MODULE

Legal and Regulatory Compliance

Overview

Focus Areas

Tools and Resources

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.

FOCUS AREAS

1. Common legal and regulatory issues with blockchain use

What are the most common legal and regulatory issues that arise when using blockchain technology?

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.

> *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

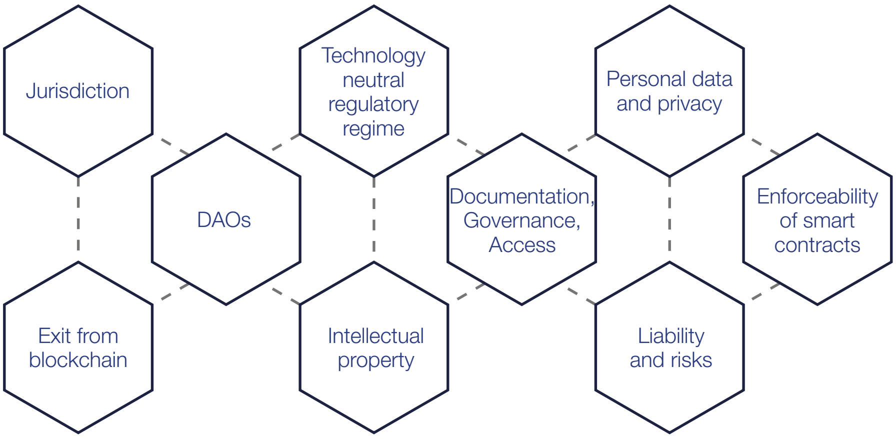
Jurisdiction
Technology neutral regulatory regime
Personal data and privacy
DAOs
Documentation, Governance, Access
Enforceability of smart contracts
Exit from blockchain
Intellectual property
Liability and risks

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.

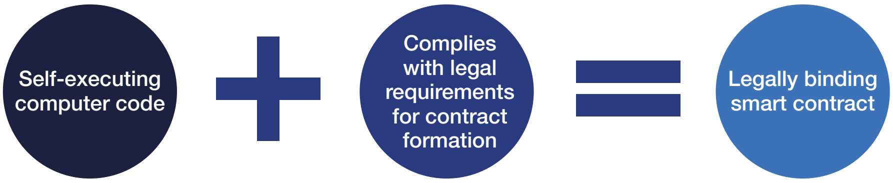
Self-executing computer code
Complies with legal requirements for contract formation
Legally binding smart contract

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.

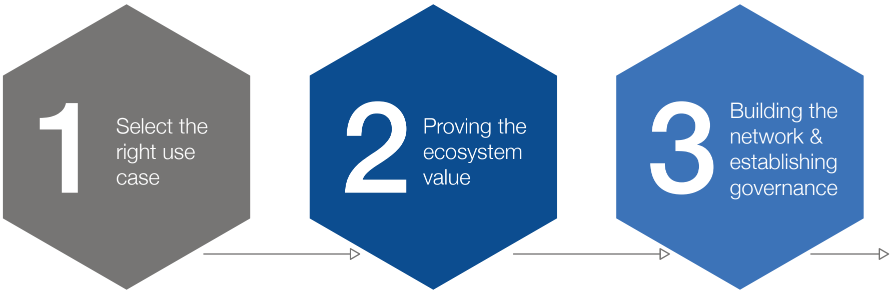
1
Select the right use case
2
Proving the ecosystem value
3
Building the network & establishing governance

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.

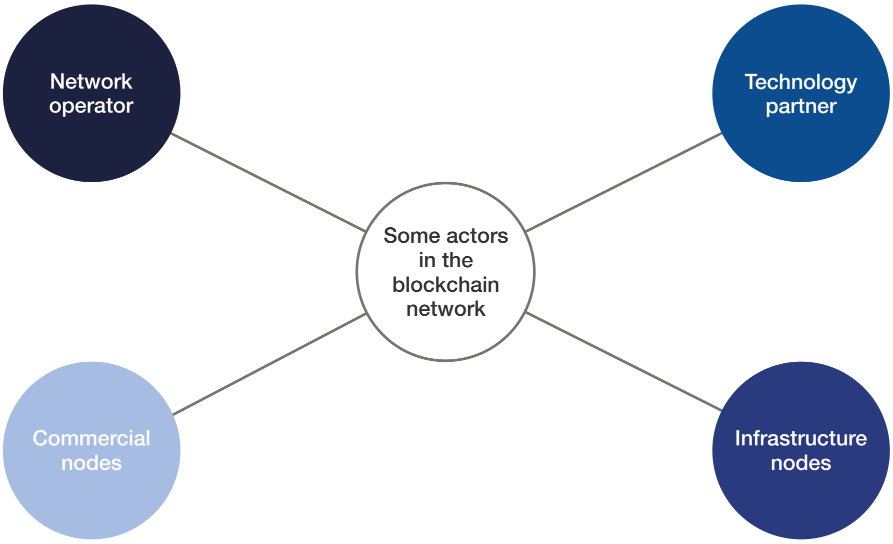

Figure 12.4 – Each participant to a blockchain network will have different and distinct legal responsibilities and concerns

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.