TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 1109 - 1118

Disrupting Fraud: Auditing In the Digital World – A Block chain Perspective

Moez Mustafa
Research Scholar,
Asia Pacific University of Technology & Innovation, Jalan Teknologi 5
57000 Wilayah Persekutuan Kuala Lumpur, Malaysia.
moezmustafamojo@gmail.com

Geetha A. Rubasundram
Senior Lecturer,
Asia Pacific University of Technology & Innovation, Jalan Teknologi 5
57000 Wilayah Persekutuan Kuala Lumpur, Malaysia.
geetha@apu.edu.my

Article Info
Volume 82
Page Number: 1109 - 1118
Publication Issue:
January-February 2020

Article History
Article Received: *14 March 2019*
Revised: *27 May 2019*
Accepted: *16 October 2019*
Publication: *06 January 2020*

Abstract

The increasing adaption of Blockchain technology internationally has had many implications towards the business environment, including its control environment, controls and the perceived reliability, transparency and integrity of the transactions and system. Although the mechanism for this technology seems strong, with the use of the private keys, protocol consensus, validation protocols, triple entries and Smart Contracts, there are still ways to apparently manipulate the ecosystem, depending on the size, complexity, validation nodes protocol etc. This qualitative research interviewed seven experts to gauge the actual risk environment. The main aim of this research was to assess the changes to the auditing profession and its relevance. Though the changes expected is magnified, the auditing procedures would possibly focus on more predictive and analytical relevance, focusing on related and associated parties and ultimately, trying to opine if a transaction not only falls within the validation protocols, but also ultimately, the legitimacy of the overall process. Audit trails leading to related parties and intentions to deceive would definitely be a priority. Although the strong trails would seem as a deterrent for would be fraudsters, it is expected that audit would still be relevant to pick up the scent. In order to achieve this balance, a hybrid between the traditional audit and information technology (IT) audit is predicted.

Keywords: *Blockchain, Distributed Ledger Technology, Consensus Protocol, Blockchain Auditing.*

I. INTRODUCTION

"Digitalization is the use of digital technologies to change a business model and provide new revenue and value producing opportunities; it is the form of Blockchain, Artificial Intelligence (AI), Big Data, Robotics, Internet of Things (IoT) and IR 4.0. Apart from having significant impacts on the way businesses are run, it will also change the accounting and auditing profession. Just like every other profession, the accounting and auditing profession should be prepared to embrace the changes digitalization brings.

A popular technology is the Blockchain platform with a reputation of being more secure. Blockchain has been classified as one of the primary disruptive innovations and impactful creations (Tan and Low, 2017). Blockchain is predicted to be a game-changer in different sectors

January - February 2020
ISSN: 0193 - 4120 Page No. 1109 - 1118

with the ability to transform modern business models and market structure. Blockchain has already started to show its disruptive influence in various sectors such as financial services, agriculture, commerce, healthcare, transportation and government,

The Blockchain was initially made popular by Bitcoin. Its unique consensus algorithm validates transactions or information on a network in a secure and delicate manner. Also known as Distributed Ledger Technology (DLT), the Blockchain protects and validates transactions across multiple devices connected to a peer to peer network using the algorithms mentioned above.The DLT allows a cryptographic audit trail that is secure and searchable.This key feature proposes that the Blockchain is able to preserve data integrity and provides immediate, real time

information which could facilitate the development of a new accounting and auditing ecosystem, impacting transactions and processes such as the procurement to pay process, record to report, order to cash and others.

In today's accounting practice, one key time consuming task is the validation and reconciliation process especially if there is conflicting information between parties.The Blockchain technology can be integrated within the company's ERP system which will make it convenient to share information from the shared ledger. The use of Smart Contracts within the Blockchain is purported to remove the need for reconciliation with its self-validating feature(Dai and Vasarhelyi, 2017). A Smart Contract is a computer protocol in the Blockchain system that digitally facilitates, verifies, or enforces the negotiation or performance of a contract. It enables the performance of credible transactions without the involvement of third parties. As an example, Smart Contracts facilitates the exchange of money, property, shares, or anything of value in a transparent and conflict-free way while avoiding the services of a middleman such as lawyers.

