Emerging Blockchain Implications: Governance and Cybersecurity Considerations for Accounting Professionals

Dr Sean Stein Smith
Department of Economics & Business
Carman Hall, Lehman College of The City University of New York
250 Bedford Park Blvd. West Bronx, NY 10468, USA

Email: sean.steinsmith@lehman.cuny.edu

Abstract
Blockchain is perhaps one of the most widely discussed topics in the accounting and financial services professions during the last several decades, but it is much more than yet another technology tool. At the core of the idea, blockchain has the potential to redefine many of the core functions and tasks currently performed by accounting practitioners employed both within private industry and public accounting firms. Auditing and attestation functions, tax reporting and analysis, and the broader cryptoasset arena are presenting practitioners with both opportunities and challenges that have been analyzed in numerous practitioner and scholarly venues. Even with these substantive conversations, however, there remain areas and topics open for further discussion and analysis. Specifically, what this piece does is analyze two areas of emerging importance; corporate governance (CG) and cybersecurity. Already driving change and opportunities for practitioners, blockchain can amplify these trends, and are examined in a manner applicable for both practitioner and academic users of this research.

Keywords: Blockchain, corporate governance, cybersecurity, disruption, fiduciary

Introduction
The topics of blockchain, and blockchain applications for financial services professionals, have been an extremely popular and emerging topic since it was introduced to the wider marketplace via bitcoin and other cryptocurrencies beginning in 2017. Applications and opportunities for financial professionals to better utilize blockchain and blockchain based applications are applicable for virtually every aspect of the accounting and finance fields. Tax reporting and analysis can be streamlined via the increased efficiency with which data can be shared between network members, in addition to the encryption that lies at the core of the blockchain model. Auditing and assurance engagements can also be improved and completed with increased speed since, by default, information stored on a blockchain is confirmed in some manner by the various network members. Confirmations, valuation exercises, and other audit and attestation tests and tasks can either be augmented or rendered obsolete as blockchain becomes increasingly integrated in the business landscape. As potentially paradigm shifting as blockchain may be for accounting, however, those are just some of the options and opportunities that blockchain can create for financial scenarios. Alongside the rise of this technological tool, however, is also the growing importance of how accounting data connects to CG. CG relies on the consistent and transparent

distribution of information to internal and external end users, and accounting information is an important component of the total data produced by the organization.

Connecting blockchain to CG

Prior to analyzing the specific characteristics of blockchain, which are important for both practitioners and academics to understand, viewing the conversation from a bigger picture perspective also seems logical. Corporate governance, especially from an accounting and financial service perspective, connects to the need for stakeholders – both internal and external – to be able to trust and effectively leverage the information generated by the organization. For the purposes of this research, stakeholders can be defined and specified as the users of financial information who are dependent on data produced by the organization itself. Stated differently, stakeholders can include creditors, investors, regulators, and other governmental entities that interact with the organization a regular basis. Upon initial review, such a broad audience may seem excessive, but that reflects how CG has evolved and developed over time in the face of different scandals and market events.

Beginning with the corporate fraud at Enron, which at the time was the largest bankruptcy in the U.S. history, and continuing to the failing of Lehman Brothers, which surpassed Enron as the largest bankruptcy when it failed during the Great Recession, there does appear to be a common theme. In both of these instances, in addition to the questionable ethics and actions taken by the management team, there was a lack of transparency and clarity connected to the accounting data published to the marketplace. Drilling down, a core problem that arose in both situations were accounting systems and reporting processes that did not accurately safeguard and secure accounting information. In both cases, the ability of management teams to manipulate or selectively disclose or certain pieces of information led directly to the failings of these firms.

Blockchain, although not initially designed or intended to function as an accounting system, holds a particular technological imperative for accounting professionals to be aware of as it connects to data integrity and transparency. Discussed in more depth in the following section, the following connections and links will be addressed and expanded upon. From an accounting perspective, how does blockchain connect to current and future accounting considerations, as well as the rising importance of accounting data to corporate governance. After reading this research and analysis, both practitioner and academic users will leave better educated on both blockchain specifics and how blockchain technology connects to accounting information. Building on this linkage, the connections and relationship between accounting, CG, and the possibility to use blockchain as an accounting tool will be illustrated and communicated in a manner that produces actionable business intelligence.

