Blockchain: Identifying Risk on the Road to Distributed Ledgers

Blockchain technology, commonly expected to drive the next wave of digital infrastructure and process innovation, is rapidly developing into maturity. Five IT risk subdisciplines are of significant interest when embarking on blockchain-driven projects: cyber and information risk, architecture and design risk, IT compliance risk, third-party and vendor risk, and integration risk.

Blockchains allow multiple entities to achieve consensus on transaction data, i.e., a single version of the truth, without the need for a trusted central authority or notary function. The technology is a new data recording paradigm that lets multiple, potentially unknown or untrusted, networked entities share and append to digital ledgers. The integrity and confidentiality of the data in the digital ledgers are cryptographically guaranteed.

Three core features—immutability, transparency and autonomy—drive the technology’s ability to disrupt current products, processes and business models in a variety of industries. As the single version of the truth (i.e., immutable and up-to-date data) is available to all networked entities, the information asymmetry between the entities is reduced, and costly reconciliation activities between different information sources can be avoided. For example, a blockchain solution could provide a complete overview of a patient’s medical history—resulting in significant advantages in case of emergencies—instead of housing records among multiple health care institutions as is done now. Blockchain technology also ensures that the recording of data is in accordance with mutually agreed-on conditions, enabling disintermediation of central validating entities.

It is hard not to be fascinated by something so transformative. That being said, technology-driven opportunities to improve process efficiency and effectiveness rarely come without challenges and risk. This article aims to identify IT risk that should be considered during the development of a blockchain-driven solution and provides strategies to minimize this risk.

Cyber and Information Risk

Cyberattacks may compromise the confidentiality, integrity and availability of the data recorded in a blockchain. Technical vulnerabilities that can be exploited by hackers to cause loss or harm remain omnipresent. There is no evidence to indicate that this would be different for blockchain implementations. Additionally, the response strategies for dealing with cyberincidents are often inadequate. For example, in June 2016, the DAO, a

Filip Caron, Ph.D.
Is a faculty member at the KU Leuven Research Centre for Information Management and the Leuven Institute for Research on Information Systems (Belgium). He teaches graduate courses on business analysis and process management, and he is a researcher in the field of information security and governance, risk and compliance (GRC) practices. Caron is the author of more than 30 academic publications. He can be reached at Filip.Caron@kuleuven.be.
decentralized autonomous organization based on the Ethereum blockchain, suffered a cyberattack that deployed a combination of vulnerabilities, resulting in a loss of one third of its funds (approximately US $50 million). While a security patch had been proposed days before the attack, there were neither security teams nor procedures in place to act. Instead, the proposed patch needed to be adopted through a formal voting process with 23,000 eligible voters, as specified in the mutually agreed-on conditions.

Security weaknesses can also be found at the endpoints writing to a blockchain application and securely storing the cryptographic keys that are used as digital signatures. The cyberincidents at Bitcoin exchanges Mt.Gox (US $450 million lost) and Bitfinex (US $72 million lost) are notable examples of cyberattacks that centered on compromising the IT infrastructures at endpoints of the network.

Cyber security measures that could assist in mitigating this risk include:

- Conducting extensive penetration tests on the blockchain application.
- Implementing adequate endpoint security that includes the design, implementation and maintenance of controls that ensure a secure delivery of services (e.g., preventive controls such as access control and firewalls) and measures to identify the occurrence of an incident (e.g., network and system monitoring). An overview of appropriate controls can be found in COBIT® 5, the International Organization for Standardization (ISO) 27000 series, and the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).
- Instigating incident response processes that focus on incident analysis, containment, eradication and recovery. In preparing these processes, organizations should also consider communication policies and arrangements with specialized cyberemergency response teams.

Details on effective incident response strategies can be found in NIST Special Publication (SP) 800-61 Revision 2.

Architecture and Design Risk

A broad variety of both technical and organizational design decisions must be made during the development of a blockchain solution. These design choices may have a significant impact on the performance of the solution and, consequently, on the achievement of the business objectives.

