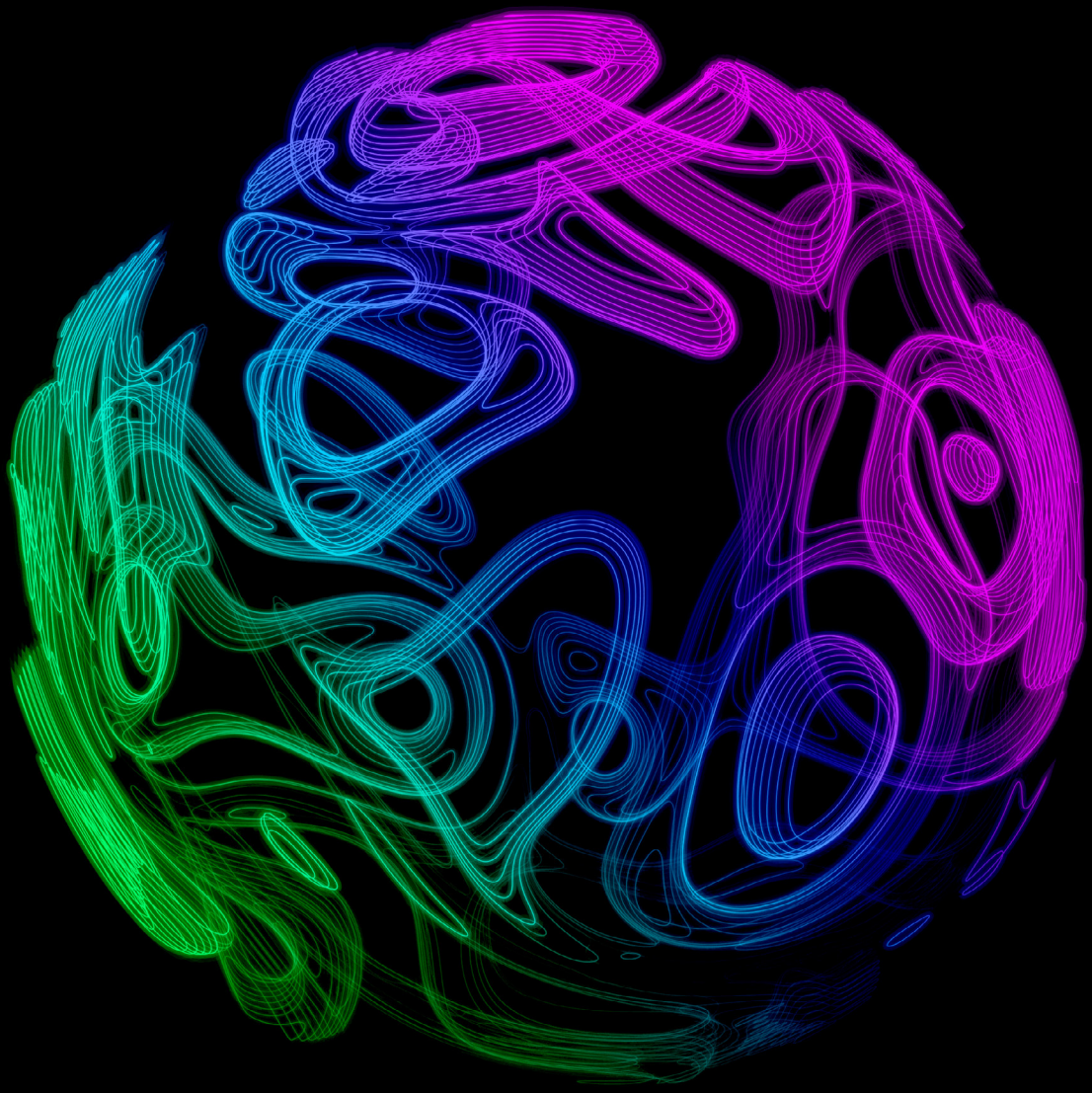
Deloitte.



