Deloitte.

An internal auditor's guide to blockchain

Risk considerations in blockchain technology

GET STARTED

Contents

Overview

Technology-based solutions work best when they are designed to solve real-world problems. In a world where swipe left or right and one-click dominate the market, there is a genuine desire to streamline complex business problems. The complexity of business transactions and a potential lack of trust between parties create opportunities for innovative solutions. One such innovation, *blockchain technology*, also called distributed ledger technology, has experienced explosive growth.

Blockchain technology-based new proofs of concept (PoC) continue to develop in many industries, and a certain number of them are close to advancing from the pilot phase to implementation. As blockchain technology continues to evolve and expand on its promise to simplify transactional complexities, it also gives rise to previously unforeseen risks for businesses. As organizations consider implementing blockchain-based solutions, internal auditors need to assess these emerging risks and retroactively advise management on ways to implement appropriate safeguards.

For an introduction to blockchain for internal auditors, read part one of this series.[1] We introduced the concept of blockchain, peer-to-peer networks, and asymmetric key cryptography consensus mechanism. In addition, we provided an overview of cryptocurrencies, smart contracts, tokens, and initial coin offerings. We also discussed key features of different types of blockchains and how blockchain technology works.

[1] "An internal auditor's guide to auditing blockchain: Blurring the line between physical and digital," Deloitte Perspectives, accessed May 2019.

Overview (cont.)

In part 2, we will discuss risk considerations related to implementing blockchain technology through an internal audit lens. As a third line of defense, an internal audit is entrusted with the responsibility of providing the board and its management with comprehensive assurance while maintaining its independence and objectivity within the organization.

Predictions

A recent article published by Gartner made the following blockchain predictions:[2]

- By 2023, most of the technical challenges with blockchain will have been resolved.
- Enterprises that fail to conduct sufficient scenario planning and delay consideration of blockchain's decentralization and tokenization risk being disintermediated or failing to seize the greatest business value from blockchain.
- Leaders who want to make good investments in blockchain need a clear model of the blockchain universe, its evolution, and the various aspects of associated technologies and their importance. They will also need to understand the impact of these capabilities on the enterprise's operating model initially and its business models over time.

[2] David Furlonger and Rajesh Kandaswamy, "Blockchain technology spectrum: A Gartner theme insight report," Gartner, October 8, 2018.

Case in point

While trust is a key principle of blockchain, the technology is not free from other risks. As always, internal auditors must think through the lens of "what could go wrong" when performing an assessment of a blockchain-based solution being considered by the business for implementation.

