Online Early — Preprint of Accepted Manuscript

This is a PDF file of a manuscript that has been accepted for publication in an American Accounting Association journal. It is the final version that was uploaded and approved by the author(s). While the paper has been through the usual rigorous peer review process for AAA journals, it has not been copyedited, nor have the graphics and tables been modified for final publication. Also note that the paper may refer to online Appendices and/or Supplements that are not yet available. The manuscript will undergo copyediting, typesetting and review of page proofs before it is published in its final form, therefore the published version will look different from this version and may also have some differences in content.

We have posted this preliminary version of the manuscript as a service to our members and subscribers in the interest of making the information available for distribution and citation as quickly as possible following acceptance.

The DOI for this manuscript and the correct format for citing the paper are given at the top of the online (html) abstract.

Once the final published version of this paper is posted online, it will replace this preliminary version at the specified DOI.
### Abstract:

As companies begin to explore and develop technology solutions based on blockchain and smart contracts, there is a need to understand the impact of blockchain and smart contracts on the assessment of internal controls and enterprise risk. Especially, since the distributed ledger and smart contracts blur the system boundaries between trading partners, there is a need to understand whether internal control assessments based on a single company approach is adequate in an integrated and collaborative environment. We provide an overview of smart contracts for practitioners and describe the associated risks of engaging in a blockchain consortium. We also list potential questions related to internal controls that may be considered when either engaging in a consortium or executing a smart contract. We then discuss whether current frameworks, specifically the Committee of Sponsoring Organization (COSO) integrated and COSO Enterprise Risk Management (ERM) frameworks, adequately address a collaborative supply chain ecosystem.
Evaluating Blockchain Using COSO

Nishani Edirisinghe Vincent
Assistant Professor of Accounting
The University of Tennessee at Chattanooga
615 McCallie Avenue
Chattanooga, TN 37403
Phone: (813) 368-7103
Email: surani-vincent@utc.edu

Reza Barkhi
KPMG Professor, Accounting & Information Systems
Virginia Tech
3090 Pamplin, 880 West Campus Drive
Blacksburg, VA 24061
Phone: (540) 231-9640
Email: reza@vt.edu
Evaluating Blockchain Using COSO

SUMMARY

As companies begin to explore and develop technology solutions based on blockchain and smart contracts, there is a need to understand the impact of blockchain and smart contracts on the assessment of internal controls and enterprise risk. Especially, since the distributed ledger and smart contracts blur the system boundaries between trading partners, there is a need to understand whether internal control assessments based on a single company approach is adequate in an integrated and collaborative environment. In this paper, we provide an overview of smart contracts for practitioners and describe the associated risks of engaging in a blockchain consortium. We also list potential questions related to internal controls that may be considered when either engaging in a consortium or executing a smart contract. We then discuss whether current frameworks, specifically the Committee of Sponsoring Organization (COSO) integrated and COSO Enterprise Risk Management (ERM) frameworks, adequately address a collaborative supply chain ecosystem.

Keywords: Blockchain; COSO integrated framework; COSO ERM; Blockchain Internal controls; internal controls

I. INTRODUCTION

Technology design, development, implementation, operations, maintenance, and risk assessment, to date, consider one company and its relationship to other parties that transact with the company such as customers and vendors. Therefore, when assessing the internal controls of a firm and its information systems using an established framework, management and auditors can focus on a system boundary that is fairly aligned with the company boundary. Even though Electronic Data Interchange (EDI) and vendor managed inventory systems have enabled the integration of systems within a supply chain, these technologies enable companies to adequately identify the system boundary.

Blockchain technology and smart contracts, on the other hand, feature not only integration but also process automation throughout the supply chain. Smart contracts initiated on blockchain technology can automate processes among trading partners (Dai and Vasarhelyi
2017). For example, once a smart contract is initiated, the payment will be automatically withdrawn and held in escrow until the goods are shipped. Once the smart contract receives data about the shipment of goods the payment will be released to the seller without the customer having to approve, record, and initiate the payment. The transparency created through the use of a distributed ledger (a common record available to all blockchain participants) and smart contracts eliminates the need for reconciliations between trading partners. Consequently, the use of automated rules that reduce the need for explicit authorization, and the distributed ledger that eliminates the need for reconciliations, blur a company’s system boundary. Further, when adding transactions to the distributed ledger a company has to rely on nodes owned/operated by separate parties for recording and processing transactions, which further blurs a company’s system boundary. Therefore, all parties involved in a smart contract need good internal controls not only around their internal information systems but also around the whole blockchain ecosystem/consortium.

