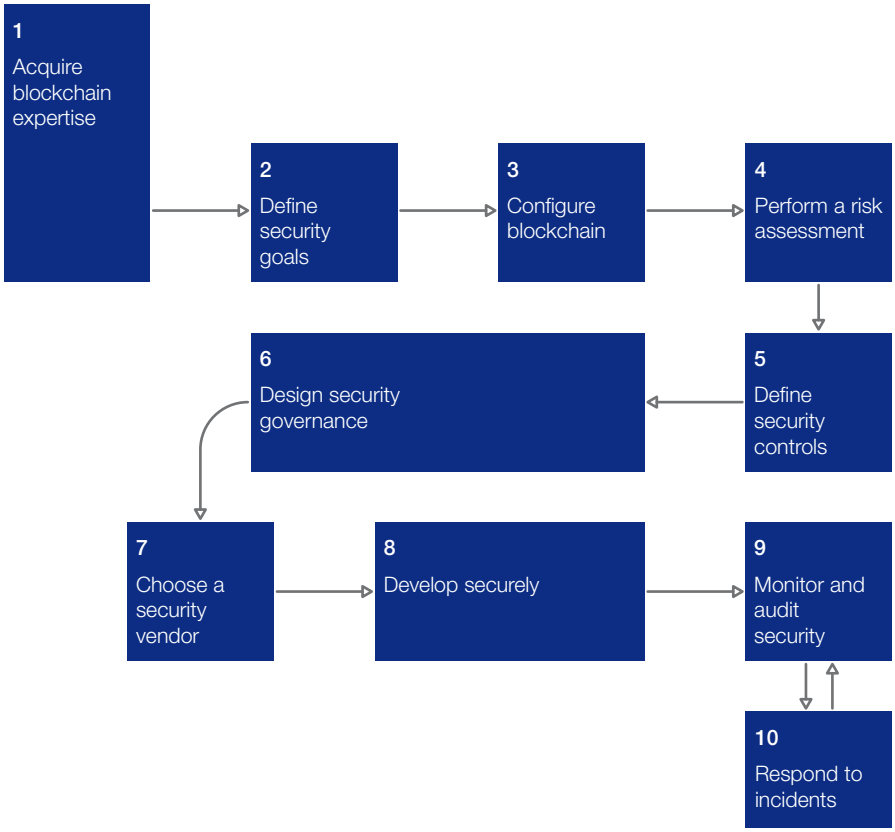


Figure 11.6 – Ten-step blockchain secure deployment process

Step 1: Acquire blockchain expertise

Depending on the organisation's resources, and the criticality and objectives of the blockchain use case, this can range from outsourcing to a trusted third party to hiring or training staff with the necessary skills to oversee a secure deployment. With regards to blockchain security expertise, it may prove more effective and efficient for project teams to retain qualified cybersecurity experts and train them in blockchain technology rather than to hire blockchain advocates and train them as security experts. To assist project leaders in assessing credentials, there are several international information security accrediting bodies.[107]

Step 2: Define security goals

Defining which security goals the organisation will prioritise in the CIA triad is a prerequisite. These goals must align with the organisation's strategy, crisis management, and business continuity policies.

Step 3: Configure blockchain

Depending on the business objectives and the security goals, choose which blockchain type would provide the best platform. Pay attention as well to other basic configurations such as whether smart contracts will be used and which consensus mechanism will verify transactions. It is quite probable that the business rationale and functional specifications will inform these decisions. While this is not true security-by-design, it is the means by which most real-world implementations will begin.

Step 4: Perform a risk assessment

Determining which specific risks are associated with a particular blockchain is key to being able to deploy it securely. Refer to focus area Top blockchain security risks and Blockchain cybersecurity risk management in this module for more details on how to perform a risk assessment.

Example

The Port of Valencia recently commissioned a blockchain solution to enable different entities working at the port to share data in a more efficient way. Before developing a proof of concept, the leadership team defined the following high-level security objectives, among others:

- Data confidentiality is critical
- The availability of the blockchain solution must be better than the one currently in place
- Ability to identify all entities participating in the consortium

The blockchain network must be compliant with the European Union's General Data Protection Regulation (GDPR).

Example

To better understand the risks of a planned blockchain solution, the Port of Valencia had the opportunity to assess the security risks of a blockchain solution during a proof-of-concept implementation.

Examples of the main potential vulnerabilities identified:

- The scenario where an attacker rewrites the ledger by compromising a sufficient number of nodes. This will put the community (this case a consortium) at serious risk.
- The administrator's secret key becomes accessible to other parties, who can then impersonate the administrator and even change the smart contracts.
- Node administrators are able to access confidential data stored in the node.
- The administrator leaves the organisation.

Examples of the main potential threats:

- A competitor in the consortium with administration rights to the node could be accessing confidential data from other organisations in the ledger.
- Someone with administration rights can access the data stored in an external database that is linked to data found on the blockchain.
- Hacktivists could be drawn to the blockchain network.

Step 5: Define security controls

Security controls may be able to reduce risks by technical countermeasures before residual risks are transferred, avoided or accepted. Further details about mitigation strategies are outlined in focus area Blockchain cybersecurity risk management.

Step 6: Design security governance

It is critical for a governance model and security-related processes to be defined prior to development kick-off. Once development starts, even a test version of the use case can be a source of security threats. The governance processes will largely depend on the risks to be monitored. The more risks there are to manage, the more thorough the governance process will need to be.

Step 7: Choose a security vendor

Choose the right security products and services, then evaluate vendors. There are several established enterprise solutions out there, all offering broad levels of security service. In addition, boutique companies and smaller consulting firms can help with niche needs.

Step 8: Develop securely

Ensure that the development team follows secure development practices, also known as DevSecOps, and, in particular, a secure software development life cycle (S-SDLC) methodology. S-SDLC ensures that security assurance activities such as penetration-testing, smart code auditing or architecture analysis are embedded in the development of the blockchain solution.

Step 9: Monitor and audit security

Blockchain is an information technology like any other, so it is wise to integrate procedures and runbooks regarding the blockchain solution into the organisation's existing overall security plans. On top of these, a blockchain solution will require more collaborative actions with external organisations including node owners and consortium members. In addition to regular

exercises to test staff, it is important to check external communication required upon a potential incident and distributed decision-making processes. Blockchain security incident response will require multiple stakeholders.

For further reference, the major blockchain configuration over public or private is discussed in the module Structure: Public / Private. For security goals, the modules such as Data Protection, Data Integrity, and Personal Data Handling are most relevant. Designing governance on security aspects is part of topics in the module Consortium Governance.

5. Risk management template

Table 11.1 is an example of the worksheet for risk assessment which is introduced in focus area Blockchain cybersecurity risk management. The table is followed by a guide illustrated with an example to fill the risk assessment worksheet (Table 11.2).

Table 11.1 – Worksheet for risk assessment with a demonstrative example

Security objective	Type of information	Vulnerability	Threat actor	Risk likelihood	Risk impact	Mitigation strategy	Security controls
Confidentiality	Cargo manifest	Encryption key stolen from an unpatched client PC	Monetarily incentivised attacker	High	Medium	Reduce	Advanced key management

Instructions for filling in the above table are given below. Overall, the security objective and type of information will specify what to protect. Vulnerabilities and threats are related to the potential attack on the information. From these, risk likelihood and risk impact are evaluated. After comparing across rows, one prioritises and assigns resources and defines the mitigation strategy and security control for each entry.

Table 11.2 – Guide and example to fill the risk assessment worksheet

Column item	What to fill in	Example
Security objective	Confidentiality, data integrity, or availability	Confidentiality: the type of information should be readable only by legitimate users
Type of information	Information asset that the solution tries to secure, for example information, data, history, or code to protect	Trade secret information described in cargo manifest. This is secured by encryption
Vulnerability	Potential weakness of the solution that an attacker may exploit	Encryption key disclosure due to hack on an unpatched client PC that stores the encryption key
Threat actor	Type of attackers. Incentive and capability	Monetarily motivated attacker to frighten and try to draw money from the cargo owner
Risk likelihood	High, medium, or low	High (the cargo owner is a large enterprise)
Risk impact	Large, medium, or small	Medium (trading secret may be an advantage to competitors, but not so large)
Mitigation strategy	Accept, transfer, reduce, or avoid	Reduce
Security controls	Method for the chosen mitigation strategy	Advanced key management including frequent key updates, machine generated keys, biometric authentication to get access to the key, etc.

6. Secure deployment process

Table 11.3 summarises the blockchain secure deployment process which is described in focus area Blockchain secure deployment. Refer to the focus area for details regarding each step.

Table 11.3 – Ten-step process of secure deployment

Secure deployment steps	Prior steps	Parties involved	End goal / deliverable
[1] Acquire blockchain expertise	-	Human resources department	Creation of a blockchain security team with in- and out-sourced resources
[2] Define security goals	1	Blockchain security team, Chief Information Security Officer (CISO), Chief Strategy Officer	A one-pager outlining the security goals
[3] Configure blockchain	1,2	Blockchain security team, blockchain experts	A list of security and business advantages and trade-offs of the various blockchain configurations considered
[4] Perform risk assessment	1,2,3	Blockchain security team, IT security department	A list all of the risks and the different management strategies chosen. See risk management template
[5] Define security controls	1,4	Blockchain security team, IT security department	A list of the security functional specifications of the blockchain and recommended security controls for the development team
[6] Define security governance	1,3,5	Blockchain security team, CISO and CISOs of all the organisations that play a relevant role in the operation of the blockchain	Revised business continuity and disaster recovery plans
[7] Choose security vendors	1,5	Blockchain security team, blockchain security vendor	One or more contracts with security vendors
[8] Develop securely	1,7	Blockchain security team, blockchain solution vendor	Well-documented source code and planned security activities
[9] Monitor and audit security	1,6,8, 10	Blockchain security team, security operations centre, third party auditors	Active monitoring of the blockchain solution in the SOC
[10] Respond to incidents	1,6,9	Blockchain security team, incident response team or consultants	Timely mitigation of security incidents

7. Key questions in securing a blockchain solution

Below is a checklist meant for assisting organisations in structuring their thoughts around key questions to secure a blockchain solution.

- ☐ Does a blockchain solution improve the project effort's overall security posture?
- ☐ What nuances does blockchain security entail and how will the project team achieve a satisfactory level of security?
- ☐ What are the specific cybersecurity considerations to have in mind before developing a blockchain solution?
- ☐ What are the security trade-offs in using one particular type of blockchain over another?
- ☐ What should you absolutely not store on a blockchain?
- ☐ Which are the most relevant information security risks that impact blockchain solutions specifically?
- ☐ How should security be managed throughout the lifecycle of a blockchain solution, from ideation to inception, and through development, deployment, and operation?
- ☐ Have you considered needed cybersecurity and blockchain security expertise prior to developing the blockchain solution?
- ☐ Have you referred to the wider security goals of the organisation prior to developing the blockchain solution?
- ☐ Have you defined the security objectives that the blockchain solution will need to meet?
- ☐ How confident are you that the blockchain solution's underlying infrastructure allows the organisation to achieve both its business and security objectives?
- ☐ Have you listed, prioritised, and acted upon the different information security risks the blockchain solution will face?
- ☐ Have you implemented security controls for residual risks?
- ☐ Have you discussed with the other parties involved in the operation of the blockchain solution how security governance will take place?
- ☐ Have you researched various security vendors and are you confident that the blockchain developers will follow a secure development lifecycle process?
- ☐ What will you do to monitor the security of the blockchain solution over time?
- ☐ Have you updated the crisis management and business continuity procedures in light of the blockchain solution?
- ☐ Have you identified Security Operations Centre resources to monitor and respond to blockchain incidents?
- ☐ Are you committed to ongoing penetration testing, monitoring, and innovation in the security of the blockchain throughout the entire lifespan of the project?

MODULE

Legal and Regulatory Compliance

Overview

Focus Areas

1. Common legal and regulatory issues with blockchain use
2. Legal matters: roles in the blockchain network
3. Legal matters: nature of the transactions
4. Legal matters when establishing a blockchain network
5. Understanding the jurisdictional issues of the network
6. Smart contracts

Tools and Resources

7. Starting point to identify legal and regulatory matters

Overview

Transitioning to cutting-edge technologies has often involved a significant hurdle and the transition to blockchain is no different: laws written decades ago were not drafted with distributed data exchange or self-executing contracts in mind. This may lead to uncertainty about the new technology's compliance requirements within organisations, sometimes exacerbated by differences between regulators in different jurisdictions.

That said, there are some common considerations that need to be addressed by blockchain projects from a legal and regulatory standpoint. A discussion of them follows, with the caveat that projects should also consider jurisdiction and industry-specific laws and regulations, and the advice of local counsels where the organisations operate should always be taken.

1. Common legal and regulatory issues with blockchain use

What are the most common legal and regulatory issues that arise when using blockchain technology?

> *There is no settled "law of blockchain" so we are interpreting existing legal and regulatory concepts in light of this new technology. As the scope and breadth of use cases increases, the legal certainty will also increase but this will take time. It is crucial for any project to embed legal and regulatory compliance into the design at the outset.*
>
> **Stuart Davis,** Partner, Latham & Watkins

Blockchain technologies may expose the blockchain network operator and/or participants in the network to legal and regulatory uncertainty because many governments and regulators are still working to understand blockchain and whether certain laws should be updated to properly address decentralisation.

While some governments are spearheading the adoption of blockchain, many national and regional regulators are adopting a wait-and-see approach, preferring to explore and understand blockchain's implications before moving forward with additional legal and regulatory requirements or guidance. The lack of regulatory certainty and evolving legal and regulatory position is challenging for market participants, and it is necessary that they continually assess their participation in blockchain networks.

In essence, blockchain network participants' dual challenge for now is to ensure that they are compliant with current regulations while also mitigating as much as possible the business risks associated with possible changes in the regulatory environment.

The following are some of the most common compliance-related issues that arise with the use of blockchain technology, though, of course, this would be subject to the specific use case and jurisdiction and industry specific rules and regulations.

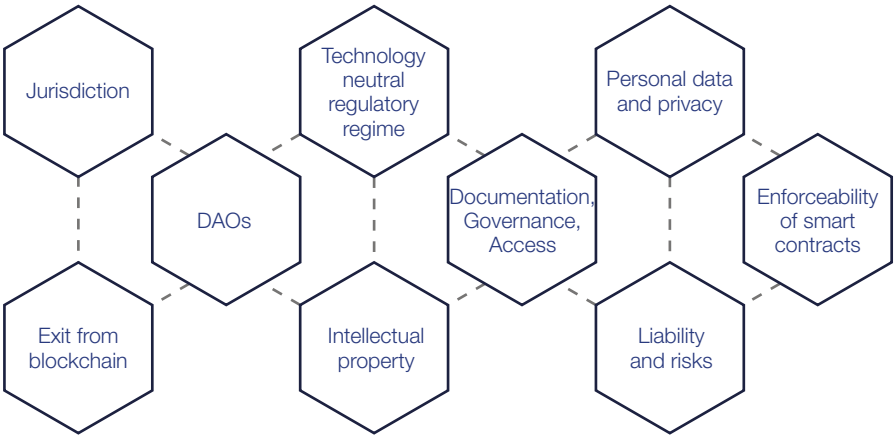


Figure 12.1 – Legal and regulatory common compliance issues

Jurisdiction

Blockchain has the ability to cross jurisdictional boundaries as the nodes on a blockchain can be located anywhere in the world. This can pose a number of complex jurisdictional issues which require careful consideration in relation to the relevant activities of the platform and its participants, as well as the contractual relationships among them. To address such issues, there are increasingly a number of legal and regulatory regimes that have extra-territorial effect, such as the European Union's GDPR or tax laws. As a result, even if blockchain users and nodes are located across the world, local laws may still

apply where there is considered to be a sufficient nexus to that jurisdiction. It is the types of activities occurring in each jurisdiction and the role of each participant on a blockchain which should be carefully considered to see if they might be subject to the local laws of a particular jurisdiction.

Technology neutral regulatory regime

Regulatory licensing and compliance regimes are typically not drafted with the intention of regulating specific technologies. Rather the usual intent is to regulate the activities that the technology helps facilitate. However, neutral drafting can make it difficult to interpret how regulation should apply and which participants should be caught. It is, therefore, necessary to carefully assess the nature and activities of a blockchain network and its participants and determine where that platform and its participants should sit within the regulatory landscape.

Governance and legal documentation

The utility-like nature of a blockchain platform means that it is necessary to properly document the relationship between the blockchain network, the network operator (if any), and its participants through legally enforceable contracts. It is important to establish a clear and robust governance model concerning interactions among participants in the network. The model should also set out clearly the applicable terms and conditions to the blockchain platform, e.g. the mechanisms by which the network operator may implement changes to the network or the requirements around its participation. Objective and fair criteria should be set to govern access to the network and suspension or termination of participants from the network. For further discussion of such issues, see sub-section Legal documentation under focus area Legal matters when establishing a blockchain network in this module.

Liability

Blockchain poses novel and different risks as a consequence of the nature of the technology and manner of operations, including risks relating to security, confidentiality, regulation, taxation, data protection, immutability, automation and decentralisation, among other risks. Therefore, the allocation and attribution of risk and liability in relation to the blockchain network and the transactions processed on the network (including any errors, failures or malfunctions) must be carefully assessed and documented within each layer of network participation.

Intellectual property (IP)

To truly unlock the potential of blockchain, the underlying technology, including its software, will have to be shared in order for value to be gained. The nature of such 'sharing' depends entirely on the specific nature of the blockchain in question, including its purposes, subject matter, and relationship between the blockchain participants. It is therefore important to consider questions around the nature of the underlying IP, IP ownership and licensing arrangement as part of the structuring of the blockchain.

The core considerations and possible IP options (e.g. in respect of IP ownership and licensing) are, to a large extent, no different than that of any other traditional IP regime or software development agreement and, depending on the agreed licensing provisions, are likely to hinge on whether those specific requirements could give a customer a competitive edge and/or can be used by the blockchain vendor (i.e. is there any exclusivity, what is the nature and extent of the licensing provision). Developers and IP owners will have to determine their IP strategy, including who owns what, and protection

on all levels. Vendors will likely want to capitalise on any other commercial benefits to be generated from the blockchain, including commercialisation of the underlying dataset by way of licensing-out the underlying IP. Especially in public blockchains based on open-source software, this can be challenging, but creating mechanisms to identify who created and who owns what (e.g. time-stamps) should be considered. In addition to considerations on the ownership of the IP in the underlying blockchain, another important question relates to whether the blockchain can be used to record ownership, use and remuneration of IP licensing/transactions. For additional discussion of IP considerations, see sub-section Intellectual Property under focus area 2 in this module and the modules Consortium Governance and Risk Factors.

Personal data privacy

One of the key unique selling points of a blockchain system is that once data is stored, it cannot be altered easily, if at all. This clearly has implications for data privacy, particularly where the relevant data is personal data or metadata sufficient to reveal someone's personal details. Data protection regulation may require that personal data be kept up-to-date and accurate or deleted at the discretion of the individual, and the immutability of a blockchain system may not be consistent with such requirements. For further discussion of such issues, see sub-section, Data protection and cybersecurity, under focus area 4 in this module and the module Personal Data Handling.

