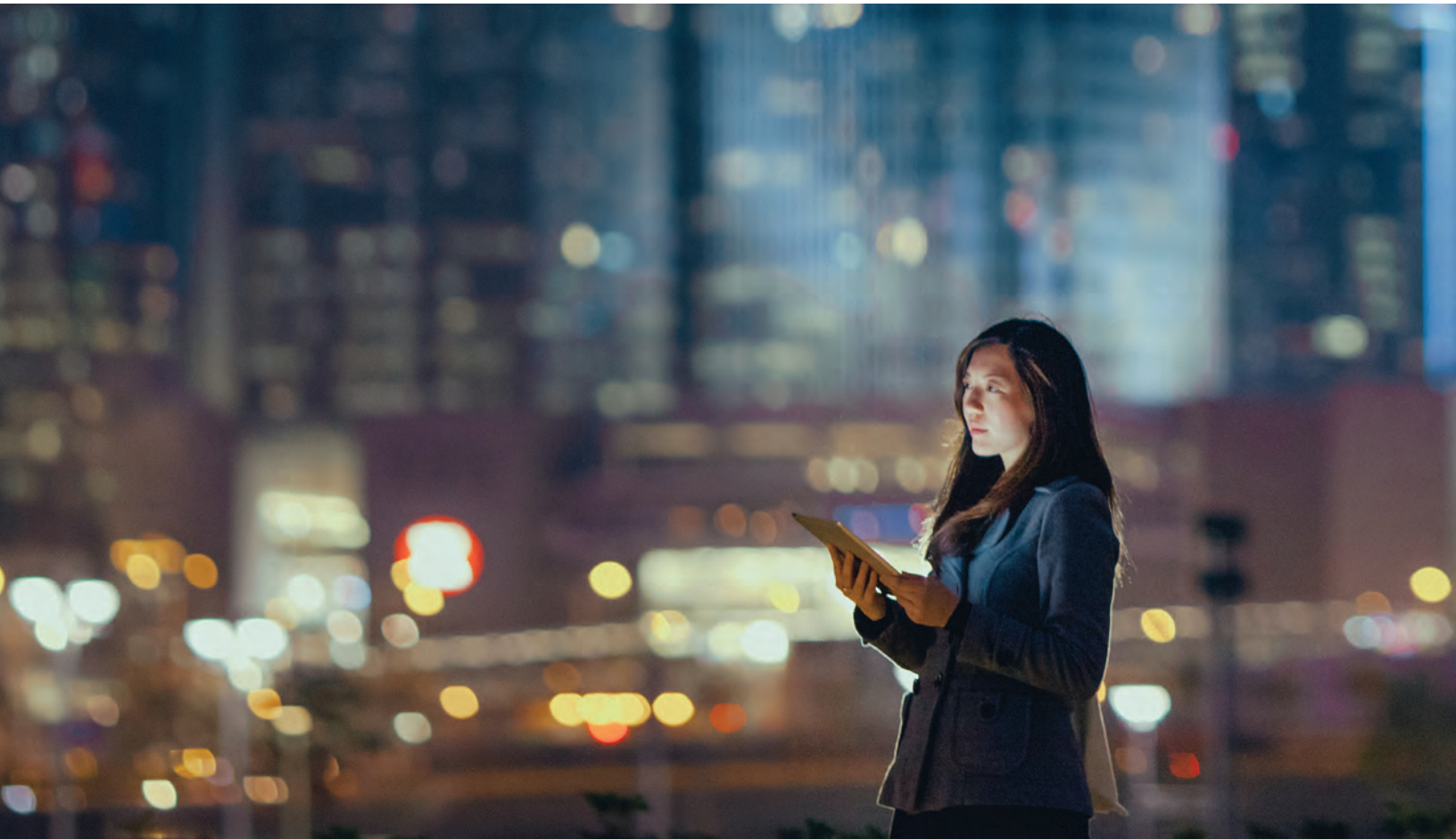
Crowe

Smart decisions. Lasting value.℠

June 2019

Smart Contract Audit: Ensuring Your Blockchain's Integrity

An article by Michael W. High; Richard C. Kloch Jr., CPA; and David Uhryniak



Smart contracts enabled by blockchain technology present organizations with a compelling promise of speed, cost savings, and autonomy. Use cases for smart contracts using blockchain are sparking conference room discussions in enterprises small and large. As chief information officers and chief technology officers explore the opportunities, they should consider the impact of smart contract adoption on their organizations, including how these smart contracts will be developed and maintained.

Smart contracts are business logic written as software code and deployed using blockchain – an emerging technology that is a combination of metadata, including transaction information, consensus algorithms, blocks, and hashes. Smart contracts are widely predicted to be disruptive to many industries, such as financial services, healthcare, and consumer products.

Blockchain technology is still evolving. As of August 2018, the technology entered the Gartner Hype Cycle Trough of Disillusionment, which typically precedes significant adoption.[1] However, Gartner predicts that by 2021 "less than 2 percent of global organizations will have adopted complex smart contracts, yet 20 percent of organizations will be subject to them."[2] If this prediction holds true, companies of all sizes will find themselves on the receiving end of a smart contract, perhaps before deploying blockchain technology in their organizations.

As with any new technology, internal audit departments will be among the vanguard, as they are challenged to develop new skills, audit controls, processes, and procedures to ensure each smart contract functions as designed.