Hence, this new approach to record-keeping that combines a shared distributed ledger with process automation introduces several challenges to the current approach to corporate governance and internal control assessment. The primary challenge to corporate governance and internal control assessment introduced by blockchain technology is the shift in the focus from a single company to collaborative commerce (Stein Smith and Castonguay 2020). Therefore, when assessing the risks of blockchain technology and smart contracts, one should consider multiple party interactions and take a broader and holistic view of all trading parties. The contract terms in smart contracts are enforced by automating the processes between contracting parties; the processes enforcing contract terms can be initiated by a company other than the company assessing the internal controls. Hence, risk and control assessment should consider the entire
ecosystem of companies and other parties interacting through smart contracts and blockchain (PwC 2019). Further, the automated enforcement of contract terms blurs the system boundary because there is no verification of transactions entering a company’s information system. Therefore, before the technology is widely adopted, management, auditors, and regulators should address issues such as internal vs external controls for blockchain (PwC 2019), how blockchain technology will disrupt the existing governance requirements, and how the enhanced transparency can potentially equalize power structures within the governance of the company and the supply chains. The use of a distributed ledger system introduces additional challenges such as who should provide governance over the distributed ledger, what risk factors should be disclosed, who (which company) should disclose the risk factors, what internal controls should be established over the blockchain, and who should be responsible for enforcing these controls (Stein Smith and Castonguay, 2020). Consequently, company management, auditors, and risk advisory divisions of audit firms would want to evaluate whether a company can still comply with the Sarbanes-Oxley Act of 2002 (SOX) and continue to use established frameworks in assessing controls and reporting the scope and adequacy of the internal controls in a blockchain environment. Furthermore, standard setters such as the AIPCA would want to consider whether additional areas of focus should be defined for SOC reports specific to blockchain and/or smart contracts.

The existing internal control frameworks are developed with a focus on a single company perspective to assess governance, management, internal controls, and relationships with third parties. The proper maintenance of the blockchain ledger relies on all participants (transacting parties as well as processing nodes) adhering to common governance mechanisms and internal controls. Therefore, it is likely that companies may need to obtain some assurance that shows all
parties to the blockchain are adhering to established common governance mechanisms and internal controls to demonstrate that the distributed blockchain ledger consisting of smart contracts is reliable as an accounting ledger. We evaluate whether additional concerns arise when the boundary of a company is blurred due to the use of blockchain and smart contracts. For this purpose, we examine the blockchain environment using COSO integrated and COSO Enterprise Risk Management (ERM) frameworks and discuss additional issues that should be considered during internal controls and risk assessment of blockchain and smart contracts.

II. BLOCKCHAIN AND SMART CONTRACTS

Traditionally, each company records business transactions in a ledger that is not accessible to others; hence, two transacting companies can document inconsistent or potentially fraudulent records in the individual ledgers. To assure one version of the truth between transacting parties, often a third-party (e.g., bank or an auditor) verifies the transactions for each company involved, manifesting in a centralized trust mechanism. Potentially, blockchain technology can be used to maintain a shared distributed ledger to provide transparency of transactions where each company has its copy of a distributed ledger that is verified and validated by the network. When a transaction is initiated on the blockchain each participant (each node) verifies the appropriateness of the transaction. The distributed trust mechanism (consensus mechanism) makes the transactions tamper-evident because transactions are validated by the nodes on the network before it is added as a new block (a set of shared records) on the blockchain. Which nodes on the network have the authority to add a set of transactions to a block will depend on whether the blockchain is permissioned (private) or permissionless (public). In permissioned blockchains, the nodes on the network are authorized by, and known to, the network. Hence, specific nodes will be explicitly approved to participate in verifying and
validating transactions. In permissionless blockchains, any node is allowed to participate in verifying and validating transactions. There is increased interest in the use of permissioned and permissionless blockchains in auditing, however, the implications, opportunities, and challenges may differ between the type of blockchain used (Liu, Wu, Xu, 2019). We focus on blockchain consortiums that are a semi-private system where the participants are known to the network but use the distributed validation mechanism available in a public blockchain.