CG

CG, at the core of the idea, represents how the organization interacts with different internal and external user groups. Specifically, CG can be thought of as the vectors and methods by which the organization manages relationships, assets, and the

responsibilities they have been entrusted with by stakeholders. Information sharing is not new, however, and has long represented both an opportunity and a challenge for practitioners (Pratt & Storrar, 2017). Specifically, from an accounting and technology perspective, the loss of access to information may have actually been a result of, and generated by, the very technologies that have enabled more real time reporting in other ways. As technology and the digitization of data continues to become increasingly integrated into how organizations operate, it is increasingly apparent that in order to maintain adequate disclosures, this dialogue needs to be proactively pursued by professionals. Stakeholders, virtually by default, are going to have a variety of expectations, requirements, and needs as it connects to the organization, but one common thread appears to remain consistent. The management of information and data, both generated internally, and that information obtained from external sources, is increasingly important to manage as the volume of this information continues to increase. Internal stakeholders include employees and management professionals, and external stakeholders include a range of users from investors to creditors to regulators; all parties involved rely on the organization produce and communicate high quality data to enable effective decision making. Drilling down to identifying what specific types of information, and taking into account that every organization is different, it becomes clear that the effective and efficient distribution of financial information lies at the core of how CG connect to accounting and blockchain itself. Financial information and data is often a primary tool used to judge by the organization itself as well as the management team of the organization, so it does make sense that this would fall under the categories of data applicable to a CG conversation.

The sharing of information is a fiduciary responsibility and duty of all organizations, and will also have an impact on how blockchain becomes integrated within the broader business landscape (Campbell-Verduyn & Goguen, 2018). CG obviously applies to other classes of information generated and communicated within the organization, but building the bridge between accounting, blockchain, and CG also requires incorporating the hierarchy of shareholders and stakeholders. Whether the conversation connects to the 2019 Congressional examination of Facebook and Libra or some other analysis of blockchain itself, the financial services implications are becoming clear. Financial data serves an important role to both internal stakeholders as well as external shareholders, which also provides an opportunity for blockchain to add value. This value can be derived with via the increased traceability associated with blockchain, or the tamper resistant nature of records stored therein, but in any case it returns to the security and transparency connected to organizational data. Clearly not every instance of a lack of transparency, should be affiliated with fraud or unethical behavior, but opacity and lack of timeliness do represent issues that blockchain seems able to at least partially address. Building on this, the linkage between CG and various blockchain options continue to emerge and crystallize.

The management of organizational data, and the communication of certain pieces of information to different stakeholder groups, is one of the most well know and arguably important responsibilities of a board of directors at an organization. Ensuring that all material data is disclosed, stakeholders are kept informed of what is occurring at the

firm, and that privacy regulations are not violated also fall into this category. The technological disruption and changes generated as a result of digitization and technology integration continue to drive change in virtually every aspect of accounting. Specifically, audit processes, procedures, and the education of auditors and attestation professionals will need to evolve alongside the changing marketplace (Cong, Du, & Vasarhelyi, 2018). Whether it is connected to the ability to conduct continuous audits, real time analytics, or new types of financial reporting it is clear that technology will generate both opportunities and challenges for the profession. Blockchain is based on the sharing and distribution of information between network members, and is done so on a nearly continuous basis, which has the potential to generate efficiencies and benefits across industry lines. With these benefits, however, also come challenges and obstacles that can hinder or inhibit the full implementation of blockchain at different organizations. For example, customer data and information – in addition to representing a hot topic and something that is on the agenda of every board and organization – can also be a source of exposure and liability for the firm if handled incorrectly or by unauthorized personnel.

Consumers who do not sign off on, or who are not aware of the actions being undertaken at the organization with regards to potentially confidential and identifiable information, may lead to negative repercussions from both a reputational and financial perspective. Another implication that must be taken into account is the rise of smart contracts, automated sections of code that execute specific commands via a blockchain based platform, which should lead to closer coordination between financial and legal professionals (Butlet, Khalil, Ceci & O'Brien, 2017). Stated in a different manner, in order for the fiduciary duties of an organization to be fulfilled, even as emerging technologies such as blockchain continue to be more mainstream, means that practitioners need to understand how current roles and responsibilities connect to these new areas of importance and responsibility.

Regardless of whether the specific data point in question is connected to consumer data, healthcare data, or financial information, the connection between CG responsibilities and accounting professionals continues to emerge. Linking back to the goal of CG, distributing operational and financial data to internal and external users of organizational data, blockchain does seem to offer a potential solution to data governance considerations. Specifically, breaches, hacks, and possibly unintentional leaks of confidential and personal information represent risks from an operational and financial perspective. The encrypted nature of the information stored and distributed via a blockchain, the specifics of which are outlined throughout this research, also creates the need for differentiated and iterative accounting services.

