Int. J. Economics and Accounting, Vol. XX, No. XX, xxxx

Fraud Prevention and Detection in a Blockchain Technology Environment: Challenges posed to Forensic Accountants

Musbaudeen Titilope Oladejo*
School of Accounting, Finance and Economics
Faculty of Management
University of Waikato
Hamilton, New Zealand
Email: mo163@students.waikato.ac.nz
* Corresponding author

Lisa Jack
Portsmouth Business School
University of Portsmouth
United Kingdom
Email: Lisa.Jack@port.ac.uk

Abstract: This paper set out to explore the challenges posed by blockchain to forensic accountants in the prevention and detection of fraud. Blockchain will create a decentralised environment where transactions and data have no third-party control. This technology is capable of disrupting accounting and audit because it is capable of automating financial records and audit processes. The fraud analysis in a digital environment is complex and the evolution of new technologies or innovations such as blockchain, artificial intelligence, and robotics have added to these challenges. The framework for analysis adopted is a qualitative study using the library research methodology. The findings portray that blockchain technology is not 100% flawless, impenetrable to malicious attacks, and hacking. The results of the study found that technology will affect the core functions of accountants, but the overall effects on the roles of forensic accountants and auditors are still unknown.

Keywords: Blockchain, Fraud, Fraud prevention and detection, Forensic accounting skills, Data Mining, Audit, Digital Age

Reference to this paper should be made as follows: Oladejo, M.T. and Jack, L. (xxxx) ‘Fraud prevention and detection in a blockchain technology environment: Challenges posed to forensic accountants’, *Int. J. Economics and Accounting*, Vol. XX, No. XX, pp. xx-xxxx.

Biographical Notes: Musbaudeen Titilope Oladejo is a PhD student at the Waikato Management School, University of Waikato, New Zealand. He holds a Bachelor’s degree in Accounting from the University of Lagos, Nigeria, a Masters in Forensic Accounting from the University of Portsmouth, United Kingdom and a Masters in War Studies (with a major in the maritime domain) from National Defence University, Islamabad, Pakistan. Musbaudeen is a Chartered Accountant Member of the Chartered Institute of Taxation of Nigeria and a Fellow of the Institute of Chartered Accountants of Nigeria. Musbaudeen’s research focuses on the likely practical implications blockchain technology will have on the accounting and auditing profession. This research paper originates from research conducted by Musbaudeen for his dissertation in his master’s studies at the University of Portsmouth, the United

Kingdom under the supervision of Professor Lisa Jack, a Professor of Accounting at the Portsmouth Business School.

Lisa Jack is currently Professor of Accounting in the Faculty of Business and Law in Portsmouth Business School. She is also currently President of the British Accounting and Finance Association, a learned society for academics in the UK. Lisa has worked as an auditor in local government and higher education. After ten years of auditing, she moved into teaching professional accountancy and management programmes in further education and HEIs. She currently teaches on the module 'Financial Crime and the Law' on the MSC Forensic Accounting course. Lisa is on the Editorial Review Boards of several journals, including British Accounting Review; Accounting, Auditing and Accountability Journal and Accounting Forum. She is an Associate Editor for the AAA Journal of Forensic Accounting Research.

1 Introduction

Blockchain has attracted significant attention since the launching of Bitcoin in 2008 (Alarcon & Ng, 2018; Zouina & Outtai, 2019). Researchers have highlighted blockchain's potential to revolutionise the social-economic landscape (Angelis & Ribeiro da Silva, 2019; Casino, Dasaklis, & Patsakis, 2019; McCallig, Robb, & Rohde, 2019; Zouina & Outtai, 2019) as this technology continues to evolve. Blockchain intends to create a decentralised environment where transactions and data have no third-party control (Casino et al., 2019; Nowiński & Kozma, 2017). Amongst its potential uses in accounting and audit are the facilitation of traceable audit trails, automated audit processes, development of smart contracts and inventory management (Maupin, 2017; Peters & Panayi, 2016; Schmitz & Leoni, 2019). Blockchain can assist businesses with their financial transactions, reporting, and accounting functions (Bizarro, Mankowski, & Mankowski, 2018).

Financial fraud is an issue with far-reaching implications for the finance sector, governments, and corporate organisations including consumers (Abdallah, Maarof, & Zainal, 2016). The problem is compounded with the evolution of new technologies like mobile and cloud computing that facilitate electronic transactions in banking and commerce, and the recent emergence of blockchain. Many businesses now rely on the use of technology and computer-based system for business processes and traditional accounting transactions (Pearson & Singleton, 2008) which has necessitated the audit practitioners to use IT in audits for fraud detection purposes. Regardless of its intricacy, a blockchain is a form of database for recording transactions and a distributed ledger, which shares data to all participating computers in a network.

Blockchain technology is expected to bring transparency, accountability, and auditability to e-commerce (Brandon, 2016). However, empirical studies on the extent of how this new technology can aid the prevention and detection of fraud are non-existent. The modality to be adopted by auditors in auditing transactions on blockchain is still evolving (de Meijer, 2016; Schmitz & Leoni, 2019). Additionally, payment for goods or services is impossible without an intermediary or a third party like a bank or credit card company. One of the core features of blockchain technology is the elimination of these intermediaries like the regulator, government, banks or credit card firm from transaction processes (Bizarro et al., 2018; Brandon, 2016; Casino et al., 2019). It is yet unclear whether the elimination of these intermediaries will happen in blockchain transactions in practice. History has shown that innovations have *intended or unintended consequences* and blockchain may not be an exception. For instance, hacking of online transactions, malicious attacks on databases, pirated media, drug peddling, smart card fraud and other fraudulent financial activities are intended or unintended consequences of using the Internet.

Financial fraud prevention and detection has become an emerging topic of importance for academic researchers, regulators and investors in a digital environment. The focus of this paper is to examine whether there are challenges posed by blockchain technology to forensic accountants in the prevention and detection of fraud in this digital age. The paper further explores the usefulness or otherwise of the Data Mining (DM) techniques as fraud detection tools in blockchain transactions, the technology possible effects on the future of accounting and auditing, and the technical skills required of accountants for this technology.

2 Background

The 21st century has seen the rise of some advancing, albeit, disruptive technologies like the Internet and mobile computing which have enhanced seamless connectivity of billions of people globally, and now there is blockchain (Marechaux, 2019; Peters & Panayi, 2016; West & Bhattacharya, 2016; Xu et al., 2019). Several business and social processes have changed due to the development of fast computers, digital communication platforms and infinite data storage, but accounting and auditing professions are considered laggard in embracing these innovations (McCallig et al., 2019). Researchers have identified benefits and challenges relating to the need for and use of blockchain technology for all transactions (Bradbury, 2016; Fanning & Centers, 2016; Iansiti & Lakhani, 2017; Markelevich, 2018; Martindale, 2016; Xu et al., 2019). Blockchain technology is capable of creating a decentralised environment where transactions and data have no third-party control (Swan, 2015; Tan & Low, 2019). Markelevich (2018) explains that blockchain helps in the organisation and storage of data in a distributive manner.

Forensic accountants are required to sieve through very large databases to detect patterns of fraud and expose efforts to conceal anomalies in complex fraud schemes (Kreuter, 2017). The additional basic forensic accounting skills in the performance of an audit will enhance the ability and competence of auditors to spot fraud (DiGabriele, 2016). It is important to evaluate the challenges posed by blockchain technology in this digital age to forensic accountants in fraud prevention and detection. The rationale for this study is that blockchain is a technology revolution, which could eliminate the current intermediation roles of government/regulators and facilitate the seamless interface of stakeholders. It has been described as disruptive technology as its application in theories could change the ways things are done in virtually all areas of business and economy (Biswas & Gupta, 2019; Markelevich, 2018; Peters & Panayi, 2016; Swan, 2015; Xu, 2016).

