

How do the current auditing standards fit the emergent use of blockchain?

Marion Pauline Gauthier and Nathalie Brender

Geneva School of Business Administration, HES-SO, University of Applied Sciences and Arts Western Switzerland, Geneva, Switzerland

Received 23 December 2019
Revised 15 July 2020
23 November 2020
Accepted 7 December 2020

Abstract

Purpose – Blockchain is expected to impact reporting and auditing processes. Indeed, the increasing use of blockchain could affect the nature and extent of information available to auditors and how audits are performed. This paper aims to investigate how auditors are assessing the relevance of the current auditing standards in light of the emergent use of blockchain technology.

Design/methodology/approach – Based on qualitative content analysis, this paper analyzed semi-structured interviews with auditors to understand their shared perception of how the current auditing standards address blockchain's emergence.

Findings – The findings reveal a growing demand for information technology (IT) auditing standards, as well as a mismatch in timing between the quickly changing IT environment and the regulators' slowness in releasing new standards or updating standards.

Research limitations/implications – The findings reflect the external auditors' points of view and cannot be generalized to all countries, but future studies should address the development of specific IT-related auditing standards to better fit the fast-evolving technology environment in ways that consider the other stakeholders' points of view, including those of the standard setters.

Practical implications – The results of this study show that auditors consider the current auditing standards for IT to be too vague, and they need more guidance on both auditing blockchain and using technologies as audit tools.

Originality/value – The original contribution of this study lies in the in-depth understanding it provides of the adequacy of the current auditing standards to audit companies using blockchain, which is an under-researched topic.

Keywords Auditing, Blockchain, New technologies, Auditing standards

Paper type Research paper

1. Introduction

Since its inception in 2008 with Bitcoin, blockchain technology has first been extended to cryptocurrencies and then to pilot projects for financial applications and more recently to business applications (Stratopoulos *et al.*, 2020) such as health care, supply chain management, market monitoring, smart energy and copyright protection (Xu *et al.*, 2019).

© Marion Pauline Gauthier and Nathalie Brender. Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at <http://creativecommons.org/licenses/by/4.0/legalcode>

This research was supported by the University of Applied Sciences and Arts Western.

Switzerland, Economics and Management funding commission for research (RCSO) and by the Swiss National Science Foundation (SNF).



Blockchain has been described as both a disruptive and a foundational technology with the potential to impact business and society in ways not seen since the internet's introduction (Sheldon, 2019; Tapscott and Tapscott, 2016a, 2016b; Casey and Vigna, 2018; Iansiti and Lakhani, 2017). Foundational technologies usually need time to seep into the economic and social infrastructure. For example, it took more than 30 years for the internet to go from single localized use to reshaping the whole economy. Therefore, some specialists think that blockchain mass adoption might take several years or even decades (Iansiti and Lakhani, 2017; Behlendorf, 2016). However, the diverse ongoing blockchain projects have started to demonstrate this new technology's potentials, notably a possible transformation of intermediary activities, such as audit and control activities (Schatsky and Muraskin, 2015; Swan, 2015; Atzori, 2017). Indeed, blockchain's key characteristics – transparency, traceability and decentralization – combined with the possibility of embedding rules and procedures into the technology itself (smart contracts) can significantly change how audits and other control activities are performed.

The goal of our first research project was to understand external auditors' level of knowledge about blockchain technology and assess the impacts they anticipate the technology could have on their profession. As such, we set up a qualitative study based on semi-structured interviews with financial and information systems (IS) auditors working in Switzerland in Certified Public Accounting (CPA) firms of different sizes. Unexpectedly, most of the auditors questioned the relevance of the current auditing standards in the face of new technologies, including blockchain. This finding triggered a new research question: how do current auditing standards fit the emergent use of blockchain?

We analyzed the interviews to identify and understand the external auditors' perceptions on how the current auditing standards address blockchain. We also examined the interviewees' thoughts on data analytics, which several of them mentioned in their responses, in association with blockchain, as a "new technology" expected to impact their audit practice. Finally, we looked at how the current standards, from the interviewees' point of view, address – or fail to address – auditors' evolving need to integrate such technologies into their audits.

According to the results of our study, which presents the points of view of external auditors, most of the interviewees believe that standards on information technology (IT) are too vague to face the increasing complexity of the IS environment. Their answers reveal their uncertainties about how to audit a blockchain network, how to audit data stored within a blockchain and how to use data analytics to support their work. They shared with us their need for more IT standards, including specific standards on blockchain and data analytics, for two main reasons, namely, to maintain audit quality and to ensure proper compliance with their regulatory environment. Our findings also highlight the external auditors' concern regarding the contrast between the fast-evolving IT environment, which impacts their daily work, and the slowness of the standards setters in updating or issuing auditing standards. According to our interviewees, this difference of timing creates situations that may jeopardize audit quality, audit efficiency and audit effectiveness.

The paper is organized as follows. In Section 2, we review the existing literature related to blockchain and data analytics, auditing practices and the related auditing standards. In Section 3, we describe the research methodology. In Section 4, we present and discuss the results. This is followed by Section 5, in which we conclude our paper by presenting current and future work.

2. Literature review

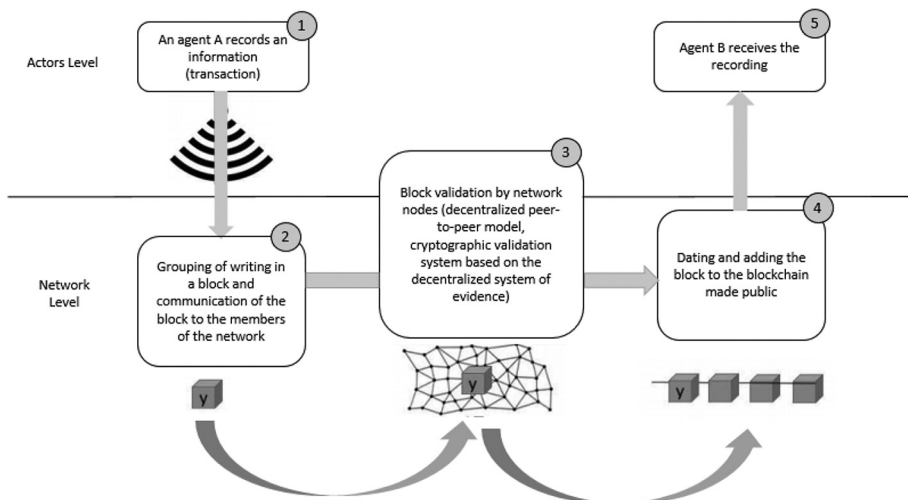
A blockchain is a cryptographic database of peer-to-peer transactions that is maintained by a network of computers called nodes (Alexander, 2019; Orcutt, 2019). Transactions are

verified, validated and added to the chain based on a blockchain protocol, which uses cryptography, game theory and economics to encourage the nodes to properly secure the network. Once verified and validated according to the protocol, transactions are grouped together into a block that it timestamped (Orcutt, 2019) and chronologically added to the chain of previous blocks. The most up-to-date version of the database or the chain of blocks (hence, the name “blockchain”) is accessible by all blockchain participants. Figure 1 below depicts blockchain’s functioning.

Moreover, as rules and procedures can be embedded into the blockchain at the transaction level, this technology can contribute to standardizing process activities and help businesses to design applications and conduct transactions that are simultaneously self-executing and autonomous (DuPont and Maurer, 2015). The three principles characterizing blockchain technology – transparency, data security and decentralization – can contribute to redefining the foundational patterns of business applications (Schatsky and Muraskin, 2015; Swan, 2015; Mahajan *et al.*, 2018). The trusted third parties and the intermediary activities in several sectors – such as finance, art, health and literacy (Swan, 2015) – as well as corporate audits and accounting (Schatsky and Muraskin, 2015; Tysiac, 2017; Smith, 2018; Tysiac and Drew, 2018), could even become useless and be replaced by blockchain-based distributed trust.

