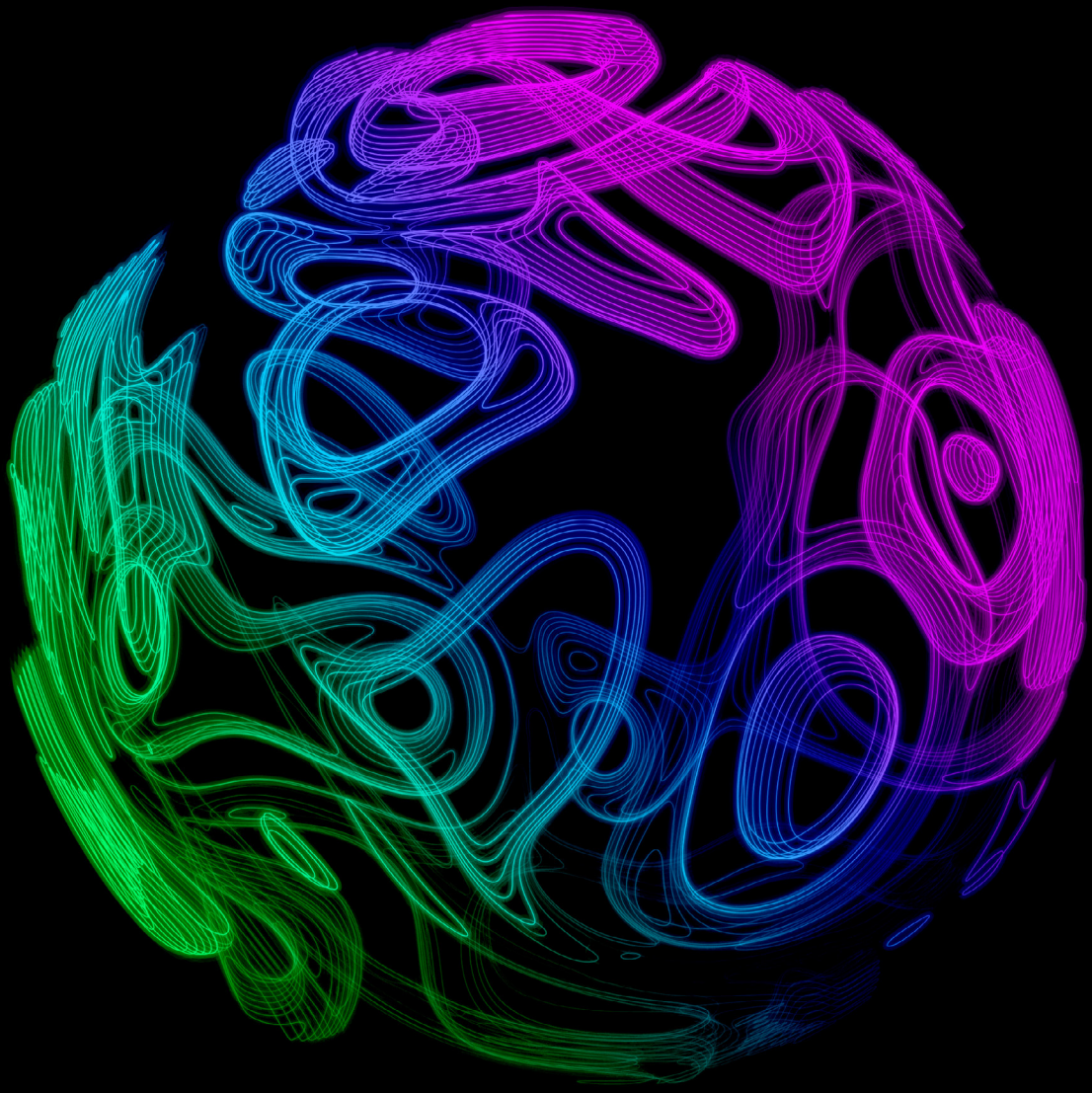
Deloitte.



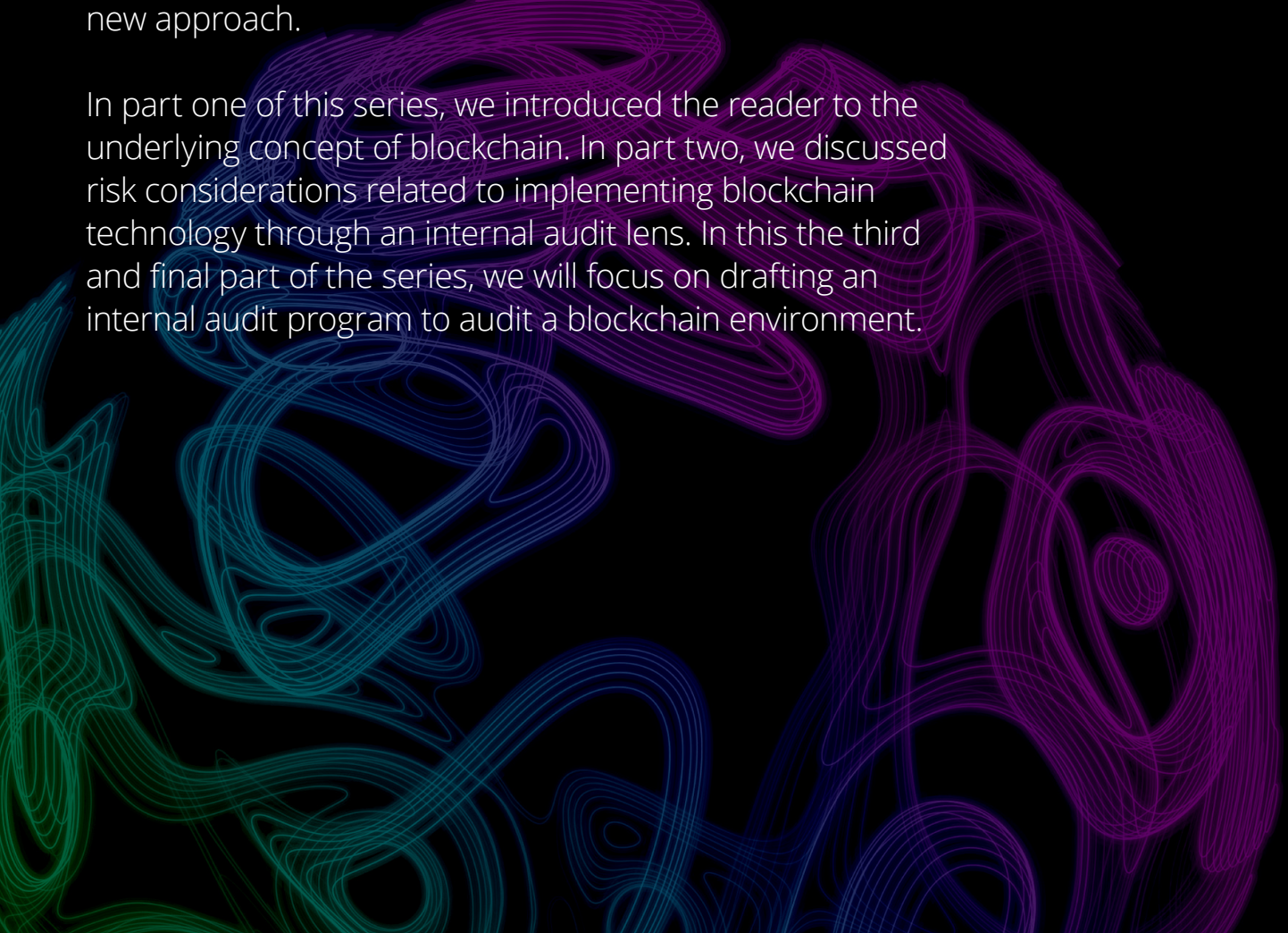
An internal auditor's guide to blockchain

Auditing blockchain environments

Introduction

Effectively adopting any new technology depends upon managing the risks associated with it. This is especially the case when the technology is more than an application and is part of the organization's core infrastructure. While blockchain-based systems offer exciting opportunities, they also present specific risk considerations and auditing challenges. Internal auditors not only need to understand these risks themselves, but also need to be able to proactively advise and prepare their business clients on the new risk and controls framework that will be needed to manage such risks. Accordingly, auditing blockchain systems often requires internal auditors to take an entirely new approach.