Blockchain technology has developed from merely providing a distributed ledger for cryptocurrencies (Peters and Panayi 2016), to offering higher-order functionality such as smart contracts which enable distributed computing supporting other asset classes (Fanning and Centers 2016; Swan 2015). Smart contracts are self-executing computer programs that automate and execute contract terms between trading companies. The idea of smart contracts (Szabo 1997) predates the idea of blockchain, however, the blockchain platform enables the use of smart contracts. Blockchain smart contracts can process complex financial applications (Swan 2015) and other data-intensive and real-time applications. Further, a smart contract can convert legal obligations into automated processes that rely on a distributed trust mechanism, while enhancing transaction security and minimizing transaction costs. Smart contracts can enforce terms of the contract by converting and embedding the contract rules into computer algorithms and automate the process by triggering tasks based on a specified time, an event, or a set of events (e.g., title transferred when payment made, Kiviat 2015; Peters and Panayi 2016; Zheng et al. 2017).

In this paper, we define a ‘smart contract initiator’ as the company that develops and executes the algorithm on the blockchain. Even though all parties to a contract will agree on the terms of the contract, the smart contract initiator will develop the algorithm based on the agreed-upon rules of a legal contract that define the rights and obligations of the transacting parties and
execute it on the blockchain. Consequently, it is likely, that the company with the greatest stake in the blockchain consortium would be responsible for initiating the smart contract as they have the greatest incentive for the contract to “work”. The rules embedded in the contract alleviate the risk of one of the companies not delivering their contract obligations. If they were to cheat other participants, those participants would simply leave and not transact with that party preserving incentives to be fair given the increased transparency. The rules in smart contracts work on an “If-Then-Else” principle to specify how the terms of the contract should be executed (e.g., if the payment is made, then the title is transferred). Smart contracts are most useful when there are complex contracts involving various counterparties. The successful completion of one smart contract can serve as a trigger that starts another smart contract. Therefore, one can view organizations running entirely on smart contracts. This allows organizations to minimize transaction costs and minimize opportunities for fraud and errors by weaving a tapestry of transactions that have been assured by the network.

Various industries are currently exploring use-cases of smart contracts on a blockchain. Blockchain and smart contracts can add value and improve the following five areas in a supply-chain context (Oracle/Deloitte 2018). First, product tracking throughout the supply chain; for example, physical markings of diamonds and gemstones can be stored in a distributed ledger to enable tracking and verification of precious stones throughout the supply chain. Second,

---

1 A smart contract can be executed in a permissioned or a permissionless blockchain. A smart contract initiator would develop the algorithm on the blockchain. Most smart contract capable blockchains currently follow an order-execute architecture where the consensus protocol first, validates, orders the transaction and then propagate the code to other nodes, and second, each node then executes the transaction (hyperledger-fabric). When the algorithm is submitted to a permissioned blockchain, the node responsible for validating the transactions performs the first step, whereas in a permissionless blockchain every node in the network will perform the first step hence validate the transaction. Regardless of permissioned or permissionless blockchain, the execution will be carried out by every node in the network.

2 A group of smart contracts working together to function like an application is a distributed application (DApp), and a group of DApps working together can create a distributed autonomous organization (DAO), which is an autonomous organization that runs completely by smart contracts / DApps.
digitization of supply chain documentation and online auto-verification; digital property records, titles of ownership, and/or encumbrances can be digitized and authenticated, validated, and transferred using blockchain. Third, rules-based monitoring; with the advent of the Internet-of-Things (IoT), automotive equipment manufacturers, parts distributors, dealerships, insurance providers, mechanics, and others could support the ability for equipment within the car to autonomously sense its own needs and communicate these needs to the rightful stakeholder. Fourth, settlement or reverse logistics based on rules-based monitoring; for example, product lifecycle from procurement, reclamation, recycling, and disposal can be seamlessly managed using smart contracts. Fifth, direct peer-to-peer settlement without the use of intermediaries; smart contract and blockchain enables making a payment directly to a vendor without the use of a banking system (e.g. Bitcoin payment). Smart contracts enable a response to real-time events by connecting product components and various stakeholders without any human interaction throughout the supply chain. Next, we discuss challenges in evaluating internal controls based on the components of the COSO integrated, and COSO ERM frameworks.