In today’s business ecosystem, financial auditors are trusted professionals who guarantee the existence of transactions; attest to their evidence, accuracy and completeness; and present related information in financial statements (Hayes *et al.*, 2014). To fulfill these objectives, auditors:

- Need a good understanding of their client’s business, including its nature, environment, internal controls and IS – such as blockchain, if in use – related to business processes and financial reporting (ISA 315; AS 2110).



Notes: Original graph is in French. E.G. Consortium LaBchain groups 25 organisations including la caisse des dépôts, le credit Agricole, Allianz, Groupama, Natixis
Source: Processus de fonctionnement de la blockchain (Desplebin *et al.* 2018)

Figure 1.
Blockchain operating process

– Use different types of audit tools, including new technologies such as data analytics. According to [Cao et al. \(2015\)](#), “data analytics can be defined as the process of inspecting, cleaning, transforming and modeling Big Data to discover and communicate useful information and patterns, suggest conclusions and support decision-making;” with Big Data being large and unstructured data sets produced by people, transactions and machines ([Bender, 2017](#)). In the context of auditing, data analytics would allow auditors to test 100% of their clients’ transactions, and therefore, get a deeper insight into their processes and identify not only errors but also anomalies in the data patterns, which would increase audit quality ([Liddy, 2014](#); [Earley, 2015](#); [Murphy and Tysiac, 2015](#)).

– Must conform to auditing standards while performing their work. Those standards serve as effective measures of performance quality and must provide clear, concise and definitive imperatives for auditors to follow ([Carmichael, 2014](#)).

The development of new rules and standards by the various professional and regulatory bodies is intended to improve audit quality but it simultaneously increases not only the complexity of audits but also the costs of both control and reporting activities for companies. As reported by [Protiviti \(2018\)](#) the average annual compliance costs with the Sarbanes–Oxley Law (SOX) have increased over the past few years and are expected to continue to grow in the future. Indeed, many organizations are spending more hours complying with SOX compared to prior years because they are becoming subject to more frequent, significant and fast-moving changes, such as changing organizational structures because of digital transformation, which calls for changes in SOX compliance practices and greater demands from external auditors ([Protiviti, 2018](#)).

In this context, blockchain – which allows entities to make digital interactions and to record any transactions, assets or documents in a way that is transparent, secure, auditable, efficient and highly resistant to interruptions ([Schatsky and Muraskin, 2015](#)) – is expected to facilitate access to data, which would ease the completion of financial audits and reduce both the manual work needed ([Drane, 2016](#); [CPA and AICPA, 2017](#)) and the auditing and compliance costs ([Schatsky and Muraskin, 2015](#); [Spoke, 2015](#); [CPA and AICPA, 2017](#); [Desplebin et al., 2019](#)). Direct access could even be granted to auditors and regulators ([Roberts, 2017](#)), which would enable real-time auditing ([MacManus, 2017](#); [Schmitz and Leoni, 2019](#)).

However, even though blockchain offers many features, several impediments exist to its wide adoption. First, several technical challenges need to be addressed. The blockchain infrastructures have interoperability issues, and compatibility issues with enterprise IS (e.g. enterprise resource planning (ERP)), which often include several functional modules such as for accounting, controlling, logistics, manufacturing, warehousing and procurement ([Kacina et al., 2017](#)).

Another key technical challenge is scalability, which is a system’s ability to continue to function well when it increases in size or volume ([Rouse, 2006](#)). Scalability has several components. The first, latency, is the “time for a transaction to confirm” ([Croman, 2016](#)), which tend to be higher within any blockchain infrastructure than that of current payment processing systems; for example, it takes 10 min for a transaction to be confirmed with the blockchain Bitcoin and 14 s with Ethereum ([Kanaracus, 2016](#); [Harris, 2018](#)). Size and storage also need to be worked on. Indeed, because a blockchain ledger keeps all of the transactions since the first block when the numbers of users and transactions grow, the size of the ledger grows as well. Bandwidth is another important aspect as transactions need to be broadcast through the network before being validated through a consensus algorithm. When the number of transactions increases, better network connectivity is necessary, which, coupled with a large storage capacity, requires effective record management, leading to

centralization, increased costs (Harris, 2018), and more energy consumption. The last component of scalability is throughput, which is the maximum rate at which the network can work properly (i.e. to transmit, receive and validate transactions). Because of the blockchain infrastructure's design, the number of transactions transmitted, received and validated over the network is small compared to other existing centralized infrastructures.

The second impediment is that blockchain integrates complex components (consensus algorithms and cryptography) that require technical understanding and that are usually not shown to users. This complexity translates into end-users finding blockchain hard to understand (Marr, 2018; Price, 2019), which represents a barrier for a wider adoption.

Third, regulators do not yet trust blockchain. Indeed, several risks exist, which can result in financial loss. These include, for example, programming errors, system weaknesses, key information being lost or stolen and more recently, 51% attacks in which hackers take control of the blockchain to create an alternate version of the blockchain with false transactions such as the hit against Ethereum Classic (Orcutt, 2019). Regulators caution that the technology is neither mature nor scalable enough, and that it lacks standards. Indeed, even though several countries have started to assess blockchain and, more specifically, its impacts on financial services, the regulatory environment remains unsettled (PwC, 2018; Deloitte, 2020).

Overall, the audit standards and controls in place are currently insufficient to ensure that the blockchain-based systems are functioning as intended (Alarcon and Ng, 2018). Indeed, there is currently no auditing standards for blockchain, and it is difficult to predict if there will be any or how long it might take to issue such standards. As reported by Dai and Vasarhelyi (2016) in their article on Audit 4.0, the adoption of technology by the audit profession has substantially lagged behind technology's development and utilization by companies, and standard-setting bodies' consideration of technology lags even further (Dai and Vasarhelyi, 2016). Because standards are mostly reactive in nature, they tend to respond to particular needs instead of anticipating them, which means that they are likely to be behind what is happening now (Duncan and Whittington, 2014). This becomes even more of an issue for international auditing standards due to the differing agendas being pursued by different countries, which can further increase the time lag to implementation (Duncan and Whittington, 2014). Therefore, it seems that changes may only accelerate when management's needs or technological changes force accounting methods to adapt, in turn, creating pressure for changes in assurance (Dai and Vasarhelyi, 2016; Krahel and Titera, 2015), and therefore, for standards to adapt. For example, the adoption of large databases and cloud technology prompted the development of software and application layers for measuring performance, leading to a demand for assurance (Dai and Vasarhelyi, 2016). Similarly, the main driver of big data applications and blockchain usage by auditors will be client-side demands (Alles, 2015). Alles (2015) showed the analogy between ERP systems and big data in terms of their impacts on audit practice. If ERP can create the motivation for the audit profession to adopt IT-based audits, then the same should apply to big data (Tang and Karim, 2017) and by extension to the blockchain.

Auditors need standards and guidelines to perform audits. In a context in which new technologies, including blockchain developments, are flourishing but standards tend to lag behind, our study reveals how external auditors in practice assess and use current auditing standards according to their evolving needs.

3. Methodology

For the purposes of this study, we used data that were originally collected to understand the external auditors' knowledge about blockchain technology and their expectation on the potential impacts the technology could have on their profession.