However, Iansiti and Lakhani (2017) assert that blockchain is not a disruptive technology, but a foundational technology with potentials to unlock opportunities for an economic and social system. Maupin (2017) reflects that it is participative digital globalisation, which requires no audit, secure and transparent to all stakeholders. It is a foundational technology and still evolving, there is currently limited research on fraud prevention and detection in blockchain transactions.

The main research question is "Are there challenges posed by blockchain technology to forensic accountants in fraud prevention and detection?" The sub-questions further evaluate whether the existing fraud detection tools like DM technique would be useful, what are the possible effects blockchain would have on the future of accounting and auditing and the technical skills required of forensic accountants for effective fraud detection analysis in blockchain.

3 Fraud Prevention and Detection in Blockchain Technology

Fraud is a global concern, which affects negatively on organisations and economies in general (Gbegi & Adebisi, 2014; Jurgovsky et al., 2018; Seetharaman, Senthilvelmurugan, & Rajan, 2004). Fraud is a key consideration whenever there is a new revolution which affects business transactions (Bănărescu, 2015), and modern banking systems place much emphasis on a precise method of fraud detection (Jurgovsky et al., 2018). Some researchers note that effective detection of accounting fraud in a digital age is a major challenge for the accounting profession (Ngai, Hu, Wong, Chen, & Sun, 2011; Sharma & Panigrahi, 2012). The use of Computer Assisted Audit Techniques (CAATs) in detecting fraud using analytical tests yield little or no result (Bay, Kumaraswamy, Anderle, Kumar, & Steier, 2006). Complete reliance on the use of the traditional audit mechanisms for detection of modern accounting fraud is considered inadequate, and this inadequacy in identifying accounting fraud necessitated the use of forensic accounting techniques for fraud detection (Abdallah, Maarof, & Zainal, 2016; Gbegi & Adebisi, 2014; Kotsiantis, Koumanakos, Tzelepis, & Tampakas, 2006; Sharma & Panigrahi, 2012).

Organisations are prone to fraud in a digital environment due to ever-changing technological innovations (Abdallah et al., 2016). However, every organisation should institute adequate mechanisms for the prevention and detection of anomalies, but in practice, the instituted fraud mechanisms could be overwhelmed as fraudsters keep pace or outsmart the system. Blockchain has the potential to prevent and protect some fraudulent activities because it uses cryptography and the P2P network. Despite this, it is obvious that blockchain is not immune to fraudulent entries. Similarly, as the internet produced spammers and hackers, blockchain will create a new breed of cybercriminals who rely on encryption and darknets to wreak havoc (Burmester & Mulholland, 2006; Xu, 2016).

Fraud prevention and detection is a complex domain in a digital age and poses a challenge to forensic accountants, management and regulators alike (Abdallah et al., 2016; Lin, Chiu, Huang, & Yen, 2015). Fraud prevention is aimed at halting a fraud, but the evolving technology seems to have outpaced the existing fraud prevention mechanisms while fraud detection discovers, identifies and reports anomalies as they find their way into the system (Abdallah et al., 2016; Ahmed, Mahmood, & Islam, 2016; West & Bhattacharya, 2016). In the meantime, while blockchain technology continues to evolve; forensic accountants are required to keep pace with this new evolution to facilitate fraud investigation and detection in the blockchain transactions.

3.1 Data Mining Techniques as Fraud Detection Tool in Blockchain

The evolution of modern and global communication is significantly contributing to an increase in fraud (Abdallah et al., 2016; Kou, Lu, Sirwongwattana, & Huang, 2004). Financial fraud is a topical issue and its effective detection is a challenge for accounting professionals (Ahmed et al., 2016; Lin et al., 2015; Ngai et al., 2011). The limitation in exchange of fraud detection ideas and inaccessible fraud data has made expansion in the development of new fraud prevention and detection methods difficult (Kou et al., 2004; West & Bhattacharya, 2016). Fraud prevention system (FPS) describes mechanisms put in place to stop frauds or anomalies from occurring in the first instance (Estévez, Held, & Perez, 2006). In contrast, Fraud detection system (FDS) is a computerised and automated system designed to enhance detection of fraud using DM, statistics and artificial intelligence (AI) (Abdallah et al., 2016; Kou et al., 2004; West & Bhattacharya, 2016), to optimise accuracy rate and reduce false positives (Kou et al., 2004), and enable management to develop mechanisms to reduce the incidence of fraud (Ngai et al., 2011). The difficulty in accessing real fraud data for empirical research to facilitate the development of a robust mechanism for prevention and detection of fraud in the existing new technological innovations may also affect blockchain technology, as organisations are often protective of their financial data. Consequently, this difficulty limits the application of DM techniques for research to only using hypothetical figures.

DM involves "statistical, mathematical, AI and machine learning language to extract and identify useful information and subsequent knowledge from large databases" (Abdallah et al., 2016, p.93). DM incorporates techniques from other disciplines like "statistics, machine learning, visualisation, neural networks, inductive logic, computing and many other fields" (Han, Kamber, & Pei, 2012). DM uses two approaches to fraud: proactive and reactive approaches. The proactive approach identifies who and what can make a specific set of transactions or actions that characterise fraud before they occur, whereas, the reactive approach detects anomalies that happen in a set of transactions (Deepak, 2019). Accordingly, DM techniques can be tailored or adapted specifically for a set objective such as telecommunication, finance, e-mail, audit or census (Abdallah et al., 2016; Han et al., 2012). In a study conducted by Bhasin (2015), DM was ranked the most important software tool for forensic accountants among other software tools. It may be inferred that since DM inculcates techniques from various disciplines for the prevention and detection of anomalies, it could be adapted for use in blockchain transactions. However, empirical support is required to test its full usefulness in the light of the inbuilt detection mechanisms in blockchain.

Fraudsters employed diverse approaches to breach the e-commerce system, and FPS are insufficient to provide adequate security to the e-commerce system (Abdallah et al., 2016; Jurgovsky et al., 2018). In contrast to FDS, which work to unearth fraud, blockchain has a predictive fraud prevention and detection systems. Nonetheless, research has shown that the FPS and FDS on blockchain are also prone to malicious attacks (Cai & Zhu, 2016; Xu, 2016). With appropriate methods and approaches, computer programmers can modify the existing FDS using DM tools for fraud analysis on blockchain. Han et al. (2012) affirm that DM can be applied to any form of meaningful data on a specific application such as database data, transactional data, data warehouse and advanced data types. Blockchain has some preventive mechanisms like cryptography and distributed consensus to check or minimise dangers of cyber-attacks *(Swan, 2015; Zhao, Fan, & Yan, 2016)*, but other researchers found out that blockchain is vulnerable to attacks such as 51% attack, Distributed Denial of Service (DDoS) and hacking (Peters & Panayi, 2016; Xu, 2016; Zhu & Zhou, 2016). Besides, all the nodes work concurrently with access to all data. Hence, privacy and confidentiality remain problems with blockchain (Wang, Shen, Li, Shao, & Yang, 2019).