In part one of this series, we introduced the reader to the underlying concept of blockchain. In part two, we discussed risk considerations related to implementing blockchain technology through an internal audit lens. In this the third and final part of the series, we will focus on drafting an internal audit program to audit a blockchain environment.

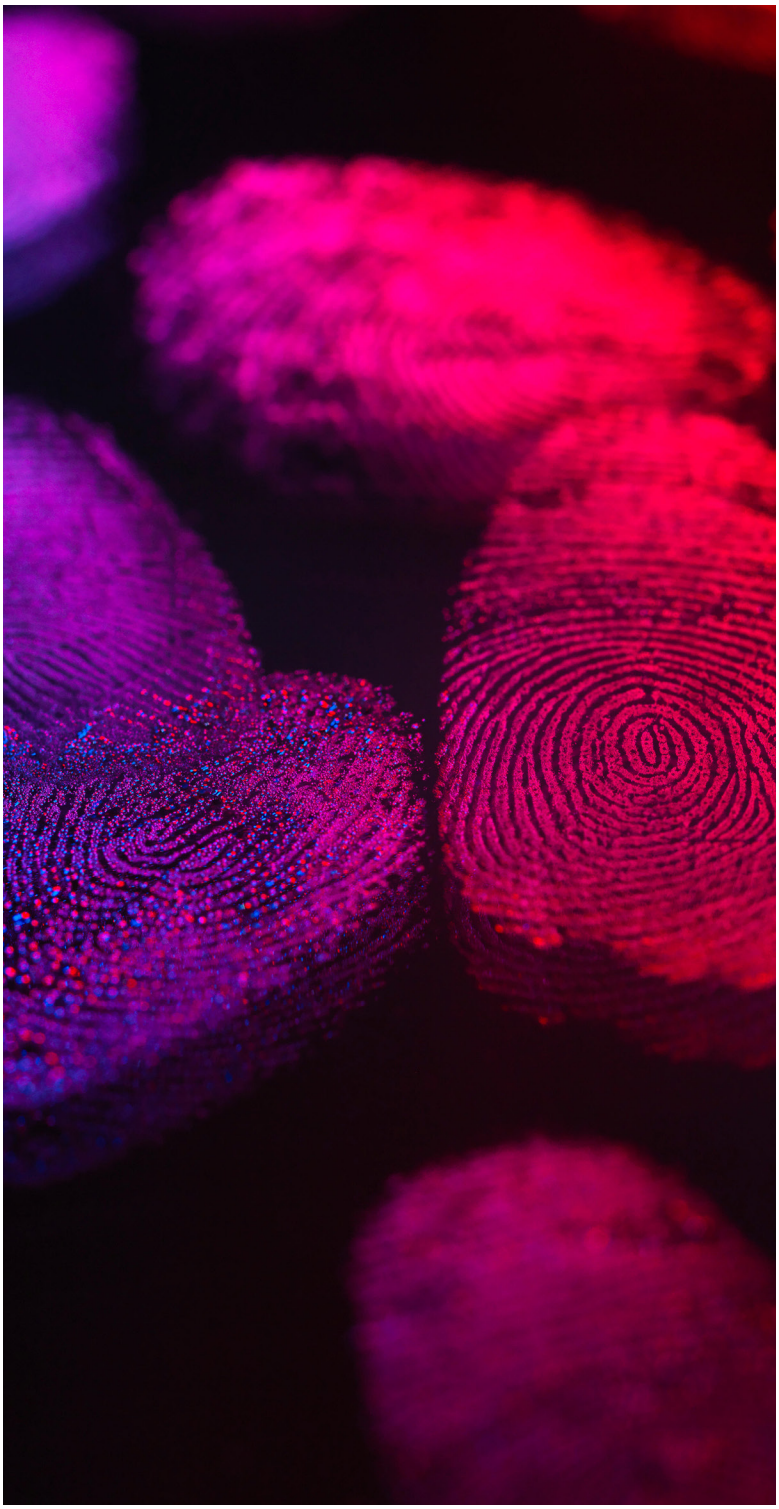


Case in point

In the second part of this series, we learned that Distributed Bank, LLC (DBL), a retail bank with global operations, was building a proof of concept using a blockchain-based solution for its international trade finance (ITF) department. The proposed solution would create a blockchain-enabled consortium comprising corporate clients (i.e., buyers and suppliers), correspondent banks, trade-facilitation service providers, and regulators.

The preimplementation review of the proposed solution was performed by John Block, the bank's internal auditor.

After the review, DBL decided to move forward with a blockchain-based solution for its ITF business, which would help the bank to distinguish itself from the competition. Accordingly, John Block was charged with creating an internal audit program that could effectively address the risks presented by the new blockchain-based solution.



Advantages of auditing a blockchain-based system

Since John Block had no prior experience auditing a blockchain-based system, he decided to document the key differences between traditional systems and blockchain-based ones. John noted that, unlike traditional databases, blockchain-based systems maintain historical transactional data in blocks. In the case of a permissioned blockchain like the one DBL would be using, blockchain data is only accessible to the users and entities who are granted access.

Also, unlike traditional systems, the new system would not have a centrally maintained database controlled by a single administrator. Moreover, completed transactions cannot be modified, since the blocks are linked through cryptography. This inherent immutability means that certain data integrity risks would not apply to the new system. **From an internal audit perspective, John noted several other advantages to a blockchain-based solution:**

Robust analytics: Since information is stored in a structured and consistent way across the permissioned blockchain, complex analytics can be performed reliably, and dashboards can be updated frequently.

Real-time auditing: Blockchain-based solutions can facilitate 100 percent population testing rather than traditional sampling. Since all transactions are recorded in a shared ledger, inclusive of certain counterparties, blockchain transactions can also be audited in real time as they occur. For instance, internal audit departments can maintain a read-only node on the blockchain to monitor and flag transactions in real time, and they can potentially use analytics to automate auditing of routine transactions.

Shortened audit cycle: Internal auditors often spend a great deal of time collecting, organizing, and cleansing data to generate meaningful insights and areas of audit interest. In a blockchain, transaction data is stored in a structured and consistent manner, and it is accessible in real time. Access to this detailed, timely information can provide a more informed and targeted risk assessment, which in turn can reduce the time required to plan the audit. Also, instead of relying on process owners to provide supporting documentation for testing, internal auditors can trace transactions throughout the blockchain on their own, which can further shorten the audit cycle.

Automated contractual enforcement: Contract risk compliance (CRC) often requires a lot of attention from internal auditors, since tracking adherence to certain contractual terms is a highly manual activity and subject to error. Smart contracts, which have been coded to execute based on certain agreed-upon business conditions, can expedite this process. With a blockchain-based system that supports smart contracts, CRC compliance can be almost fully automated, thus allowing auditors to shift their focus from sample-based CRC testing to automated functionality testing, which is a higher-value activity.

Trustworthy reconciliations with counterparties: Since the data is consistent and reliable across entities, some reconciliation controls may not need to be tested in a blockchain environment, allowing internal auditors to focus on other topics of audit interest.

Rapid data recovery: Due to the redundancy of ledgers hosted by each party within the blockchain, data can be recovered more easily during a disruptive event. This unique specific puts data retention and retrieval controls in a low risk category.

After understanding the uniqueness of blockchain technology, John developed the audit program for DBL's blockchain-based ITF system:

Governance framework

John knew that data-sharing within the blockchain-based system is fundamentally different from traditional systems. Accordingly, the new ITF system should be governed effectively in order for it to function as intended. Therefore, John decided to review the following areas of governance:

- **Approval and endorsement** of the new ITF system by executive management and key stakeholders
- **Relevance and ongoing pertinence** of the documented governance framework, policies, and procedures, including confirmation that the framework's mandate has been communicated across the enterprise
- **Relevant governance committees have been formed,** and they are actively engaged in overseeing the blockchain solution (e.g., arbiter of unintentional transactional errors, review of relevant meeting presentations and minutes to determine whether benefits of the new systems are being assessed and issues are properly being tracked and mitigated)
- **Controls over data-sharing** with other participants within the blockchain
- **Executive oversight** in negotiating and monitoring the terms of contracts with third parties

Change management

With John's prior internal audit experience, he knew that whenever a new system is implemented, the change management process is prone to control weaknesses. After the system goes live, the system should be periodically assessed to confirm that standard IT change controls are in place. New systems also require bug fixes and frequent enhancements. Therefore, it was important for John to confirm that the change management process was effective, along with defining the appropriate system-development life cycle for any major upgrades. Accordingly, John planned to review:

- **Code management and permissions,** with an emphasis on maintaining appropriate segregation of duties during the software development life cycle (SDLC)
- **Policies and procedures** around change management, SDLC, and emergency modifications to confirm they are documented and approved
- **Procedures related to creating, testing, and approving** changes to confirm they are documented and approved
- **Interfaces** between the blockchain solution and legacy systems to confirm completeness and accuracy of shared data across the enterprise
- **Data migration** strategy and controls over data conversion

IT security and operations

While reviewing the blockchain-based solution, John also considered the different layers of IT security required to protect the new system and monitor its operation. This included confirming that user access is granted on a need-to-know or need-to-do basis; confirming that superusers are removed when separated from the company; and confirming that password parameters are enforced. John knew that the ITF system was based on an asymmetric key cryptography in which a private key controlled the ability to transact within the system. Given that users relied on private keys for their ability to execute transactions, protecting the key rights from generation to disposal (i.e., the key life cycle) was critical to safeguarding the bank's customers and their funds. John also needed to review the consensus mechanisms for adding records to a distributed ledger. In addition, any vulnerabilities in consensus mechanisms and/or private key management could compromise the integrity of the ledger. So, he decided to review:

- **Process for granting user access,** confirming that it follows the principle of least privilege
- **Effectiveness of consensus mechanisms,** confirming that they are detailed, accepted by all participants, and capable of resolving unforeseen issues
- **Efficacy of private key management,** including controls around key generation, storage, distribution, recovery, and disposal
- **Scalability of the system** to confirm that it is capable of handling peak volumes
- **Data confidentiality,** confirming that data-sharing between the blockchain participants is based on the principle of least privilege

Penetration testing

A blockchain-based system is a highly connected environment that simultaneously collaborates with multiple participants to update the distributed ledger. Therefore, it was critical to evaluate such a system continually for cybersecurity vulnerabilities and to confirm that any loopholes on a new system didn't pose any risk to connected systems. Specifically, John needed to ascertain if processes were in place for assessing the security state of the new blockchain-based system and if security loopholes could be detected and corrected quickly. So, he planned to test:

- **The process** for periodically reviewing the code and performing static and dynamic testing
- **The plan** for reviewing, mitigating, and remediating system issues and unexpected functionality
- **The adequacy of system resiliency** by reviewing reports from prior penetration tests performed by the bank to assess system vulnerabilities, as well as confirming that identified issues had been addressed in a timely manner

Blockchain data integrity

There are many stages where data integrity can be compromised within a blockchain. Therefore, John needed to confirm that the data within the new system was reliable, timely, complete, and accurate for all participants. Accordingly, he reviewed the following:

- **Appropriateness of data sources** to confirm that only authorized individuals, organizations, and oracles can create data and enter it into the ecosystem
- **Effectiveness of controls** to prevent man-in-the-middle attacks, in which an oracle interferes with legitimate data input and modifies the source data to meet a desired outcome
- **Efficacy of controls** around recording transactions to confirm timeliness, accuracy, and completeness
- **Effectiveness of application controls** related to data transfer, storage, and retrieval
- **Sufficiency of fraud prevention** controls
- **Immutability of transactions** within the blockchain-based system

Smart contracts

Even though smart contracts execute automatically when certain conditions are met on a blockchain, they are still subject to unintentional software bugs in the system that can materially affect transaction processing. They are also subject to common IT risks, such as inappropriate access and improper code modification. Additionally, since open-source code is used in many smart contracts, hackers may be able to exploit unpatched vulnerabilities that exist on the network. Accordingly, John decided to review the following aspects of smart contracts within the new ITF system:

- **Appropriateness** of user access
- **Effectiveness of the change management process** for developing, testing, updating, or patching smart contracts
- **Efficacy of the incident management process** to identify and respond to events identified during contract execution
- **Network layer controls** to prevent external attackers from exploiting smart contract functionality
- **Robustness of authority-delegation process** for executing smart contracts on behalf of the bank
- **Periodic review of the automation code** by an independent third party
- **Effectiveness of contract enforcement**

Despite the widely recognized benefits of speed and transparency, blockchain technology is still maturing, and there is no generally accepted global regulatory framework in place. This obligates all parties within a blockchain to agree on mutually accepted terms while complying with local laws and regulations.

Business continuity and disaster recovery management

John had previously tested DBL's business continuity plan and its processes for disaster recovery management, and the results were satisfactory. However, he wanted to see if the existing plan considered the changes that could occur after implementing the new ITF solution. Therefore, John decided to include the following in his audit program:

- **Confirm that bank's business continuity** and disaster recovery management plans have been updated to incorporate changes associated with the new blockchain-based system
- **Confirm that inputs for the plan** were obtained from relevant stakeholders, including those from information security, legal, and risk
- **Determine whether the business continuity plan** for the blockchain solution has been formally approved by the appropriate authority
- **Verify the adequacy of the business continuity plan** for the blockchain system by assessing the testing methodology, test results, and remediation plan

Legal and regulatory risk management

Despite the widely recognized benefits of speed and transparency, blockchain technology is still maturing, and there is no generally accepted global regulatory framework in place. This obligates all parties within a blockchain to agree on mutually accepted terms while complying with local laws and regulations. Consequently, John included the following areas in his audit program:

- **Confirm that blockchain-specific risk factors** have been embedded into an existing risk management framework or that a new reasonable and pertinent framework has been created
- **Review the bank's approach** for managing blockchain regulatory risk, confirming that the following elements have been incorporated as mechanisms for monitoring the regulatory landscape, such as risk committees, regulatory reporting, and interfaces with regulatory agencies
- **Consider existing rules and regulations** and how they affect the blockchain solution, such as anti-money laundering regulations, know-your-customer rules, and the General Data Protection Regulation (GDPR)
- **Obtain evidence** that relevant stakeholders are engaged in overseeing blockchain regulatory risk by reviewing applicable meeting minutes, as well as mapping items identified during risk assessments to the information shared with relevant stakeholders

Talent management and skills development

DBL seeks to continually evolve its talent management process as a means of achieving exceptional organizational performance. However, blockchain-based systems create new challenges for acquiring and retaining resources, making talent management and skill development a moderate risk area for internal audit. As such, John decided to include the following in his audit program:

- **Processes used to attract and retain talent** with the requisite skills to effectively develop and utilize the new system
- **Confirm that the bank has a process** in place for assessing its staffing needs related to the ITF solution
- **Assess whether the bank's human resources policies** and programs are designed to both attract new talent and to retain the existing workforce
- **Review medium-to-long-term plans** for retraining and cross-training the existing workforce on blockchain technology in order to effectively manage future contingencies
- **Examine training programs** to confirm that new team members are able to be effective with their job responsibilities
- **Confirm that the bank's training program** includes basic and advanced training modules related to blockchain
- **Affirm that these training modules** are assigned to relevant resources and are tracked for timely completion
- **Consider whether employees are encouraged** to participate in external training programs to stay abreast of ongoing developments
- **Assess the overall efficacy** of the bank's training program in relation to disruptive technologies such as blockchain

Third-party risk management

Third-party vendor support will continue to be critical for ITF until the new blockchain-based system fully matures and initial glitches are ironed out. Moreover, the blockchain vendor landscape is fragmented, with many vendors having nascent capabilities and relatively little experience. To mitigate these risks, John decided to incorporate the following areas into the audit program:

Vendor selection process

- **Confirm that the vendor selection process** is thoroughly defined and well-documented and that it incorporates the requisite technical parameters needed to select a suitable blockchain service provider, such as depth and breadth of talent pool; reliability, including financial soundness; and cost
- **Verify that the bank's existing blockchain vendors** were selected based on the established criteria.

Contracting

- **Confirm that third-party contracts** have been designed in such a way that they safeguard the interests of the bank while providing the flexibility to manage unforeseen challenges. Considerations include:

Ongoing relationship management

- **See if relationship management meetings** are periodically scheduled with key blockchain vendors
- **Verify that blockchain vendors** are providing the enterprise with the necessary management reports covering risk, past performance, present issues, regulatory concerns, performance metrics, and service-level agreements (SLAs).

Periodic appraisal

- **Confirm that existing vendors** are reviewed periodically based on predefined criteria
- **Verify that vendors** are meeting the terms of their contracts or SLAs
- **Examine whether relevant stakeholders** are actively engaged in vendor oversight

Conclusion

Blockchain technology has the potential to revolutionize transaction processing through its ability to create a secure, trusted, distributed ledger that can be managed without the overhead of a central authority. But reaping the full benefits of a blockchain-based system requires a fundamental shift in both the mindset and processes of internal audit. With blockchain, the underlying foundations of auditing and internal control can be embedded into each transaction.

