Communications of the IIMA

Volume 19
Issue 1 *2021*

Article 5

2021

# Evaluation Approach for an Effective Blockchain Implementation in an Accounting Environment

Angel R. Otero
*Florida Institute of Technology*, aotero@fit.edu

Ryan P. Fink
*Florida Institute of Technology*

# Evaluation Approach for an Effective Blockchain Implementation in an Accounting Environment


## ABSTRACT

*Blockchain has the potential to revolutionize accounting transactions in the same way the Internet revolutionized the collection and dissemination of information. Nonetheless, like the Internet, blockchain technology is a double-edged sword offering tremendous benefits but also drawbacks. The literature points to inadequacies in blockchain implementations, particularly when evaluating and selecting controls to help ensure an effective blockchain implementation in organizations. This research develops an approach that not only addresses the inadequacies identified in the literature, but also prompts organizations to a more precise evaluation and selection of controls to achieve effective blockchain implementation. The approach uses Desirability Functions to quantify the desirability of each control after considering its benefits and drawbacks, providing organizations with an objective metric when assessing and selecting controls. Through a case assessment exercise, the approach proved successful in providing accurate evaluation, ranking, and potential selection of controls for organizations to consider when implementing blockchain accounting technology.*



**Keywords**: Blockchain Technology, Accounting, Controls, Evaluation, Security


## INTRODUCTION

Blockchain technology is here to stay and "starting to be taken seriously by numerous industries" (Brewer, 2020, p. 11). Brender and Gauthier (2018) define blockchain as a "distributed transactional database…in which details of transactions (date, place, amount, anonymized participants and their encrypted signatures) are recorded and verified through consensus algorithms" (p. 27). Otero (2018) further calls it a "digital ledger of economic transactions that is fully public and continually updated by countless users" (p. 460). Distributed ledgers use independent computers (referred to as nodes) to record, share, and synchronize transactions in their respective electronic ledgers instead of keeping data centralized as in a traditional ledger.

As its name suggests, blockchain technology stores batches of transaction data in blocks that are continually linked into a growing chain as transactions are added (Gupta, 2020). A block is a grouping of transactions that is tied, or associated with, the block preceding it (Brender & Gauthier, 2018). Each block is time and sequence stamped, providing assurance to all users that the data is original and has not been altered. In the blockchain process, "each completed transaction is encrypted, the involved participants are identified by a string of characters and, after a certain amount of time, the transaction becomes part of the block" (Brender & Gauthier, 2018). This type of technology can be thought of as a "single version of the truth," as it can independently confirm transaction data without the need for verification from other parties (Caron, 2018). Bitcoin, for example, is a popular digital currency that is based on blockchain technology. By eliminating the need for intermediary banking systems or currency exchanges, bitcoins provide a safe and secure method of conducting business with all parties instantly aware of all transactions.

Perhaps the business sector that has most readily embraced blockchain is supply chain management. Blockchain allows businesses to have a transparent supply chain that can be relied on for accuracy (Francisco & Swanson, 2018). Supply chain management immediately benefitted from the transparency and efficiency of a shared ledger system which offers "increased accuracy and trustworthiness of records" and "simplifies back office processes" (Brender, Gauthier, Morin & Salihi, 2019, p. 35). Other industries that have experienced with blockchain include food and agriculture, pharmaceuticals, and aerospace. Food suppliers such as Walmart use blockchain technology to trace the exact sourcing of every product down to the fields where they are grown, and De Beers can ensure responsibly-sourced diamonds by tracking them every step from the mine to the customer (Marr, 2018). Pharmaceuticals is another industry perfectly suited for blockchain adoption as it can frequently trace every bottle of pills from the manufacturer to the patient (White, 2020). Even the aerospace industry's major players are exploring the efficacy of blockchain to ensure the fidelity of their subcontractor supply chains (Young & Desai, 2020).

Gupta (2020) claims that blockchain can revolutionize transactions in the same way the Internet revolutionized the collection and dissemination of information, namely, to allow "increased trust and efficiency in the exchange of almost anything" (p. 1). Much like the Internet, the emerging blockchain technology is a double-edged sword, offering tremendous benefits but also significant drawbacks that must be mitigated and controlled.

## Challenges of Blockchain Technology

Based on the AICPA (2017), blockchain is not a one-size-fits-all solution, and its usefulness varies greatly based on industry and business size. Notwithstanding the advantages of blockchain to industries and organizations presented above, the AICPA (2017) realizes that "blockchain technology is still emerging and has not yet been fully proven at enterprise scale..." (p. 1). Brender et al. (2019) point out various obstacles and challenges when implementing blockchain technology that includes current understanding of blockchain technology; concerns on security, privacy, and transparency of the data; interoperability; and lacking an international set of accepted best practices and standards; among others. Another major challenge for many organizations is the cost of implementation. White (2020) points to larger multinational organizations like Walmart and IBM as having a clear financial advantage when adopting blockchain. In organizations, recurrent challenges related to blockchain implementations, including the ones mentioned above, can be classified into five sections: Interoperability, Scalability, Security and Privacy, Regulation, and Others. These are described in Table 1.

**Table 1. Challenges with Blockchain Technology Implementation.**

| Challenge | Description |
|---|---|
| Interoperability | Interoperability refers to the ability of computer systems to readily connect, integrate, and exchange information with one another. According to Brender et al. (2019), interoperability in information systems, specifically those related to accounting and finance, is a frequent blockchain challenge. KPMG (2018) supports the above by stating that interconnecting blockchain protocols and data formats with organizations' accounting systems represents a significant challenge for organizations which may also create sever implementation roadblocks. |
| Scalability | Brender et al. (2019) defines scalability as "the ability for a system to continue to function well when it changes in size or volume — typically, to a larger size or volume" (p. 38). In a blockchain context, scalability refers to the ability to adapt to usage fluctuations by the |

| | |
|---|---|
| | consumer. Latency is essential in the discussion of scalability and refers to the amount of time that is required to validate a blockchain transaction such as bitcoin, for example (Brender et al., 2019). Transactions involving digital currencies that are secured by cryptography such as, Bitcoin or Ethereum, take much longer than traditional methods of processing payments (Ruoti, Kaiser, Yerukhimovich, Clark & Cunningham, 2019). With blockchain, every transaction gets added to the ledger. Therefore, as usage grows, so must the ledger, resulting in a prolonged processing time. |
| Security and Privacy | Blockchain technology brings new cybersecurity risks like reliability of input information and the system's vulnerability to attacks. While blockchain helps maintain the integrity of information, "it cannot guarantee the reliability of information added in the first place" (Frizzo-Barker, Chow-White, Adams, Mentanko, Ha, & Green, 2019). Additionally, similar to other emerging technologies, blockchain is vulnerable to coordinated and traditional network attacks due to its decentralized nature. In terms of privacy, misconfigured access permissions within blockchain systems result in trust issues for organizations (KPMG, 2018). Moreover, in today's information age, third-party data holders collect, analyze, correlate, and control others' data (Bernabe, Canovas, Hernandez-Ramos, Moreno & Skarmeta, 2019). The above makes these third-party holders in command of blockchain systems and frequently an easy target for hackers. |
| Regulation | The present lack of a regulatory framework, guidelines, standards, and/or best practices to lead blockchain implementations puts organizations at risk (Atlam, Alenezi, Alassafi & Wills, 2018; Brender et al., 2019). Such lack of formality increases the risk of organizations violating regulations and standards directly impacting their financial position and industry reputation (Otero, 2019b; Caron, 2018; Otero, 2015). Brender et al. (2019) further supports that the current lack of sufficient standards and guidance may prevent blockchain systems to function effectively as intended. Without established laws, rules, and regulations, organizations' data may be at risk of being stolen, manipulated, and/or uncompliant with critical regulations (Otero, 2019a). |
| Other Challenges | Additional problems related to blockchain implementations comprise high implementation costs, resources availability to aid in the implementation, and the technology's complexity. Blockchain's required hardware, system customization, and electricity make the technology complicated and very expensive to implement (Morkunas, Paschen, & Boon, 2019; Frizzo-Barker et al., 2019; Batubara, Ubacht, & Janssen, 2018). |

Blockchain technology must be implemented to protect the integrity of organization systems hosting sensitive accounting information. Both Lavion (2018) and Otero (2014) stress that the absence of effective controls triggers opportunities for cyberattacks or corporate fraud to occur. Additionally, business objectives, such as reliability of the entity's financial reporting process, effectiveness and efficiency of operations, and compliance with applicable laws and regulations, are common objectives constantly threatened in organizations. Organizations must thus implement internal controls that can protect the information, mitigate risks preventing a company from achieving its business objectives, and remain in compliance with existing laws and regulations (Lavion, 2018; Deloitte's Risk Advisory, 2018; GTAG, 2009). In the case of blockchain implementations, however, organizations cannot implement all required blockchain technology controls (BC) due to constraints like cost, scheduling, resource availability, etc. Therefore, an effective selection of BC within organizations' constraints becomes a critical management task.