Decentralised autonomous organisations (DAOs)

DAOs are essentially online, digital entities or organisations that operate through the implementation of pre-coded rules maintained on a blockchain platform. The decentralised nature of DAOs presents unique questions that did not need to be addressed previously as traditional entities were centralised and had a recognisable legal structure and form. What legal status or liability will attach to a DAO? Are they simple corporations, partnerships, legal entities, legal contracts or something else? This will depend on how each DAO is structured and the jurisdiction in which the DAO is incorporated (if any). There is a section on DAOs in focus area Understanding the jurisdictional issues of the network of this module where these issues are more extensively examined.

Smart contracts

Smart contracts aren't always or necessarily legal contracts in the traditional sense, despite the word 'contract'. Whether smart contracts are considered to be legal contracts is a question of whether the elements of a legal contract are present. In essence, smart contracts are self-executable computer codes and as a result, their use may present enforceability questions if attempting to analyse them within the traditional 'legal contract' definition. For further clarification, a smart contract is not a blockchain per se but an application of blockchain, i.e. one possible use of blockchain. Many smart contracts are structured to automate actions, instructions or clauses of separate legal contracts but they do not constitute legal contracts themselves and these non-legal contracts present fewer legal risks.

However, some smart contracts themselves are being structured as legal contracts and therefore have the full force of law. In such cases, it will be necessary to understand how they meet the pre-conditions for contract formation in different jurisdictions, as well as how they will be construed and interpreted by a court or arbitral body in the event of a dispute. For further discussion of such issues, see focus area Understanding the jurisdictional issues of the network in this module where this is discussed more extensively.

Figure 12.2 – Highlighting that there is a distinction between smart contracts that are legal contracts and those that are not

Exit from blockchain

The need for exit assistance will be determined in large part by the specific solution and the extent to which the blockchain vendor holds the customer's data and how data is stored on the blockchain. If the customer does not have its own copy of the data, it will require data migration assistance to ensure the vendor is obliged to hand over all such data on expiry or termination.

Issues outlined in this focus area are not an exhaustive list of all possible regulatory and legal considerations. Data localisation laws and industry specific laws must be considered when relevant.

Due to the extensive considerations that ought to be given to some of the matters discussed in this focus area, the rest of the module examines some of those in more depth below.

2. Legal matters: roles in the blockchain network?

What are the legal concerns given my organisations role in a blockchain network?

When building and scaling the blockchain network and establishing the governance, discussed in the modules Ecosystem, Consortium Formation, and Consortium Governance, it is important to understand key legal considerations. This and the following few focus areas look at the most common legal concerns when establishing and managing a blockchain network.

Figure 12.3 – When building the network (step 3), it is important to pay attention to important legal and regulatory concerns

When establishing and building a blockchain network, consider the legal concerns per network participant. Different actors in a blockchain network will have different legal concerns. An entity might play more than one of the roles below, but it can be helpful to think of each role as bringing different and distinct responsibilities.

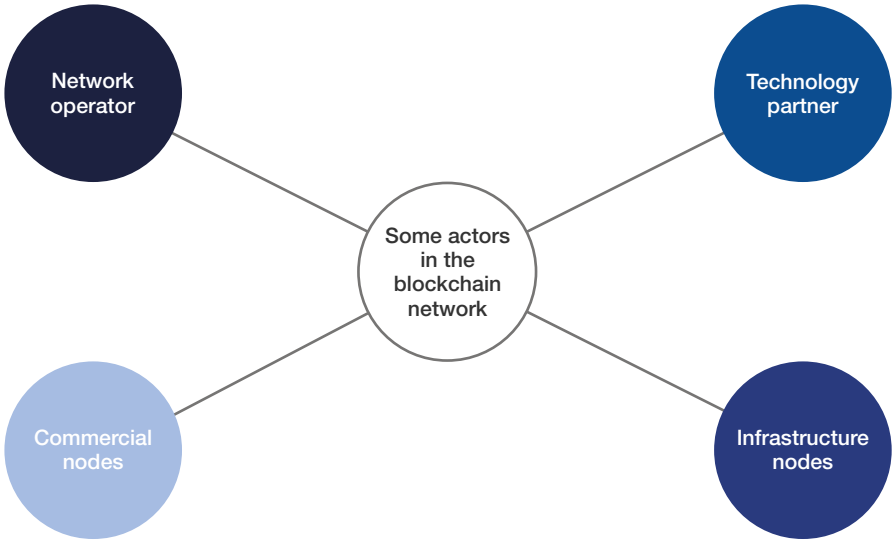


Figure 12.4 – Each participant to a blockchain network will have different and distinct legal responsibilities and concerns

The respective legal considerations of each blockchain network participant can include:

- **Network operator** who drafts or leads most of the contractual arrangements.

  Network operator will need to lead on enforceability and transparency of documentation in order to ensure the legal and regulatory compliance of the network. There may also be requirements for global information reporting depending upon which jurisdictions the network is attached to.

  Additionally, it will be important for participants to conduct due diligence regarding the regulatory position of the network and/or network operator to ensure that it has formalised its regulatory arrangements and holds the necessary regulatory licences, in case of risk of the discontinuation of the service if the network is found not to hold sufficient licences.

- **Technology partner** who provides a sustainable technology platform.

  Technology partners are often the experts when it comes to designing data and cybersecurity law-compliant systems and will need to maintain the operation of the technology platform.

- **Commercial nodes** that primarily purchase or sell goods.

  Commercial nodes will need to ensure that they balance maximising data sharing to improve efficiency or effectiveness of their business without revealing commercially sensitive information or trade secrets. See the module Personal Data Protection for further discussion.

- **Infrastructure nodes** that facilitate financial or physical infrastructure.

  Banks or shipping companies will need to push for data exchange that meets local compliance standards for authentication, audit and other regulations like customs.

Each participant should be solely liable for considering its own legal and regulatory position when joining the network and ensuring that it holds any necessary licences in relation to their activities on the network. Participants should determine whether the services provided through the network constitute outsourcing and whether the additional compliance requirements are met.

Another consideration for participants at the outset is who holds legal/regulatory liability in a permissioned network for cases such as data breach or smart contracts errors? Considering this up front is essential to ensure that the network operator and network implement proper systems and controls to mitigate such risks.

3. Legal matters: nature of the transactions

What are the types of transactions that take place on the blockchain network and their related risks?

It is crucial for network operators and participants to understand the nature of the platform and the transactions taking place on the network in order to assess the legal steps that need to be taken.

There are specific legal and regulatory regimes that apply to different types of transaction and the legal and regulatory requirements, as well as the documentation suite, attached to these transaction types can differ markedly (both within a single jurisdiction and across borders).

For example:

- **Transactions relating to goods and services:** May be subject to sale of goods legislation in both the jurisdiction of the seller and the buyer.
- **Bills of exchange and letters of credit:** Typically governed by specific legislation and, potentially, regulatory requirements depending on the activities being carried out.
- **Securities and derivatives:** Typically fall within financial services licensing and regulatory regimes.
- **Cryptocurrencies and cryptoassets:** May or may not fall within financial services or payment services/money services business regulatory licensing and compliance requirements, depending on the activities and jurisdictions involved.

Regulatory risk considerations as they relate to transactions:

- Depending on the activities of the blockchain network operator and/or participants, the relevant transactions may fall within the scope of legislative or regulatory requirements. In many jurisdictions, carrying on a regulated activity without a licence is a criminal offence.
- There is a current lack of regulatory clarity on digital assets and tokens. For instance, do they qualify as securities, derivatives, electronic money, or are they unregulated? This leads to potential regulatory re-characterisation risk as well as varied outcomes for taxation.
- There is a level of complexity involved in the reconciliation of internally held records with blockchain data. This may be particularly relevant if the transactions are regulated because there are specific regulatory requirements which apply to regulated entities on keeping accurate books and records. Blockchain technology is very useful to assess whether the data remains unchanged and valid but the possibility to lawfully store data on the blockchain to comply with legal or regulatory requirements (e.g. storage requirements) needs a case by case assessment.

- Different standards/prohibitions on data/information sharing may apply in relation to different products and this may conflict with the open/permissionless nature of some decentralised networks. For example, financial instruments which are traded on a regulated market or trading venues are subject to market abuse/manipulation laws, whereas non-financial products (e.g. goods and services) may not be.

4. Legal matters when establishing a blockchain network

What are the legal concerns when building and establishing a blockchain network?

It is important for blockchain network participants to consider a host of issues, including the legal structure, liability and governance model of a blockchain network and to clearly set out all rules, rights and obligations in legal documentation. Clear legal documentation is critical to ensure participants have clarity over the functioning of the blockchain network.

Clear legal documentation is critical to ensure participants have clarity over the functioning of the blockchain network.

Below are some considerations which blockchain network participants should have at the outset before embarking on their blockchain project:

Legal structure

- How will the blockchain network be structured from a legal perspective?
- Will the network sit within a legal entity, such as a company or partnership?
- Will there be one or more network operators?
- Who owns and controls the network and how is its ownership structured?
- How will participants join the network, and will they take an ownership stake?

Legal documentation

As mentioned above, clear legal documentation on all aspects of the blockchain network, e.g. the legal structure, liability and governance, is essential for clarity. Furthermore, it is important to ensure that the following is considered and covered within the scope of any blockchain network's legal documentation.

Example

Legal documentation should be established for the governance and terms of use of the blockchain network, the relationship between blockchain network participants, network operator and the users, limitation of liabilities, and ownership and use of IP.

- Will the blockchain network have a legally enforceable rulebook / terms of use which participants must sign up to? Are there civil law sanctions for breach of the rules?
- Alternatively, will each participant sign a separate contract with the network operator and/or network owners? Will this contract be separately negotiated such that every participant is subject to separate and distinct terms?
- What are the rights and obligations of participants? Will there be different classes of participants with different rights and obligations? If so, how does the network/network operator ensure fair treatment of different classes of participant?
- Is there a fee for participants to join the network and how is that structured?

- Will participants benefit from network revenues and, if so, how are payments to be structured?
- Are there anti-trust considerations and are there contractual (and other steps) that can be taken to mitigate these?
- Does the network utilise smart contracts and are these legally enforceable?
- Are there limitations of liability and indemnities? If so, who benefits? Are they enforceable in all relevant jurisdictions?
- How will the ownership/licensing and/or other intellectual property rights be dealt with?
- How should termination/exit rights be structured? What data should remain within the network on termination?
- How does the network protect confidentiality of its members, and what confidentiality provisions need to be included within the documentation?

Legal liability

- How will the liability of network participants be determined? Ideally, this should be determined at the outset and put down in the contract (if any) signed by network participants.
- What will be the criteria for factors being considered when assessing the apportionment of liability?

Governance

- What is the governance model of the blockchain network? For example, is it governed by the network operator, governed by a committee of participants, or governed by a staking/voting mechanism?
- Who is responsible for enforcing the rules of the network?
- Who is responsible for due diligence on participants?
- What is the necessary disaster recovery, business continuity, and contingency planning arrangements and who is responsible for executing them?

Outsourcing requirements

If outsourcing arrangements are contemplated, participants should ask themselves:

- Do the arrangements constitute an outsourcing, and is it necessary to enter into a service agreement?
- If a service agreement is applicable, is it entered into with the platform operator or each node/user on a back to back basis?
- Are there regulatory requirements that apply to the outsourcing?

Anti-trust law violation

There may be anti-trust risks arising from blockchain collaboration models (e.g. consortium) being viewed as:

- Abuse of dominance: pulling a significant share of the market into a closed ecosystem causing disadvantage to competitors and consumers.
- Disfavouring competitors, such as by excluding them, offering discounts to select partners, punishing competitors using alternative private currencies.

- Collusive conduct: fixing or manipulating prices to gain competitive advantage.
- Entering into collusion amongst significant members within a blockchain consortium leading to manipulation of services offered to smaller entities, preferential confirmation of transactions etc.

Anti-money laundering, KYC and sanctions

Blockchain network participants, particularly network operators, should consider the following risks and put in place appropriate systems and controls to mitigate them:

- Non-compliance with applicable AML/KYC regulations or sanctions requirements.
- Anonymity of transactions and identities on the blockchain.
- Lack of rigor in conducting "Know your supplier" checks.
- Payment to/from parties or countries on the sanctions list or with "politically exposed person" status.
- Deploying distributed applications that accept or transmit value without necessary controls and compliance programs.
- Lack of surveillance and monitoring activities to detect and prevent inappropriate activities'; or perform trend analysis of patterns that inform usage.

Blockchain network participants should also consider who should bear overall responsibility for AML/KYC functions.

Data protection and cybersecurity

Data protection and cybersecurity need to be considered carefully when designing a blockchain solution. The important questions to ask in this area include:

Though, strictly speaking, cybersecurity and data protection are separate areas of law, they are often grouped together as they both aim to safeguard (personal) data. Consequently, some of their key principles around implementing and maintaining a certain level of security, or addressing data breaches, overlap.

- How does one design a blockchain solution to be compliant with data protection laws?
- Can data protection be made an essential part of the core functionality of the supply chain, and how can one build a robust data protection compliance framework?
- Will personal data be processed? If so, what categories of personal data will be processed?
- Will the blockchain network fall into the territorial scope of a particular data privacy regulation, such as the GDPR or CCPA?
- What types of technologies can be used to meet data protection regulation requirements?
- How is the accuracy of data maintained? Can the data subject rights such as data access, correction, and erasure be satisfied when a data subject exercises one of such rights?
- What kind of potential vulnerabilities are there in the solution? What type of blockchain structure (public/private, permissionless/permissioned) offers the necessary level of security? Should security governance be fully decentralised or controlled by a select group?

There are a number of laws in place that govern cybersecurity, most notably the EU Network and Information Security directive (NIS Directive). This provides legal measures to boost the overall level of cybersecurity in the EU by ensuring, among other things, that 'operators of essential services' across sectors which are vital for the economy and society (e.g. banking, financial market infrastructures, and digital infrastructure) will have to take appropriate security measures and to notify serious cybersecurity incidents to the relevant national authority.

Intellectual property

IP considerations in a blockchain network will depend on the nature of the specific blockchain in question, including its purposes, relationship between the blockchain participants, the underlying software (e.g. open-source) and whether the underlying IP is intended to be commercialised. The importance of protecting IP comes as an extension of addressing trade secrets, confidential information and other proprietary rights potentially contained in the data shared on or linked to a blockchain. The following are core legal concerns and questions for blockchain network participants considerations and questions around IP in blockchains:

- Each type of IP (e.g. patents, trademarks, copyrights, trade secrets) has its own ownership rules (e.g. the work for hire doctrine in copy right which applies to certain jurisdictions). Parties will need to consider each type of IP right that would be created in respect of a supply-chain blockchain network. IP rights vary in each jurisdiction. Therefore, jurisdictional details need to be considered together with the governing law of the blockchain agreement (i.e. the agreement to access and use the blockchain infrastructure).
- It will be key to determine who owns the IP in the blockchain?
    - Depending on the structure of the blockchain, the IP in the blockchain can be the property of one or various parties (e.g. joint ownership, through this is not always straightforward and should be carefully considered within the context of the specific blockchain in question). For example, IP in the blockchain could be owned by the company behind the platform (or its shareholder/investor), the developer, the founding consortium members, the node operator, or the participants who contribute know-how and data in order to develop the platform. This assessment may become more complex when using open-source software built by communities of developers.
    - Where a consortia is involved in the development of a blockchain platform the ownership of IP rights (including foreground and background IP) as well as any associated licensing rights (and the accompanying parameters of such licence e.g. limited, worldwide, etc.) should be covered as part of the pre-consortium or consortium agreement, if applicable.
- It is necessary to consider how membership agreements will assign IP rights and license IP to blockchain network participants, or whether there is an implied license to blockchain users. As part of this, these must be considered: the terms of the licensing of IP to network participants, including what IP is licensed, whether licences are granted on an exclusive/non-exclusive basis, or whether they are granted on FRAND (fair, reasonable and non-discriminatory) terms?
- What is the value of the IP in the blockchain network and is any of the IP intended for commercialisation?
- How is access granted to intended parties? Is an escrow agreement an appropriate means of holding any source code in software, for instance? It is important to understand the contractual relationship and relevant implications (transfer pricing, model design).

- IP-related risks:
    - Lack of clarity on the most optimal IP management model for a blockchain consortium, if applicable (e.g. ownership by the leading participants, ownership by the developer, use of open source etc.).
    - Risk of suboptimal monetisation of IP created on the blockchain.
    - Risk of IP infringement within a consortium or by other consortia as some organisations are part of multiple consortia.
    - Risk of lack of control on how members and third parties can contribute/enhance a current IP due to shared accountability on blockchain.
    - Risk around non-compliance with underlying open source licence terms of blockchains that are based on, for example, the Ethereum or Bitcoin ledgers by software developers.
    - Risk around potential enhancement of open-source software, including possible criticisms when "open washing" (when proprietary software is portrayed as open source but in reality, key code contribution is held back from public repositories).
    - Complexities and uncertainties involved in complying with IP protection laws when the blockchain extends across multiple jurisdictions.
    - Risk around lack of support from the members in the IP development or maintenance lifecycle.
    - Uncertainty around IP sharing in the event of insolvency (e.g. Escrow account to hold the IP).
- Consider additional IP implications in more complicated blockchain structures that deal with IP rights of third parties for certain use cases (e.g. anti-counterfeiting, brand management, enforcement of IP rights).
- Another important question relates to whether the blockchain can be used to record ownership, use and remuneration of IP licensing/transactions.

Forming a network?

Alongside designing consortium governance in a way that is helpful to the success of a project, there are also some aspects of governance that are helpful to consider in order to avoid legal dispute. For further details on consortium governance considerations, refer to the modules on Consortium Formation and Consortium Governance.

Tax considerations

The blockchain network may be subject to taxation in many jurisdictions. Thoughtful analysis should be undertaken to make sure that the network understands where it is subject to taxes or other informational reporting. For further details on tax considerations, refer to the module on Tax Implications.

5. Understanding the jurisdictional issues of the network

What are the jurisdictional issues and considerations when using blockchain?

As alluded to in the sub-section, Jurisdiction, in focus area Common legal and regulatory issues with blockchain use to this module, in a decentralised environment, it may be difficult to identify the appropriate set of jurisdictional requirements that apply to a given blockchain platform. As nodes on a decentralised platform can be located anywhere in the world, networks often cross jurisdictional boundaries.

At the simplest level, every transaction could potentially fall under the jurisdiction(s) of the location of each and every node in the network. But this could result in the blockchain needing to be compliant with an unwieldy number of legal and regulatory regimes. Even in a permissioned network, a use case in the supply-chain arena will inevitably have cross-border elements, often involving conflicting laws in different jurisdictions.

While there are international regulations which seek to address conflicts of laws, such as the European Union's Rome I and Rome II Regulations and the United Nations Convention on the Use of Electronic Communications in International Contracts, interpretation of these texts for cross-border projects can be complex. In addition, regulatory regimes can be even less harmonised and different regulators take very different views on the territorial applicability of their local regulators in relation to cross-border business.

Example

Examples of different regional regulations that blockchain platforms might have to comply with include:

- The European Union's General Data Protection Regulation
- The California Consumer Privacy Act in the U.S.
- The Rome I and Rome II Regulations

Below consider some key jurisdictional challenges specific to blockchain and those that generally apply when engaging in e-commerce.

Decentralised digital identities

To see an explanation and more details on what a decentralised digital identity is, see the module Digital Identity.