The increase in fraud in online transactions has been a topical issue (Abdallah et al., 2016; Yufeng, Chang-Tien, Sirwongwattana, & Yo-Ping, 2004). Hence, stakeholders' priority is how to prevent and detect anomalies/fraud in any innovation (Ahmed et al., 2016). The early adopters of blockchain technology embrace the use of Bitcoin because of its potential to prevent and detect fraud (Huberman, Leshno, & Moallemi, 2017; Maurer, Nelms, & Swartz, 2013; Tapscott & Tapscott, 2016, 2017; Treiblmaier & Beck, 2019). Using blockchain technology will facilitate the creation of permanent, immutable, transparent and auditable transactions since the record kept on it, is distributed among all the participating computers' nodes for accountability (Sarda, Chowdhury, Colman, Kabir, & Han, 2018; Viriyasitavat & Hoonsopon, 2019). However, the P2P network could provide an avenue for malicious attack and the spread of a virus (Cai & Zhu, 2016; Xu, 2016). The recent hack on blockchain showed that no technology is unhackable (Zachariadis, Hileman, & Scott, 2019). Therefore, there is a need to find suitable means of combating fraud on blockchain. The existing fraud-detecting tool like DM was explored. The current research on prevention and detection of fraud using DM techniques are on hypothetical data as it is hard to have access to fraud data in real life (Ahmed et al., 2016; Yufeng et al., 2004). However, at best, for now, considering that DM draws its techniques from different fields and has wide application, it can be inferred that DM can be adapted to meet the needs of blockchain by IT experts.

As an emerging subset of e-commerce, the challenges posed by blockchain technology are that it cannot guarantee the source documents and reliability of the records kept on it as hackers can breach its cryptographic to commit fraud and malicious attack (Cai & Zhu, 2016; Xu, 2016; Yli-Huumo, Ko, Choi, Park, & Smolander, 2016). The issue for forensic accountants is how to prevent and detect fraud in blockchain transactions using the existing fraud detection tool. Despite the preventive technology mechanism such as cryptography and P2P network in blockchain, there are no fraud detection techniques that fit into all applications (Xu, 2016). Therefore, forensic accountants may need to find a suitable combination of tools and techniques. Bănărescu (2015) note that human and technical elements are critical factors in an actual fraud prevention and detection mechanism. He submits that irrespective of the technical sophistication of any system it is still subject to human manipulation (Bănărescu, 2015). In blockchain technology, the human errors and technical factors may also affect a fraud prevention and detection system since individuals with opportunity, pressure and rationalisation can still override the technology (Nickerson, 2019). However, a machine-learning algorithm has been suggested to facilitate fraud prevention and detection in blockchain transactions (Xu, 2016).

4 Technical Skills required by Accountants in the Blockchain Technology

New technological innovations often require training and retraining of users for effective deployment of such technology. The germane question is, are the existing skills possess by auditors and forensic accountants still sufficient in this digital age? The study briefly highlights how technology is reshaping core services of the accounting profession, technical skills required of forensic accountants and auditors in blockchain technology.

4.1 How Technology is Reshaping Core Services of the Accounting Profession

Over time, IT has revolutionised tax and accounting. Gillon (2017) observes that the technology looks set to reform the audit, a major service of the traditional accounting practice. The emerging innovations like AI, machine learning, cloud computing and blockchain could reshape the entire accounting profession (Boomer, 2017; Gillon, 2017). Before emerging technologies from IT, the training focus for auditors and accountants is to provide relevant information to decision-makers and stakeholders on financial matters. This is achieved by extracting meanings from large volumes of business data using available analytical tools (Janvrin & Watson, 2017). Janvrin and Watson (2017) note further that internal and external auditors examined data to make sure it complied with GAAP, applicable laws, and management’s directives. This is achieved by using different automated techniques including generalised audit software and continuous auditing that could scrutinise all transactions of a firm (Janvrin & Watson 2017).

The roles of accountants are closely linked with the acquisition of skills and training. Many researchers argue that forensic accountants require more of technical, communication, analytical, and leadership skills in addition to knowledge in financial accounting, business and law (Digabriele, 2008; Gillon, 2017; Houck, Morris, & Riley, 2006) to be robust professionals. As such, the training curriculum of prospective forensic accountants and auditors are tailored towards making them proficient in these skills. The need to enhance the IT and computer skills of accountants has made professional accounting bodies and accounting degree qualifications from higher education institutions to include requisite IT training in their curricula. However, Davis, Farrell, and Ogilby (2008) refers to these skills as traditional accounting core skills and not sufficient in a digital age. Some studies show that auditors and forensic accountants have poor IT skills and knowledge to effectively explore latest technological innovations such as AI, audit expert and blockchain (Kearns, 2010; Pearson & Singleton, 2008; Ramaswamy, 2005). In the same vein, Pan and Seow (2016) point out that there is inadequate advanced IT knowledge and skills in areas like It forensic, IT audit, and data analytics among many accounting professionals. The transformation impact of technologies compelled the Pathways Commission (2012), set up by the American Accounting Association (AAA) and the American Institute of Certified Public Accountants (AICPA) to study the future structure of higher education for the accounting profession, to recommend integration of accounting programs with emerging accounting and business IT throughout their academic curricula.

In the same vein, some professional accounting bodies such as the AICPA and CPA Canada have launched an initiative that could assist in integrating data analytics into the audit process to enhance audit quality (Janvrin & Watson, 2017). This initiative will require IT skills because data analytic involves automation and use of IT software tools. Besides, several accounting firms also expose their audit trainees, interns and staff to further training to hone their IT and computer skills amongst others.

The importance of IT skills is emphasised in the 2020 standards for Association to Advance Collegiate Schools of Business (AACSB) business accreditation in which schools are expected to describe “how degree programs include learning experiences that develop competencies related to the integration of IT” (AACSB, 2020, p. 28). Besides this, AACSB expects schools to submit the list of the current or emerging technology employed in each degree program to support their accreditation. In addition to these efforts, considering the dynamic nature of the IT innovations, auditors and forensic accountants will need continuous updating of their IT skills for fraud prevention and detection in the digital age.

4.2 Skills Required by Forensic Accountants for Fraud Analysis Detection in Blockchain Transactions

The increased IT usage to perpetrate fraud and the need to prevent or detect such fraudulent activities have also been topical issues. The gaps in the provision of fraud and accounting training are due to insufficient IT skill in fraud and forensic accountants, and a mismatch between the present higher education curriculum and reliance on IT by modern businesses (Ramaswamy, 2005; Pearson & Singleton, 2008; Kearns, 2010). The recent corporate scandals and media attention have emphasised the importance of training forensic accountants especially on Accounting Information System (AIS) since the basic auditing, and accounting skills are insufficient in a digital age (Ramaswamy, 2005; Houck *et al.*, 2006; Pearson & Singleton, 2008; Bressler, 2011). Boomer (2017) notes that to remain relevant accountants need a change of mindsets, skill sets and tool-sets because existing technologies like Apple Siri, Microsoft Cortana, Amazon, Alexa coupled with AI can replace human roles. Thus, there is a need to enhance the forensic accountants’ technical skills for fraud detection in a digital age. It can, therefore, be inferred that forensic accountants and auditors require adequate training in AIS to meet the emerging challenges associated with the blockchain transactions.

An audit is defined in ISO 19011:2018 as a "systematic, independent and documented process for obtaining audit evidence [records, statements of fact or other information which are relevant and verifiable] and evaluating it objectively to determine the extent to which the audit criteria [a set of policies, procedures or requirements] are fulfilled" (https://asq.org/quality-resources/auditing). Essential in the first place is, therefore, finding the data. Hannink (2013) explains that "…most fraud schemes are initiated by upper management with complicity from others like employees and external entities" (p.282). Furthermore, Hannink argues that "with people involved at different levels, the signs of fraud are disguised making fraud schemes incredibly difficult to detect" (ibid) and that while analysts and auditors can look for warning signs, it is not easy without disclosure of pertinent information from management. Therefore, the aspect of blockchain that will significantly impact upon forensic accountants is their ability to investigate data and interrogate transactions. Blockchain transactions are claimed to have an inbuilt mechanism to prevent and detect fraud and fraudulent activities (Maurer et al., 2013; Xu, 2016; Zhao et al., 2016). Similarly, the technology does not require an audit or any third-party monitoring (Brandon, 2016; Fanning & Centers, 2016; Maupin, 2017; Xu, 2016). However, emerging technologies come with expectations and fears. Marvin (2017) and Zhao, et al. (2016) note that the technology is in its infancy and further research is needed to determine its efficiency and security. Forensic accountants require specialised knowledge and skills beyond the traditional accounting curricula to operate in a digital environment. The IT fraud detection software that can enhance audit through the computer and the AIS software is essential (Pearson & Singleton, 2008; Gbegi & Adebisi, 2014).