We initially gathered data using purposeful sampling, which is widely used in qualitative research to identify and select information-rich cases for in-depth study. This involves identifying and selecting individuals or groups of individuals who are especially knowledgeable about or experienced with a phenomenon of interest (Cresswell and Plano Clark, 2011). Studying information-rich cases yields insights and in-depth understanding, rather than empirical generalizations and breadth of understanding (Patton, 2002). As such, we used a field study and engaged with practitioners employed by several auditing firms. We purposely sought interviewees with wide-ranging experience in the auditing field, either as financial auditors or as IS auditors with different levels of responsibility, ranging from manager to partner, all located across Switzerland (except one auditor, who was covering the Swiss market from France at the time of the interview) and participants working at audit firms that varied in size from small local firms to the Big Four. We conducted semi-structured interviews to discuss each interviewee's observations on blockchain in depth.

Theoretical saturation, when nothing new emerges (Miles and Hubermann, 1994), was reached after interviewing 34 auditors (either financial or IS) working in 23 audit firms. The sample size of our study is consistent with that of other qualitative studies, for which data are commonly based on 1 to 30 informants (Fridlund and Hildingh, 2000).

The interviews lasted 50 min on average; they were conducted in either French or English (depending on the auditors' ability) and were either recorded or transcribed through notes (depending on the auditors' specific request) for analysis using the ATLAS.ti research software.

Table 1 – Interviewee categorization presents the categorization of the sample population by level of experience, the field of expertise and employment in a big four.

When we analyzed data as part of the initial study, we found that an unexpected matter was raised by most of the auditors, which translated into a new research question on how the current auditing standards fit the emergent use of blockchain. We investigated this matter using the content analysis method, which involves first coding textual data and then summarizing and analyzing the coded text (Drisko and Maschi, 2015). The coding process started with open coding (Berg, 2001), during which each researcher defined his or her codes as he or she started to review the data. In qualitative research, codes facilitate the identification of concepts around which the data can be assembled into blocks and patterns (Catanzaro, 1988; Bengtsson, 2016). Then, we compared our codes and agreed on 13 categories and their definitions (Burnard, 1991; Graneheim and Lundman, 2004). A category consists of codes that deal with the same issue (Erlington and Brysiewicz, 2017). The purpose of creating categories is to provide a means of describing the phenomenon, increasing understanding and generating knowledge (Cavanagh, 1997). The 13 categories focus exclusively on the external auditors' prominent and shared perceptions about how the current auditing standards address the growing use of technologies and blockchain's

Table 1.
Interviewees'
categorization

Specialists/categorization	(%) of interviewees
<i>Partner</i>	38
<i>Non-partner (manager and above)</i>	62
IT (audit, security)	25
Financial audit	65
Advisory/risk	9
Standards specialist	1
<i>Big four</i>	35
<i>Non-big four</i>	65

emergence. The categories and their definition are provided in [Table 2](#) – categories. We then grouped the categories into three themes. Themes express underlying data and are formed by grouping two or more categories together ([Erlington and Brysiewicz, 2017](#)). Each theme (presented in the next section) represents the concerns that the interviewees reported.

We note that one of the categories is on data analytics. Indeed, even though our study initially focused on blockchain, the interviewed auditors mentioned other technologies such as data analytics, process automation, digitalization, robotization and artificial intelligence, regardless of each technology's characteristics. We noticed that the two major auditing standards bodies [International Auditing and Assurance Standards Board (IAASB) and public company accounting oversight board (PCAOB)] do not differentiate technologies from one another and have both set up working groups to investigate "new technologies," which include data analytics and blockchain, among others. As several interviewees referred to data analytics in their answers, we decided to include it in our results to shed light on commonalities or differences in the auditors' evaluation of their respective impact on their work.

We further evaluated and rated the knowledge of blockchain among the interviewed auditors ([Appendix A](#) – Maturity Level of Auditors' Knowledge of Blockchain) based on a scale that we had defined (none, basic, aware, intermediate and advanced. See definitions in [Appendix A](#)). These blockchain knowledge maturity levels allowed us to put the auditors' comments in perspective with their understanding (basic, aware or intermediate) or mastery (advanced) of the technology. See [Table 3](#) – Interviewees' Concerns According to their Knowledge of Blockchain.

4. Results and discussion

In this section, we present the shared patterns of external auditors' perceptions on auditing standards in relation to the use of blockchain and data analytics. It is structured around the three themes that emerged from the content analysis and that are of interest to the scientific community, professionals in practice, standard setters and regulatory bodies.

4.1 Concerns about audit planning, including scope definition and audit realization

As explained by several interviewees, organizations increasingly use or plan to use technologies such as dematerialization, artificial intelligence or blockchain in their business processes, but the current auditing standards do not yet address these new IT capabilities and their related audit impacts. However, to perform an audit, auditors need guidelines that set levels of audit performance, and thus, quality. In this context, one of the financial audit managers working for a smaller audit firm explained that "standards were thought about as if audit evidence such as documents would always be paper-based." Moreover, an IS audit partner with advanced knowledge of blockchain and who worked for a Big Four firm stressed "the necessity to translate the old world into the new IT-oriented world." These remarks are consistent with current literature. Indeed, [Dai and Vasarhelyi \(2017\)](#) explain that auditing's basic approach has been very slow to evolve; traditional auditing remains centered on the audit of paper-based income statements with a limited use of technology, which is an approach that no longer represents the world in which business operates ([Dai and Vasarhelyi, 2017](#)).

The interviewed auditors specifically reported that no auditing standard currently covers blockchain, and yet some auditors already face the challenge of auditing enterprises that have set up blockchain platforms to execute some of their business processes or enterprises with crypto-currency wallets based on blockchain. This situation raises two types of uncertainty among the interviewees.

Table 2.
Categories

Categories	Definition	Themes
Increase IT standards	Current standards do not include enough guidelines on IT	Concerns about audit quality
No standard on data analytics	Current standards require the use of samples and are silent on data analytics when their use is increasing	Concerns about audit planning, including scope definition and audit realization
No standard on blockchain	No standards on blockchain audit whereas audit cases emerge	Concerns about audit planning, including scope definition and audit realization
Reactive	Standards are reactive and slow to evolve	Concerns about audit planning, including scope definition and audit realization
Use of a specialist	Blockchain would be assessed by a specialist and not by an auditor	Concerns about compliance with current standards
Impact on audit costs	More standards increase audit costs and not necessarily audit quality	Concerns about audit quality
Blockchain governance	Open questions on blockchain governance need to be answered because they will affect audit practice	Concerns about audit quality
Auditing process	Audit process follows auditing standards	Concerns about audit planning, including scope definition and audit realization
Method to change standards	The method to update standards provides the Big Four with preponderant influence	Concerns about audit quality
Auditors responsibility	How the deployment of blockchain may affect the auditors' responsibility	Concerns about compliance with current standards
ISO	Blockchain auditing standards should come from ISO (and not from PCAOB, IAASB or national bodies)	Concerns about audit quality
Data quality	Auditing needs raw data quality. Auditors raised questions on ways to ensure that the data entered a blockchain are accurate	Concerns about audit planning, including scope definition and audit realization
Auditor's understanding	Auditors understand what a blockchain is	Concerns about compliance with current standards