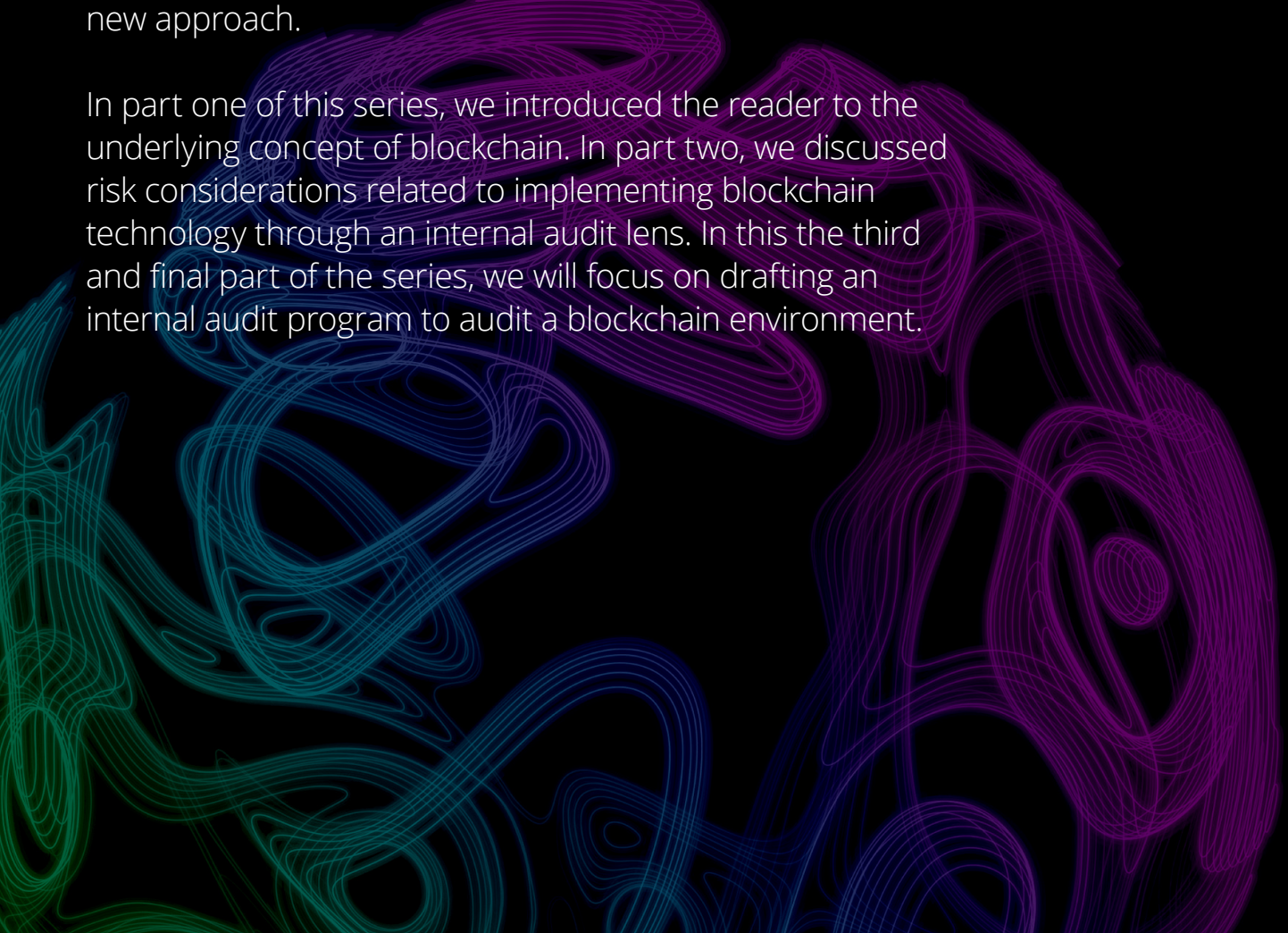
An internal auditor's guide to blockchain

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.