It has been suggested that accountants may need to improve their knowledge of mathematics and statistics (Boomer, 2017), big data which include the skill to analyse data, ask pertinent questions and comprehend the limits of the analysis (McKinney, Yoos, & Snead, 2017). Casal, vice-chair audit at KPMG, in a round table discussion, notes that cognitive technologies like robotic process automation, AI and blockchain need to be adopted because they have potential to improve audit quality (Baer, Casal, Fornelli, Shamon, & Thompson, 2017). Similarly, from the result of a survey conducted by Digabriele (2008) which involves academics, forensic accounting practitioners and users, he lists the relevant skills of forensic accountants to include (a) deductive analysis, (b) critical thinking, (c) unstructured problem solving, (d) investigative flexibility, (f) analytical proficiency, (g) oral communication, (i) written communication, (j) specific legal knowledge and (k) composure.

5 Findings

This research adopted a qualitative methodology using library-based documentary research and the use of secondary data. A meta-analysis method was adopted to make useful meaning from the vast literature on the subject. Most of the analysed data were from the available existing academic journals, magazines, conferences papers, online publications, and publications from professional accounting bodies. The literature research methodology has been described as a careful analysis and sorting of literature for identification of the essential attribute of materials in which to grasp sources of relevant research and to comprehend the contributions of other researchers (Lin, 2009). Secondary data is appropriate for a research project that requires national and international comparisons and large data from many recipients (Saunders, Lewis, & Thornhill, 2016). Consequently, this study applied a literature research methodology and obtained relevant information from secondary data because it entails sourcing information from multiple sources. Additionally, publications from the Internet, broadcast and blog which are directly relevant to the research objectives were used to buttress other sources. The purpose was to use two or more independent lines of evidence on the subject to yield sufficient good-quality data and broad investigation. The reason being that blockchain is relatively a new topic and still evolving, there are few published empirical studies on it (Cai & Zhu, 2016; Zhao et al., 2016). Thus, the researcher relies on the available sources of information which usually comes up like “breaking news”. The evolution of blockchain could be traced to the creation of bitcoins in 2008 by Nakamoto (Kiviat, 2015; Miers, Garman, Green, & Rubin, 2013). Therefore, most of the data used for this study are from 2008 to 2020. From 2008 till date, numerous ideas have been published and still being published by the scholars, governments, financial institutions, IT companies and other stakeholders to make meanings out of the emerging blockchain technology.

It is straightforward for the research data to become unmanageable and disorganised due to the large volume of accessed data. To prevent this, from the available secondary data, the research data are organised into the key themes: Blockchain technology, fraud prevention, fraud detection, DM techniques and skills required by forensic accountants and digital age. An online search was conducted using these identified themes. The results were further grouped into textbooks, academic journals, newspapers and magazines, and online publications. The saved results were later sorted and arranged excluding those publications that do not directly discuss blockchain and fraud prevention and detection mechanisms. Similarly, e-message alerts were set up on popular search engines such as Google Scholar and other websites for the latest news or information on the blockchain technology. This assists in keeping abreast of the current information on blockchain, thereby providing a platform to cross-check available data and ensure the only verifiable and latest information is included in the study. Computer searches provide many research opportunities in term of bibliographic citations, full texts of some documents, recent information and direct contacts with people who are knowledgeable in blockchain (Mann, 1998). In addition to the available textbooks, computer searches were used to identify most of the analysed documents and information. As it is not practicable to read and digest all available data, only relevant articles and publications were analysed. Saunders et al. (2016) note that qualitative documents potentially offer robust sources of data and description of the main events for analyses in blockchain, but great care needs to be taken regarding their original nature and purpose. This necessitated careful thought, logical approach and detailed scrutiny of the available data to ensure their suitability to this research. Despite a vast amount of data on blockchain from published documents and online publications, continuous data reduction strategy was adopted to prune them down. This involves discarding irrelevant data, sorting and analysing collated data in line with the subject of the research (Bell & Waters, 2014). Collis and Hussey (2009) note that researchers need to evaluate sources of data especially textbooks in the light of current information. However, proper evaluation of all sources was carried out by cross-referencing them to ensure that only relevant materials were included in this study.

5.1 Fraud Prevention and Detection Issues and Challenges

Blockchain is believed to have some inbuilt features like permanent record keeping, thwart double-spending, encrypted transactions and disintermediation (Peters & Panayi, 2015; Brandon, 2016; Cai & Zhu, 2016; Xu, 2016) which make some types of fraud difficult to be committed. Similarly, Xu (2016) claims that malicious activities like record hacking and double-spending are not possible on blockchain technology. However, Ngo (2016) reports that blockchain cannot detect or predict fraud or criminal behaviour, protect against identity theft, financial scam and account takeover. Xu (2016, p.6) remarks that "malefactor may find unforeseen ways to steal funds and commit fraud" on it. For instance, the vulnerability of blockchain to theft and security was revealed in the stolen Bitcoins worth $370 million on Mt. Gox in Tokyo (Vigna & Casey, 2016). Conversely, Marvin, 2017 claims that this attack was possible because the victims (Mt. Gox) attempted to centralise a decentralised blockchain system. It, therefore, means that blockchain may require machine-learning capacity like DM as a fraud detection system (Xu, 2016). Blockchain transactions are prone to fraud like other e-commerce, therefore fraud detection in such digital environment may be a challenge for forensic accountants.

Some studies show that researching financial fraud detection is limited due to the difficulty associated with obtaining real data from financial institutions (Ahmed et al., 2016), and limitation in the exchange of ideas in fraud detection (Kou et al., 2004; West & Bhattacharya, 2016). There are no fraud detection techniques that fit into all applications, as card fraud detection techniques are not useful for insurance companies (Kotsiantis et al., 2006; Ahmed, et al., 2016). Bănărescu (2015) notes that human and technical elements are the key factors in the actual fraud prevention and detection mechanism, but the human factor is the weakest link. In blockchain technology, the human and technical factors will be key in the fraud prevention and detection system.

The essence of fraud prevention is to reduce or eliminate the elements that inspire fraud: pressure, opportunity, and rationalisation, because transactions are in virtual space “reducing pressures and eliminating rationalisation has thus far proved difficult” (Zimbelman, *et al*., 2012, p.183). Some of the security measures for preventing fraud in e-commerce are direct billing practices, automated number identification and security through obscurity. Security through obscurity relies on the use of secrecy of design and encryption algorithms to ward off attackers. The use of secrecy of design has been considered its principal weakness because once an attacker breaks the codes, the entire system is vulnerable (Zimbelman, *et al*., 2012). Similarly, blockchain also relies on codes which have been considered difficult to break as it uses cryptography and P2P nodes (Cai & Zhu, 2016). For instance, it is still a mystery to the public whether millions of dollars stolen in March 2014 on Tokyo based *MtGox* was internally or externally motivated fraud because the company claimed their blockchain platform was hacked using a transaction malleability bug. In the same year, it was reported that *Mintpal* was hacked and $2m worth of Bitcoin was stolen, and about $1.5 million Bitcoin in the cover of cryptocurrency exchange was alleged to be stolen and hidden in the personal wallet of the CEO and company’s founder (The Guardian, 2017, February 21). These incidents brought to fore the likely human and technical factors in fraud investigations that will confront forensic accountants in a blockchain environment. These are some of the issues forensic accountants will be required to unravel or deal with using their investigative skills. Forensic accountants, therefore, need to understand both the human and technical elements of blockchain, since the technology is vulnerable to hackers breaking into its codes. Ngo (2016) suggests that fraud detection could be enhanced in blockchain where a machine-learning algorithm is added to the technology. This is because blockchain can neither detect fraud nor protect against issues such as identity theft and financial scams. This assertion by Ngo requires empirical studies to ascertain its validity. Blockchain as an e-commerce system could face similar issues and challenges regarding prevention and detection of fraud as an emerging e-commerce system.