(% of Auditors by understanding categories (%))	Understanding categories	Audit quality					Audit performance					Compliance		
		Current standards are sufficient (%)	Increase IT standards (%)	Impact on audit costs (%)	Blockchain governance (%)	Method to change standards (%)	ISO (%)	No standard on data analytics (%)	No standard on Blockchain (%)	Reactive (%)	Auditing process (%)	Data quality (%)	Use of a specialist (%)	Auditor responsibility (%)
9	None	33	0	66	0	0	0	0	0	0	0	0	0	66
9	Basic	0	100	33	0	0	0	0	100	67	67	67	33	33
44	Aware	20	67	27	7	13	13	40	60	7	7	47	33	13
9	Intermediate	33	33	0	0	0	0	33	33	33	66	0	33	0
29	Advanced	10	70	40	40	20	10	30	80	40	50	70	0	0

Table 3.
Interviewees's concerns according to their knowledge of blockchain

The first uncertainty concerns the integrity, completeness and security of data. Indeed, blockchain allows several parties to a value chain to exchange information and value directly (e.g. in commodity trading, participants such as raw material extractors, traders, banks, inspectors and certification providers can simultaneously access and update the data within the blockchain). However, no publicly shared and validated protocol currently guarantees data security. In this context, several auditors highlighted the importance of ensuring the reliability of both the data stored in a blockchain and the blockchain network, which leads to the second uncertainty about the actual auditing process. Because no guidelines exist on how to audit blockchain technology or transactions stored in a blockchain, the interviewed auditors explained that they would like the standard setters to formulate guidance on the following audit-related issues. First, the scope of the audit and the standards to be applied are unclear to them, in particular, whether they should audit the blockchain network itself, the data stored within the blockchain or both. Second, they expect the lack of blockchain-specific standards to impact their work in several ways. On one hand, they wonder if they can rely on the blockchain-specific capabilities to adapt the audit procedures and, for example, reduce the sample size; but in that case, they would have to document how their work meets the current auditing standards; which would potentially mitigate audit efficiency. On the other hand, if blockchain has to be considered as any other random technological implementation, the auditors would potentially lose some audit efficiency.

In addition, the interviewees also reported that they are looking for the standard setters to provide guidance on how to assess an internal control environment based on a blockchain protocol, how to adjust the related risk assessment, how to ensure transactions' integrity and overall, how to design the scope of an audit for a company using blockchain. Blockchain-specific standards would bring consistency of the audit process among all CPA firms, and would ensure that auditors follow common steps in auditing data stored in a blockchain or in auditing a blockchain network, thus increasing audit quality. Finally, some of the interviewees also expressed their concern about the way their responsibility will be assessed if they rely on a blockchain protocol in an audit engagement.

The concrete questions above need to be answered for auditors to plan and perform an audit; however, no guidelines currently exist, and auditors have to use their professional judgment and make decisions that are not supported by auditing standards.

Indeed, although "blockchain does not magically make the information contained in it inherently trustworthy" and "events recorded in the chain are not necessarily accurate and complete" (Hamm, 2018), it ensures data integrity along the chain, and therefore, creates trust among the end-users of the information. Thus, auditors will have to provide assurance on the fact that the blockchain delivers what it is intended to deliver. They will also have to verify that the link to physical reality or other sources of the information entered in the blockchain are complete and accurate. In other words, auditors must confirm interfaces with the blockchain work properly, which Alles and Gray (2019) referred to as "the first-mile problem." In doing so, they will confirm process integrity in a blockchain-based environment.

This situation has already started to translate into significant findings (deficiencies in the application of generally accepted auditing standards that could result in a restatement of a company's financials) reported by the Canadian Public Accountability Board (CPAB). Indeed, the CPAB reported in its Inspections Insights of November 2019 that it has inspected eight audits of companies with activities in the crypto-asset sector to date and found significant findings for seven of them. The most common deficiencies found by the CPAB echo the concerns raised by the interviewed auditors and encompass the following:

- Inadequate risk assessment during the audit planning therefore, several auditors did not obtain an adequate understanding of the entities being audited, and thus, failed to assess whether they could rely on information obtained from the blockchain as audit evidence.
- Inadequate reliability of blockchain records. Even though blockchain protocols are intended to make blockchain resilient to tampering, it is not appropriate for auditors to assume that all protocols are effective and that information recorded in a blockchain can be relied on with no prior testing. Indeed, before using information obtained from a blockchain as a primary source of evidence, the CPAB reminds that auditors should test the attributes of a blockchain protocol to ensure that only valid transactions are added to a blockchain ledger.

The CPAB's report refers to several auditing standards that, from their point of view, should be sufficient to perform the audit tasks properly and the significant findings seem to arise because of the misapplication of those standards by the auditors. This divergence between the audit regulators and the auditors on the adequacy of auditing standards in the context of new technologies has been reported in other studies. For example, [Christ et al. \(2019\)](#) in their research on the use of drones for inventory counts show that the standard setting bodies believe the current standards clearly allow a technology-supplemented process, whereas the auditors think that the standards *might* allow for the use of these technologies. The auditors would be more willing to adopt the technology if guidance were provided to protect the firms from both legal and regulatory risks, which was also mentioned by some of our interviewees who raised questions regarding their legal responsibilities as auditors. Moreover, most of our interviewees expressed concern about properly conducting their work to maintain the quality of the audit and to stay compliant with the auditing standards. We noted that all the interviewees (except for one) with an advanced level of understanding of blockchain, and therefore, with an advanced level of understanding of the technology specificities and impact on auditing, asked for both more IT standards in general and specific standards on the blockchain.

Many of the interviewees also explained that an increasing number of accounting firms use new IT capabilities, such as data analytics, which allow them to analyze all transactions and accounting records from a company's data, such as journal entries, to detect anomalies to investigate. However, no auditing standards currently cover the use of data analytics for financial statement audits. Thus, when audit firms analyze large volumes of data instead of doing sample-based tests, as currently requested in the auditing standards (AS 2315), they obtain a higher level of assurance on the financial data (and not on the quality of the internal control system) but do not meet the standards' requirements. Audit companies, therefore, end up in a paradoxical situation in which compliance with the auditing standards in place reduces the level of assurance that could be achieved through the full use of the technology. Many of the auditors interviewed explained that "sampling is not enough," as such the standards need to be updated to integrate data analytics capabilities. These findings echo [Austin et al. \(2019\)](#), who showed that external auditors deplore the lack of regulation over data analytics and that this lack of regulation appears to have slowed the diffusion of data analytics throughout the financial reporting environment. Their results are also in line with issues presented by [Krahel and Titera \(2015\)](#), who explained that the current standards are still geared toward a paper paradigm in terms of data collection and error response, and focus on intermittent and incomplete analyzes of available data by requesting statistical and non-statistical sampling, whereas such a methodology implies uncertainties and personal judgment ([Krahel and Titera, 2015](#)). In this context, [Tang and Karim \(2017\)](#) explained that if

the standards provided clarification on choosing between population and sampling audits, then it would be possible to perform a population-level audit that would be more effective and at a lower cost than a sampling audit. Moreover, if we consider it possible to analyze all data of a company, then the evaluation of internal controls to determine the extent of substantive testing as prescribed in the standards could become obsolete. There could also be an additional step where all data would be saved in a blockchain whose integrity would have been tested beforehand, guaranteeing data integrity, immutability and traceability, which would render the data analytics procedures unnecessary.

In this context, the two main audit standard setters – the IAASB and the PCAOB – have each launched project to assess whether a need exists for new or updated guidance. On the one hand, the IAASB established the technology working group in mid-2015 to explore how it can respond to the increased use of technology including data analytics and blockchain via new or revised International Standards on Auditing (ISA) or non-authoritative guidance and in what time frame. In January 2018, the IAASB explained that this evaluation would shape its strategy and work plan for 2020–2023.

