Blockchain technology in the future of business cyber security

Article *in* Journal of Management Analytics · February 2020

DOI: 10.1080/23270012.2020.1731721

3 authors, including:

Sebahattin Demirkan

29 PUBLICATIONS **254** CITATIONS

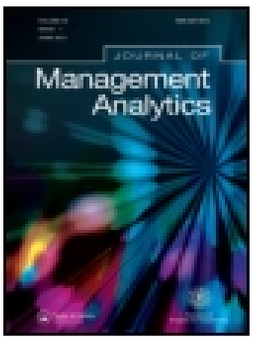
SEE PROFILE

Irem Demirkan

Loyola University Maryland

23 PUBLICATIONS **576** CITATIONS

SEE PROFILE



Journal of Management Analytics

ISSN: 2327-0012 (Print) 2327-0039 (Online) Journal homepage: https://www.tandfonline.com/loi/tjma20

Blockchain technology in the future of business cyber security and accounting

Sebahattin Demirkan, Irem Demirkan & Andrew McKee

To cite this article: Sebahattin Demirkan, Irem Demirkan & Andrew McKee (2020): Blockchain technology in the future of business cyber security and accounting, Journal of Management Analytics, DOI: 10.1080/23270012.2020.1731721

To link to this article: https://doi.org/10.1080/23270012.2020.1731721

Published online: 26 Feb 2020.

Journal of Management Analytics, 2020
https://doi.org/10.1080/23270012.2020.1731721

REVIEW

Blockchain technology in the future of business cyber security and accounting

Sebahattin Demirkan [a*], Irem Demirkan [b] and Andrew McKee[c]

[a]*The O'Malley School of Business, Manhattan College, New York, NY, USA;* [b]*Sellinger School of Business, Loyola University Maryland, Baltimore, MD, USA;* [c]*PKF O'Connor Davies, New York, NY, USA*

(*Received 26 September 2019; revised 9 February 2020; accepted 15 February 2020*)

This study looks into the current, and potential uses of Blockchain technology in business, specifically in Accounting and in cybersecurity. We relate Blockchain uses to current concerns within cybersecurity and accounting. We review the literature that includes topics such as Big Data in Accounting, blockchain's use in financial security and cybersecurity, and its use in financial accounting though the use of ledger technology and also as a system of tracking financial misconduct. We also review the Department of Homeland Security plan for cybersecurity over the next few years to understand what the US Government plans because of the importance of cybersecurity development. We show that Blockchain impacts auditing in different ways that will change the profession drastically. We also find that blockchain should be effectively implemented into different aspects of cybersecurity, and accounting, such as Auditing and general accounting procedures.

Keywords: blockchain; business; cybersecurity; accounting; big data; Department of Homeland Security

1. Introduction

Technology in the world has been changing at an unprecedented rate. This is a trend that will only continue at an increasing rate in the future years as great minds continue to develop things to make everyday life simpler and accessible to everyone. While this trend continues, changes will be rampant not only in everyday life, but also in the business world entirely. The technology has already erupted and been able to allow the businesses to accelerate to different levels of profitability and competitiveness.

As recent developments, for example, artificial intelligence and machine learning has changed not only the business landscape in terms of innovative products and technologies but also has impacted the decision making as an opportunity for business leaders to elevate lawyers to contribute further to corporate strategies and operations (Tung, 2019) and blockchain technologies are disrupting the banking industry (Hassani, Huang, & Silva, 2018; Higginson, Hilal, & Yoguc, 2019) among others such as healthcare, law, supply chain, and accounting (Frizzo-Barker et al., 2019).

While these technological advancements, specifically the blockchain technologies have allowed the accounting profession to develop further and, on the way, to establish

*Corresponding author. Email: sdemirkan@manhattan.edu; sdemirkan@gmail.com

blockchain-based accounting practices as a possible future for business information systems (Andersen, 2016; Brandon, 2016), they also raised concerns for many different companies regarding the overall cybersecurity. Advancements in the accounting area have been through the use of more specialized accounting software and cloud-based systems. Firms' clients also have become more diverse technologically. However, these advancements have come with challenges since company's cybersecurity plan now must be so evolved to try to avoid millions of dollars and private/confidential information loss because of the cybersecurity data breaches. Most of the different layers of accounting in general get affected when a new technology is adopted into use, within a company or an industry. One of the more effective technologies that is currently being adopted into the accounting field and potentially into the realm of cybersecurity.