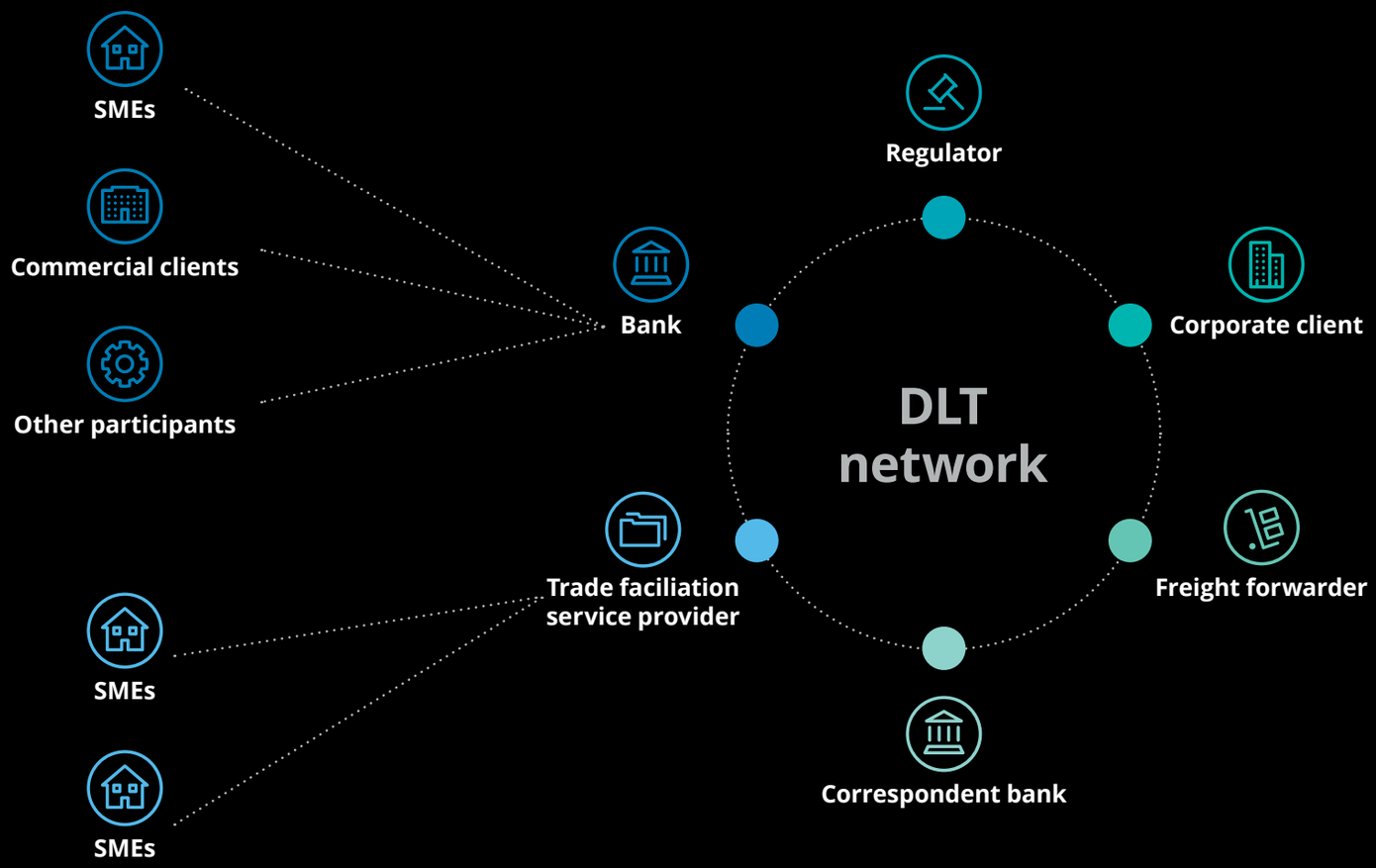
We will illustrate specific risk considerations to bring blockchain concepts to life by using a fictitious example of an internal audit department performing a preimplementation review of a blockchain-based solution being considered by a bank for implementation in its international trade finance (ITF) department (see figure 1 on page 6).

Distributed Bank, LLC (DBL) is a retail bank with global operations. During the annual planning meeting, the chief audit executive (CAE) "notified" internal audit leadership that the bank's ITF department was currently building a PoC using a blockchain technology-based solution. The proposed solution would create a consortium of participants in a blockchain that would include corporate clients (buyers and suppliers), correspondent banks, trade-facilitation service providers, and, potentially, regulators. The preimplementation review of the proposed solution was scoped in as part of the internal audit plan. The CAE assigned the preimplementation review to John Block. Before kicking off his review, John decided to enhance his understanding of blockchain application for ITF by watching a short video.[3] John learned that as goods move from the seller to the buyer, ITF operations enable the transfer of monetary payments. They also enable companies to be paid faster using "factoring," which involves the bank paying the seller of goods before the buyer of the goods makes the payment. Factoring involves multiple risk factors for all parties, including nonpayment, duplicate payment misrepresentation, and even fraud. The proposed solution should lead to more efficiency in the process.

[3] "Deloitte Mercury Trade Finance Overview," Deloitte Blockchain video, posted October 14, 2016.

Case in point (cont.)

Figure 1. Use of blockchain technology in ITF



Case in point (cont.)

How blockchain technology can benefit ITF participants:

BANKS

- Increased operational efficiencies
- Data privacy protection through permissioned access
- Ability to provide new value-added services
- Shared platform with other stakeholders, ensuring greater transparency and reduced manual reconciliation
- Prevention of double financing or abuse of transactions, resulting in more efficient capital allocation

SME (BUYERS/SELLERS)/SME/CORPORATE CLIENTS/ COMMERCIAL CLIENTS/OTHER PARTICIPANTS

- Mitigation of payment risk
- Clear oversight of delivery processes
- Reduced costs by digitizing paper-based documents
- Smart contract-triggered financing
- Potential to disintermediate "trusted third parties," as stakeholders can connect directly on the platform and access data relating to transactions

FREIGHT FORWARDERS

- Digital handling of trade documents
- Instant communication between parties
- Faster payment due to reduced processing time

REGULATORS

- Real-time oversight of processes
- Immutable ledger of transactions relating to transfer of assets
- Real-time information feed
- Improved credit rating information

Risk considerations

For the purpose of his review, John conducted a series of walk-throughs with key stakeholders at the bank. He held discussions with the bank's ITF operations, information security (IS), information technology (IT) services, treasury, legal, and compliance departments. His primary focus was to assess operational, reputational, legal, contractual, and regulatory risks associated with the proposed blockchain solution. Upon completion of his review, John submitted the report to DBL's CAE. In his report, he highlighted both the potential benefits as well as the risks associated with the blockchain-based solutions.