The use of digital identity systems in global supply chains is inherently cross-border, which means parties operate in multiple jurisdictions. At present, national legal regimes take divergent approaches to legislating/regulating digital identity and not all countries have mechanisms for cross-border recognition of digital identity. When making use of decentralised digital identity systems (instead of centralised systems), and with the cross-border nature of international trade, several legal issues arise. For instance, which law will apply to determine the validity of a contract? Which data protection laws will the supply chain be caught by, and are there any localisation requirements? Decentralised systems, such as blockchain, can encourage the development of digital identity. However, where existing laws and regulations have been drafted to consider digital identity (e.g. the eIDAS regulations in the EU), they have tended to be drafted with a traditional view of data and digital identity – i.e. based on centralised, rather than decentralised systems. This means the regulations are not fully consistent with a decentralised system of digital identity, meaning that some legal and regulatory uncertainty remains as to the legal validity of decentralised digital identities.

Decentralised autonomous organisations (DAOs)

The legal status and liability attached to a DAO will depend on how each DAO is structured and the jurisdiction in which it is incorporated in. At a practical level, the DAOs "management" is conducted automatically, meaning that it may be difficult to decide who is responsible for the DAO if laws are broken or contracts are breached. This risk should be mitigated if the DAO is structured as a legal entity since registration as a corporation, partnership or other legal entity typically requires the appointment of directors/partners etc. who would be held to be responsible for the actions of the company. However, if the DAO is not structured as a legal entity and instead exists only as computer code, it is not clear who is responsible for the DAO. The extent of liability of the founders for breach of law or contract will depend on a fact-specific assessment and different jurisdictions will take differing approaches.

Contracts

As discussed previously, contracts can pose several complex jurisdictional issues which require careful consideration in relation to the relevant contractual relationships. The principles of contract law differ across jurisdictions and therefore identifying the appropriate governing law is essential. In the event a fraudulent or erroneous transaction is made, pinpointing its location within the blockchain could be challenging. The inclusion of an exclusive governing law and jurisdiction clause is therefore essential and should ensure that a customer has legal certainty as to the laws to be applied to determine the rights and obligations of the parties to the agreement and which courts will handle any disputes. However, even where the contract is clear as to governing law, some legal and regulatory requirements are drafted to have extra-territorial effect, regardless of the choice of law in the contract. It is imperative that the legal enforceability of a contract be carefully considered given the jurisdictional problems blockchain raises.

Note that this consideration is not unique to blockchain but relates to all digital contracts, including smart contracts.

Electronic signatures

There is no consistent approach on the enforceability of documents executed by way of electronic signatures around the world. It is important when conducting due diligence that electronic signatures are valid in the relevant jurisdictions in which the platform is operating.

Note that this consideration is not unique to blockchain but relates to all digital contracts, including smart contracts.

Legal formalities of digital contracts

In some jurisdictions, it may not be possible to replicate certain types of paper-based legal contracts (e.g. notarised contracts) digitally due to the legal formalities surrounding those types of contracts. For example, the concept of a bill of exchange under English law is a fundamentally paper-based concept and it may not be possible to comply with the legal formalities for creation of a bill of exchange if it is created in digital form.

Note that this consideration is not unique to blockchain but relates to all digital contracts, including smart contracts.

Other important jurisdictional considerations

- Where will the nodes reside and are there legal limitations on where they reside (e.g. if there are localisation requirements for data)?
- What is the applicable law; do entities need to be established in all jurisdictions?
- Cross-border data sharing: if one system covers 2 or more nations, it needs to be clear whose laws apply where and to what.
- Are there restrictions on participant type that can access the platform: e.g. legal entities vs natural persons; or wholesale customers vs retail customers?
- Cross risks and sharing data: There also need to be knowledge of how entities can legally exchange data between different countries. This includes compliance with personal data and national security regulation that could apply in one state but not another.
- Mutual recognition of blockchain solutions: Currently mutual recognition efforts are largely region or domain-specific.
- Depending on law, mutual recognition frameworks may allow parties to the contract to decide what constitutes a valid blockchain transaction.
- TTP Project of eGovernment focusses on mutual recognition mechanism for trusted transboundary electronic interaction and may provide a framework for cross-border recognition of blockchain transactions.[108]

There remains significant legal and regulatory uncertainty related to blockchain solutions especially across jurisdiction. Network operators and participants are responsible for assessing their own regulatory position and ensuring compliance. Ignorance is not a defence to legal and regulatory breaches.

6. Smart contracts

What are smart contracts? Are they the same as a legally binding contract?

As indicated above, smart contracts are not always or necessarily legal contracts, despite the use of the term "contract." In many cases, the term "smart contract" is used to describe self-executable code which interacts with data from a separate legally enforceable contract and automates processes based on that data. These non-legal smart contracts present questions on who is liable if there is an error in the code which causes one party loss.

However, smart contracts are capable of being legal contracts where they meet the requirements for a legal contract. As such, certain smart contracts are indeed legally binding and contain legally enforceable rights and obligations, albeit within a code-based format.

There are a wide range of legal considerations relating to these types of "legal" smart contract:

- Many jurisdictions impose legal formality requirements for a legally binding contract, and it is not clear that smart contracts will satisfy these.
- If smart contracts operate on a decentralised permissionless network, nodes may be located anywhere in the world. This may make it difficult to determine the applicable governing law and jurisdiction of the contract if the parties have not chosen a governing law.

- In many jurisdictions, a contract can only be valid if it is entered into by a person (i.e. a natural or legal person) and this may preclude some DAOs from entering into legally binding contracts unless they are structured as legal persons.
- Interpretation of smart contracts and dispute settlement may prove to be a challenge. Inclusion of an arbitration clause in the contract may be advisable as arbitral bodies (drawing on expertise from industry experts) may be more appropriate forums in which to interpret smart contracts in a dispute scenario than the courts.
- It may be difficult to attribute liability to either party to a smart contract where there is a failure of execution of the smart contract or partial execution due to a technical flaw or malfunction. In this case, the conditions under which the parties to the smart contract can act against the developer, i.e. liability is attributed to the developer, may need to be addressed.
- Should the contractual provisions provide the authority and ability to easily reverse transactions in the event of certain circumstances, for example mistaken transactions and in what circumstances should this authority be exercised? This is relevant given the immutability of the blockchain, which means that once executed, changes to the smart contract should be impossible.

Therefore, more attention than usual should be given to the following considerations in order to ensure the smart contract is a legally binding and enforceable contract:

- **Legal formalities:** Ensuring that the smart contract satisfies the legal formalities for a legal binding contract in the relevant jurisdiction.
- **Transparency:** Making the terms of a contract accessible, readable and easily interpretable by all the parties involved in the execution of a Smart Contract and dispute resolution bodies, such as arbitrators/courts.
- **Auditability:** Ensuring that the contracts can be exported in a form acceptable for financial or other audits required of participants.
- **Retrospective resolution:** Checking if there are sufficient mechanisms in local legal systems for disputing a contract that has already been executed. Ensuring that smart contracts include a dispute resolution provision to reduce uncertainty and provide for a mechanism in the event of a dispute.
- **Marginal judgement:** Designing a system that, where possible, includes a backstop for human judgement over whether a smart contract has been fulfilled, to reduce risk of over-cautious automated systems.

Key questions regarding smart contracts:

- How is a legally binding contract formed? Are those parameters met by a certain smart contract that participants in a blockchain network want to execute?
- What event(s) trigger the smart contract to perform automated tasks?
- How is breach defined? How are smart contracts enforced? What are the legal remedies available to smart contracts?
- What happens if the smart contract malfunctions, and who is liable?
- Automation might not fulfil due process required by regulators, such as financial and safety regulators. For example, smart contracts that self-execute may not meet local audit standards for due process. They also make it harder to attribute liability in the case of a dispute (is it the code developer?).

- Self-execution of smart contracts may also be difficult for clauses which require subjective assessment. In addition, contracts are interpreted based on laws and case law, meaning that automation may be difficult to achieve in certain cases of smart contracts.
- Legislation for digital processes: As legal systems respond to increasing digitisation of contracts and transactions, sometimes legislation and regulation fall behind. For example, digital signatures are not recognised in some national legal systems.
- Need the right to reject and amend smart contracts: Self-executing elements and forming smart contracts are particularly worth examining in detail. One of the clearest issues for any legal system is that any dispute of a smart contract will likely happen after the contract is executed. They will need to be reversible or require another mechanism, such as damages, for remedy after the fact.
- Risk of increased litigation from smart contracts: Automated systems miss the human intervention that allows 'substantial' rather than 'perfect' performance of a contracted deliverable. This means that some contracts that are essentially complete would be rejected by an automated system, whereas if they were judged by a human, they would be accepted. With increased rejections, there may be increased litigation to prove that a contract was substantially fulfilled.

Regulatory risk considerations relating to smart contracts

- Lack of audit of smart contracts leading to incorrect implementation of business or legal arrangements.
- Governance of smart contract: For regulated institutions, it is necessary that a governing body of the firm and responsible senior managers exercise sufficient oversight over the smart contracts and receive regular management information in relation to their performance.
- Risk of product design errors/failures leading to non-compliance with regulations governing data. For instance, does the solution involve sensitive freight data? Do the regulations permit on-chain storage of data or does it need to be stored off-chain?
- Risk of non-compliance to cybersecurity regulations and standards in the industry that the solution needs to comply with.

TOOLS AND RESOURCES

7. Starting point to identify legal and regulatory matters

This checklist is intended as a useful starting point of key legal and regulatory considerations for any blockchain project in the area of supply chains. It should help anyone considering a new blockchain project to quickly understand some of the common legal and regulatory hurdles that will need to be addressed.

The checklist is not intended as an exhaustive list of legal and regulatory issues and is no substitute for specific legal advice. The latter will need to be sought on a case-by-case basis for every project as legal and regulatory requirements will always be project-specific. However, this checklist is intended to help frame the key issues and it should be helpful as a starting point in the engagement process with legal counsel for any blockchain project in the area of supply chains.

For detailed considerations and questions, review the relevant sections in the considerations outlined in the previous compliance sub-sections.

General concerns

This checklist covers high-level compliance considerations relating to the use of blockchain:

- ☐ What are the applicable legal and regulatory regimes to the intended transactions on the blockchain network?
- ☐ How will you monitor and enforce regulatory compliance?
- ☐ How to address and mitigate risks relating to anti-trust, anti-money laundering (AML), and "know your customer" requirements (KYC), data protection and cybersecurity?
- ☐ How to update the governance when new regulations are identified, or new members are added to a consortium?
- ☐ How will compliance with the governance model of the blockchain network be enforced?
- ☐ How to ensure the enforceability of smart contracts?
- ☐ What are the applicable legal and regulatory regimes to the intended transactions on the blockchain platform/network?
- ☐ What are the audit rights of the participants?
- ☐ Who will enforce the governance models?
- ☐ Who will participate in the creation of governance model, bylaws, etc.?
- ☐ How will penalties be paid, and assessments made?
- ☐ What audit standards have been defined for the blockchain solution and its participants?

Industry/product risks

This checklist covers high-level legal and regulatory compliance considerations relating to industry/product risks when using blockchain:

- ☐ Are there regulatory licensing and/or compliance requirements that apply to the relevant industry and/or the relevant product that is to be transacted?
- ☐ Are there regulatory disclosure requirements that must be met by participants in that industry, or product-specific disclosure requirements that apply?
- ☐ Are there rules or regulations that cover market infrastructure relating to the relevant industry and/or products?
- ☐ Are different aspects of the platform treated differently from a regulatory perspective? For example, are some activities on the platform regulated while others would not be?

Jurisdiction risks

This checklist covers the high-level legal and regulatory compliance considerations relating to jurisdiction risks when using blockchain:

- ☐ What are the jurisdictions of the blockchain network operator (if any), the network participants and the target markets of the network participants?
- ☐ How would the local regulators in those jurisdictions characterise the activities of the network/network operator, the participants and the transactions taking place on the network?
- ☐ Do different licensing and regulatory standards apply in different jurisdictions and can these be complied with on a case-by-case basis or is it necessary to take a highest common denominator approach?
- ☐ Does the platform involve the transfer of cryptocurrencies or cryptoassets? There is a wide divergence on the regulatory status of cryptocurrencies and cryptoassets between jurisdictions and, therefore, it will be important to assess the regulatory obligations of a cross-border platform which involves the transfer of these types of asset.
- ☐ Does the transaction involve electronic signatures? There is a divergent approach on the enforceability of documents executed by way of electronic signatures, and it will be important to assess and determine that electronic signatures are valid in the relevant jurisdictions in which the platform is operating.
- ☐ Does the platform seek to digitise existing types of paper-based legal contracts that have special formality requirements? In some jurisdictions, it may not be possible to replicate certain types of paper-based legal contracts digitally.

MODULE

Tax Implications

Overview

Focus Areas

1. Tax considerations of blockchain solutions
2. Digital asset considerations

Tools and Resources

3. Blockchain transactions tax process

Overview

While tax implications are rarely included with early design and development, this toolkit encourages a broad-based approach so that no part of the business is an afterthought. Tax implications are best considered from the initial scoping and strategy phase of a blockchain implementation.

The purpose of this module is to educate the deployment managers and business, identify details, and address characteristics in order to properly apply various tax implications from blockchain usage across the globe. For specific tax liability calculations and compliance reporting requirements, consult with local tax specialists in the jurisdiction as tax laws may vary based on the specific facts and jurisdictions. Proper planning and tax research can reduce tax uncertainty, meet regulatory requirements, create efficiencies with respect to operations, and reduce overall tax burden.

FOCUS AREAS

1. Tax considerations of blockchain solutions

What are the most prevalent tax considerations that may arise from a blockchain solution?

This focus area aims to cover the more common tax considerations that may arise from blockchain solutions focusing on creating a tamper-resistant, traceable record of data distributed among multiple parties. Below are steps for solution owners to understand the potential tax implications that may arise from their solutions.

Identify the parties involved in the chain

Blockchain solutions will typically have multiple participants, including owners, users, and others. An important starting point in evaluating tax implications is identifying all participants and understanding how they interact with the solution.

Understanding the characteristics of the parties involved in detail will help identify the appropriate tax ramifications to the participants and the solution. For instance, the locations of the owners of the solution should be understood as local country tax considerations may apply. Additionally, the parties involved in the transactions can impact the tax classification of the transaction.

Consider the following questions:

- Who are the relevant stakeholders involved in the transactions?
- Where are the stakeholders located?
- What roles do they play within the solution?
- What are their unique tax requirements and how can they be enabled by the solution?

Sample participants who may be part of the blockchain network include:

- Blockchain network nodes
- Consortium members
- Employees
- End users
- Investors
- Supply-chain participants (e.g. third-party intermediaries, brokers)

Potential tax considerations that may arise based on the facts around the participants include:

- **U.S. owners of a non-U.S. operation:** If U.S. investors are owners of a non-U.S. entity operating the blockchain platform, an analysis into the overall ownership mix will be necessary to understand the tax impact to the investors. A similar implication may apply to investors from other jurisdictions.
- **Compensation:** If employees are compensated through the blockchain operations, withholding taxes and reporting obligations may be triggered. With appropriate tax planning, there may be different tax considerations such as automating the withholding process with appropriate calculations

and connecting payments with those liable as well as with regulators to which payments are due.

- **Domestic and cross-border withholding and reporting obligations:** Depending on where the participants are located and their activities in the jurisdictions, separate reporting obligations, withholding taxes, or indirect taxes like a Value Added Tax (VAT) or a Goods and Services Tax (GST) could be applicable.

For instance, the solution owners could ask questions such as:

- Does the manufacturer of the solution act as a node that verifies and records the transactions?
- Is the seller located in a jurisdiction that imposes VAT, and where are the goods being shipped to and from?

The solution owners may have to ask these questions to determine if there will be separate reporting obligations and indirect taxes that could be applicable.

Example

For a purchase order management related use case, value is transferred among participants involved in a blockchain network through the purchase and sale of goods between each of the participants. Participants in the solution often include producers, manufacturers, sellers, buyers, distributors, agents, and retailers spanning different jurisdictions. The solution owners will have to identify the specific roles of these participants and their locations to determine the proper tax ramifications.

Identify the value(s) generated

Inherent in blockchain solutions is the generation of new value. For instance, value enabled by blockchain may include data analytics, identity as a service (IDaaS), or report automation. Value can be tracked (e.g. tracking physical assets in a supply-chain) or generated (e.g. generating value in the form of efficiency, transparency, traceability, or integrity).

The new value generated often creates intellectual property (IP) linked to the blockchain technology. Facts around the IP, such as the location and the ownership of IP, will bring about tax considerations. The new value could also be captured through revenue generation or cost reduction for the entities associated with the technology. For instance, through the increased efficiency of the blockchain solution, there could be higher product margins. Considerations such as where and how the margins are attributed can also bring about tax implications.

As the value is created, captured, or transferred, solution stakeholders should consider the tax ramifications associated with the new value.

Consider the following questions:

- What is the business model? Does the solution generate revenue or fees directed towards an entity or multiple entities? Is there income realised and recognised?
- What is the value generated?
- Where is the value generated and attributed to?
- Who has ownership and control of the blockchain solution?
- Will the value be transferred to a different jurisdiction?
- Will the value be shared or split among different entities, as in a consortium?

Potential tax considerations that may arise associated with the value(s) generated include:

- **Legal entity structuring:** The value of the solution may be captured through revenue generation. Any revenue-generating solution will have to consider structuring its legal entities to mitigate unnecessary costs and allow for flexibility in future expansion plans. It is important to understand how each relevant jurisdiction will seek to tax any created intellectual property or value transferred.

- **Regulatory and informational reporting requirements:** Value may be captured in different jurisdictions depending on the specific operations of the solution. Depending on the business operations, there may be different types of informational reporting or withholding requirements to the regulatory bodies. Also see the module Financial Reporting and Controls.
- **Revenue and income sourcing:** Revenue and Income sourcing are based on a combination of factors. Proper analysis will be necessary to determine where the income-driving activities occur and ultimately where the income is sourced. Blockchain platforms might also provide flexibility into the revenue and income sourcing jurisdictions. Consider asking questions such as:

    a. Where is the intellectual property located?

    b. Where are the employees and users?

    c. Is there a license, patent, or copyright on the intellectual property?

    d. By which judicial authority is the license, patent, or copyright given?

    e. Do users pay royalty fees or subscription fees for the use of the licensed solution?

Also, consider that there may be a need for licensing or service agreements to clarify rights and responsibilities. In a supply chain, for instance, IP may be generated through value drivers such as increased transparency and traceability, faster settlements, fraud reduction, increased automation, and authenticating identity.

Potential steps to identify the tax considerations associated with the IP generated within the supply chain include:

1. Identifying the IP generated through the value drivers
2. Applying transfer pricing principles to attribute the IP generated to different points in the chain
3. Considering the appropriate jurisdictions to own and operate the IP
4. Re-forecasting transfer pricing
5. Overlaying the international tax considerations for new IP generated

Identify the opportunities and benefits of blockchain for tax

Blockchain technology solutions, such as supply-chain solutions, often record the transactions of physical assets on the blockchain. Blockchain technology's ability to securely track and store transaction level data can create opportunities for generating efficiency in tax compliance and reporting in multiple jurisdictions with different types of indirect and direct tax. Solution owners may see benefit through considering the ways blockchain deployments could incorporate streamlining tax into the solutions.