The objective of this research is to develop an approach that will aid organizations in effectively identifying and implementing the right BC to address blockchain risks and challenges and ultimately safeguard organizations' sensitive accounting information. The remainder of this paper is organized as follows: Section 2 provides a summary of the literature reviewed related to blockchain implementation in organizations. Section 3 explains the theory to be used in the development of the proposed approach to assess BC. Section 4 presents a case executing the

proposed BC assessment approach on a real organization, while Section 5 includes discussions and evaluation of results. Section 6 presents conclusions and contributions, and Section 7 ends with limitations and future research.

## LITERATURE REVIEW

Various recent studies have been published about the implementation of blockchain technology in organizations. These studies, summarized below, stress the benefits and challenges experienced from utilizing blockchain as part of the business organization.

### Financial Institutions

According to Moyano and Ross (2017), the "know-your-customer" (KYC) process in financial institutions (FI) is outdated and inefficient but can be improved via blockchain implementation. Traditionally, the KYC process involves numerous documents that are filled out by the FI. The purpose of these documents is to verify that the individual is not a prominent public figure, tied to state-owned enterprises or an international organization, or involved in any prior legal activity.

Each time an individual opens a new bank account, the verification process repeats, and the FI (i.e., bank) is met with costs for each iteration of the process. Moyano and Ross (2017) focused on improving the KYC process through the implementation of blockchain. To do so, the authors posed the following research question: "Can a distributed ledger technology (DLT)-based solution reduce the cost of the KYC process for financial institutions and improve the customer's experience?" (Moyano & Ross, 2017). In examining this question, the researchers identified three criteria the new blockchain system must follow:

1. The documentation cannot be altered.
2. The new process has to be less expensive than the older one.
3. Banks must still be responsible for the KYC process.

In the blockchain KYC approach, Moyano and Ross (2017) state that when an individual becomes a customer at one FI, such as a bank, he/she is given public and private identification codes. The individual can then send/receive verification documentation to/from the bank. These documents are saved in the bank's internal database in order to protect the customer. Once these documents have been checked, the information is moved to the blockchain. From there, the information can be shared with other FI. In this way, the initial process of verification happens once, yet the outcome can be used by all banks that the customer uses thereafter (Moyano & Ross, 2017).

A fault in the blockchain KYC system, per Moyano and Ross (2017), is how to deal with sensitive customer data. This concern is twofold: deletion and storage. With blockchain's immutability, it is difficult, yet not impossible, for data to be deleted. While the authors' study did not take into account data deletion, they argued that future studies need to examine how to delete data if the customer chooses with regard to privacy laws. In the study, customer data is stored locally, which the researchers understood increased the risk. If FI do not have adequate control procedures in place, the researchers warned that customer data could be altered, which would have a ripple effect for transactions within the blockchain thereafter (Fanning & Centers, 2016). It is suggested,

therefore, that a well-controlled blockchain transaction processing system is put in place to provide reliable information within the particular organization setting (O'Leary, 2018). As evidenced above, organizations, including FI, must implement effective controls to protect the integrity and reliability of sensitive customer data within the blockchain.

According to Fanning and Centers (2016), FI use blockchain technology for the "back-office handling of transactions." The authors state that in large financial transactions, negotiations between lawyers are often costly and take up valuable time and resources. By utilizing blockchain, many intermediaries are removed, and FI could save $20 billion or more on an annual basis. Major industry players in the FI industry like Barclays, HSBC, and Royal Bank of Scotland are already utilizing blockchain technology to execute financial transactions (Fanning & Centers, 2016). The authors further stress the need for these FI to implement effective blockchain technology with the right procedures and controls to safeguard the execution and processing of financial transactions.

In a related study, Guo and Liang (2016) explained that blockchain could help improve the poor performance of the FI sector in China. They stated that "blockchain can become the core, underlying technology of the financial sector in the future" by providing "asset digitization and point-to-point value transfer." (p. 5). In essence, blockchain can perform the verification and transfer of data without the need for intermediaries, which may slow down transaction speed. This is so because each transaction is constantly verified by all nodes within the entire network. The authors further highlight the increased security of the technology and acknowledge the current lack of regulation as a challenge between the United States and Chinese governments, both of which have voiced their concerns over the emerging technology and its need for oversight. A successful blockchain technology implementation must include adequate controls, processes, and procedures to account for the challenges just described.

## Foreign Currency Exchange Contracts

Egelund-Müller, Elsman, Henglein, and Ross (2017) performed a study to assess the feasibility of blockchain application on financial contracts, specifically foreign currency exchange contracts (FCEC). The authors hoped to expedite FCEC without the need of an intermediary, and they stated that these contracts could be performed through any distributed ledger, as long as that ledger exhibited the following qualities: 1) The transactions would remain private to the parties, aside from auditors; 2) Contractual parties must be identified; and 3) The ledger has to be able to handle a large transaction volume.

Egelund-Müller et al. (2017) stressed that there is no need for an intermediary for these contracts (aside from an auditor, as stated above). Instead, they believed that the contracts would be processed on the distributed ledger through specific tasks of code, what they named "contract manager" and "contract evaluator" (Egelund-Müller et al., 2017). "A contract manager contains a reference to a contract evaluator, which can be analyzed, audited, and verified in isolation. The contract evaluator provides all functionality related to the contract language and its semantics" (p. 463). The main concern with the application of blockchain in FCEC was the scalability risks that the contracts possess. Egelund-Müller et al. (2017) admitted to this flaw, stating that it would be dangerous to put an entire currency system on one ledger. By putting a currency system on one ledger, the risk is not being mitigated. On the contrary, the risk is being increased: if the distributed

ledger fails, a whole country's financial system could collapse. Once again, the need to have the right controls and procedures in place to ensure a stable blockchain implementation, as well as the reliability and accuracy of the data being exchanged, is clear and evident.

Another study by Bhattacharya, White, and Beloff (2017) stated that "leftover foreign currency" (LFC) can be utilized through the use of blockchain rather than a foreign currency that cannot be used during overseas travel. The authors illustrate that "there are broadly two different categories of P2P currency exchange systems: the first one allows currency exchange without any associated crypto-currencies and the second one uses a virtual crypto-currency system for exchange." (p. 2). The first category, the one that does not use cryptocurrencies, "needs users to transfer money from their bank accounts to the P2P exchange system and then match and exchange directly with a peer requiring currency in the opposite direction" (p. 2). In this way, people can exchange money and decide for themselves what the exchange rate will be. The second category (the one that uses cryptocurrencies) does not use "physical currency exchanges" (p. 2). Instead, these platforms allow users to exchange cryptocurrencies, which can later be exchanged for foreign currencies. Bhattacharya et al. (2017) describe that the main advantage of the peer-to-peer LFC framework is that users can decide to exchange for currencies when the exchange rate is in their favor. However, the authors identified major scalability risks to foreign currency exchange contracts from the proposed blockchain implementation. That is, the risk would increase significantly when implementing an entire legal foreign exchange arrangement system, such as foreign currency exchange contracts, on one distributed digital ledger. If the distributed ledger fails, a whole country's financial system may be significantly impacted and could collapse. The findings above evidenced the significant necessity for organizations to implement the right controls to ensure an effective blockchain technology implementation.

## Used Car Market

Notheisen, Chowela, and Shanmugam (2017) performed a study focused on applying blockchain technology to the used car market in Denmark, particularly the Danish Motor Register (DMR). With the help of the Danish tax authority, the researchers sought to improve the existing system used by the DMR through blockchain technology. The study examined three key topics: how to reduce transaction risk by utilizing blockchain, how to ensure that blockchain works throughout the entire transaction process, and how to guarantee that each transacting party receives information about the product previously unknown to them.

