BLOCKCHAIN SECURITY : ENHANCED CONTROL EVALUATION APPROACH TO PROTECT ORGANIZATIONS' ACCOUNTING INFORMATION

Angel R. Otero

Nathan M. Bisk College of Business,
Florida Institute of Technology, Melbourne, Florida, USA

ABSTRACT

Blockchain technology can revolutionize transaction processing and reimage organizations' traditional business practices. The literature argues that blockchain may also hurt organizations when key controls necessary to guide its implementation are not in place. The literature points to inadequacies in blockchain implementations, particularly related to the effective selection and implementation of blockchain controls in organizations. This research develops an approach that addresses the weaknesses in the literature. Such approach will allow organizations to be more precise in their implementation of controls to achieve successful blockchain implementation. The proposed approach uses fuzzy set theory to prioritize business controls more precisely in organizations. It is argued that fuzzy set theory allows for a more accurate assessment of imprecise criteria than traditional assessment methodologies, and therefore generates more accurate assessments critical for decision-making. Through a case, the developed approach proved successful in providing accurate implementation of controls to protect organizations' accounting information.

KEYWORDS

Internal Controls, accounting, blockchain, Fuzzy Set Theory, assessment

1. INTRODUCTION

Blockchain has the potential to transform transaction processing like how the Internet revolutionized the collection and dissemination of information [1]. The technology stores batches of transaction data in blocks that are continually linked into a growing chain as transactions are added. A block refers to a group of transactions that is associated or attached to the preceding block [2]. Each block is properly identified (i.e., time and sequence stamped) ensuring all involved users that the data is accurate and unmodified. [2] state that 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" (p. 27). [3] supports the above by stating that blockchain technology may be thought of as a "single version of the truth" given that it can independently confirm transaction data without the need for verification from other parties. A good example here is the popular blockchain's digital currency known as Bitcoin, which allows for a safe and secure method of conducting business by eliminating intermediary banking systems or currency exchanges.

Based on [4], blockchain allows business to have a transparent supply chain process that is accurate, complete, and can be relied on. Such transparency, per [5], is key in supply chain management since it offers "increased accuracy and trustworthiness of records" and "simplifies back-office processes" (p. 35). Other business sectors that have benefited from blockchain

technology include food and agriculture, pharmaceuticals, and aerospace. Food and agriculture suppliers, like Walmart, utilize blockchain to track the flow of every product from their origin down to the fields where they are grown [6]. In the pharmaceutical sector, for example, blockchain can trace every bottle of pills from the manufacturer all the way down to the patient [7]. In the aerospace sector, [8] state that mayor sector players are currently exploring the effectiveness of blockchain to make certain the fidelity of their subcontractor supply chains.

1.1. Blockchain Technology: Problems and Challenges

Blockchain technology has great potential to revolutionize industries, from financial institutions and banking to retail, public sector, and healthcare. Nonetheless, it is also argued that blockchain may hurt industries' processes and procedures in a major way. Based on the [9], 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 [9] realizes that "blockchain technology is still emerging and has not yet been fully proven at enterprise scale..." (p. 1). Obstacles to implementing blockchain, per [5], comprise the technology's lack of adequate understanding; concerns on security, privacy, and data transparency; interoperability; and the limited oversight from lacking an international set of accepted and standardized best practices; among others. Another major challenge for many organizations is the cost of implementation. [7] points to larger multinational organizations like Walmart and IBM as having a clear financial advantage when adopting blockchain.

[1] states that, like the Internet, blockchain is a double-edged sword that allows for significant benefits and advantages, but also for pitfalls and challenges that must be identified and addressed. In organizations, recurrent challenges related to blockchain implementations, including the ones mentioned above, can be classified in the five sections presented in Table 1.

Table 1. Challenges with Blockchain Technology Implementation.

Challenge	Description
Interoperability	Interoperability refers to the ability of computer systems (i.e., blockchain) to readily connect, integrate, and exchange information with one another. According to [5], interoperability in accounting and finance information systems is a frequent blockchain challenge. [10] 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	[5] 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 [5]. Transactions involving digital currencies that are secured by cryptography such as, Bitcoin or Ethereum, take much longer than traditional methods of processing payments [11]. 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" [12]. Additionally, like 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 [10]. Moreover, in today's information age, third-party data holders collect, analyze, correlate, and control others' data [13]. 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 guide blockchain implementations puts organizations at risk [14]; [5]). Such lack of formality increases the risk of organizations violating regulations and standards directly impacting their financial position and industry reputation [15], [3], [16]. [5] 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 [17], [18].
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 [19], [12], [20].

Blockchain must be implemented to protect the integrity of organization systems hosting sensitive information (i.e., accounting information). Both [21] and [22] stress that the absence of effective controls opens opportunities for cyberattacks or corporate fraud to occur. 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 an organization [23]. Organizations must 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 [21], [24], [25]. However, organizations cannot implement all required blockchain technology controls (BTC) due to constraints like cost, scheduling, resource availability, etc. Therefore, an effective selection of BTC within organizations' business 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 BTC to address blockchain risks and challenges, and ultimately safeguard organizations' sensitive accounting data. The remainder of this research 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 BTC. Section 4 presents a case executing the new BTC assessment approach on a real organization while Section 5 presents discussions and evaluation of results. Section 6 presents conclusions and contributions and Section 7 ends with limitations and future research. Major contributions from this research include the development of a flexible theory-based approach that addresses risks and challenges from the blockchain literature, as well as promotes usage in practical business environment scenarios.

2. BACKGROUND WORK

The literature reviewed includes published studies in blockchain implementation and describes advantages and challenges to organizations resulting from such implementation.

2.1. Banking Financial Institutions and Transaction Processing

[26] state that a common process in banking financial institutions (BFI) known as the "know-your-customer (KYC) process" is not only outdated, but it is inefficient and can be significantly enhanced with blockchain. Generally, a KYC process involves the completion of several forms and documents by the customer and the BFI. The purpose of this exercise is to substantiate the profile of the customer, particularly, that the customer is not a prominent public figure, is not

associated to state-owned enterprises or an international organization, and not involved in any prior legal activity. The verification above is repeated every time a new customer's bank account is opened, resulting in costs incurred by the BFI per every verification iteration. The study by [26] focused on finding an alternative solution, using blockchain, for cost savings and efficiency purposes, as well as enhancing the KYC process just described.