This wouldimprove and change the audit process as well. The supposedly immutable characteristic of the Blockchain platform implies a reduced risk assessment and at the same time, auditors may not need to focus on transactional sampling errors and subjective judgment since the audit could focus on analytics and exception reporting. Auditors would need to re-focus their attention on other areas such contract fraud etc.

There are two types of Blockchain networks, the public and private network. There has been a noticeable growth of the private Blockchain networks. This would provide a more secure and personalized network for businesses to enhance their operations and protect it from fraud and external threats. Although Blockchain reportedly has the capabilities to prevent fraud, it is pertinent to be cautious still since it is man-made and open to weaknesses and loopholes. As an example, a US based security consulting firm published a report on the stolen Ethereum private keys that had been hacked by "Blockchain Bandit" who managed to collect 45,000ether (ETH) by successfully guessing frail private keys.

This would be a concern for the auditing profession as the assurance provider. Due to its reasonably newer growth, the Private Blockchain would need to be assessed based on its vulnerabilities and security measures. This would require additional knowledge and skillsets, as well as a different approach towards audit for auditors to place reliance on the output of the Blockchain. Auditing standards and guidelines would also need to be enhanced to ensure the integrity of the platform, information and reports.

Therefore, this study is focused on the implications of the Private Blockchain systems in the business-controlled environments, the associated risks (including fraud) and the subsequent impact on the auditing environment.

January - February 2020
ISSN: 0193 - 4120 Page No. 1109 - 1118

II. AUDITING A BLOCKCHAIN: A FRAUD DISRUPTER?

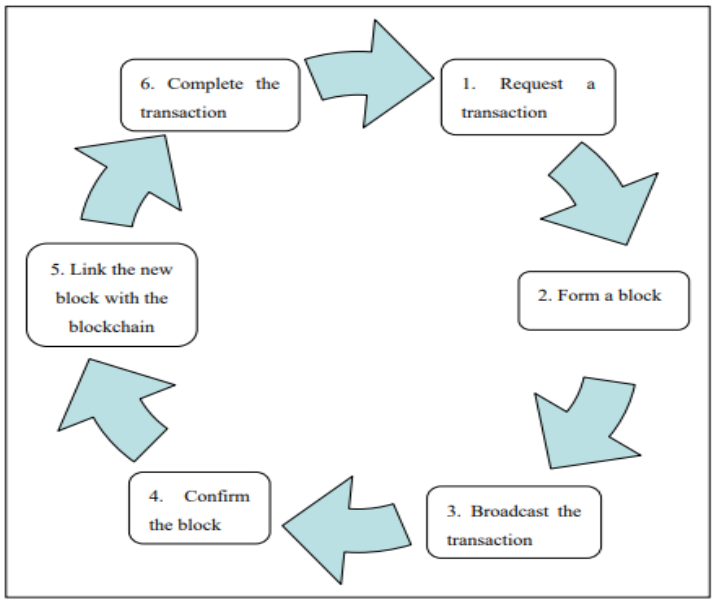

Figure 1: Impacts of Blockchain on Audit procedures

Source: (Li, 2017)

More companies are now exploring the Blockchain technology and availing the business opportunities in it (Li, 2017). The Blockchain ecosystems works differently, and impacts the way the business is run, including the firm's control environment and reporting mechanisms. It is a decentralized systems using a distributed ledger, hence, it disregards claims of a single ownership of data and records, and will change the way financial records are created, recorded and reported. The private Blockchain uses a unique private key to authorize transactions using a majority based consensus protocol. Using cryptographic programming, the key is based on highly complex configurations and is only available to the authorized user. Apart from that, the use of Smart Contracts and triple entry accounting would also increase the confidence on the reliability, integrity and accuracy of the information. Hence, the presumption that the Blockchain ecosystem is immutable and reliable. However, it must be cautioned that there could be many varieties of private Blockchain mechanisms. Depending on size and complexities, this could open up several loop holes that could manipulate the overall transparency of the system. For now, the risks is deemed to be higher internally rather than perpetrated externally.