When examining transaction risk, the study highlighted the value of blockchain. For example, there is no need for "centralized governance" with blockchain. By the very nature of the technology, no intermediaries exist between two parties in a transaction – only the blockchain itself. As a result, trust is no longer a critical factor in the transaction process. Additionally, the unalterable nature of information minimizes risk because parties can have confidence that all information will remain unchanged throughout the transaction process. Moreover, smart contracts that can independently verify transactions also help reduce the risk associated with blockchain technology. Finally, all relevant information is disclosed to each party (Notheisen et al., 2017). Despite the highlighted benefits, the researchers also pointed to some drawbacks of the technology.

The creation of blocks means that organizations have to incur significant costs to prevent the dissemination of corrupted information. Also, leaving everything up to algorithms has its pitfalls (Notheisen et al., 2017). According to the authors, without a central authority governing the contracts, users become obedient to the algorithm, which cannot reason as a human can. Added to this, decentralized ledger technology is a new technology that must be met with caution. Even researchers and practitioners do not have a comprehensive understanding of its entire usage (Notheisen et al., 2017). From this, one can conclude that while blockchain can certainly assist the buying and selling used car market industry, controls need to be put in place to protect financial and sensitive transactions going in and out of the blockchain.

Another study applicable to blockchain technology in the used car market industry dealt with the importance of the technology when addressing buyers' needs in the market for lemons. Zavolokina, Miscione, and Schwabe (2019) show that there is a large amount of distrust in the used car market – potential buyers have little faith that sellers are telling the truth about the automobile that they are attempting to sell. To increase trust between buyers and sellers, the authors proposed the use of blockchain technology to verify and validate vehicle information. Rather than rely on the sellers' words alone, Zavolokina et al. (2019) proposed the usage of a mobile phone application that collects historical car data and stores it using blockchain. They further stress how blockchain technology will provide benefits to customers in terms of data processing speed (i.e., no intermediaries) and integrated security. However, the implemented technology used to store and process the data must include the right controls to prevent data from being tampered with, manipulated, and/or stolen.

## Tax Fraud

In their study, Hyvärinen, Risius, and Friis (2017) explained that in many countries, investors can deceive federal governments by applying for fraudulent tax credits. Normally, these tax credits allow individuals to avoid being taxed in the country where the profits were earned, as well as in the country they reside in – which is referred to as double taxation. In Denmark, where the study took place, "there is no central information system dedicated to managing the flow of information between involved parties in order to reliably check an applicant's eligibility for a tax refund" (p. 442). As a result, the researchers proposed blockchain technology to verify tax credit requests.

According to Hyvärinen et al. (2017), blockchain holds the key to preventing double-spending. "Double spending occurs when several transactions are created for the same unit(s) of currency…the double-spending problem arises from a lack of monitoring and information rather than a technical failure; more than one person can apply for the same tax refund on a dividend without being detected" (p. 444). In other words, under the current system, officials are not able to identify when multiple tax refund applications are submitted (i.e., there is no way to track what country the person is from and what dividend they are requesting from).

Hyvärinen et al. (2017) explained that blockchain is a feasible solution to the problem just described. Compared to traditional database systems, blockchain provides a comprehensive solution that can be tailored with relatively little effort by other stakeholders, such as tax authorities, financial institutions, and individual users. Furthermore, it has an immutable log of historical transactions, which "prevents banks from submitting erroneous reports and enables swift

retraction of transactions in order to detect fraudulent applications" (p. 454). The key to preventing this fraud from occurring, per the authors, is the use of tokens that are traceable back to the original dividend and have an "official value backing" (Hyvärinen et al., 2017). The dividend could be located easily by authorities who would then be able to determine the country and company it was from. In the words of Hyvärinen et al. (2017), "tokens are transferred in the blockchain parallel to the cash flow. Thus, the ultimate dividend recipient also receives the respective amount of tokens, which can be redeemed for a tax refund with the tax authorities" (p. 454). To summarize, the amount of dividends is matched with a certain number of tokens. An individual can then apply for a tax refund with these tokens. Thus, the tokens provide traceability. A critical element of this solution is how the tokens are issued.

While this system works well for the Danish tax authority, it would require a major design restructuring and, most importantly, the necessary controls and procedures in order to be applicable to other countries and their respective tax authorities. This is because each country has its own specific tax regulations. Added to this, even when the system is rebuilt in order to accommodate other countries, those other countries must also be willing to implement the necessary controls for the system to function properly. Faccia and Mosteanu (2019) also agree with the aforementioned and further support the need for implementation of the right controls and procedures to address tax evasion and fraudulent tax instances from taking place.

In a similar study, Ainsworth and Shact (2016) stated that current tax collection systems for governments across the globe are not secure and may open doors for fraud to occur. Specifically, the authors stated that centralized ledgers represent single points of failure for an entire system, are prone to corruption, inherently insecure, and are inadequate as a comprehensive compliance mechanism. Moreover, Ainsworth and Shact (2016) stated that a single, jurisdictionally-bound database could never capture all relevant transactional data. The nature of centralized ledgers is to store data from taxpayers within their jurisdiction, and additional measures must need to be implemented to store taxpayer data from other outside jurisdictions.

Based on the above, the authors understand that a distributed ledger system (i.e., blockchain) would correct the taxation system with the right controls and procedures in place. Such distributed system could verify more effectively and efficiently the responsibilities of taxpayers rather than having one single government system verifying that each party has fulfilled their responsibilities (i.e., paid their taxes). In other words, rather than having one Internet system checking to see if each party has fulfilled their responsibilities, there would be a "system of systems" with blockchain technology cross-checking one another.

## Pretty Good Privacy and ProvChain

Other recent cases involving the implementation of blockchain include Pretty Good Privacy (PGP) and ProvChain. Based on Draper, Familrouhani, Cao, Heng, and Han (2019), "PGP is an encryption program which provides the user with privacy as well as authenticity in their data communication through the use of cryptography." (p. 1) PGP has been enhanced using Bitcoin-based blockchain technology (Sharma, 2018). Nonetheless, there have been weaknesses identified that relate to trust.

As it is well known, a Public Key Infrastructure (PKI) provides for a secure connection between two or more parties (Wilson & Ateniese, 2015). Also involved in this secure connection is a third party or certification authority (CA) that is responsible for certifying the authenticity of the public keys' ownership. Because PGP is a decentralized model based on the web of trust, it is at the moment the best protection alternative for PKI. However, as stated by Draper et al. (2019), it does have a few weaknesses, mainly involving trust. For instance, the trust relationships within PGP are based on a subjective system of honor, and therefore, not trustworthy. Also, problems have been identified from being too reliant on the "web of trust" (e.g., certification and endorsement of another user's public keys, etc.). Lastly, issues related to increased overhead in public key maintenance, compatibility with different PGP versions, and authentication are some other limitations identified (Draper et al., 2019).

ProvChain, on the other hand, and according to Draper et al. (2019), refers to "a cloud data storage application which enhances its availability and privacy through the use of blockchain" (p. 1). For ProvChain, specifically, existing blockchain capabilities provide a form of data provenance to enhance both the privacy as well as the availability of its data (Liang, Shetty, Tosh, Kamhoua, Kwiat, & Njilla, 2017; Kelly, 2017). Challenges and problems identified here by Yli-Huumo, Ko, Choi, Park and Smolander (2016) include high costs (from the cost of energy), security being still vulnerable from attacks, lack of regulations to ensure compliance with laws, latency involved when processing these transactions, and size allocated to blockchain nodes to digitally store data.

Based on the above studies, it is evident that blockchain technology requires the implementation of the right controls and procedures to ensure its proper functioning. With this in mind, the proposed evaluation approach will aim at assisting organizations in identifying and implementing only the right BC to address the problems and challenges just presented, resulting in a successful blockchain implementation that will, in turn, safeguard organizations' sensitive financial and accounting data. The proposed approach will use Desirability Functions to quantify the desirability of each BC after considering its benefits and drawbacks, providing organizations an overall measurement for each BC. The derived quality measurement will then be used as the main metric for selecting BC to address the aforementioned problems and challenges and, ultimately, assist organizations in successfully implementing blockchain.