The PCAOB also formed a task force on data and technology to explore whether a need exists for new guidance or changes to PCAOB standards, taking into consideration the increased use of technology, including big data and data analytics, in audits, as well as other new and emerging technology-based tools. As of November 2020, it reported that nothing indicates that PCAOB standards impede auditors' use of technology-based tools. As such, they do not plan to update the current standards but will continue their on-going assessment.

4.2 Concerns about audit quality

Auditing standards are sets of standards against which audits are performed and their quality may be judged (Carmichael, 2014). However, our findings show that many auditors deplored a lack of IT-related audit standards. Indeed, as confirmed by a member of the IT Technical Subcommittee at EXPERTsuisse (the Swiss auditing standards setter), no IT audit standard stands on its own among the different sets of auditing standards (PCAOB, IAASB and Swiss national auditing standards). Therefore, auditors cannot use a specific internal control framework when evaluating business or IT controls (Sheldon, 2019). Instead, IT audit guidelines are embedded into general auditing standards such as the PCAOB Auditing Standard No. 5 – an audit of internal control over financial reporting that is integrated with an audit of financial statements, which includes guidance on automated systems and controls, as well as IT general controls. Consequently, most of the larger professional accounting and auditing firms have created their own audit templates (Sheldon, 2019; ISACA, 2014) or use the control objectives for information and related technology framework as a reference. The scientific literature also shows that even though the business IT environment is becoming increasingly complex and dynamic, auditing standards only provide vague guidance (Axelsen *et al.*, 2017). One of the partners with a basic understanding of blockchain who worked for a mid-size international CPA firm emphasized that “as IT risks increase, IT standards should also increase.” However, the current auditing standards on IT are at best vague or even silent in particular situations, such as blockchain audit or the use of data analytics by CPA firms. This situation raised questions among the interviewees about their ability to issue proper assurance. Several interviewed auditors with different levels of understanding of the blockchain technology specifically asked for the standards to update the way audit evidence can be collected, taking into consideration the various new technologies, including blockchain. This demand is also reported in the literature; for example, Christ *et al.* (2019) for the use of drones and Brown-Liburd and

Vasarhelyi (2015) and Austin *et al.* (2019) for the use of data analytics. Some interviewees expressed that having more IT rules would increase audit quality by ensuring the security, quality and integrity of raw data, especially within a blockchain environment and would also increase stakeholders' assurance in the audit results. Above all, as some auditors reported, "standards should provide confidence."

On the contrary, other highly experienced auditors highlighted that even though they need more IT auditing standards, those standards should not be too prescriptive. They seek auditing guidelines, not rules. One auditor explained that "having more standards does not necessarily translate into more quality and more added value for the clients but instead can translate into administrative compliance overhead, which increases audit costs." Another interviewee even stated that it could create a "check-the-box mindset" in which the auditor's only concern is to complete checklists to ensure that all standards are properly followed, whereas audit report users expect a critical evaluation and skeptical mindset from the auditors. In their study of data analytics, Austin *et al.* (2019) also reported the contrasted preferences between prescriptive, rule-based standards and guidelines or "loose regulation." They explained that accountants tend to prefer rules-based standards because they provide protection in case of litigation (Donelson *et al.*, 2012) and that technology users often prefer the flexible interpretation of technology-related rules (Geels, 2004). Our results are more nuanced: the majority of our interviewees who specialized in IT, and therefore, have an advanced level of knowledge of the blockchain technology, ask for more guidance and specific standards, whereas the proportional share of financial auditors asking for more guidance and specific standards is smaller. This might be the expression of blockchain's specificity and potential pervasive impact on the auditing profession.

At this stage, some of the highly experienced auditors with different levels of knowledge on the blockchain (from aware to advanced) believe that the International Organization for Standardization (ISO), through its TC 307 – Blockchain and distributed ledger technology should deliver blockchain certifications. In this context, the interviewees proposed that blockchain specialists review and certify blockchain's set-up and deployment according to ISO standards. Financial auditors would use and rely on their report, as authorized by the auditing standards, which would nonetheless require that the financial auditors be sufficiently blockchain savvy to understand the conclusions of the report. As explained in the next section, this represents a challenge.

Some of the interviewed auditors raised another shared perception that the standards are reactive in nature, which is consistent with the current literature as discussed in Section 2. They explained that because the standards are reactive, they are not quick enough to adapt to continuous business updates and auditors'-related needs. As one of the interviewees with an advanced level of knowledge on blockchain who worked for one of the Big Four stated, "standards represent a limit: auditors cannot take full advantage of new technologies because the standards and the technology do not change at the same pace." This can be illustrated by a review of the PCAOB and IAASB websites. To the best of our knowledge, there is currently no scientific or professional study on the time needed to issue new auditing standards or update existing ones. We reached out to the PCAOB and IAASB to ask if information (studies, reports or statistics) was available on this topic, but neither replied. Only the Swiss auditing standard-setting body EXPERTsuisse explained that even though it tends to rely on existing ISAs, the process can take up to three years in Switzerland. Therefore, we reviewed the latest auditing standards issued by the PCAOB and the IAASB to gain information on the standards-issuing time frame and noted that for both institutions it takes on average six years between the initiation and the adoption dates.

An interviewee emphasized that “technology advances constantly and rapidly.” However, the auditing standards take time to change and tend to change only when incidents happen that challenge the auditors’ work. This finding is aligned with the conclusions of [Dagilene and Kloviene \(2019\)](#), who reported in their article on the motivation to use big data and data analytics in external auditing that companies started to use data analytics tools more than five years ago, external auditors began using them three years ago and regulators have no experience with them to date. This results in transition periods, during which auditors do not have clear guidelines on how to conduct their audits. In those periods, auditors perform their audits with no guidance according to which the audit can be performed, measured and judged. They have to rely on their professional judgment, even when they face complex audit questions such as the ones mentioned above, which could negatively impact not only the audit quality but also financial statement users’ confidence, and even the capital market at large.

4.3 Concerns about compliance with current standards

The interviewed auditors recognize that blockchain is a sophisticated and complex technology that is difficult to understand. Yet, auditing standards require auditors to obtain a good understanding of their client’s business, including the IT infrastructure and IT systems relevant to financial reporting and the controls in place (ISA 315; AS 2110). To do so, financial auditors are allowed to team up with IS auditors to gather and interpret evidence (ISA 220; AS 1201; [Axelsen et al., 2017](#)). However, as demonstrated in the answers obtained, the current state of many auditors’ understanding of this technology is not sufficient to comply with ISA 315, ISA 402 and AS 2110.

As mentioned by some auditors, one way to address this issue could be working with a specialist, which is consistent with the recommendation from the [CPAB \(2019\)](#). Indeed, the standards allow engagement auditors to use a specialist’s work to obtain appropriate evidential matter. A specialist is defined as a person (or a firm) possessing special skills or knowledge in a particular field other than accounting or auditing, such as an engineer or IT programmer (ISA 220; AS 1201). Because blockchain is a complex technology, some interviewees mentioned the possibility of having it reviewed and assessed by a specialist, who would issue a report that the financial auditors would use and rely on. However, this hypothetical situation raised additional questions and concerns among some of the interviewees. Indeed, ISA 620 and AS 1210 require that the engagement auditors evaluate the specialist’s professional qualifications to ensure that he or she possesses the necessary skills (including professional certifications or licenses, reputation and experience). Some of our interviewees pointed out that they would not be able to evaluate these competencies and could not be assisted by IS auditors because IS auditors tend to work only in bigger firms. As such, they think that the standards need to be updated to include guidance on how to assess the competency of blockchain specialists.