Both accounting and auditing firms should take initiatives to understand this technology, the changes expected and its implications. The Blockchain mechanism is not limited to one industry or sector, as the mechanism has the capability to be eventually used worldwide and industry wide. One example of how the Blockchain can benefit a business is the reconciliation of payment to the instruction or source. Either an invoice doesn't match up with a payment, or an outgoing payment is not being matched with the customer's systems. By storing information, such as invoices, on a distributed ledger, the information can be shared with the counter parties and colleagues. This allows them to verify that every party in the value chain is using the exact same information which allows further to cut down on errors and costs in processing financial transactions. Smart Contracts

January - February 2020
ISSN: 0193 - 4120 Page No. 1109 - 1118

are one of the technical applications that is used to accomplish this and it basically cuts down on errors made in the financial processes throughout the year. This allows to reconcile the transaction, the balance and the reporting process. These three parts of financial processes are essential to run a solid business and Blockchain can integrate these three steps into one process.

The Blockchain is said to be the platform that is capable of auditing itself leaving the auditor with no such audit work because of the nature of the network that is designed to record and validate the information that is audited with several opinions. Distributed ledgers are based on promoting confidence and resilience without a key, trusted party controlling the process. However, while a Blockchain entry can be trusted as an official record of a transaction but it does not necessarily provide evidence of the nature of the transaction, why it occurred, or if all transactions were recorded(Smith, 2019). There is also the possibility of the inclusion of preferred nodes of validation, with some having more power than others based on the requirement of the private Blockchain. Whilst this may remain required and within legal perspectives, this could also open opportunities for overriding of controls, fraudulent exchanges and collaboration to carry out fraudulent activities. These risks increase if the size of the private Blockchain is smaller.

Therefore, it is speculated that some level of audit or checking mechanism would still be required. However, the audit procedures would need to be transformed into a hybrid of traditional and Information Technology (IT audit) to remain relevant in the Blockchain ecosystem. IT audit goals most often focus on substantiating the existence of inner checks and controls, whilst functioning to minimize company risk as anticipated. These audit goals include ensuring compliance with legal and regulatory demands, as well as information systems and data confidentiality, integrity, and accessibility (CIA). Therefore, the IT audit framework covers the risks and control measures that can be used for the Blockchain audit.

Adopting literature from the typical risk based auditing, auditors are needed to know the particular hazards to an entity's IT-related financial statements and how the entity responds to these hazards by implementing IT controls. As Blockchain technology is increasingly being adopted, auditors will need to increase the bar by offering progressively complicated assurance services in more flexible company settings and supporting future digital transformations. To meet the expectations of stakeholders and company owners in this world, a distinct professional mindset and extra knowledge will be needed (Psaila, 2018), relying heavily on the professional skepticism especially in an unknown terrain.

The objective of an audit is to enable the auditor to express an opinion on whether the financial statements are prepared, in all material respects, in accordance with an applicable financial reporting framework. Based on the brief description of the mechanism, the Blockchain has the potential to minimize the work load on the auditor which will let the auditor to focus on more important tasks. For instance, as the audit involves an assessment that recorded transactions are supported by evidence that is relevant, reliable, objective, accurate, and verifiable so the verification of the occurrence of a transaction will be able to be confirmed by the Blockchain network along with the amount of transaction and the parties involved which will be an audit evidence. However, the main audit work would shift on the authenticity of the transaction by checking on if the product that was agreed to be exchanged is delivered or not. Therefore, the Blockchain transactions may or may not provide sufficient appropriate evidence related to the nature of the transaction. There are possibilities in Blockchain transactions to be unauthorized, fraudulent or may be illegal, they might have been executed between related parties

and linked to side agreement that is off-chain (Kokina, J., Mancha, R., & Pachamanova, D. 2017). The valuation could be incorrectly classified in the financial statement that reflects the estimated values that differ from historical cost. Auditors would have to change their approach towards the audit procedures and would need to test on the areas that are new in the Blockchain system.