## DESIRABILITY FUNCTIONS

To adequately assess the desirability and significance of BC, organizations must implement an approach that considers all relevant characteristics and attributes of the particular BC. To approach developed in Otero, Sonnenberg, and Delgado-Perez (2020) using Desirability Functions is modified to achieve the above and solve the problem of prioritizing BC in organizations. Desirability Functions provide capabilities to mathematically compute the overall significance of each evaluated BC after considering its relevant characteristics and quality attributes. When using Desirability Functions, a set of significant and relevant attributes is first identified as the criteria used for evaluating BC. These attributes are defined in terms of features, where each feature is either present or not. Once all features have been identified, every BC is assessed against each feature using a binary scale (i.e., 0 or 1). BC that meet the highest number of features will result in a higher desirability or priority for that particular attribute. After all BC are assessed and measurements computed for all features, the proposed approach will fuse all measurements into

one unified value that will represent the overall desirability or relevance of the BC. This unified value considers the priority of each quality attribute (QA) consistent with the organization's specific goals and objectives, resulting in a BC assessment approach based on how well BC meet relevance attributes and how important those attributes are for the organization.

Based on Derringer and Suich (1980) and Montgomery (2008), Desirability Functions have been extensively used in the literature for process optimization in industrial settings, where finding a set of operating conditions that optimize all responses for a particular system is desired. When using Desirability Functions, per Montgomery (2008), each system response $y_i$ is converted into an individual function $d_i$ within the range $0 \leq d_i \leq 1$, where $d_i = 1$ when the objective is met, and $d_i = 0$ when the objective is not met. Upon transforming each response, the levels of each factor are generally selected in order to maximize the overall preference or desirability, which is represented as the geometric mean of all $m$ transformed responses (Derringer & Suich, 1980). Alternatively, when factors are uncontrollable, the overall desirability value can be used to characterize the system based on the multiple selected criteria.

Evaluation of the desirability of each BC in organizations, similar to the characterization of industrial processes, can be addressed by finding a set of criteria that provide the optimal benefit versus cost value for a particular environment. When formulated this way, Desirability Functions can provide a unified measurement that characterizes the quality and relevance of BC based strictly on a set of predefined evaluation criteria. Once the desirability of all BC has been computed, organizations can be in a better position to determine the relative relevance and priority of each of the BC and ultimately select the most desirable ones for the particular environment.

## Development of Evaluation Approach

The proposed evaluation approach requires the identification of all possible BC that could be implemented in the organizational environment. For purposes of this research paper, BC will be obtained from the ISACA's Blockchain Audit Program intended to assist organizations "identify and develop key policies, procedures and controls" suitable to mitigate risks and streamline blockchain processes (ISACA, 2020). The potential BC selected will be presented in the BC vector shown in (3.1).

$$X = \begin{bmatrix} n_1 \\ n_2 \\ \vdots \\ n_n \end{bmatrix} \qquad (3.1)$$

Each BC within the vector can be assessed against a set of relevance or quality attributes $QA_1$, $QA_2$,.., $QA_n$. The assessment process will take place as follows: First, each quality attribute is defined in terms of m features, where $m > 1$. The evaluation scale for each feature is binary, meaning that the feature is evaluated as being either present/true (i.e., 1) or missing/false (i.e., 0). For quality attributes where the presence of features affects blockchain implementation practices negatively (e.g., restrictions, etc.), the reverse is true. With this framework in place, a measurement of the importance of the $j^{th}$ BC based on the $i^{th}$ quality attribute (e.g., regulation) can be computed using (3.2),

$$y_{ij} = \frac{\sum_{x=0}^{m} f_x}{m} \tag{3.2}$$

where $m$ is the number of features identified for the $i^{th}$ quality attribute. This computation normalizes the evaluation criteria to a scale of 0-100, where 0 signifies the lowest score and 100 the highest (backward for restrictions or penalties). The overall assessment of the BC set based on all quality attributes is captured using the quality assessment matrix $Q$ presented in (3.3). As seen, each $y_{ij}$ value in the matrix represents the score of the $j^{th}$ BC based on each individual $i^{th}$ quality attribute. It is important to point out that the quality assessment matrix can be extended to evaluate BC based on any quality attributes containing numerous features.

$$Q = \begin{matrix} QA_1 & QA_2 & \cdots & QA_m \end{matrix} \begin{bmatrix} y_{11} & y_{21} & \cdots & y_{m1} \\ y_{12} & y_{22} & \cdots & y_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ y_{1n} & y_{2n} & \cdots & y_{mn} \end{bmatrix} \tag{3.3}$$

The final step will be to assess the significance of each quality attribute. For this, a weight vector $W$ is created in (3.4) with $r_i$ representing the importance of the $QA_i$ quality attribute using the scale 0-10. A value of 0 represents the lowest importance, while a value of 10, for example, will represent the highest importance.

$$W = \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_m \end{bmatrix} \tag{3.4}$$

After information from vectors $X$, $Q$, and $W$ has been obtained, desirability values for each BC can be generated using the matrix $d$ in (3.5). As seen, each $d_{ij}$ value of the matrix represents the desirability of the $j^{th}$ BC based on each individual $i^{ih}$ quality attribute.

$$d = \begin{bmatrix} d_{11} & d_{21} & \cdots & d_{m1} \\ d_{12} & d_{22} & \cdots & d_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ d_{1n} & d_{2n} & \cdots & d_{mn} \end{bmatrix} \tag{3.5}$$

Each individual desirability value $d_{ij}$ for the BC is computed according to the specific organization's needs, goals, and objectives. For instance, and as stated by Montgomery (2008), quality attributes that are represented positively by a higher $y_{ij}$ value are transformed using the *maximization* function in formula (3.6), while quality attributes represented negatively by a higher $y_{ij}$ value are transformed using the *minimization* function in (3.7), where $L$ and $U$ are the lower and

$$d_{ij} = \begin{cases} 0 & y_{ij} \leq L \\ \left(\frac{y_{ij}-L}{T-L}\right)^{r_i} & L \leq y_{ij} \leq T \\ 1 & y_{ij} > T \end{cases} \tag{3.6}$$

$$d_{ij} = \begin{cases} 1 & y_{ij} < T \\ \left(\frac{U - y_{ij}}{U - T}\right)^{r_i} & T \leq y_{ij} \leq U \\ 0 & y_{ij} > U \end{cases} \quad (3.7)$$

upper limits, respectively, *T* is the target objective (e.g., 100 for maximization, 0 for minimization), and $r_i$ is the desirability weight for the $i^{th}$ quality attribute. It must be noted that (3.6) and (3.7) represent normal equations as defined by the Desirability Function approach. Nonetheless, through experimentation, the BC selection and prioritization approach were found to perform better when $d_{ij} > 0$. Therefore, as heuristic, when $d_{ij}$ is less than .0001, the $d_{ij}$ value is set to .0001. A desirability weight of $r = 1$ results in a linear Desirability Function; however, when $r > 1$, a curvature is exposed by the Desirability Function to emphasize closeness to the target objective (*T*). When $0 < r < 1$, being close to the target objective is less important. Once individual desirability values for each quality attribute are computed, the overall BC desirability value can be computed using (3.8). Each overall desirability value is computed as the geometric mean of all *m* individual desirability values for BC *1, 2, …, n*.

$$D = \begin{bmatrix} (\prod_{i=1}^{m} d_{i1})^{1/m} \\ (\prod_{i=1}^{m} d_{i2})^{1/m} \\ \vdots \\ (\prod_{i=1}^{m} d_{in})^{1/m} \end{bmatrix} \quad (3.8)$$

Following the computation of overall desirability values for all potential BC, the organization can use these values as a measurement for selection derived from the predefined quality attributes and their relative importance for the particular organization environment.

## CASE ASSESSMENT: INSURANCE ORGANIZATION

This section presents the development of the BC assessment approach applied to an insurance organization currently in the process of implementing blockchain technology. The organizational requirement is to identify and implement the most effective BC to help ensure a successful blockchain implementation. The organization, selected based on convenience and availability, is located in the southeast U.S. and offers property and casualty insurance products and services, investments, and insurance policies financing. The target audience involved seventeen personnel with finance, accounting, and information security management backgrounds. Due to their knowledge and experience, the target audience reflects an accurate representation of the population, allowing for results to be consistently applied to other populations with the same characteristics in different settings (Salkind, 2009).