Consider the following questions:

- How can the transaction data captured be tax-sensitised?
- What are the transaction flows with tax considerations?
- Could the transaction flows provide data with increased accuracy for tax reporting and tax liability?
- Could some tax compliance tasks be automated?

> *Building out a blockchain solution involves significant technical considerations in architecture and design. Having a tax lens at the table during the design phase enables tax efficiencies in compliance processes, and a greater ability to gather tax sensitive data for use in compliance, planning and in support of a tax examination.*
>
> **Rob Massey,** Partner and Global Tax Leader – Blockchain and Cryptocurrency, Deloitte Tax LLP

Tax-sensitised data

Tax-sensitised data incorporates relevant tax compliance, reporting, and planning considerations for increased tax efficiency. Figure 13.1 depicts a diagram with steps. Deployment owners should:

1. Analyse where in the transaction flow data relevant to tax will be captured
2. Build mechanisms to extract the data
3. Capture the relevant data)

Potential considerations for tax efficiency that the solution owners may consider include:

- **Indirect tax tracking:** The process for calculating indirect taxes is often driven by manual efforts prone to inefficiency and error. A blockchain-based system of recording indirect taxes and automating payments to regulators may help save costs and time for parties involved in the blockchain ecosystem as well as for authorities.
- **FDII Substantiation:** A lower effective U.S. tax rate is provided with respect to a domestic corporation's foreign-derived intangible income (FDII), which includes certain qualifying transactions like sales of property to foreign persons for foreign use and the provision of services to persons or with respect to property located outside the United States. Understanding the transaction flows and tracking transaction data through blockchain can help determine whether a transaction constitutes an FDII-qualifying transaction, establish appropriate documentation required for FDII substantiation, and, if applicable, provide data for the computation of FDII.
- **Automating Manual Processes:** Organisations will often have processes that have rules and parameters required for tax compliance and regulatory purposes. Consider building in tax sensitivities to the transaction level data and integrating with tax compliance tasks to streamline efficiency and enhance quality. Also consider smart contract protocols to automate manual processes and large volumes of data.

The below figure depicts steps to consider when tax sensitising the transaction level data in a supply chain and the potential increased benefits achieved through the process.

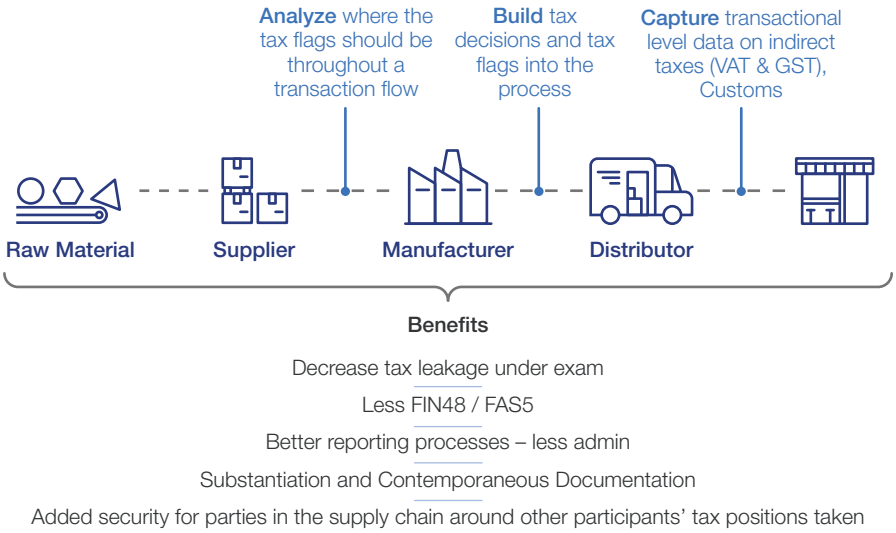


Figure 13.1: Steps to consider when tax sensitising transaction-level data with potential benefits

Example

Implementing processes to capture the relevant data for tax processes, such as VAT or GST, and embedding this data into the supply chain solution may drive efficiency and cost-savings, especially as the supply chain solution begins to scale and launch into full production with multiple users and thousands of transactions. Blockchain technology provides the ability for transaction level data in a supply chain (e.g. flowing from raw materials to the manufacturers, sellers, distributors, retailers, and to the consumers) to be captured in an immutable and traceable organised manner that can easily be retrieved.

2. Digital asset considerations

What are the most prevalent tax considerations that may arise from a blockchain solution?

This focus area covers blockchain use cases utilising digital assets. With relatively little guidance from the taxing authorities and with inconsistent tax rules on digital assets among various jurisdictions, the tax implications around digital assets are often complex. The tax considerations start with understanding and determining the nature of the digital asset for tax purposes.

Blockchain is often considered to be the underlying technology behind creating the "Internet of Value", where monetary value could be transferred freely just as information is transferred with the internet we have today. The prospect of the "Internet of Value" is made possible due to blockchain's ability to create, store, and transfer digital representations of assets in a secure, immutable, and efficient manner.

Whatever is being transacted within the solution is a key factor in determining the tax classification and implications of the transactions on the blockchain. The digital asset may be a virtual currency or virtual representation of cash, physical assets, securities, income, or other benefits. This variable can create additional complexities as well as potential opportunities. It will be important to apply a tax lens to analyse how the digital asset is used across the solution as the tax analysis may differ from the analysis for accounting, legal, and/or regulatory purposes. Moreover, the tax analysis may differ across tax type (i.e. direct tax versus indirect tax) or in one jurisdiction versus another.

The specific details surrounding the digital asset will matter in classifying the nature of the digital asset for tax purposes. Some questions to consider include:

- How are the digital assets being used and what is the underlying value represented? Are they used as payments, compensation, securities, commodities, and so on?
- Do the digital assets have readily convertible values?
- Where and who are the parties transacting with the digital assets?
- Are the digital assets operated in a closed-looped system or are they open for third parties to access?
- In what entity type and jurisdiction will the development and transfer of digital assets be conducted?

Potential tax implications and considerations associated with digital assets include:

- **Basis tracking:** If the digital asset is representing property, the transaction could be considered a barter exchange and trigger gain or loss at the time of the transaction – an additional consideration compared to transacting in cash. Designing basis tracking into the blockchain solution would be necessary to compute gain and loss to provide to all the parties participating in the transaction with the information needed for their own reporting purposes.

- **Inventory methods:** The analysis into the nature of the digital asset combined with the blockchain's ability to record information in an accurate, real-time, and reliable manner may give more flexibility and efficiency around choosing the inventory methods to record the transactions. For instance, specific identification methods may become possible where before FIFO (First In, First Out) or LIFO (Last in, Last Out) were the only acceptable methods available.
- **Indirect tax & withholding requirements:** If the digital asset is considered property, there could be withholding requirements and indirect tax considerations on the purchase or sale of the digital asset.

TOOLS AND RESOURCES

3. Blockchain transactions tax process

The following figure depicts a high-level framework for thinking about tax in all blockchain solutions. Owners should work with their tax specialists to identify the tax implications specific to the developed solution and relevant jurisdictions.

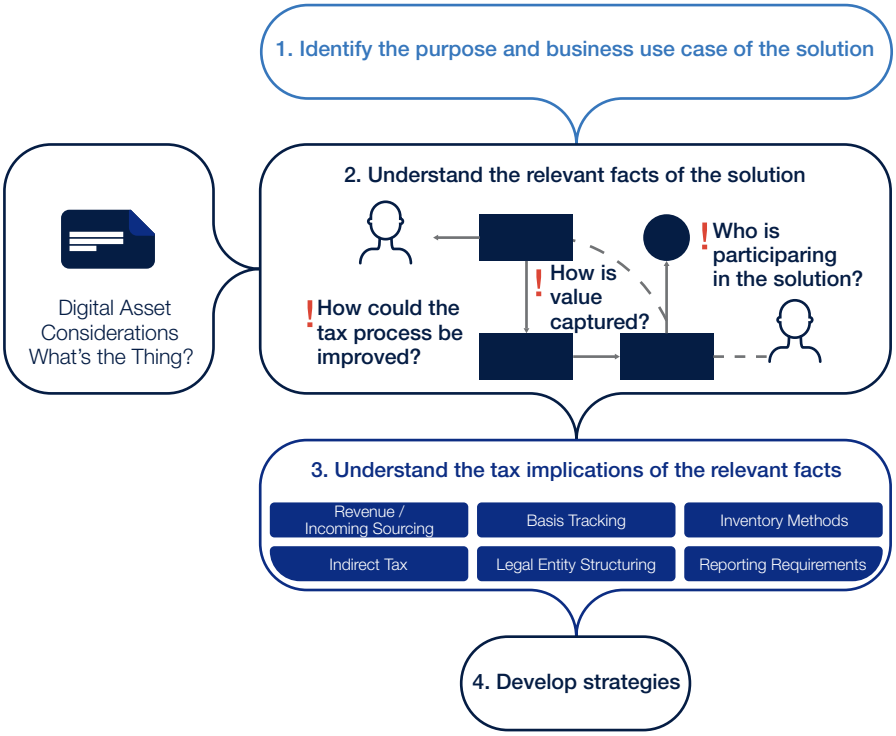


Figure 13.2: Overview of key steps to understanding tax implications

Process:

1. **Identify the purpose and business use case of the solution:** Having a clear idea on the purpose and the business use case of the blockchain solution will help identify tax treatment and potential tax liabilities.
2. **Understand the relevant facts of the solution:** Tax is driven by the detailed facts surrounding the business use case. Small changes in the details could lead to completely different tax consequences. For instance, is there a contract in place with the users of the solution? Is there a lease or full transfer of custodial rights? Is the user paying royalty or subscription fees for the use of the solution?
3. **Understand the tax implications of the relevant facts:** Each fact will lead to different tax implications. The above graphic highlights some of the key tax issues arising in blockchain deployments. However, as tax rules are complex, there could be many other tax implications to consider. Therefore, the need to consult with a tax specialist for each solution before concluding the possible tax results.
4. **Develop strategies:** Could unintended tax consequences be mitigated? What are the risks? Are there opportunities for efficiencies? Consider the strategies to drive not only decisions around tax but decisions around the overall business solution.

MODULE

Financial Reporting and Controls

Overview

Focus Areas

1. Relevance of financial reporting

Tools and Resources

2. Design and deployment considerations

Overview

Any blockchain solution designed and deployed for a supply-chain business network should consider the requirements of participants' financial reporting, internal controls, as well as their stakeholders - for any business case to be successfully addressed. When combined with more traditional forms of business bookkeeping, blockchain information can help companies support the preparation of timely and reliable financial statements.

It is important to address the many challenges that may exist when an organisation relies on information obtained from a blockchain and the underlying technology as part of its financial reporting process and system of internal control. Not all of the relevant controls operate within the company's legal structure or in a verifiably reliable environment; these challenges are amplified as most companies' professionals have limited experience using blockchains and may not recognise potential implications to financial reporting activities.

FOCUS AREAS

1. Relevance of financial reporting

When and to whom are considerations for the financial reporting process and financial statement audit during blockchain deployment relevant?

Relevance: Who and when

This topic is relevant to the organisation's managers and leaders responsible for financial reporting (including CFO, CAO, board of directors, audit committee), external auditors, internal auditors, regulators, IT/cryptography/ cyber security personnel, advisors and other third-party service providers, and relevant end-users. This topic is relevant during the design phase and then revisited along the way during deployment.

It is imperative to engage all relevant stakeholders with requisite expertise early. While financial reporting and audit considerations and their implications aren't typically what project managers or deployment managers primarily get involved with, this toolkit encourages a holistic approach. The implications to the financial reporting process should not be an afterthought, rather they should be among the considerations set right from the initial scoping and strategy phase of blockchain implementation.

> *Start with considering if there's an appropriate blockchain use case for a particular organisation and then get the right people in the room at the very beginning. The discussion is not just in the IT department; others such as accounting, audit, even the audit committee, should know what's involved. Have the dialogue up front because blockchain adoption is going to have such a profound impact on all the parties in financial reporting.*
>
> **Amy Steele,** Partner, Deloitte & Touche LLP

The importance of financial reporting considerations

Any design and deployment of a blockchain supply chain solution should consider management's responsibility for the financial reporting process (maintaining books and records, establishing a system of internal control and producing financial statements). Blockchain deployment may impact financial reporting in various ways depending on the use case. For example, settling transactions with digital assets or relying on data exchange on a blockchain to support an accounting estimate. This is true regardless of whether a blockchain is used to fundamentally change how transactions are settled or simply increase information transparency; a careful assessment of the supply chain design can identify unique considerations or necessary changes to management's financial reporting process (including a system of internal control). Management's assessment may also identify unique risks and forms of evidence that an external auditor may consider having an effect on their ability to conduct an audit of the financial statements under professional standards.

External auditor engagement

An external auditor is typically engaged to perform an audit or assurance engagement under the standards issued by an authoritative body such as the International Auditing and Assurance Standards Board and other bodies in specific countries such as the American Institute of Certified Public Accountants in the US. Examples of audit and assurance engagements are a financial statement audit, a sustainability assurance engagement, and an assurance engagement on compliance with laws and regulations.

Nevertheless, by designing a blockchain solution well, management's financial reporting process may benefit from a reliable blockchain to help automate activities such as reconciliation with counterparties in use cases for trade finance, product tracking, or payments to transportation providers.

It is important to establish what the accounting treatment will be for blockchain-based transactions before the system's recordkeeping and data-collection requirements are finalised. This starts with management understanding any relevant guidance and consulting with experts. It may also be a good idea to then engage regulators regarding the proposed accounting as the accounting treatment can be complex and will have a significant influence on how the systems are designed and what data needs to be collected.

It is important to work with internal and external auditors, along with relevant stakeholders, to determine what aspects (e.g. management's risk assessment process, system internal control) may be impacted by a blockchain-based supply chain and avoid potential pitfalls or deficiencies in the design of the supply chain before it goes into production. This will also help the auditor understand the risks, identify the need for specialists, determine the impact on audit scope, and consider the use of specialised audit tools.

TOOLS AND RESOURCES

2. Design and deployment considerations

The following figure lists key design and deployment considerations for individuals involved in the financial reporting process. It is illustrative only and not all-inclusive but can be a helpful guide as an agenda of meetings or aid as a conversation tool among various stakeholders concerned with financial reporting and financial statement audits; significant regulatory, technological and professional hurdles may remain before management determines blockchain solutions are appropriate to incorporate within the financial reporting process and ready when the solution scales up.

These considerations can help identify issues to address during the design phase, but they also can help determine areas of potential risks in the financial statements that will be further assessed by management for their system of internal control and the external auditor for audit procedures.

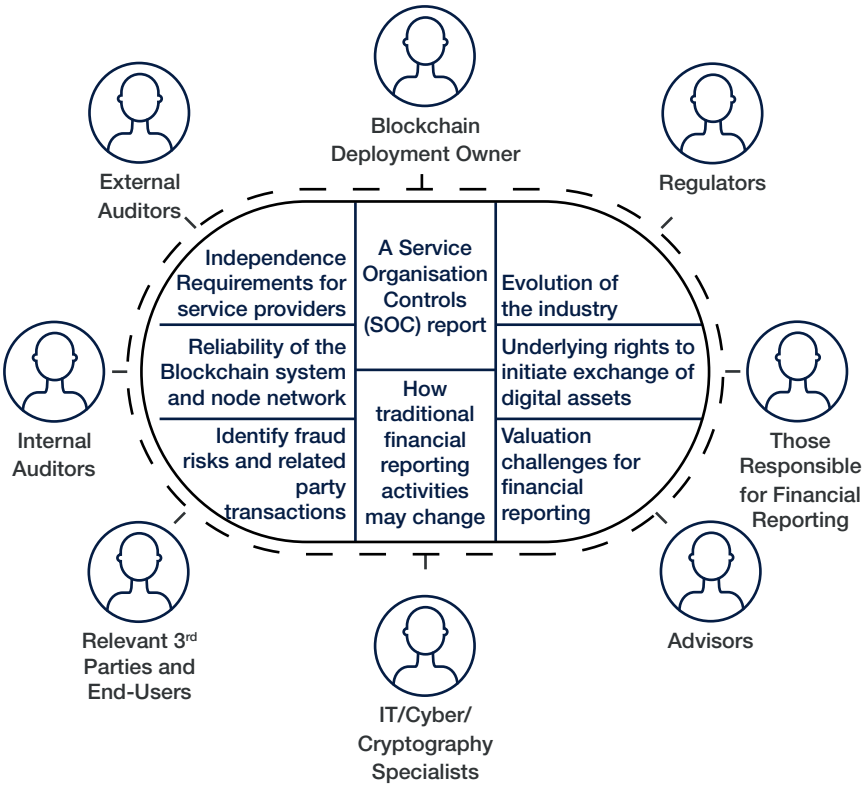


Figure 14.1 – Relevant stakeholders and considerations for assessing financial reporting

Reliability of the blockchain system and node network

The reliability of a blockchain system is foundational for the trusted recording and immutability of data (including digital assets) recorded to the blockchain. When speaking about reliability, it is important to recognise that management is responsible for the design and operation of the blockchain, including the system of internal control.

Controls over the blockchain system will come from numerous sources (as summarised below) at all technology layers – node network, services, and application layers, etc - but will typically be consolidated at the organisation or other entity managing the permissioned blockchain (see Figure 14.2). Consider whether management and auditors will need access to the nodes or customised nodes to perform activities and procedures for internal controls.

These controls, including those in a shared system of internal control, will typically fall into the following categories:

- Internal controls at the organisation node level in particular logical access controls, and data entry validation and approval, including private key management
- Internal controls at the entity managing the permissioned blockchain, in particular, controls over how blockchain participant nodes are added or removed, the reliability of the "oracle" that provide off-chain data, and controls over monitoring the health/safety of the blockchain
- Internal controls inherent to the blockchain technology itself (e.g. consensus mechanism), including cryptography
- General information technology controls (GITC) supporting the nodes at the master node (blockchain network operator) and participating node levels (blockchain business network participants), including smart contracts

> *When deploying a blockchain solution, a company will need to assess the risks and adequacy of controls over all aspects of the blockchain solution, not just the technology they are implementing internally to participate in the blockchain. This might include risks associated with the blockchain ledger system, or how the blockchain network operator performs its responsibilities. That assessment of third party risk should drive how the company responds when designing its own controls to ensure those risks are mitigated.*
>
> **Tim Davis,** Principal, Deloitte & Touche LLP

Management will typically need to identify and evaluate Service Organisation Controls (SOC) reports (e.g. ISAE 3402, SOC1) as part of their evaluation of internal controls over financial reporting because there are typically numerous third parties within a shared system of internal control who are responsible for the controls discussed above. For example, a global supply chain system (blockchain network operator) that utilises a cloud service provider may need to provide its users with a SOC report that encompasses the evaluation of controls at the cloud service provider and others within the technology solution stack.

As the external auditor considers internal controls, they will need to evaluate controls over the blockchain system itself as well as the controls over the implementation at the organisation node level to which they are the external auditor. The external auditor will typically need to test internal controls relevant to certain risks when auditing blockchain solutions in the context of a financial statement audit. This is because the substantive evidence alone may not be sufficient to address the certain risks when a blockchain solution is relevant to financial reporting.

