Journal of Forensic and Investigative Accounting
Volume 12: Issue 1, January–June 2020

Blockchains Impact on Risk Assessment Procedures

*Sean Stein Smith**

Introduction

The accounting and financial services landscape has experienced a significant change in terms of technological integration since the 1980s. Beginning with personal computing and compounded by the widespread adoption of the internet, virtually every aspect of business and accounting has changed in a tangible way. More recently, and accelerating since the mid-2010s, the integration and implementation of advanced technology tools, such as data analytics, robotic process automation, artificial intelligence, and now blockchain, continues to drive change and innovation across different industry sectors as well as the accounting space. That said, there appears to be one subset of the accounting profession that has yet to fully adopt and consider the suite of technology tools now available to management professionals. Audit practices, clearly, have evolved and changed over time in the face of emerging technology tools and options, but recent technological developments such as blockchain pose entirely new questions to how these practices will work going forward.

Blockchain was probably introduced indirectly by the dramatic increase in price of bitcoins during 2016 and 2017, but since this introduction the technology has seized the attention of both practitioner and academic audiences. As the ecosystem continues to evolve, from public blockchains to ICOS to whatever lays beyond, so to do the needs and expectations of financial services professionals in terms of the information they must possess to offer concise and value additive services. At this point, however, one must differentiate the hype and excitement that has surrounded blockchain from the operational realities of what this technology can accomplish.

Blockchain was introduced with the potential and opportunity to completely redefine not only how audits function, but also how accounting and attestation engagements would interact with other facets of the business environment. Much has been discussed and analyzed about the opportunities and implications of blockchain technology, including the research, debate, and investments underway at audit firms connected to blockchain implementation (Boillet, 2017). While the technology remains a work in progress for many organizations in terms of comprehensive adoption, blockchain has amplified and accelerated other audit related trends that were already present in the marketplace. Implementing blockchain itself at an enterprise level still remains a technically complicated and financially costly procedure, but it is certainly having an impact on how audit and attest engagements are planned, executed, and documented, not to mention the impact it is already having in other industries or fields (Mundra, 2018). Connecting these trends, the increased integration of technology like blockchain into the audit environment, and the changing expectations and needs of client organizations, forms the basis and usability of this research. Not meant to be an all-inclusive nor authoritative piece, this research and the findings contained herein should be utilized as a starting off point for further conversation and debate. The core point, however, is that technology tools—be they blockchain or more mundane automation practices—are driving change in the audit and attestation environment. Connecting these changes with broader audit changes is an important part of any audit analysis and forms the basis for the next segment of research.

Research Purpose

The purpose of this research and analysis is to provide the users of this analysis with actionable business intelligence as it connects to blockchain technology as well as the implications for blockchain on risk assessment practices. Risk assessment procedures are at the core of any attestation or assurance engagement and appear to be the areas in which blockchain is most likely to have a significant initial impact. In addition to discussing core functionalities of blockchain technology, this study also touches on a few of the emerging issues in the space, and identifies what practitioners need to be aware of moving forward. What this analysis seeks to accomplish is to identify what changes are connected to blockchain integration as well as how the profession might need to evolve and change as a result.

* The author is a professor at the City University of New York—Lehman College

Audit Trends

The fundamental value proposition of an audit or attestation engagement has not, and does not appear to be, posed to change or radically evolve over time but rather evolve and shift with the needs of client organizations and marketplace trends. Blockchain, in and of itself, will not transform the audit and attestation process, but does appear to be a future tool and technology that will play an integral role moving forward in terms of both engagements and specific processes (Mahbod and Hinton, 2019). While attempting to not overly generalize the developments in terms of audit and attestation engagements, there do appear to be several changes that arise consistently in analyses of the audit and attestation subset of the accounting field. Perhaps the most important place to start this analysis is the changing nature of risk assessment that needs to be incorporated into any audit or attestation planning process. The assessment of risk, clearly, is an important piece of the audit and attestation process in and of itself, as well as helping guide next steps and applications that will be included as components of the engagement.

Integrating technology into this risk assessment process is not something that is necessarily new or innovative or an emerging topic or theme in the audit field, but as emerging technologies such as blockchain, robotic process automation, and artificial intelligence become more prevalent, the potential risk of performing an inadequate risk assessment process will continue to increase. Even if practitioners are well informed about the implications of certain technology tools, the roles and processes associated with audit and attestation work continue to evolve and shift as technological integration continues (Alexander, 2018). Specifically, the risk of conducting and reporting an incomplete or incorrect risk assessment is linked directly to two forces. First, the nascent nature of these technologies means that there will invariably be gaps in knowledge between some audit professionals, current best practices, and the expectations of clients. Second, even as professional knowledge becomes more mainstream, the specter of the increasing risk of a "black box" audit issue will continue to increase as technology continues to increase and eventually possibly outpace the ability of practitioners to keep pace.