Initial data were collected from the target audience via an online survey questionnaire. The online survey questionnaire was emailed to the target audience and requested them to identify from a well-known, all-inclusive list of BC, those BC they believed were necessary to assist the organization in attaining a successful blockchain implementation. The purpose of identifying these initial BC was to compare them against those eventually selected by the proposed approach and evaluate whether the BC initial selection was adequate and enough to ensure a sound implementation that ultimately protects its sensitive accounting information. The BC listed in the questionnaire were obtained from the internationally-known ISACA's Blockchain Preparation

Audit Program, which provides an all-inclusive list of BC within the categories of Pre-implementation, Governance, Development, Security, Transactions, and Consensus (ISACA, 2020). Refer to Appendix A for an illustration of the online survey questionnaire used. ISACA was sourced for the preparation of the online survey questionnaire because it is an authoritative, globally known organization responsible for the generation of widely used standards, guidance, and best practices within the information system arena. Consistent with Emory and Cooper (1991), the questionnaire's content and validity were pre-tested and edited for semantic and syntactic checking purposes. The questionnaire was assessed by three subject matter experts with 20-30 years of relevant working experience, including management positions in global Big Four accounting and audit firms, as well as in major corporations. The experts have also been involved in numerous consulting engagements providing services to similar size type organizations, including insurance organizations and other industries.

Following the initial collection of questionnaire results (which had a 100% response rate), the target audience was asked to input data evaluating each blockchain control against a set of blockchain-specific relevant quality attributes and features as discussed earlier. The requirement was for the target audience to determine for each blockchain control whether a particular quality attribute or feature was either present/true (i.e., 1) or missing/false (i.e., 0).

The next step required the target audience to agree on specific Desirability Function parameters to measure the importance of each blockchain control based on the quality attribute or feature, normalizing the evaluation criteria to a scale of 0-100, where 0 signifies the lowest score and 100 the highest. Lower and upper boundaries were set to 0 and 100, respectively, and weight was set to $r = 1$ for all quality attributes to indicate equal priority. Finally, different target values were identified for each quality attribute. This means that the threshold for achieving 100% desirability was customized for each quality attribute. For example, quality attributes where $T = 70$ are considered 100% desirable if they exhibit 70% (or more) of the features that define them.

With the input information above, the proposed assessment approach was now ready to generate desirability scores for the organization to evaluate. For purposes of this research, 10 BC were identified from the online survey questionnaire and then assessed based on the quality attributes criteria defined below and applicable to blockchain technology (ISACA, 2020).

1. *Interoperability* – According to KPMG (2018), organizations experience significant roadblocks when interconnecting blockchain protocols and data formats with accounting systems. Interoperability refers to the way in which the blockchain integrates with and understands existing systems (Brender et al., 2019). Effective interoperability, as it applies to blockchain, represents a major problem for several organizations (Brender et al., 2019). BC will ensure that blockchain, once implemented, will integrate effectively and without restrictions or interruptions with the organization's financial and accounting systems already in place, which may include: Enterprise Resource Planning (ERP) systems and (non-ERP) standalone financial systems (FS). Organizations may select BC to address interoperability on either ERP or FS systems depending on their particular needs.
2. *Scalability* – Scalability is defined as the ability for a system to function effectively even when changes in transaction size or volume take place (Brender et al., 2019). Transactions of cryptocurrencies, such as Bitcoin and Ethereum, are good examples here as they take longer

to process compared to traditional methods of processing payments (Ruoti et al., 2019). With blockchain, every transaction is added to the ledger, meaning that as usage grows, so must the ledger, which will further prolong processing time. For purposes of scalability, implementation of BC will ensure that both latency (La) and the size and volume of such transaction (SV) are adequate and controllable for the blockchain system to function properly. Organizations may select BC to address the criteria above depending on their particular needs.

3. *Security and Privacy* – While blockchain helps maintain the accuracy and integrity of information, it cannot guarantee the reliability of the information added (Frizzo-Barker et al., 2019). Implementation of blockchain technology in organizations brings rise to new security risks like the accuracy of input information and vulnerability to attacks due to its decentralized nature. In regard to privacy, KPMG (2018) claims that inadequately configured privacy access permissions within the blockchain may result in significant trust issues. Along the same line, organizations' data managed by third parties also represent a risk as these third parties' systems may be targeted by hackers and put the hosted data at risk (Bernabe et al., 2019). Another privacy-related risk pertains to blockchain data being immutable or un-editable once it has been entered (Bernabe et al., 2019). Implementation of a BC for this quality attribute criteria will promote appropriate levels of security and privacy to ensure the protection of the organization's information. Organizations may implement BC that address the reliability of input information (RI), vulnerability to attacks (VA), configuration of access permissions (AP), security at third party organizations (TP), and user permissions allowed to modify or delete undesired personal information under the appropriate controls and supervision (MoD). Organizations may select BC to address all of the above or just some depending on their specific needs.
4. *Regulation* – Currently, there are no uniform regulatory standards to follow for blockchain implementations in organizations (Atlam et al., 2018). ISACA states that the absence of a regulatory and standard framework "increases the risk of violating regulations and industry standards that could directly impact the participants' financial position, organization, and reputation" (Caron, 2018). When regulations and standard requirements are not in place and, therefore, not carried forward during a blockchain implementation, financial and customer data may be at risk of being stolen, manipulated, and not in compliance with appropriate rules and regulations, leading to numerous legal fees, payments to customers in the form of reimbursements, and expenditures for the purchase and implementation of new security systems. BC that effectively address the three categories above will have a higher priority of selection. Organizations may thus implement BC to ensure financial data is not stolen (DNS), not manipulated (DNM), and it is in compliance with existing rules and regulations (CRR). Organizations may select BC to address all of the above or just some depending on their goals, mission, and objectives.
5. *Other Challenges* – Other challenges include restrictions that organizations must take into account before deciding to implement blockchain. These may include whether the costs involved in the implementation of blockchain technology are high, whether resources with adequate knowledge and expertise are not available, and the complexity or lack of understanding by the organization resulting from such critical implementation. The presence of any of these restrictions will negatively affect this specific quality attribute. That is, BC with all features present will show a low priority and therefore will be less desirable. On the contrary, BC with all restriction features missing will be highly desirable or have a higher priority. A high desirable scenario will be one where the implementation cost of a specific BC

is considered adequate, resources are available and capable to implement the particular implementation, and understanding the particular technology is solid. Other Challenges is then defined as Costs (C), Availability of Resources (AoR), and Understanding (U). Organizations may select BC to address all challenges above or just some depending on particular needs.

## Case Results

Using the binary input data collected evaluating each BC against blockchain-specific relevant quality attributes (Table 2) and the agreed-upon Desirability Functions parameters (Table 3), results were generated from executing the Desirability Functions and documented in Table 4.

**Table 2. Binary Input Assessment.**

| BC | QA1: Interoperability | | QA2: Scalability | | QA3: Security and Privacy | | | | | QA4: Regulation | | | QA5: Other Challenges | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ERP | FS | La | SV | RI | VA | AP | TP | MoD | DNS | DNM | CRR | C | AoR | U |
| 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |
| 2 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| 3 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| 4 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |
| 5 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| 6 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 7 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| 8 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 9 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 10 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**Table 3. Agreed Desirability Parameters.**

| BC | QA1: Interoperability | QA2: Scalability | QA3: Security and Privacy | QA4: Regulation | QA5: Other Challenges |
|---|---|---|---|---|---|
| L | 0 | 0 | 0 | 0 | 0 |
| U | 100 | 100 | 100 | 100 | 100 |
| T | 70 | 70 | 100 | 70 | 100 |
| *r* | 1 | 1 | 1 | 1 | 1 |

**Table 4. Desirability Function Results.**

| BC | QA1: Interoperability | | QA2: Scalability | | QA3: Security and Privacy | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | ERP | FS | La | SV | RI | VA | AP | TP | MoD |
| 1 | 1.0000 | | 0.0014 | | 1.0000 | | | | |
| 2 | 1.0000 | | 1.0000 | | 1.0000 | | | | |
| 3 | 1.0000 | | 1.0000 | | 0.0010 | | | | |
| 4 | 1.0000 | | 0.7143 | | 0.3333 | | | | |
| 5 | 1.0000 | | 0.7143 | | 0.3333 | | | | |
| 6 | 1.0000 | | 0.0014 | | 0.0010 | | | | |
| 7 | 1.0000 | | 0.7143 | | 0.6667 | | | | |
| 8 | 0.0001 | | 1.0000 | | 0.6667 | | | | |
| 9 | 1.0000 | | 0.7143 | | 0.0010 | | | | |
| 10 | 1.0000 | | 0.0014 | | 0.6667 | | | | |