Blockchain characteristics

Although the earlier coders and programmers of blockchain based platforms may have operated purely as programming experts, this piece addresses a core question and consideration that arises as blockchain becomes more mainstream; what are the fiduciary responsibilities of programmers and implementers of blockchain based

solutions (Walch, 2016)? Generally speaking the implications of CG from a financial services sector has not traditionally laid at the nexus of accounting services, but distributed ledgers and blockchains continues to change that perspective. Key factors that need to be considered include how blockchains – designed to be immutable and distributed – can be adapted to contend with the array of administrative and operational issues facing organizations. More to the point, it seems appropriate to draw on previous informational technology architecture and control oriented research to assist in addressing these current, and future, questions (Zachariadis, Hileman, & Scott, 2019). Specifically, can the interoperability struggles that impact traditional computing systems be allayed, at least partially, in a blockchain centric environment. In addition to the issues connected to scalability and latency, practitioners should also draw on established technology control policies to how systems adapt and interoperate with other platforms.

Even as accounting organizations contend with the ramifications of blockchain, numerous questions remain about how blockchain and other technologies will change the future of the profession (Alarcon, 2018). A core strength and positive attribute of blockchain is that the information that has – via a consensus methodology of some kind – been stored onto this distributed and decentralized ledger is than communicated to network members on a continuous basis. Such a continuous flow of information, especially when coupled with other automating technologies such as robotic process automation and artificial intelligence create both challenges and opportunities for practitioners (Brazina & Urgas, 2018). This information is able to be communicated in a secure manner due to the encryption that underpins many blockchain platforms. For example, information that is stored and communicated on the bitcoin blockchain utilizes a proof of work consensus approval methodology that, combined with a 256-bit encryption hash protocol, has proved resistant to all hacking attempts as of this research. This combination of factors, the hashing protocols embedded at the core of blockchain and the distribution of data on a continuous basis, represents a potential paradigm shift in how data is stored, processed, and analyzed between different individuals and institutions. This communication and sharing of data, even in an encrypted manner, simultaneously is a strength of the technology but also a potentially obstacle for future mainstream adoption.

Third, and the final core aspect of blockchain that connects this technology to broader business issues like cybersecurity and corporate governance, is that blockchains need not utilize or be associated with cryptocurrencies. Although the idea of blockchain may have been introduced to the wider business marketplace via Bitcoin and other cryptocurrencies that is merely one application of this technology. Wider utilization and adoption of blockchain may simultaneously drive more comprehensive regulatory and business adoption, but also means that more robust control policies must be put into place as well. Especially as blockchain begins to store and transmit a wider array of information, it seems logical to conclude that fundamental audit practices will need to evolve and change (Raphae, 2017). Specifically audit practices and procedures will need to evolve to not only reflect the technological changes generated by blockchain, but alsos the expectation of more continuous reporting. Examples of how this is already

happening can be seen in how analytics, workflow automation, and data visualization are being implemented and utilized in the audit process. Additionally, the education and continuous training linked to auditors will also need to evolve and change to keep pace with both technology changes as well as process changes linked to attestation services. In earlier stages and iterations, with blockchain primarily serving as a vehicle for cryptocurrencies, the institutional and systemic risk posed by breaches and hacks connected to blockchain were limited. That said, as blockchain becomes more integrated throughout different industry sectors, these are risks and components of the broader dialogue that financial professionals need to remain aware of.

An associated issue that practitioners need to remain informed about during the greater integration of blockchain into business applications are the different types of blockchain platforms currently available in the marketplace. Public blockchains, private blockchains, and consortium based models of implementing a specific blockchain model are going to continue to develop and evolve on parallel, but related, tracks during the coming years. Record keeping, and performing a variety of accounting functions, increasingly prevalent among existing and emerging software platforms should lead to a comprehensive analysis of the pros and cons of implementing such a system (Lemieux, 2017). While every type or iteration of blockchain has certain core characteristics that are similar, the implementation of these tools as well as the implications of these options on cybersecurity concerns will vary. Much like every software program or system has different operating protocols it is reasonable to expect that – depending on the type of blockchain that is implemented, that the control and broader governance considerations will also differ. One specific application and use that should be explored includes the potential application and hurdles for seeking to implement blockchain to improve the credit card and payment processing conversation.