Technical designs for blockchain solutions may not be aligned with functional requirements. The selection of a consensus protocol, used for validating proposed additions to a blockchain-based ledger, is an often-cited design choice that impacts operational capacity. While VISA can process approximately 56,000 transactions per second (reported in 2015), Bitcoin’s consensus protocol limits the payment system to only seven transactions per second.

In a “code is law” environment, the completeness of the coded rule set is of primary importance. Incomplete rule sets may allow for undesirable, but not forbidden, user behavior. Incentives for strategically voting, which prevents voting based on sincere preference, have been exposed in the DAO’s code and could have a significant impact on the investment decisions of the organization.
Approaches that could partially mitigate architecture and design risk include:

- Establishing requirements and engineering processes comprising the effective elicitation, analysis and prioritization of business functional, technical and compliance requirements. Formal confirmation and a timely update of the requirements specifications are considered best practices. Guidance can be found in the COBIT 5 specification for the Build, Acquire and Implement (BAI) domain’s BAI02 Manage requirements definition process.
- Adopting a security-by-design focus in the development of the blockchain solution. Technical measures include restricting access to the blockchain (i.e., creating a permissioned blockchain) and establishing role differentiation (e.g., supporting the use of trusted record validators or asset registrars). Business measures could include strict onboarding processes and ensuring geographical spread.
- Conducting strict code reviews and acceptance tests for the blockchain solutions
- Assessing technological evolutions that might support or impact the achievement of the business objectives
- Setting up formal governance structures and procedures to deal with the strategic long-term evolution (e.g., a technology renewal or a revision of the encoded rules) and incidents that need to be resolved in the short term

IT Compliance Risk

As regulations proliferate and stakeholders’ expectations increase, there is an increased risk of violating regulations and industry standards that could directly impact the participants’ financial position, organization and reputation. Compliance challenges regarding the consensus mechanisms and information security have already been identified. The financial industry has strict requirements for the absolute finality of a transaction, as specified in the Settlement Finality Directive (SFD). Distributed consensus protocols that are based on computational work, such as the proof-of-work protocol underlying bitcoin, typically provide only probabilistic finality. Technically, transactions are never truly final as there

Compliance challenges regarding the consensus mechanisms and information security have already been identified.

Organizational design decisions include access restrictions and role differentiation. Restricting access to the blockchain solution to a preselected, trusted set of nodes (i.e., permitted blockchains) can have important advantages such as working with trusted participants, more efficient consensus protocols and greater levels of privacy. Permitted blockchains are better suited for establishing formal governance structures and procedures to react in case of incidents and to actively manage the encoded rules. In contrast, public blockchains are open to everyone to participate in and review the encoded rules. Therefore, public blockchains tend to lower the barrier to participation and can protect users against developers willing to take control.

Differentiating the roles and responsibilities of the participants, (e.g., only allowing a trusted authority to perform the initial registration of real estate in a blockchain-based land registry, might be desirable. Several authors also indicated that blockchain might not be the most appropriate technology for a setup in which all participants are IT systems operated by the same real-world entity.7
is always a possibility that a longer chain is created that does not include the block of the transaction. However, as more blocks are added, it becomes less economically viable and/or computationally possible. It remains to be tested whether probabilistic finality complies with the SFD requirements.

A wide variety of industry-specific and generally applicable regulations regarding the confidentiality, integrity and availability of data have been put in place. In the US, blockchain solutions for sharing and recording patient records are subject to the US Health Insurance Portability and Accountability Act (HIPAA), whereas in Europe, requirements for personal data are strengthened and unified by the General Data Protection Regulation (GDPR). The GDPR includes, among others, requirements for the export of personal data outside the European Union.

The variety of regulations may make it difficult to determine the appropriate regulations for the blockchain solution as participants and copies of potentially sensitive data ledgers may be dispersed over multiple jurisdictions with varying regulatory objectives.