A fault identified from the authors' solution related to the handling of sensitive customer information. This concern was 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 consider data deletion, they stated that opportunities for future work include the effect and impact that deleting sensitive customer data may have about privacy laws. In their study, customer data was stored locally prompting additional risks to trigger. If the BFI do not have adequate controls in place, customer data may be altered or manipulated, which would have a ripple effect for transactions within the blockchain thereafter [27]. 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 [28]. As evidenced above, organizations, including BFI, must implement effective controls to protect the integrity and reliability of sensitive customer data within the blockchain.

2.2. Foreign Currency Exchange Contracts

[29] performed a study to assess the feasibility of blockchain application on financial foreign exchange contracts, specifically, foreign currency exchange contracts (FCEC). These legal arrangements are commonly used when organizations buy from a foreign supplier and desire to hedge (i.e., offset potential losses or gains) against the risk of an unfavourable foreign exchange rate fluctuation before the payment is due. The above legal arrangements are also used by speculators to attempt to profit from expected changes in exchange rates. The purpose of the study was to identify efficiencies when expediting FCEC, particularly without the need of an intermediary. The authors believed that FCEC should not be executed through intermediaries, but through specific tasks by a blockchain distributed ledger.

Consistent with the findings of [30], the authors identified major scalability risks to FCEC from the proposed blockchain implementation. That is, the risk would increase to dangerous levels when implementing an entire legal foreign exchange arrangement system, such as FCEC, 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.

2.3. Used Car Market

Another reviewed study involved applying blockchain technology in the used car market industry, particularly, in the Denmark's Danish Motor Register (DMR) [31]. With the assistance of the Danish tax authority, the authors attempted to improve the existing DMR system through blockchain. The study focused on examining key topics such as: how blockchain would reduce the risk of executing daily transactions in the used car market industry (e.g., selling used cars, obtaining them through auctions, etc.); how to ensure that blockchain works throughout the entire transaction process; and how to guarantee that each transacting party would receive the information they need accurately and timely.

With blockchain, however, the authors identified that the creation of transaction records or blocks means that organizations must incur significant costs to prevent the dissemination of information.

[31] also stated that trusting entirely on computer algorithms has its pitfalls. Without a central authority governing the contracts and relevant information, users become obedient to the algorithm and do not reason as a human can [32]. Moreover, decentralized ledger technology is a new technology that must be met with caution, and even researchers and practitioners may not have a comprehensive understanding of its entire usage [31]. Controls must therefore be carefully assessed and selected to address the issues identified above, as well as to protect relevant financial transactions and sensitive customer data within the blockchain.

2.4. Tax Fraud

According to [33], investors in many countries are allowed to deceive federal governments by requesting and filing fraudulent tax credits. These tax credits permit taxpayers, especially investors, to avoid paying taxes in the country where they earned their income, as well as in the country where they reside. The aforementioned "tax strategy" is frequently executed to avoid what is usually referred to as "double taxation". [33] stated that, at present, the country of Denmark (where the study took place) does not have a central tax information system "dedicated to managing the flow of information between involved parties to reliably check an applicant's eligibility for a tax refund" (p. 442). With this in mind, the authors proposed the implementation of blockchain technology to assist current systems in verifying those specific tax credit requests.
Blockchain technology can effectively prevent tax evasion and fraudulent tax credit requests from being processed [34]. However, under the current system, Denmark officials are not able to identify when multiple tax credit applications are submitted (i.e., there is no way to track what country the person is from and what dividend or credit request they are applying for). [33] claim that blockchain provides a feasible solution to the problem just described. The blockchain's immutable capability, as it relates to the logging of transactions, prevents stakeholders like tax authorities "from submitting erroneous reports and enables swift retraction of transactions to detect fraudulent applications" (p. 454). [33] stated that while the proposed blockchain system may be a potential solution for the Denmark tax authority problem, it would still require a major design restructuring with the right controls and procedures in place. [34] also agree with the aforementioned and further support the need for implementation of the right controls to address tax evasion and fraudulent tax instances from taking place.

2.5. Pretty Good Privacy and Provchain

Additional literature reviewed includes the implementation of blockchain technology in specific organizations' applications and programs like Pretty Good Privacy (PGP) and ProvChain. Per [35], PGP refers to "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 through the use of bitcoin-based blockchain technology, however, there have been major trust-related weaknesses identified evidencing a clear lack of procedures in place [36]. A Public Key Infrastructure (PKI), as stated by [37], provides for a secure connection between multiple parties. It specifically involves technology for authenticating users, devices, and securing transmissions within the digital world. To add security to these connections, a certification authority (CA) from a 'third party' is responsible for verifying the authenticity of the public key ownership. Because PGP is a decentralized model based on the web of trust, it is at the moment the best protection alternative for PKI. Nonetheless, [35] state that it does have weaknesses that involve trust. As an example, relationships within PGP are not deemed trustworthy since they are based on a subjective system of honor. Additionally, 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.). Finally, issues related to increased overhead in public key maintenance, compatibility with different PGP versions, and authentication are some other

limitations identified [35]. The necessity of selecting and implementing the right controls and procedures to address the issues just noted once again becomes critical.

ProvChain, as defined by [35], refers to "a cloud data storage application which enhances data availability and privacy through the use of blockchain" (p. 1). According to [38] as well as [39], existing blockchain capabilities provide a form of data provenance to enhance data privacy and availability. Nonetheless, [40] have identified challenges and problems in ProvChain that include compromised application security, noncompliance with laws and regulations, latency when processing transactions, and lack of management and control when allocating storage size to blockchain nodes. The aforementioned stresses once more for an effective selection of controls to aid organizations' blockchain technology implementations.