A Service Organisation Controls (SOC) report

The data maintained in permissioned blockchains (those likely to be deployed for supply chain business networks) are highly dependent on controls that are either inherent to the operation of the blockchain digital ledger or dependent on the administration by the blockchain node network operator and the technology infrastructure it is based on. As such, a company's management (and their external auditors) will look for evidence that those controls are designed and operating effectively and that is typically satisfied via the transmission of Service Organisation Controls (SOC) reports.

Managers of each participant's financial reporting process typically consider the relevant controls of a service organisation as a component of their system of internal control. In this example (see Figure 14.2), an assurance engagement is conducted together or separately for each layer of the stack, and their report is transmitted to management (and subsequently to their auditor) of the blockchain business network participant.

In Scenario 1, separate auditors perform their audit procedures for each layer of the stack and each SOC report will include Complimentary User Entity Controls (CUECs) that the management of the layer above needs to consider in the design of its controls.

In Scenario 2, a single auditor performs their procedures for each layer of the stack and incorporates their results in a single SOC report (also includes CUECs). This would typically be the scenario if the blockchain network operator runs the master node from its own on-premise technology.

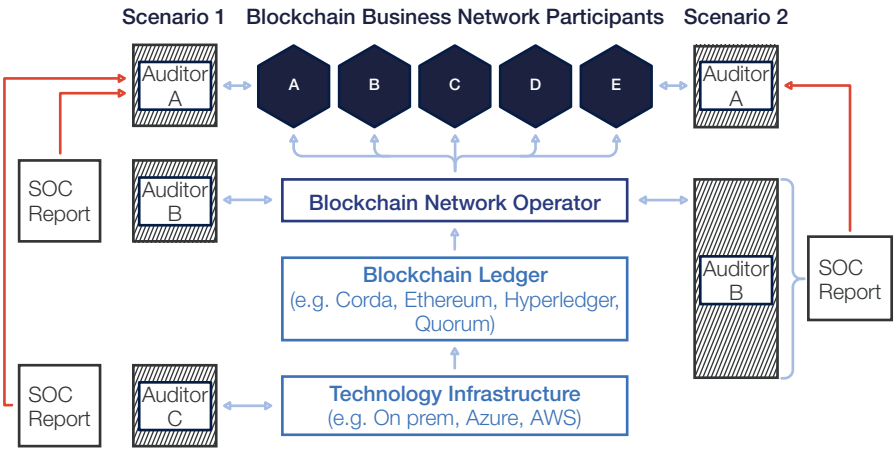


Figure 14.2 – Separate auditors or a single auditor audits each layer of the technology stack and summarises it in an SOC Report for the auditor of the blockchain node network participant

Underlying rights to initiate exchange of digital assets

It may be challenging to understand the underlying rights and obligations associated with blockchain solution. This relates to the form of access to the blockchain - to initiate data exchange (information sharing) or convey ownership or partial ownership of a digital asset (i.e., cryptocurrency).

For supply chain use cases that involve digital assets (e.g. transaction settlement for shipments received), access may require the use of a private key. The control or knowledge of private key material is a strong indicator of ownership (who has the rights to convey ownership) for the associated digital asset. Consider how private key management will be designed and the tools that may be necessary for management to govern the control or knowledge of their private keys as part of their system of internal control. Also, consider how management may demonstrate control or knowledge of their private keys in the context of a financial statement audit without revealing the contents of the private key.

How traditional financial reporting activities may change

Some traditional financial reporting activities may be changed or replaced in a blockchain based system. For example, management may need to design procedures and tools to enable a reconciliation – which may include a reconciliation of monetary value – between blockchain records and the company's internal books and records. Consider if the company's management and personnel have the right technology to effectively interface between a blockchain and their legacy accounting systems. Also consider if they have the technical expertise to design and perform the controls for a reconciliation as well as other necessary accounting and financial reporting activities.

In the context of the financial statement audit,[109] consider if the external auditor also has the blockchain tools and expertise to conduct an effective audit considering evidence that may be obtained from both on-chain and off-chain sources.

Evolution of the industry

Markets will naturally change as blockchain-based systems are adopted across industries, enable new products and services, and new customer behaviours. As this change occurs, legal and regulatory frameworks will evolve. Consider how management can monitor the changes in rules and guidelines to ensure their organisation remains compliant.

Valuation challenges for financial reporting

The quantity and characteristics of the monetary value of a transaction or balance at a point in time may be represented on the blockchain where a fair value model may be applied through the code logic of a smart contract. Consider that inputs for the fair value model may come from another blockchain supply-chain business network for interoperability or an off-chain source (i.e. oracle). These inputs, in addition to the smart contract, may come from a shared system of internal control that management will need to rely upon. Also, consider if the supply-chain business network has agreed upon the attributes that contribute to value creation in transactions recorded to the blockchain. These attributes may include product location, status of transport and quality of finished product, for which management's internal controls and the external auditor's procedures will need to be designed.

Identify fraud risks and related party transactions

Blockchain adoption may facilitate new and unforeseen business models, legal structures, contract terms, transaction flows, and relationships. Within this new ecosystem, consider how management will be able to identify and monitor related-party transactions. Additionally, new or modified fraud risks in financial reporting have the potential to emerge and should be considered for management's design of fraud prevention and detection controls.

Independence requirements for service providers

A professional requirement for external auditors, and their affiliates, is to remain independent from their audit clients. Blockchain ecosystems add complexity to the assessment of auditor independence. Management and external auditors should be aware of the planned roles of entities in the blockchain ecosystem (for all technology layers – blockchain, node network, services and application layers) and evaluate whether the external auditor or its affiliates have provided prohibited non-audit services related to the blockchain ecosystems to other participants that could impact the external auditor's independence with respect to its audit client. Consider the nature and scope of services provided by external auditors who may be obligated to remain independent of more participants in the ecosystem.

MODULE

Risk Factors

Overview

Focus Areas

1. Identifying blockchain-related risks

Tools and Resources

2. Risk identification checklist

Overview

New technologies carry potential downsides that need to be identified and managed. This is especially true when that technology is not merely an overlaying application but rather a core part of the organisation's underlying IT infrastructure, as is often the case with blockchain.

The checklist included in this module covers some common potential risks and missteps associated with the deployment of blockchain technologies. Note, however, that this list is not meant to be exhaustive. With that in mind, project managers should view the information as generic guidance and work with relevant internal stakeholders, such as cybersecurity, internal audit, finance, compliance, legal, operations, and information technology teams to identify and prioritise risks that are significant for their deployment and develop mechanisms to manage the risks proactively.

FOCUS AREAS

1. Identifying blockchain-related risks

What are the new risks associated with blockchain solution deployment?

As the organisation considers developing blockchain use cases, building proofs of concept, or scaling and deploying them in a production environment, the focus should not be diluted from catering for critical blockchain-related risks. Also, it is important to study if the organisation's enterprise risk framework account for blockchain-specific risks.

Organisations should adopt a proactive approach in recognising new risks stemming from blockchain. Risk management should not be an afterthought; rather, it should be baked into the consideration set from the initial scoping and strategy phase of a blockchain project itself. While this list of potential risks might seem rather long and daunting, many of those pitfalls are ones your organisation is likely to face in the implementation of any other new technology as well. This checklist is designed to help organisations identify those risks that are significant for them to manage in order to drive the success of their blockchain initiative.

With a richer, more collective, and nuanced understanding of the opportunities and risks of blockchain, decision-makers will be better equipped to deploy systems that support their business needs while engendering trust.

> *No technology, including blockchain, is without risk. The long-term winners in the blockchain space know how to recognise the risk, quantify the risk, and manage the risk in a blockchain-based application.*
>
> **Michael Prokop,** Blockchain Leader, Deloitte US Risk & Financial Advisory

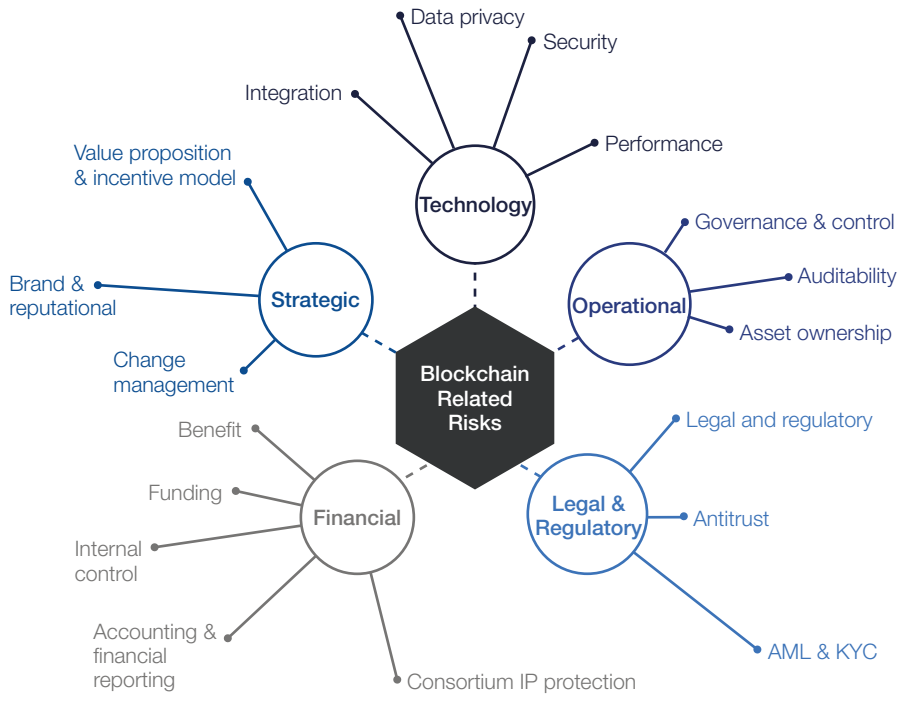


Figure 15.1 — The common risks can be sorted into five broad categories

2. Risk identification checklist

Following is a checklist of potential risks and missteps often associated with blockchain deployments. While all blockchain use cases may not involve digital assets, this checklist also outlines risks pertaining to use cases that involve digital assets. Note that this list includes some of the prominent risks but is not meant to be exhaustive. The checklist items are neither ranked in order of priority nor equally weighted. The probability of risks manifesting into actual events are dependent on a range of factors.

Organisations should treat this checklist as generic guidance, and work with relevant internal stakeholders to identify, prioritise, and manage the risks relevant for their particular project proactively. The scope of this module doesn't include guidance on enterprise risk management programs.

Also note that some of the specific risks mentioned below – for instance, Cybersecurity – are covered in greater detail in other modules in this toolkit. Be sure to refer to the modules dedicated to those particular issues as required by the needs of your project.

Technology risks

Effective development and deployment of blockchain-based solutions require the identification and addressing of a list of technological risks and challenges. The list includes privacy of data and transactions on the blockchain, security risks, performance-related limitations of the underlying blockchain platform, and integration-related issues with other enterprise systems.

Data privacy risks

- ☐ Could flaws in the blockchain-based system design lead to non-compliance with regulations or confidentiality agreements governing data? For instance, does the application involve personally identifiable information (PII) or confidential freight data? Do the requirements permit on-chain storage of data, or does it need to be stored off-chain?
- ☐ Does the application incorporate appropriate controls across the data lifecycle (e.g. collection/creation, storage, usage, and sharing/transfer as data is shared across the blockchain nodes)?
- ☐ Is there a risk of exposure of sensitive data due to inadequate policies, procedures, standards and guidelines for data encryption and obfuscation?
- ☐ Could incoming data potentially be inaccurate? If so, how to identify and correct errors?
- ☐ Is the blockchain system required to comply with "right to be forgotten" regulations? If so, is it in conflict with potential immutability of data on a blockchain?

For a detailed overview on protecting sensitive data and GDPR considerations, refer to the modules Data Protection and Personal Data Handling.

Performance-related risks

- What are the performance-related limitations of the underlying blockchain platform relative to the proposed blockchain use case (e.g. transaction throughput, settlement time, and availability)?
- Could the blockchain platform being used be suboptimal in terms of developer support and/or vendor lock-in?
- Is the selected blockchain protocol interoperable with other protocols required by the project?

For further details on blockchain protocol interoperability with other protocols, see the module Interoperability.

Security risks

Like other technology-enabled system, blockchain systems also need to be assessed for a variety of cyber security risks, such as confidentiality of users, security of private keys that secure access to digital assets, and endpoint protection. For further details on security risks, see the module Cybersecurity.

Integration-related risks

- Will there be integration issues with any mission-critical legacy systems used within the organisation?
- Are there standards available for integration of blockchain applications with enterprise systems?
- Is there appropriate integration testing at both the participating entities and the blockchain consortium entity?
- Could lack of common data architecture and data directory lead to enterprise systems feeding misaligned data to the blockchain system?

Operational risks

Implementation of blockchain-based applications, especially in a consortium of several organisations, is complex and involves addressing a number of operational risk issues such as governance, controls, auditability of blockchain transactions, and proof of assets ownership.

Governance and controls risks

- Is the legal entity structure of the blockchain consortium appropriate for tax implications and benefits of the participants?
- Could decision making within a consortium be suboptimal due to lack of proper structure and processes?
- Are there appropriate controls to mitigate conflicts stemming from decentralised accountability and shared ownership?
- Is there a lack of structure and policy in the consortium to onboard new members and accept new use cases?
- Have the smart contracts been audited to avoid incorrect implementation of business or legal arrangements?

For details on important governance items to consider, see the modules Consortium Formation and Consortium Governance.

Auditability Risks

- Is there enough technical experience or capability in conducting IT/ technology audit of the blockchain application or platform?
- Will management and/or auditors be able to obtain information required to support financial statement disclosures?
- Will management be able to value digital assets in accordance with relevant accounting policies?
- Is there risk of a "hard fork" of the blockchain to modify past transactions, allow previously disallowed transactions, or bring about other structural changes to the blockchain?

Asset ownership risks

- Is there a risk of theft or loss of digital assets because of the irreversible nature of transactions in the blockchain protocol?
- How is the real-world change of ownership of assets made consistent with the change reflected on-chain?
- Can real-world identity be adequately confirmed to establish ownership of assets when required? Is there additional complexity due to the potential anonymity of participants on the blockchain protocol?
- Are adequate industry standards available for designing interoperable blockchain-based tokens?

For more detailed information on the questions covered in this section, see the module Financial Reporting and Controls.

Legal and regulatory risks

Blockchain as a technology may not be regulated, but applications built using blockchain technology will need to adhere to relevant regulations, such as the European Union's General Data Protection Regulation (GDPR) relating to data protection and privacy. Legal and regulatory risks include uncertainty around cross-jurisdictional regulations, anti-trust violations, smart contract enforceability, anti-money laundering (AML) and know-your-customer (KYC), and intellectual property (IP) protection.

Legal and regulatory risks

- What are potential legal and regulatory risks and challenges to be anticipated with the deployment of this blockchain-based application? These may include uncertainty around cross-jurisdictional regulations, antitrust violations, smart contract enforceability, anti-money laundering (AML) and know-your-customer (KYC), and intellectual property (IP) protection.
- Could there be legal conflicts between consortium participants or consumers due to unclear legal liability in a permissioned network for cases such as data breach or smart contract errors?
- Is there risk stemming from regulatory uncertainties related to blockchains and related systems, especially across jurisdictions? Different data privacy and security regulations may apply in different jurisdictions around the world, for example.

For more details on important items to consider, see the module Legal and Regulatory Compliance.

Antitrust risks

- Are there safeguards against a blockchain consortium fixing or manipulating prices to gain competitive advantage?
- Could significant members within a blockchain consortium collude, leading to manipulation of services offered to smaller entities or preferential treatment of certain transactions?
- Are there antitrust risks arising from a certain blockchain consortium potentially pulling a significant share of the market into a closed ecosystem, thus causing disadvantage to competitors and consumers?
- Could a large blockchain consortium disfavour competitors, such as by excluding them, offering discounts to selected partners, or punishing competitors using alternative private currencies?

AML and KYC risks

- Is the blockchain system subject to compliance for AML or KYC regulations governing money service businesses?
- Are rigorous "know-your-supplier" checks required for compliance?
- Are there safeguards against payment being made to or from parties or countries subject to international sanctions, or with "politically exposed person" status?
- Could decentralised applications (Dapps) be deployed that accept or transmit value without necessary controls and compliance programs?
- Are requisite surveillance and monitoring controls implemented to detect and prevent money laundering activities?
- Are there additional risks due to anonymity of transactions and identities on the blockchain?

For more details on the legal and regulatory risks highlighted in this section, see the module Legal and Regulatory Compliance. More details on IP within consortia are available in the module Consortium Governance.

Financial risks

A common aim of blockchain deployment is to facilitate transfers of value. A variety of financial risks need to be considered while designing such blockchain applications, platforms, and infrastructure, such as potential for financial loss, transaction settlement finality, consortium funding-related risks, and intellectual property protection issues. In addition, there are a number of accounting and reporting challenges that should be considered when depending on blockchain-based applications for financial transactions and for information used in financial reporting.

Funding related risks

- Could funds run short to operate the consortium due to inappropriate choice of funding model? Will an initial coin offering (ICO), member fee structure, equity funding among partners, government grants, or some other funding source be used?
- Does the funding model of the consortium clearly define which participating entity will fund what?

Benefit related risks

- ☐ Has a revenue and other benefits sharing model been defined amongst entities of the blockchain consortium?
- ☐ Might participants be subject to financial loss due to absence of a trusted intermediary in blockchain-based business models to remedy errors or revert transactions? Could an alternative method of resolving disputes be created?

Internal control risks

- ☐ Is there a risk of financial loss due to the absence of a trusted intermediary in blockchain-based business models to remedy errors or revert transactions?
- ☐ Is there risk of financial loss due to incorrect representation of commercial contracts in the smart contract code?

Accounting and financial reporting risks

- ☐ If digital assets (e.g. cryptocurrency tokens) are used to transact in the blockchain system, is there a risk of incorrect accounting due to lack of standard guidance on accounting for digital assets?
- ☐ Is there a risk of misinterpretation of existing accounting literature while accounting for digital asset transactions?
- ☐ Could underlying rights and obligations associated with digital assets be potentially misunderstood?
- ☐ When the use case involves digital assets, is technical experience available to determine the fair value of digital assets?
- ☐ Is technical experience available to perform traditional financial reporting activities (e.g. complexity involved in reconciliation of internally held records with blockchain data)?
- ☐ Is there a risk of noncompliance due to continuing evolution of market and industry and changing requirements from regulators and standard setters?
- ☐ Is the management equipped to mitigate new and unforeseen forms of related party transactions or fraud schemes in financial reporting?
- ☐ Is there a mechanism to assess the beneficiaries of services provided by third parties who are obligated to remain objective of one or more entities of the blockchain network?
- ☐ Can unreliability of blockchain systems render blockchain data and digital assets inaccessible?

More details on the requirements of participants' financial reporting as well as their external auditors in the module Financial Reporting and Controls.

Consortium intellectual property protection risks

- Does the blockchain consortium have an appropriate intellectual property (IP) management model? For instance, IP may be owned by the lead members, by a separate consortium legal entity, or be provided under open source license.
- Has an appropriate IP monetisation model been established?
- Could there be IP infringement within a consortium or by other consortia that member organisations participate in?
- Are there appropriate controls in place governing how members and third parties can contribute or enhance IP assets on the blockchain?
- If the application is based on a protocol that is open source – for instance, Bitcoin or Ethereum – is there a risk around non-compliance with underlying open source license terms?
- Could there be a lack of support from the members in the IP development or maintenance lifecycle?
- If the consortium legal entity should become insolvent, are there contingency plans regarding custody and maintenance of IP? For example, it could be that the IP is held in an escrow account in such a scenario.