From a market perspective, for example, even though equity and bond trades may appear to settle instantly – especially with the rise of mobile based trading applications – the actual settling of transactions can take several days. If the conversation is focused around international transactions the time it takes to settle transactions can take even longer. The example of credit card processing and other financial transactions is simply one of the many opportunities that can and are being generated via blockchain and other tools of digital disruption (Banham, 2017). As it directly connects back to this research, the digitization of information means that CG will need to removed exclusively from the realm of IT and handled by a broader audience, and cybersecurity controls will need to be updated and modified to reflect the current environment. Trade finance, such as letters of credit and other related tools connected to shipping and logistics, have only had slight updates and modifications during the last hundred years. Although some applications and technology solutions have resulted in increased efficiency and speed for which trades are completed and settled, many of the back end solutions have, for the most part, remained unchanged. An additional aspect of finance that can be changed or augmented via greater blockchain integration and technology is the credit card industry. Credit cards, although convenient and again seemingly instantly settling in nature, do have several issues that blockchain may be able to address.

Instantaneous payments and swipes on the surface obscure the fact that, in order for a credit card transaction to actually complete the payment and transmission process the transaction might have to pass through 3 or 4 different financial institutions. Increasing the complexity of transactions and associated information only increases if purchases are made online or from vendors operating in international markets. Given these areas for improvement, including efficiency related and financially driven reasons, it is important for financial professionals to understand the fundamentals of how this technology works. Clearly there do not appear to be expectations that financial professionals are going to have to become compute programming experts, but it seems logical to expect practitioners to have fundamental understandings of how this technology works. Prior to analyzing considerations connected to governance and cybersecurity it seems reasonable to examine some of the core characteristics of blockchain and how it functions versus existing technology tools.

Cybersecurity with blockchain

Even as identified above, since blockchain has provided tamper resistant and encrypted to date, that does not mean that cybersecurity issues can be put on the back burner. To the contrary, as different blockchain models and platforms are readily identified and adopted at the enterprise level the importance of cybersecurity is only set to increase over time (Nallengara, Alsop, & Halbhuber, 2018). This includes increased focus on data input, data quality, and data access controls, as well as the ability to control which parties have access to the underlying code. Auditing and offering assurance level of services over different types of controls and information associated with controls is, in and of itself, nothing new or innovative, as practitioners have performed this service for decades, but with blockchain entering the landscape the attestation conversation must change. As addressed by (Crosman, 2018), the questions related to the blockchain implications connected to fraud prevention are significant, and are already driving debate and analysis across different aspects of the financial services profession.

Cyber threats and cybersecurity themselves are not necessarily new to the financial services profession, but blockchain does have the ability to change virtually every aspect of cybersecurity and cyber policies at an individual and institutional level. During the course of a SOC 1 or SOC 2 audit, for example, there is almost always an examination, review, and testing of the controls that in place at an organization. Drilling down, there is also evidence that blockchain based platforms, and the controls and procedures to be built around these systems, can also assist with helping to ensure compliance with emerging regulations such as GDPR and SRD II (Tashea, 2018 & Pablor Mayo Cerqueiro, 2018). Additionally, for a financial audit itself, an audit of internal controls also must be conducted as mandated by the passage of the Sarbanes Oxley act or 2002. Standard control testing processes and reporting requirements have been well established as a result of these requirements, but similar standards remain – as of this research – unavailable for blockchain based applications. One of the first questions that has been asked with regards to different type of information secured via a blockchain model is whether or not this data is able to be audited, assured, or attested to in a manner similar to traditional financial data.

This is not merely an academic issue, as the death of the CEO of Canadian cryptocurrency firm in early 2019 exposed a core weakness, at the cost of $250 million USD, at the heart of many of these emerging systems. Events such as this also illustrate that as financial technology platforms and tools mature and become integrated into the mainstream financial system the founders and managers of these platforms will have to contend with problems that have up until presently remained hypothetical in nature (Kanach, Cross & Moynihan, 2017) The security and encryption over access to cryptocurrencies and different cryptoassets is, in many cases, so robust that without the appropriate identifying information it is virtually impossible to access information even in cases where doing so is necessary. The implementation of Sarbanes-Oxley, although not an ideal or perfect regulation, did indeed outline and document the roles and responsibilities that accounting professionals need to fulfill from a cybersecurity and data governance perspective (Damianides, 2007). Specifically, the roles and duties of accounting and attestation professionals, whether employed internal or external to the organization itself, must understand and be able to articulate the appropriate tactics and strategies to safeguard and accurately report financial and operational data. Establishing protocols for redundancy of information, off site storage of access information, and other techniques to allow the accessing of data by different members are steps that are gradually being taken. That said, it also remains true that many blockchain based applications remain little changed – at an operational level – from the earliest models underpinning bitcoin and ether.