The literature reviewed above clearly evidence the need for organizations to identify and select the right controls to aid and ensure a sound blockchain implementation. Blockchain technology provides organizations many benefits as presented earlier but can also disrupt them in a significant and critical manner. Selection of the right controls to effectively safeguard such a major implementation becomes essential. The literature argues that an approach anchored in Fuzzy Set Theory (FST) is crucial to aid organizations perform a more detailed, less subjective assessment of procedures and activities (i.e., BTC) in order to identify and implement only the right ones. An approach based on FST is expected to assist organizations in implementing accurate BTC that not only address risks and challenges presented earlier, but also ensure a solid implementation that safeguards the organization's sensitive information [41].

3. THEORETICAL BASIS

Based on [42], FST is an uncertainty theory useful in the absence of probabilities and in the presence of subjective assessments. Per [42], the idea of FST is "the extension of the (crisp) membership concept in traditional set theory by providing for a degree with which an element belongs to a set" (p. 8). Such degree is specified by a membership function. The degree of truthfulness of propositions also allows parameters to be represented with simple linguistic terms [41]. The association of linguistic terms with membership functions forms fuzzy sets.

[43] state that fuzzy sets can be defined mathematically by assigning a value to each possible individual in the universe of discourse. Such value or grade refers to the degree to which that individual, entity, etc. is similar or compatible with the concept represented by the fuzzy set. That is, those individuals or entities may belong in the fuzzy set, to a greater or a lesser degree, as indicated by a larger or smaller membership grade [43]. Membership in a fuzzy set is not a matter of affirmation or denial, right or wrong, but rather a matter of a degree [44].

Membership grades (also known as membership functions) map elements from any universal set into real numbers within the range 0 - 1. The resulting number represents the degree of membership of elements to particular fuzzy sets, where values closer to one represent higher degrees of membership. Figures 2 and 3 show examples of trapezoidal and triangular fuzzy sets, respectively. Figure 2 denotes SCOPE by a particular BTC as a function of a rating from one to five. Here, ratings of one and four represent the lower and upper bounds, respectively. Ratings of two and three are the lower and upper modal values, meaning that BTC that protect two and three application systems, for instance, will fully belong to the fuzzy set (and therefore have a higher priority of selection). On the other hand, BTC that do not protect any application (i.e., rating less than one) and those that protect five or more applications, according to Figure 1, will fall outside of this fuzzy set. Similarly, in Figure 2, a triangular fuzzy set denotes RELEVANCE by a particular BTC with a rating from one to 10. A rating of five fully belongs to the fuzzy set; therefore, the degree of membership is 1.0. Ratings of four and six have 0.5 degrees of

membership to the fuzzy set, while ratings less than three and greater than seven are not part of the fuzzy set.

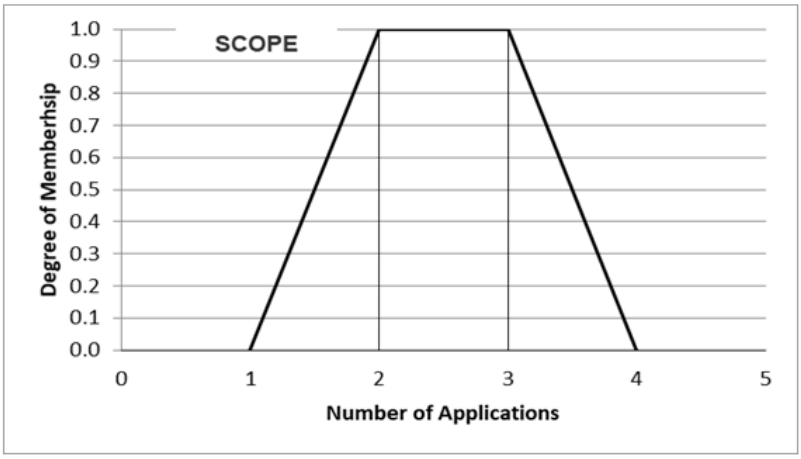

Figure 1. Example of a Trapezoidal Fuzzy Set

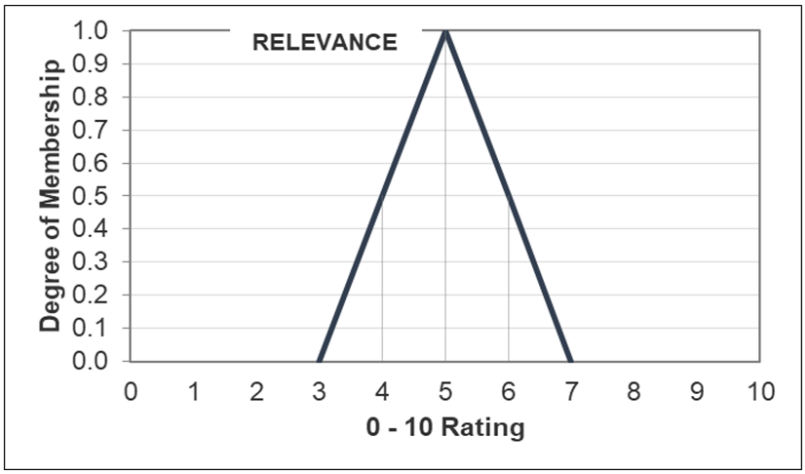

Figure 2. Example of a Triangular Fuzzy Set

As seen, FST provides for various forms of membership functions. [43] state that determining appropriate membership functions is essential for making FST practically useful. Common membership functions used to represent fuzzy numbers include triangular, trapezoidal, and linear shapes. Triangular membership functions are usually preferred due to their combination of solid theoretical basis and simplicity [45]. Nevertheless, there are situations where more complex functions may be required to represent the degrees of membership of elements in fuzzy sets. [43] discuss direct/indirect methods to form fuzzy sets by gathering and processing responses from subject matter experts, or literature reviews.