Technology in and of itself, is not the only change and market pivot that is changing how audit and attestation intersects with client needs and expectations; there are several other trends and forces that continue to drive innovation, change, and development among the audit profession and landscape. These developments include but are not limited to the following; the need for audit and attestation services on a broader array of information, more continuous information and reporting, and the expectation that technology will play an increasingly important role in the audit process at large. Drilling down specifically, it becomes clear that core components of how audit engagements are conducted, managed, and evaluated will evolve and change (Raphael, 2017) Challenging and interesting in their own right, these changes and developments also indicate that the risk assessment and internal control portion of the audit process and work will also need to change and evolve going forward.

Another significant shift and change that is underway in the audit profession and accounting overall is the increasing need and expectation on the side of clients and customers for information that is updated and reported on a continuous basis. This transition is a result of a shift internal to the accounting profession as well as changing needs and expectations from a client, customer, and stakeholder perspective. As technology, personalization, customization, and digitization have become increasingly entrenched in virtually every other aspect of the business landscape it seems logical that accounting services will follow suit. Stakeholders and end users of operational and financial information, expecting information and data provided in real time, will also assume that technology tools adopted by other organizations—including blockchain—have been integrated into the accounting and attestation processes (Jun and Vasarhelyi, 2017). This seems a necessary evolution and iteration of these tools to ensure that the data produced and communicated is accurate in nature. From an operational point of view, it is also logical for management and other end users to expect more real time financial information to assist with management decision making from a compliance, reporting, and analytics perspective. Additionally, the importance of speed and transparency in the decision-making process also has resulted in the shift of accounting information from a periodic reporting process to a more continuous conversation and dialogue.

What also has occurred, however, as the need for more information delivered on a continuous basis has increased, is the need for risk assessment protocols and controls to evolve alongside the creation and reporting of information. Put another way, in order for data to be both delivered continuously and also be done so in a manner that is accurate and useful to decision makers, there must be proper controls and data management protocols in place to maintain custody and control over this flow of information as it enters the organization, as it is processed, and as it is delivered to a multitude of end users. Audits and the information produced as a result of them must be able to not only report what had previously occurred, but to also add value to the organization as it moves forward (Crosley and Anderson, 2018). This need for increased data security

and integrity also is connected to the changing requirements from a risk assessment perspective, especially as it interacts with audit and attestation engagements.

Changing Risk Assessment Needs

Risk assessment is a core component of the audit and attestation process, but the increasing implementation and integration of technology throughout the process means that the items that need to be incorporated into the risk assessment process must evolve. Specifically, the rise of blockchain and other encrypted distributed ledger technologies means that as information is uploaded and stored on these various platforms, the following questions and considerations need to be considered on top of present control and assessment practices (Alexander, 2019). First, which individual or firms have access to the core programming language and protocols that govern how the distributed ledger (or blockchain) technology operates? Second, are the internal controls that are in place at the organization being updated and modified to reflect the reality that blockchain represents a paradigm shift in how data and other types of information are stored, processed, and disseminated? Third, does the organization correctly map over and integrate the blockchain platform and information stored therein appropriately to both existing internal systems as well as any counterparty systems, such as EDI, that currently transmit and share data between organizations. Additionally, considerations that must be considered when evaluating the control structure and state around blockchain based or blockchain augmented systems include, but are not limited to, the following:

1. Is the original programming language, aka the reset code, that was implemented by the organization, maintained or stored somewhere secure?
2. Does the firm have a succession plan in place to maintain custody over the authorization mechanism in place to access, edit, and extract data stored on the blockchain platform?
3. Have internal controls been updated or modified to reflect the reality that, by implementing a blockchain augmented method of storing or transmitting information, the control structure will have changed?
4. Is the blockchain platform implemented at the organization updated or otherwise kept current to keep pace with modification to the open source origin of the platform? For example, if the Ethereum blockchain is the underlying platform, are sufficient efforts made to integrate approved EIPs into the organizational version?
5. Are the controls and plan, both linked to data access and the succession plan over data access mechanisms, articulated and enforced at the organization?