This means that the internal audit design itself can be shifted from a retroactive, point-in-time examination to an ongoing, real-time monitoring process that is informed by previous transactions.

Despite its enormous potential, blockchain is still a nascent technology. This, in turn, implies that the associated risk assessments and control frameworks are also formative. For many internal auditors, this is uncharted waters. The good news is that much of their legacy knowledge and skills still apply. As approaches to auditing blockchain-based systems evolve, traditional auditing risks related to data availability, processing integrity, governance, privacy, security, confidentiality, and change management will continue to be relevant. However, internal auditors should familiarize themselves with the technical aspects of distributed ledgers so they can adapt their traditional audit programs to accommodate the brave new world of risks and benefits to which blockchain technology gives rise.

Contact us

Adam Regelbrugge
Partner
Risk & Financial Advisory
Deloitte & Touche LLP
aregelbrugge@deloitte.com

Sarah Fedele
Principal
Risk & Financial Advisory
Deloitte & Touche LLP
sarahfedele@deloitte.com

Manu Mankad
Managing director
Risk & Financial Advisory
Deloitte & Touche LLP
mmankad@deloitte.com

Seth Connors
Senior manager
Risk & Financial Advisory
Deloitte & Touche LLP
sconnors@deloitte.com

Deloitte.

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.

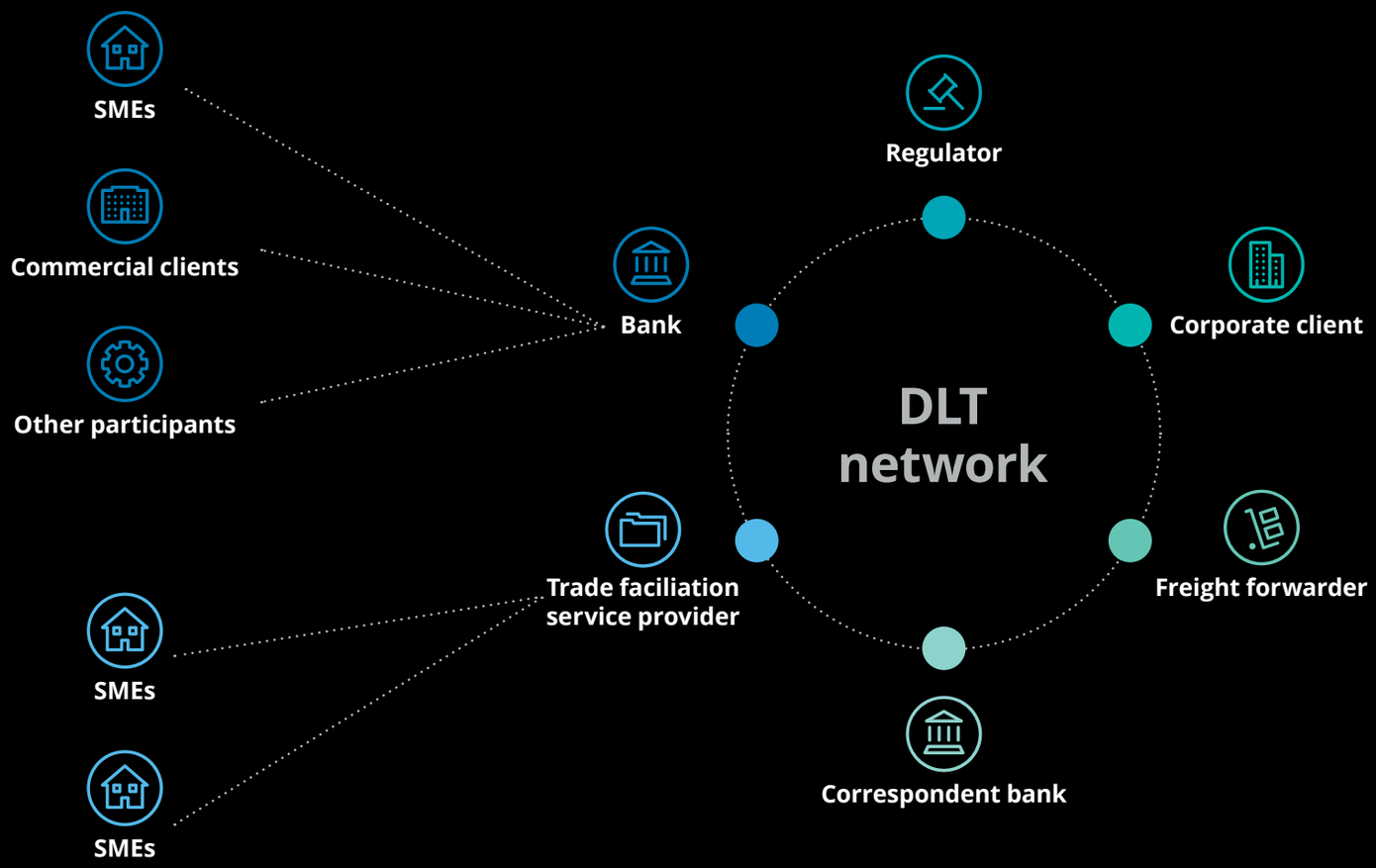
We will illustrate specific risk considerations to bring blockchain concepts to life by using a fictitious example of an internal audit department performing a preimplementation review of a blockchain-based solution being considered by a bank for implementation in its international trade finance (ITF)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

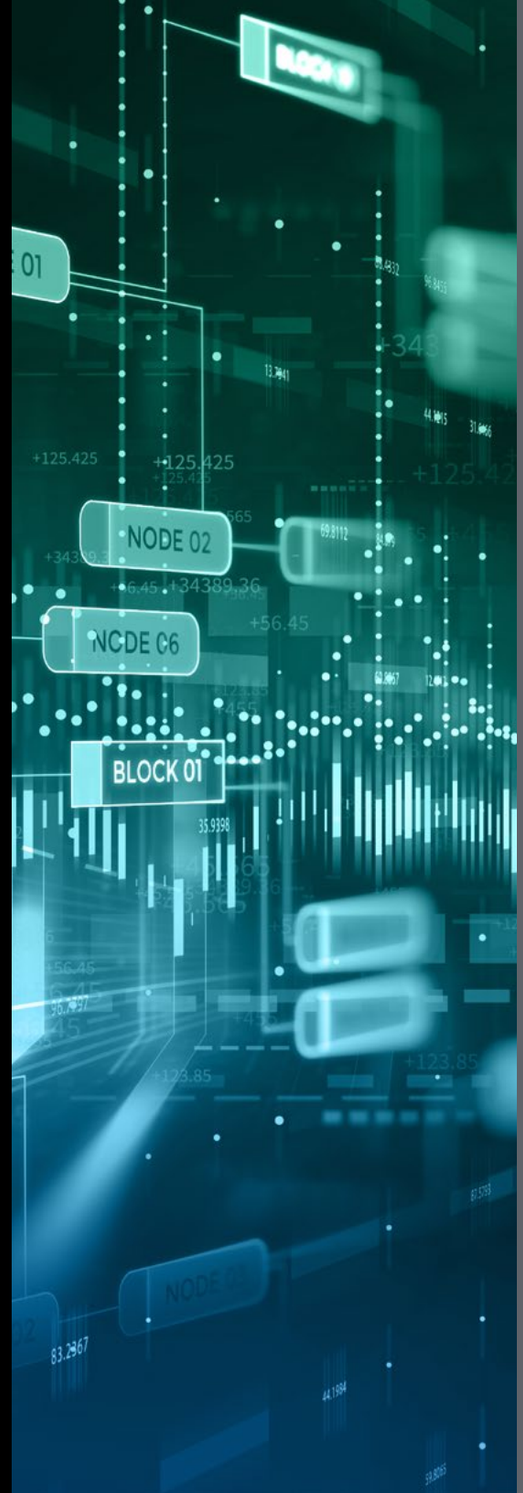
Risk considerations (cont.)