3.1. Fuzzy Reasoning

Based on [46], fuzzy reasoning refers to the process of developing logical inferences from imprecise premises. A very common inference rule used in classical logic is the *modus ponens*, which states that a conclusion can be inferred provided there is a conditional proposition and a fact. For instance, a classical *modus ponens* inference using the relationship between the value of

a particular BTC, and its level of priority can be expressed as indicated in Table 2. Table 2 shows that if the generated score of BTC_1 is x (Proposition 1), and x implies a 'low priority' BTC as specified by the organization (Proposition 2), then it can be inferred that BTC_1 has a 'low priority' for selection (Conclusion). Notice that this type of inference structure deals with binary-valued propositions. That is, the solution set to describe the priority level of a BTC is {0, 1} when using the classical *modus ponens*.

Table 2. Classical Modus Ponens.

Type of Statement	Statement
Proposition 1	Generated score of BTC_1 = x
Proposition 2	'x' ⇒ A low priority BTC as specified by the organization
Conclusion	BTC_1 = A low priority BTC

The classical *modus ponens* must be customized (i.e., generalized) in order to be used for fuzzy reasoning purposes. Such generalization is obtained as follows: first, the generalized version considers degrees of membership of elements to fuzzy sets. This means that the solution set to describe the priority level of BTC is expanded from {0, 1} to [0, 1]. Second, propositions showing completely true implications via the '=>' symbol are replaced with fuzzy rules. Fuzzy rules are conditional and unqualified propositions implying fuzzy relationships between an antecedent and a consequence [43]. This relationship, also known as a fuzzy implication, is not explicit but rather embedded within the proposition and determined for all values of antecedents and consequences [47]. The third way to generalize the classical *modus ponens* is to use the minimum compositional rule of inference, which provides for a fuzzy conclusion given both, a fuzzy rule and a fuzzy fact, as shown in equation (1).

$$\mu_B(y) = \sup_{x \in X} \min [\mu_A(x), R(x, y)] \quad (1)$$

[43] state that equation (1) obtains degree of membership $\mu_B(y)$ for all $y \in Y$ given a fuzzy implication *R*; as well as degree of membership $\mu_A(x)$ given that *R* is a fuzzy relation on *X* x *Y* and *A* and *B* are fuzzy sets on *X* and *Y*, respectively. With the compositional rule of inference, a fuzzy conclusion can be obtained given both, a fuzzy rule and a fuzzy fact. The generalized *modus ponens* form of inference (shown in Table 3) is considered by many as the foundation for various fuzzy reasoning methods presented in the literature [48].

Table 3. Generalized Modus Ponens.

Type of Statement	Statement
Fuzzy Rule	If *x* is *A*, then *y* is *B*
Fact	$\mu_A(x)$
Fuzzy Conclusion	$\mu_B(y)$

The fuzzy reasoning technique to be used is the Mamdani Max-Min (Mamdani) method, which engages the generalized *modus ponens* just described for each fuzzy rule. To generate output for decision-making, Mamdani provided fuzzy, non-linear conclusions obtained provided both fuzzy rules and fuzzy facts. Mamdani offers organizations advantages when providing for mathematical convenience due to its simplicity and low computational complexity, high degree of accuracy when evaluating imprecision and subjective information, and ease of implementation and testing

[43]. According to [49], another critical advantage of using a rule-based approach such as the Mamdani method is that processing for all received inputs, via fuzzy 'if-then' rules, is strictly human based. This approach can be expressed in simple language words using the logic a human would use to perform the tasks. The Mamdani method is the most common fuzzy inference technique [43], and it is performed in four steps: (1) Fuzzification of the input variables; (2) Evaluation of rules (inference); (3) Aggregation of the rule outputs (composition); and (4) Defuzzification. The Mamdani method follows the multi-conditional reasoning structure illustrated in Table 4.

Table 4. Multi-conditional Reasoning Structure.

Type of Statement	Statement
Rule 1	If x is A_1, then y is B_1
Rule 2	If x is A_2, then y is $B2_2$
…	…
Rule n	If x is A_n, then y is B_n
Fact	$\mu_A(x)$
Conclusion	$\mu_B(y)$

Based on the Mamdani Max-Min method, the fuzzy implication (required by the compositional rule of inference) equals the truth value of the antecedent. In other words, the fuzzy implication for singleton fuzzy rules equals the degree of membership of the only statement in the antecedent [49]. For non singleton fuzzy rules and based on operator 'AND', the fuzzy implication is computed as the intersection or conjunction of the statements in the antecedent via the minimum logical operation shown in equation (2).

$$\mu_{A\cap B}(x) = \min [\mu A(x), \mu B(x)] \quad (2)$$

Equation (2) returns the smallest element where A and B are limited to the range (0, 1). Fuzzy operator 'OR', on the other hand, is known as the fuzzy union or disjunction, returning the maximum elements where again A and B are limited to the range (0, 1). It is denoted by equation (3), where A and B are two given fuzzy sets with memberships functions $\mu A(x)$ and $\mu B(x)$.

$$\mu_{AUB}(x) = \max [\mu A(x), \mu B(x)] \quad (3)$$

An antecedent with a truth value greater than zero automatically implies that its consequence also has a truth value greater than zero. In fuzzy reasoning terms, a true antecedent causes a rule to fire. The fired rules are then combined into a new fuzzy set which will be used to make final inferences. The evaluation criteria for this proposed research study includes common literature-based blockchain risks and challenges, as defined earlier. These criteria include interoperability, scalability, security and privacy, regulation, and other challenges. Fuzzy sets will be created to represent each of the above risks and challenges as the criteria to be used to assess and determine ultimate BTC selection. Each criteria element will have its own set of fuzzy or inference rules defined to assist with the evaluation. Upon the result of truth values from antecedents, fired rules will be aggregated per criteria, and utilized for final BTC selection inference.