5.2 Technical Skills required by Accountants in the Blockchain Technology

Blockchain and other emerging technologies will reshape audit and by extension forensic accounting. Shamon, the national audit leader at RSM in the United States, observes that the audit team is likely to be working more with the IT team rather than the client’s finance team to have access to relevant information due to the possible elimination of the labour-intensive manual audit (Baer et al., 2017). However, despite the potentials of blockchain, it cannot be relied upon as a source for the initiation of a transaction because the genuineness of original entries requires verification (Peters & Panayi, 2015). Researchers tend to agree that what the accounting profession needs in a digital age are accountants who are versed in AIS, business processes and technology (Ramaswamy, 2005; Houck, et al., 2006; Davies, *et al*. 2008;

DiGabriele, 2008; Pearson & Singleton, 2008; Bressler, 2011; Kearns, 2010; Lombardi & Dull, 2016; Boomer, 2017; McKinney, *et al*., 2017). It can be deduced that in addition to the existing skills a sound knowledge of AIS, business processes and IT is the key technical skill forensic accountants and auditors require in the blockchain environment. The next significant issue and challenge for consideration are how forensic accountants could acquire knowledge of IT, AIS and algorithms deemed relevant in this digital age.

Researchers have identified the benefits relating to the need for forensic accountants and auditors to have requisite knowledge and understanding of IT, AIS and algorithms. One of the challenges of the digital age is implementing technology in educational programs because technology develops exponentially (Apostolou, Dorminey, Hassell, & Rebele, 2017). Despite that technology involves substantial investment in both financial and human resources and requires time and energy of accounting faculty to learn the new technologies, it is difficult to identify whether it achieves desired impact on students' learning ability and development of technology skills (Apostolou, Hassell, Rebele, & Watson, 2010; Jackson, 2004). Nonetheless, Apostolou et al. (2010) observe further that the efficient use of technology is a general problem and not an issue isolated to accounting educators.

5.3 Disruptive Innovation of Blockchain Technology

The computer and the Internet are the leading digital creative paradigms that have disrupted and still disrupting the entire sector of man's activities (Hazlett, 2016; Tapscott & Tapscott, 2016; Vigna & Casey, 2016). This is because these revolutions ushered in the e-mail, the World Wide Web (WWW), dot-coms and IoTs, and achieved the unthinkable things. There is practically nothing that computer and the internet applications are not used for, and the new revolutions submerged the old ones. Hazlet (2016) observed that creative destruction is more pronounced in mobile ecosystems from the Nokia earlier dominated smartphone to the users' friendly Apple iPhone and Google's Android. The potentials of computers and the Internet have facilitated the discovery of intended and unintended consequences associated with technological innovations: dark web, hacking, drug trafficking, cyber-crimes and fraud. Similarly, blockchain comes with opportunities, the risk of disruption and dislocation. Consequently, blockchain is a technology that may have an enormous impact on the future of the world economy (Swan, 2015; Tapscott & Tapscott, 2016; Vigna & Casey, 2016).

As with major paradigm shifts before the blockchain, the intended usage as propounded by its creator, Nakamoto is to provide a platform based on mutual trust where transactions are verified and recorded on a P2P basis without a central authority and at no cost to the participants (Maurer, 2013; Meiklejohn, 2016). The whole essence is to cut off the financial intermediaries who are regarded as extortionists. However, some of the unintended consequences could be seen in the recent hacking of Mt. Gox 2014, Bitfinex in 2016; DAO and Ponzi scheme (Vigna & Casey, 2016). For instance, a UK dealer was charged in the US over a multimillion-dollar fake Bitcoin site scam (The-Guardian, 2017). Besides, Reid and Harrigan (2011) note that the anonymity and disintermediation of the blockchain have the potentials to harm the society through tax evasion, money laundering and other illegal activities. The technology has the potential to reshape the financial landscape, disrupt the existing business activities and render some professionals redundant. The extent to which the blockchain will disrupt the global financial services remain unknown as the technology is still evolving. The absence of empirical studies makes it difficult to examine the diffusion of innovation theory to the blockchain in this study.

6 Discussion and Conclusion

This study was conducted to explore the challenges posed by blockchain technology to forensic accountants in the prevention and detection of fraud in this digital age. It also examined the effects on the future of accounting and auditing, the technical skills required by accountants and the usefulness of DM as a fraud detection tool. From the available existing literature, blockchain can prevent and protect fraudulent activities because it encompasses the use of a cryptographic signature, distributed ledger, and P2P network. This study notes that blockchain cannot guarantee the genuineness of source documents since input determines the output. This finding provides clarifications on the research question: are there challenges posed by blockchain to forensic accountants in the prevention and detection of fraud? Despite the preventive technology mechanism like cryptography and P2P network, it is noted that the technology is not 100% immune to malicious attacks and hacking. This study buttresses the fact that the human and technical factors, which affect fraud prevention and detection system in other e-commerce innovations, could have an impact on the blockchain technology since the human element remains the weakest link in any setup. Where source documents are vulnerable, therefore, it means the output may not be reliable. This presents a problem for users of blockchain because the technology is expected to regulate itself without any external control authority. However, these challenges are not limited to the accountants, but also affect other stakeholders.

The DM techniques are known to be a robust fraud detection analysis tool, and its usage has been empirically studied by some researchers but mainly using hypothetical figures rather than real data. This research explored the use of DM technique in blockchain transactions since forensic accountants need to consider how to prevent and detect fraud using the existing fraud detection tools. Findings could not ascertain whether the DM techniques will be a useful analysis tool for transactions in the new technology, but there is a possibility that the techies can modify them for that purpose. The primary reason adduced is because the technology is still at the developmental stage and there is no empirical research to support the use of DM technique on blockchain. Forensic accountants in obtaining audit evidence will now need to explore how to prevent and detect fraud in blockchain transactions using the existing fraud detection tool or seek the assistance of IT experts.

The general notion by some researchers is that the impact of the blockchain is beyond the virtual currencies as it applies to any business that uses ledgers. This is responsible for the ongoing efforts by NASDAQ, IBM, MIT, financial institutions, the big four accounting firms, central banks of the UK and US, governments, ECB, IMF and OECD to harness its potentials applications. The current trials of blockchain technology include but are not limited to IPO, smart contracts, public records and health management, power generation, crowdfunding, land registry, and TSA. The general view is that with a distributed database, P2P network, computational logic, transparency, and irreversibility of records, blockchain can take over the primary core functions of accountants such as processing of transactions, tracking, reconciliation, and control. It has been argued that full automation of the external audit is feasible, thus leading to a significant reduction in the functions of auditors or possible elimination of the audit. It has been found that blockchain will affect the core functions of accountants, but the overall effects on the roles of forensic accountants and auditors are yet to be empirically ascertained. This study found that empirical support is required to determine what the auditor will review/examine in the blockchain.

