

Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession



Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession



DISCLAIMER

This paper was prepared by the Chartered Professional Accountants of Canada (CPA Canada) and the American Institute of CPAs (AICPA), as non-authoritative guidance.

CPA Canada and AICPA do not accept any responsibility or liability that might occur directly or indirectly as a consequence of the use, application or reliance on this material.

Copyright © 2017 Deloitte Development LLC.

All rights reserved. This publication is protected by copyright and written permission is required to reproduce, store in a retrieval system or transmit in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise).

For information regarding permission, please contact permissions@cpacanada.ca

Table of Contents

Executive Summary	1
The ABCs of Blockchain	3
What Is Blockchain Technology?	3
Characteristics of a Blockchain	4
What Are the Benefits?	4
Blockchains Are Not Made Equal	5
Permissionless Blockchain	5
Permissioned Blockchain	6
Evolution of Blockchain: Smart Contracts	6
Where Can Blockchain Be Applied?	8
The Potential Impact of Blockchain on the Financial Statement Audit and the Assurance Profession	9
Financial Statement Auditing	9
How Audit and Assurance Might Evolve with Blockchain	10
Opportunities for Future Roles of the CPA in the Blockchain Ecosystem	11
Auditor of Smart Contracts and Oracles	11
Service Auditor of Consortium Blockchains	12
Administrator Function	12
Arbitration Function	13

Conclusion	14
Call to Action	15
Other Resources	15
About the Authors	16
About Deloitte	16

Executive Summary

Blockchain was first introduced as the core technology behind Bitcoin,¹ the headline-grabbing decentralized digital currency² ecosystem proposed in 2008. The appeal of blockchain technology lies in its use of peer-to-peer network technology³ combined with cryptography.⁴ This combination enables parties who do not know each other to conduct transactions without requiring a traditional trusted intermediary such as a bank or payment processing network. By eliminating the intermediary and harnessing the power of peer-to-peer networks, blockchain technology may provide new opportunities to reduce transaction costs dramatically and decrease transaction settlement time. Blockchain has the potential to transform and disrupt a multitude of industries, from financial services to the public sector to healthcare. As a result, a number of venture capital firms and large enterprises are investing in blockchain technology research and trials to re-imagine traditional practices and business models.

In recent years, blockchain technology has evolved far beyond bitcoin and is now being tested in a broad range of business and financial applications. However, blockchain technology is still emerging and has not yet been proven at enterprise scale, which is a fundamental challenge to blockchain's transformative potential. In addition, many accounting firms have undertaken blockchain initiatives to further understand the implications of this technology. It is important for the audit and assurance profession to stay abreast of developments in this space, and we encourage Chartered Professional Accountants and Certified Public Accountants (collectively, CPA auditors) to learn more about this technology. The focus of this paper is to explain blockchain technology and how it could potentially impact the financial statement audit, introduce possible new assurance services and new roles for the CPA auditor in the blockchain ecosystem.

- 1 The term "bitcoin" is used when describing a bitcoin as a unit of account, whereas "Bitcoin" is used when describing the concept or the entire network designed by Satoshi Nakamoto.
- 2 Digital currency can be defined as an Internet-based form of currency or medium of exchange (as distinct from physical currency such as banknotes and coins) that exhibits properties similar to physical currencies but allows for instantaneous transactions and borderless transfers of ownership.
- 3 Peer-to-peer computing or networking is based on a distributed application architecture that shares tasks among peers. All participants engage equally in the application to form a peer-to-peer network of nodes.
- 4 Modern cryptography uses mathematics, computer science and electrical engineering to enable secure communication between two parties in the presence of a third party.

Blockchain technology has the potential to impact all recordkeeping processes, including the way transactions are initiated, processed, authorized, recorded and reported. Changes in business models and business processes may impact back-office activities such as financial reporting and tax preparation. Independent auditors likewise will need to understand this technology as it is implemented at their clients. Both the role and skill sets of CPA auditors may change as new blockchain-based techniques and procedures emerge. For example, methods for obtaining sufficient appropriate audit evidence will need to consider both traditional stand-alone general ledgers as well as blockchain ledgers. Additionally, there is potential for greater standardization and transparency in reporting and accounting, which could enable more efficient data extraction and analysis.

