MODULE
Risk Factors

Overview

Focus Areas
1. Identifying blockchain-related risks

Tools and Resources
2. Risk identification checklist
Overview

New technologies carry potential downsides that need to be identified and managed. This is especially true when that technology is not merely an overlaying application but rather a core part of the organisation’s underlying IT infrastructure, as is often the case with blockchain.

The checklist included in this module covers some common potential risks and missteps associated with the deployment of blockchain technologies. Note, however, that this list is not meant to be exhaustive. With that in mind, project managers should view the information as generic guidance and work with relevant internal stakeholders, such as cybersecurity, internal audit, finance, compliance, legal, operations, and information technology teams to identify and prioritise risks that are significant for their deployment and develop mechanisms to manage the risks proactively.
What are the new risks associated with blockchain solution deployment?

As the organisation considers developing blockchain use cases, building proofs of concept, or scaling and deploying them in a production environment, the focus should not be diluted from catering for critical blockchain-related risks. Also, it is important to study if the organisation’s enterprise risk framework account for blockchain-specific risks.

Organisations should adopt a proactive approach in recognising new risks stemming from blockchain. Risk management should not be an afterthought; rather, it should be baked into the consideration set from the initial scoping and strategy phase of a blockchain project itself. While this list of potential risks might seem rather long and daunting, many of those pitfalls are ones your organisation is likely to face in the implementation of any other new technology as well. This checklist is designed to help organisations identify those risks that are significant for them to manage in order to drive the success of their blockchain initiative.

With a richer, more collective, and nuanced understanding of the opportunities and risks of blockchain, decision-makers will be better equipped to deploy systems that support their business needs while engendering trust.

---

**Figure 15.1 — The common risks can be sorted into five broad categories**

---

Michael Prokop, Blockchain Leader, Deloitte US Risk & Financial Advisory
Following is a checklist of potential risks and missteps often associated with blockchain deployments. While all blockchain use cases may not involve digital assets, this checklist also outlines risks pertaining to use cases that involve digital assets. Note that this list includes some of the prominent risks but is not meant to be exhaustive. The checklist items are neither ranked in order of priority nor equally weighted. The probability of risks manifesting into actual events are dependent on a range of factors.

Organisations should treat this checklist as generic guidance, and work with relevant internal stakeholders to identify, prioritise, and manage the risks relevant for their particular project proactively. The scope of this module doesn’t include guidance on enterprise risk management programs.

Also note that some of the specific risks mentioned below – for instance, Cybersecurity – are covered in greater detail in other modules in this toolkit. Be sure to refer to the modules dedicated to those particular issues as required by the needs of your project.

**Technology risks**

Effective development and deployment of blockchain-based solutions require the identification and addressing of a list of technological risks and challenges. The list includes privacy of data and transactions on the blockchain, security risks, performance-related limitations of the underlying blockchain platform, and integration-related issues with other enterprise systems.

**Data privacy risks**

- Could flaws in the blockchain-based system design lead to non-compliance with regulations or confidentiality agreements governing data? For instance, does the application involve personally identifiable information (PII) or confidential freight data? Do the requirements permit on-chain storage of data, or does it need to be stored off-chain?

- Does the application incorporate appropriate controls across the data lifecycle (e.g. collection/creation, storage, usage, and sharing/transfer as data is shared across the blockchain nodes)?

- Is there a risk of exposure of sensitive data due to inadequate policies, procedures, standards and guidelines for data encryption and obfuscation?

- Could incoming data potentially be inaccurate? If so, how to identify and correct errors?

- Is the blockchain system required to comply with “right to be forgotten” regulations? If so, is it in conflict with potential immutability of data on a blockchain?

For a detailed overview on protecting sensitive data and GDPR considerations, refer to the modules Data Protection and Personal Data Handling.
Performance-related risks

- What are the performance-related limitations of the underlying blockchain platform relative to the proposed blockchain use case (e.g. transaction throughput, settlement time, and availability)?
- Could the blockchain platform being used be suboptimal in terms of developer support and/or vendor lock-in?
- Is the selected blockchain protocol interoperable with other protocols required by the project?

For further details on blockchain protocol interoperability with other protocols, see the module Interoperability.

Security risks

Like other technology-enabled system, blockchain systems also need to be assessed for a variety of cyber security risks, such as confidentiality of users, security of private keys that secure access to digital assets, and endpoint protection. For further details on security risks, see the module Cybersecurity.

Integration-related risks

- Will there be integration issues with any mission-critical legacy systems used within the organisation?
- Are there standards available for integration of blockchain applications with enterprise systems?
- Is there appropriate integration testing at both the participating entities and the blockchain consortium entity?
- Could lack of common data architecture and data directory lead to enterprise systems feeding misaligned data to the blockchain system?

Operational risks

Implementation of blockchain-based applications, especially in a consortium of several organisations, is complex and involves addressing a number of operational risk issues such as governance, controls, auditability of blockchain transactions, and proof of assets ownership.