The study further assessed the technical skills that forensic accountants need for effective fraud detection in blockchain transactions. This is because the continuous advancement in technology will require forensic accountants to up their technical competencies in this digital age. The investigation and detection of fraud need forensic accountants to embark on almost 100% analytical examination of manual and digital data. The reviewed literature noted that forensic accountants are proficient in the traditional core accounting skills: analytical, communication and knowledge of financial accounting, which, hitherto, are inadequate in a digital age. The general expectation is that for efficient operation in a digital age, forensic accountants need IT skills. The study buttressed this point by suggesting that the critical skills needed by forensic accountants are IT and AIS skills.

Apostolou et al. (2017) posit that one major problem of the digital age is implementing technology in educational programmes because technology develops exponentially. The study further considers the existing educational facilities in training accountants. The problem with the existing structures is that they are tailored to provide majorly traditional accounting skills. This study suggests that to explore the latest technological innovations such as AI, audit expert, algorithm and blockchain, forensic accountants and auditors need sound IT and AIS knowledge which includes IT Security issues, IT auditing, IT governance, computer-based analytical methods and fraud investigative auditing experience techniques. This led to another issue, which is how the accountants will obtain these skills. The study identifies that the IT and AIS skills can be acquired through a formal classroom setting, OJT and from professional studies, internship or combination in addition to their inclusion in the training programme, instructional techniques and academic curriculum of the various higher accounting institutions of learning and audit firms. The technicalities and the practicalities of dealing with the blockchain security are beyond the forensic accountant and auditor expertise. Alternatively, the study suggested that accountants can outsource the IT requirements to the IT experts. It is, however, important to weigh the implications or consequences of outsourcing IT needs of accountants to techies. It is equally necessary to examine whether accounting faculty are resistant to adopting the latest educational technologies. But, technologies evolve at an exponential rate, this could be among reasons the AACSB 2020 standards emphasize IT in its accreditation requirements. Similarly, audit and assurance firms are keeping pace with technology development by providing auditing education to enhance the understanding of their staff (Masoud, 2017) and professional accounting bodies have integrated IT into both the membership qualification examinations and continuing professional education courses for members.

The disruptive innovation of blockchain is found to be like the technological revolutions of the computer and the Internet. The blockchain technology could have an enormous impact on the future of the world economy as it may integrate with other emerging technologies like IoT, Big Data, cloud computing and AI. This study provides important evidence that the blockchain technology could modify the core functions of accountants and change the roles of an external auditor. The unintended consequences of blockchain as identified in this study could be in the form of the recent hacking into the Mt. Gox and DAO, Silk road, ransom, money laundering, Ponzi scheme and fraud. It could also harm the society through tax evasion, terrorist financing and dark web activities. The extent to which blockchain will disrupt the world economic system remains unclear and require further empirical studies since the technology is at an innovative stage. Empirically, the study cannot ascertain the relevance of the DM as a fraud analysis tool in the blockchain transactions.

The findings of this study contribute to the currently limited literature surrounding blockchain technology as it affects the accounting profession particularly the forensic accountants in fraud prevention and detection. This study reveals that blockchain is prone to malicious attack and cannot guarantee the correctness of source documents. This study cannot ascertain how to utilise DM techniques as a fraud analysis tool in a blockchain environment. Consequently, the study will be of assistance to forensic accountants in determining DM techniques appropriate for fraud analysis. This study indicates that the core characteristics of blockchain such as anonymity, decentralisation and P2P are also its limitations. On the one hand, these features make blockchain attractive to criminals, money-launders and terrorists while on the other hand, the regulatory authority may find it difficult to track suspicious transactions. This makes the technology features to be a double-edged sword. This study emphasises the need for empirical research to ascertain the likely practical implications blockchain will have on the accounting and auditing profession. The paper highlights some technical skills such as IT and AIS knowledge require by forensic accountants in this digital age. Such insight and the value gained from this information may assist academic, professional accounting firms and accountants, in general, implementing IT educational programmes.

This paper is limited in several ways. The chief among the constraints is the inadequate empirical studies on the blockchain technology, which address the challenges the technology posed to forensic accountants in the prevention and detection of fraud. The available studies dwell on the general applications of the technology as relating to the cryptocurrencies, financial services; accounting records and other potential areas, that blockchain could be applied. Other limitations are the reliance on the use of secondary data and the inability to engage professional accountants in a discussion through interview. The inability to conduct an interview does not have any significant impact on the research findings because some journalistic interviews conducted in the available magazines were analysed. Despite these limitations, the study attempts to fill the research gap by exploring available data on blockchain with emphasis on understanding the challenges posed to forensic accountants in the prevention and detection of fraud. Most of the data used are from journal articles, professional publications, releases from IMF and OECD, newspapers, magazines and online publications. The used secondary sources provide large representative samples and add depth to the research. It is important to note that information regarding the potential applications of the blockchain technology is published daily as breaking news.

Further empirical studies are required on: (a)What will the accountant audit in blockchain transactions? (b) What is the cost-benefit of outsourcing the IT aspects of financial activities to the IT experts to the accounting profession? (c) Is it feasible to use or modify the DM technique as a fraud analysis tool in the blockchain transactions? (d) How will dispute or conflict be resolved in a decentralised system like blockchain? and (e) How will the diffusion of innovation theory impact blockchain?

References

Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network & Computer Applications*, *68*, 90-113. https://doi.org/10.1016/j.jnca.2016.04.007

Ahmed, M., Mahmood, A. N., & Islam, M. R. (2016). A survey of anomaly detection techniques in financial domain. *Future Generation Computer Systems*, *55*, 278-288. https://doi.org/10.1016/j.future.2015.01.001

Alarcon, J., & Ng, C. (2018). Blockchain and the future of accounting. *Pennsylvania CPA Journal*, *88*(4), 26-29.

Angelis, J., & Ribeiro da Silva, E. (2019). Blockchain adoption: A value driver perspective. *Business Horizons*, *62*(3), 307-314. https://doi.org/10.1016/j.bushor.2018.12.001

Apostolou, B., Dorminey, J. W., Hassell, J. M., & Rebele, J. E. (2017). Accounting education literature review (2016). *Journal Of Accounting Education, 39*, 1-31. http://doi.org/10.1016/j.jaccedu.2017.03.001

Apostolou, B., Hassell, J. M., Rebele, J. E., & Watson, S. (2010). Accounting education literature review (2006–2009). *Journal of Accounting Education, 28*, 145-197. http://doi.org/10.1016/j.jaccedu.2011.08.001

ASQ. (2020). *What is Auditing? American Society for Quality*. Retrieved from https://asq.org/quality-resources/auditing

Association to Advance Collegiate Schools of Business. (2020). *2020 Standards for AACSB Business Accreditation.* Retrieved from https://www.aacsb.edu

Baer, M., Casal, F., Fornelli, C., Shamon, J., & Thompson, J. (2017). *Scoping out the audit of the future*. Retrieved from https://www.accountingtoday.com/news/scoping-out-the-audit-of-the-future

Bănărescu, A. (2015). Detecting and preventing fraud with data analytics. *Procedia Economics and Finance, 32*, 1827-1836. https://doi.org/10.1016/S2212-5671(15)01485-9

Bay, S., Kumaraswamy, K., Anderle, M. G., Kumar, R., & Steier, D. M. (2006). Large scale detection of irregularities in accounting data. *Sixth International Conference on Data Mining* (pp. 75-86). Hong Kong: IEEE. https://doi.org/10.1109/ICDM.2006.93

Bell, J., & Waters, S. (2014). *Doing your research: A guide for first-timer researchers* (6th ed.). Maidenhead, England: Open University Press.