Blockchain technology could bring new challenges and opportunities to the audit and assurance profession. While traditional audit and assurance services will remain important, a CPA auditor's approach may change. Just as the audit and assurance profession is evolving today, with audit innovations in automation and data analytics, blockchain technology may also have a significant impact on the way auditors execute their engagements. Moreover, CPAs may need to broaden their skill sets and knowledge to meet the anticipated demands of the business world as blockchain technology is more widely adopted.

The Chartered Professional Accountants of Canada (CPA Canada), the American Institute of CPAs (AICPA), and the University of Waterloo Centre for Information Integrity and Information System Assurance (UW CISA) all encourage the audit and assurance profession to continue the discussions already begun in regard to the impact of blockchain technology on the profession and auditing standards.

The ABCs of Blockchain

What Is Blockchain Technology?

A blockchain is a digital ledger created to capture transactions conducted among various parties in a network. It is a peer-to-peer, Internet-based distributed ledger which includes all transactions since its creation. All participants (i.e., individuals or businesses) using the shared database are “nodes” connected to the blockchain,⁵ each maintaining an identical copy of the ledger. Every entry into a blockchain is a transaction that represents an exchange of value between participants (i.e., a digital asset that represents rights, obligations or ownership). In practice, many different types of blockchains are being developed and tested. However, most blockchains follow this general framework and approach.

When one participant wants to send value to another, all the other nodes in the network communicate with each other using a pre-determined mechanism to check that the new transaction is valid. This mechanism is referred to as a consensus algorithm.⁶ Once a transaction has been accepted by the network, all copies of the ledger are updated with the new information. Multiple transactions are usually combined into a “block” that is added to the ledger. Each block contains information that refers back to previous blocks and thus all blocks in the chain link together in the distributed identical copies. Participating nodes can add new, time-stamped transactions, but participants cannot delete or alter the entries once they have been validated and accepted by the network. If a node modified a previous block, it would not sync with the rest of the network and would be excluded from the blockchain. A properly functioning blockchain is thus immutable despite lacking a central administrator.

5 The blockchain is managed by a network of nodes. When a node first accesses the database (i.e., the blockchain), it downloads its own instance of the entire ledger.

6 An algorithm is a process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer. Consensus involves multiple nodes agreeing on values. A consensus algorithm is used to agree among the nodes. In practice, there are different types of consensus algorithms and mechanisms.

Characteristics of a Blockchain

As a near real-time and distributed digital ledger, a blockchain has several unique and valuable characteristics that, over time, could transform a wide range of industries:

Near real-time settlement	A blockchain enables the near real-time settlement of transactions, thus reducing risk of non-payment by one party to the transaction.
Distributed ledger	The peer-to-peer distributed network contains a public history of transactions. A blockchain is distributed, highly available and retains a secure record of proof that the transaction occurred.
Irreversibility	A blockchain contains a verifiable record of every single transaction ever made on that blockchain. This prevents double spending of the item tracked by the blockchain.
Censorship resistant	The economic rules built into a blockchain model provide monetary incentives for the independent participants to continue validating new blocks. This means a blockchain continues to grow without an "owner". It is also costly to censor.

What Are the Benefits?

A major advantage of blockchain technology is its distributed nature. In today's capital markets, the transfer of value between two parties generally requires centralized transaction processors such as banks or credit card networks. These processors reduce counterparty risk for each party by serving as an intermediary but centralize credit risks with themselves. Each of these centralized processors maintains its own separate ledger; the transacting parties rely on these processors to execute transactions accurately and securely. For providing this service, the transaction processors receive a fee. In contrast, a blockchain allows parties to transact directly with each other through a single distributed ledger, thus eliminating one of the needs for centralized transaction processors.