III. EXISTING FRAMEWORKS: COSO-INTEGRATED FRAMEWORK AND COSO ERM

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) released the internal controls-integrated framework in 1992. Since then, the framework has gained global acceptance as a leading framework for designing, implementing, and assessing internal controls (COSO 2013). Janvrinet al. (2012) recommends incorporating technology in the 1992 framework. Consequently, the updated version in 2013 recognizes the importance and interdependence of technology in companies and emphasizes the need to understand the technological environment when evaluating risks and controls. Landsittle and Rittenberg (2010)
provide a good discussion of the history of COSO, the framework development process, and current and proposed projects. This widespread acceptance of the framework for internal controls over financial reporting assessments can be attributed to the introduction of the Sarbanes-Oxley Act in 2002. COSO defines internal controls as “the process, effected by an entity’s board of directors, management, other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance (COSO 2013).” The framework identifies five components: 1) control environment, 2) risk assessment, 3) control activities, 4) information and communication, and 5) monitoring activities required to achieve the objectives set by the company. According to the framework, to minimize the risk of not achieving an entity’s objectives, each of the five components and the relevant principles should be present, function, and operate together.

In 2017, the COSO board published an updated document titled ‘Enterprise Risk management (ERM)-integrating with strategy and performance’ recognizing the effects of enterprise risk management on strategic planning hence, the company’s growth and performance. The updated framework focuses on five components: 1) governance and culture, 2) strategy and objective setting, 3) performance, 4) review and revision, and 5) information, communication, and reporting. Further, the update introduces 20 key principles within each of the five components creating a link to the internal control framework and eliminating the repetition of key aspects of internal control common to ERM.3

IV. EVALUATION OF BLOCKCHAIN AND SMART CONTRACTS USING FRAMEWORKS

COSO Integrated

3 See Balakrishanan et al. (2019) for a side by side evaluation of COSO internal control-integrated framework and ERM.
Table 1 details the challenges for evaluating internal controls of blockchain using the COSO integrated framework. The most significant challenges reside in the control environment, risk assessment, and control activities. Given the blurred system boundary, increased connectivity, automated contract execution, and the distributed ledger, defining the control environment in a blockchain scenario can be difficult. The autonomous nature of smart contracts can blur the control and ownership of the system. Therefore, understanding the control environment and board involvement can be different from establishing traditional supply chain integrations.

An assessment of controls related to governance should address to what extent the board of a specific company should be involved, and whether they have the authority to oversee certain aspects of the blockchain and smart contracts if the company is not the initiator of smart contracts. Blockchain is expected to increase transparency and eliminate the need for centralized trust between trading parties; however, risk assessment of blockchain and smart contracts to consider whether risks can be adequately assessed and an adequate risk response can be established will pose a major challenge to companies that are not smart contract initiators. In contrast to current technologies such as vendor managed inventory systems, where a company is able to control access, set security protocols, and manage the process, a non-initiator company will have to depend on the development and execution of smart contracts without being able to verify the accuracy and potential biases of the algorithms that automate the process throughout the supply chain eco-system. In a recent survey (NC State and Protiviti 2019), board members indicate acquiring talent in short supply as a top ten risk. According to the survey, technology and innovation risks dominate the top ten risks which suggest concerns related to principles three, four, and five in the
control environment component of the COSO integrated framework and principle five in the governance and culture component of the ERM framework. In a blockchain context, companies will be challenged to acquire the right skillset not only for IT staff but also for accounting, internal audit, and general management with the expertise required to develop proper protocols to manage risks. Therefore, companies will need the most guidance and new expertise in risk assessment and control activities. Companies will need to thoroughly evaluate the adequacy of policies and procedures and also consider whether new policies should be developed in the absence of a centralized trusted source in a transparent environment. See Table 1 for an explanation of challenges and a list of concerns related to each of the principles in the frameworks.

[Insert Table 1 about here]

**COSO ERM Framework**

Table 2 details the COSO ERM framework components and the 20 principles. Given that these are more generic principles applicable to any company, companies may have to evaluate how to expand and apply these principles to a blockchain context. If a company is a mere participant and not the initiator of smart contracts\(^4\), to what extent should the principles related to a company’s governance and culture reflect smart contracts? What are good measures of the board’s oversight of the strategy related to blockchain and smart contracts? Should there be an expert and/or committee on the board of directors? How should the company establish roles and responsibilities of blockchain and smart contracts that span supply chains if the company is not the initiator of a contract? If the company is a mere participant, what are acceptable staffing requirements for the company? The major challenge in the strategy and objective setting

\(^4\) We define a participant in a smart contract as a firm that is impacted by the conditions defined on the smart contract but is not responsible for the development or the execution of the contract.
component is identifying and analyzing the risks and the impact of risks on a company’s business strategy if the company is not the initiator of a contract. If risks are set by the smart contract initiator or an alliance of companies, what would be the impact of risk on the company’s risk appetite? The imposed risk on a company will also affect other principles related to risks such as evaluating alternative strategies, and various risk levels.