As blockchain emerged into the mainstream business conversation during 2018 and continuing into 2019 a common theme also emerged among organizations seeking to leverage the benefits of this tool. Addressing some of the issues listed above, namely the time and energy required to post and approve entries, several iterations and blockchains are entering the marketplace as viable options to the proof of work consensus approval methodology. Whether it is proof of stake, proof of elapsed time, or some other version of consensus methodology, these are the options and versions that are generating significant interest in the enterprise space. While these different iterations and versions, clearly, do have benefits in terms of efficiency and the speed with which transactions can be processed, the do also raise a question that practitioners need to be aware of moving forward. Drilling down to the core essence of the issue, the key question is whether or not these enterprise blockchain options – fully equipped with different approval methodologies – raise other significant cybersecurity and CG for practitioners to consider

Emerging issues

The ultimate goal of many blockchains, or blockchain affiliated organizations, is that these platforms can be adopted and implemented for enterprise utilization and adoption. That said, a consistent hurdle and obstacle for many organizations attempting to achieve this goal is that, as currently constituted and implemented, blockchain does not meet the criteria or usage expectations of corporations. Payment options, transferring capital between different individuals and institutions, and the ability of organizations to leverage the tamper resistant and encrypted nature of blockchain platforms represent

options for organizations to maximize going forward, including reducing errors, omissions, and opportunities for unethical activities (Lai, 2018). That said, as enterprises modify and customize blockchain based or blockchain augmented platforms for corporate use or to implement within different organizations, there are additional cybersecurity issues that need to be evaluated as this process occurs. Drilling down specifically into some of these core issues that will invariably accompany the continued development of enterprise blockchain, the following issues connect blockchain implementation to both cybersecurity and corporate governance.

First, if a blockchain based platform is modified and customized to be put to work within a corporation or group of organizations, does that undermine the very strength of the blockchain model itself? At the core of the concept lay both the encryption protocols built into the blockchain itself and the tamper resistant nature of the information that is stored on the blockchain as a result of this encryption. Second, as these enterprise blockchains continue to gather steam and accelerate in 2019 and beyond, the challenges and questions that arise as far as connecting blockchain based information to current enterprise planning systems will only become more prevalent and important. For practitioners some of the core takeaways and implications connected to this increased implementation will have to do with internal controls, the transferring of information between interested parties, and the auditability of said data (Herian, 2018). These topics and trends, important as they are, may actually end up masking or overshadowing a bigger structural shift that CPAs and other accounting practitioners will have to embrace moving forward. Technology, as is already occurring, will continue to disrupt, augment, and fundamentally change the role that practitioners play in terms of both internal functionality and external advisory services.

Specifically, cybersecurity issues and considerations that should be examined as blockchain based solutions are considered should include, but are not limited to, the following:

- Are current internal controls around information technology appropriate for dealing with blockchain based solutions?
- Do members of the organization understand the implications of blockchain on cybersecurity procedures and controls?
- Have clients and customers been consulted as to the implications of blockchain on how identifiable and confidential information may be shared?

As controllers and CFOs continue to become increasingly integrated with technology teams and individuals at different organizations these practitioners will need to understand just what some of the cybersecurity implications around blockchain actually represent. Clearly blockchain is still an emerging field and topic that must be addressed, but that also means that the change and shift of accounting professionals to a blend of financial and technological experts will only continue to accelerate and gain momentum across industry lines. Additionally, it is also important that practitioners understand how this impacts the professional landscape currently. Continuing this shift, however, also requires that professionals understand how cybersecurity, emerging technologies such

as blockchain, and CG intersect. In addition to the implications for practitioners and professional at various staff levels, the importance of CG in an increasingly blockchain based environment should be a point of focus for boards across industry lines (Landefeld, Mejia, Handy & Hinnen, 2017). While not necessarily a combination of topics that might traditionally have been associated together, the ideas and concepts of CGand cybersecurity may be more closely aligned than previously imagined.

Internal Controls

Linking back to the concepts of blockchain and cybersecurity, the implications of CG for accounting professionals becomes clearer. Accounting practitioners have a fiduciary responsibility to protect and secure all of the organizational data falling under the purview of accounting and attestation work. The sharing of information between network partners and coordinating the flow of data between different stakeholders Connecting these two concepts, and drawing a bright line between the implications of cybersecurity and blockchain is possible by emphasizing the importance of more robust and comprehensive internal controls, especially the controls that are related to the disclosure and reporting of information.