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:

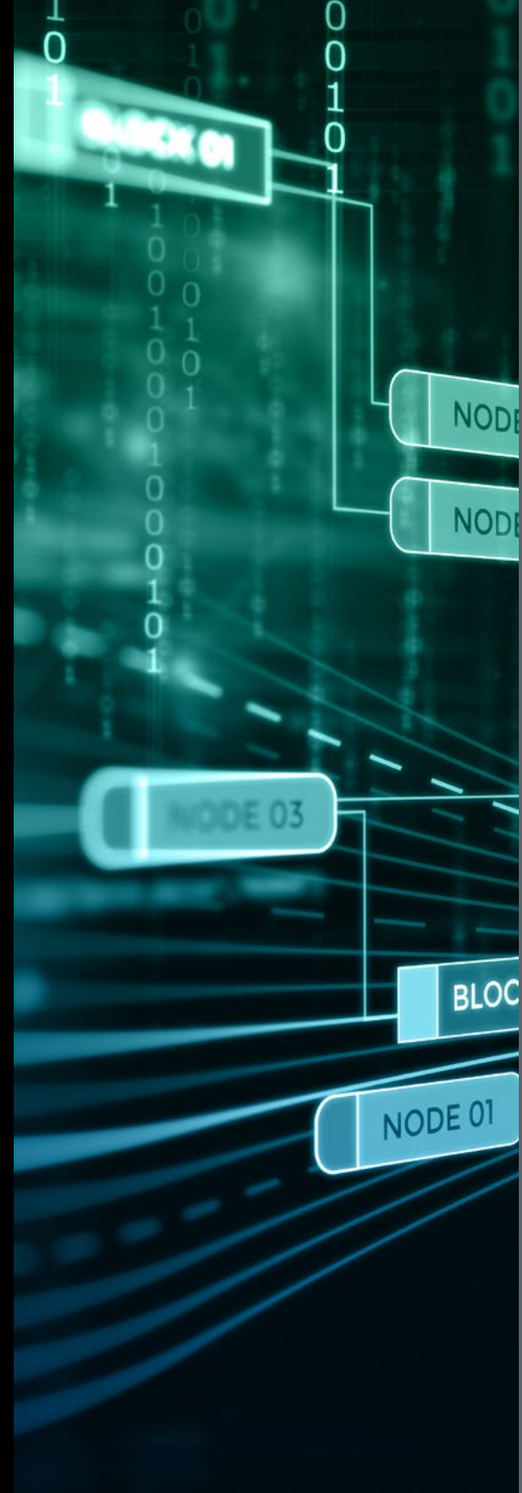
- The type of governance structure that best serves the participants in the consortium
- Support for sound decision-making, risk management, change, incident, and emergency-response management should any alterations need to be made in the consensus mechanism or governance decisions



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.”

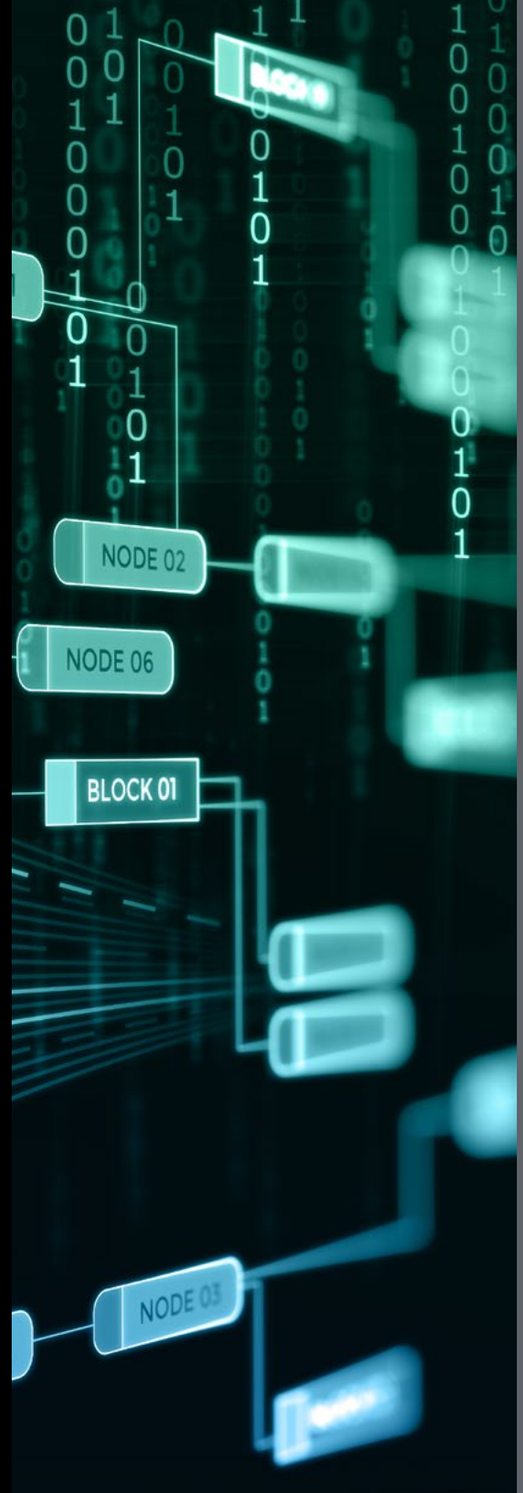
Risk considerations (cont.)

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.

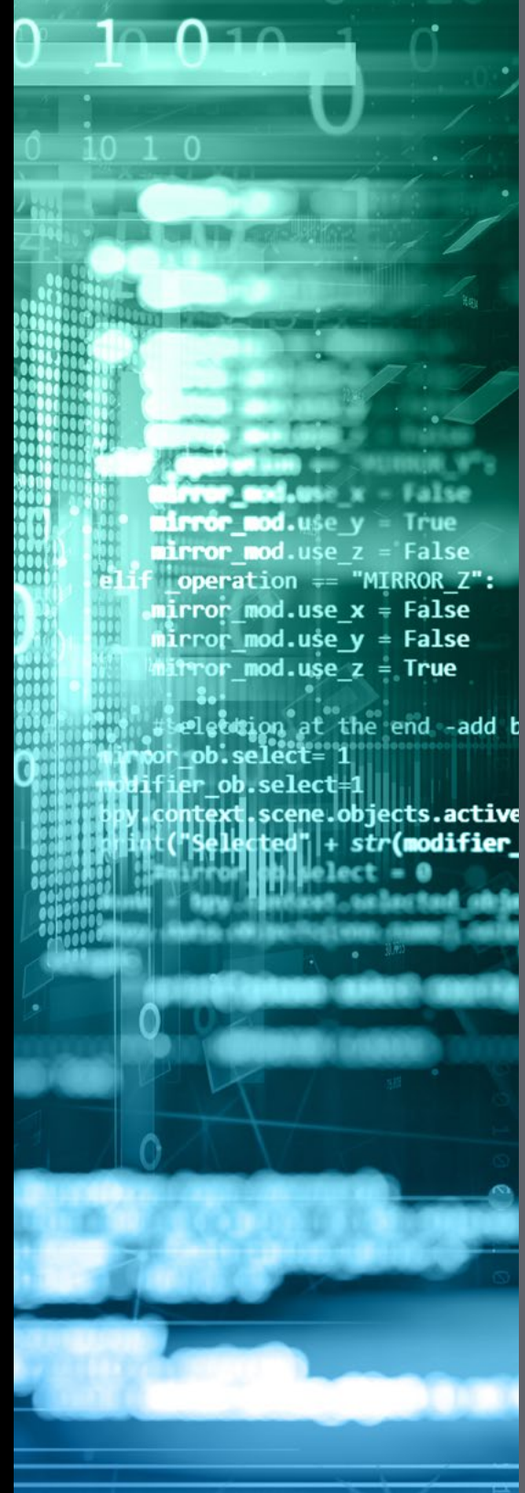
John further stated, "Smart contracts must be codified and tested for compliance with the trade, economic, legal, and regulatory environment at every stage of the journey between seller and buyer. In terms of regulatory issues, contracts need to be designed with adequate change management policies that 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.)