In addition to being efficient, the blockchain has other unique characteristics that make it a breakthrough innovation. Blockchain is considered reliable because full copies of the blockchain ledger are maintained by all active nodes. Thus, if one node goes offline, the ledger is still readily available to all other participants in the network. A blockchain lacks a single point of failure. In addition, each block in the chain refers to the previous blocks, which prevents deletion or reversing transactions once they are appended to the blockchain. Nodes on a blockchain network can come and go but the network integrity and reliability will remain intact as long as it is being used. In this way, no single party controls a blockchain and no single party can modify it or turn it off.

Blockchains Are Not Made Equal

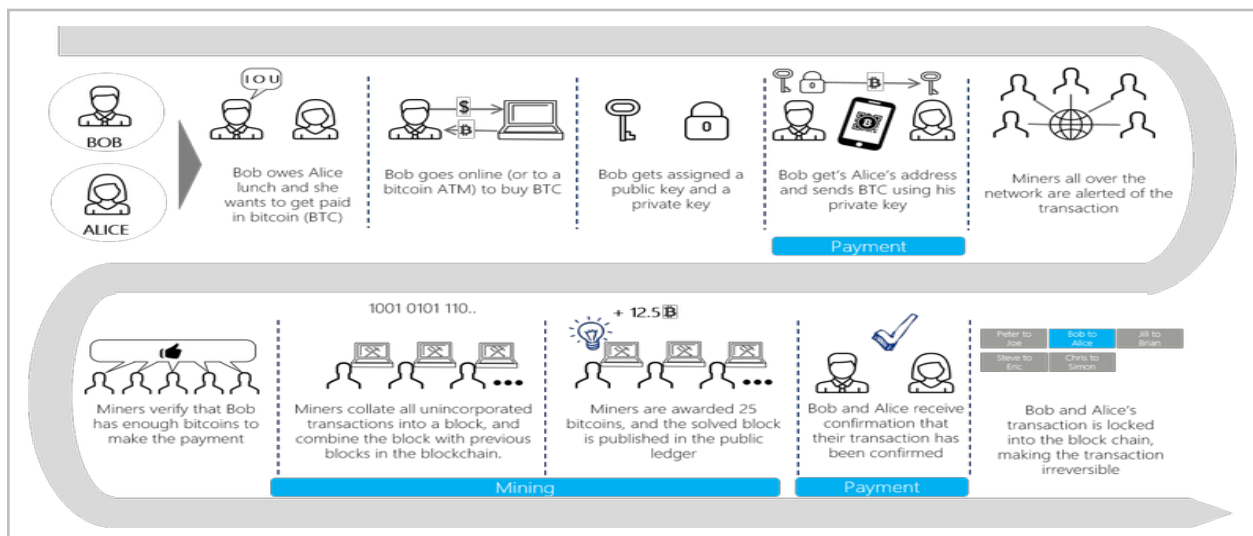
CPA auditors should be aware that blockchain technology is a new form of database and each blockchain implementation may have different characteristics that make it unique. While the technology is emerging, there is a risk that a specific blockchain implementation does not live up to the promise of the technology. In the current ecosystem, there are two major classifications of blockchain networks: permissionless and permissioned. The biggest difference is the determination of which parties are allowed access to the network. A blockchain may be shared publicly with anyone who has access to the Internet (i.e., permissionless or “public” blockchain), or shared with only certain participants (i.e., permissioned or “private” blockchain).

Permissionless Blockchain

A permissionless blockchain is open to any potential user. For example, the Bitcoin blockchain is a public or permissionless blockchain; anyone can participate as a node in the chain by agreeing to relay and validate transactions on the network thereby offering their computer processor as a node. Joining the blockchain is as simple as downloading the software and bitcoin ledger from the Internet. Because the blockchain maintains a list of every transaction ever performed, it reflects the full transaction history and account balances of all parties.