Measures for dealing with IT compliance risk as it applies to blockchain include:

• Reviewing broader regulatory requirements and standards, including both industry-specific and generally applicable rules
• Monitoring regulatory developments and evolutions in the standard-setting processes
• Engaging with the relevant regulators, preferably at an early stage of the design phase, to ensure adherence to policy objectives. Some authorities have set up specific frameworks (e.g., the regulatory sandboxes of the UK’s Financial Conduct Authority) that allow innovators in the financial industry to test their ideas without immediately incurring all the normal regulatory consequences.

• Defining restrictions on access to the blockchain solution (e.g., only allowing identified and vetted partners in order to comply with anti-money laundering regulations) and restricting the allowable locations for participants who maintain copies of the ledgers to avoid noncompliance in specific jurisdictions

Third-Party and Vendor Risk

While the bitcoin peer-to-peer electronic cash system has been designed to operate without trusted third parties, most blockchain projects are developed in the context of a strategic partnership with a blockchain software vendor. Associated with these strategic partnerships is another type of third-party risk—the risk that the vendor will not be able to deliver reliable and secure services.

It is not uncommon that the blockchain software vendor is a start-up or scale-up organization. While start-ups may be successful, many start-ups may have strategic evolution issues, regulatory compliance issues, unstable financial conditions and/or lack proper human resources. For example, in mid-2015, Ripple, a start-up blockchain software vendor, announced that it would discontinue the development of its Codius platform.9 In the same year, Ripple was fined by the US Department of the Treasury for violating several regulatory requirements, including failing to implement adequate anti-money laundering programs into its products.9 Ripple has since agreed to remedial actions. Financial risk is also a frequent concern. Many blockchain start-ups fail due to a lack of funding.10 Finally, attracting blockchain experts—and avoiding attrition—can be challenging for start-ups.11

Actions for managing risk associated with blockchain software vendors include:

• Implementing risk management strategies that cover the continuous life cycle of third-
Further, integration issues might arise when reconciliation between multiple blockchain-based ledger systems is needed. For example, in its utopian view of capital markets using blockchains, Euroclear flags the need for synchronization between ledgers holding different asset types (e.g., cash and derivatives). In the same report, Euroclear argues that certain participants in the capital market could be disintermediated, which would impact the activities and business processes of the remaining financial institutions.

To mitigate integration risk, an organization might:

- Focus on developing repeatable testing procedures and extensive testing plans, in addition to stressing the importance of requirements engineering
- Manage organizational change enablement as detailed in COBIT’s BAI05 Manage organisational change enablement process to prepare and commit stakeholders for business change
- Opt, where possible, for generally accepted blockchain technology and interface standards

Integration Risk

When organizations face technological changes that could disrupt their products, processes and business models, their managers may be tempted to react hastily and push for a premature technology renewal. These organizations risk that their technology renewal strategy will be inadequate, either due to a lack of integration with existing systems (technology perspective) or business processes that are not appropriately adapted (business perspective). A Deutsche Bank research analyst concluded that traditional banks’ struggle with legacy systems is a major inhibitor of technological innovation. Interfaces for integrating new technologies in existing systems cannot be developed within an acceptable time frame. Other proposals, (e.g., the Swedish Lantmäteriet’s proposal for a real estate transaction system) stretch the integration requirements even beyond the internal systems.
Conclusion

An analysis of blockchain solution development risk reveals the potential benefits of establishing formal governance structures and procedures. While this finding contradicts the base premise for which blockchain was pioneered in a cryptocurrency setting, it may prove invaluable for risk prevention and recovery.

As with blockchain technology, the regulatory framework around it has not yet fully matured, which elevates the likelihood of compliance risk materialization. Furthermore, permitted blockchains with strict onboarding and effective access management might be more appropriate to satisfy the business, technical, security and compliance requirements for contemporary ledger solutions.

Endnotes

6 Mark, D.; V. Zamfir; E. G. Gun Sirer; A Call for a Temporary Moratorium on “The DAO,” 26 May 2016, https://docs.google.com/document/d/10kTyCmGPhvZy94F7VWySdQ4lsBacR2dUgGTTv98C40/edit#