Currently, smart contract developers are considering whether transaction data should be submitted to the blockchain similar to bitcoin transactions. Submitting transaction data can have serious confidentiality issues. Therefore, others suggest submitting a hash of the transaction (Vincent et al., 2020). Conceptually, having a distributed ledger assumes increased access to data. However, whether a company will have access to the data to evaluate concerns suggested in the review and revision component will depend on whether transaction data is submitted to the blockchain instead of merely the hash of a transaction. Consequently, companies will have to consider additional issues suggested in Table 2.

[Insert Table 2 about here]

Information, communication, and reporting component concerns related to identifying and establishing performance metrics, and obtaining access to the data might pose a challenge for companies if they are mere participants in a blockchain coalition. Further, once the barrier to obtaining the data is overcome, the company will have to identify how to use the data, who should be held responsible for monitoring and responding to the performance issues, and what communication channels should be established and how to establish these channels. Once all of the above challenges have been addressed, companies will have to consider the reporting requirements of data pertaining to smart contracts, who is the audience, what aspects to be
reported, how to obtain the transaction data from smart contracts, and how to maintain security, privacy and confidentially of such reports.

V. DISCUSSION AND CONCLUSION

Blockchain technology and smart contracts can improve transparency and information sharing, hence facilitate a single version of the truth. Despite this, internal controls assessment for a particular company can be challenging because the company may be just a participant and may not have any influence over how the technology and smart contracts are implemented. Consequently, most companies will have to accept the single source of truth without having any assurance of whether there are any preventive, detective, and corrective controls for creating, updating, and processing of transactions. Hence, a critical question that requires further exploration is whether existing frameworks designed to approach risk and controls from a single company perspective is appropriate in a blockchain and smart contract environment that spans multiple companies.

There are several areas of concern for the accounting and assurance profession that deserves further exploration and discussion. First, we should consider whether the governance of blockchain should be addressed in addition to the governance of the company. Who would be responsible for the governance and management of blockchain should be clearly defined and addressed holistically rather than at a participating company level. Lee and Green (2015) suggest taking a systems thinking approach (taking a holistic view) to ERM. Using this approach, one potential solution is for the blockchain coalition to hire auditors that provide assurance that spans the boundaries of any single company. Second, we should consider whether COSO integrated and ERM framework, as is, can be applied to the blockchain at an industry or blockchain consortium level, and if not how should the framework be modified to fit an industry coalition.
Third, regulators should consider the best way to perform and share audit and assurance services of blockchain. For example, should a blockchain coalition perform a SOC audit of controls and share the information with the participating companies? Before recommending a SOC audit for a blockchain coalition, regulators will have to consider whether a competitor would want to provide an inside look at their controls, identify proprietary information using a SOC report, and if providing a SOC report for the coalition members is adequate? These considerations could potentially help standard-setters and regulators to provide authoritative guidance.
References

Arnold, V., Benford, T. S., Hampton, C., and Sutton, S. G. (2012). Enterprise risk management as a strategic governance mechanism in B2B-enabled transnational supply chains. *Journal of Information Systems*, 26(1), 51-76.

Arnold, V., Benford, T. S., Hampton, C., and Sutton, S. G. (2014). Enterprise risk management: Re-conceptualizing the role of risk and trust on information sharing in transnational alliances. *Journal of Information Systems*, 28(2), 257.

Balakrishnan, R., Matsumura, E. M., and Ramamoorti, S. (2019). Finding common ground: COSO's control frameworks and the levers of control. *Journal of Management Accounting Research*, 31(1), 63-83.

Braumann, E. C. (2018). Analyzing the role of risk awareness in enterprise risk management. *Journal of Management Accounting Research*, 30(2), 241.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). Internal control-integrated framework. Retrieved from https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise risk management: Integrating with strategy and performance. Retrieved from https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

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

Deloitte. (2018). Breaking blockchain open. Deloitte’s 2018 global blockchain survey. Retrieved on December 04, 2018, from https://www2.deloitte.com/us/en/pages/consulting/articles/innovation-blockchain-survey.html.

Fanning, K., and D.P. Centers. (2016). Blockchain and Its Coming Impact on Financial Services. *Journal of Corporate Accounting & Finance*, 27(5), 53–57.