Governance and controls risks

- Is the legal entity structure of the blockchain consortium appropriate for tax implications and benefits of the participants?
- Could decision making within a consortium be suboptimal due to lack of proper structure and processes?
- Are there appropriate controls to mitigate conflicts stemming from decentralised accountability and shared ownership?
- Is there a lack of structure and policy in the consortium to onboard new members and accept new use cases?
- Have the smart contracts been audited to avoid incorrect implementation of business or legal arrangements?

For details on important governance items to consider, see the modules Consortium Formation and Consortium Governance.
Auditability Risks

- Is there enough technical experience or capability in conducting IT/technology audit of the blockchain application or platform?

- Will management and/or auditors be able to obtain information required to support financial statement disclosures?

- Will management be able to value digital assets in accordance with relevant accounting policies?

- Is there risk of a “hard fork” of the blockchain to modify past transactions, allow previously disallowed transactions, or bring about other structural changes to the blockchain?

Asset ownership risks

- Is there a risk of theft or loss of digital assets because of the irreversible nature of transactions in the blockchain protocol?

- How is the real-world change of ownership of assets made consistent with the change reflected on-chain?

- Can real-world identity be adequately confirmed to establish ownership of assets when required? Is there additional complexity due to the potential anonymity of participants on the blockchain protocol?

- Are adequate industry standards available for designing interoperable blockchain-based tokens?

For more detailed information on the questions covered in this section, see the module Financial Reporting and Controls.

Legal and regulatory risks

Blockchain as a technology may not be regulated, but applications built using blockchain technology will need to adhere to relevant regulations, such as the European Union’s General Data Protection Regulation (GDPR) relating to data protection and privacy. Legal and regulatory risks include uncertainty around cross-jurisdictional regulations, anti-trust violations, smart contract enforceability, anti-money laundering (AML) and know-your-customer (KYC), and intellectual property (IP) protection.

Legal and regulatory risks

- What are potential legal and regulatory risks and challenges to be anticipated with the deployment of this blockchain-based application? These may include uncertainty around cross-jurisdictional regulations, antitrust violations, smart contract enforceability, anti-money laundering (AML) and know-your-customer (KYC), and intellectual property (IP) protection.

- Could there be legal conflicts between consortium participants or consumers due to unclear legal liability in a permissioned network for cases such as data breach or smart contract errors?

- Is there risk stemming from regulatory uncertainties related to blockchains and related systems, especially across jurisdictions? Different data privacy and security regulations may apply in different jurisdictions around the world, for example.

For more details on important items to consider, see the module Legal and Regulatory Compliance.
Antitrust risks

- Are there safeguards against a blockchain consortium fixing or manipulating prices to gain competitive advantage?
- Could significant members within a blockchain consortium collude, leading to manipulation of services offered to smaller entities or preferential treatment of certain transactions?
- Are there antitrust risks arising from a certain blockchain consortium potentially pulling a significant share of the market into a closed ecosystem, thus causing disadvantage to competitors and consumers?
- Could a large blockchain consortium disfavour competitors, such as by excluding them, offering discounts to selected partners, or punishing competitors using alternative private currencies?

AML and KYC risks

- Is the blockchain system subject to compliance for AML or KYC regulations governing money service businesses?
- Are rigorous “know-your-supplier” checks required for compliance?
- Are there safeguards against payment being made to or from parties or countries subject to international sanctions, or with “politically exposed person” status?
- Could decentralised applications (Dapps) be deployed that accept or transmit value without necessary controls and compliance programs?
- Are requisite surveillance and monitoring controls implemented to detect and prevent money laundering activities?
- Are there additional risks due to anonymity of transactions and identities on the blockchain?

For more details on the legal and regulatory risks highlighted in this section, see the module Legal and Regulatory Compliance. More details on IP within consortia are available in the module Consortium Governance.

Financial risks

A common aim of blockchain deployment is to facilitate transfers of value. A variety of financial risks need to be considered while designing such blockchain applications, platforms, and infrastructure, such as potential for financial loss, transaction settlement finality, consortium funding-related risks, and intellectual property protection issues. In addition, there are a number of accounting and reporting challenges that should be considered when depending on blockchain-based applications for financial transactions and for information used in financial reporting.

Funding related risks

- Could funds run short to operate the consortium due to inappropriate choice of funding model? Will an initial coin offering (ICO), member fee structure, equity funding among partners, government grants, or some other funding source be used?
- Does the funding model of the consortium clearly define which participating entity will fund what?
Benefit related risks

- Has a revenue and other benefits sharing model been defined amongst entities of the blockchain consortium?

- Might participants be subject to financial loss due to absence of a trusted intermediary in blockchain-based business models to remedy errors or revert transactions? Could an alternative method of resolving disputes be created?