Figure 1 is an example of a transfer of bitcoin (BTC) from one individual to another. When one party sends bitcoin (i.e., buyer sending value) to another party (i.e., seller receiving value), the Bitcoin blockchain is updated by the following process, including a process referred to as “mining”:⁷

FIGURE 1



An example of a bitcoin transaction which is a public/permissionless blockchain: peer-to-peer payment over the Bitcoin network. **Note:** Permissioned blockchains may have consensus protocols that may be similar to or different from Figure 1 because they are dependent on the agreement of the participants.

⁷ Mining is the act of adding new transactions to the blockchain by solving algorithmic problems with computing resources. Miners or participants in this process are awarded bitcoin for the computational effort they expend in order to support the network.

While a permissionless blockchain lives up to the potential of the technology by allowing anyone access, it can have limitations that are difficult to remedy. For example, when the blockchain is created, transaction volume or size may be set to the best available technology at the time. As technology advances, initial settings may become limitations that may make the blockchain out of date, potentially slowing transaction speeds. Users of permissionless blockchains should also be aware that their transaction history is exposed to anyone who downloads the database for as long as the database is active. While it may be difficult for an outside party to identify a participant on the blockchain, if a participant is identified, their entire transaction history would be public.

Permissioned Blockchain

The limitations of permissionless blockchains have led some organizations to explore the use of private or permissioned/consortium blockchains, which restrict participation in the blockchain network to participants who have already been given permission by agreed-upon administrators.⁸ These blockchains address some of the drawbacks of public blockchains, but also sacrifice some of the potential benefits (e.g., decentralized transactions, wide distribution of the ledger, and a truly decentralized environment without any intermediaries). Permissioned blockchains are likely to be set up by a consortium of parties that can collectively benefit from a shared ledger system. For example, a supply chain network may want to use a blockchain to track the movement of goods.

Given the widely acknowledged limitations inherent in public blockchains, private or permissioned/consortium blockchains are expected to have a higher adoption rate in the near term, especially in enterprise environments. However, adoption of public blockchains is also expected to increase in the longer term once the key infrastructure and technical challenges of the new technology have been addressed. The paradigm shift introduced by blockchain (and the level of interest in blockchain-based initiatives) in many ways parallels the development of the Internet in the 1990s. With Internet technology, there was a strong initial emphasis on corporate intranets until a critical mass was reached and the broader public Internet began to offer more benefits to offset the perceived risks of participating in an open network.

Evolution of Blockchain: Smart Contracts

A key development in blockchain technology was the introduction of smart contracts. Smart contracts are computer code stored on a blockchain that executes actions under specified circumstances. They enable counterparties to automate tasks usually performed manually through a third-party intermediary. Smart-contract technology can speed up business processes, reduce operational error, and improve cost efficiency.

⁸ A consortium is a group of organizations that aims to achieve a common objective.

For example, two parties could use a smart contract to enter into a common derivative contract to hedge the price of oil at the end of the year. Once the terms of the contract have been agreed to, it is appended to the blockchain and the wagered funds are held in escrow and registered on a blockchain. At year end, the smart contract would read the price of oil by referencing a trusted source defined in the smart contract (known as an “oracle”), calculate the settlement amount, and then transfer funds to the winning party on the blockchain.

Ethereum⁹, at the time of publication the second largest blockchain network after Bitcoin (based on market capitalization), was the first platform to introduce the concept of a smart contract that could be deployed and executed on a distributed blockchain network. Ethereum is a public protocol that allows anyone accessing the Ethereum blockchain network to view the terms of each contract unless they are protected by encryption. This may prove problematic for contracts involving sensitive information (e.g., a hedge fund using smart contracts to execute a proprietary investment strategy or to quietly build a position in a particular stock). However, developers are actively building solutions to preserve confidentiality while taking advantage of public blockchains. Even with such perceived limitations, there is significant market interest across industries in smart contract applications because they could transform the processing and settlement of a wide range of contracts, from hedging and futures derivatives to automated payments under lease contracts.

Smart contracts are a method to automate the contracting process and enable monitoring and enforcement of contractual promises with minimal human intervention. Automation can improve efficiency, reduce settlement times and operational errors. Because using smart contract technology requires the translation of all contractual terms into logic, it may also improve contract compliance by reducing ambiguity in certain situations.