Based on the mechanism itself, it would seem that the audit trail and identity traceability is non disputable. Therefore, the implication would be that once an investigation is started or a red flag (suspicion or discrepancy is noted), the perpetrators would not be able to escape detection. This should serve as a demotivation to carry out such fraudulent activities, however, there is also a possibility of using identity theft, hacking or virus attacks as a defense. Hence, all avenues should be explored, with auditors being able to justify their opinion on various angles of the financial reports.

III. RESEARCH METHODOLOGY

Due to the level of expertise and depth that is required to assess the objectives of this research sufficiently, a qualitative research will be carried out. The primary data in the study will be collected via having semi-structured interviews in which open ended questions will be asked to the participants. The target population for the purpose of interviews will consist ofBlockchain experts, Blockchain solutions providers and auditors specializing in IT and Blockchaininternationally. The respondents were made aware of the pre-requisite that they needed to have practical and in-depth knowledge of Blockchain related issues. The population of Blockchain experts is relatively unknown. However, the researcher used various keywords to search for such experts using business networks online. The researcher approached 25 such experts internationally. However, only 12 initially agreed to the interviews as the rest were unsure of the discussed scope. Out of the 12, this research only included the results of the interview with 7 of the experts, as the remaining 5 responses were incomplete or insufficient to add value to the scope.

RESEARCH FRAMEWORK

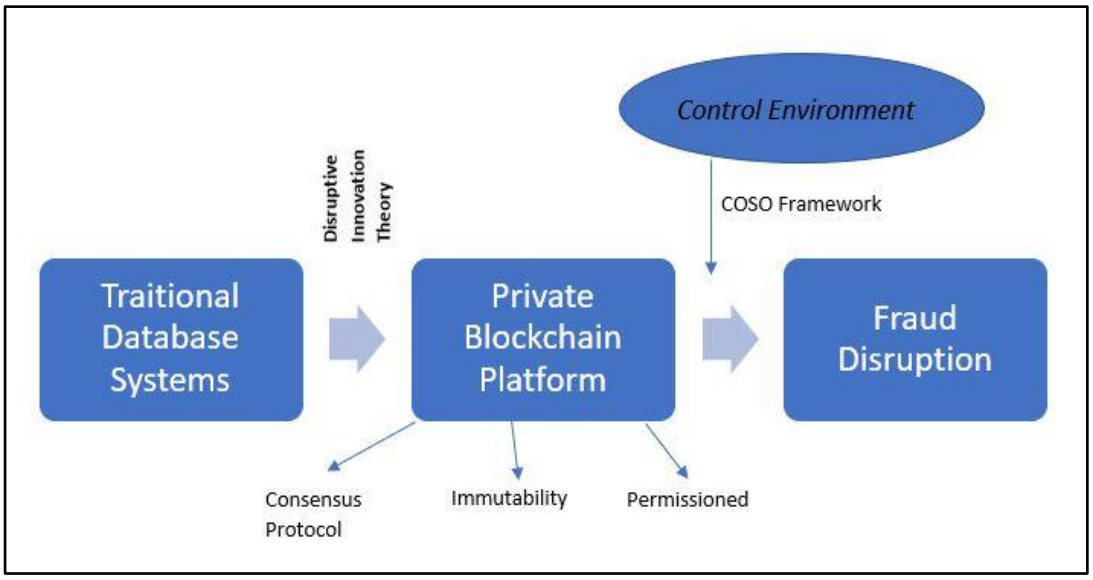

Figure 2: Research Framework (Self Authored)

January - February 2020
ISSN: 0193 - 4120 Page No. 1109 - 1118

IV. FINDINGS & DISCUSSION

Table 1 reports the demographics of the respondents consisting of gender, profession and experience.