John acknowledged that blockchain technology has an advantage over traditional systems as it can operate in the absence of trust among the participants. Also, the blockchain data structure enables the creation of an encrypted digital ledger of transactions that can be distributed securely among a digital network of parties. The buyers, sellers, shippers, correspondent banks, and other stakeholders such as regulators, can access and update the common information on a shared platform. Depending on the degree of integration and the requirements of privacy, the blockchain technology may eliminate the need for stakeholders to maintain their own databases for documents related to a transaction (for example, letters of credit, bills of lading, and invoices).

While there are numerous advantages to blockchain technology for ITF, its implementation introduces new and specific risks[4] that may not exist in more traditional centralized systems.

John's report identified the following specific risk considerations in the implementation of blockchain technology. While John's report was based on an assessment of blockchain technology for ITF (as illustrated through this example), the risks identified are common to permissioned blockchains in general.

[4] "Blockchain risk management—Risk functions need to play an active role in shaping blockchain strategy," Deloitte Perspectives, accessed May 2019.

Risk considerations (cont.)

Data confidentiality risks

Based on the walk-through John performed with the departmental heads of the IS and IT groups, he noted that the consensus mechanism of permissioned blockchain enables all participants within the network to have access to certain information. While the information can be restricted and encrypted, it can still be vulnerable to inadvertent exposure. Therefore, participating organizations need to address the risks related to data privacy and confidentiality to ensure that any personally identifiable information (PII) is not compromised or stolen. In the ITF example, diverse participants such as the buyers, sellers, banks, freight forwarders, and regulators will require access to sensitive customer information and transaction records, which will have to be protected by appropriately defined rules, regulations, and protocols to ensure privacy and compliance with applicable jurisdictions.

While blockchain encrypts key information, such as buyer and seller names, and addresses to prevent unintentional information leakage, this does not mean that the data and associated metadata are inherently secure. For example, "Seller A" transacts with the bank to arrange for preshipment financing. As part of the transaction, "Seller A" also engages with "Freight entity X." The details of this transaction may be encrypted so that "Buyer B" could not view the confidential transaction details, but would still be able to see that a specific network participant engaged in a transaction with the bank and freight company.

On its own, this information is not meaningful. However, if aggregated with thousands of other transactions, the data might provide pertinent information to "Buyer B" that was not intended in the design of the application.

While network participants will have multiple modes to interact with a distributed ledger, companies need to think of risks associated with data sharing among participants of the value chain. As such, the buyers, sellers, regulators, freight forwarders, and correspondent banks have different information-sharing requirements that will need to be considered in the design of the blockchain consortium.

Risk considerations (cont.)

Private key management risk

After meeting with the IS and IT groups, John learned that for a permissioned blockchain (such as the technology used in ITF), each participant on the network is given at least one private key that is used to authorize and sign transactions. For example, if the blockchain consortium admits a new correspondent bank (for example, “Bank Y”), part of the onboarding of that entity would be to grant a private key. This private key is then used by “Bank Y” to sign future transactions. This provides assurance to the other network participants that this correspondent bank has duly authorized the transaction. If this bank loses its private key material, a bad actor may be able to sign transactions on behalf of “Bank Y.” As a result, the bad actor could agree to unauthorized transactions on behalf of “Bank Y” and/or forge documents that appear to be legitimate to other members in the blockchain consortium.

Loss of private key material could cause significant harm to other network participants. Therefore, the safety and security of the private key of each participant is critical for the success of blockchain.