For different IP ownership modules to consider, see focus area Intellectual property in the module Consortium Governance. For core legal and regulatory concerns and questions around IP in blockchain, see focus area Intellectual property in the module Legal and Regulatory Compliance.

Strategic risks

Adoption of blockchain technologies and business models is a strategic bet for organisations. It thus entails a range of strategic questions, such as defining the applicable value proposition, brand and reputation management, and handling change management.

Value proposition and incentive model

- What are the potential strategic risks and challenges to be anticipated with the deployment of the blockchain system?
- Has the blockchain's (use case) value proposition been clearly communicated to participants? (e.g. secure transactions, operational savings, revenue, or other benefits)
- Is the network's incentive model structured correctly to attract the desired participants or to get participants to commit the desired level of resources?
- Is there a risk of participants not willing to share sensitive information or to accept rules that may be counter to their individual interests?

Brand and reputational risks

- ☐ Could there be lawsuits from breach of contract, compromise of data, or other incidents if stakeholder expectations aren't met?
- ☐ Who is responsible for external communications in the consortium? How will credit be attributed for accomplishments of joint efforts within the consortium?

Change management risks

- ☐ Have change management plans been formulated while accounting for potential future scenarios arising from blockchain-based business models?
- ☐ Is there clarity on workforce, talent, and role changes needed to make the blockchain-based business model effective?
- ☐ Are there appropriate measures in place to account for cultural changes within the consortium (e.g. shared accountability)? Is there a plan in place to communicate changes to the stakeholders within and outside the consortium legal entity?
- ☐ Has an exit strategy been defined for consortium participants who may wish to leave?

As you get to the end of this checklist, remember that while this list covers a wide array of blockchain-specific risks, it is not meant to include every possible risk. As such, it only outlines prominent risks. You should keep in mind a range of factors, many of which may be organisation- or project-specific, to evaluate the risk profile of your project.

So, how should your organisation think about managing the identified risks from a blockchain? The next step is to proactively address identified priority risks through a risk management framework.

The scope of this toolkit doesn't include guidance on enterprise risk management programs. However, in the breakout box that follows there is a risk management framework reference that can serve as a foundation for formulating a plan appropriate for your specific organisation or project.

Reference to example of risk management framework:

The previous resources provided an overview and checklists of potential blockchain risk considerations. Organisations deploying a blockchain need to implement a risk management program to manage the relevant risks.

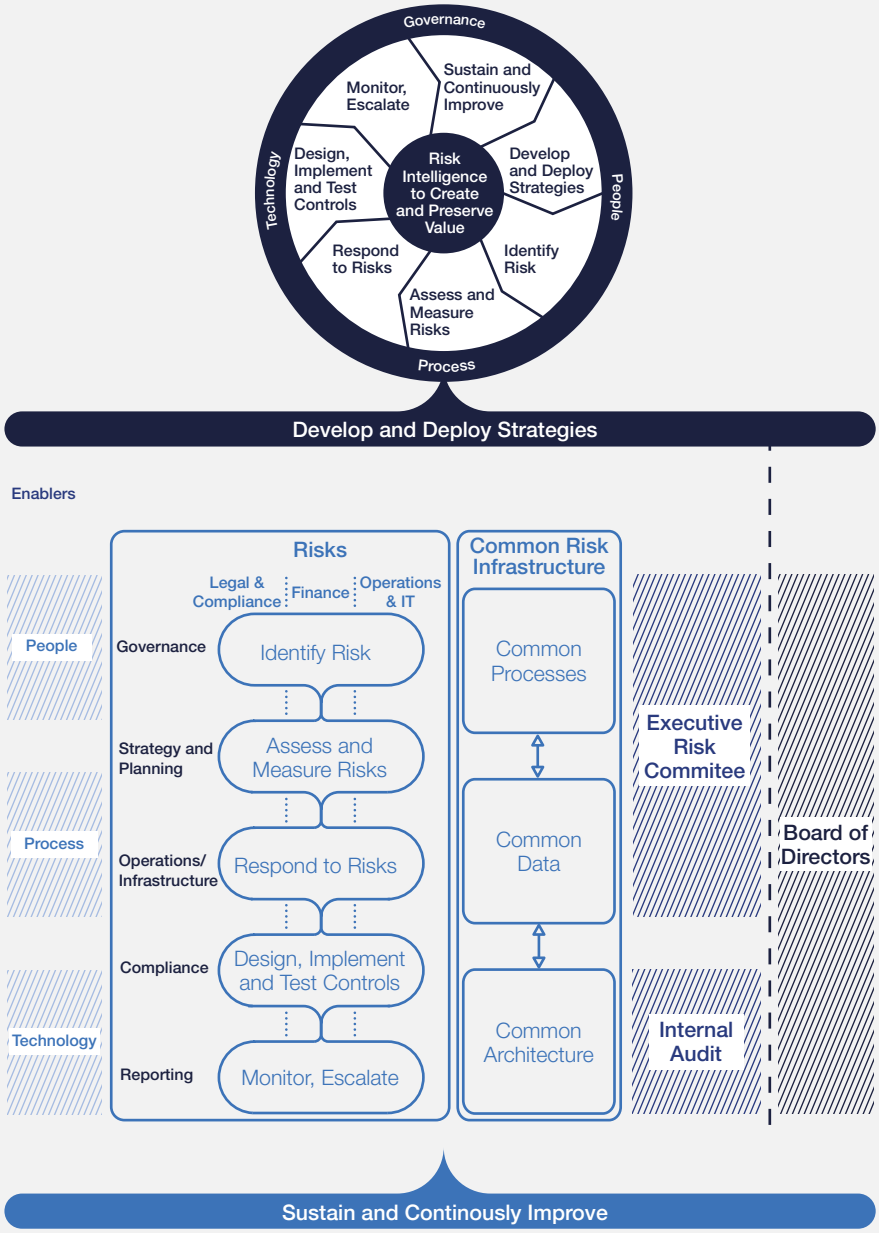


Figure 15.2 – Risk management framework[110]

In this framework, risk management is orchestrated by three broad layers of responsibility – as shown below.

- Responsibility for risk governance, including strategic guidance and risk oversight, led by the consortium governance board
- Responsibility for risk infrastructure and management, including designing, implementing, and managing an effective risk program, led by consortium executive management
- Responsibility for risk ownership, including identifying, managing, measuring, monitoring, and reporting on specific risks, led by consortium functions

Navigate Key Questions

Each of the toolkit 14 modules addresses several key questions that may arise throughout the lifecycle of a blockchain solution deployment. Those questions are presented below as a checklist, which may be a useful reference to help you locate a particular part of the toolkit that's most pertinent to a specific blockchain-related issue you're facing. For an excel workbook that consolidates the main tools and key questions of the toolkit, you may download and tailor "Blockchain Deployment Toolkit – Tools and Resources".

Ecosystem

- ☐ How does an organisation adapt its planning and development practices to suit the unique characteristics of this emerging technology?
- ☐ Why is an ecosystem both an essential component for a blockchain solution and the reason most solutions fail to scale?
- ☐ What are the various partnership models through which a blockchain ecosystem organises today?
- ☐ What are the roles and responsibilities of each participant in an ecosystem?
- ☐ What are the key governance considerations when forming a blockchain ecosystem?
- ☐ Has one considered both the short-term and long-term value propositions for the ecosystem?

Consortium Formation

- ☐ Why do supply-chain organisations often form consortia as vehicles to explore the potential of blockchain? What about the technology lends itself to this collaboration model in particular?
- ☐ Is there a blockchain consortium that is already active in the industry that can tackle a specific use case, or one already working on a similar problem?
- ☐ Which types of blockchain consortia are prevalent today?
- ☐ Which type of blockchain consortium should be formed?
- ☐ What types of business structures are useful to consider for a blockchain consortium?
- ☐ What are the important steps in creating and setting up the pre-consortium agreement?
- ☐ What are important pre-consortium agreement considerations?
- ☐ What are the key lessons learnt from others who have participated in blockchain consortia?

Consortium Governance

- ☐ Has the consortium defined governance at both a business and operational level?
- ☐ How does the purpose of the consortium impact governance? How does the consortium's lifecycle stage impact governance?
- ☐ What are the key roles and responsibilities and who will fill those positions?
- ☐ What intellectual property ownership models should be considered?
- ☐ How will you ensure that governance is not viewed as overly exclusive while also creating a functional system?
- ☐ What type of legal liabilities are consortium members exposed to, if any? What mitigating actions can be taken?
- ☐ How will the consortium be funded, both initially and on an ongoing basis? What drives decisions related to product development?
- ☐ What criteria should blockchain network participants have to meet? How can ex-participants be transitioned from the network?
- ☐ Does the blockchain network need an internal dispute resolution mechanism? When should rollback or cancellation of transactions occur?
- ☐ What processes and procedures need to be in place in order to ensure continuity and compatibility? What procedures are in place to manage code?
- ☐ What data storage and sharing approach is optimal? What data standards should be followed?

Digital Identity

- ☐ What is digital identity, and why is digital identity important?
- ☐ What actors are involved in the blockchain use case, and how does identity affect them?
- ☐ What models for digital identity should be considered? How can one ensure digital identities are secure and interoperable?
- ☐ How can one ensure digital identities are sustainable and scalable to support ever-changing technology landscapes?
- ☐ What data will be created and associated with particular people or entities in a blockchain solution, and what specific steps should be taken to ensure adequate protection of that information?
- ☐ What are the important non-technical processes and governance points to consider when designing and building the digital identity system?
- ☐ How is decentralised identity a different model, and what additional governance and technology decisions need to be made?

Interoperability

- ☐ 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?
- ☐ 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?
- ☐ What approaches exist for achieving blockchain interoperability?
- ☐ How does an organisation pick the right approach for its use case?

Structure: Public / Private

- ☐ What are the specific factors related to the needs of a particular project and its participants that affect the decision whether to utilise a public or private blockchain?
- ☐ What questions must be addressed when making a rapid initial analysis of whether a public or private blockchain is appropriate solution for the use case?

Data Protection

- ☐ What are the top action items to consider for protecting the confidentiality of sensitive data shared on a blockchain network?
- ☐ What are some of the current technologies that establish data protection on a blockchain supply chain?
- ☐ How should data protection technologies be applied in a real-world use case?

Data Integrity

- ☐ What are the key requirements for achieving data integrity in a blockchain context?
- ☐ How exactly does data move from the point of origin to a blockchain network? Where should one look for potential data integrity violations?
- ☐ What could cause data submitted to the blockchain to be inaccurate? What could go wrong at each stage in the data pipeline?
- ☐ What techniques and solutions are available to support data integrity in a blockchain deployment?
- ☐ How do I ensure that digital twins are synchronised with the physical objects they represent? What are the major components of digital-twin integrity?
- ☐ What are the different realms of correspondence between physical and digital twins? What are the solutions for common cyber-physical correspondence issues?

Personal Data Handling

- ☐ Is there a general understanding that personal data regulation will apply to your blockchain solution? What factors do organisations need to consider when determining the applicability of data protection and privacy obligations?
- ☐ Can a blockchain solution be GDPR-compliant given its characteristics of immutability and distributed nature?
- ☐ What features can be built into a blockchain solution to make GDPR compliance possible?
- ☐ What are four key principles for GDPR-compliant blockchain solutions to follow?

Cybersecurity

- ☐ What are the basics of blockchain security, including factors unique to this new technology and concepts that apply to other areas of IT as well?
- ☐ What are the top blockchain security risks, how can they be mitigated, and how do they compare to traditional databases or other familiar technologies?
- ☐ What specific steps can project teams take to manage blockchain security risks, including initial assessment of potential pitfalls and ongoing management?
- ☐ What are the key steps to maintaining the security of a new blockchain solution as it moves from planning and development into everyday use by end users?

Legal and Regulatory Compliance

- ☐ What are the most common legal and regulatory issues that arise when using blockchain technology?
- ☐ What are the legal concerns given my organisations role in a blockchain network?
- ☐ What are the types of transactions that take place on the blockchain network and their related risks?
- ☐ What are the legal concerns when building and establishing a blockchain network?
- ☐ What are the jurisdictional issues and considerations when using blockchain?
- ☐ What are smart contracts? Are they the same as a legally binding contract?

Tax Implications

- ☐ What are the most prevalent tax considerations that may arise from a blockchain solution?
- ☐ What is the nature of the digital asset being transferred? And what does this mean for tax purposes?

Financial Reporting and Controls

- ☐ When and to whom are considerations for the financial reporting process and financial statement audit during blockchain deployment relevant?

Risk Factors

- ☐ What are the new risks associated with blockchain solution deployment?

Glossary

Access control: This is a means to ensure that access to assets is authorised and restricted based on business and security requirements.[111]

Anonymity: Characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly.

Anti-money laundering (AML): A set of laws and regulations designed to ensure that financial services companies do not aid in criminal and/or terrorist enterprises. Efforts to combat money laundering and terrorism finance include KYC requirements, suspicious activity reports and currency transaction reports, all of which require financial institutions to investigate and report any customers or transactions that could be furthering a criminal enterprise. AML obligations can be burdensome, but failure to comply can result in heavy criminal and civil penalties. Global AML obligations differ by jurisdiction.

Application Program Interface (API): 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.

Artificial intelligence (AI): The capacity of a machine to imitate intelligent human behaviour.

Authentication: Verifying the identity of a user, process or device, often as a prerequisite to allowing access to resources in an information system.[112]

Autonomous software agent (ASA): An autonomous software agent is a component that has the intelligence necessary to autonomously decide when to perform an action. An ASA runs autonomously on the blockchain and enables a network participant to collaborate and negotiate transactions among themselves on behalf of, and instructed by, the entities controlling them. It is also called a decentralised application (Dapp).

Availability (in computer security): Property of being accessible and useable upon demand by an authorised entity.

Bill of landing (B/L or BOL): A document issued by a carrier to acknowledge receipt of cargo for shipment.

Commercially sensitive data: Data of a commercial nature or origin that, if known to parties other than the owner of the data, can result in adverse business consequences. Examples of such data include pricing, identity of subcontractors, true cost of goods and identity of end buyers downstream in a supply chain.

Confidentiality: Property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

Consensus mechanism: Set of rules and process(es) that determines how nodes reach agreement about a set of data and whether to approve (validate) transactions in the blockchain network. As per the MIT Center for Information Systems Research's definition, it is defined as the algorithm used to validate transactions and blocks. Consensus may rely on cryptography and a percentage of participant votes (nodes) to validate a block. Consensus protocols must also provide a mechanism for resolving block conflicts. At the other end of the spectrum, in some privately owned blockchains the owner

may decide that only the transacting parties and one other node are required to validate. The amount of time and computing power necessary to run a blockchain vary significantly based on the consensus type and percentage of nodes required.

Consortium: Companies often collaborate and partner up with other companies for various projects, and in doing so they form consortiums or joint ventures. Generally, a consortium or a joint venture is a strategic business association, combination or group of two or more entities or individuals formed to undertake an enterprise together. The intention when entering into a consortium or joint venture is to combine the individual resources and strengths of the parties involved to ensure the success of the new business venture. There are differences between a consortium and joint venture, but those differences depend on the jurisdiction in question.

Controller: Under the GDPR (Article 4), the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by European Union or EU member state law, the controller or the specific criteria for its nomination may be provided for by those laws.

Credentials: An object or data structure that authoritatively binds an identity – via an identifier or identifiers – and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber.

Cryptocurrency: The generic term for any digital asset or "token" that can be mined, purchased or transacted within a blockchain or distributed ledger network. The most famous cryptocurrency is bitcoin and others, of which there are over 1,000, include ether, Litecoin and NEO.

Cryptographic key: Sequence of symbols that controls the operation of a cryptographic transformation. A cryptographic transformation can include but is not limited to encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification.

Cryptographic techniques/cryptography: A discipline or technique that embodies principles, means and mechanisms for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use.

Data subject: As defined in the GDPR (Article 4), an identified or identifiable natural person where an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Decentralised application (Dapp): A digital program that runs on a P2P network of computers and utilises Smart Contracts to access a Blockchain network and enforce each term of agreement between two parties.

Decentralised autonomous organisation (DAO): An organisation that operates autonomously in accordance with preset rules, utilising a blockchain and coordinated through a distributed consensus model. The DAO, established in 2016 utilising Ethereum, was an example of this type of organisation.

Denial-of-service (DoS): Prevention of authorised access to a system resource or the delaying of system operations and functions, with resultant loss of availability to authorised users.

Digital asset: An asset that is digitally represented on an electronic medium or stored on a digital device.[113]

Digital document: Digital information that has been compiled and formatted for a specific purpose, that includes content and structure and may include context.

Digital identity: A unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service but doesn't necessarily need to uniquely identify the subject in all contexts.

Digital signature: Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

Distributed ledger technology (DLT): Software that uses a blockchain or similar data structure shared over a network of participants who distribute and verify information about transactions.

eIDAS: The eIDAS Regulation 910/2014 sets a framework for electronic identification and trust services for electronic transactions in the European single market.

Endpoint security: This is the process of securing the various endpoints on a blockchain network, often defined as end-user devices such as mobile devices, laptops, and desktop PCs, although hardware such as servers in a data centre are also considered endpoints. Precise definitions vary among thought leaders in the security space, but essentially, endpoint security addresses the risks presented by devices connecting to an enterprise network.[114]

Fourth industrial revolution (4IR): A way of describing the blurring of boundaries between physical, digital and biological worlds created from advancements in artificial intelligence, the Internet of Things, and other technologies.[115]

General Data Protection Regulation 2018 (GDPR): Regulation number 2016/679 entitled Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Goods and services tax (GST): A tax on goods and services sold domestically for consumption which is included in the final price and paid by consumers at the point of sale to the government from the seller.

Hacktivism(-vist): (A person to) computer hacking (as by infiltration and disruption of an IT network or website) done to further the goals of political or social activism.[116]

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

Homomorphic encryption: Symmetric or asymmetric encryption that allows third parties to perform operations on plaintext data while keeping them in encrypted form.

Immutability: Refers to the ability not to be changed – data stored in a blockchain is very hard to be changed, even by administrators. However, absolute immutability does not exist.

Initial coin offering: A fundraising method through which an entity creates a certain number of Tokens or Coins and sells them to the public.

Internet of things (IoT): A network of items – each embedded with sensors – that are connected to the internet.

JIT inventory: JIT, or just-in-time, inventory is a supply chain management technique whereby inventory is procured and transported to the point of need only when that inventory will be used imminently for production or the fulfilment of orders. Using this technique, supply chain managers can avoid holding excess inventory.

Know your customer (KYC): The requirement, pursuant to the US Bank Secrecy Act, that financial institutions conduct due diligence on their customers prior to engaging in transactions with them. The goal is to avoid inadvertently engaging in criminal activity by furthering money laundering, terrorism finance or other criminal enterprises, or engaging in business with persons on the Office of Foreign Assets Control sanctions list.

Membership service provider (MSP): A modular component that is used to manage identities on the blockchain network. This provider is used to authenticate clients who want to join the network. A certificate authority (CA) will be used in MSP to provide identity verification and binding service.

Memorandum of understanding (MOU): A document that expresses mutual accord on an issue between two or more parties. To be legally operative, it must (1) identify the contracting parties, (2) spell out the subject of the agreement and its objectives, (3) summarise the essential terms of the agreement, and (4) be signed by the contracting parties.