Variables	Frequency	Percentage
Gender		
Male	6	85%
Female	1	15%
Profession		
Blockchain Experts	3	42%
Blockchain solution Providers	2	28%
I.T and Blockchain Auditors	2	28%
Experience		
Less than 5 Years	2	28%
5-10 Years	3	42%
10-15 Years	2	28%

Table 1: Demographics of Respondents

The initial part of the interviews aimed to understand the impact of Blockchain on the business environment. The respondents were positive in their feedback, by asserting that the Blockchain control environment would be more effective and secure due to its data distribution, ultimately improving communication, governance and internal controls. The respondents did highlight the necessity to assess the different types of private Blockchain networks separately as they were not made equal. Unlike the public Blockchain, the private Blockchain can be designed according to the organization size and the issues on hand. Similarly, the private Blockchain are more secure of the public Blockchain because of the restrictive access amongst private participants.

The respondents also stressed that automation would ensure the integrity of the information, transactions and audit trail in concurrence with accounting and other regulatory requirements, enabling a more reliable oversight with those charged with governance and compliance. The respondents strongly asserted that cryptographic elements within the Blockchain ecosystem would assure the integrity, immutability and reliability of "tamper-proof" records. This would be via the private key, a unique authorization tool that is required by each node in the network to perform transactions. The key is designed with cryptographic programming based on highly complex configurations. The authorization can only be carried out with the use of the private key of the majority of the participants following a consensus protocol, hence adding on the process of validation and authentication. The transactions could be encrypted before uploading to the Blockchain ledger to protect the privacy of a company's sensitive data, and only users with the decryption key should be able to view the transaction content. This removes the risk of third-

January - February 2020
ISSN: 0193 - 4120 Page No. 1109 - 1118

party interference or disruption due to permissioned based Blockchain.

Depending on circumstances, the respondents also proposed that the validation method to be limited to certain participants, such as lawyers, managers, auditors etc. These guidelines could also be programmed to allow automatic checks in Blockchain. After checking, legitimate transactions would be divided into blocks and attached to the primary chain, and then users or customers with permissions could view and discover them. The respondents also propose that auditors and regulators (standard setting bodies) should be included in the development and implementation of Smart Contracts. Collaborations such as this would promote the execution, automation and self-monitoring of such agreements and ultimately, guarantee the legitimacy and honesty of the transactions. Apart from the transaction logs in the Blockchain mechanism which could be submitted periodically to the regulators, the respondents also propose an option of setting a regulatory node in the private Blockchain system for the regulators to monitor the network. However, this may create certain delays especially if the regulatory bodies are able to block or suspend any activity that are not within the given guidelines, until corrective measures have been taken.

The respondents also mentioned that the private networks can be designed based on needs. Whilst this ensures flexibility, it may also create loopholes for manipulation whilst within the realm of the "valid consensus". One possibility is to design the network where each node won't have equal power of validating the transaction. This implies a more centralized network, where certain nodes would have more governance and control over the network, allowing the controllers of these nodes to override the system. The overriding could also be possible in a private network with a smaller and more personal group, where the participants could collude to achieve their targets. The respondents felt that the administrative node should only be there for the overall governance and should not interfere in the validation of the transactions as it will be a threat to internal controls because of its centralized nature. By taking all this measures the internal frauds can be disrupted on a large scale as the technology is new and impenetrable and not a lot of people possess expertise which might challenge the safety of Blockchain.

In addition, the respondents believe that the Smart Contract technology and the triple Blockchain accounting entry system will create a self-verification accounting information mechanism according to accounting standards, business process controls and other regulatory frameworks. The research of Abreu, Aparicio and Costa(2018) agree that Blockchain will provide assurance on the accounting practices as it provides a trail of tamper proof records that can also proof the decision making ability of the strategic management. 40% of the respondents mentioned that the Smart Contracts can be used to automate payments. Although, it would improve the efficiency of the process, the current resistance towards cryptocurrency adoption has not allowed this possibility to expand. Instead, the Smart Contracts cannot automate payments directly but are being used to send confirmed instructions to the middle party (banks) to perform the payment. The respondents also mention that erroneous or fraudulent transactions cannot be reversed, and can only be corrected depending on the mutual agreement between the payer and payee to alter the previous record, which can be tedious and time consuming. The Smart Contract is designed to facilitate transactions that are based on predefined terms, which just like any traditional practice, allow changes to be made. However, two respondents dispute this as Smart Contracts through several layers of testing that makes it almost impossible for any error or fraud. Large sum transactions also require specialized Smart