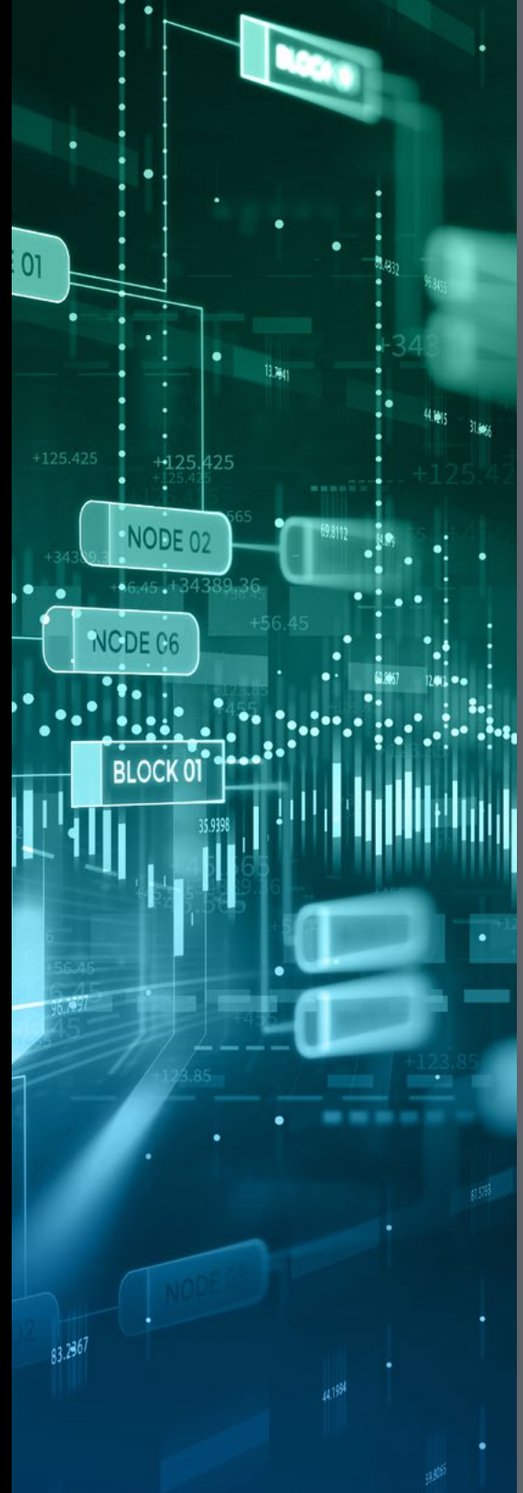
Risk considerations (cont.)

Consensus and governance risks

John also identified consensus and governance as one of the key risks in permission blockchain. John defined consensus as a process of agreeing on one continuous version of a blockchain ledger. Further, he defined governance as the process of ongoing maintenance and enhancement of protocols and code changes. In his report, John stated that "Consensus and governance go together through a combination of people and code execution. The primary risk regarding consensus and governance is related to members not agreeing to a change of a protocol leading to a dispute and resolution process, which can be lengthy. Further, dispute resolution requires a comprehensive framework to ensure orderly operation of the consortium, especially given the global nature of the technology. It also encompasses a risk that settlement can't be relied upon as a legally defined moment because of the possibility that a transaction, block of transactions, or the blockchain ledger could eventually be rewritten."

John believed that as blockchain involves an arrangement of sharing information with multiple stakeholders, companies need to evaluate the following:

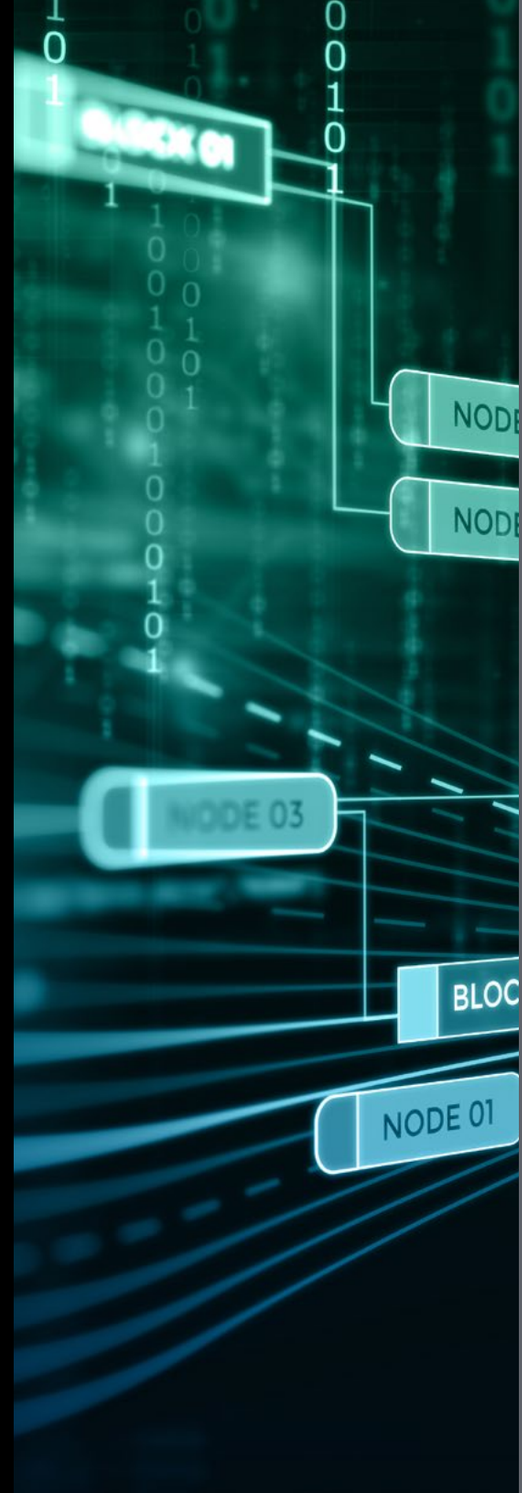
- The type of governance structure that best serves the participants in the consortium
- Support for sound decision-making, risk management, change, incident, and emergency-response management should any alterations need to be made in the consensus mechanism or governance decisions