Bhasin, M. L. (2015). Contribution of Forensic Accounting to corporate governance: An exploratory study of an Asian Country. *International Business Management*, *10*(4) http://doi.org/10.2139/ssrn.2676488

Biswas, B., & Gupta, R. (2019). Analysis of barriers to implement blockchain in industry and service sectors. *Computers & Industrial Engineering, 136*, 225-241. https://doi.org/10.1016/j.cie.2019.07.005

Bizarro, P., Mankowski, R., & Mankowski, H. (2018). Blockchain technology: benefits, risks, and the future. *Internal Auditing*, *33*(4), 12-16.

Boomer, L. (2017). Blockchain — hype or reality? *Accounting Today, 31*(7), 22.

Bradbury, D. (2016). Blockchain's big deal. *Engineering & Technology, 11*(10), 44-47. https://doi.org/10.1049/et.2016.1003

Brandon, D. (2016). The blockchain: The future of business information systems. *International Journal of the Academic Business World, 10*(2), 33-40

Bressler, L. (2011). Forensic investigation: The importance of accounting information systems. *International Journal of Business, Accounting, & Finance, 5*(1), 67-77. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=60073591&site=ehost-live&custid=s4804380

Burmester, M., & Mulholland, J. (2006). The advent of trusted computing: Implications for digital forensics. *ACM*, 283-287. https://doi.org/10.1145/1141277.1141344

Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: A perspective from blockchain technology. *Financial Innovation, 2*(1), 1-10. https://doi.org/10.1186/s40854-016-0039-4

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36*, 55-81. https://doi.org/10.1016/j.tele.2018.11.006

Collis, J., & Hussey, R. (2009). *Business research: A practical guide for undergraduate & postgraduate students*. New York, NY: Palgrave Macmillan

Davis, C., Farrell, R., & Ogilby, S. (2008). *Characteristics and Skills of the Forensic Accountants (AICPA Report).* Retrieved from http://thefraudgroupllc.com/tools/library/documents/forensic.pdf

de Meijer, C. R. W. (2016). Blockchain and the securities industry: Towards a new ecosystem. *Journal of Securities Operations & Custody, 8*(4), 322-329

Deepak, S. (2019). *Use data analytics for fraud prevention and detection.* Retrieved from https://www.techaheadcorp.com/blog/data-analytics-fraud-prevention/

Digabriele, J. A. (2008). An empirical investigation of the relevant skills of Forensic Accountants. *Journal of Education for Business, 83*(6), 331-338. https://doi.org/10.3200/JOEB.83.6.331-338

DiGabriele, J. A. (2016). The expectation differences among stakeholders in the financial valuation fitness of auditors. *Journal of Applied Accounting Research, 17*(1), 43-60. 10.1108/JAAR-06-2013-0043

Estévez, P. A., Held, C. M., & Perez, C. A. (2006). Subscription fraud prevention in telecommunications using fuzzy rules and neural networks. *Expert Systems With Applications, 31*(2), 337-344. https://doi.org/10.1016/j.eswa.2005.09.028

Fanning, K., & Centers, D. P. (2016). Blockchain and its coming impact on financial services. *Journal of Corporate Accounting & Finance, 27*(5), 53-57. 10.1002/jcaf.22179

Gbegi, D., & Adebisi, J. (2014). Forensic accounting skills and techniques in fraud investigation in the Nigerian Public Sector. *Mediterranean Journal of Social Sciences*, *5*(3), 242-253. http://doi.org/10.5901/mjss.2014.v5n3p243

Gillon, K. (2017). *Artificial intelligence and the future of accountancy.* Retrieved from https://ion.icaew.com/technews/b/weblog/posts/artificial-intelligence-and-the-future-of-accountancy

Han, J., Kamber, M., & Pei, J. (2012). *Data Mining: Concepts and Techniques* (3rd ed.). London, United Kingdom: Morgan Kaufmann.

Hannink, L. (2013). Examining financial statement fraud: Causes, warning signs, and the future. *International Journal of Economics and Accounting, 4*(3) 10.1504/IJEA.2013.055891

Hazlett, T. W. (2016). Understanding the disruptive innovation wrought by computers and the internet: A review. *International Journal of the Economics of Business, 23*(3), 391-408. https://doi.org/10.1080/13571516.2016.1220472

Houck, M., Morris, B., & Riley, R. (2006). Forensic Accounting as an Investigative Tool: Developing a model curriculum for fraud and forensic accounting. *The CPA Journal, 76*(8), 68-70.

Huberman, G., Leshno, J., & Moallemi, C. C. (2017). *Monopoly without a monopolist: An economic analysis of the Bitcoin payment system*. Bank of Finland Research Discussion Paper No 27/2017. Retrieved from https://ssrn.com/abstract=3032375

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review, 95*(1), 118-127. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=heh&AN=120355131&site=ehost-live&custid=s4804380

Jackson, R. A. (2004). Get the most out of audit tools. *Internal Auditor, 61*(4), 36-47. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=14037941&site=ehost-live&custid=s4804380

Janvrin, D. J., & Watson, W. M. (2017). "Big Data": A new twist to accounting. *Journal of Accounting Education, 38*, 3-8. https://doi.org/10.1016/j.jaccedu.2016.12.009

Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P.-E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. *Expert Systems with Applications, 100*, 234-245. https://doi.org/10.1016/j.eswa.2018.01.037

Kearns, G. (2010). Computer Forensics for Graduate Accountants: A Motivational Curriculum Design Approach. *Proceedings of the Conference on Digital Forensics, Security and Law*, 141-157.

Kiviat, T. I. (2015). Beyond bitcoin: Issues in regulating blockchain transactions. *Duke Law Journal, 65*(3), 569-608

Kotsiantis, S., Koumanakos, E., Tzelepis, D., & Tampakas, V. (2006). Forecasting fraudulent financial statements using data mining. *International journal of computational intelligence, 3*(2), 104-110

Kou, Y., Lu, C.-T., Sirwongwattana, S., & Huang, Y.-P. (2004). Survey of fraud detection techniques *IEEE International Conference on Networking, Sensing and Control, 2004* (pp. 749-754). Taipei, Taiwan: https://doi.org/10.1109/ICNSC.2004.1297040

Kreuter, E. (2017). Forensic Accounting: A value-adding skill for the CPA: Certified Public Accountant. *The CPA Journal, 87*(11), 6-8.

Lin, C.-C., Chiu, A.-A., Huang, S. Y., & Yen, D. C. (2015). Detecting the financial statement fraud: The analysis of the differences between data mining techniques and experts' judgments. *Knowledge-Based Systems, 89*, 459-470. https://doi.org/10.1016/j.knosys.2015.08.011

Lin, G. (2009). Higher education research methodology: Literature method. *International Education Studies, 2*(4), 179-181. Retrieved from https://files.eric.ed.gov/fulltext/EJ1065734.pdf

Mann, T. (1998). *The Oxford guide to library research*: Oxford University Press, USA.

Marechaux, J. L. (2019). *Towards advanced Artificial Intelligence using blockchain technologies.* Retrieved from https://blockchain.ieee.org/technicalbriefs/march-2019/towards-advanced-artificial-intelligence-using-blockchain-technologies?highlight=WyJpbmR1c3RyeSIsImluZHVzdHJ5J3MiXQ==

Markelevich, A. (2018). What is blockchain technology? *Accounting Education News, 46*(4), 20.