ISA 620 and AS 1210 also require that the auditors obtain an understanding of the nature of the work performed, including the methods used, the form and the content of the specialist’s findings, etc. Indeed, even though auditors are allowed to use the work of a specialist, the engagement auditors are ultimately responsible for the audit opinion. As such, some auditors interviewed reported that they are not sufficiently blockchain savvy to understand the conclusion of such a report, and therefore, are not able to comply with ISA 620 and AS 1210. They also believe that the standards should be updated to include the key steps of a blockchain audit, including its acceptable outcome.

Overall, some auditors were concerned that the current set of standards coupled with their lack of understanding of the technology prevented them from concluding an audit for

which the client used blockchain. This last point is also reported in the literature, which states that “if we imagine an environment filled with clients using blockchain in their business operations, an auditor without sufficient knowledge and skills will have a hard time understanding the client’s business and the client’s environment, and therefore, will have a hard time providing assurance” (Tang and Karim, 2017).

5. Conclusion

Because blockchain offers many interesting characteristics (e.g. transparency, traceability, security and immutability of transactions) and is based on shared and distributed features, we anticipate that its adoption will most probably be general once it starts to become rooted into the business ecosystem, which seems to be confirmed by recent studies. PwC (2018) reported that in the 15 countries where it surveyed leaders, 84% of them explained that their company was already engaged in a project related to blockchain. Another recent survey from Deloitte (2020) shows that an increasing number of organizations are moving away from “blockchain tourism” to define and develop a permanent implementation. Thus, the survey shows that 39% of the global respondents (1,488 senior executives and practitioners in 14 countries) report that they have already incorporated blockchain into production (41 % of respondents working for companies with revenue greater than \$100m), which represents a 16-point increase compared to past year.

The magnitude of technology’s impact on the audit profession is not clear at this stage. Nonetheless, some commentators have suggested that the potential impact of blockchain technology on the auditing profession could be as significant as the internet’s impact on industries such as travel and retail (Sheehan, 2017). According to Gerard Brennan, auditing and blockchain expert, “there is an urgency for consensus, regulations and standards” (CPA.com, 2019), especially as blockchain will probably affect audit firms at two levels. First, CPA firms will have to develop new audit procedures to provide assurance for clients whose business processes are based on this technology. Second, they will have to integrate blockchain into the audit firms’ tools to increase their audit efficiency, which is probably also valid for other technologies such as digitalization, data analytics, robotics, process automation and artificial intelligence. Indeed, as reported in the Request for Input issued by the IAASB in September 2016, stakeholders raise questions about how data analytics fits into the current risk-based audit model, inquire about the auditor’s data analytics capabilities and in some cases expect the auditor to perform the audit using more technology to improve accuracy and efficiency.

The two major setters of auditing standards (the PCAOB and the IAASB) have identified the growing use of technologies and have considered on an ongoing basis whether the auditing standards continue to meet the needs of those who rely on auditors’ reports in a fast-paced digital world. They also take into consideration whether they should reflect the digital era in the application guidance.

The results of our study show that external auditors think that to maintain audit quality at least to its current level and to ensure that the auditing standards continue to be robust and relevant in a fast-paced environment, those standards will have to be adapted to address new technologies sooner rather than later. Indeed, the interviewees stressed the lack of auditing standards addressing new technologies and shared with us a growing list of technology-related questions that need to be answered to continue to perform high-quality and efficient audits and, in turn, secure the investor’s and other stakeholders’ confidence. Many of them also referred to data analytics and explained that they are looking for standards that explicitly cover this topic to develop and generalize their use. Our study also shows that most of the auditors with an advanced level of understanding of the blockchain

technologies, and therefore, of the technology specificities and impacts on the audit risk, ask for specific standards addressing blockchain.

Furthermore, the time frame considered by the IAASB (2020 to 2023) coupled with the time necessary to issue new standards (between 5 and 10 years) does not fit the fast pace at which the technology is developing and being adopted. As one of the interviewed IT audit partners with an advanced understanding of blockchain reported, “the blockchain deployment will most probably have a transversal impact. It will, therefore, be difficult for the standard-setting bodies to grasp it and translate it into audit guidelines.” As such, these bodies might have to innovate and adapt their ways of working and issuing new standards from now on. For example, to support auditors through transition phases such as the present one, the standard setters might regularly issue best-practice recommendations rather than detailed and prescriptive standards. Moreover, as IT systems are becoming increasingly complex and sophisticated, and increasingly important to audit risk-based assessment, the regulator could consider having the audit opinion signed by both a financial audit partner and an IT audit partner, with each being either responsible for their part of the audit or jointly responsible for the whole audit. It also seems that as the world continues to become more interconnected, especially with IT systems such as blockchain, the major auditing standard-setting bodies need to accelerate their convergence project to ensure that all CPA firms follow common audit steps to promote the same level of confidence worldwide. However, today, it seems that in lieu of consensus, there is only confusion and uncertainty (CPA.com, 2019).

Notwithstanding the limitations because of the nature and extent of our study, which focused on external auditors working in Switzerland, our findings could be interesting for an international audience, in particular, the regulators or auditing standard boards as they indicate possible action points to issue new and adequate IT-related standards regarding the use of blockchain and other so-called “new technologies.” Although the Swiss findings may not be fully applicable to other countries, they are relevant in expressing the need for further guidance because Swiss auditors widely use IASB and PCAOB standards in their audits or use Swiss national auditing standards that are closely linked to the international ones. Similar surveys could be conducted in different contexts (national or international, including standard-setters and regulators) to generalize such findings. Future research could also more specifically address the contribution of new blockchain or other technologies dedicated IT auditing standards for auditing practice. New release and update schemes to better fit the fast-evolving environment, and in particular the technology evolution, also represent an interesting issue in this still understudied area of the impact of new technologies on the audit profession.

References

- Alarcon, A.J. and Ng, C. (2018), “Blockchain and the future of accounting”, *Pennsylvania CPA Journal*.
- Alexander, A. (2019), “Unlocking new potential: the various applications of blockchain mean this young technology will bring big opportunities to the accounting profession”, *Accounting Today*, Vol. 33 No. 12.
- Alles, M. (2015), “Drivers of the use and facilitators and obstacles of the evolution of big data by the audit profession”, *Accounting Horizons*, Vol. 29 No. 2, pp. 439-449.
- Alles, M.G. and Gray, G.L. (2019), “The first mile problem: deriving an endogenous demand for auditing in blockchain-based business processes”, *11th Biennial Symposium on Information Integrity and Information Systems Assurance*, Toronto.