Janvrin, D. J., Payne, E. A., Byrnes, P., Schneider, G. P., & Curtis, M. B. (2012). The updated COSO internal control-integrated framework: Recommendations and opportunities for future research. Journal of Information Systems, 26(2), 189-213.

Kiviat, T.I. (2015). Beyond Bitcoin: Issues in Regulating Blockchain Transactions. *Duke Law Journal* 65, 269.

Landsittel, D. L., & Rittenberg, L. E. (2010). COSO: Working with the academic community. *Accounting Horizons*, 24(3), 455-469.

Lee, L. S., and Green, E. (2015). Systems thinking and its implications in enterprise risk management. *Journal of Information Systems*, 29(2), 195.
Liu, M., Wu, K., and Xu, J.J. (2019). How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain, *Current Issues in Auditing*, 13(2), A19-A29.

NC State and Protiviti. (2019). Executive perspectives on top risks 2020. Key issues being discussed in the board room and C-suite. Retrieved on February 19, 2020, from https://erm.ncsu.edu/az/erm/i/chan/library/2020-erm-execs-top-risks-report.pdf

Oracle/Deloitte. (2018). Enhancing supply chains with the transparency and security of distributed ledger technology. Retrieved from https://www2.deloitte.com/us/en/pages/technology/articles/deloitte-oracle-value-driven-supply-chain-by-blockchain-iot.html

Peters, G.W., and E. Panayi. (2016). Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. *Banking Beyond Banks and Money New Economic Windows*, 239–78, 2016. https://arxiv.org/pdf/1511.05740.pdf.

PwC. (2018). Blockchain is here. What’s your next move? Retrieved on December 04, 2018, from https://www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.html.

PwC. (2019). Re-inventing internal controls in the digital age. Retrieved on February 19th, 2020, from https://www.pwc.com/sg/en/publications/assets/reinventing-internal-controls-in-the-digital-age-201904.pdf

Sheldon, M.D., (2019). A Primer of Information Technology General Control Considerations on a Private and Permissioned Blockchain Audit, *Current Issues in Auditing*, 13(1), A15-A29.

Stein Smith, S., and J. Castonguay. (2019). Blockchain and accounting governance: Emerging issues and considerations for accounting and assurance professionals. *Journal of Emerging Technologies in Accounting In-Press*. https://doi.org/10.2308/jeta-19-01-22-2

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday* 2(9).

Swan, M. (2015). *Blockchain: A Blueprint for a New Economy*. O’Reilly & Associates, 2015.

Vincent, N., Skjellum, A., and S. Medury. (2020). Blockchain architecture: A design that helps CPA firms leverage the technology. *Working Paper*.

Zheng, Z., Xie, s., Dai, H., Chen, X., and H. Wang. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, 557–64.
Table 1: Evaluation of Blockchain Use Case for Supply Chain Integration with COSO Integrated Framework

| COSO – Integrated Framework Principles | Challenges |
|---------------------------------------|------------|
| 1. The organization demonstrates a commitment to integrity and ethical values. | In a blockchain environment, the biggest challenge would be to identify the information system boundary. |
| 2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. | Sheldon (2019) explains the need for general controls around a blockchain consortium as governance becomes more complex. Therefore, companies will have to address the following related to blockchain and smart contracts. |
| 3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | How do we evaluate smart controls built into smart contracts if we are not the contract initiating company? |
| 4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | To what extent will staffing needs change as a result of blockchain and smart contracts? |

- Given the blurring boundaries, whose integrity and ethical values should be evaluated here?
- If the company is a participant in a smart contract, but not the initiator, should we evaluate the integrity of the initiating company? If not, why?
- To what extent should the board of directors be involved?
- Should the board collaborate with other participating companies’ boards of directors?
- If the board of directors comprises of senior executives of companies belonging to the blockchain coalition, how do you assess independence?
- How do we evaluate smart controls built into smart contracts if we are not the contract initiating company?
- What is the extent of board oversight over smart contracts?
- Can the board of directors collaborate with the board of directors of other companies?
- What is a good reporting structure between boards of directors of various companies?
- Will the extent to which oversight is needed differ based on permissioned vs permissionless blockchain?
- To what extent will staffing needs change as a result of blockchain and smart contracts?
- If a company is a participant what skills would be required?
- Given the novelty of blockchain, what competencies are required?
| Risk Assessment                                                                 | Control Activities                                                                 |
|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| 5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | 10. Selects and develops control activities  