These controls and control protocols that are going to have to be developed and implemented are not going to be, implemented or designed in vacuum; it may ultimately end up being an integral component of current financial statement audits (Bhaskar, Schroeder and Shepardson, 2019). Specifically audit and attestation related practitioners are going to also need to assess what characteristics of blockchain technology, as it currently exists, intersects most directly with internal controls and other accounting protocols. A seemingly simple and straightforward requirement and expectation, but in order to accurately perform this comparison and assessment correctly practitioners are going to also need to understand what iteration and subset of blockchain is being implemented, as well as the specific challenges associated with that specific model. Building these bridges in a logical manner between current audit considerations and practices, and the blockchain technology as implemented at the organization, is also a responsibility and fiduciary duty of practitioners that cannot be relegated to that of secondary importance.

Headwinds to Adoption

This research does seek to analyze and present the considerations practitioners and firms will need to factor into the decision-making process as they connect changing risk assessment requirements connected to blockchain. Such research, however, does not assume that said adoption is guaranteed nor that it will be an easy task for the accounting industry or other professions. Significant headwinds do exist toward more widespread adoption, with perhaps the most powerful headwind being represented by the lack of consistent regulation and enforcement of blockchain standards (Price, 2016). Various jurisdictions have, it is true, adopted a forward-looking approach—including regulatory sandboxes—toward experimentation and implementation of various blockchain tools. Such forward looking jurisdictions are offset, however, by nation states and regulatory areas that have taken a more measured approach, or have banned cryptocurrencies, the most well-known blockchain application, altogether. This lack of consistency and standardization with regards to how blockchain is treated from an operational perspective does mean that adopting this technology poses a risk to the organizations that

adopt as early adopters. In addition to a legal patchwork that can lead to confusion and frustration on the part of business owners and investors, it also raises the very real risk of a lawsuit or motion made by a regulatory body that impacts a firm several years after the fact. As with the Kik lawsuit launched in the 2019 by the SEC, this time delay and still emerging regulatory framework can exacerbate an environment that already has elevated risk levels (Roberts, 2019).

Building on this lack of consistency, there is little authoritative guidance issued by either the FASB, PCAOB, or IASB to govern the cryptoasset space or how blockchain fits into the risk assessment process. Relatively simple matters including what counts as audit evidence, how to run substantive tests or analytical procedures, or what constitutes industry standards remain ambiguous at best. All of these factors do increase the risk of conducting attestation and assurance work in this space, as the industry practices currently under development may very well not end up being what is ultimately approved. An additional factor to consider is the liability and financial risk connected to offering assurance over an emerging technology platform with applications for so many industry sectors. Put simply, there are just not enough studies and authoritative groups to establish and determine what standard blockchain products and services should resemble.

In order to foster broader adoption, an increase in the standardization of these products and services must occur (Chender, 2018). As blockchain continues to be implemented and integrated into areas like financial services, healthcare, and food distribution, the risks of conducting an improper assessment, reporting incorrect findings, or fraud are substantial. Industry and trade associations, including the Blockchain Council, the Wall Street Blockchain Alliance, and the Digital Chamber of Commerce, have worked with regulators and industry partners to assist in resolving some of these questions, but these risks connected with blockchain are strong headwinds to broader adoption.

Connecting Blockchain to Audit Considerations

Regardless of the specific blockchain iteration that is adopted and implemented by an organization, there are a few core characteristics and traits that are common across blockchain projects and platforms. Prior to fully benefitting from these blockchain characteristics; however, practitioners must have a basic understanding as to how this technology connects to internal controls and other attestation considerations. Accounting practitioners will not have to become expert programmers or coders, but they must have a working knowledge connecting blockchain to controls and to the impact these changes will have on attestation engagements and the possibility of fraud (Sheldon, 2019). In addition to the commonality of these core traits and characteristics, there are also common audit considerations that need to be considered when assessing risk and completing the audit itself. The tamper resistant nature, which may also be labeled as the immutability of data once it has been validated and added to the existing blockchain, can prove to be a powerful tool under the control of an experienced audit professional or team. However, the immutability and tamper resistant nature of blockchain information also increases the importance of developing, implementing, and maintaining appropriate controls over the input of information on to the blockchain platform itself.

Consensus based validation and confirmation of information is also a core trait and strength of how blockchain operates and differentiates itself from existing database management systems. In essence and realizing that the specific consensus methodology will differ depending on the network specifications, this consensus protocol means that network members must approve of, and review, data as it is batched and posted onto the blockchain. Combined with the tamper resistant nature of the information after it has validated and posted onto the blockchain itself, this consensus-based process can create a virtually ready-made audit trail for future examination. Conversely, however, this process also means that care must be taken in order to prevent any one single entity or group of entities from obtaining an inappropriate level of control or dominance over the data posting and approval process.