3.2. Defuzzification

Defuzzification converts conclusions from fuzzy sets into a real number, or a single crisp value [50]. [43] also define the defuzzification process as the conversion of a fuzzy quantity to a precise quantity, represented by the logical union of two or more fuzzy membership functions defined on the universe of discourse of the output variable. In other words, the purpose of defuzzification is to find one single crisp value that summarizes the fuzzy set. Available defuzzification methods include the center of gravity approach (i.e., centroid), which uses integrals to calculate the area of a combination of fuzzy sets, and the common weighted average method. The centroid method takes the center of gravity (COG) and uses integrals to calculate the area of a combination of fuzzy sets. Equation (4) describes the algebraic expression for this method, where μ_A are the degrees of membership. The calculation of the COG is simplified if a finite universe of discourse and thus a discrete membership function is considered. In equation (5), μ_i is the value of the membership function of the fuzzy set rule *i*, A_i is the corresponding area, and $\alpha_i$is the degree that the rule *i* is fired (between 0 and 1).

$$COG = \frac{\int_a^b \mu_A(x)\, x\, dx}{\int_a^b \mu_A(x)\, dx} \tag{4}$$

$$COG = \frac{\sum_{i=1}^{n} \alpha_i \mu_i}{\sum_{i=1}^{n} \alpha_i A_i} \tag{5}$$

The weighted average method, on the other hand, is reliable, less complicated and time consuming, and also used to approximate the center of gravity [51]. The weighted average defuzzification method, based on peak values for every fuzzy set, calculates weighted sums of the peak values. Based on those weight values and the degree of membership for fuzzy outputs, crisp values of the output are determined using equation (6), where μi is the degree of membership in output singleton *i*, and *Wi* is the fuzzy output weight value for the output singleton *i* [48], [43].

$$Z_0 = \frac{\sum \mu(x)_i \times W_i}{\sum \mu(x)_i} \tag{6}$$

4. CASE: ACCOUNTING FIRM

This section presents the development of the proposed BTC assessment of the BTC approach executed on an accounting firm organization currently in the process of implementing blockchain technology. The accounting firm, situated in the southeast U.S. and selected based on convenience and availability, offers its clients services in the areas of accounting and bookkeeping, wealth management, tax management, audit and advisory, estate trust planning, and computer consulting. The firm's organizational requirement regarding blockchain

implementation is to identify and implement the most effective BTC to help ensure a successful blockchain implementation.

Initial data was collected from the firm's accounting and information technology (IT) management personnel (i.e., target audience) via online survey questionnaire to determine initial degree of need and relevance of BTC. The target audience consisted of seven firm personnel with accounting and IT backgrounds. Due to their knowledge, expertise, and experience, the target audience reflected an accurate representation of the population required to contribute to this research, allowing for results to be consistently applied to other populations with the same characteristics in different settings [52].

The online survey questionnaire was emailed and requested the target audience to identify from a well-known, all-inclusive list of BTC, those BTC they (subjectively) believe may be necessary to assist the firm attain a successful blockchain implementation. The purpose of identifying these initial BTC was to compare them against those eventually selected by the proposed FST approach and evaluate whether the BTC initial selection was adequate or not. The BTC listed in the questionnaire were obtained from the internationally known ISACA's Blockchain Preparation Audit Program, which provides an all-inclusive list of BTC within the categories of Pre-implementation, Governance, Development, Security, Transactions, and Consensus [53]. 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 use standards, guidance, and best practices within the information system arena. Consistent with [54], 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 accounting organizations and other industries. Following collection of questionnaire results (with 100% response rate) and based on the initial degree of need and relevance of the BTC obtained, analyses were performed to rank BTC by fusing their respective assessment values into a single, quantified measure using the Mamdani fuzzy reasoning technique. This provides organizations with a measurement of relevance for each BTC based strictly on organizational objectives and goals. The derived relevance measurement was used as the main metric for evaluating and selecting BTC. The solution approach employs FST to create fuzzy sets of crisp rating levels (i.e., very high (VH), high (H), medium (M), low (L), and very low (VL)) for BTC identified from the questionnaires. The rating levels were defined based on the literature, and supported, validated, and agreed by decision-makers within the organization. Decision makers agreed on a rating scale from one to five (i.e., VL(1), L(2), M(3), H(4), VH(5)), where higher ratings represent a higher criticality of the BTC. This rating scale is commonly used in the industry to describe relevance of controls [55]. Establishment of linguistic terms (e.g., VH, H, L, etc.) then followed to denote the levels of criticality of BTC based on the crisp ratings assigned. Fuzzy sets were created for each linguistic term in order to determine the degrees of membership of crisp evaluation ratings in each fuzzy set. Lastly, fuzzy reasoning was implemented using the Mamdani Max-Min method to develop logical inferences from imprecise premises defined by the fuzzy sets, as well as to evaluate and prioritize each BTC. This detailed evaluation significantly assisted the firm's management decision-making process in implementing only the most effective BTC to aid the implementation and safeguard accounting information.

Results from the BTC evaluation using the proposed FST-based assessment approach are shown in Table 5. Overall, the fuzzy inference system model evaluated a total of 35 BTC against literature-based challenge criteria mentioned earlier that includes: interoperability, scalability, security and privacy, regulation, and other challenges. After the required analyses were

performed consistent with Section 3, fuzzy logic/reasoning was put to work to rank BTC by fusing their respective assessment values into a single, quantified measure using the Mamdani Max-Min fuzzy reasoning technique. The crisp scores computed in Table 5 provide the accounting firm with a precise measurement of relevance for each BTC evaluated. The derived relevance measurement can now be used as the main metric for determining BTC selection.

Table 5. BTC Evaluation Using the Proposed FST-based Approach.