-
- Atzori, M. (2017), "Blockchain technology and decentralized governance: is the state still necessary?", *Journal of Governance and Regulation*, Vol. 6 No. 1, pp. 45-62.
- Austin, A. Carpenter, T. Christ, M. and Nielson, C. (2019), "The data analytics journey: interactions among auditors, managers, regulation, and technology", available at: <https://ssrn.com/abstract=3214140>
- Axelsen, M., Green, P. and Rideley, G. (2017), "Explaining the information systems auditor role in the public sector financial audit", *International Journal of Accounting Information Systems*, Vol. 24, pp. 15-31.
- Behlendorf, B. (2016), "Meet hyperledger: an 'umbrella' for open source blockchain and smart contract technologies", available at: www.hyperledger.org/blog/2016/09/13/meet-hyperledger-an-umbrella-for-open-source-blockchain-smart-contract-technologies
- Bender, T. (2017), "The effect of data analytics on audit efficiency", available at: <https://thesis.eur.nl/pub/38929>
- Bengtsson, M. (2016), "How to plan and perform a qualitative study using content analysis", *NursingPlus Open*, Vol. 2, pp. 8-14, doi: [10.1016/j.npls.2016.01.001](https://doi.org/10.1016/j.npls.2016.01.001).
- Berg, B.L. (2001), *Qualitative Research Methods for the Social Sciences*, Allyn and Bacon.
- Brown-Liburd, H. and Vasarhelyi, M. (2015), "Big data and audit evidence", *Journal of Emerging Technologies in Accounting*, Vol. 12 No. 1, pp. 1-16, doi: [10.2308/jeta-10468](https://doi.org/10.2308/jeta-10468).
- Burnard, P. (1991), "A method of analysing interview transcripts in qualitative research", *Nurse Education Today*, Vol. 11 No. 6, pp. 461-466.
- Canadian Public Accountability Board (2019), "Auditing in the crypto-asset sector: inspections insights", available at: https://cpab-ccrc.ca/docs/default-source/inspections-reports/2019-crypto-inspections-insights-en.pdf?sfvrsn=9aa5c0d2_20
- Cao, M., Chychyla, R. and Stewart, T. (2015), "Big data analytics in financial statement audits", *Accounting Horizons*, Vol. 29 No. 2, pp. 423-429.
- Carmichael, D. (2014), "Reflections on the establishment of the PCAOB and its audit standard-setting role", *Accounting Horizons*, Vol. 28 No. 4, pp. 901-915.
- Casey, M. and Vigna, P. (2018), *The Truth Machine: The Blockchain and the Future of Everything*, St. Martin's press.
- Catanzaro, M. (1988), "Using qualitative analytical techniques", *Nursing Research: Theory and Practice*, Mosby Incorporated, St Louis, pp. 437-456.
- Cavanagh, S. (1997), "Content analysis: concepts, methods and applications", *Nurse Researcher*, Vol. 4 No. 3, pp. 5-13, doi: [10.7748/nr1997.04.4.3.5.c5869](https://doi.org/10.7748/nr1997.04.4.3.5.c5869).
- Christ, M. Emmett, S. Summers, S. and Wood, D. (2019), "Prepare for takeoff: improving asset measurement and audit quality with drone enabled inventory audit procedures", available at: <https://ssrn.com/abstract=3335204>.
- CPA and AICPA (2017), "Blockchain technology and its potential impact on the audit and assurance profession", available at: www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf
- CPA.com (2019), "2019 Blockchain symposium: experts' insights indicate growing use cases and value for the technology", available at: www.cpa.com/sites/cpa/files/2019-12/2019-blockchain-symposium-report.pdf
- Cresswell, J.W. and Plano Clark, V.L. (2011), *Designing and Conducting Mixed Method Research*, 2nd ed., Sage, Thousand Oaks, CA.
- Croman, K. Decker, C. Eyal, I. Gencer, A. Juels, A. Kosba, A. Miller, A. Saxena, P. Shi, E. Song, D. and Wattenhofer, R. (2016), "On scaling decentralized blockchains: financial cryptography and data security: FC 2016 international workshop", pp. 106-125, available at: <https://fc16.ifca.ai/bitcoin/papers/CDE±16.pdf>

-
- Dagliene, L. and Kloviene, L. (2019), "Motivation to use big data and big data analytics in external auditing", *Managerial Auditing Journal*, Vol. 34 No. 7, pp. 750-782.
- Dai, J. and Vasarhelyi, M. (2016), "Imagineering Audit 4.0", *Journal of Emerging Technologies in Accounting*, Vol. 13 No. 1, pp. 1-15.
- Dai, J. and Vasarhelyi, M. (2017), "Toward blockchain-based accounting and assurance", *Journal of Information Systems*, Vol. 31 No. 3, pp. 5-21.
- Deloitte (2020), "Deloitte insights", available at: www2.deloitte.com/content/dam/insights/us/articles/6608_2020-global-blockchain-survey/DI_CIR%202020%20global%20blockchain%20survey.pdf
- Desplebin, O., Lux, G. and Petit, N. (2019), "Comprendre la blockchain: quels impacts pour la comptabilité et ses métiers?", *ACCRA*, Vol. N°5 No. 2, pp. 5-23.
- Donelson, D.C., McInnis, J.M. and Mergenthaler, R.D. (2012), "Rules-based accounting standards and litigation", *The Accounting Review*, Vol. 87 No. 4, pp. 1247-1279.
- Drane, J. (2016), "Wait, blockchains need audited!?", available at: www.linkedin.com/pulse/wait-blockchains-need-audited-jeremy-drane/
- Drisko, J. and Maschi, T. (2015), *Content Analysis*, Oxford University Press.
- Duncan, B. and Whittington, M. (2014), "Compliance with standards, assurance, and audit: does this equal security?", *The 7th International Conference on Security of Information and Networks. Association for Computing Machinery*.
- DuPont, Q. and Maurer, B. (2015), *Ledgers and Law in the Blockchain*, King's Review magazine.
- Earley, C.E. (2015), "Data analytics in auditing: opportunities and challenges", *Business Horizons*, Vol. 58 No. 5, pp. 493-500.
- Erlingsson, C. and Brysiewicz, P. (2017), "A hands-on guide to doing content analysis", *African Journal of Emergency Medicine*. doi: [10.1016/j.afjem.2017.08.001](https://doi.org/10.1016/j.afjem.2017.08.001).
- Fridlund, B. and Hildingh, C. (2000), *Qualitative Research, Methods in the Service of Health*, Studentlitteratur, Lund, pp. 13-25.
- Geels, F.W. (2004), "From sectoral systems of innovation to socio-technical systems: insights about dynamics and change from sociology and institutional theory", *Research Policy*, Vol. 33 Nos 6/7, pp. 897-920.
- Graneheim, U.H. and Lundman, B. (2004), "Qualitative content analysis in nursing research: concepts, procedures and measure to achieve trustworthiness", *Nurse Education Today*, Vol. 24 No. 2, pp. 105-112.
- Hamm, K.M. (2018), "Mexican mangos, diamonds, cargo shipping containers, Oh My! What auditors need to know about blockchain and other emerging technologies: a regulator's perspective", *Speech at the 43rd World Continuous Auditing & Reporting Symposium*.
- Harris, C. (2018), "The risks and dangers of relying on blockchain technology in underdeveloped countries", *IEEE/IFIP Network Operations and Management Symposium*.
- Hayes, R., Dassen, R., Schilder, A. and Wallage, P. (2014), *Principles of Auditing. An Introduction to International Standards on Auditing*, 3rd ed., Pearson, Chap 1.
- Iansiti, M. and Lakhani, K.R. (2017), "The truth about blockchain", Harvard Business Review, available at: <https://hbr.org/2017/01/the-truth-about-blockchain>
- ISACA (2014), *IT Control Objectives for Sarbanes-Oxley: Using COBIT5 in the Design and Implementation of Internal Control over Financial Reporting*, 3rd ed., ISACA, Rolling Meadows, IL.
- Kacina, J., Harler, M. and Rajnic, M. (2017), "The blockchain for business", available at: www.sophiatx.com/storage/web/SophiaTX_Whitepaper_v1.9.pdf
- Kanaracus, C. (2016), "Don't believe the blockchain hype: examining the weaknesses and risks." ZDNet", available at: www.zdnet.com/article/dont-believe-the-blockchain-hypeexamining-its-weaknesses-and-risks/