The final component of blockchain that differentiates it from other distributed ledger technology tools and data management options is that, as data is uploaded and added to the blockchain it is continuously updated and communicated to all network members with access to the full record of transactions. Drilling down specifically, the communication and distribution of information differs from simply a decentralized database, which copies information to decentralized members but still relies on a centralized copy and storage platform to back up and maintain integrity over the data. The lack of reliability and other security considerations linked to distributed databases routinely generate headlines and new stories, regardless of where the data itself is stored or what specific subset of the business landscape is analyzed. It is increasingly clear that, under the current data control and security mechanisms, consumer and organizational data are continuously at risk of breaches.

Connecting the core characteristics and components of blockchain to audit and attestation engagements can be distilled into two general categories that appear to be especially applicable to the audit and attestation subset of the profession (Alarcon and Ng, 2018). First, the internal control component of the audit and attestation process, be it the internal control audit at large or the SOC 1 or SOC 2 engagement part of the audit, requires that the audit team be able to obtain a satisfactory level of understanding and comfort with the controls as they have been implemented. This need means that for every point of intersection and connection between blockchain and other technology systems there need to be a set of controls and protocols to protect the integrity and custody of data. Second, the interoperability of information and data between various input sources, the extraction and reporting of information based off of blockchain information, and the reporting of information that originates from different blockchain models remain open items from a practitioner and organizational perspective.

Identifying Appropriate Blockchains

Expanding the role of risk assessment, and acknowledging the fact that with any emerging technology there are bound to be learning curves and periods of adjustment, another aspect of the risk assessment process that needs to be conducted is the determination as to which type of blockchain is being utilized at the organization in question. Briefly recapping there are two major categories of blockchain in marketplace; public and private blockchains (PC Magazine, 2017). Drilling down there are multiple types and iterations of blockchains that have been distilled and developed under the private blockchain umbrella; fully private, consortium, and federated. As different blockchain options continue to enter the marketplace it is also important for practitioners to be able to balance the potential application of blockchain with the current state of the ecosystem. In order words, as the hype cycle inevitably continues and evolves to, possibly, the trough of disillusionment, practitioners need to be able to understand what blockchain is capable of, and what it is not capable of at the current time (Bicknell, 2019).

Working definitions for the iterations and types of blockchains can be presented as follows:

Public or permissionless blockchains are free to join, operate on a voluntary basis, and usually provide an inventive mechanism to encourage participants and members to remain an active part or the network. In order to maintain date integrity and security, a consensus methodology such as Proof-of-Work may be used, which while the most secure consensus method, is also the most time and energy intensive, as well as being the slowest (from a transaction throughout perspective) consensus methodology.

Private, or permissioned blockchains are on the other end of the blockchain spectrum, and while incorporating some aspects and benefits of blockchain technology, are controlled and managed by a single firm, usually referred to as the organizing firm. Since the network itself is controlled and managed by a single firm, there is a higher level of trust between network participants, which in turn means a less rigorous consensus methodology can be utilized such as Proof-of-Stake or an alternative methodology.

Consortium or federated—an offshoot and iteration of the private blockchain space, a consortium or federated model of blockchain can be interpreted as a hybrid between a public blockchain and private blockchain. While not completely permissionless in nature, the fact that this type of blockchain is managed by a group of organizations differentiates it from either a purely public or purely private model. In addition to spreading the management and governance of the blockchain among several organizations, this approach also results in lower costs and liability issues for each individual managing entity. This model would appear to be the logical iteration and step toward the development of sector specific or industry focused blockchain models since it allows several organizations in the same industry to pool resources and expertise to construct, implement, and maintain the blockchain for business purposes.

Every organization or group of organizations will design and implement a blockchain in a different manner, but in any event, it is important to recognize the reality that the implementation of a blockchain based model changes the internal control environment and what must be assessed. Specifically, the tamper resistant nature of the information once it has been added to the blockchain, as well as the real time nature in which that information is then distributed can present both an opportunity and challenge for practitioners seeking to attest to, or offer assurance services linked to, various aspects of organizational data.