Accordingly, in this paper we study the current, and potential uses of Blockchain technology in business, specifically in Accounting and we discuss related issues in Cybersecurity. We also relate Blockchain uses to current concerns within cybersecurity and accounting. Similarly, to Hassani, Huang, and Silva's statements in their 2018 article where they look into the development of blockchain technology for banking, despite developments in blockchain technology in accounting area in practice there is a gap in the literature from more academic perspective and this gap, we suggest, may impede the academics to lead the way and propose policies to the practice and further development of blockchain technologies in accounting area. Accordingly, this study aims to fill this void in the literature and to contribute to previous studies that offer big picture perspectives on blockchain technologies' impact on accounting (such as Coyne & McMickle, 2017; Lu, 2018a, 2018b) and offer insights on cybersecurity issues that these potential developments bring.

In the next section, we discuss what blockchain technology is, followed by how it relates to accounting. Then we open up the discussion of cybersecurity concerns that parallels the use of more technology such as the blockchain and discuss the validity of such concerns and we exemplify how the Department of Homeland Security approaches those concerns. In the following sections we include a more in-depth look at the blockchain technology and accounting specifically by reviewing topics such as big data in accounting, blockchain's use in financial security and cybersecurity, and its use in financial accounting through the use of ledger technology and also as a system of tracking financial misconduct. Overall, in this paper we document that while blockchain technology offers so many opportunities through its use in accounting, it also impacts accounting practices in areas of auditing in different ways that will change the profession drastically (Deloitte, 2016a, 2016b, 2016c). We also observe that blockchain should be effectively implemented into different aspects of cybersecurity, and accounting, such as Auditing and general accounting procedures to make the transition applicable to all industries.

2. Literature review

2.1. *Blockchain technology*

A blockchain is essentially a digital decentralized ledger that consists of blocks of transactions between parties. Crosby, Pattanayak, Verma, and Kalyanaraman (2016, p. 8) define blockchain as "distributed database of records, or public ledger

of all transactions or digital events that have been executed and shared among participating parties". Blockchain has no central control, and has great potential benefits for many industries (Al-Jaroodi & Mohamed, 2019). The technology itself does not rely on third party members. Blockchain was introduced to the world in 2008, and over the following years it started to catch popularity in use due to its efficiency, and its high level of security. This high level of security comes from the fact that to change anything in a blockchain, a majority of all parties to transactions in subsequent blocks within the chain need to agree to the change and blockchains use sophisticated math and innovative software technologies that is mostly hard to manipulate (Orcutt, 2018). This makes the blockchain technology appealing and interesting, because it makes the verification process easy that speeds up the transaction process overall.

Across the globe there are two major categories of the blockchain accounting including public blockchains where every person has the access to the network and there is no network required to participate in the blockchain activities and transactions and private blockchains that are more private and complex form of accounting in which the permission must be granted to an external person in order to join the groups. Private Blockchains may be formed by the firms and organizations working in a particular industry and may require authentication (Piscini, 2017). For example, Perera, Nanayakkara, Rodrigo, Senaratne, and Weinand (2020) suggest that private blockchain networks can provide trustworthy business software solutions to the construction industry since construction industry work with sensitive data.

One of the most popular uses of blockchain is the use of blockchain in cryptocurrency, specifically Bitcoin which is the application of public blockchain type. Lu (2018a) surveys IEEE papers and proceedings to document the broad range of practical applications, because blockchain is more than just Bitcoin. While Bitcoin, is not the starting point for blockchain it definitely ignited the content of blockchain to the level that it is in use today. Blockchain, as a technology on its own, is more interesting and profound innovation than that of Bitcoin (Kaushal & Tyle, 2016). Bitcoin is an application that runs on the blockchain and similarly, blockchain is used as the Hyperledger since the beginning of 2015.