As smart contracts continue to evolve, inherent risks may emerge that need to be mitigated. For example, when setting up a smart contract, the parties may decide not to address every possible outcome, or they may include some level of flexibility so they do not limit themselves. This could lead to smart contracts with vulnerabilities or errors that could lead to unexpected business outcomes. Parties may find it difficult to renegotiate the terms of a deal or modify terms due to an unforeseen error. Also, incomplete or flexible contracts can lead to settlement problems and disputes. Perhaps most importantly, however, at the date of this publication, smart contracts have not been tested thoroughly in the court system. Nevertheless, smart contracts offer a compelling use case for blockchain adoption.

9 www.ethereum.org

Where Can Blockchain Be Applied?

Blockchain technology offers the potential to impact a wide range of industries. The most promising applications exist where transferring value or assets between parties is currently cumbersome, expensive and requires one or more centralized organization. A specific activity attracting significant interest is securities settlement, which today can involve multi-day clearing and settlement processes between multiple financial intermediaries. Certain financial services experts believe the financial services industry is on the verge of being disrupted: advances in innovative technologies such as blockchain are expected to transform the industry and its workforce by automating many of the activities currently performed by humans.

The table below illustrates industries where interest in blockchain technology and its potential transformative benefits has been high, as demonstrated by significant investments from both venture capital firms and large enterprises.

Financial services	Several stock exchanges around the world are piloting a blockchain platform that enables the issuance and transfer of private securities. Additionally, multiple groups of banks are considering use cases for trade finance, cross-border payments, and other banking processes.
Consumer and industrial products	Companies in the consumer and industrial industries are exploring the use of blockchain to digitize and track the origins and history of transactions in various commodities.
Life sciences and healthcare	Healthcare organizations are exploring the use of blockchain to secure the integrity of electronic medical records, medical billing, claims, and other records.
Public sector	Governments are exploring blockchain to support asset registries such as land and corporate shares.
Energy and resources	Ethereum is being used to establish smart-grid technology that would allow for surplus energy to be used as tradable digital assets among consumers.

Since all businesses track information and face the challenge of reconciling data with counterparties, blockchain technology has the potential to be relevant to everyone. The first major adoptions, however, may transform business processes and old legacy systems that are cumbersome to maintain.

The Potential Impact of Blockchain on the Financial Statement Audit and the Assurance Profession

Financial Statement Auditing

The public looks to CPA auditors to enhance trust in the audited information of the companies they audit and help a multi-trillion dollar capital markets system function with greater confidence. CPA auditors practice under strict regulations, professional codes of conduct and auditing standards, and are independent of the entities they audit. They apply objectivity and professional skepticism to provide reasonable assurance about whether an entity's financial statements are free of material misstatement and, depending on the engagement, about whether a company's internal controls over financial reporting are operating effectively.

Some publications have hinted that blockchain technology might eliminate the need for a financial statement audit by a CPA auditor altogether. If all transactions are captured in an immutable blockchain, then what is left for a CPA auditor to audit?

While verifying the occurrence of a transaction is a building block in a financial statement audit, it is just one of the important aspects. An audit involves an assessment that recorded transactions are supported by evidence that is relevant, reliable, objective, accurate, and verifiable. The acceptance of a transaction into a reliable blockchain may constitute sufficient appropriate audit evidence for certain financial statement assertions such as the occurrence of the transaction (e.g., that an asset recorded on the blockchain has transferred from a seller to a buyer). For example, in a bitcoin transaction for a product, the transfer of bitcoin is recorded on the blockchain. However, the auditor may or may not be able to determine the product that was delivered by solely evaluating information on the Bitcoin blockchain.

Therefore, recording a transaction in a blockchain may or may not provide sufficient appropriate audit evidence related to the nature of the transaction. In other words, a transaction recorded in a blockchain may still be:

- unauthorized, fraudulent or illegal
- executed between related parties
- linked to a side agreement that is “off-chain”
- incorrectly classified in the financial statements.