Data Authorization Mechanisms

The concept and idea of restricting access to certain classes of information to a subset of individuals has long been a mainstay of sound internal control and data management policy. That said, the specifics of how data can be accessed and transmitted across blockchain based platforms means that current control policies and concepts, in and of themselves, do not appear to be sufficient to keep pace with the changing needs and expectations of organizations and the individuals employed therein. Put simply, in order to effectively advise clients or provide attestation services linked to the blockchain space, understanding the vocabulary and terminology linked to blockchain is a fiduciary responsibility of both regulators and practitioners (Walch, 2017). Specifically, if an organization wishes to increase security over the release, authorization, or modification of data once it has been posted to the blockchain ledger, establishing a multi-sig wallet, or some other form of combination-based access control seems to be a logical step. In short, a multi-sig wallet can be thought of as follows: if an organization has five key executives who have the authority to release potentially sensitive information or allow the transfer of funds, any three of those individuals must be present, or provide an authorization code or other indicator, to ensure that the information is only released when appropriate.

If such a multi-sig protocol is established, however, this multiplies the number of individuals who could, in theory, be compromised, indisposed, or otherwise inadvertently release data or authorize transfers in an unethical or unexpected manner. In order to successful combat this possibility, which is a real and objective business risk, the risk assessment process must be able to accurately evaluate several items. First, is there a mechanism or policy in place to safeguard the individual components of information required to form the combinations—as defined by the multi-sig protocol—necessary to authorize or approve the release of information or data? Additionally, for each individual with the level of access, a succession plan must also be established to help ensure that in the event of an unforeseen occurrence or event, that the organization maintains custody and control of its information.

On top of incorporating a multi-sig or succession planning perspective for the authorization of information, there must also be controls implemented to safeguard the information and data that is ultimately stored on the blockchain platform. In addition to the controls and policies that should be implemented over the core programming language itself, the organization must also integrate control procedures over the maintenance and implementation of blockchain at various phases of the firm. While it is true that some of these trends and directions will shift over time as the blockchain ecosystem and underlying technology matures, it is true that several audit implications have already entered the mainstream audit conversation. Information, and the effective utilization of that information, are increasingly at the core of competitive advantages across different aspects of the business landscape. Building on this direction and trend, however, are also the audit and attestation implications that have arisen from a professional perspective.

Audit Implications of Blockchain

Following the assessment and considerations that need to be considered, the implications of blockchain on the various aspects and parts of the audit process continue to increase and differentiate the work and expectations or practitioners moving forward. Whether from strictly an accounting or attestation perspective, or from a broader business point of view, it is important for practitioners in the financial services space to remain aware of both current future blockchain implications (Brainard, 2016). For example, from a SOC 1 and SOC 2 perspective, it is clear that the security processes both around information inside of an organization as well as the data reported to external stakeholders will have to change in response to the marketplace forces generated by blockchain and other emerging technology forces. Drilling down specifically, there appear to be the following three general areas of audit and attestation work that appear to lay at the center of the changes and ripple effects of blockchain on the audit and attestation ecosystem.

Take the following example: a private blockchain—be it a consortium or public-permissioned blockchain model—is established with a large organizing firm at the center leading the implementation cycle. Such an organization invites various suppliers and partner organizations to join the network and assigns various levels of access and data access rights to different organizations. One such organization that has been invited to join the network is the external accounting firm that conducts the audit of the organizing firm. As a relatively passive member of the network itself, the audit firm only is granted, in essence, read only rights to the financial and other sorts of information validated and stored on the blockchain. The specifics of how data can be read, be via a public/private key mechanism or some other methodology, can be established between the network members and the organizing firm.

During the business cycle, the accounting firm can have access to the information that has been validated and posted onto the private blockchain and can decrypt data pertinent to the audit and attestation workflow. Specifically, the following

components of the audit and data control process that can be most directly influenced by the implementation of blockchain into data management and attest work include, but are not limited to, the following:

1. Confirmation of payments and outstanding balances. A key pain point, both in audit work and in business at large, is the necessity to confirm both payments and outstanding balances from counterparties. Usually this process involves the manual reconciliation of multiple sets of books between counterparties, and the transmission of that data to the audit team. Even if the transmission of data takes place via a dedicated portal or messaging channel it does require time and effort to reconcile any outstanding differences. In a blockchain environment, where blocks of information are validated and posted by a various consensus methodology, this process—by default—means that there should be greater clarity and confidence in the current outstanding balances between different organizations. In other words, if balances are more readily confirmed and verified the need for confirmations to take place at the end of any given business period or cycle, as currently constituted, are not going to be as necessary.
2. Reconciliations also appear well situated to be disrupted, augmented, and changed at a fundamental level by the implementation and integration of blockchain throughout the accounting process. Making this transition, from the current environment where reconciliations occupy large amounts of accounting time and effort, to an environment where blockchain technology has moved more mainstream, is not going to be a short term or immediate transition. At the core of the idea, a reconciliation is necessary because there are two or more organizations that have to compare information to validate and or confirm that the information reported is indeed accurate. If, however, the information is not accurate, these differences and variances are documented and reported via the reconciliation process. In a blockchain environment, however, where data is reported, validated, and posted on a continuous basis by network members, the need for these comparisons are not as necessary.
3. Periodicity to continuous auditing and reporting of information also represents a shift and trend that appears well positioned to be accelerated or augmented via greater utilization of blockchain technology and trends. As other organizations and service offerings deliver personalized and customized information a near continuous basis, the accounting and auditing profession must be able to keep pace with the changing expectations of the marketplace. In addition to the other benefits related to encryption, security, and validation of data that blockchain can, and does, deliver, it also helps to enable to continuous reporting of data to both internal and external stakeholders. This reporting capability, in essence, relies on the network members and sharing of information to facilitate the delivery of data both between members and communication of that data to various end users.

What the specific area that is examined is, it is clear that the integration of blockchain within the audit, attestation, and assurance subsets of the accounting profession holds the potential to continue to drive change and disrupt current accounting services. Both in terms of accounting and financial services at large, it is clear that blockchain holds numerous potential opportunities as well as challenges for individuals and institutions alike (Varma, 2019). On top of the specific audit implications that are associated with the implementation of blockchain options and platforms, next level applications have the ability to either compound potential audit issues or streamline certain processes further. Smart contracts represent just one example of a next level application that is being adopted by industry at an accelerating pace and is something that could drive change in how audits and other attestation engagements are performed.

Smart Contracts Impact on Audits

An additional consideration and factor that should be considered when analyzing audit implications and considerations related to blockchain projects and implementation initiatives is the growing implementation of smart contacts (Crosman, 2018). Prior to analyzing specific implications and considerations, it is worth revisiting what a smart contract represents as well as how it is differentiated from other technology tools or platforms. Lying at the core of the idea and technology underpinning a smart contact should be the following working definition; a smart contract is neither smart nor a contact, but rather represents executable programming language that has been embedded onto a blockchain platform. Depending on the type of blockchain that has been implemented and linking back to the earlier analysis linked to the different iterations of blockchain technology the implementation of smart contacts will differ, but several considerations must be considered regardless.

First and foremost, the smart contract itself must accurately represent and translate the intentions of involved counterparties in a manner that is objective, logical, and able to be interpreted for business purposes. Building on this process, logically, in addition to understandability, enforceability is a key consideration as it connects to how smart

contracts can actually be used in a commercial enterprise (Aelbrecht, 2018). While this consideration may seem rather straight forward and obvious, it is also important to realize that even traditional contacts can lead to debates, misinterpretations, and liability between involved organizations. Best practice to avoid additional confusion as written contacts are translated into programming would be to work with an interdisciplinary team of experts and professionals, namely legal, technical, and management professionals (Mazero, 2018). Ensuring that both the programming language itself is accurate, and that the programming language accurately represents the original legal intent of the contract is also an important component of the control conversation. Drilling down, the audit considerations should focus on which individuals or organizations have access to the programming language, and which parties are associated with the development and translation of contracts into the programming language in the first place.

Second, and realizing that even with the consensus-based methodology of how information is added and validated by blockchain platforms, policies and controls must be in place to resolve disagreements that will invariably arise over time. Even the best written contact that has been approved and verified by experts may, at some point in the future, become the point of contention or disagreement between those entities that are involved. Especially as consortium blockchains continue to become more mainstream, whether in current iterations or the development of sector specific blockchain models, the possibility of cross agreements and contracts will continue to increase. Counterparty risk, ensuring that all stakeholders are properly identified and disclosed, and that controls are in place both at the organizations and between organizations lie at the intersection of smart contracts, audit and attestation work, and compliance. Specifically, the audit questions and considerations that need to be taken into account involve 1) are proper controls in place to secure the translation of legal contracts to programmable contracts, 2) do all involved counterparties have sufficient controls around the enforcement and validation of smart contracts, and 3) are steps in place to resolve disagreements that arise as a result of smart contract implementation.