The Hyperledger is an enterprise-based ledger that is based on blockchain technology and is used to support all the blockchain based distributed ledgers (Lu, 2018a). Hyperledger is designed for enterprise-level blockchain applications and introduces member management services ensuring data security and trust among users. The goal of the use of Hyperledger (or the Hyperledger project) is to support blockchain technology and transform and advance global business transactions (Cachin, 2016; Kokina, Mancha, & Pachamanova, 2017).

The development of Blockchain can be classified under the three streams of Blockchain 1.0, 2.0, and 3.0 (Lu, 2018a, 2018b; Zhang & Jacobsen, 2018). Blockchain 1.0, is the first stream, which is where most people would identify as the most popular. It is made up of mostly cryptocurrencies, including Bitcoin in the capital markets, examples are Bitcoin, Litecoin, Ethereum, etc. Blockchain 2.0, includes the distribution ledger agreements and the other base technologies, such as smart contracts and other protocols. Blockchain 3.0 can be considered as the "future of the blockchain", meaning what else it may be able to do for us as a society. The use of this technology will impact human life in a multitude of different ways. Blockchain 3.0 is beyond 1.0 and 2.0 and it includes applications such as the domain name, digital identity, eGovernment, smart cities, and online electronic voting among others (Dogo,

Nwulu, Olaniyi, Aigbavboa, & Nkonyana, 2018). Identifying Blockchain 1.0 through 3.0 and beyond is significant in understanding what kind of cybersecurity issues these technologies will face with.

2.2. *Blockchain technology and accounting*

Dramatic changes in accounting area has occurred with the introduction of software capable of producing different information and keeping records of transactions. At the preliminary stages of its use, the use of software gradually expanded in to a decentralized system using internet from limited or centralized system of accounting (Gautham, 2017). As Blockchain technologies have evolved Blockchain accounting has been introduced to help professionals and keep tracking of orders in "blocks" in a secured manner. Through blockchain not only we can not only record the transactions but also verify the transactions without the intervention or need for an intermediary, the technology is completely based on automated system (Kwilinski, 2019; Walch, 2016). This also eliminates the errors that occur due to intermediary, it cuts out intermediaries and eliminates the need for paying out commissions and other secondary transactions to other people. Also, anyone can see what transactions have occurred and it is completely transparent and verified by thousands of computers at a time (Rosic, 2019). Moreover, the blockchain algorithms that are used in accounting enable the collaborative creation of a digital ecosystem with more properties and capabilities that go far beyond what is used today, i.e. the traditional ledgers (Watson & Mishler, 2017). These show that blockchain technologies will benefit and have positive impact on real time accounting practices (Byström, 2019).

The global economy is about to experience revolutionary changes in different domains and multiple industries (Dai & Vasarhelyi, 2017). The expansion of this blockchain accounting is expected to occur because of vast internet infrastructure present everywhere and the potential is expected to reshape the finance and accounting practices of healthcare, public institutions, manufacturing, energy, and financial companies in a disruptive manner (Kokina et al., 2017). There are so many interdependencies not only among competitors but also among companies operating along the value chain of the industry. Given this, businesses are also motivated to enhance the operation dependency of the organizations and companies. The major ones include safe and sound environment for financing and accounting, transparency in the processes, minimal risk and resilience from the external threats, better and in-depth accountability and most importantly efficiency. The market analysts have predicted a more massive increase in the utility of blockchain accounting in the coming five years as the year 2016 has been a remarkable witness of immense investment in this field reaching at about $1 billion (Deloitte, 2017). The major contributors towards the exponential growth of the blockchain technologies are the financial service firms and technology-oriented organizations (Piscini, 2017). This growth is mainly due to the real time and reliable updates that blockchain technology enables in decentralized public ledgers. This in turn enables companies to view the entire history of transactions in this ledger and hence timely, reliable, and trustworthy updates that minimizes human errors that occur when reconciling complex information from multiple sources (Deloitte, 2016a, 2016b, 2016c).

However, on the negative side of this new blockchain accounting, business network always remains quite high because of the cyberattacks. The future

and fortune of many mega companies across the globe now depend on their capabilities to protect themselves from such external threats. Most of such attacks are always focused on getting access to the intimate information about the transactions and financial resources occupied by any firms or any individuals (Voices, n.d.). The threatening situation asks for an international scale collaboration of the involved businesses and parties to join hands and share expertise in the best favor of making block chain accounting more protective (Barzilay, 2017).