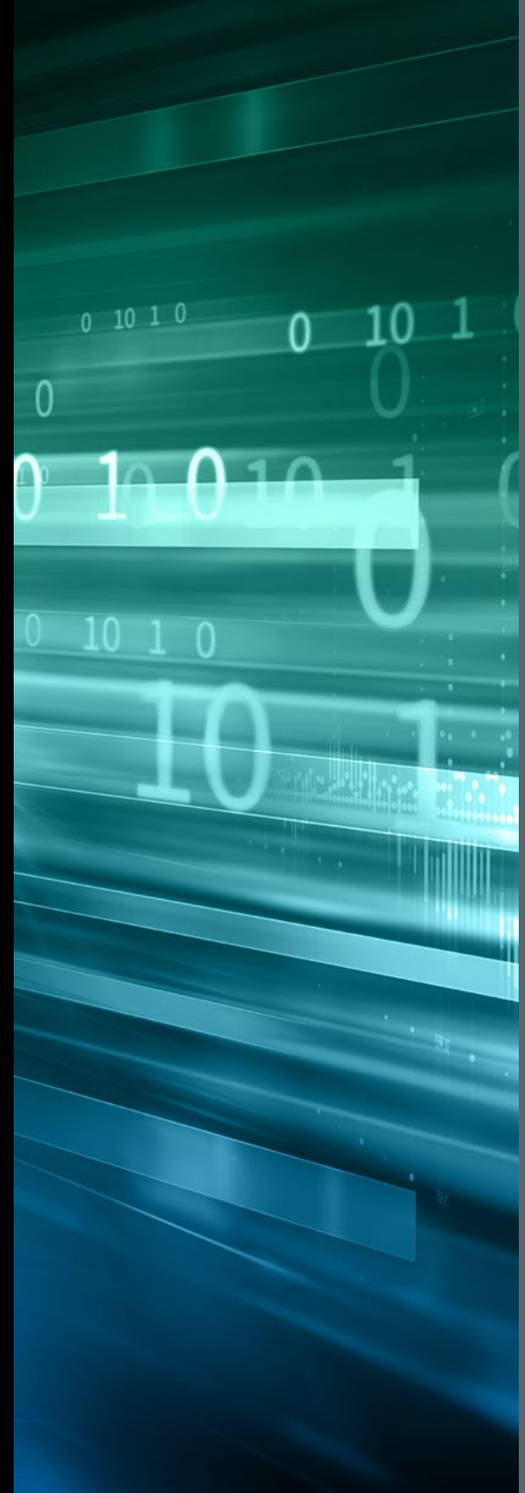
Business continuity and disaster recovery risks

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

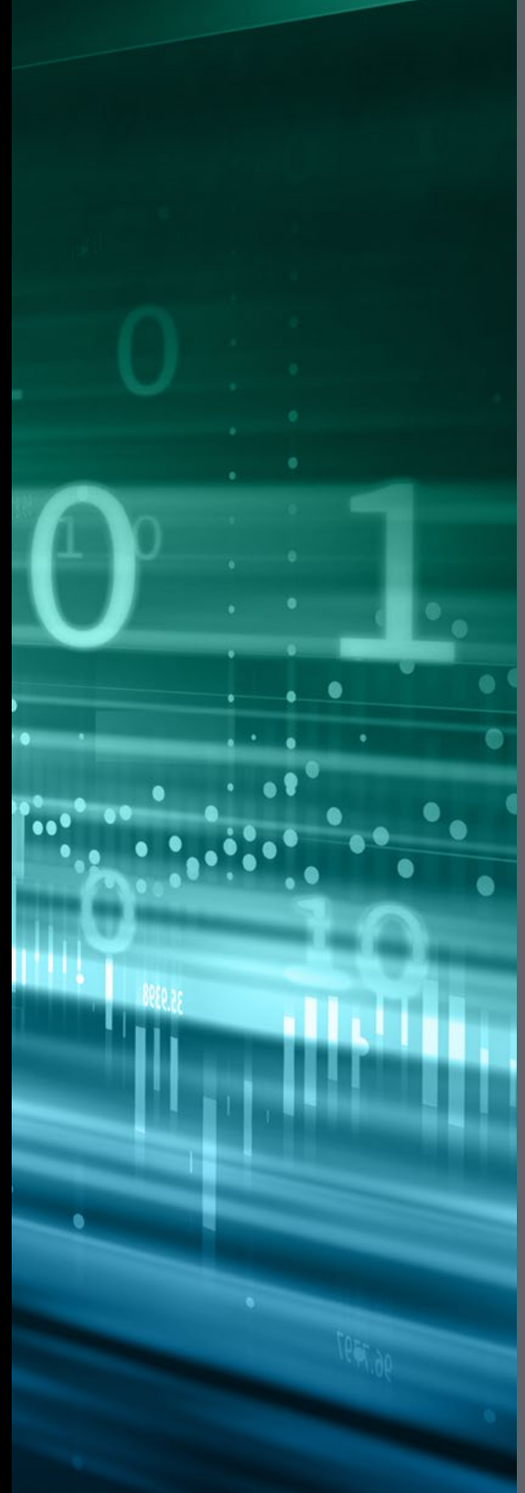
Adam Regelbrugge
Partner, Internal Audit
Deloitte & Touche LLP
aregelbrugge@deloitte.com

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.

Deloitte.

An internal auditor's guide to blockchain: Blurring the line between physical and digital

Part one: Introduction to blockchain

The world is being ushered into the Fourth Industrial Revolution (Industry 4.0) at breakneck speed. In this age, disruptive technological advances and trends are rapidly reshaping business models, improving productivity, and enabling innovation in the way organizations provide products and services to their consumers, thereby creating entirely new markets. As Industry 4.0 gains momentum, how the world works and lives is being redefined, reengineered, and reinvented. The line between the digital and physical is blurring.

Blockchain technology is poised to be one of the key pillars of Industry 4.0. According to a 2018 report by Gartner,[1] the business value from blockchain will reach $3.1 trillion by 2030 through cost reduction and revenue growth. Further, according to its 2017 CEO Survey,[2] 25 percent of participating CEOs perceive the impact of blockchain to be either "major" or "transformational." Blockchain was also the most-searched term on Gartner.com throughout most of 2017.[3]

In addition, Deloitte Touche Tohmatsu Limited's (DTTL) global survey[4] of more than 1,000 global blockchain-savvy executives from seven countries indicates that momentum is shifting from a focus on learning and exploring the potential of the technology to identifying and building practical business applications. For example, 74 percent of those surveyed report that their organizations see a "compelling business case" for the use of blockchain and many of these organizations are moving forward with the technology. About half of that number (34 percent) report that their organization already has some blockchain system in production while another 41 percent of respondents say they expect their organizations to deploy blockchain applications within the next 12 months. Furthermore, nearly 40 percent of respondents reported that their organization will invest $5 million or more in blockchain technology in the coming year.

The evolving role of internal audit and blockchain

According to the recent DTTL 2018 Global Chief Audit Executive (CAE) survey[5]:

Only 40 percent of surveyed CAEs reported that their functions had a strong impact and influence within the organization. In addition, while 46 percent of the respondents believe that the broader organization is generally very aware of internal audit, only 33 percent believe the function is viewed very positively. In many cases, these findings may indicate a need for internal audit to deliver more value around issues and risks that impact the organization's ability to achieve its goals.

To enhance its impact and influence within the organization, internal audit needs to not only provide assurance services, but must also advise on complex business issues and anticipate risk. Further, at a time when enterprises in every industry are innovating, it is imperative that the internal audit function also keep pace with the climate of constant disruption by employing advanced analytics and focusing on newer technologies.

As blockchain technology continues to grab the attention of board members and CXOs of many organizations, it becomes imperative for the internal audit function to proactively acquaint itself with the opportunities and risks emerging from the implementation of this technology. Internal audit functions have an opportunity to enhance their impact and influence within the organization. In this age of information overload, it becomes very important for the internal audit practitioner to cut through the noise. The internal audit group should be able to separate facts from fiction, and provide an objective, independent, and well-thought-out point of view.

With this objective in mind, this series on blockchain is designed to educate internal auditors on the following topics related to blockchain.

Part one: **Introduction to blockchain:** This paper introduces internal auditors to the concepts of distributed ledger technology and blockchains, key features and types of blockchains, how blockchains work, and smart contracts, as well as cryptocurrencies, tokens, wallets, and Initial Coin Offerings (ICOs).

Part two: **Risk considerations in blockchain.** This paper will inform internal auditors on some risks that organizations are exposed to when implementing blockchain technology, with consideration to specific use cases.

Part three: **Auditing blockchain environments.** This paper will focus on the uniqueness of auditing in a blockchain environment such as how a blockchain processing environment differs from a traditional processing environment.

Blockchains are protocols that allow entities to store and share transactional information in a controlled and systematic way.