Internal controls, rather obviously, are a topic and theme that financial and accounting professionals are well versed in regardless of which industry subset or sector practitioners are employed within. For the purposes of this research, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) provides a concise and relevant definition applicable to this research. The framework defines internal control as a process, effected by an entity's board of directors, management and other personnel, designed to provides reasonable assurance regarding the achievement of objectives in the following categories:

1. Effectiveness and efficiency of operations
2. Reliability of financial reporting
3. Compliance with applicable laws and regulations

Since blockchain, even if operated in a more centralized manner than a fully public blockchain such as those launched by many organizations, operates differently than many existing data management systems, controls and control processes must evolve and change alongside the increased integration of technology tools. Data sharing is nothing new, but the distributed nature of blockchain leads, rather logically, to the rise of distributed accounting and distributed ledgers playing a more prominent role in the financial services space. Data sharing has been long been a mainstay of financial services and the distribution of information, and has consistently been a point of concern for managers inside and outside of the accounting space.

First, and even though automation and increased technology integration may appear to reduce the risk associated with the processing and reporting of information these technologies my actually increase the risk of breaches and hacks. At the core of any robust and comprehensive cybersecurity platform or policy is the ability of the organization to control the flow of data both as it enters and as it exits the organization. One of the core attributes and benefits of blockchain is the sharing and communicating

of information, something that is already being implemented and generating benefits for organizations. Connecting blockchain to other enterprise ready technology developments, such as the internet of things, may simultaneously increase efficiency and productivity of certain operations, but also inadvertently expose the organization to a broader array of risks. For example, a counterparty organization may have the same level of controls or policies as the organizing firm, opening the entire network to increased risk.

Automation in and of itself, if not layered on top of processes with appropriate controls and safeguards against the misuse or mistreatment of organizational data may merely compound existing problems and issues. Taking these facts into account it seems logical to also view the importance of controls from a governance perspective. In the case of a financial institutions, for example, and something that has been demonstrated by the record setting fines levied on some institutions, breaches or the misuse of organizational data can have a substantial bottom line impact. In a business environment where business hacks and breaches are becoming increasingly common, and data is increasingly evidenced viewed as a competitive asset, a core duty of all professionals should be to safeguard and secure the information flowing through the organization. Tactics and tools to translate this desire and expectation into reality are, where in almost every organization, internal controls can play a pivotal role.

Internal control considerations

Clearly every organization is different and will contain different areas of focus with regards for internal control implementation, but it is something that should be taken into account across industry lines. Once again, the connection between CG cybersecurity may initially seem to be tenuous at best, but it is something is increasingly possible due to the importance of controls. Data, both its management and the potential for breaches and hacks can cost organizations both financially and reputationally, and accounting professionals are usually tasked with managing the analysis and stewardship of said information. Taking a look at control considerations, as well as how these considerations connect to governance, the following items should be considered, but should not be considered all exhaustive in nature.

First, even as emerging technologies, including blockchain and robotic process automation, continue to become more mainstream in nature, the importance of connecting these tools to existing enterprise planning systems will continue. Issues of data cleanliness, standardization, and the protecting of pieces of information will only increase in importance as automation continues to become integrated within the profession. Moving forward from a strictly financial conversation, although outside of the traditional scope of accounting and financial services, represents another connection between governance, cybersecurity, and emerging technologies. Organizations are already using these and similar tools to redefine and augment existing business models, and these changes also could, if implemented incorrectly or haphazardly, potentially expose the organization to liability. For example, if a manufacturing organization seeks to implement greater uses of blockchain to track inventory information on a continuous

and real time basis – to be shared amongst network members – the loss of this information could be devastating from a financial and operational perspective.

Second, and connecting to the earlier point raised about blockchain modification to make it more readily useable from an enterprise perspective, controls and control policies over who has access to the blockchain itself are imperative. If external consultants were brought into the firm to assist with other types of projects or initiatives the management team at the firm would certainty take steps to ensure that access organization data was limited only to what was necessary. Information technology projects, including blockchain and other emerging technologies, are not different from a project perspective than other projects. Ensuring that, even if the consultants employed by the firm come from a reputable organization, that access is limited only to what is specifically needed to complete the work is a dialogue that accounting professionals should be a part of. This restricted access and information also connects to a third consideration and point that needs to be part of the internal control conversation; internal considerations that professionals need to remain aware of going forward.