Risk considerations (cont.)

Integration risks

John noted in his report that, “Entities seeking to integrate blockchain need to decide if integration of the technology will be performed to process transactions with their business partners or become a subledger that replaces a current system supporting a business process. Depending on the path chosen, different risks become relevant. In the case of trade finance, the business may choose to integrate existing systems with the distributed ledger rather than use the system as a subledger to process transactions. This gives the business more visibility into a transaction life cycle but does not warrant replacement of the core systems responsible for the trade finance business process.”



Risk considerations (cont.)

Scalability risk

In his report, John also indicated that with the expansion of business, the technology supporting the business should have the capacity to manage a growing volume of data over time. He stated, "While blockchain has an inherent characteristic of decentralization, this feature results in the increasing participation of every single node, which stores fully immutable copies of the ledger. Expanding ledgers eventually leads to a need for continuous enhancement of storage capacity. Additionally, the need arises for computing power without the usage of blockchain platforms to enable culling of aged transaction details to preserve storage. In a traditional database system, with expanding business data volume, one can simply add servers to the existing hardware to accommodate and store additional data. A decentralized blockchain environment, where every node must validate every transaction, would require additional computational power and energy consumption. This might affect transaction processing speed along with an increased cost and latency associated with processing a transaction.

In a blockchain environment, every recordable transaction requires peer-to-peer verification, which can become time consuming depending on the number of blocks involved and their geographic distribution. For ITF, given the volume of trade finance transactions globally, it is easy to predict that scalability, geographic distribution, and processing power could become relevant risks in a short period of time."

Risk considerations (cont.)

IT operations risk

John noted that while integrating blockchain into an existing infrastructure will result in companies dealing with issues related to speed, scalability, and interface with legacy systems, it will further require revisions to existing policies and procedures to reflect the modified processing environment. John states in his report, “For ITF, operational concerns may also include handling fluctuations in payment, clearing, and settlement transaction volumes. Because blockchain is a nascent technology, companies will need to retrain their staff to stay abreast of operational risk resulting from failures associated with internal procedures, people, and systems as well as be agile in adapting to rapid technological changes.”

