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.

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.
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).

<table>
<thead>
<tr>
<th>Is there already an active blockchain consortium or trade partnership?</th>
<th>Is shared data proprietary and confidential?</th>
<th>Does data contain personal information?</th>
<th>Is trusted time-stamping, proof of existence or proof of provenance enough for your use case?</th>
<th>Does your solution require smart contracts?</th>
<th>Does your solution require near real-time processing or big data?</th>
<th>Do you require a high degree of control over blockchain governance?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Blockchain</td>
<td>Private Blockchain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

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
Very few institutions have the requisite skills to run bleeding-edge decentralized architecture and applications.

Souleima 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