Even though virtually every accounting professional is familiar and well versed with the terms and concepts related to blockchain, cryptocurrencies, and automation software, organizational understanding often remains at the conceptual level. Despite the reality that these topics have been discussed and debated at virtually every conference and publication across accounting and financial services lines, this also presents a control challenge.

Let’s take a look at some of the considerations and topics that could very form the basis for how CPAs and other financial professionals contend with blockchain as well as the associated issues of cybersecurity and corporate governance.

1. Make sure that emerging technology platforms can be integrated into existing technology platforms and options. Although blockchain has certainly developed and become more refined since initial implementation via the bitcoin blockchain, a pain point that remains is the bridging of these platforms with existing technology tools. In addition to the convenience and data clarity issues that may arise if information is not standardized or recorded in a consistent manner, this also raises a control issue. For example, if information is not migrating consistently or accurately between different modules or platforms this creates an opportunity for unethical individuals to take advantage of these gaps. Either by accident or by deliberate action, not having robust controls over the intersection of data between different tools is an area that CPAs should play a prominent role in addressing.

2. Ensure that the types and classes of information being stored on a blockchain or blockchain based platform are actually able to be shared. Linking back to an earlier point about the consistency and standardization of information, it is equally important to recognize that not all information is applicable for storage via blockchain based tools. As blockchain becomes increasingly integrated into different organizations and industry subsets, including organizations that handle

personally identifiable information, this is not a minor point that can be overlooked or relegated to the proverbial back burner. Examples of the types of information that might not always be appropriate or applicable for blockchain based storage include healthcare information, tax information, and potentially confidential or proprietary information.

3. Coordinate with different network members. At the core of blockchain technology is the idea that data, encrypted and secured via a variety of methodologies, is shared between different network members on an almost continuous basis. Sharing this information can, of course, bring significant benefits to the organizations in question, but also the raise the specter of control issues and data security concerns. While these are not necessarily new concerns or issues for practitioners to have to contend with when sharing information, the speed and tamper resistant nature of this data sharing and analysis can amplify existing issues. Drilling down to a control perspective and issues, this means that CPAs must coordinate with information technology professionals to ensure that the data integrity and management processes in place at different member organizations are both consistent and enforced. This point, the importance of enforcing controls that are on the books in any case, is something of even more importance in a business environment becoming more influenced by blockchain and blockchain based applications.

4. Maintain open communications with customers and clients. While regulation and legislation may be a driving force in this conversation it remains important that clients and customers are aware of the implications of blockchain on shared data and information. As networks, be they private or consortium in nature, continue to include customers and clients, the sharing and distribution of this information may result in some individuals or institutions being taken aback by the implications of this sharing. Connecting back to an earlier issue that was raised, albeit that was between different organizations, the sharing and distribution of customer and client information may raise issues that need to be addressed. In addition to the obvious control issues that will become evident due to the sharing of data between different customers and clients, there is also the reality that different recipients of this information might not operate with the same level of data integrity or control vigor.

    a. Drilling down, the individuals and teams tasked with the implementation of new technology tools or platforms – such as blockchain – may not fully understand the range of implications of what these tools represent. CPAs, who have experience dealing with confidential client information and are aware of just how valuable this data can be to unethical actors, should be a part of this conversation around how clients are informed and updated on this issue.

5. Training and education must become a core component of the organization. New tools, such as blockchain and other emerging technologies, need to become part of what employees are educated about moving forward. From a fiduciary

perspective it is absolutely imperative that, from the top down in an organization, that training and education programs and instituted to ensure that employees are aware of the following two items. First, obtaining and developing a technical understanding of just what blockchain means from an accounting and other financial services point of view is clearly necessary for employees to leverage these tools effectively. Second, and perhaps most important, employees must be able to converse, articulate, and explain the implications of these tools to internal colleagues and external clients.

Trends and Directions Moving Forward

The topics of CG cybersecurity may seem like topics and items that are of strategic concern to management professionals, but traditionally have not been at the center of the accounting conversation and dialogue. As tools such as blockchain, and other distributed ledger platforms continue to become more widespread and integrated into the financial services landscape and profession, these are topics that are becoming linked to the roles and responsibilities of accounting professionals. What this means is that accounting and other financial professionals are going to need to integrate these tools into both the financial reporting and internal control conversation. While it may be tempting to write off controls as something that is not as necessary in an environment with automation and tamper resistant records becoming more commonplace the truth of the matter is more complicated. From an accounting perspective, and no matter which subset of the accounting profession is being analyzed, the implications of increased blockchain integration are clear. Understanding the implications and ramifications of blockchain and blockchain based tools on current accounting procedures, including internal controls, are duties increasingly responsibilities of accounting professionals.