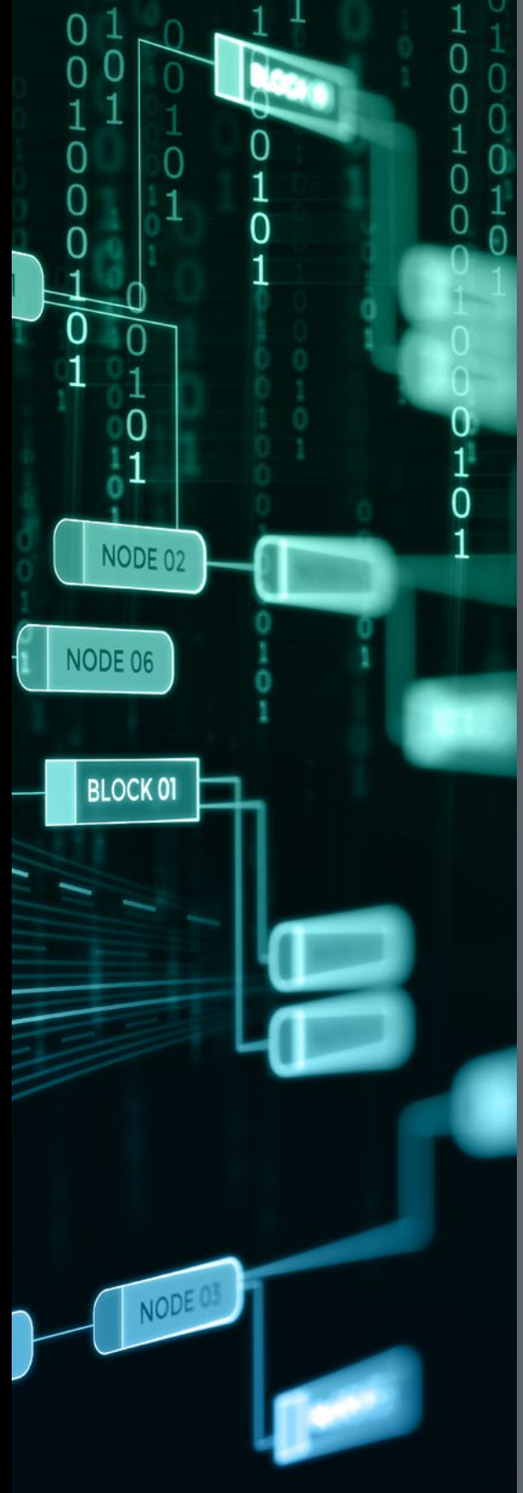
Risk considerations (cont.)

Business and regulatory risks

John performed a detailed walk-through with the legal and compliance team to understand the impact of smart contracts. John noted that since blockchain and smart contracts are nascent technologies and still in the process of maturing, there is not yet a generally accepted global regulatory framework in place. This makes it obligatory that parties agree on mutually accepted terms and comply with current laws and regulations.

In the case of ITF, if a buyer in Denmark is planning to buy 5,000 tires from a seller in Hong Kong, it must be ensured that the network's smart contracts are able to handle exceptions and that the terms of the contracts are not explicitly void in the respective countries. Smart contracts should be able to handle exceptional situations such as loss or damage of goods during transit. Further, the participating parties need to agree on the arbitration clause and how disputes can be resolved.

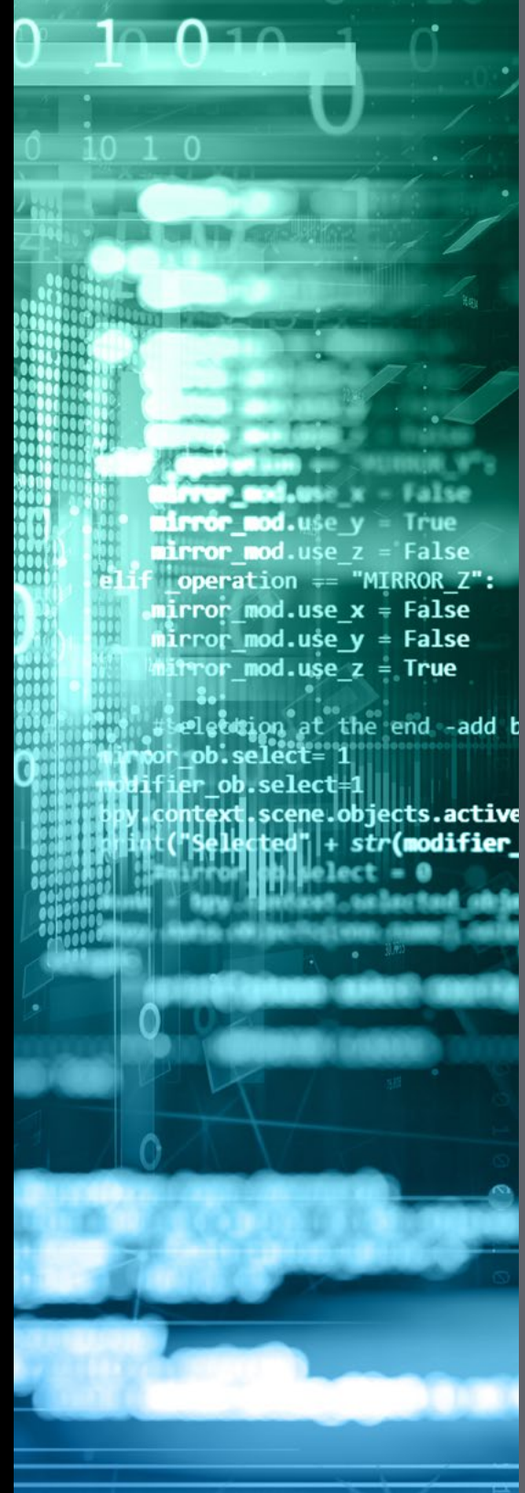
John further stated, "Smart contracts must be codified and tested for compliance with the trade, economic, legal, and regulatory environment at every stage of the journey between seller and buyer. In terms of regulatory issues, contracts need to be designed with adequate change management policies that allow for an agile yet secure response to changes in the regulatory framework. It is imperative to mention that mature smart contracts may allow for straight-through processing that does rely on external systems and therefore may significantly enhance existing business processes."