January - February 2020
ISSN: 0193 - 4120 Page No. 1109 - 1118

Contracts, which need more time for execution and can also be stopped if any errors are detected. This would produce cryptographically safe and transparent reporting, which fitted with the real time abilities would motivate flexible yet accurate reporting mechanisms to suit stakeholders requirements. 43% of the respondents confidently believed that real time recording was possible due to the characteristics mentioned, with another 43% agreeing to the possibility of real time, but felt that it could be impacted depending on the size of the private Blockchain network.

Based on the above discussion, it would seem that most of the risk for a private Blockchain stems from an internal perspective rather than an external perspective. As an example, recent cyber-attacks happened on the public Blockchain networks based on the theft of cryptocurrencies such as the Ethereum database. The respondents were unsure and unconvinced about the recent cyber-attacks as they were confident of the privateBlockchainbeing a secure platform.The respondents believed that the risk of external fraud stems from the type of confidential information that the private Blockchain may hold such as its digital assets etc. As of now, the private Blockchain networks have not integrated crypto currencies in it, hence there could be a reduced external risk in terms of monetary theft. The respondents believe that although the risk maybe prevalent, but there are counter measures to lower the impact such as the use of encryption software's to restrict the entry of bad nodes or unauthorized users as well the use of several layers of administrative security. Similarly, even for the internal fraud possibilities, the perpetrators can be identified from the private keys, and hence this might serve as a demotivation to consider carrying out a fraudulent activities. However, a key consideration should be a possible identity theft, hacking or virus attack which could open up other possibilities.

Therefore, is the Blockchain fraud or error proof and does it require an auditing or checking mechanism?Unanimously, the respondents agree that regulators, auditors and those involved in the monitoring/investigative/compliance should have profound knowledge of Blockchain and its ecosystem, prior to reengineering the audit paradigm or any other legal or regulatory perspective. This is important as it not only impacts the growth of Blockchain based technology in terms of the business environment, but also creates many other benefits to the accounting, auditing and compliance perspective. The reconciliation of accounting and other audit-related information would also promote oversight and monitoring of accounting data streams, exchange accounting information among associate parties, carry out predictive and preventive audits, and possibly attaining near real-time assurance, expanding audit scope along with the quality assurance.

In terms of the auditing objective, auditors should provide their opinion on the sufficiency of the Blockchain technology control environment design and operations and identify any material risks especially in terms of going concern, reputational or financial aspects, taking into account both technical and non-technical factors. The respondents stress that the current auditing standards and procedures are not equipped to audit the Blockchain ecosystem.Dai, J. and Vasarhelyi, M.A (2017) concur with this statement.

The Audit preparation should be built on the principles of Pre-Implementation, Governance, Development, Security, Transactions and Consensus.Even from a traditional auditing approach, the priority of the auditor would be to assess if sufficient confidence could be placed on the credibility of information. 86% of the respondents suggested that the automated decentralized self-validating mechanism using the independent participants in the network should be a sufficient audit test by itself. Analytical

January - February 2020
ISSN: 0193 - 4120 Page No. 1109 - 1118

procedures would highlight any discrepancies that could impact the in the integrity of the data. This includes a time series check against historical data or checking of the logs for any possible duplication of transactions as part of a corrective action.Five out of seven respondents mentioned that the transactions cannot be deleted from the network because of immutable record, which provides the auditor with audit trails to get sufficient confidence on the information and historical data. The Blockchain process justifies and records transactions which is then established into blocks and scheduled in a chain that is linked to cryptography and validated. This method allows proving that a file existed at a given time in a particular version without revealing the data throughout the file. This presents that every single change to the ledger will be logged and timestamped by a Blockchain.