Digital ledgers

Evolution of ledgers—physical, digital, distributed: It all started with a need to record, store, and exchange information. During the Bronze Age, physical ledgers were used to maintain records of agricultural goods. Represented by records stored in a codex, ledgers were "pages" organized into volumes that formed an authoritative source of information. The 1950s and '60s led to the development of business computers, and a ledger was represented by records stored in a database. Distributed ledgers came into prominence in 2008 with the release of Bitcoin and are represented by the consensus view of a group of peers who share responsibility for maintaining the ledger.

Today, traditional physical and digital ledgers record entries in a single place. As a central agency is typically responsible for them, they are often called central ledgers. Central ledgers allow one authoritative copy of the data. For physical ledgers, this is a single codex or a volume in a series. Existing digital ledgers use a single system of record, typically in the form of an enterprise resource planning (ERP) system. Security of central ledgers focuses on managing access to this single source of stored information. Access to the ledger enables one to add entries as well as read or change existing ones. Distributed ledgers, on the other hand, do not rely on a single authoritative copy of information. As a result, ensuring the integrity of the ledger is more complicated because a central authority to control the ledger can no longer be relied upon.

What is being "distributed" in a distributed ledger is the responsibility for managing the ledger—deciding what entries to include and their order, and ensuring entries are not changed once added. Generally, a group of peers shares this responsibility, rather than leaving it to a central authority. With no single agent responsible for maintaining the ledger, participants must rely on the consensus of the peers involved. The current state of the ledger is simply the peers' consensus view. Consequently, distributed ledgers aren't defined in terms of how or where the information they contain is stored—each peer may store ledger data how and where they prefer. Instead, they are defined by the ledger's consensus model—the process peers use to reach consensus. It is important to note that many distributed ledgers may not have blocks, nor do they inherently require a blockchain. Based on this, there are different risks and opportunities that are relevant when considering distributed ledger technology.

Introduction to blockchain

Businesses exist to create and transfer value and, in the age of Industry 4.0, value is frequently derived from digital assets, records, and identity. The transfer of value has been traditionally seen as an expensive and slow process. Three technologies have come together to lay the groundwork for blockchain and to address this challenge (see figure 1):

- **Peer-to-peer network:** Every peer in the network is a server and a client, both supplying and consuming resources. This enables the facilitation of a distributed ledger without a central, privileged third party.
- **Asymmetric key cryptography:** A method for verifying digital identity with a high degree of confidence, enabled by the use of private and public keys.
- **Consensus mechanisms:** A process used to achieve agreement among distributed processes or systems. These are designed to achieve trustworthiness in a network involving multiple, unreliable nodes.

A blockchain is a distributed ledger that allows digital assets to be transacted in a real-time, immutable manner. In other words, a blockchain is a record, or **ledger**, of digital events organized in chronological **blocks**—one that is encrypted and "distributed" between many different parties (see figure 1). It can only be **updated by consensus** of a majority of the participants in the system. Once entered, information is secured using cryptography in order to preserve the integrity of the data. The blockchain contains a **certain and verifiable record** of every single transaction ever made.

Figure 1. Laying the groundwork for blockchain's invention

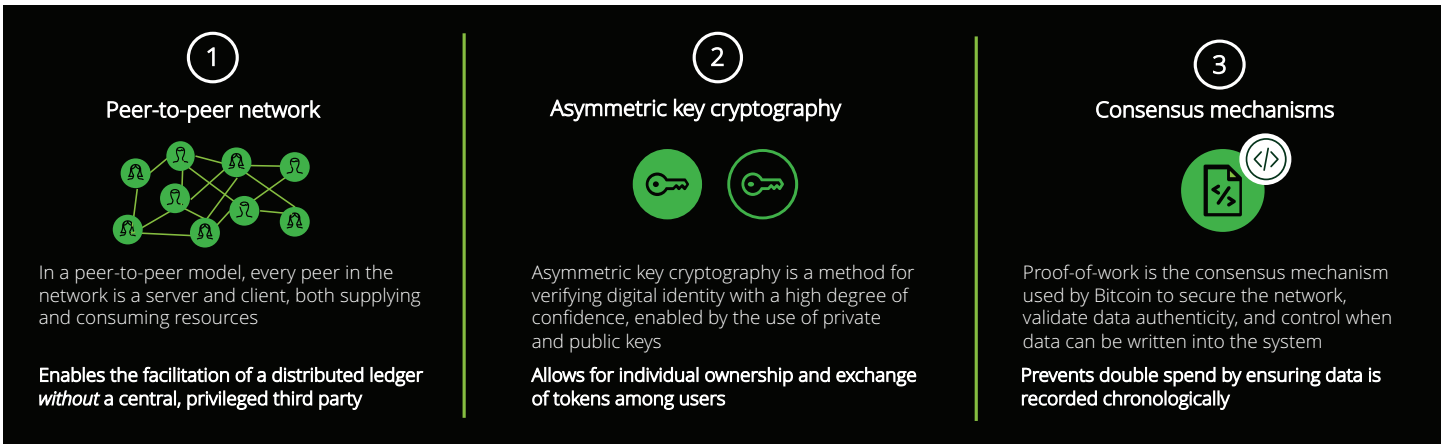
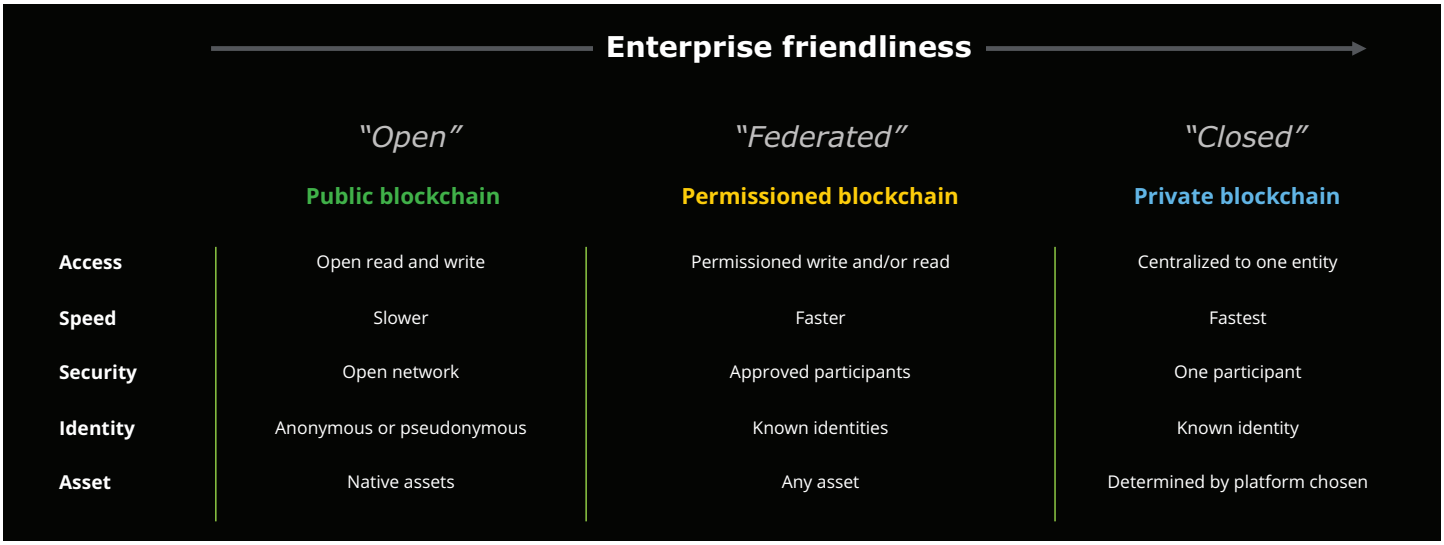


Figure 2. Specific features of different types of blockchain



Blockchains are **protocols** that allow entities to store and share transactional information in a controlled and systematic way. Generally, the technology acts as a platform and the associated plumbing that allows applications to build on top. Therefore, it is entirely possible that an end user of a blockchain-enabled application is unaware of the fact that a blockchain is being used to support the processing.

Because the blockchain protocol uses a **peer-to-peer** or **machine-to-machine** value-transfer framework, every participant **node** on the blockchain has an exact copy of the data, and a consensus protocol synchronizes the updates across participant nodes. It therefore facilitates a near **real-time** value transfer (e.g., assets, records, identity) among participants without having to wait for a central authority ("trusted third party") to validate the transactions. This **disintermediation** replaces the need for a "trusted third party" with cryptographic proof. The cryptographic consensus protocol also ensures **immutability and irreversibility of all transactions** posted on the ledger.