Risk considerations (cont.)

Code development risks

In his report, John noted that "Every new technology has teething issues. Therefore, solutions need to be tested to gain assurance that the systems are working as intended. The proper level of assurance requires companies to check their own code for bugs before, during, and after implementation. The risk of a weak method of encryption without the expected level of security can result in inadvertent exposure of data stored on the network. Companies need to ensure that the blockchain network, including smart contracts, is kept current to mitigate code and cryptography risks."



Risk considerations (cont.)

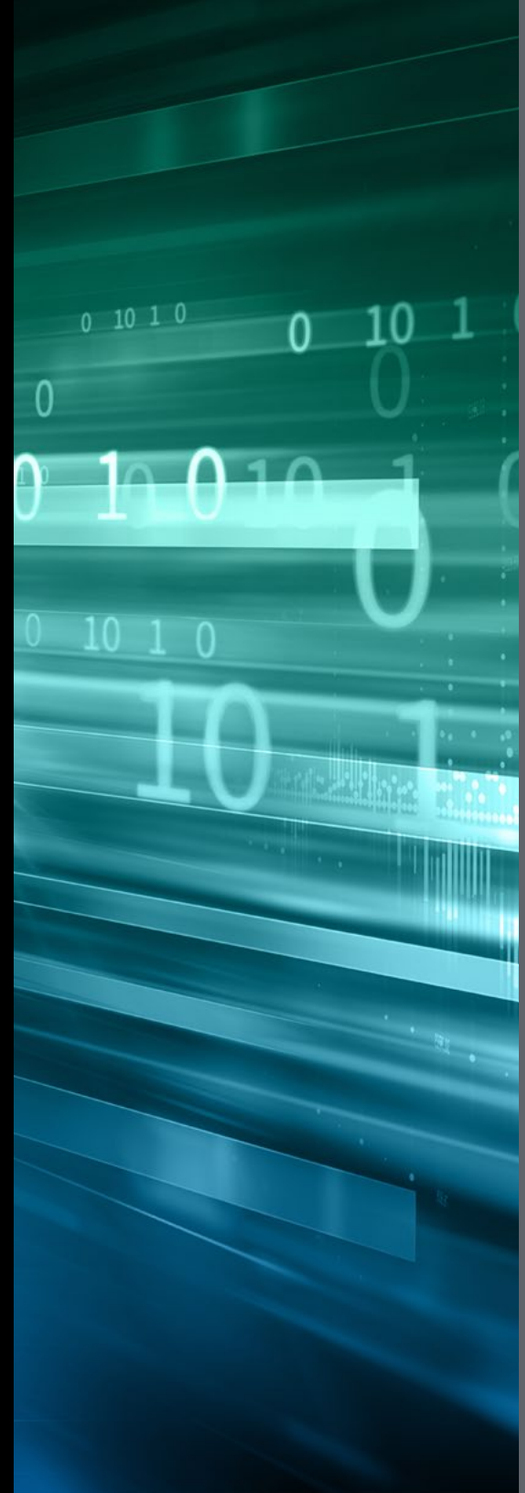
Business continuity and disaster recovery risks

John noted that "Blockchain technologies are generally resilient due to the redundancy resulting from the distributed nature of the technology. However, the business processes built on blockchains may be vulnerable to technology and operational failures as well as cyberattacks. Companies implementing blockchain technology need to have an enterprise-wide business continuity plan and governance framework installed to help mitigate such risks. Since blockchain solutions have a potential to shorten the duration of many business processes, business continuity plans should account for a shorter incident response and recovery time. Companies need to consider how participation in a blockchain network may affect their business continuity plans and whether the network has appropriate measures in place to effectively recover from a significant disruption."