However, the respondents also caution that although the Blockchain features boast of tamper proof and immutable records, the auditor using the expected professional skepticism should design technology based tests to vouch and verify the authenticity of the transaction's backend process, the approval process and not just the integrity of thedata. The governance testing would be done by performing an analysis on the logs of the administrative node in the network based on its computational power and how many transactions it is validating. Using the risk based assessment approach, the loopholes identified in the discussion above should be assessed. One crucial area to be tested is the power and independence of the approval nodes, assessing the possibility of collusion or overriding to fraudulently approve data. The respondents also recommended checks and assessment of the participants in the private Blockchain network. This would enable the auditors to assess the familiarity of the participants in anticipation of the risk of colluding.

Further document checks or even interviews with the approvers may be required, especially to prove a possibility of fraudulent activities. The auditors should focus on assessing the possibility of overriding or the creation of false validations by the administrators, especially those with more computational power. This would be a crucial step for the auditor have sufficient confidence to rely on the integrity of the data. Abreu, Aparicio and Costa (2018) concur with this observation, as the researchers also caution that auditors need to approach the information with professional skepticism since internal sources may still be able to manipulate the otherwise secure Blockchain platform.

V. CONCLUSION

It is still an exploratory stage, but insofar there seems to be a conclusive response from the experts interviewed. The private Blockchain mechanism boasts of flexibility and sufficient controls. Although acknowledging that there are possible loopholes and weaknesses, the respondents seem to be confident in the private Blockchain platform in being able to mitigate the risks sufficiently. However, the question arises on the need of auditors? The role of auditors is provide an opinion on the credibility of the financial statements which includes an assessment of the internal controls. The respondents have proposed that the accounting standards and other regulatory requirements should be included within the ecosystem, with possible validation roles where needed. They have also cautioned that it may cause delays or other complexities if discrepancies are noted. Checking mechanisms would definitely still be required, but if predictive analysis and other technology based solutions are able to provide accurate and responsive exception reporting, the need would dwindle. Auditing techniques would change as well, not only having to encompass the new ecosystem, but to all also include the revolving accounting and auditing standards. Though, the auditing procedures may

January - February 2020
ISSN: 0193 - 4120 Page No. 1109 - 1118

have also borrowed from the IT Audit literature, a further merge between traditional and IT audit is expected.

References

[1] Abreu, P.W., Aparicio, M. and Costa, C.J., 2018, June. Blockchain technology in the auditing environment. In *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6). IEEE.

[2] Dai, J. and Vasarhelyi, M. (2017). Toward Blockchain-Based Accounting and Assurance. *Journal of Information Systems*, 31(3), pp.5-21.

[3] Gartner (2016). IT Glossary. Gartner. http://www.gartner.com/itglossary/Digitalization. Retrieved 2017-04-10 Michael Rachinger, Romana Rauter, Christiana Müller, Wolfgang Vorraber, Eva Schirgi, (2018) "Digitalization and its influence on business model innovation", Journal of Manufacturing Technology Management, https://doi.org/10.1108/JMTM-01-2018-0020

[4] Kokina, J., Mancha, R., & Pachamanova, D. (2017). Blockchain: Emergent industry adoption and implications for accounting. *Journal of Emerging Technologies in Accounting*, *14*(2), 91-100.

[5] Li, Z., 2017. Will Blockchain Change the Audit. 16(6), pp. 294-298.

[6] MCQUINN, A. and CASTRO, D. (2019). *A Policymaker's Guide to Blockchain*. Information Technology & Innovation Foundation.

[7] Psaila, S., 2018. *Blockchain: A game changer for audit processes.* [Online] Available at: https://www2.deloitte.com/mt/en/pages/audit/articles/mt-Blockchain-a-game-changer-for-audit.html

[8] Smith, P., 2019. *ACCA.* [Online] Available at: https://www.accaglobal.com/my/en/member/discover/cpd-articles/audit-assurance/Blockchain-audit.html

[9] Tan & Low. (2017). Blockchain and Its Coming Impact on Financial Services. Journal of Corporate Accounting & Finance. 27. 53-57. 10.1002/jcaf.22379.