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.

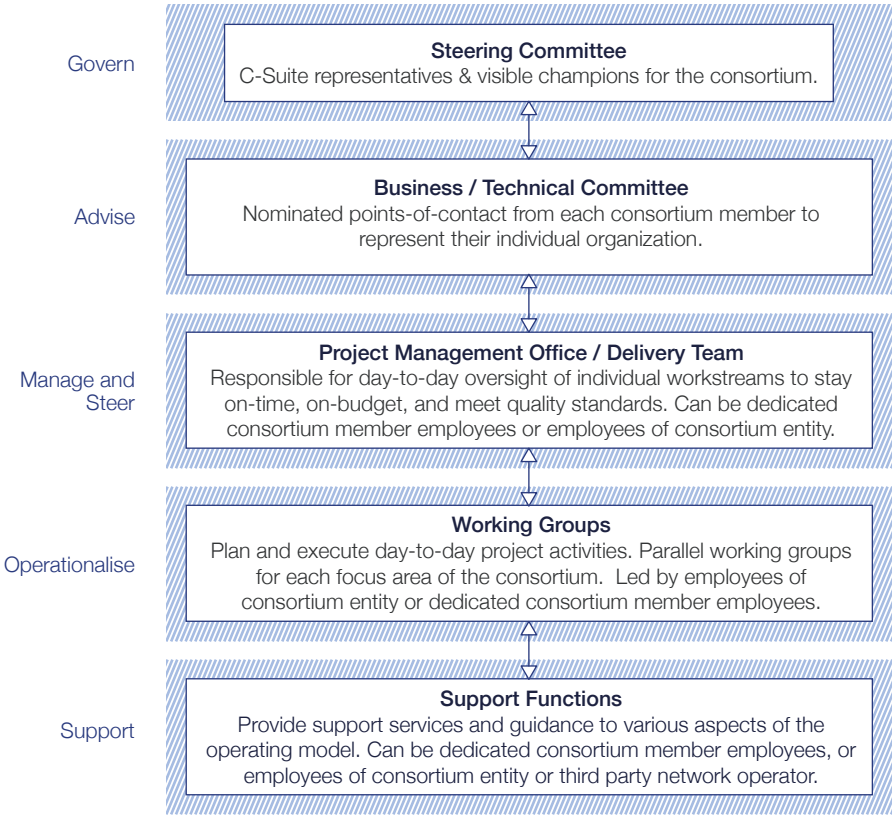



*Figure 4.1 – Example set of roles for a consortium*

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

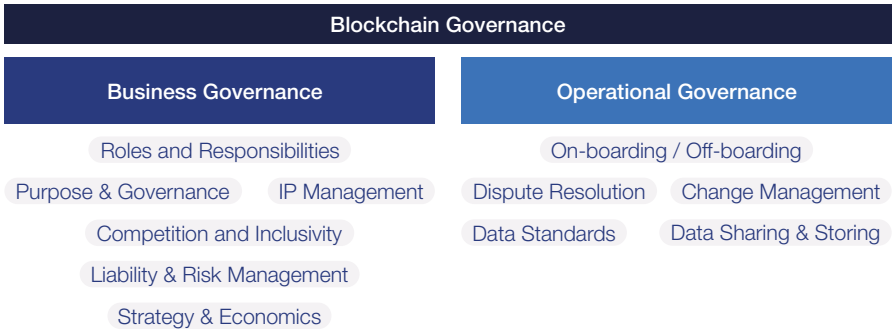



*Figure 4.2 – Two types of governance in a blockchain ecosystem and their key considerations*

# 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.

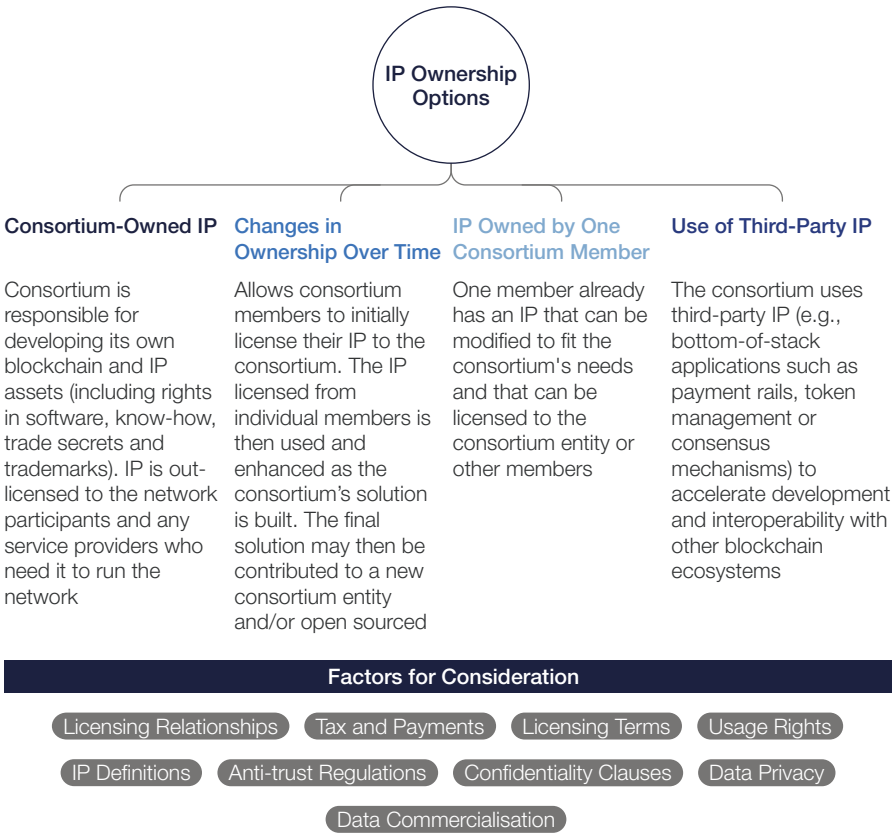



*Figure 4.3 – Overview of intellectual property ownership options*

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.

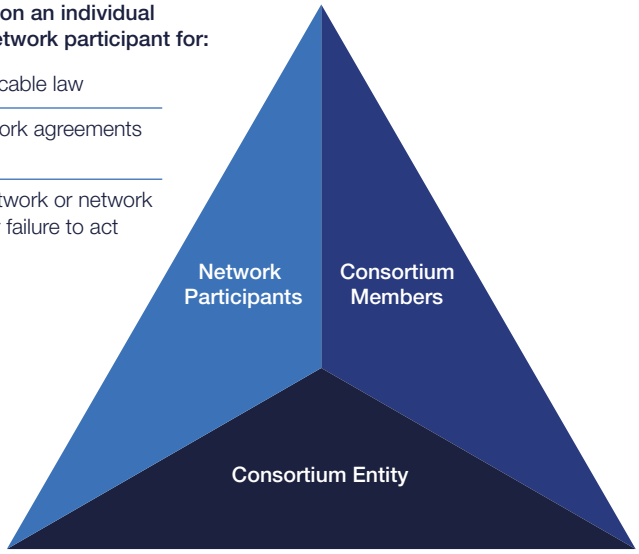
- **Liability of Network Participants:** Liability may be imposed on a blockchain network participant for its failure to comply with applicable law, network agreements or policies, or other damages caused to the network or network participants by its bad acts or failure to act. This type of liability 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?