**Table 4. Desirability Function Results. (Cont'd)**

| BC | QA4: Regulation | | | QA5: Other Challenges | | | Desirability |
|---|---|---|---|---|---|---|---|
| | DNS | DNM | CRR | C | AoR | U | |
| 1 | 0.4762 | | | 0.6667 | | | 27.72% |
| 2 | 0.4762 | | | 0.6667 | | | 82.59% |
| 3 | 0.4762 | | | 0.3333 | | | 23.27% |
| 4 | 0.4762 | | | 1.0000 | | | 69.57% |
| 5 | 0.4762 | | | 0.6667 | | | 65.02% |
| 6 | 1.0000 | | | 0.6667 | | | 9.92% |
| 7 | 0.9524 | | | 0.3333 | | | 72.99% |
| 8 | 0.9524 | | | 0.3333 | | | 16.63% |
| 9 | 0.4762 | | | 0.3333 | | | 52.00% |
| 10 | 0.9524 | | | 0.6667 | | | 29.08% |

## DISCUSSION AND EVALUATION OF CASE RESULTS

As shown, the proposed approach based on Desirability Functions presents a detailed, more accurate evaluation and prioritization of BC based specifically on the organization's criteria, goals, and objectives. In evaluating case results, senior management and three subject matter experts (SME) agreed that BC with scores of 50% and higher would represent the most desirable for the organization and thus selected for implementation. This means that BC 2, 4, 5, 7, and 9 were the ones to be selected as listed in Table 4. It must be noted that the proposed BC evaluation and ranking approach shown in the research is unique for the specific insurance organization and, therefore, dependent on the particular scenario at hand. In this case assessment, results are based on the Desirability Functions parameters agreed and configured in Table 3. However, if changed to reflect a higher priority on different quality attributes, the results would vary from the ones presented in Table 4. Moreover, different applications of the approach can contain numerous features, which make it fully customizable for practical applications.

The three SME identified earlier were contacted and requested to perform an evaluation of the case assessment results. According to the literature, having a panel of experts to perform this type of evaluation and validation is very common (Huang, Hung, Yen, Chang, & Jiang, 2011; Dhillon & Torkzadeh, 2006; Emory & Cooper, 1991). The criteria used for selecting the SME included significant working experience in the finance, accounting, and IT domains. The SME, each with 20-30 years of experience, have held management positions in organizations within the private industry, including global Big Four accounting firms. The SME have also been involved in numerous consulting engagements providing related services to similar size type and industry organizations throughout the southeast U.S. and internationally. The SME agreed to perform the requested BC assessment via interview meetings and/or phone calls. Involvement of SME with the required professional experience and competence added value to this research, specifically when interpreting, evaluating, and validating case results.

In terms of evaluation, the SME were requested to compare the BC initially selected by the target audience with the BC selected by the proposed approach, and determine based on their evaluation, whether:

- the set of BC that were initially selected by the target audience were adequate and enough by themselves to aid the insurance organization in effectively implementing blockchain and ultimately safeguarding its sensitive accounting data;
- the BC selected by the proposed approach were the only ones needed to help the insurance organization implement an effective blockchain system that adequately safeguards accounting data; or
- a combination of both the initially-selected BC and the BC identified by the proposed approach would be the most effective in ensuring a successful blockchain implementation that protects the organization's sensitive accounting information.

Table 5 shows the BC initially selected by the target audience and those identified for selection by the proposed approach with a Desirability Function score of 50% or higher. Moreover, Table 5 identifies differences resulting from instances where BC were selected initially by the target audience, but not by the proposed approach, and vice versa, were BC were selected by the proposed approach, but were not initially chosen by the target audience.

**Table 5. BC Results Comparison.**

| Initially Selection | | Proposed Approach Score and Evaluation | | Difference Noted between Initially Selected BC and BC Selected per Proposed Approach |
|---|---|---|---|---|
| BC Number | BC Initially Selected by Target Audience | BC Desirability Score | Selected Per Proposed Approach (is score above 50%)? | |
| 1 | The enterprise has a process for managing blockchain technology vendors. | 27.72 | No | **X** |
| 2 | The enterprise has created and maintains a blockchain technology business case assessment. | 82.59 | Yes | |
| 3 | The enterprise has a test strategy/test plan for the blockchain solution. | 23.27 | No | **X** |
| 4 | The enterprise has a plan for deploying the blockchain solution. | 69.57 | Yes | |
| 5 | The enterprise has a blockchain change-management program that operates effectively. | 65.02 | Yes | |
| 6 | The enterprise has implemented a process for managing loss or theft of private keys. | 9.92 | No | **X** |
| 7 | A process is in place to manage blockchain network vulnerabilities. | 72.99 | Yes | |
| 8 | A process exists to manage endpoint security for devices using the blockchain solution. | 16.63 | No | **X** |
| 9 | Senior management supports deployment of blockchain technology and its vendors. | 62.00 | Yes | |
| 10 | The enterprise includes regulatory risk in its risk assessment of blockchain | 29.08 | No | **X** |

| Initially Selection | | Proposed Approach Score and Evaluation | | Difference Noted between Initially Selected BC and BC Selected per Proposed Approach |
|---|---|---|---|---|
| BC Number | BC Initially Selected by Target Audience | BC Desirability Score | Selected Per Proposed Approach (is score above 50%)? | |
| | technology and periodically reviews the assessment to maintain relevance. | | | |

To perform their BC evaluation, the SME were specifically asked to validate if common, literature-based blockchain risks, as provided by ISACA (2020), were addressed by either the initially-selected set of BC, the BC identified by the proposed approach, or by the combination of the two sets of controls in order to safeguard the organization's sensitive accounting information.

Overall, and based on evaluation interviews and phone calls (captured in Appendix A), SME determine that the most effective set of BC to aid the insurance organization in addressing and/or mitigating common, literature-based blockchain risks, as well as protect its accounting information are those selected by the proposed approach. SME further validated that the proposed assessment approach has practical value to organizations when planning and implementing blockchain technology. The added value mainly results from accurately identifying which BC have higher priority and must therefore be implemented to aid the organization attain a solid, well-implemented blockchain technology that adequately safeguards sensitive accounting information.

## CONCLUSION AND CONTRIBUTIONS

The purpose of this research paper was to develop an approach to assist organizations in assessing, quantifying, and ranking the quality of BC based on multiple quality evaluation criteria in order to address blockchain risks and challenges, and ultimately safeguard organizations' sensitive accounting data. The approach, developed using Desirability Functions, generated a unified measurement that represents how well BC met quality attributes and how important the assessed quality attributes were for a specific organization. Through a case evaluation applied on an insurance firm organization, the approach proved successful in measuring the quality and priority of BC to ensure a solid blockchain technology implementation. In addressing the above, specific data were collected from an insurance organization located in the southeast United States. Following the collection of data, an approach was built using Desirability Functions, and results were generated. Development of the proposed approach, as well as the generated assessment scores, were next evaluated by SME. Based on the expert evaluations, the proposed approach favorably assisted the insurance organization in selecting the right controls and implementing a sound blockchain system that effectively protects sensitive data.

The research presented herein develops an innovative approach for evaluating the quality of BC in organizations based on multiple-attribute assessment criteria. As seen, the proposed approach proved to be a feasible technique for organizations when evaluating the quality of BC, ensuring an effective blockchain implementation that adequately safeguards organizations' sensitive financial and accounting information.

Various contributions resulting from the developed assessment approach can be identified. First, the developed approach is flexible enough to extend additional quality attributes that were not originally included in this research. The approach is readily available for implementation using a spreadsheet, thereby promoting its usage in practical scenarios where highly complex methodologies for BC evaluation and selection may be impractical. The proposed approach fuses multiple assessment criteria, attributes, and features that provide a holistic view of the overall quality and significance of each BC. Finally, the developed approach was designed to provide a mechanism to assess the quality of BC in multiple domains. By modifying the parameters of the Desirability Functions, the quality and ranking of a particular BC can be evaluated considering only the quality attributes necessary and specific to the organization.