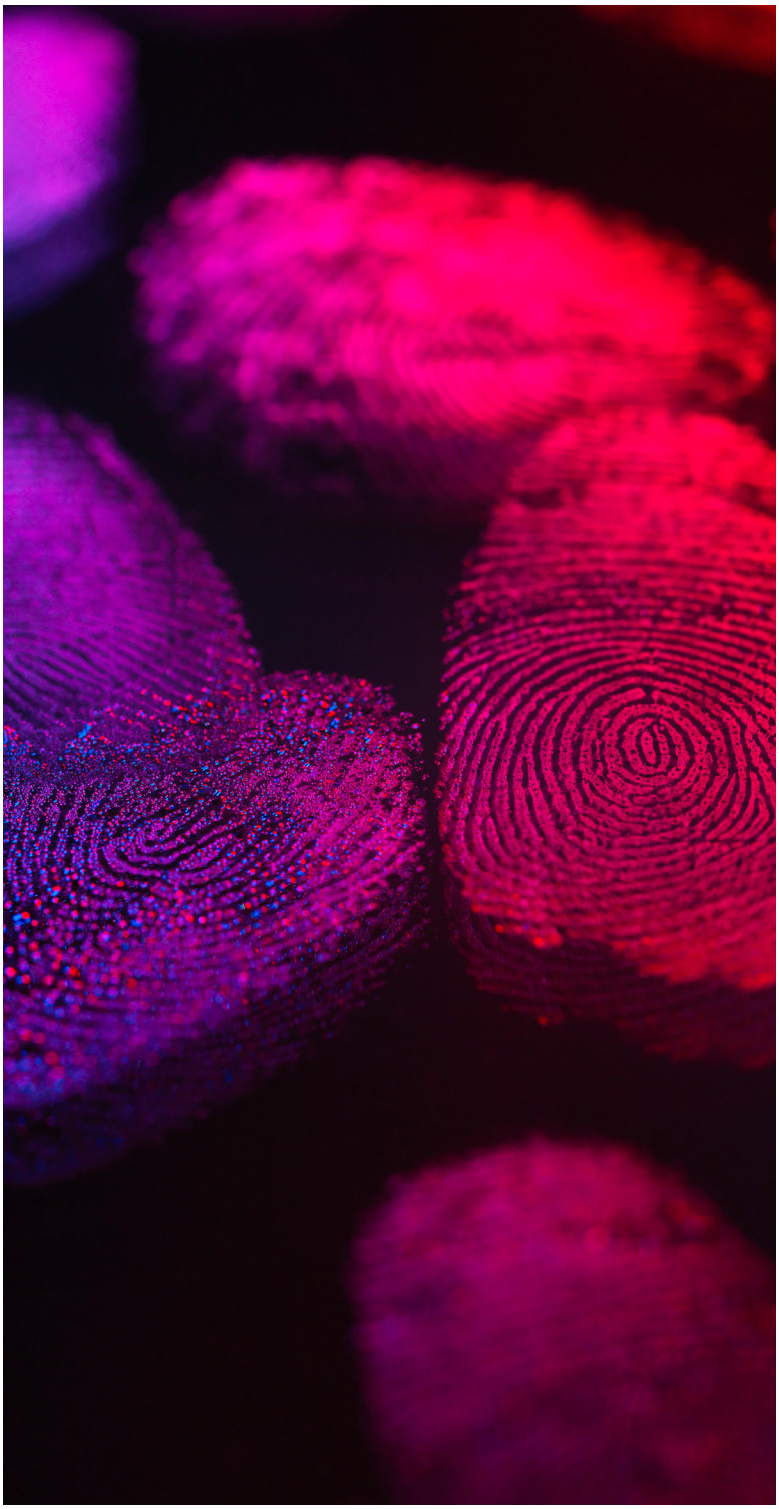


Case in point

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.