**If smart contracts eliminate the need for human involvement, how do we assess accountability, responsibilities, and authorization levels?**

**What are the objectives related to blockchain and smart contracts (faithful representation, information sharing, the integrity of data, etc.)?**

**Can objectives be identified with sufficient clarity?**

**What is the extent of the risk analysis given that smart contracts can be written to include external environmental changes?**

**Also, if the company is not the initiator of smart contracts, the need to assess risk responses build into smart contracts may be a major challenge.**

**Given the interconnectivity, fraud scenarios will need to be expanded to include other companies as well. Therefore, how do we identify fraud scenarios that would be embedded in smart contracts and manipulation of smart contract trigger events?**

**What impact will blockchain have on the existing system of internal controls?**

**One challenge would be to determine how to embed controls into the smart contract.**

**Sheldon (2019) mentions six areas of concern namely source code, consensus protocol, communication protocol, smart contracts, Dapps, and oracles. Consequently, control activities should be defined for all these six areas. Since smart contracts act on a given set of conditions, it would be challenging to identify and assess whether all possible scenarios have been embedded into a smart contract.**

**Who should be responsible for determining the adequacy of built-in controls?**

**What criteria should determine the best set of controls applicable to a given smart contract?**

**Is there generalizability?**
| 11. Selects and develops general controls over technology | • What impact will smart contracts and blockchain have on the existing general controls over technology? The company will need to reevaluate the adequacy of general controls and establish compensating controls if the company is not an initiator of smart contracts.  
• Companies will have to determine whether a permissioned vs permissionless blockchain would require different control mechanisms. |
|---|---|
| 12. Deploys through policies and procedures | • What impact will smart contracts and blockchain have on the existing policies and procedures? |
| 13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control. | • Since smart contracts may depend on inputs from external sources, how do we determine the integrity and quality of such data?  
• If the company is a participant in a public permissionless blockchain, how do we determine the integrity and quality of the input data? |
| 14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. | • Companies will need to assess the adequacy of existing communication channels and extend these channels to include smart contracts. |
| 15. The organization communicates with external parties regarding matters affecting the functioning of internal control. | • Companies will have to evaluate the impact blockchain and smart contracts will have on existing communications with external parties.  
• If a company is not an initiator, the company will need to consider how it will establish the adequate functioning of internal controls. |
| 16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. | • How do we monitor whether smart controls built into a smart contract are present and functioning? |
| 17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. | • Who should be responsible for monitoring if the company is not the initiator of smart contracts? Companies will have to consider whether the evaluation of internal controls should be done at the coalition level using, for example, a service organization controls report. |
### Table 2: Evaluation of Blockchain Use Case for Supply Chain Integration with COSO ERM Framework