Furthermore, many transactions recorded in the financial statements reflect estimated values that differ from historical cost. Auditors will still need to consider and perform audit procedures on management’s estimates, even if the underlying transactions are recorded in a blockchain.

Widespread blockchain adoption may enable central locations to obtain audit data, and CPA auditors may develop procedures to obtain audit evidence directly from blockchains. However, even for such transactions, the CPA auditor needs to consider the risk that the information is inaccurate due to error or fraud. This will present new challenges because a blockchain likely would not be controlled by the entity being audited. The CPA auditor will need to extract the data from the blockchain and also consider whether it is reliable. This process may include considering general information technology controls (GITCs) related to the blockchain environment. It also may require the CPA auditor to understand and assess the reliability of the consensus protocol for the specific blockchain. This assessment may need to include consideration of whether the protocol could be manipulated. As more and more organizations explore the use of private or public blockchains, CPA auditors need to be aware of the potential impact this may have on their audits as a new source of information for the financial statements. They will also need to evaluate management’s accounting policies for digital assets and liabilities, which are currently not directly addressed in international financial reporting standards or in U.S. generally accepted accounting principles. They will need to consider how to tailor audit procedures to take advantage of blockchain benefits as well as address incremental risks.

How Audit and Assurance Might Evolve with Blockchain

Despite these complexities, blockchain technology offers an opportunity to streamline financial reporting and audit processes. Today, account reconciliations, trial balances, journal entries, sub-ledger extracts, and supporting spreadsheet files are provided to a CPA auditor in a variety of electronic and manual formats. Each audit begins with different information and schedules that require a CPA auditor to invest significant time when planning an audit. In a blockchain world, the CPA auditor could have near real-time data access via read-only nodes on blockchains. This may allow an auditor to obtain information required for the audit in a consistent, recurring format.

As more and more entities and processes migrate to blockchain solutions, accessing information in the blockchain will likely become more efficient. For example, if a significant class of transactions for an industry is recorded in a blockchain, it might be possible for a CPA auditor to develop software to continuously audit organizations using the blockchain. This could eliminate many of the manual data extraction and audit preparation activities that are labour intensive and time consuming for an entity's management and staff. Speeding up audit preparation activities could help reduce the lag between the transaction and verification dates—one of the major criticisms of financial reporting. Reducing lag time could offer the opportunity to increase the efficiency and effectiveness of financial reporting and auditing by enabling management and auditors to focus on riskier and more complex transactions while conducting routine auditing in near real time.

With blockchain-enabled digitization, auditors could deploy more automation, analytics and machine-learning capabilities such as automatically alerting relevant parties about unusual transactions on a near real-time basis. Supporting documentation, such as contracts, agreements, purchase orders, and invoices could be encrypted and securely stored or linked to a blockchain. By giving CPA auditors access to unalterable audit evidence, the pace of financial reporting and auditing could be improved.

While the audit process may become more continuous, auditors will still have to apply professional judgment when analyzing accounting estimates and other judgments made by management in the preparation of financial statements. In addition, for areas that become automated, they will also need to evaluate and test internal controls over the data integrity of all sources of relevant financial information.

Opportunities for Future Roles of the CPA in the Blockchain Ecosystem

As blockchain systems standardize transaction processing across many industries, a CPA, including CPA auditors, may be able to help provide assurance to users of the technology. The CPA may be able to fill a potential future role because of their skill sets, independence, objectivity, and expertise.

The following list of potential new roles for a CPA is illustrative only and not all-inclusive; significant regulatory and professional hurdles may remain before a CPA is able to take on these potential roles.