Interoperability

Another consideration that should be considered when analyzing the audit and attestation implications of blockchain on audit and attest functions is an issue that appears to be of emerging importance within the blockchain ecosystem. As enterprise blockchains increasingly become part of the mainstream business landscape and are adopted by any number of specific firms across industry lines, the following will become an operational as well as attestation issue; interoperability (Manif and Marsh, 2017). The concept of interoperability is not necessarily a new topic, concept, or audit consideration; computer and technology systems have always had to be able to communicate and transmit data to each other. Integrating blockchain, however, into this conversation, raises additional issues that should be factored into the risk assessment process and audit procedures overall. Without claiming to be an all-inclusive or exhaustive listing of factors to consider, the following do appear important and logical to incorporate into risk assessment and testing practices.

First, an analysis and examination of blockchains that will be a part of the audit or attestation engagement must be conducted. It is not enough to simply examine and analyze the blockchain protocols and guidelines in place at the client or primary client, but practitioners must also be able to incorporate blockchain trends and protocols that are associated or interrelated to other organizations. These guidelines and best practices can also lead to unexpected complications, costs, and delays on the side of organizations and consortia that had previously shown enthusiasm for the blockchain based model (Wack, 2019). Put another way, if the client organization is a part of several blockchains the audit and attestation engagement must include testing, examinations, and review of all associated blockchains. In the case of supply chains, cross border payments, and transfers of intellectual capital and property these supply chains—be they digital or physical in nature—can include dozens, if not hundreds, or organizations. Documenting and reporting the controls, data access mechanisms, and succession plans for data access and management are integral to a successful and comprehensive audit.

Second, the connection points, portals, or application programming interfaces (APIs) in use between various blockchains should also be an area of focus for practitioners seeking to audit the integrity of data both within the organization and that information stored on the blockchain itself. Numerous headline stories of breaches, hacks, and other costly incidents that have occurred at blockchain based organizations, exchanges, and cryptocurrency related organizations have occupied the mindshare of practitioners in both accounting and other fields. With financial institutions still often struggling to integrate and incorporate existing technology systems with each other, the addition of a blockchain based platform can significantly compound the interoperability risk, in addition to increasing the cost of doing so in a compliant manner (Lai, 2019). That said, it is important to drill down deeper into these incidents to understand what specifically occurred to cause the breach or hack itself. Many, if not the majority, of losses and breaches have been generated by a lack of controls and

protocols in place around how data is validated, reported, and extracted from the blockchain itself. Regardless of the specific platform that is implemented, and the nature of the blockchain platform, robust controls must be integrated into every aspect of how the data is imported and exported from the blockchain itself.

Third, and amplified in situations where multiple organizations are utilizing multiple iterations of blockchains, maintaining appropriate segregation of duties and responsibilities is important for a comprehensive analysis of blockchain platforms that have been put into place (Nair and Sutter, 2018). For example, in a consortium blockchain such as interbank information network (IIN) organized and led by JP Morgan, is JPM the only firm that can grant access to information from an audit and attestation perspective? Additionally, are there communication channels in place for network members to communicate and document how business changes could change how the currently implemented blockchain interacts with the rest of technology infrastructure? Finally, the attestation or audit team must feel satisfied that, on top of having documentation available, that said policies and practices are actually being followed and utilized. Interoperability is not a new concept of idea, but it is something that has the potential to become even more interconnected and complicated as blockchain integration continues to advance and become more mainstream.

Future Directions

The analysis of blockchain technology on the accounting profession, and more specifically the analysis of how blockchain will drive change in the audit and attestation subsets of the profession both represent areas of emerging importance with much work yet to be conducted. Even with that reality acknowledged, however, it is becoming clear that several fundamental changes, including but not limited to technology advances like blockchain, are driving change and disruption across the accounting landscape (Tysiac and Drew, 2018). Rising in importance alongside the specific tools and protocols associated with blockchain are client and customer expectations of both a more continuous and more comprehensive audit process. Understandably there are questions as to how exactly the integrity of the attestation and audit process can be maintained as increasing amounts of information are stored, validated, and communicated via a decentralized and distributed system. While it is yet to early to state with certainty how the professional practices will evolve and develop to contend with said changes, it is evident that such efforts are already underway. The various aspects of blockchain and audit that have been presented within this research are by no means the only considerations for the profession, but rather a starting block for continued research, discourse, and analysis. In order to remain relevant and competitive in a fast-changing marketplace, practitioners will need a mastery of both the technology platform itself, as well the ripple effects greater integration of blockchain will have on business, data management, and reporting of financial and nonfinancial information. Researchers and practitioners alike, seeking to obtain both a robust understanding of the technology itself, and of the implications it will have on the profession, are well positioned to benefit from these advances and developments moving forward.