Features of a blockchain

Blockchains can be grouped into the following two categories: permissionless or permissioned. Where a permissionless system is "open" to the public, a permissioned system can be "private" or "semi-public" (see figure 2):

- **Permissionless** – A public, shared system that allows anyone to join the network, write to the network, and read the transactions from those networks. These systems have no single owner—everyone on the network has an identical copy of the "ledger." Cryptocurrencies such as Bitcoin and Ethereum are examples of products that run on these systems.
- **Permissioned (semi-public)** – Semi-public, shared systems are a form of hybrid system that provide for situations where only preauthorized nodes are permitted on the network; therefore, data would not inherently be viewable to the world. The data would be viewable only to those who have a preauthorized node on the network and can view and collect the data.
- **Permissioned (private)** – Private, shared systems are those that operate within an entity, whereby outside entities are not able to participate.

Blockchain consensus models:
The lack of trust inherent to public, and to a lesser degree, permissioned blockchain systems underlines the importance of consensus models. This lack of trust requires consensus models to function effectively in normal and adversarial conditions.

While this paper will not delve into the different types of consensus models, it is important for internal audit practitioners to understand some examples of issues that can result when an inappropriate consensus mechanism is selected. Some issues that may result include:

- **Blockchain hard fork(s)** – Defined as an event whereby two divergent copies of the blockchain are created. Typically occurs as a result of a disagreement amongst network participants on the rules governing the blockchain.
- **Double spending** – Double spending is a problem principally with cryptocurrencies whereby the same digital asset can be promised/transferred to multiple entities.
- **51% dominance** – Defined as a problem primarily in the permissionless crypto world whereby one entity controls more than 51% of the processing power of the network. As a result, the entity has the technical ability to act maliciously.
- **Poor performance** – Consensus mechanisms are a trade-off between the level of distrust amongst participants and the speed at which consensus needs to be achieved. Some software vendors have developed a multitude of consensus mechanisms that are measured in transactions per second of processing power.

Cryptocurrencies

There are more than 1,000 different cryptocurrencies that exist according to CoinMarketCap, each of which have their own digital asset inherent to their unique blockchain. For example, the bitcoin network has "Bitcoin/BTC" that are created and maintained on the Bitcoin blockchain. Cryptocurrency, otherwise known as digital assets, are stored on the blockchain at addresses that are owned by participants. The digital assets are secured on the blockchain using complex cryptographic functions. It is important to note that cryptocurrencies are just the first real-world use case of blockchain technology.

The minimum viable ecosystem (MVE) for a cryptocurrency that holds value is generally composed of:

Coins: A coin is a unit of value native to a blockchain. It is a means of exchange within the blockchain to incentivize the network of participants to use the blockchain. Cryptocurrencies such as Bitcoin, Ether, XRP, and Litecoin are all examples of native coins. The sole purpose of a coin is to exchange value, and it has limited functionality beyond that. A common feature of all these coins is that they each possess their own independent blockchain where transactions related to their own native coins occur.

Wallets: A wallet stores the public addresses and corresponding private keys, which can be used to receive or send the cryptocurrency. Unlike physical currency that are stored in physical wallets, the cryptocurrency itself is stored on the blockchain.

Two basic types of cryptocurrency wallets are "hot wallets" and ("cold wallets.") The key distinction between to the two wallets is the degree to which the wallets are connected to the Internet. While hot wallets are connected to the Internet, cold wallets are offline. There are different reasons why an investor might want his or her cryptocurrency holdings to either be connected to or disconnected from the Internet. It's not uncommon for cryptocurrency enthusiasts to hold multiple wallets, some of them hot and some of them cold.

Digital Currency Exchange (DCE): These are businesses that allow customers to trade digital assets for other assets, such as conventional fiat money, or other digital currencies.

Consensus mechanism: With the proof-of-work consensus mechanism, mining is the process by which transactions are verified and added to the blockchain, and also the means through which new bitcoins are released.

Smart contracts, tokens, and ICOs

Smart contracts: A smart contract is a computer program that directly controls the transfer of digital assets between parties under certain conditions. Smart contracts act in a manner like a vending machine. Customers can put a dollar into a machine, provide a product selection, the machine will validate the dollar and the product selection, and if available, the machine will dispense that asset. If the product is unavailable or the dollar is fictitious, the machine will reject the transaction. A smart contract seeks to define formal contract language into computer code in an effort to automatically enforce obligations. Smart contracts are inherent in specific blockchain implementations, but not all blockchains have the functionality available. The Ethereum network is an example of one permissionless network that has smart contract functionality.

Tokens: Tokens are created on existing blockchains using smart contract code. Many tokens have utilized Ethereum's ERC-20 standard, of which code has been made public to allow for the creation of new tokens. In this context, the smart contract functionality allows logic to be coded into the blockchain that allows for the creation of tokens based on predefined inputs.

The main difference between coins and tokens is in their structure. Coins are on their own separate blockchains while tokens operate on top of a blockchain that facilitates the creation of decentralized applications.

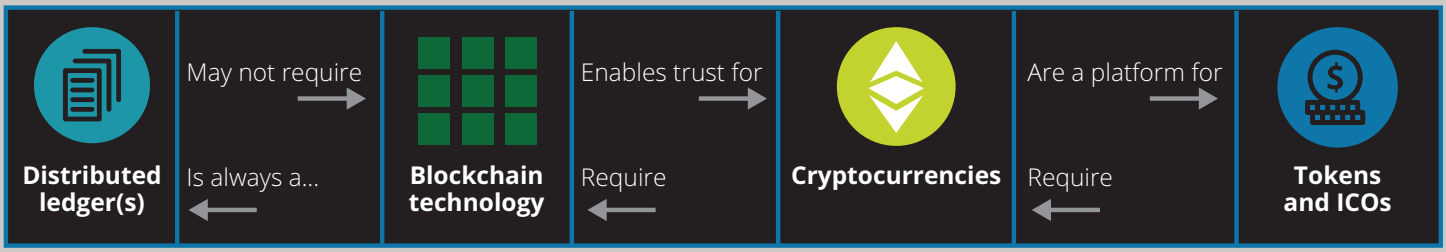
ICOs: An initial coin offering (ICO) is a "token sale" or "token launch" whereby an entity or group of entities creates tokens on a predefined date in order to generate capital or allow users to buy into an ecosystem. Many of the token launches plan to utilize the tokens in a future ecosystem that relies on the token in order to function.

Many ICOs have come under recent scrutiny by regulatory entities including the SEC, which launched their own ICO, known as HoweyCoins (https://www.howeycoins.com/index.html) in an effort to promote awareness and educate the investing public.

As internal auditors navigate through this complex ecosystem, they should be aware of how inherently complex it is and understand that each use case should be evaluated and carefully considered in light of the above concepts.

A summary of the key concepts presented in this document are presented in figure 3.

Figure 3. Summary of key concepts



Internal audit's role in the digital revolution

While blockchain may be the next step in the digital evolution, specific implementations of blockchain technology are still susceptible to emerging and existing risks. These developments will require Internal Audit to play a pivotal role in not only providing traditional assurance, but also acting as a trusted business adviser and anticipating/evaluating newer risks to the organization.

As a new emerging technology, blockchain will continue to be evaluated for its use. The rate of adoption of blockchain technology may differ for each company. Therefore, the preparedness level of each Internal Audit function to respond to the risks posed will also vary. But the overall challenge remains the same: Staying current on the risks and opportunities that come along with technological advancements such as blockchain.

Contacts

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

Rajat Bhattacharya
Senior Manager, Internal Audit
Deloitte & Touche LLP
rbhattacharya@deloitte.com

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

Endnotes

1. Rajesh Kandaswamy and David Furlonger, *Blockchain Primer for 2018*, Gartner, February 1, 2018, https://www.gartner.com/doc/3850677/blockchain-primer-.
2. Linda Pawczuk, Rob Massey, and David Schatsky, *Breaking blockchain open: Deloitte's 2018 global blockchain survey*, Deloitte Development LLC, 2018, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-2018-global-blockchain-survey-report.pdf.
3. *The innovation imperative: Forging Internal Audit's path to greater impact and influence*, Deloitte Touche Tohmatsu Limited, May 2018, https://www2.deloitte.com/nl/nl/pages/risk/articles/forging-internal-audits-path-to-greater-impact-and-influence.html.

Deloitte.

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.