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.

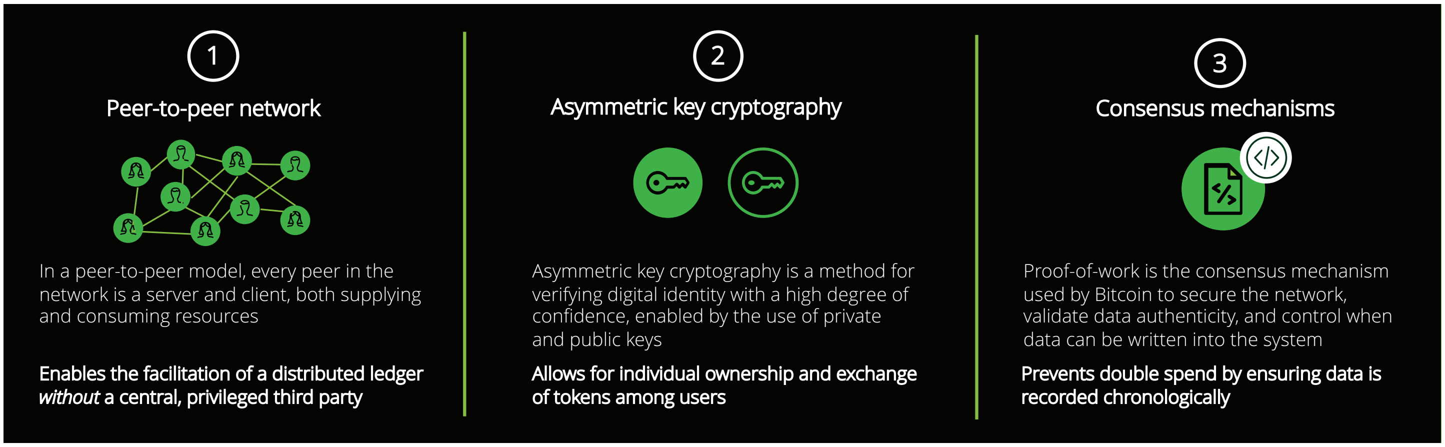
Introduction to blockchain

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



1 Peer-to-peer network

In a peer-to-peer model, every peer in the network is a server and client, both supplying and consuming resources

Enables the facilitation of a distributed ledger *without* a central, privileged third party

2 Asymmetric key cryptography

Asymmetric key cryptography is a method for verifying digital identity with a high degree of confidence, enabled by the use of private and public keys

Allows for individual ownership and exchange of tokens among users

3 Consensus mechanisms

Proof-of-work is the consensus mechanism used by Bitcoin to secure the network, validate data authenticity, and control when data can be written into the system

Prevents double spend by ensuring data is recorded chronologically

Figure 2. Specific features of different types of blockchain

Enterprise friendliness

	"Open"	"Federated"	"Closed"
	Public blockchain	Permissioned blockchain	Private blockchain
Access	Open read and write	Permissioned write and/or read	Centralized to one entity
Speed	Slower	Faster	Fastest
Security	Open network	Approved participants	One participant
Identity	Anonymous or pseudonymous	Known identities	Known identity
Asset	Native assets	Any asset	Determined by platform chosen

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.

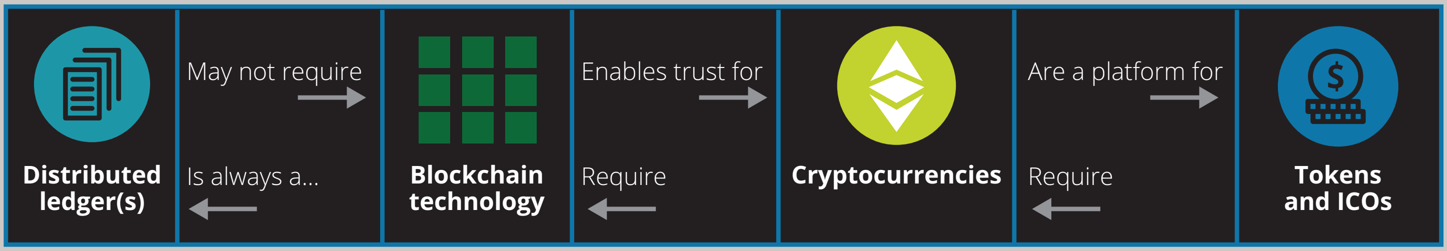
ICOs: An initial coin offering (ICO) is a "token sale" or "token launch" whereby an entity or group of entities creates tokens on a predefined date in order to generate capital or allow users to buy into an ecosystem. Many of the token launches plan to utilize the tokens in a future ecosystem that relies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



Distributed ledger(s)

May not require →

Is always a... ←

Blockchain technology

Enables trust for →

Require ←

Cryptocurrencies

Are a platform for →

Require ←

Tokens and ICOs

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.

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

Copyright © 2019 Deloitte Development LLC. All rights reserved.