References

Aelbrecht, J. (2018). Enforceability for smart contracts is key—lawyer. *Global Investor*, 67.

Alarcon, J. L. "John," and Ng, C. (2018). Blockchain and the future of accounting. *Pennsylvania CPA Journal*, 3–7.

Alexander, A. (2019). The audit transformed: New advancements in technology are reshaping this core service. *Accounting Today*, *33*(1), N.PAG.

Alexander, A. (2018). Changing tools, changing roles: Technology is driving the audit of the future. Accounting Today, 32(3), 10–14.

Boillet, J. (2017). Are auditors ready for blockchain? The audit profession is eyeing blockchain. Accounting Today, 31(9), 34.

Bhaskar, L. S., Schroeder, J. H., and Shepardson, M. L. (2019). Integration of internal control and financial statement audits: Are two audits better than one? *Accounting Review*, *94*(2), 53–81. https://doi.org/10.2308/accr-52197

Bicknell, D. (2019). Balancing Blockchain Hype with Reality. *MEED Business Review*, 30–31.

Brainard, L. (2016). Distributed Ledger Technology: Consider the implications. *North Western Financial Review*, *201*(12), 8.

Chender, L. (2018). Standardized products needed to maximize DLT – DTCC. *Global Investor*, N.PAG. Retrieved from http://search.ebscohost.com/login.aspx?direct=trueanddb=bahandAN=130438217andsite=ehost-live

Crosley, G., and Anderson, A. (2018). The audit of the future: Daring, disruptive and data-driven but poised to add significant value to firms and clients. *Public Accounting Report*, *42*(2), 5–8.

Crosman, P. (2018). Could smart contracts sideline banks? *American Banker*, *183*(224), 1.

Dudgeon, N., and Malna, G. (2018). Distributed Ledger Technology: From Blockchain to ICOs. *Banking* and *Financial Services Policy Report*, *38*(2), 4–9. Retrieved from http://search.ebscohost.com/login.aspx?direct=trueanddb=bahandAN=128096007andsite=ehost-live

Jun Dai, and Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems*, 31(3), 5–21. https://doi.org/10.2308/isys-51804

Lai, K. (2019). Fintech: banks still struggle with culture and legacy systems. *International Financial Law Review*, N.PAG. Retrieved from http://search.ebscohost.com/login.aspx?direct=trueanddb=bahandAN=136132258andsite=ehost-live

Mahbod, R., and Hinton, D. (2019). Blockchain: The future of the auditing and assurance profession. *Armed Forces Comptroller*, 64(1), 23–27.

Manif, J. L., and Marsh, W. B. (2017). Banking on distributed ledger technology: Can it help banks address financial inclusion? *Economic Review (01612387)*, *102*(3), 53–77.

Mazero, J. (2018). Blockchain: How to use smart contracts. *Franchising World*, *50*(11), 19–22.

Mundra, S., and Lawlor, B. (2018). Blockchain initiatives and implementation. *Information Services* and *Use*, *38*(3), 187–189. https://doi.org/10.3233/ISU-180022

Nair M., and Sutter, D. (2018). The blockchain and increasing cooperative efficacy. *Independent Review*, *22*(4), 529–550.

Price, E. (2016). Regulatory divergence could hamper blockchain. *International Financial Law Review*, 8. Retrieved from http://search.ebscohost.com/login.aspx?direct=trueanddb=bahandAN=118183727andsite=ehost-live

Raphael, J. (2017). Rethinking the audit. *Journal of Accountancy*, 223(4), 29–32.

Roberts, J. J. (2019). Does the SEC's ICO Lawsuit Against Kik Go Too Far? *Fortune.Com*, N.PAG

Sheldon, M. D. (2019). A Primer for Information Technology General Control Considerations on a Private and Permissioned Blockchain Audit. *Current Issues in Auditing*, *13*(1), A15–A29. https://doi.org/10.2308/ciia-52356

Tysiac, K., and Drew, J. (2018). Accounting firms: The next generation. *Journal of Accountancy*, *225*(6), 3–9.

Varma, J. R. (2019). Blockchain in finance. *Vikalpa: The Journal for Decision Makers*, *44*(1), 1–11. https://doi.org/10.1177/0256090919839897

Wack, K. (2019). BofA, Wells Fargo sour on blockchain. *American Banker*, *184*(61), 1.

Walch, A. (2017). Blockchain's treacherous vocabulary: One more challenge for regulators. *Journal of Internet Law*, *21*(2), 1–16.