Conclusion

Distributed ledger technology comes with the potential to transform current business processes by improving transparency across the entire chain, removing duplication of efforts, offering transactional immutability, providing resilience to censorship, and creating an environment in which trust is removed as a risk factor in value transfer. While the benefits are distinct for this technology, they come with specific business, technological, and operational risks. Before an organization adopts this new technology, it should ensure that the associated risks are duly assessed and addressed.

One of the specific strategic advantages that internal auditors have is their knowledge of the organization and its various business functions. This broad view places internal auditors in a favorable position to effectively assess organizational governance, risk, and control environments. The Institute of Internal Auditor's professional practice framework specifies that internal auditors must possess the knowledge and skills and other competence in the performance of internal audit services.[5] While internal auditors are competent with traditional risks and controls, they should continuously enhance their skills in emerging technologies such as blockchain to remain effective at not only delivering assurance but advising on critical business issues and anticipating risk.



[5] 1210—Proficiency—International standards for the professional practice for internal auditing (Standards—effective 2017), The Institute of Internal Auditors, accessed May 2019.

Contact us

Sandy Pundmann
US Managing Partner, Internal Audit
Deloitte & Touche LLP
spundmann@deloitte.com

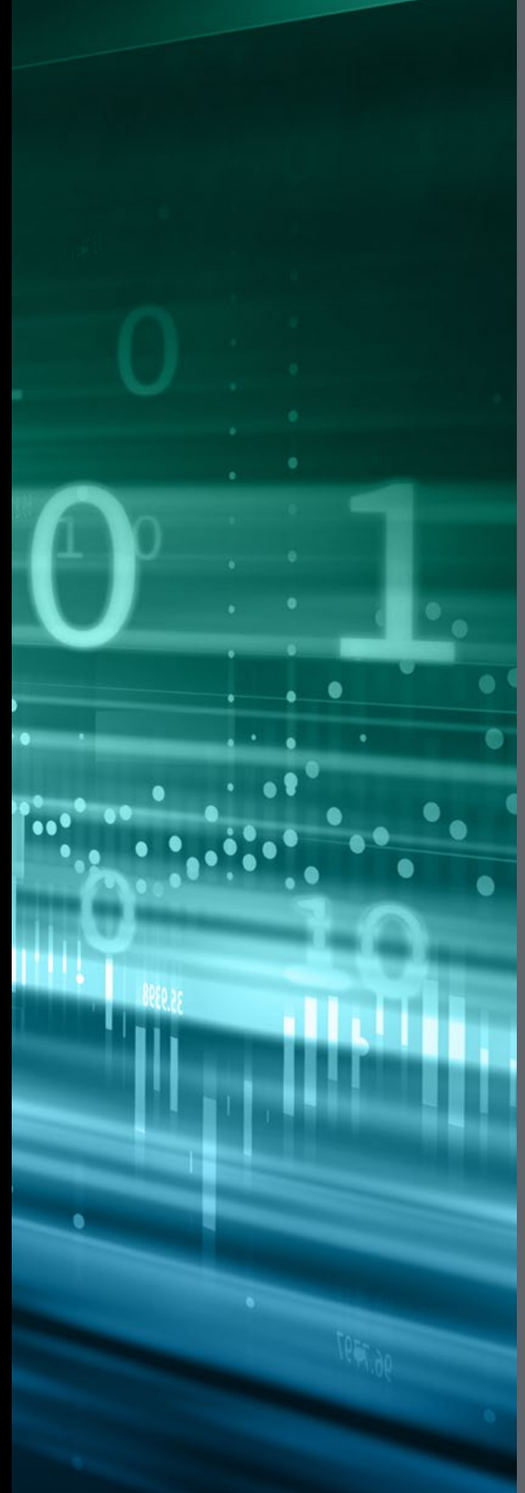
Adam Regelbrugge
Partner, Internal Audit
Deloitte & Touche LLP
aregelbrugge@deloitte.com

Manu Mankad
Managing Director, Internal Audit
Deloitte & Touche LLP
mmankad@deloitte.com

Seth Connors
Senior Manager and
Deloitte Blockchain Fellow
Deloitte & Touche LLP
sconnors@deloitte.com

Amitesh Joshi
Specialist Leader, Internal Audit
Deloitte & Touche LLP
amjoshi@deloitte.com

Yogeeta Raisinghani
Manager, Internal Audit
Deloitte & Touche LLP
yoraisinghani@deloitte.com



Deloitte.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

Copyright © 2019 Deloitte Development LLC. All rights reserved.