Internal control risks

- Is there a risk of financial loss due to the absence of a trusted intermediary in blockchain-based business models to remedy errors or revert transactions?

- Is there risk of financial loss due to incorrect representation of commercial contracts in the smart contract code?

Accounting and financial reporting risks

- If digital assets (e.g., cryptocurrency tokens) are used to transact in the blockchain system, is there a risk of incorrect accounting due to lack of standard guidance on accounting for digital assets?

- Is there a risk of misinterpretation of existing accounting literature while accounting for digital asset transactions?

- Could underlying rights and obligations associated with digital assets be potentially misunderstood?

- When the use case involves digital assets, is technical experience available to determine the fair value of digital assets?

- Is technical experience available to perform traditional financial reporting activities (e.g., complexity involved in reconciliation of internally held records with blockchain data)?

- Is there a risk of noncompliance due to continuing evolution of market and industry and changing requirements from regulators and standard setters?

- Is the management equipped to mitigate new and unforeseen forms of related party transactions or fraud schemes in financial reporting?

- Is there a mechanism to assess the beneficiaries of services provided by third parties who are obligated to remain objective of one or more entities of the blockchain network?

- Can unreliability of blockchain systems render blockchain data and digital assets inaccessible?

More details on the requirements of participants’ financial reporting as well as their external auditors in the module Financial Reporting and Controls.
Consortium intellectual property protection risks

- Does the blockchain consortium have an appropriate intellectual property (IP) management model? For instance, IP may be owned by the lead members, by a separate consortium legal entity, or be provided under open source license.

- Has an appropriate IP monetisation model been established?

- Could there be IP infringement within a consortium or by other consortia that member organisations participate in?

- Are there appropriate controls in place governing how members and third parties can contribute or enhance IP assets on the blockchain?

- If the application is based on a protocol that is open source – for instance, Bitcoin or Ethereum – is there a risk around non-compliance with underlying open source license terms?

- Could there be a lack of support from the members in the IP development or maintenance lifecycle?

- If the consortium legal entity should become insolvent, are there contingency plans regarding custody and maintenance of IP? For example, it could be that the IP is held in an escrow account in such a scenario.

For different IP ownership modules to consider, see focus area Intellectual property in the module Consortium Governance. For core legal and regulatory concerns and questions around IP in blockchain, see focus area Intellectual property in the module Legal and Regulatory Compliance.

Strategic risks

Adoption of blockchain technologies and business models is a strategic bet for organisations. It thus entails a range of strategic questions, such as defining the applicable value proposition, brand and reputation management, and handling change management.

Value proposition and incentive model

- What are the potential strategic risks and challenges to be anticipated with the deployment of the blockchain system?

- Has the blockchain’s (use case) value proposition been clearly communicated to participants? (e.g. secure transactions, operational savings, revenue, or other benefits)

- Is the network’s incentive model structured correctly to attract the desired participants or to get participants to commit the desired level of resources?

- Is there a risk of participants not willing to share sensitive information or to accept rules that may be counter to their individual interests?
Brand and reputational risks

- Could there be lawsuits from breach of contract, compromise of data, or other incidents if stakeholder expectations aren’t met?

- Who is responsible for external communications in the consortium? How will credit be attributed for accomplishments of joint efforts within the consortium?

Change management risks

- Have change management plans been formulated while accounting for potential future scenarios arising from blockchain-based business models?

- Is there clarity on workforce, talent, and role changes needed to make the blockchain-based business model effective?

- Are there appropriate measures in place to account for cultural changes within the consortium (e.g. shared accountability)? Is there a plan in place to communicate changes to the stakeholders within and outside the consortium legal entity?

- Has an exit strategy been defined for consortium participants who may wish to leave?

As you get to the end of this checklist, remember that while this list covers a wide array of blockchain-specific risks, it is not meant to include every possible risk. As such, it only outlines prominent risks. You should keep in mind a range of factors, many of which may be organisation- or project-specific, to evaluate the risk profile of your project.

So, how should your organisation think about managing the identified risks from a blockchain? The next step is to proactively address identified priority risks through a risk management framework.

The scope of this toolkit doesn’t include guidance on enterprise risk management programs. However, in the breakout box that follows there is a risk management framework reference that can serve as a foundation for formulating a plan appropriate for your specific organisation or project.
Reference to example of risk management framework:
The previous resources provided an overview and checklists of potential blockchain risk considerations. Organisations deploying a blockchain need to implement a risk management program to manage the relevant risks.

In this framework, risk management is orchestrated by three broad layers of responsibility – as shown below.

- Responsibility for risk governance, including strategic guidance and risk oversight, led by the consortium governance board
- Responsibility for risk infrastructure and management, including designing, implementing, and managing an effective risk program, led by consortium executive management
- Responsibility for risk ownership, including identifying, managing, measuring, monitoring, and reporting on specific risks, led by consortium functions