Miner: A person engaged in Mining, and an opportunity for computer geeks to sound tough when asked what they do. In addition, the Miners act almost as shareholders and earn voting rights when a change, such as a Fork, is proposed.

Minimum Viable Ecosystem (MVE): A network that has enough diverse stakeholders on board to be able to create the basic amount of interactions to function.

Mutual recognition: A principle of international law whereby states party to mutual recognition agreements recognise and uphold legal decisions taken by competent authorities in another member state.

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

Network nodes: Nodes represent blockchain network agents or participants, such as banks, government agencies, individuals, manufacturers and securities firms within a distributed network. Depending on the permissions set in the network, they may be able to approve/validate, send or receive transactions and data. They may validate transactions through a consensus mechanism before committing them to a shared ledger (though not all nodes perform validations depending on the system, architecture and other elements).

Off-chain: A transaction in which the value moves outside of a blockchain.

On-Chain: A transaction that occurs on the records of a blockchain.

Oracle: An interface with a data source external to a blockchain that provides input data (e.g., share price information) required for a determination of outcomes under a Smart Contract.

Oracle problem: A problem of ensuring the accuracy and correctness of data at the time it is submitted to the blockchain.

Peer to Peer (P2P): The transfer of an asset from one person to another person. It is a model in which two or more persons share resources and distribute tasks through a Decentralised Network, rather than a centralised server or network.

Penetration testing (pentesting): The process of probing and identifying security vulnerabilities and the extent to which they are used to a cracker's advantage. It is a critical tool for assessing the security state of an organisation's IT systems, including computers, IT network components, and applications. Hackers of the White Hat variety are often hired by companies to do penetration testing. It is money well spent; computer security experts contend.[117]

Permissioned: A system that uses a layer of access control to dictate the actions that may be taken by the Node users of such systems.

Permissionless: A blockchain network in which users have equal permission to utilise and interact with the network and in which users' permission to utilise and interact with the network is not set by the network itself or any central person or institution.

Personal data: As defined in the GDPR (Article 4), personal data means any information relating to a data subject. It is important to note that information that relates to a data subject, even without a name, can qualify as personal data under the GDPR.

Private blockchain: A blockchains to which access is restricted. A private blockchain is often controlled by a central person or institution.

Processing: As defined in the GDPR (Article 4), any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor: As defined in the GDPR (Article 4), a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

Proof of existence: The ability to show that a document has not been changed since it was written to the blockchain.

Public blockchain: A blockchains that anyone may access and participate in. The Bitcoin blockchain is an example of a public blockchain.

Risk management: Process of assessing and quantifying risk and establishing an acceptable level of risk for the organisation.

Role-based access control (RBAC): Permissions attributed to a role granting access to an object.

Service provider: An entity that delivers application functionality and associated services across an IT network to multiple service consumers.

Smart contract: A smart contract is a computerised transaction protocol that automatically executes (whether by all or a large number of blockchain network nodes) the terms of a contract upon a blockchain once predefined conditions are met. Blockchains can be programmed to automate business processes (e.g. making payments) in different entities.

Threat: Potential cause of an unwanted incident, which may result in harm to a system or organisation.

Token (for a blockchain network): A digital asset used in a blockchain transaction. A token can be native to the blockchain, such as a cryptocurrency, or it can be a digital representation of an off-chain asset (known as tokenised asset) such as the title to a house.

Tokenisation: The process of replacing a primary account number (usually a credit card) with a surrogate number (or token – different from a Token) that is randomly generated and not otherwise associated with a payment device. Tokenisation is supposed to provide account holders with additional security, especially at point-of-sale terminals, so that their credit card numbers are not vulnerable to hacking.

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

Trust anchor: An organisation that conducts identity proofing, then issues physical documents and/or digital credentials/attestation on which others rely.

Validator (blockchain): Someone who is responsible for verifying transactions within a blockchain. In the Bitcoin Blockchain, any participant can be a blockchain validator by running a full-node.

Value added tax (VAT): A tax added on a product whenever value is added at each stage of the supply chain, from production to the point of sale.

Vulnerability: Weakness of software, hardware, or online service that can be exploited.

Wallet: A non-physical storage device for cryptocurrency that a person downloads as a software file and that remains connected to the internet. A Wallet can be downloaded and installed on a computer, run online via the cloud, or run on a smart device via a mobile application.

Contributors

The World Economic Forum's Blockchain Deployment Toolkit is a global, multi-industry, multi-stakeholder endeavour aimed at helping organisations build and scale well-thought-out blockchain solutions. More than 100 stakeholders across multiple industries and governments from around the world engaged in co-designing this toolkit to encourage responsible blockchain deployment. This toolkit is a combined effort of all involved based on numerous discussions, workshops, user feedback groups and research. However, the opinions expressed herein may not necessarily correspond with each individual involved with the project. Sincere thanks are extended to those who contributed their insights, including those not captured below.

Lead Authors

Core Team

Nadia Hewett, Project Lead Blockchain and Digital Currency, World Economic Forum, USA

Sumedha Deshmukh, Project Specialist Blockchain and Digital Currency, World Economic Forum, USA

Soichi Furuya, Senior Researcher, Hitachi (and World Economic Forum Fellow), USA

Francis Jee, World Economic Forum Fellow, USA

AbdulHakim Alhabib, Systems Consultant, Saudi Aramco (and World Economic Forum Fellow), USA

We are very grateful for the generous commitment and support of the organisations who dedicated Fellows to the project.

Module Authors

Adrien Ogée, Project Lead Cyber Resilience, World Economic Forum, Switzerland

Alexandra Ashpole, Decentralized Identity Consultant, Accenture, USA

Andrew Moyle, Partner and Global Chair of Fintech Practice, Latham & Watkins, United Kingdom

Anne Flannagan, Project Lead Data Policy, World Economic Forum, USA

Bianca Lee, Trainee Solicitor, Latham & Watkins, United Kingdom

Chris Hanebeck, Founder & CEO, Truckl, USA

Christine Leong, Managing Director and Decentralized Identity Global Lead, Accenture, USA

Frida Montenius, Associate, Latham & Watkins, United Kingdom

Henrik Hvid Jensen, Senior Digital Business Advisor, Trustworks A/S, Denmark

Jarick Poulson, Tax Managing Director, Deloitte, USA

Jenny Cieplak, Partner, Latham & Watkins, USA

Jesper Mathias Nielsen, Manager, Deloitte, Denmark

Joseph Koo, Tax Consultant, Deloitte, USA

Linda Pawczuk, Global Consulting Blockchain and Digital Assets Leader, Deloitte Global, USA

Max Fang, Blockchain Specialist, University of Berkeley, USA

Paul Sin, Partner, Deloitte, China

Peter Taylor, Audit and Assurance Senior Manager, Deloitte, USA

Rebecca Liao, Co-Founder and Executive Vice President, Skuchain, USA

Shawn Muma, Technology Researcher Leader, Center for Global Enterprise, USA

Stuart Davis, Partner, Latham & Watkins, United Kingdom

Sugathri Kolluru, Research Associate, Center for Global Enterprise, USA

Susan Joseph, Principal, Susan Joseph LLC, USA

Swagatam Chakraborty, Advisory Senior Solution Advisor, Deloitte, India

Wolfgang Lehmacher, Operating Partner, Industrial Innovation Partners, Anchor Group, Switzerland

Yang Chu, Advisory Senior Manager, Deloitte, USA

Pilot Partners

Sincere thanks to those who tested the toolkit on their use cases and Yingli Wang at Cardiff University that independently evaluated the pilot results.

Pilot Organisations & Individuals

Abu Dhabi Digital Authority, Pilot Partner, United Arab Emirates

Saudi Aramco, Pilot Partner, Saudi Arabia

Marek Termanowski, Partner, Accelliance, United Arab Emirates

Mariam Obaid Al Muhairi, Head, Centre for the Fourth Industrial Revolution UAE, United Arab Emirates

Mark Balovnev, Partner, Accelliance, Canada

Core Contributors

Aida Jamak, Project Manager, Point Jupiter, Bosnia and Herzegovina

Andrej Antolović, Design Lead, Point Jupiter, Croatia

Andrew Ballinger, Analyst, Wave Financial, USA

Andrew Rudnick, Consulting Business Analyst, Deloitte, USA

David Jelić, Chief Technical Officer, Point Jupiter, Croatia

Homan Farahmand, Independent Contributor, Canada

Jayavaradhan Sambedu, Co-Founder and Chief Technology Officer, Curl Analytics, India

Lucy Hakobyan, Head of Programs, Mobility Open Blockchain Initiative, USA

Mariam Obaid Al Muhairi, Head, C4IR UAE, United Arab Emirates

Masha Smith, Legal Counsel, Latham & Watkins, USA

Milly Perry, Chair, Blockchain University Global and DAO 4 DAO's Institute, Israel

Monia Škurtan, UX/UI Designer, Point Jupiter, Croatia

Nakul Lele, Consulting Managing Director, Deloitte, USA

Peter McKay, Founder/Consultant, Indizr, USA

Ricky Franks, Consulting Manager, Deloitte, USA

Sheila Warren, Platform Head – Blockchain, Digital Currency, and Data Policy, World Economic Forum, USA

Shelby Botula, Project Coordinator, Blockchain and Distributed Ledger Technology, World Economic Forum, USA

Yingli Wang, Professor, Cardiff University, United Kingdom

Zvika Krieger, Head of Technology Policy & Partnerships, World Economic Forum, USA

Reviewers

Alastair Pryor, Portfolio Manager - Frontier Technology, United Nations World Food Programme Innovation Accelerator, Germany

Alisa DiCaprio, Head of Trade and Supply Chain, R3, USA

Alexander Varvarenko, CEO & Founder, SHIPNEXT, Belgium

Anastasia Kuskova, Transformation and Sustainability Director, Eurasian Resources Group, The Netherlands

Andreas Kuehn, Senior Program Associate, Global Cooperation in Cyberspace Initiative & Global Security, EastWest Institute, USA

Andrew Borene, Chief Executive Officer, Cipherloc Corporation and Fellow at Georgetown University's Center for Security Studies, USA

Anina van der Walt, Student Researcher, University of Auckland, New Zealand

Anoop Nannra, Technical Steering Committee Member / DLT Task Group Co-Chair, Industrial Internet Consortium, USA

Antonio Senatore, Director, Deloitte, Ireland

Ben Singh-Jarrold, Head of Product Marketing, R3, United Kingdom

Benjamin O'Neal, Attorney, Strategic Solutions & Counsel LLC, USA

Bob Crozier, Head of Allianz Global Blockchain Center and Board Member of B3i, Switzerland

Boris Polania, Lead Engineer of Payments & Blockchain, Honda Innovations, USA

Chris Brodersen, Consulting Specialist Leader, Deloitte, USA

Claudina Castro Tanco, Consulting Enabling Manager, Deloitte, USA

Daniela Barat, Head of Legal & Compliance, World Economic Forum, Switzerland

David Kappos, Partner, Cravath, Swaine & Moore LLP, USA

Dhananjay Goswami, Consulting Specialist Leader, Deloitte, USA

Dominique Guinard, CTO & Co-Founder, EVRYTHNG, Switzerland

Dusko Karaklajic, Senior Manager, Deloitte, Switzerland

Fiona Maclean, Partner, Latham & Watkins, United Kingdom

Floris Landi, Graphic Design and Publications Lead, World Economic Forum, Switzerland

Gadi Benmoshe, CIO, Israel Ports Ltd., Israel

Gary D. Sprague, Partner, Baker McKenzie, USA

Gayle Markovitz, Editor, World Economic Forum, Switzerland

Han Wang, Consultant, Technology & Innovation Lab, World Bank Group, USA

Heidi Eggert, Head of Innovation Entrepreneurs, Nike Inc., USA

Helena Correia Mendonça, Principal Consultant, VdA Legal Partners, Portugal

Inês Antas de Barros, Managing Associate, VdA Legal Partners, Portugal

Jaka Mele, Chief Digital Officer, CargoX, Slovenia

Jan Scheele, Chief Executive Officer, Bitcanna, The Netherlands

Jana Krimpe, Partner & Founder, B.EST Solutions, Estonia

Jean-Philippe Stanway, Graphic Designer, World Economic Forum, Switzerland

Jens Munch Lund-Nielsen, Head of Global Trade & Supply Chains, IOTA Foundation, United Kingdom

John Choi, Chief Executive Officer, MarkAny, Korea

Joseph Koo, Tax Consultant II, Deloitte, USA

Kateryna Isirova, Junior Associate, B.EST Solutions Estonia, Ukraine

Kathryn Troxel, Tax Professor, Seattle University, USA

Kei Fukuta, Director, Hitachi Ltd., Japan

Larry Pang, Head of Business Development, IoTeX, USA

Lidia Kamleh, General Counsel, Museum of the Future, Dubai Future Foundation, United Arab Emirates

Lisa Simpson, Consulting Manager, Deloitte, USA

Luca Castellani, Legal Officer, United Nations Commission on International Trade Law, Austria

Madhav Durbha, Group Vice President, LLamasoft, USA

Magda Cocco, Partner and Head of ICT Practice, VdA Legal Partners, Portugal

Malika Sajdik, Associate, Latham & Watkins, Hong Kong

Mark Sun, Associate, Latham & Watkins, United Kingdom

Michael Prokop, Advisory Managing Director, Deloitte, USA

Michael Taylor, Member, Trusted IoT Alliance, Switzerland

Mikkel Boding Kildetoft, Consultant, Deloitte, Denmark

Mitch Rabinowitz, Partner, Latham & Watkins, USA

Moritz Petersen, Senior Researcher, Kühne Logistics University, Germany

Naveed Ahmed, Head of Media, Communications and IT Contracts Section, The Government of Dubai Legal Affairs Department, United Arab Emirates

Niamh O'Connell, Project Manager at Treum, ConsenSys U.S., USA

Nicolas Verschelden, Managing Partner Dream Tech Alliance, AB InBev, Belgium

Oleksandr Potii, Professor, JSC Institute of Information Technology, Ukraine

Olushola Ibironke Joanne Martins, IT Officer, Technology & Innovation Lab, World Bank Group, USA

Pankaj Kulkarni, Consulting Manager, Deloitte, India

Partha Das Chowdhury, Head Blockchain Centre of Excellence, Vara Technology, India

Peder Muller, Advisory Specialist Leader, Deloitte, USA

Prakash Santhana, Advisory Managing Director, Deloitte, USA

Prema Shrikrishna, IT Officer, Technology & Innovation Lab, World Bank Group, USA

Punit Shukla, Project Lead Blockchain and Distributed Ledger Technology, World Economic Forum, India

Rachel Alexandra Halsema, IT Officer, Technology & Innovation Lab, World Bank Group, USA

Rajesh Dhuddu, Global Practice Leader-Blockchain, Tech Mahindra, India

Raunak Mittal, Consultant, Technology & Innovation Lab, World Bank Group, USA

Rene Alvarenga, Sr. Director of Software Product Management, GE Transportation, USA

Richard Morton, Secretary General, International Port Community Systems Association, United Kingdom

Robert Learney, Lead Technologist Blockchain & DLT, Digital Catapult, United Kingdom

Robert Leo Maslamoney, Managing Director Maersk Angola, Angola

Robert Massey, Tax Partner, Deloitte, USA

Ryan Rugg, Head of Industry Verticals, R3, USA

Ryoko Imai, Senior Research Scientist, Hitachi America, USA

Sandra Corcuera-Santamaria, Integration and Trade Senior Specialist, Inter-American Development Bank, USA

Sergey Tyan, Strategy Director, Eurasian Resources Group, The Netherlands

Shelby Murphy, Audit & Assurance Managing Director, Deloitte, USA

Simon Kiilerich Vedel, Senior Product Manager, Maersk, Denmark

Sue McLean, Partner, Baker McKenzie, USA

Tamara Levin, Partner, Baker McKenzie, USA

Tim Davis, Advisory Partner, Deloitte, USA

Valesca Molinari, Co-Head of Innovation and Legal Tech for Germany and Austria, Baker McKenzie (and World Economic Forum Fellow), USA

Varun Jain, Consulting Manager, Deloitte, USA

Vincent Annunziato, Director, US Customs & Border Protection, USA

Virginia Cram-Martos, CEO, Triangularity SáRL, Spain

Wendy Henry, Consulting Managing Director, Deloitte, USA

Zhijun William Zhang, Senior IT Officer Security, Risk and Compliance, World Bank Group, USA

Ziyang Fan, Head of Digital Trade, World Economic Forum, USA

Acknowledgements

Additional thanks goes to Christoph Wolff, Margi Van Gogh, Jayant Narayan, Amanda Russo, Alexandra May, Linda Lacina and all of the individuals and organisations – experts, supply chain actors, company executives, policy-makers and others – for your input in workshops, interviews, user-feedback, scoping exercises, surveys and more to shape the outcome of this toolkit.