While no analysis of such a fast moving area like blockchain and other emerging technologies can ever be thought of as comprehensive or all inclusive, the points raised within this piece represent logical places to start the conversation. Corporate governance, particularly in light of the growing importance and influence of millennials and Gen-Z investors, is something that organizations are paying increasing amounts of attention, especially as it connects to what firms are doing with customer data. Connecting the bigger picture issue with tangible practices more familiar to accounting practices at large are the issues of cybersecurity and internal control development. Accounting professionals, already familiar with dealing with confidential and identifiable client data, must remain aware of how emerging technologies will change the cybersecurity conversation and landscape. What is evident, regardless of the specifics, is that corporate governance, cybersecurity, and the intersection these topics have with accounting technology are going to change the profession moving forward. Motivated professionals, proactive firms, and proactive financial associations are well positioned to create new business opportunities in these rapidly evolving areas.

References

Alarcon, J. L. “John,” & Ng, C. (2018). Blockchain and the Future of Accounting. *Pennsylvania CPA Journal*, 3–7.

Banham, R. (2017) Digital Disruption creates Opportunities. *Journal of Accountancy*, Vol. 277, Issue 2, pp. 1-3.

Brazina, P. R., & Ugras, Y. J. (2018). Accounting Automation: A Threat to CPAs or an Opportunity? *Pennsylvania CPA Journal*, 3–7.

Butler, T., Al Khalil, F., Ceci, M., & O’Brien, L. (2017). Smart Contracts and Distributed Ledger Technologies in Financial Services: Keeping Lawyers in the Loop. *Banking & Financial Services Policy Report*, *36*(9), 1–11.

Campbell-Verduyn, M., & Goguen, M. (2018). A Digital Revolution Back to the Future: Blockchain Technology and Financial Governance. *Banking & Financial Services Policy Report*, *37*(9), 1–11.

Cong Y, Du, H. and Vasarhelyi, M.A. (2018) Technological disruption in Accounting and Audit. *Journal of Emerging Technologies in Accounting,* Vol. 15, Issue 2, pp. 1-11.

Crosman, P. (2018). Could blockchain tech help prevent bank fraud? *American Banker*, *183*(55), 1.

Damianides, M. (2007) *Sarbanes-Oxley and IT Governance: New Guidance On IT Control And Compliance*, [Online], Available from: <http://www.infosectoday.com/SOX/Damianides.pdf> [18 Dec 2006].

Herian, R. (2018). Regulating Disruption: Blockchain, Gdpr, and Questions of Data Sovereignty. *Journal of Internet Law*, *22*(2), 1–16.

Kanach, J. P., Cross, A. P., & Moynihan, M. C. (2017). As Fintech Platforms Grow Up, Investment Management Firms Face the “Problems of Tomorrow.” *Investment Lawyer*, *24*(3), 17–35.

Landefeld, S., Mejia, L., Handy, A., & Hinnen, T. (2017). “Is That a Target on Your Back?”: Board Cybersecurity Oversight Duty After the Target Settlement. *CGAdvisor*, *26*(6), 1–9.

Lai, K. (2018). Singapore banks using DLT to tackle money laundering. *International Financial Law Review*, 1.

Lemieux, V. L. (2017). Blockchain Recordkeeping: A Swot Analysis. *Information Management Journal*, *51*(6), 20–27.

Nallengara, L., Alsop, R., & Halbhuber, H. (2018). SEC Adopts Interpretive Guidance on Cybersecurity Disclosures. *Computer & Internet Lawyer*, *35*(10), 18–25.

Pratt, K.C. and Storrar, A.C. (1997) UK shareholders' lost access to management information. *Accounting and Business Research*, Vol. 27 Issue 3, pp. 205-18.

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

Pablo Mayo Cerqueiro. (2018). Blockchain could help SRD II compliance – Broadridge. *Global Investor*, N.PAG.

Walch, A. (2016). Call Blockchain Developers What They Are: Fiduciaries. *American Banker*, *181*(153), 1.

Tashea, J. (2018). What do AI, blockchain and GDPR mean for cybersecurity? *American Bar Association Journal*, *104*(12), N.PAG.

Zachariadis, M., Hileman, G., and Scott, S. V. (2019) Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in the financial services. *Information and Organizations*, Vol. 29, pp. 105-117.