| COSO ERM Framework Principles | Challenges |
|-------------------------------|------------|
| **Governance and Culture**    |            |
| 1. Exercises Board Risk Oversight—The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategic and business objectives. | • Braumann (2018) finds risk awareness carries the effects of the organizational environment to risk management effectiveness. Therefore, to what extent should the company’s board of directors provide oversight of blockchain and its alignment to the company’s strategy is an important challenge that should be addressed. |
| 2. Establishes Operating Structures—The organization establishes operating structures in the pursuit of strategy and business objectives. | • Who should be responsible for smart contracts?  
• What is a good practice operating structure for a blockchain coalition?  
• Will these good practices differ based on whether the company participates in a permissioned vs permissionless blockchain?  
• Given the findings from Braumann (2018) that reporting processes affect risk management effectiveness, companies should consider the adequacy and effectiveness of reporting structures with regard to smart contracts. |
| 3. Defines Desired Culture—The organization defines the desired behaviors that characterize the entity’s desired culture. | • How do we establish the desired culture of a blockchain smart contract environment when there are multiple parties involved?  
• Is the need for ‘culture’ for moderating behavior reduced by the transparency and immutability of blockchain? |
| 4. Demonstrates Commitment to Core Values—The organization demonstrates a commitment to the entity’s core values. | • Which company’s core values should be assessed here?  
• If a company is simply a participant, what would be the effect of core values enforced by the blockchain coalition? |
| 5. Attracts, Develops, and Retains Capable Individuals—The organization is committed to building human capital in alignment with the strategy and business objectives. | • What are the staffing needs of the company with regard to blockchain and smart contracts? |
| Strategy and Objective Setting | 6. Analyzes Business Context—The organization considers the potential effects of business context on risk profile. |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
|                               | • If a company is not the initiator of a smart contract how does the company identify and analyze the risks and their impact on business strategy? |
|                               | 7. Defines Risk Appetite—The organization defines risk appetite in the context of creating, preserving, and realizing value. |
|                               | • If risk appetite is set as a collective what is the management’s role in defining risk? |
|                               | 8. Evaluates Alternative Strategies—The organization evaluates alternative strategies and potential impact on risk profile. |
|                               | • If the risk exposure is imposed on a company, what is the benefit of alternative strategies? |
|                               | 9. Formulates Business Objectives—The organization considers risk while establishing the business objectives at various levels that align and support strategy. |
|                               | • Companies involved in a blockchain coalition should consider how each company’s business objectives are aligned with its business strategy and the blockchain coalition’s strategy. |
|                               | • Companies who are not initiators of smart contracts should consider the additional risks arising from participating in smart contracts and evaluate the impact of these risks on their business objectives and strategy. |
|                               | 10. Identifies Risk—The organization identifies the risk that impacts the performance of the strategy and business objectives. |
|                               | 11. Assesses Severity of Risk—The organization assesses the severity of risks. |
|                               | 12. Prioritizes Risks—The organization prioritizes risks as a basis for selecting responses to risks. |
|                               | 13. Implements Risk Responses—The organization identifies and selects risk responses. |
|                               | 14. Develops Portfolio View—The organization develops and evaluates a portfolio view of risk. |
|                               | Using the IT Control Objectives for Sarbanes-Oxley: Using COBIT 5 in the Design and Implementation of Internal Control Over Financial Reporting as the guide risks related to blockchain and smart contracts could be assessed using the following domains: program development and change management, computer operations, and access to programs and data (Sheldon, 2019). |
|                               | • Blockchain and smart contracts may pose difficulties for companies to identify risks. Especially, if contracts are complex and are triggered based on external events, participating companies may not be able to adequately identify all the risks associated with smart contracts and hence may not be able to adequately evaluate the impact on the company’s performance and strategy. |
|                               | • If smart contracts are imposed on a company, not being able to identify the risks adequately will lead to inadequate assessment of the severity of the risks. Consequently, participating companies may not be able to correctly prioritize the risks, select appropriate risk responses, and develop an adequate risk portfolio. |
| Review and Revision | 15. Assesses Substantial Change—The organization identifies and assesses changes that may substantially affect strategy and business objectives. | • Further, companies may have to assess risks at the blockchain level and establish a reporting structure to communicate these risks to the participating companies. |
|---------------------|--------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | 16. Reviews Risk and Performance—The organization reviews entity performance and considers risk. | • Companies may find it challenging to obtain performance data to assess the risks and performance of smart contracts. Consequently, companies may face difficulties in assessing substantial changes that may affect other business processes related to smart contracts. |
|                     | 17. Pursues Improvement in Enterprise Risk Management—The organization pursues improvement of enterprise risk management. | • Arnold et al. (2014) find that a company’s ERM is associated with decreased risk, increased trust, and enhanced information sharing. Given this finding, we can assume that the strength of a smart contract initiator’s ERM will impact the comprehensiveness of the smart contract. Therefore, companies should consider assessing and verifying ERM of the smart contract initiator. |
|                     |                                                                                                                             | • Even if an individual company wants to pursue improvements in ERM, the inability to obtain data about the performance and risks related to the blockchain environment and smart contracts will hinder companies to improve ERM. Arnold et al. (2012) find that strengthening ERM enables trading partner’s absorptive capacity. If a smart contract initiator is not able to monitor performance and review risks with smart contracts and blockchain, it may hinder the absorptive capacity of the trading partners involved. |
|                     |                                                                                                                             | • Contrary to the above argument, since smart contracts automate all possible alternatives, the trading partner may not need to be concerned with the ability to react to external knowledge. |
| Information, Communication, and Reporting | 18. Leverages Information Systems—The organization leverages the entity’s information and technology systems to support enterprise risk management. |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                           | • What performance measures should be established?  
* Does the company have access to performance measures?  
* Who should be responsible for distributing the metrics to individual companies? |
| 19. Communicates Risk Information—The organization uses communication channels to support enterprise risk management. | • What communication channels should be established and how? |
| 20. Reports on Risk, Culture, and Performance—The organization reports on risk, culture, and performance at multiple levels and across the entity. Enterprise Risk Management | • Establishing what should be reported related to blockchain risks, how should it be evaluated and who should be aware and held responsible? |