Auditor of Smart Contracts and Oracles

As described above, smart contracts can be embedded in a blockchain to automate business processes. Contracting parties may want to engage an assurance provider to verify that smart contracts are implemented with the correct business logic. In addition, a CPA auditor could verify the interface between smart contracts and external data sources that

trigger business events. Without an independent evaluation, users of blockchain technologies face the risk of unidentified errors or vulnerabilities. To take on this new role, a CPA auditor may need a new skill set, including understanding technical programming language and the functions of a blockchain. This type of role also raises important questions for the auditing profession, including:

- What types of skill sets does the profession need to remain relevant?
- What factors would impact assurance engagement risk?
- What would an assurance provider's ongoing responsibility entail once a smart contract is released into a blockchain?

In the context of a financial statement audit, management will be responsible for establishing controls to verify whether the smart-contract source code is consistent with the intended business logic. An independent CPA auditing an entity with smart contracts/ blockchain is likely to consider management's controls over the smart contract code. However, many companies may choose to reuse smart contracts built by other entities already active on a blockchain. Future auditing standards and auditing guidance may need to contemplate this technology and thereby bring clarity to the role of the CPA auditor in those scenarios.

Service Auditor of Consortium Blockchains

Prior to launching a new application on an existing blockchain platform or leveraging or subscribing to an existing blockchain product, users of the system may desire independent assurance as to the stability and robustness of its architecture. Instead of each participant performing their own due diligence, it may be more efficient to hire a CPA to achieve these objectives. In addition, critical blockchain elements (e.g., cryptographic key management) should be designed to include sophisticated GITCs that provide ongoing protection for sensitive information, as well as processing controls over security, availability, processing integrity, privacy and confidentiality. On an ongoing basis, a trusted and independent third party may be needed to provide assurance as to the effectiveness of controls over a private blockchain. This type of service raises important questions for the profession:

- When providing assurance across a blockchain, who is the client?
- How would a CPA auditor assess engagement risk for an autonomous system?
- How would independence rules apply to users of a blockchain?

Administrator Function

Permissioned blockchain solutions may benefit from a trusted, independent and unbiased third party to perform the functions of a central access-granting administrator. This function could be responsible for verification of identity or a further vetting process to be completed by a participant before they are granted access to a blockchain. This central administrator could validate the enforcement and monitoring of the blockchain's protocols. If this function is performed by a user/node of the blockchain, then an undue advantage could exist and trust among consortium members could be weakened. Since this role would be designed

to create trust for the blockchain as a whole, due care will be needed when establishing both its function and its legal responsibilities. As a trusted professional, an independent CPA may be capable of carrying out this responsibility. However, this role would raise new questions for the profession:

- By taking on such a critical role, is the assurance provider independent from the blockchain participants?
- Could the CPA auditor conduct financial statement audits on those participants?

Arbitration Function

Business arrangements can be complex and result in disputes between even the most well-intentioned parties. For a permissioned blockchain, an arbitration function might be needed in the future to settle disputes among the consortium-blockchain participants. This function is analogous to the executor of an estate, a role typically filled by various qualified professionals, including CPA auditors. Participants on the blockchain may require this type of function to enforce contract terms where the spirit of the smart contract departs from a legal document, contractual agreement or letter. Further considerations should be explored to determine whether an arbitration function is necessary. If CPAs want to take on this role, critical questions will need to be answered, such as:

- What legal framework would be used to settle disputes?
- What skill set would be required for a CPA auditor?
- Could this role create unintended threats to independence regarding attest clients?

Conclusion

There are still many unknowns with respect to how blockchain will impact the audit and assurance profession, including the speed with which it will do so. Blockchain is already impacting CPA auditors of those organizations using blockchain to record transactions and the rate of adoption is expected to continue to increase. However, in the immediate future, blockchain technology will not replace financial reporting and financial statement auditing. Audited financial statements are a cornerstone of business and play a key role in debt and equity financing, participation in capital markets, mergers and acquisitions, regulatory compliance, and the effective and efficient functioning of capital markets. Financial statements reflect management assertions, including estimates, many of which cannot be easily summarized or calculated in blockchains.