Martindale, N. (2016, July 20). *How blockchain will impact accountants and auditors.* Retrieved from http://economia.icaew.com/features/july-2016/how-blockchain-will-impact-accountants-and-auditors

Marvin, R. (2017). *Blockchain: The invisible tech that's changing the World.* Retrieved from https://au.pcmag.com/features/46389/blockchain-the-invisible-technology-thats-changing-the-world

Masoud, N. (2017). Audit expectation gap among undergraduate accounting students at Jordanian Universities. *The Journal of Private Equity, 20*(2), 73-89. http://dx.doi.org/10.3905/jpe.2017.20.2.073

Maupin, J. (2017). Blockchains and the G20: Building an inclusive, transparent and accountable digital economy. https://doi.org/10.2139/ssrn.2935261

Maurer, B., Nelms, T., & Swartz, L. (2013). "When perhaps the real problem is money itself!": The practical materiality of Bitcoin. *Social Semiotics, 23*(2), 261-277. https://doi.org/10.1080/10350330.2013.777594

McCallig, J., Robb, A., & Rohde, F. (2019). Establishing the representational faithfulness of financial accounting information using multiparty security, network analysis and a blockchain. *International Journal of Accounting Information Systems, 33*, 47-58. https://doi.org/10.1016/j.accinf.2019.03.004

McKinney, E., Yoos, C. J., & Snead, K. (2017). The need for ‘skeptical’ accountants in the era of Big Data. *Journal of Accounting Education*, *38*, 63-80. https://doi.org/10.1016/j.jaccedu.2016.12.007

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2016). A fistful of Bitcoins: Characterizing payments among men with no names. *Communications of the ACM*, *59*(4), 86-93. https://doi.org/10.1145/2896384

Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). Zerocoin: Anonymous distributed e-cash from bitcoin *2013 IEEE Symposium on Security and Privacy* (pp. 397-411): https://doi.org/10.1109/SP.2013.34

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, *50*(3), 559-569. https://doi.org/10.1016/j.dss.2010.08.006

Ngo, D. (2016). *How blockchain technology can enhance fraud detection.* Retrieved from http://coinjournal.net/how-blockchain-technology-can-enhance-fraud-detection-interview-with-feedzais-cto/

Nickerson, M. A. (2019). Fraud in a World of Advanced Technologies. *CPA Journal*, *89*(6), 28-34.

Nowiński, W., & Kozma, M. (2017). How can blockchain technology disrupt the existing business models? *Entrepreneurial Business and Economics Review*, *5*(3), 173-188. https://doi.org/10.15678/EBER.2017.050309

Pan, G., & Seow, P.-S. (2016). Preparing accounting graduates for digital revolution: A critical review of information technology competencies and skills development. *Journal of Education for Business*, *91*(3), 166-175. 10.1080/08832323.2016.1145622

Pearson, T. A., & Singleton, T. W. (2008). Fraud and forensic accounting in the digital environment. *Issues in Accounting Education*, *23*(4), 545-559. https://doi.org/10.2308/iace.2008.23.4.545

Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In P. Tasca, T. Aste, L. Pelizzon & N. Perony (Eds.), *Banking beyond bank and money* (pp. 239-278). Retrieved from http://arxiv.org/abs/1511.05740

Ramaswamy, V. (2005). Corporate governance and the Forensic Accountant. *The CPA Journal*, *75*(3), 68-70.

Reid, F., & Harrigan, M. (2011). An Analysis of Anonymity in the Bitcoin System *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing* (pp. 1318-1326). Boston, MA: https://doi.org/10.1109/PASSAT/SocialCom.2011.79

Sarda, P., Chowdhury, M. J. M., Colman, A., Kabir, M. A., & Han, J. (2018). Blockchain for fraud prevention: A work history fraud prevention system *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 1858-1863): https://doi.org/10.1109/TrustCom/BigDataSE.2018.00281

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students* (7th ed.). Colchester, England: Pearson.

Schmitz, J., & Leoni, G. (2019). Accounting and auditing at the time of blockchain technology: A research agenda. *Australian Accounting Review, 29*(2), 331-342. https://doi.org/10.1111/auar.12286

Seetharaman, A., Senthilvelmurugan, M., & Rajan, P. (2004). Anatomy of computer accounting frauds. *Managerial Auditing Journal, 19*(8), 1055-1072. https://doi.org/10.1108/02686900410557953

Sharma, A., & Panigrahi, P. K. (2012). A review of financial accounting fraud detection based on data mining techniques. *International Journal of Computer Applications, 39*(1), 37-47. Retrieved from https://arxiv.org/ftp/arxiv/papers/1309/1309.3944.pdf

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. Beijing, China: O'Reilly Media.

Tan, B. S., & Low, K. Y. (2019). Blockchain as the database engine in the accounting system. *Australian Accounting Review, 29*(2), 312-318. https://doi.org/10.1111/auar.12278

Tapscott, D., & Tapscott, A. (2016). The impact of the blockchain goes beyond financial services. *Harvard Business Review, May 10*, 2-5.

Tapscott, D., & Tapscott, A. (2017). How blockchain will change organizations. *MIT Sloan Management Review, 58*(2), 10-13. Retrieved from http://mitsmr.com/2gbIHrI

The-Guardian. (2017, July 1). UK dealer charged in US over multimillion-dollar fake Bitcoin site scam. Retrieved from https://amp.theguardian.com/technology/2017/jul/01/bitcoin-fake-site-uk-dealer-charged-us-multimillion-dollar-scam11/08/2017

The Guardian. (2017, February 21, February 21). British serial entrepreneur missing as $1.4m Bitcoin is apparently stolen. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2014/oct/23/british-serial-entrepreneur-missing-bitcoin-apparently-stolen

Treiblmaier, H., & Beck, R. (2019). *Business transformation through blockchain : Volume II*. Cham: Cham: Palgrave Macmillan US.

Vigna, P., & Casey, J. (2016). *The age of Cryptocurrency: How Bitcoins and the blockchain are challenging the global economic order*. New York, NY: Picardor.

Viriyasitavat, W., & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial*

Information Integration, *13*, 32-39. https://doi.org/10.1016/j.jii.2018.07.004

Wang, L., Shen, X., Li, J., Shao, J., & Yang, Y. (2019). Cryptographic primitives in blockchains. *Journal of Network and Computer Applications*, *127*, 43-58. https://doi.org/10.1016/j.jnca.2018.11.003

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security*, *57*, 47-66. https://doi.org/10.1016/j.cose.2015.09.005

Xu, J. J. (2016). Are blockchains immune to all malicious attacks? *Financial Innovation*, *2*(1), 25. https://doi.org/10.1186/s40854-016-0046-5

Xu, X., Lu, Q., Liu, Y., Zhu, L., Yao, H., & Vasilakos, A. V. (2019). Designing blockchain-based applications: A case study for imported product traceability. *Future Generation Computer Systems*, *92*, 399-406. https://doi.org/10.1016/j.future.2018.10.010

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), 1-27. https://doi.org/10.1371/journal.pone.0163477

Yufeng, K., Chang-Tien, L., Sirwongwattana, S., & Yo-Ping, H. (2004). Survey of fraud detection techniques. *In IEEE International Conference on Networking, Sensing and Control, 2004* (pp. 749-754). Taipei, Taiwan: https://doi.org/10.1109/ICNSC.2004.1297040

Zachariadis, M., Hileman, G., & Scott, S. V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. *Information & Organization*, *29*(2), 105-117. https://doi.org/10.1016/j.infoandorg.2019.03.001

Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation*, *2*(1), 28. https://doi.org/10.1186/s40854-016-0049-2

Zhu, H., & Zhou, Z. Z. (2016). Analysis and outlook of applications of blockchain technology to equity crowdfunding in China. *Financial Innovation*, *2*(1), 29. https://doi.org/10.1186/s40854-016-0044-7

Zimbelman, M. F., Albrecht, C. C., Albrecht, W. S., & Albrecht, C. (2012). *Forensic Accounting, International Edition* (4th ed.). United Kingdom: Cengage Learning.

Zouina, M., & Outtai, B. (2019). Towards a distributed token based payment system using blockchain technology *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)* (pp. 1-10): https://doi.org/10.1109/COMMNET.2019.8742380