	ISACA's Blockchain Audit Program Area / Blockchain Control Description	**Score**
	Pre-implementation	
1	The enterprise has created and maintains a blockchain technology business case assessment.	93.53
2	Senior management supports deployment of blockchain technology.	92.32
3	A governance framework for blockchain technology has been created and approved.	87.18
4	A governance framework for blockchain technology has been created and approved.	80.14
5	Vendors are properly vetted by the enterprise.	33.53
	Governance	
6	Management oversight is periodically reviewed to ensure that the governance framework for blockchain is effective.	80.67
7	The enterprise includes regulatory risk in its risk assessment of blockchain technology and periodically reviews the assessment to maintain relevance.	98.89
8	The enterprise has a business continuity plan for the blockchain solution.	91.25
9	The enterprise has a process for managing blockchain technology vendors.	90.14
	Development	
10	The enterprise adequately sources blockchain technology developers.	34.93
11	The enterprise provides adequate blockchain training for existing developers.	96.32
12	Business requirements for the blockchain solution have been documented and approved by the appropriate person/group within the enterprise.	96.23
13	The blockchain solution is adequately designed to support business requirements (e.g., platform architecture is consistent with enterprise needs).	33.53
14	The enterprise has a test strategy/test plan for the blockchain solution.	69.36
15	Test cases have been appropriately designed and executed.	33.53
16	The enterprise has a plan for deploying the blockchain solution.	69.36
17	Features for the blockchain solution have been adequately deployed.	97.18
18	The enterprise has designed and implemented standard methods and procedures for operational changes.	90.14
19	The enterprise has a blockchain change-management program that operates effectively.	33.53
	Security	
20	Private keys are secured appropriately.	92.63
21	The enterprise has implemented a process for managing loss or theft of private keys.	38.10
22	Source code repositories are secure.	45.89
23	Source code is reviewed for vulnerabilities.	80.67
24	Vulnerabilities identified during source-code reviews are properly managed in terms of mitigation, action plans and communication to relevant stakeholders.	98.89
25	A process is in place to manage blockchain network vulnerabilities.	91.25
26	The process for managing blockchain network vulnerabilities is operationally effective and demonstrable.	78.56

	ISACA's Blockchain Audit Program Area / Blockchain Control Description	Score
27	A process exists to manage endpoint security for devices using the blockchain solution.	82.77
28	The process for managing endpoint security is operationally effective and demonstrable.	90.14
	Transactions	
29	A process ensures that transactions on a blockchain are immutable and traceable.	96.23
30	Transactions on a permissioned (i.e., private) blockchain adhere to defined processes.	33.53
31	Transaction fees are monitored.	93.36
32	Transaction fees are budgeted appropriately.	33.53
	Consensus	
33	The enterprise has developed and implemented consensus functionality on the relevant protocols.	80.67
34	The enterprise has designed and implemented the necessary infrastructure to support blockchain mining.	98.89
35	Infrastructure for cloud-based/leased mining is appropriate.	91.25

5. DISCUSSION AND EVALUATION OF CASE RESULTS

For purposes of evaluating case results, both senior management and three subject matter experts agreed that BTC with scores of 90 and higher were to be selected consistent with the membership functions previously defined. This means that BTC 1, 2, 7, 8, 9, 11, 12, 17, 18, 20, 24, 25, 28, 29, 31, 34, and 35 were the ones to be selected as listed in Table 5.

The three subject matter experts identified earlier were contacted and requested to perform the evaluation of the case results. According to the literature, having a panel of experts to perform this type of evaluation and validation is very common [56], [55], [54]. The criteria used for selecting the experts included significant working experience in the accounting and IT domains. The subject matter experts, each with 20-30 years of experience, have held management positions in the private industry, including global Big Four accounting firms. The experts have also been involved in numerous consulting engagements providing services to similar size type organizations, including accounting firms, throughout southeast U.S. and internationally. The experts agreed to perform the requested BTC assessment via interview meetings or phone calls. Involvement of experts 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 experts were requested to compare the BTC initially selected by the target audience against the BTC selected by the proposed approach (shown in Table 6), and determine based on their evaluation, whether:

- the set of BTC that were initially by the target audience were adequate (by themselves) to aid the firm in effectively implementing blockchain, and ultimately safeguarding its sensitive accounting data;
- the BTC selected by the proposed FST-based approach were the only ones needed to help the firm implement an effective blockchain systems that adequately safeguard accounting data; and/or
- a combination of the initially selected BTC and the BTC identified by the proposed FST approach would be the most effective in ensuring a successful blockchain implementation that protect the firm's sensitive accounting information.

Table 6 shows the BTC initially selected by the target audience and those identified for selection by the proposed approach. Moreover, Table 6 identifies differences resulting from instances where BTC were selected initially by the target audience but not by the proposed approach, and vice versa where BTC were to be selected based on the proposed approach but were not chosen by the target audience.

Table 6. BTC Selections.

Initially Selected BTC?		ISACA's Blockchain Audit Program Area / Blockchain Control Description	Score	Selected by FST?	Difference Noted
		Pre-implementation			
	1	The enterprise has created and maintains a blockchain technology business case assessment.	93.53	Yes	X
Yes	2	Senior management supports deployment of blockchain technology.	92.32	Yes	
	3	A governance framework for blockchain technology has been created and approved.	87.18	No	
	4	A governance framework for blockchain technology has been created and approved.	80.14	No	
	5	Vendors are properly vetted by the enterprise.	33.53	No	
		Governance			
	6	Management oversight is periodically reviewed to ensure that the governance framework for blockchain is effective.	80.67	No	
	7	The enterprise includes regulatory risk in its risk assessment of blockchain technology and periodically reviews the assessment to maintain relevance.	98.89	Yes	X
	8	The enterprise has a business continuity plan for the blockchain solution.	91.25	Yes	X
Yes	9	The enterprise has a process for managing blockchain technology vendors.	90.14	Yes	
		Development			
	10	The enterprise adequately sources blockchain technology developers.	34.93	No	
	11	The enterprise provides adequate blockchain training for existing developers.	96.32	Yes	X
	12	Business requirements for the blockchain solution have been documented and approved by the appropriate person/group within the enterprise.	96.23	Yes	X
	13	The blockchain solution is adequately designed to support business requirements (e.g., platform architecture is consistent with enterprise needs).	33.53	No	
Yes	14	The enterprise has a test strategy/test plan for the blockchain solution.	69.36	No	X
	15	Test cases have been appropriately designed and executed.	33.53	No	
Yes	16	The enterprise has a plan for deploying the blockchain solution.	69.36	No	X
	17	Features for the blockchain solution have been adequately deployed.	97.18	Yes	X
	18	The enterprise has designed and implemented standard methods and procedures for operational	90.14	Yes	X