Endnotes

[1] Redesigning Trust: Blockchain for Supply Chains, World Economic Forum, 2019, https://www.weforum.org/projects/redesigning-trust

[2] Redesigning Trust: Blockchain for Supply Chains, World Economic Forum, 2019, https://www.weforum.org/projects/redesigning-trust

[3] Inclusive Deployment of Blockchain for Supply Chains: Part 1 - Introduction, World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Introduction_to_Blockchain_for_Supply_Chains.pdf

[4] Inclusive Deployment of Blockchain for Supply Chains: Part 2 - Trustworthy Verification of Digital Identities, World Economic Forum,2019, http://www3.weforum.org/docs/WEF_Trustworthy_Verification_of_Digital_Identities_2019.pdf

[5] Inclusive Deployment of Blockchain for Supply Chains: Part 3 - Public of Private Blockchains -Which One is Right for You?, World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Inclusive_Deploymentof_Blockchain_for_Supply_Chains.pdf

[6] Inclusive Deployment of Blockchain for Supply Chains: Part 4 - Protecting your Data, World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Inclusive_Deployment_of_Blockchain_for_Supply_Chains_Part_4_Report.pdf

[7] Inclusive Deployment of Blockchain for Supply Chains: Part 5 - A Framework for Blockchain Cybersecurity, World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Inclusive_Deployment_of_Blockchain_for_Supply_Chains_Part_5.pdf

[8] Inclusive Deployment of Blockchain: Case Studies and Learnings from the United Arab Emirates, World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Inclusive_Deployment_of_Blockchain_Case_Studies_and_Learnings_from_the_United_Emirates.pdf

[9] Inclusive Deployment of Blockchain for Supply Chains: Part 6 - A Framework for Blockchain Interoperability, World Economic Forum, 2020, http://www3.weforum.org/docs/WEF_A_Framework_for_Blockchain_Interoperability_2020.pdf

[10] Inclusive Deployment of Blockchain for Supply Chains: Part 1 - Introduction, World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Introduction_to_Blockchain_for_Supply_Chains.pdf

[11] Enterprise Ethereum Alliance, https://entethalliance.org/technical-documents/

[12] Blockchain and distributed ledger technologies -Reference architecture, ISO, https://www.iso.org/standard/75093.html

[13] Blockchain in Banking: While the interest is huge, challenges remain in for large scale adoption, Deloitte, 2017, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/strategy/in-strategy-innovation-blockchain-in-banking-noexp.pdf

[14] Jensen, Henrik, “Blockchain -the corporate weapon against disruption”, Medium, 2018, https://medium.com/@henrikhvidjensen/blockchain-the-corporate-weapon-against-disruption-5784adbeabb6

[15] Jensen, Henrik, Blockchain -the corporate weapon against disruption, Medium, 2018, https://medium.com/@henrikhvidjensen/blockchain-the-corporate-weapon-against-disruption-5784adbeabb6

[16] Blockchain Beyond the Hype,World Economic Forum, 2018, https://www.weforum.org/whitepapers/blockchain-beyond-the-hype

[16] Building Value with Blockchain Technology: How to Evaluate Blockchain’s Benefits”, World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Building_Value_with_Blockchain.pdf

[16] ”These 11 questions will help you decide if blockchain is right for your business”, World Economic Forum, 2018, https://www.weforum.org/agenda/2018/04/questions-blockchain-toolkit-right-for-business

[17] Redesigning Trust: Blockchain for Supply Chains, World Economic Forum, 2019, https://www.weforum.org/projects/redesigning-trust

[18] Inclusive Deployment of Blockchain for Supply Chains: Part 1 - Introduction, World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Introduction_to_Blockchain_for_Supply_Chains.pdf

[19] Inclusive Deployment of Blockchain for Supply Chains: Part 2 - Trustworthy Verification of Digital Identities, World Economic Forum,2019, http://www3.weforum.org/docs/WEF_Trustworthy_Verification_of_Digital_Identities_2019.pdf

[20] Inclusive Deployment of Blockchain for Supply Chains: Part 3 - Public of Private Blockchains -Which One is Right for You?, World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Inclusive_Deploymentof_Blockchain_for_Supply_Chains.pdf

[21] Inclusive Deployment of Blockchain for Supply Chains: Part 4 - Protecting your Data, World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Inclusive_Deployment_of_Blockchain_for_Supply_Chains_Part_4_Report.pdf

[22] Inclusive Deployment of Blockchain for Supply Chains: Part 5 - A Framework for Blockchain Cybersecurity, World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Inclusive_Deployment_of_Blockchain_for_Supply_Chains_Part_5.pdf

[23] Inclusive Deployment of Blockchain: Case Studies and Learnings from the United Arab Emirates, World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Inclusive_Deployment_of_Blockchain_Case_Studies_and_Learnings_from_the_United_Emirates.pdf

[24] Inclusive Deployment of Blockchain for Supply Chains: Part 6 - A Framework for Blockchain Interoperability, World Economic Forum, 2020, http://www3.weforum.org/docs/WEF_A_Framework_for_Blockchain_Interoperability_2020.pdf

[25] Blockchain Beyond the Hype,World Economic Forum, 2018, https://www.weforum.org/whitepapers/blockchain-beyond-the-hype

[25] Building Value with Blockchain Technology: How to Evaluate Blockchain's Benefits", World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Building_Value_with_Blockchain.pdf

[25] "These 11 questions will help you decide if blockchain is right for your business", World Economic Forum, 2018, https://www.weforum.org/agenda/2018/04/questions-blockchain-toolkit-right-for-business

[26] Inclusive Deployment of Blockchain for Supply Chains: Part 1 - Introduction, World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Introduction_to_Blockchain_for_Supply_Chains.pdf

[27] Jensen, Henrik, "Blockchain -the corporate weapon against disruption", Medium, 2018, https://medium.com/@henrikhvidjensen/blockchain-the-corporate-weapon-against-disruption-5784adbeabb6

[28] "Blockchain Beyond the Hype",World Economic Forum, 2018, https://www.weforum.org/whitepapers/blockchain-beyond-the-hype

[29] Building Value with Blockchain Technology: How to Evaluate Blockchain's Benefits, World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Building_Value_with_Blockchain.pdf

[30] These 11 questions will help you decide if blockchain is right for your business, World Economic Forum, 2018, https://www.weforum.org/agenda/2018/04/questions-blockchain-toolkit-right-for-business

[31] Wood, Miranda, "Repsol contracts Finboot for bclockchain oil certification project", Ledger Insights, 2019, https://www.ledgerinsights.com/blockchain-repsol-contracts-finboot-oil-certification

[32] Veale, James, SAP and SUSTAIN launch blockchain Palm Oil traceability initiative, https://www.linkedin.com/pulse/sap-sustain-launch-blockchain-palm-oil-traceability-initiative-veale

[33] Trace Labs and OneAgrix Launch Blockchain-Based Halal Certification System, Medium, 2019, https://medium.com/origintrail/trace-labs-and-oneagrix-launch-blockchain-based-halal-certification-system-45a3bcfa404e

[34] Wood, Miranda, "Repsol contracts Finboot for blockchain oil certification project", Ledger Insights, 2019, https://www.ledgerinsights.com/blockchain-repsol-contracts-finboot-oil-certification

[35] This Figure is adopted from the World Economic Forum white paper Inclusive Deployment of Blockchain for Supply Chains: Part 6 - A framework for blockchain interoperability done in collaboration with Deloitte

[36] This Figure is adopted from the World Economic Forum white paper Inclusive Deployment of Blockchain for Supply Chains: Part 6 - A framework for blockchain interoperability done in collaboration with Deloitte

[37] Rosabeth Moss Kanter, Collaborative Advantage: The Art of Alliances, Harvard Business Review, 1994, https://hbr.org/1994/07/collaborative-advantage-the-art-of-alliances

[38] SAP, Bumble Bee Foods and SAP Create Blockchain to Track Fresh Fish from Ocean to Table, YouTube, May 11 2019, https://www.youtube.com/watch?v=-bq8fp7_l4k

[39] Bumble Bee Foods and SAP Create Blockchain to Track Fresh Fish from Ocean to Table, SAP, 2019, https://news.sap.com/2019/03/bumble-bee-foods-sap-create-blockchain-track-fish/?source=social-global-sap+digital+business+services-youtube-audienceengagement-dbs-services-scp-spr-2182044493&campaigncode=CRM-YA19-VIN-SOCIALM

[40] Difference between consortium and joint ventures, Malescu Law, 2019, https://malesculaw.com/difference-consortium-joint-ventures/

[41] Port News: Steering in Information Waves, http://en.portnews.ru/news/290245/

[42] Trace Labs and OneAgrix Launch Blockchain-Based Halal Certification System, Medium, 2019, https://medium.com/origintrail/trace-labs-and-oneagrix-launch-blockchain-based-halal-certification-system-45a3bcfa404e

[43] Inclusive Deployment of Blockchain for Supply Chains: Part 1 - Introduction, World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Introduction_to_Blockchain_for_Supply_Chains.pdf

[44] "Peers", Hyperledger Fabric, https://hyperledger-fabric.readthedocs.io/en/release-2.0/peers/peers.html

[45] Hyperledger -Chapter 6 - Hyperledger Fabric Components -Technical Context, Medium, 2018, https://medium.com/swlh/hyperledger-chapter-6-hyperledger-fabric-components-technical-context-767985f605dd

[46] Muma, Shawn, "Your Blockchain Project is Doomed If You Don't Ask These Five Questions", SupplyChain Management Review, February 7 2020, https://www.scmr.com/article/your_blockchain_project_is_doomed_if_you_dont_ask_these_five_questions

[47] Clary, "Softwareismeanttobefree.Abriefhistoryofopensource", hackernoon, January2019, https://hackernoon.com/software-is-meant-to-be-free-a-brief-history-of-open-source-892d29e803a0

[48] Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, Bitcoin.org, 2008, https://www.bitcoin.com/bitcoin.pdf

[49] "Deloitte's 2019 Global Blockchain Survey: Blockchain gets down to business", Deloitte, 2019, https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf

[50] Joseph, Susan, "Do Blockchains and Consortia Go Together like PB & J", Medium, April 1 2019, https://medium.com/@SusanJoseph1786/do-blockchains-and-consortia-go-together-like-pb-j-c70879c0601

[51] R3 Website, https://www.r3.com/history/

[52] "The Right Way to do Blockchain Consortiums", Coindesk, May 3 2019, https://www.coindesk.com/the-right-way-to-do-blockchain-consortiums?amp=1

[53] Lohchab, Himanshi, "Blockchain fight against spam may not be landslide victory", Economic Times, November 25 2019, https://m.economictimes.com/industry/telecom/telecom-news/blockchain-fight-against-spam-may-not-be-landslide-victory/amp_articleshow/72193464.cms

[54] The Institutes' Risk and Insurance Knowledge group website, https://www.theinstitutes.org/guide/riskstream-collaborative

[55] Anwar, Hasib, "Contour Blockchain (Voltron): A Milestone for Trade Finance", 101 Blockchains, February 2 2020, https://101blockchains.com/contour-blockchain/amp/

[56] Neuburger, Jeffrey, "Supply Chain Blockchain Initiative Receives Federal Antitrust Exemption", The National Law Review, February 11 2020, https://www.natlawreview.com/article/supply-chain-blockchain-initiative-receives-federal-antitrust-exemption?amp

[57] Do Blockchains and Consortia Go Together like PB & J", Medium, April 1 2019, https://medium.com/@SusanJoseph1786/do-blockchains-and-consortia-go-together-like-pb-j-c70879c0601

[58] "Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology", 2020, available at https://www.isda.org/a/4RJTE/Private-International-Law-Aspects-of-Smart-Derivatives-Contracts-Utilizing-DLT.pdf

[59] Inclusive Deployment of Blockchain for Supply Chains, Part 2: Trustworthy Verification of Digital Identities, World Economic Forum, 2019. http://www3.weforum.org/docs/WEF_Trustworthy_Verification_of_Digital_Identities_2019.pdf

[60] Inclusive Deployment of Blockchain for Supply Chains, Part 2: Trustworthy Verification of Digital Identities, World Economic Forum, 2019. http://www3.weforum.org/docs/WEF_Trustworthy_Verification_of_Digital_Identities_2019.pdf

[61] Identity in a Digital World: A new chapter in the social contract, World Economic Forum, 2019. http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

[62] Proof of existence "covers any electronic information which can document that an entity is a legal entity under a specific jurisdiction." p.8 World Economic Forum, Inclusive Deployment of Blockchain for Supply Chains, Part 2: Trustworthy Verification of Digital Identities, 2019. http://www3.weforum.org/docs/WEF_Trustworthy_Verification_of_Digital_Identities_2019.pdf (accessed 12/20/2019).

[63] Identity in a Digital World: A new chapter in the social contract, World Economic Forum, 2019. http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

[64] Inclusive Deployment of Blockchain for Supply Chains, Part 2: Trustworthy Verification of Digital Identities, World Economic Forum, 2019. http://www3.weforum.org/docs/WEF_Trustworthy_Verification_of_Digital_Identities_2019.pdf

[65] https://vonx.io/

[66] National Institute of Standards and Technology, NIST Special Publication 800-63 -Revision 3, 2019. https://pages.nist.gov/800-63-3/sp800-63-3.html (accessed 12/20/2019).

[67] Blockchain is not a magic bullet for security. Can it be trusted? World Economic Forum, 2019. https://www.weforum.org/agenda/2019/08/blockchain-security-trust/

[68] Morrow, Susan, "When identity data eclipses digital identity", CSO, August 23 2017, https://www.csoonline.com/article/3217708/when-identity-data-eclipses-digital-identity.html

[69] Data Minimalism, Fjord, 2018, https://trends19.fjordnet.com/trends/data-minimalism

[70] Cavoukian, Ann Privacy by Design –The 7 Foundational Principles, https://www.ryerson.ca/content/dam/pbdce/seven-foundational-principles/The-7-Foundational-Principles.pdf

[71] Jensen, Henrik, Blockchain Do Not Add Additional Security -Blockchain Adds Distributed Trust, 2018, https://medium.com/@henrikhvidjensen/blockchain-do-not-add-additional-security-blockchain-adds-distributed-trust-132991b6e57e

[72] Wood, Miranda, Digital Bazaar, GS1 US Working on Digital Identities For Supply Chain, Ledger Insights, 2019, https://www.ledgerinsights.com/digital-bazaar-gs1-digital-identities-for-supply-chain/

[73] Trust Your Supplier website, https://www.trustyoursupplier.com/

[74] DTCC and Accenture Unveil Governance Operating Model to Manage Risks and Promote Safety Across Distributed Ledger Technology Landscape, 2019. https://newsroom.accenture.com/news/dtcc-and-accenture-unveil-governance-operating-model-to-manage-risks-and-promote-safety-across-distributed-ledger-technology-landscape.htm?_ga=2.21015419.1303829891.1576763496-566277452.1570458062

[75] Inclusive Deployment of Blockchain for Supply Chains: Part 6 - A Framework for Blockchain Interoperability, World Economic Forum, 2020, http://www3.weforum.org/docs/WEF_A_Framework_for_Blockchain_Interoperability_2020.pdf

[76] ISO. (2020). ISO/CD 23257.2 Blockchain and distributed ledger technologies - Reference architecture. Retrieved 01 09, 2020, from https://www.iso.org/standard/75093.html?browse=tc

[77] Deloitte. (2017). Figure 2: Blockchain in banking. Retrieved 01 09, 2020, from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/strategy/in-strategy-innovation-blockchain-in-banking-noexp.pdf

[78] BIA, 2019. BIA. [Online], available at: https://bialliance.io [Accessed 09 01 2020]

[79] BiTA, 2019. BiTA. [Online], available at: https://www.bita.studio/standards [Accessed 09 01 2020].

[80] BRI, 2018. BRI. [Online], Available at: https://www.beltroad-initiative.com [Accessed 09 01 2020].

[81] BSI, 2019. BSI. [Online], available at: https://www.bsigroup.com/en-MY/About-BSI/Media-Centre/press-releases/2019-press-releases/january-2019/bsi-partners-with-origintrail-to-develop-blockchain-enabled-solutions [Accessed 09 01 2020]

[82] CESI, 2019. CESI. [Online], available at: http://www.cc.cesi.cn/english.aspx [Accessed 09 01 2020]

[83] DCSA, 2019. DCSA. [Online], available at: https://www.dcsa.org [Accessed 09 01 2020]

[84] EBP, 2019. EBP. [Online], available at: https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership [Accessed 09 01 2020]

[85] EEA, 2019. EEA. [Online], available at: https://entethalliance.org [Accessed 09 01 2020]

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

[87] IEEE, 2019. IEEE. [Online], available at: https://blockchain.ieee.org [Accessed 09 01 2020]

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

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

[90] EU Blockchain Observatory and Forum. (2019, September). www.eublockchainforum.eu. Retrieved from www.eublockchainforum.eu: https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf

[91] Hedera. (2019). Hedera: A Public Hashgraph Network & Governing Council. Retrieved 01 09, 2020, from https://www.hedera.com/hh-whitepaper-v2.0-17Sep19.pdf

[92] Deloitte. (2019). So, you've decided to join a blockchain consortium. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology/us-cons-blockchain-consortium.pdf

[93] "Inclusive Deployment of Blockchain for Supply Chains: Part 3 - Which one is right for you: Public or Private", World Economic Forum, http://www3.weforum.org/docs/WEF_Inclusive_Deploymentof_Blockchain_for_Supply_Chains.pdf

[94] "Inclusive Deployment of Blockchain for Supply Chains: Part 4 - Protecting Your Data, White Paper", World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Inclusive_Deployment_of_Blockchain_for_Supply_Chains_Part_4_Report.pdf

[95] Ten troublecome blockchain terms: What's accurate? What's not? Federal Reserve Bank of Minneapolis, 2019, https://www.minneapolisfed.org/~/media/files/news_events/bank-updates/2019-02/ten-troublesome-blockchain-terms.pdf?la=en

[96] "Inclusive Deployment of Blockchain for Supply Chains: Part 4 - Protecting your Data", World Economic Forum, 2019, https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-for-supply-chains-part-4-protecting-your-data

[97] Inclusive Deployment of Blockchain for Supply Chains: Part 4 - Protecting your Data, World Economic Forum, 2019, https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-for-supply-chains-part-4-protecting-your-data

[98] "Blockchain and the GDPR", European Union Blockchain Observatory and Forum, 2018, https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf

[99] "Blockchain and the General Data Protection Regulation", European Parliament Research Service, 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

[100] Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles?, CNIL, 2018, available at: https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf.

[101] Supra CNIL 2018.

[102] The Right to be Forgotten Meets the Immutable - A Practical Guide to GDPR-Compliant Blockchain Solutions, The Center for Global Enterprise, Cravath, Swaine & Moore, DSCI and Slaughter and May, 2019, available at: https://www.cravath.com/files/Uploads/Documents/Publications/3898415_1.pdf

[103] Inclusive Deployment of Blockchain for Supply Chains, Part 5 - A Framework for Blockchain Cybersecurity", World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Inclusive_Deployment_of_Blockchain_for_Supply_Chains_Part_5.pdf

[104] Inclusive Deployment of Blockchain for Supply Chains, Part 5 - A Framework for Blockchain Cybersecurity", World Economic Forum, 2019, http://www3.weforum.org/docs/WEF_Inclusive_Deployment_of_Blockchain_for_Supply_Chains_Part_5.pdf

[105] "Guide for Conducting Risk Assessments", NIST,2012, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[106] Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, National Institute of Standards and Technology, 2016, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[107] Some examples:

CISSP: Certified Information Systems Security Professional, https://www.isc2.org/Certifications/CISSP

CEH: Certified Ethical Hacker, https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

CISM: Certified Information Security Manager, https://www.isaca.org/credentialing/cism

CompTIA Security+, https://www.comptia.org/certifications/security

CISA: CertifiedInformation Security Auditor, https://www.isaca.org/credentialing/cisa

GIAC Security Essentials (GSEC) certification, https://www.giac.org/certification/security-essentials-gsec

[108] "eGovernment Domain Discussion", 2019, https://www.unece.org/fileadmin/DAM/cefact/cf_forums/2019_Geneva/PPT_eGov-Domain.pdf

[109] William Bible, Jon Raphael, Matthew Riviello, Peter Taylor, Iliana Oris Valiente, "Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession,", 2017, https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf

[110] Source for the reference risk management framework:

Take the right steps: 9 principles for building the Rist Intelligent Enterprise", Deliotte, 2009, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/Board%20of%20Directors/in-gc-putting-risk-in-the-comfort-zone-nine-principles-for-risk-intelligent-enterprises-noexp.pdf

"Enterprise Risk Management: a risk intelligent approach", Deloitte, 2015, https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/audit/deloitte-uk-erm-a-risk-intelligent-approach.pdf

"Blockchain Risk Management: Risk functions need to play an active role in shaping blockchain strategy", Deloitte, 2017, https://www2.deloitte.com/us/en/pages/advisory/articles/blockchain-risk-management.html

[111] ISO/IEC 2700:2018

[112] NIST SP 800-128

[113] The Book of Jargon: Cryptocurrency & Blockchain Technology, Latham & Watkins, https://www.lw.com/bookofjargon-apps/boj-CryptocurrencyandBlockchain

[114] "What is Endpoint Security? Data Protection 101", Digital Guardian, https://digitalguardian.com/blog/what-endpoint-security-data-protection-101

[115] "What Is the Fourth Industrial Revolution?" Salesforce, https://www.salesforce.com/blog/2018/12/what-is-the-fourth-industrial-revolution-4IR.html

[116] https://www.merriam-webster.com/dictionary/hacktivism

[117] Penetration Testing: The Third Part Hacker, SANS, 2006, https://www.sans.org/reading-room/whitepapers/testing/paper/264