-
- Krahel, J. and Titera, W. (2015), "Consequences of big data and formalization on accounting and auditing standards", *Accounting Horizons*, Vol. 29 No. 2, pp. 409-422.
- Liddy, J.P. (2014), "The future of audit", *Forbes*, available at: www.forbes.com/sites/realspin/2014/08/04/the-future-of-audit/
- MacManus, E. (2017), "The audit of the future: EY financial services thought gallery", available at: <https://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2017/04/Audit-of-the-Future-Accountancy-Ireland.pdf>.
- Mahajan, S., Piscini, E., Dalal, D. and Holdowsky, J. (2018), "Blockchain: a technical primer", *Deloitte Insight*.
- Marr, B. (2018), "The 5 big problems with blockchain everyone should be aware of", *Forbes*, available at: www.forbes.com/sites/bernardmarr/2018/02/19/the-5-big-problems-with-blockchain-everyone-should-be-aware-of/#4c7e8cdf1670
- Miles, M. and Huberman, A. (1994), *Qualitative Data Analysis: An Expanded Sourcebook*, 2nd ed., Sage, Thousand Oak, CA.
- Murphy, M.L. and Tysiac, K. (2015), "Data analytics helps auditors gain deep insight", *Journal of Accountancy*, available at: www.journalofaccountancy.com/issues/2015/apr/data-analytics-for-auditors.html
- Orcutt, M. (2019), "Once hailed as unhackable, blockchains are now getting hacked", *MIT Technology Review*, available at: www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/
- Patton, M. (2002), *Qualitative research and evaluation methods*, 3rd ed., Sage, Thousand Oak, CA.
- Price, S. (2019), "Connecting the 'average' user: 'user experience in blockchain medium", available at: https://medium.com/@Price_Steven/connecting-the-average-user-user-experience-in-blockchain-dad84d66c763
- Protiviti (2018), "2018 Sarbanes oxley survey", available at: www.protiviti.com/FR-fr/insights/sox-compliance-survey
- PwC (2018), "Global blockchain survey", available at: www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.htm
- Roberts, M. (2017), "Utilizing blockchain in your development", Qualcomm, available at: www.qualcomm.com/news/onq/2017/12/19/utilizing-blockchain-your-development
- Rouse, M. (2006), "Scalability definition", available at: <https://searchdatacenter.techtarget.com/definition/scalability>
- Schatsky, D. and Muraskin, C. (2015), "Beyond bitcoin, blockchain is coming to disrupt your industry", *Deloitte Insight*.
- Schmitz, J. and Leoni, G. (2019), "Accounting and auditing at the time of blockchain technology: a research agenda", *Australian Accounting Review*, Vol. 29 No. 2.
- Sheehan, K. (2017), *The Ongoing Audit Transformation*, Accountancy Ireland.
- Sheldon, M. (2019), "A primer for information technology general control considerations on a private and permissioned blockchain audit", *Current Issues in Auditing*, Vol. 13 No. 1, pp. A15-A29.
- Smith, S. (2018), "Blockchain augmented audit – benefits and challenges for accounting professionals", *Journal of Theoretical Accounting Research*, Vol. 14 No. 1, pp. 117-137.
- Smith, S. (2018), "Implication of next step blockchain applications for accounting and legal practitioners: a case study", *Australasian Accounting, Business and Finance Journal*, Vol. 12 No. 4, pp. 77-90.
- Spoke, M. (2015), "How blockchain tech will change auditing for good", available at: www.coindesk.com/blockchains-and-the-future-of-audit/
- Stratopoulos, T., Wang, V. and Ye, J. (2020), "Blockchain Technology Adoption", doi: 10.2139/ssrn.3188470, available at SSRN: <https://ssrn.com/abstract=3188470>
-

- Swan, M. (2015), *Blockchain: blueprint for a New Economy*, O'Reilly.
- Swan, M. (2015), "Bitcoin and blockchain explained: not just cryptocurrencies, economics, and markets, applications in art, health, and literacy", available at: <https://fr.slideshare.net/lablogga/bitcoin-and-blockchain-technology-explained-not-just-cryptocurrencies-economics-and-markets-applications-in-art-health-and-literacy>
- Tang, J. and Karim, K. (2017), "Big data in business analytics: implications for the audit profession", *The CPA journal*, available at: www.cpajournal.com/2017/06/26/big-data-business-analytics-implications-audit-profession/
- Tapscott, D. and Tapscott, A. (2016a), "Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Portfolio", p. 368.
- Tapscott, D. and Tapscott, A. (2016b), *Blockchain Revolution: how the Technology behind Bitcoin is Changing Money, Business, and the World*, Portfolio Penguin.
- Tysiac, K. (2015), "5 Key issues that merit CPA's attention", *Journal of Accountancy*.
- Tysiac, K. (2017), "Blockchain: an opportunity for accountants? Or a threat", *Journal of Accountancy*.
- Tysiac, K. and Drew, J. (2018), "Accounting firms: the next generation", *Journal of Accountancy*.
- Xu, M., Chen, X. and Kou, G. (2019), "A systematic review of blockchain", *Financial Innovation*, Vol. 5 No. 1, pp. 5-27.

Further reading

- International Auditing and Assurance Standards Board (2018), "Feedback statement – exploring the growing use of technology in the audit, with a focus on data analytics".
- International Auditing and Assurance Standards Board (2009), "ISA 220: quality control for an audit of financial statement".
- International Auditing and Assurance Standards Board (2009), "ISA 315: identifying and assessing the risks of material misstatement through understanding the entity and its environment".
- International Auditing and Assurance Standards Board (2009), "ISA 402: audit consideration relating to an entity using service organization".
- International Auditing and Assurance Standards Board (2009), "ISA 620: using the work on an auditor's expert".
- Public Company Accounting Oversight Board "As 1210: Supervision of the audit engagement".
- Public Company Accounting Oversight Board "As 2110: identifying and assessing risks of misstatement. Appendix B – consideration of manual and automated systems and controls".
- Public Company Accounting Oversight Board "Changes in use of data and technologies in the conduct of audits", available at: <https://pcaobus.org/Standards/research-standard-setting-projects/Pages/data-technology.aspx>
- Public Company Accounting Oversight Board "Update on PCAOB efforts to enhance audit quality", available at: <https://pcaobus.org/News/Speech/Pages/Franzel-update-PCAOB-efforts-enhance-audit-quality-12-5-17.aspx>

Appendix A. Maturity level of auditors' knowledge of blockchain

None – The interviewee has not heard of the technology at the time of the interview or has heard the name but does not know what the technology's features and possibilities are.

Basic – The interviewee is aware of the technology. He or she may understand some key characteristics (no central control and data security) but associates them only to cryptocurrencies and does not know their functioning.

Aware – The interviewee differentiates the technology from the cryptocurrencies. He or she understands that this is a type of distributed ledger and knows some key characteristics (no central control and data security) but does not know how they are implemented.

Intermediate – The interviewee understands that this is the technology behind Bitcoin and cryptocurrencies but that it offers business applications beyond that field. He or she is aware of the main features of the technology and understands that the key functionalities of the chain involve a distributed data structure where transactions are peer-to-peer (with no central control), validated and added to the chain in a chronological order and immutable way.

Advanced – The interviewee understands the overall features and functionalities of the technology and the jargon around it (nodes and mining/miners), the different types of validation protocols (proof of stake and proof of work) and the different types of the blockchain (private, public and consortium). He or she is aware of the potential applications of the technology in various businesses and industries and understands the strengths (data safety, immutability, timestamping, impossible double spending, transparency and traceability) and weaknesses of the technology (scalability and interoperability). He or she understands smart contracts and how they can be used.

Corresponding author

Marion Gauthier can be contacted at: marion.gauthier@hesge.ch