Initially Selected BTC?		ISACA's Blockchain Audit Program Area / Blockchain Control Description	Score	Selected by FST?	Difference Noted
		changes.			
Yes	19	The enterprise has a blockchain change-management program that operates effectively.	33.53	No	X
		Security			
	20	Private keys are secured appropriately.	92.63	Yes	X
Yes	21	The enterprise has implemented a process for managing loss or theft of private keys.	38.10	No	X
	22	Source code repositories are secure.	45.89	No	
	23	Source code is reviewed for vulnerabilities.	80.67	No	
	24	Vulnerabilities identified during source-code reviews are properly managed in terms of mitigation, action plans and communication to relevant stakeholders.	98.89	Yes	X
Yes	25	A process is in place to manage blockchain network vulnerabilities.	91.25	Yes	
	26	The process for managing blockchain network vulnerabilities is operationally effective and demonstrable.	78.56	No	
Yes	27	A process exists to manage endpoint security for devices using the blockchain solution.	82.77	No	X
	28	The process for managing endpoint security is operationally effective and demonstrable.	90.14	Yes	X
		Transactions			
	29	A process ensures that transactions on a blockchain are immutable and traceable.	96.23	Yes	X
	30	Transactions on a permissioned (i.e., private) blockchain adhere to defined processes.	33.53	No	
Yes	31	Transaction fees are monitored.	93.36	Yes	
Yes	32	Transaction fees are budgeted appropriately.	33.53	No	X
		Consensus			
	33	The enterprise has developed and implemented consensus functionality on the relevant protocols.	80.67	No	
	34	The enterprise has designed and implemented the necessary infrastructure to support blockchain mining.	98.89	Yes	X
	35	Infrastructure for cloud-based/leased mining is appropriate.	91.25	Yes	X

To perform the BTC evaluation, the experts were specifically asked to validate if common, literature-based blockchain risks, as provided by [53], were addressed by either the initially selected set of BTC, the BTC identified by the proposed FST approach, or by a combination of the two sets of controls. The evaluation prompted the experts to ultimately determine which set of BTC best assists the accounting firm in attaining a sound blockchain implementation that effectively protects its sensitive accounting information.

Overall and based on evaluation interviews and phone calls, the experts determine that the most effective set of BTC to aid in addressing and/or mitigating common, literature-based blockchain risks and challenges are those selected by the proposed FST approach. The experts further validated that the proposed assessment approach has practical value to organizations when

planning and implementing blockchain. The value-added results mainly from accurately identifying which BTC have higher priority and must therefore be implemented to aid organization attain a solid blockchain that adequately safeguards sensitive accounting data.

6. CONCLUSION AND CONTRIBUTIONS

The objective of this research is to develop an approach that will aid organizations in effectively identifying and implementing the right BTC to address blockchain risks and challenges, and ultimately safeguard organizations' sensitive accounting data. Through a case evaluation executed on an accounting firm organization, the approach proved successful in measuring the quality and priority of BTC to ensure a solid blockchain technology implementation. The research conducted herein generated various contributions both theoretical and practical. The main theoretical contribution was the development of an approach, anchored in FST, that addresses common risks and challenges identified in the blockchain literature, and enhances the process of selecting and implementing BTC in organizations. The approach created serves as the foundation for the development of a fuzzy expert system as a solution to the existing BTC evaluation and ranking problem. A BTC assessment approach that is anchored in FST contributes significantly to the literature by utilizing strict mathematical approach to more precisely and rigorously examine vague conceptual phenomena or grey areas. FST also has been used as a problem-solving tool to understand the phenomenon of reality by performing adequate predictions; learning about controlling the phenomenon; and utilizing such capabilities for various other ends. Furthermore, an approach that is based on FST generates detailed and thorough assessment data that are critical in a decision-making process.

Regarding practical contributions, the approach created here is flexible, can be implemented with a software tool, and promote usage in practical scenarios where highly complex methodologies for BTC selection become impractical. It fuses multiple evaluation criteria to provide a holistic view of the overall quality of BTC. Moreover, the approach is easily extended to include other evaluation criteria, as well as provides a mechanism to evaluate the quality of BTC in various domains. A suitable FST-based BTC evaluation approach accounts for imprecise parameters and criteria when calculating the relevance of BTC. Such evaluation is also focused on how well BTC address organization objectives, goals, and restrictions. Overall, results from this research support the FST-based approach to assist organizations in evaluating and determining the most effective BTC to guide their blockchain implementations.

7. LIMITATIONS AND FUTURE RESEARCH

There were few limitations associated with this research. First, due to convenience and availability, the investigation involved a single accounting firm located in the southeast U.S. Further similar studies may be needed at organizations, specifically accounting firms, 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 BTC was limited to five risks. Even though the risks used in this research were based in the literature and also well known throughout industries and organizations, additional blockchain-related risks may be included and considered in order to strengthen the assessment. Third, a total of 35 standard and generic BTC were identified for evaluation purposes, and these were obtained from ISACA, a relevant and well-known authority in the field. However, organizations may also consider adding other controls and procedures for evaluation which are unique to their specific environments.

Future research work opportunities to improve the work herein involve considering additional risks and controls, consistent with the organization's unique environment, to customize and enhance the evaluation. Another opportunity for future research work involves comparing and evaluating the case results herein with results from similar evaluations in related organizations or industries. The purpose of the comparison and evaluation is to identify the best and most effective approach for selecting BTC. Combining the FST approach used in this research with other well-known, traditional assessment approaches (e.g., Analytic Hierarchy Process, Grey Systems Theory, etc.) into a hybrid approach would likely improve the current investigation and enhance existing BTC evaluation processes.

ACKNOWLEDGMENTS

The authors would like to thank the reviewers whose constructive critique greatly improved the quality of the paper.