## LIMITATIONS AND FUTURE RESEARCH

There were few limitations associated with this research. First, due to convenience and availability, the investigation involved a single insurance organization located in the southeast U.S. Further similar studies may be needed at organizations, specifically insurance organizations, from other locations and from different sizes and industry types in order to generalize the findings to a broader scope. Second, the list of blockchain risks used by the subject matter experts to evaluate BC was limited to five risks. Even though the five risks used in this research were strictly based in the literature and are also well known throughout industries and organizations, additional blockchain-specific risks may be included and considered to strengthen the assessment. Third, a total of 10 standard and generic BC were identified for evaluation purposes, and these were obtained from ISACA, a well-known authority in the field. However, organizations may also consider adding other controls and procedures for evaluation that are unique to their specific environments.

In regard to future research opportunities, additional criteria factors like specific organizations' restrictions, goals, and others can be incorporated to extend the scope and coverage and, thus, enhance the current investigation. An additional research opportunity includes combining Desirability Functions with other traditional control assessment methodologies like Analytic Hierarchy Process, Fuzzy Set Theory, etc., into a hybrid approach when evaluating BC. A hybrid approach can certainly strengthen the blockchain control evaluation process implemented in this research. Moreover, results from this research can be examined and compared to BC assessment results from other similar organizations or industries in order to expand the research. Future research opportunities to improve the current investigation involve considering additional risks and controls, consistent with the organization’s unique environment, to customize and enhance the evaluation. Lastly, additional interviews with field experts may identify new quality evaluation criteria sets that can improve the existing investigation and potentially be utilized as industry guidelines, policies, and/or procedures for the organization under evaluation.

## Appendix A. Online Survey Questionnaire

**Target Audience:** Finance, Accounting, and Information Security – Management Personnel

**Instructions:** Please identify with an “X” the blockchain controls that you believe may be necessary to assist the organization attain a sound and successful blockchain implementation that ultimately protects sensitive accounting information. The blockchain controls listed in this Survey

Questionnaire were obtained from the ISACA's Blockchain Preparation Audit Program, which provides an all-inclusive list of blockchain controls in the categories of Pre-implementation, Governance, Development, Security, Transactions, and Consensus (ISACA, 2020).

| Select with an "X" | | ISACA's Blockchain Audit Program Area / Blockchain Control Description |
|---|---|---|
| | | **Pre-implementation** |
| | 1 | The enterprise has created and maintains a blockchain technology business case assessment. |
| | 2 | Senior management supports deployment of blockchain technology. |
| | 3 | A governance framework for blockchain technology has been created and approved. |
| | 4 | A governance framework for blockchain technology has been created and approved. |
| | 5 | Vendors are properly vetted by the enterprise. |
| | | **Governance** |
| | 1 | Management oversight is periodically reviewed to ensure that the governance framework for blockchain is effective. |
| | 2 | The enterprise includes regulatory risk in its risk assessment of blockchain technology and periodically reviews the assessment to maintain relevance. |
| | 3 | The enterprise has a business continuity plan for the blockchain solution. |
| | 4 | The enterprise has a process for managing blockchain technology vendors. |
| | | **Development** |
| | 1 | The enterprise adequately sources blockchain technology developers. |
| | 2 | The enterprise provides adequate blockchain training for existing developers. |
| | 3 | Business requirements for the blockchain solution have been documented and approved by the appropriate person/group within the enterprise. |
| | 4 | The blockchain solution is adequately designed to support business requirements (e.g., platform architecture is consistent with enterprise needs). |
| | 5 | The enterprise has a test strategy/test plan for the blockchain solution. |
| | 6 | Test cases have been appropriately designed and executed. |
| | 7 | The enterprise has a plan for deploying the blockchain solution. |
| | 8 | Features for the blockchain solution have been adequately deployed. |
| | 9 | The enterprise has designed and implemented standard methods and procedures for operational changes. |
| | 10 | The enterprise has a blockchain change-management program that operates effectively. |
| | | **Security** |
| | 1 | Private keys are secured appropriately. |
| | 2 | The enterprise has implemented a process for managing loss or theft of private keys. |
| | 3 | Source code repositories are secure. |
| | 4 | Source code is reviewed for vulnerabilities. |
| | 5 | Vulnerabilities identified during source-code reviews are properly managed in terms of mitigation, action plans and communication to relevant stakeholders. |
| | 6 | A process is in place to manage blockchain network vulnerabilities. |
| | 7 | The process for managing blockchain network vulnerabilities is operationally effective and demonstrable. |
| | 8 | A process exists to manage endpoint security for devices using the blockchain solution. |
| | 9 | The process for managing endpoint security is operationally effective and demonstrable. |
| | | **Transactions** |

| Select with an "X" | | ISACA's Blockchain Audit Program Area / Blockchain Control Description |
|---|---|---|
| | 1 | A process ensures that transactions on a blockchain are immutable and traceable. |
| | 2 | Transactions on a permissioned (i.e., private) blockchain adhere to defined processes. |
| | 3 | Transaction fees are monitored. |
| | 4 | Transaction fees are budgeted appropriately. |
| | | **Consensus** |
| | 1 | The enterprise has developed and implemented consensus functionality on the relevant protocols. |
| | 2 | The enterprise has designed and implemented the necessary infrastructure to support blockchain mining. |
| | 3 | Infrastructure for cloud-based/leased mining is appropriate. |

## Appendix B. BC Evaluation by Subject Matter Experts (SME)

P.I. - Personal Interview
P.C. - Phone Call

| Blockchain Risk | SME # | Method | Is Blockchain Risk addressed in order to safeguard the organization's sensitive accounting information? |
|---|---|---|---|
| Use cases that are impractical and/or misaligned with strategic objectives. | 1, 2, 3 | P.C. | Yes / "The proposed approach generated selection of blockchain control 2, which requires the organization to create and maintain a blockchain technology business case assessment. As a result, we agree that BC 2 is a good control to address this risk and protect the organization's accounting information." |
| Poor implementation or deployment that results in wasted resources and a solution that does not function properly. | 1 | P.C. | No / "FST did not select BC 3, which requires the organization to have a test strategy/test plan to account for the implementation and deployment of the blockchain solution. Implementation of the above BC is crucial to mitigate this risk and protect sensitive and confidential organization information." |
| | 2,3 | P.C. | Yes / "We believe that implementing BC 4 and BC 5 (both identified for selection by the new approach) would be enough to mitigate a poor implementation deployment. Having a plan for deploying the blockchain solution, as well as a blockchain change-management program that operates effectively, are key in addressing this risk and ultimately safeguard the insurance firm's financial accounting data." |
| Gaps in security, including vulnerable source code, weak endpoints and theft/loss of sensitive data. | 1, 2 | P.C. | Yes / "Selected control BC 7 requires the organization to have a process in place to manage blockchain network vulnerabilities. We are certain that selection and implementation of this control would be enough in mitigating the risk and protecting organizational data." |
| | 3 | P.I. | No / "In addition to the BC 7 (selected), both BC 6 and BC 8 (not selected by the proposed approach), dealing with having processes in place for managing the loss or theft of private keys, as well as endpoint security for devices using the blockchain solution, respectively, are critical to fully mitigate this risk and maintain effective protection over the company's financial information." |
| Vendors that cannot scale effectively to support | 1, 2, 3 | P.C., P.I. | Yes / "BC 9 provides for senior management to support the deployment of blockchain technology and its vendors. The above |

| | | | |
|---|---|---|---|
| blockchain at enterprise level. | | | control alone would be sufficient to address the described risk and provide adequate safeguard to accounting data." |
| Substantial impact to customers and regulatory consequences (including fines) when deployment is faulty. | 1 | P.C. | No / "BC 10 relates to how the organization must include regulatory risk in its risk assessment of blockchain technology and periodically reviews the assessment to maintain relevance. This control was not selected from the proposed approach. Selection of BC 10 would significantly strengthen the organization's defense against this particular risk, as well as its sensitive, confidential, and private information." |

## REFERENCES


AICPA (2017). *Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession*. Deloitte Development LLC. Retrieved June 13, 2020, from https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf

Ainsworth, R. T., & Shact, A. (2016). Blockchain (distributed ledger technology) solves VAT fraud. Boston Univ. School of Law, Law and Economics Research Paper, (16-41).

Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2018). Blockchain with internet of things: Benefits, challenges, and future directions. *Modern Education and Computer Science Press*, 6, 40–48.

Batubara, F. R., Ubacht, J., & Janssen, M. (2018). Challenges of blockchain technology adoption for e-government: A systematic literature review. In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age (dg.o '18). Association for Computing Machinery, New York, NY, USA, Article 76, 1–9.

Bhattacharya, R., White, M., & Beloff, N. (2017, July). A blockchain based peer-to-peer framework for exchanging leftover foreign currency. In *2017 Computing Conference* (pp. 1431-1435). IEEE.

Bernabe, J. B., Canovas, J. L., Hernandez, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access*, *7*, 164908–164940.

Brender, N. & Gauthier, M. (2018). Impacts of blockchain on the auditing profession. *ISACA Journal*, *5*, 27–32.

Brender, N., Gauthier, M., Morin, J.-H., & Salihi, A. (2019). The potential impact of blockchain technology on audit practice. *Journal of Strategic Innovation and Sustainability*, *14*(2), 35–59.

Brewer, D. (2020). Blockchain: Love It or Hate It, It's Here. *ISACA Journal*, *2*, 11–12.

Caron, P. (2018). Blockchain: Identifying risk on the road to distributed ledgers. *ISACA Journal*, *5*, 1–6.

Deloitte's Risk Advisory (November 2018). *General IT Controls (GITC) Risk and Impact*. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-general-it-controls-noexp.pdf (Accessed February 2021).

Derringer, G., & Suich, R. (1980). Simultaneous optimization of several response variables. *Journal of Quality Technology*, *12*(1), 214-219.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, *16*(1), 293-314.

Draper, A., Familrouhani, A., Cao, D., Heng, T., & Han, W. (2019). "Security Applications and Challenges in Blockchain," 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2019, pp. 1-4, doi: 10.1109/ICCE.2019.8661914.

Egelund-Müeller, B., Elsman, M., Henglein, F., & Ross, O. (2017). Automated execution of financial contracts on blockchains. *Business and Information Systems Engineering*, *59*(6), 547–467.

Emory, C. W., & Cooper, D. R. (1991). *Business Research Methods*. Irwin, Boston, MA.

Fanning, K., & Centers, D. P. (2016). Blockchain and its coming impact on financial services. Journal of Corporate Accounting and Finance, 27(5), 53-57.

Faccia, A., & Mosteanu, N. R. (2019). Tax evasion information system and blockchain. *Journal of Information Systems and Operations Management*, *13*(1).

Francisco, K., & Swanson, D. (2018). The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency. *Logistics*, *2*(1), 2. doi: 10.3390/logistics2010002

Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2019). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management*, *51*, 102029. doi: 10.1016/j.ijinfomgt.2019.10.014

Global Technology Audit Guide (GTAG) 8: *Auditing Application Controls*. The Institute of Internal Auditors. (2009).

Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation*, *2*(1), 24.

Gupta, M. (2020). *Blockchain for Dummies*. (3rd IBM ed.) Hoboken, NJ: John Wiley and Sons, Inc.

Huang, S. M., Hung, W. H., Yen, D. C., Chang, I., & Jiang, D. (2011). Building the evaluation model of the IT general control for CPAs under enterprise risk management. *Decision Support Systems*, *50*(4), 692-701.

Hyvärinen, H., Risius, M., & Friis, G. (2017). A blockchain-based approach towards overcoming financial fraud in public sector services. *Business and Information Systems Engineering*, *59*(6), 441–456.

ISACA (2020). Blockchain Preparation Audit Program. Retrieved June 10, 2020, from https://www.isaca.org/bookstore/audit-control-and-security-essentials/wapbap

Kelly, E. (2017). "Blockchain: A ledger you can bank on, " available at: http://www.gaaaccounting.com/blockchain-a-ledger-you-can-bank-on/

KPMG. (2018). *Auditing blockchain solutions*. Retrieved from https://assets.kpmg/content/dam/kpmg/in/pdf/2018/10/Auditing_Blockchain_Solutions.pdf

Lavion, D. (2018). *Pulling fraud out of the shadows*. Global Economic Crime and Fraud Survey 2018. PricewaterhouseCoopers LLP, https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/global-economic-fraud-survey.html

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). "ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability," 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), pp. 468-477, May 2017.

Marr, B. (2018). How blockchain will transform the supply chain and logistics industry. Forbes.com. Retrieved from https://www.forbes.com/sites/bernardmarr/2018/03/23/how-blockchain-will-transform-the-supply-chain-and-logistics-industry/#76c137915fec

Montgomery, D. (2008). *Design and analysis of experiments, 7th Edition*. New York, NY: John Wiley and Sons, Inc.

Morkunas, V. J., Paschen, J., & Boon, E. (2019). How blockchain technologies impact your business model. *Business Horizons, 62*(3), 295–306. doi: 10.1016/j.bushor.2019.01.009

Moyano, J. P., & Ross, O. (2017). KYC optimization using distributed ledger technology. *Business and Information Systems Engineering*, *59*(6), 411–423.

O'Leary, D. (2018). Open information enterprise transactions: Business intelligence and wash and spoof transactions in blockchain and social commerce. *Intelligent Systems in Accounting, Finance and Management, 25*(3), 148-158.

Notheisen, B., Chowela, J. B., & Shanmugan, A. P. (2017). Trading real-world assets on blockchain: An application of trust-free transaction systems in the market for lemons. *Business and Information Systems Engineering*, *59*(6), 425–440.

Otero, A. R. (2018). *Information Technology Control and Audit, 5th Edition*. Boca Raton, FL. CRC Press and Auerbach Publications.

Otero, A. R., Sonnenberg, C., & Delgado-Perez, I. (2020). Change Management over Financial Information:A Multi-Criteria Evaluation of System Change Controls Using Desirability Functions. *Communications of the International Information Management Association, 18*(1), 1-26.

Otero, A. R. (2019a). Optimization Methodology for Change Management Controls Using Grey Systems Theory. *International Journal of Business and Applied Social Science, 5*(6), 41-59.

Otero, A. R. (2019b). System Change Controls: A Prioritization Approach Using Analytic Hierarchy Process. *International Journal of Business and Applied Social Science, 5*(8), 34-46. DOI: 10.33642/ijbass.v5n8p4

Otero, A. R. (2015). Impact of IT Auditors' Involvement in Financial Audits. *International Journal of Research in Business and Technology, 6*(3), 841-849. DOI: 10.17722/ijrbt.v6i3.404

Otero, A. R. (2014). *An Information Security Control Assessment Methodology for Organizations*. (Doctoral dissertation). Nova Southeastern University, Fort Lauderdale, FL. Retrieved from NSUWorks, Graduate School of Computer and Information Sciences. (266) https://nsuworks.nova.edu/gscis_etd/266

Ruoti, S., Kaiser, B., Yerukhimovich, A., Clark, J., & Cunningham, R. (2019). Blockchain Technology: What Is It Good for? *ACM Queue, 17*(5). 60.

Salkind, N. J. (2009). *Exploring research* (7th ed.). Upper Saddle River, NJ: Prentice Hall.

Sharma, D. (2018). "PNB fraud: How blockchain can stop future 'Nirav Modis'," available at: https://economictimes.indiatimes.com/wealth/personal-finance-news/can-blockchain-help-prevent-pnb-like-frauds/articleshow/62993770.cms

White, C. (2020). Big pharma could commercialize and save blockchain. *Freightwaves.com.* Retrieved from https://www.freightwaves.com/news/big-pharma-could-commercialize-and-save-blockchain

Wilson, D., & Ateniese, G. (2015). From Pretty Good to Great: Enhancing PGP using Bitcoin and the Blockchain. *Network and System Security, 9408*, 368-375.

Yli-Huumo, J, Ko, D, Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology - A Systematic Review. *PLoS One, 11*(10), E0163477.

Young, L., & Desai, J. (2020). Blockchain's promise for defense agency supply chains. *Boozallen.com*. Retrieved from https://www.boozallen.com/s/insight/blog/blockchain-promise-for-defense-agency-supply-chains.html

Zavolokina, L., Miscione, G., & Schwabe, G. (2019, January). Buyers of lemons: Addressing buyers' needs in the market for lemons with blockchain technology. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.