The (new) smart contract

Cryptographer Nick Szabo first coined the term "smart contract" in 1996. Szabo foresaw a future that would allow both parties in a transaction to observe each other's performance of the contract terms, verify when the performance occurred, guarantee that only the details necessary for completion of the contract would be revealed to both parties, and be self-regulating to save time on enforcement. The oft-cited example of an early smart contract is a vending machine: Put in a dollar and press a set of keys for a favorite snack, and the machine reads those keys and duly provides the snack of choice.[3]

Blockchain technology has brought Szabo's vision to life in ways that its advocates herald as transformational. Through the blockchain immutable distributed ledgers, smart contracts coded onto a blockchain can automate manual processes and therefore have the potential to be more efficient than traditional business models.

A smart contract is computer code running on a blockchain that verifies or executes business processes. It is a digital and autonomous representation of the traditional contract process, which includes contract creation, execution, and enforcement.

The potential benefits of smart contracts include:

- Increased efficiency via reduced transaction time
- Increased profitability by automating manual functions
- Reduced transactional costs by eliminating the need for third-party intermediaries such as bankers or lawyers
- Limited fraud because of the ability to verify customer and counterparty identities

The qualities that make smart contracts so compelling will also create challenges:

- There's no errata slip in blockchain. The immutable nature of a smart contract on blockchain technology means it cannot ever be modified. A logic or coding error could create a vulnerability, not execute as the counterparty expects, or deliver an outcome that does not reflect the intent of either counterparty.
- Vulnerabilities can lead to asset or privacy breaches. Any vulnerabilities or logic errors in the software code could compromise the entire blockchain. A few well-known cryptocurrency blockchains have been the victim of asset breaches that occurred because of exploited vulnerabilities in the smart contract code.
- Interactions with oracles and off-chain technologies can create flaws. Smart contracts often rely on an expert for critical pieces of information, such as a federal disaster agency to identify geographies that have been flooded. These interactions represent potential weak points, as they give people with questionable intentions an opportunity to access the blockchain network.

The new requirements of auditing smart contracts

Adopting the use of smart contracts in an organization can have an impact on an array of governance, risk, and compliance responsibilities, including the following:

- **Governance.** Internal audit will need to assess and, if necessary, recommend changes to existing processes and procedures. It also will need to develop measures for performance management, accountability, coordination, methods of communication with the board, and functions affected by the smart contract(s).
- **Operational risks.** Internal audit will help define the process to mitigate previously identified risks. Smart contracts may be just one of several systems required to fulfill contract terms. The blockchain will need to interact with existing technology at the company on the other side of the transaction and, as a result, the ecosystem might only be as strong as its weakest link.
- **Technical risks.** Contracts are only as smart as those creating the logic and code. Flaws in the logic of a contract can lead to errors, vulnerabilities, or exposure. If the smart contract code is complicated, smart contract audits will need to be scheduled regularly during development and postproduction. Internal audit will need to determine the frequency of validating the code, as well as the processes and controls required to do so.
- **Cyberrisks.** Smart contracts are immutable – but not immune – to hacking or theft, which could result in the loss of digital assets. Internal audit, along with IT, will need to ensure the security protection is in place and measure its continued performance.
- **Compliance.** Smart contracts are legal contracts that require review for liability and regulatory compliance. Although the position of the Chamber of Digital Commerce is that existing U.S. law covers smart contracts, enforceability might be complicated by geography, industry, or regulatory governing body.

Internal audit staffing and skill needs

Internal audit departments in organizations considering smart contract use will need to begin training existing employees and recruiting new employees with the ability to understand smart contracts and blockchain technology, assess the impact on the organization, and ready the operation. The learning curve might be steep.

Auditing smart contracts requires an understanding of the business logic of the code, its compliance with set inputs, the result of set outputs, event and error testing, and testing the behavior of the contract under different input conditions. Individuals or teams will need experience in both the underlying code and the blockchain-specific characteristics the contract must satisfy.

Smart contracts and blockchain technology more generally will place increased demands on internal audit to develop or deepen technical skills, particularly in IT assurance, which is not always a formal part of internal audit.

Prepare for change

What should internal audit departments be doing today to prepare for discussions on use cases within their organizations?

Widespread use of blockchain is around the corner and includes extensive use of smart contracts. The possibilities for smart contract use are endless. Imagine the internet in 1996. How many people foresaw the services provided by Amazon or the products offered by Apple? The point is that we don't yet know all of the ways that blockchain and smart contracts will affect businesses. The best course for internal auditors to prepare for this new world of unknowns is to become educated about the technology. While the duties of internal auditors are likely to change, the critical importance of the internal audit function does not.

Learn more

Mike High
+1 954 489 7423
mike.high@crowe.com

Rich Kloch
Partner
+1 818 325 8424
rich.kloch@crowe.com

---

[1] Samuel Haig, "Blockchain Enters 'Trough of Disillusionment' According to Gartner," Bitcoin.com, Aug. 24, 2018, https://news.bitcoin.com/blockchain-enters-trough-disillusionment-gartner/

[2] Lydia Clougherty Jones and Erick Brethenoux, "Use Smart Contracts and AI to Drive Value From Data Investments," Gartner Inc., Sept. 28, 2018.

[3] Nick Szabo, "Smart Contracts: Building Blocks for Digital Markets," Extropy #16, 1996, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

crowe.com

FW-19006-003A