Furthermore, the process of an independent audit of financial statements enhances the trust that is crucial for the effective functioning of the capital markets system. Any erosion of this trust may damage an entity's reputation, stock price and shareholder value, and can result in fines, penalties or loss of assets. Users of financial statements expect CPA auditors to perform an independent audit of the financial statements using their professional skepticism. CPA auditors conclude whether they have obtained reasonable assurance that the financial statements of an entity, taken as a whole, are free from material misstatement, whether due to fraud or error. Blockchains are unlikely to replace these judgments by a financial statement auditor. However, CPA auditors need to monitor developments in blockchain technology because it will impact their clients' information technology systems. CPA auditors will need to be conversant with the basics of blockchain technology and work with experts to audit the complex technical risks associated with blockchains.

In addition, CPA auditors should be aware of opportunities to leverage their clients' adoption of blockchain technology to improve data gathering during the audit. They should also consider whether blockchain technology will allow them to create automated audit routines. The auditing profession must embrace and "lean in" to the opportunities and challenges from widespread blockchain adoption. CPA auditors are encouraged to monitor developments in blockchain technology because they have an opportunity to evolve, learn, and capitalize on their already proven ability to adapt to the needs of a rapidly changing business world.

Call to Action

Blockchain technology is part of the rapid digitization of business processes. CPA Canada and the AICPA urge CPAs, including CPA auditors, to continue to monitor developments in blockchain technology (see the [Other Resources](#) section below for suggestions on additional reading). Additionally, CPA Canada and the AICPA encourage auditing and accounting standard setters to monitor progress and adoption of blockchain technology in the business ecosystem. Questions around audit evidence, internal controls, independence, risk assessment, cyber security and more are likely to emerge and require new consideration by standard setters. Finally, the CPA profession needs to contemplate the skills that will be required in the future so CPAs will be able to meet the demands of the market in a business world where blockchain technology has been widely adopted. As such, the CPA profession should consider additions to the education syllabus for new CPAs and continuing education requirements for experienced CPAs. The pace of innovation related to this technology is unrelenting; new digital asset classes are being rapidly created to “live” on the blockchain. As critical professional service providers who underpin well-functioning markets, CPAs should lean in, help identify the risks associated with this new technology, and find ways to leverage its benefits.

Other Resources

CPA Canada Blockchain Publication—[Technological Disruption of Capital Markets and Reporting? An Introduction to Blockchain](#)

CPA Canada Magazine—[An intro to blockchain technology](#)

CPA Canada Magazine—[Blockchain—Part 2: Under the Hood](#)

Deloitte Publication—[Driving FinTech innovation in financial services](#)

Deloitte Publication—[Blockchain: Enigma, Paradox, Opportunity](#)

Deloitte University Press—[Series of blockchain blog posts](#)

Deloitte Webpage—[Break through with Blockchain: How can financial institutions leverage a powerful technology?](#)

Harvard Business Review—[The Truth about Blockchain](#)

Harvard Business Review—[The Blockchain Will Do to the Financial System What the Internet Did to Media](#)

World Economic Forum Video—[What is Blockchain?](#)

Ted Talks by Don Tapscott—[How the blockchain is changing money and business](#)

About the Authors

CPA Canada, the AICPA and the UWCISA would like to express their gratitude to William Bible, Jon Raphael and Peter Taylor of Deloitte & Touche LLP, and Iliana Oris Valiente, CPA, CA, who authored this publication.

CPA Canada, the AICPA and UWCISA would also like to express their gratitude to the following professionals for their contributions to this publication: Eric Piscini of Deloitte Consulting LLP, Mawadda Basir of Deloitte Canada, Malik Datardina of Deloitte Canada, Theo Stratopoulos of the University of Waterloo, Canada, and Juli-ann Gorgi, CPA, CA, MAcc of Toronto, Canada.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), a U.K. private company limited by guarantee, 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 U.S. 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/aboutus to learn more about our global network of member firms.



CPA

CHARTERED
PROFESSIONAL
ACCOUNTANTS
CANADA

277 WELLINGTON STREET WEST
TORONTO, ON CANADA M5V 3H2
T. 416 977.3222 F. 416 977.8585
WWW.CPACANADA.CA