REFERENCES

[1] Gupta, M. (2020). Blockchain for Dummies. (3rd IBM ed.) Hoboken, NJ: John Wiley & Sons, Inc.
[2] Brender, N. & Gauthier, M. (2018). Impacts of blockchain on the auditing profession. ISACA Journal, 5, 27–32.
[3] Caron, P. (2018). Blockchain: Identifying risk on the road to distributed ledgers. ISACA Journal, 5, 1–6.
[4] 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
[5] 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.
[6] 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
[7] 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
[8] 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
[9] AICPA (2017). Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession. Deloitte Development LLC. Retrieved 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
[10] KPMG. (2018). Auditing blockchain solutions. Retrieved from https://assets.kpmg/content/dam/kpmg/in/pdf/2018/10/Auditing_Blockchain_Solutions.pdf
[11] Ruoti, S., Kaiser, B., Yerukhimovich, A., Clark, J., & Cunningham, R. (2019). Blockchain technology: What is it good for? ACM Queue, 17(5), 60.
[12] 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
[13] Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. IEEE Access, 7, 164908–164940.
[14] 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(1), 40–48.
[15] 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

[16] 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
[17] Otero, A. R., Sonnenberg, C., & Bean, L. (2019). Quality assessment of access security controls over financial information. International Journal of Network Security & Its Applications, 11(6), 1-18. DOI: 10.5121/ijnsa.2019.11601
[18] 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. DOI: 10.33642/ijbass.v5n6p4
[19] 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
[20] 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. DOI: https://doi-org.portal.lib.fit.edu/10.1145/3209281.3209317
[21] 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
[22] 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
[23] Otero, A. R., Ejnioui, A., Otero, C. E., and Tejay, G. (2011). Evaluation of information security controls in organizations by Grey Relational Analysis. International Journal of Dependable and Trustworthy Information Systems, 2(3), 36-54.
[24] 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 2022).
[25] Global Technology Audit Guide (GTAG) 8: Auditing Application Controls. The Institute of Internal Auditors. (2009).
[26] Moyano, J. P., & Ross, O. (2017). KYC optimization using distributed ledger technology. Business and Information Systems Engineering, 59(6), 411–423.
[27] Fanning, K., & Centers, D. P. (2016). Blockchain and its coming impact on financial services. Journal of Corporate Accounting & Finance, 27(5), 53-57.
[28] 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.
[29] Egelund-Müeller, B., Elsman, M., Henglein, F., & Ross, O. (2017). Automated execution of financial contracts on blockchains. Business and IS Engineering, 59(6), 457–467.
[30] 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.
[31] 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.
[32] 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.
[33] 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.
[34] Faccia, A., & Mosteanu, N. R. (2019). Tax evasion information system and blockchain. Journal of Information Systems & Operations Management, 13(1).
[35] 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.

[36] 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
[37] Wilson, D., and Ateniese, G. (2015). From pretty good to great: Enhancing PGP using Bitcoin and the Blockchain. Network and System Security, 9408, 368-375.
[38] 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.
[39] Kelly, E. (2017). "Blockchain: A ledger you can bank on, " available at: http://www.gaaaccounting.com/blockchain-a-ledger-you-can-bank-on/
[40] 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.
[41] Zimmermann, H. -J. (2010). Fuzzy set theory. New York, NY: John Wiley & Sons, Inc.
[42] Schryen, G. (2010). A fuzzy model for IT security investments. In: Proceedings of Sicherheit, Schutz und Zuverlässigkeit, October 5-7, 2010, Berlin.
[43] Klir, G. J. and Yuan, B. (1995). Fuzzy Sets and Fuzzy Logic: Theory and Applications. Upper Saddle River, NJ: Prentice Hall PTR.
[44] Zadeh, L. (1965). Fuzzy sets. Information Control, 8(1), 338-353.
[45] Pedrycz, W. (1994). Why triangular membership functions? Fuzzy Sets & Systems, 64(1), 21-30.
[46] Das, P. (2009). Adaptation of fuzzy reasoning and rule generation for customers' choice in retail FMCG business, Journal of Management Research, 9(1), 15-26.
[47] Demicco, R. V., & Klir, G. J. (2004). Fuzzy logic in geology (1st ed.). Academic Press.
[48] Mizumoto, M., & Zimmermann, H. J. (1982). Comparison of fuzzy reasoning methods. Fuzzy Sets and Systems, 8(3), 253-283.
[49] Petrovic-Lazarevic, S. (2001). Personnel Selection Fuzzy Model. International Transactions in Operational Research, 8(1), 89-105.
[50] Yager, R. R. (1996). Knowledge-based defuzzification. Fuzzy Sets Systems, 80(1), 177-185.
[51] Genske, D. D., & Heinrich, K. (2009). A knowledge-based fuzzy expert system to analyze degraded terrain. Expert Systems with Applications, 36(1), 2459-2472.
[52] Salkind, N. J. (2009). Exploring research (7th ed.). Upper Saddle River, NJ: Prentice Hall.
[53] ISACA (2020). Blockchain Preparation Audit Program. Retrieved from https://www.isaca.org/bookstore/audit-control-and-security-essentials/wapbap
[54] Emory, C. W., & Cooper, D. R. (1991). Business Research Methods. Irwin, Boston, MA.
[55] Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16(1), 293-314.
[56] 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

AUTHORS

.

Angel R. Otero, Ph.D., CPA, CISA, CITP, CICA, CRISC is an Associate Professor of Accounting Information Systems and Academic Chair for Accounting and Finance Online Programs for the Nathan M. Bisk College of Business at the Florida Institute of Technology (FIT). Dr. Otero has over 20 years of experience in the areas of public accounting and auditing, internal control audits, information technology consulting, and information systems auditing. Before joining FIT, Dr. Otero worked at Deloitte & Touche, LLP for over 10 years and attained the position of Senior Manager. His research interests involve the areas of financial audits and internal controls; information systems auditing; accounting information systems; information security audits; and risk assessments. He has published research on the assessment of general information technology controls (GITCs) surrounding financial and accounting systems. Dr. Otero is also author of a published university textbook in the area of information systems auditing.