2.3. *Cybersecurity*

As blockchain technology is utilized more in accounting and other areas in the firm, the issues related to cybersecurity is becoming more important (Gordon, Loeb, Sohail, Tseng, & Zhou, 2008). The biggest question today on the corporate level for a company when concerning their cybersecurity is not if they should be investing in their cybersecurity, but how much they should be investing into their cyber level security to ensure safety for not only their data, but their network as a whole (Gordon, Loeb, & Zhou, 2016). This suggestion can be backed up by the data that recently, 61% of all small businesses or mid-sized businesses experienced a cyber-attack in 2017 (Carfagno, 2019). Cyber Security attacks today have become so common that it is no longer characterized as an "if it" is going to happen but it is now a "when will it" happen. There are many theories proposed to explain the individual security intentions and actual behaviors in information technology environment such as general deterrence theory, protection motivation theory, theory of planned behavior, rational choice theory and naturalization theory (Donaldson & Osei-Bryson, 2020). However, Lu (2018c) states that all these models and theories are focused on extrinsic or perceived factors, not in intrinsic factors such as decision styles that may also explain the behaviors which would be essential in blockchain environment. Even with this now as the mindset of people in their personal and professional lives, businesses and people are still lacking their own ability of being prepared for these types of cyber-attacks. 86% of businesses that were part of a survey done by a cyber-security company admitted to feeling and knowing that their cybersecurity system that was currently in place was underprepared for what could happen in the present or in the future.

Companies must be more prepared to defend themselves against cyber criminals. These people who will involve themselves in cybercrime, are attacking companies looking to get a piece of any information they can from the company to potentially gain profit for themselves. Currently, many banks and other financial institutions are looking into and implementing blockchain security systems that are reducing risk and cyber threats and fraud. The NASDAQ recently announced a plan to launch a Blockchain based digital ledger which allows them to boost their equity management capabilities (Singh & Singh, 2016). This shows that the NASDAQ is concerned for their cyber security of themselves and their clients going forward for the future. While these later systems are less prone to cyberattacks that could bring down the entire network, security issues in Blockchain 3.0 technology are still critical since a cyber-attacker, if successful, would access the information stored not only at one point but also to all information in the digital ledger (Hasanova, Baek, Shin, Cho, & Kim, 2019).

Cyber criminals could gain profit from getting into the company network and system in many different ways depending on what type of entry or what type of information they are attempting to get out of a person or the company. Blackstratus, a company in the industry of cybersecurity, broke down the top 5 cybersecurity threats that people are facing today. The threats go on as Malware, Phishing, Ransomware, Fileless Attacks, and Human Error (Carfagno, 2019). We look into detail this top five cybersecurity there. First one is *Malware* that represents a huge part of the cyber scam population. These types of viruses enter and then aim to disrupt and disable a computer system. 90% of malware is delivered via email and is usually hidden as something else when an employee is opening it. The average cost of malware attacks to companies is $2.4 Million (Statistics, 2019). Second one is *Phishing* which is another top ranked threat faced by organizations. Advanced phishing schemes mirror the layout and communications of trusted businesses and common businesses you interact with. They are aimed to collect extra sensitive data from your organization. Average cost of lost or stolen data, due to data breach or phishing to companies is $150 per record (IBM, 2019).

Third one is *ransomware* which is the most rapid-paced and prevalent of cybersecurity threats lodged at organizations, with the usual intent of shutting down servers or holding data and files hostage until a suitable ransom is paid. Attacks strike every 14 s. Without a data backup, can cost businesses approx. $11.5 Billion in 2019 (Freeze, 2018). These are portrayed as one of the deadlier attacks a company or person could face. Forth one is *Fileless Attacks* that exploit applications or even operating systems already installed in a device. Nearly 77% of 2017s known compromised attacks were fileless. They can cost roughly $5 million when executed properly and fully. Final one is *Human errors* that are usually unintended disclosures, accidental data deletions or improper disposals of sensitive files all fall under human errors, a common yet under-the-radar enterprise threat. They are able to be corrected with cybersecurity awareness training for your employees. About $148 per compromised record, and is lengthy to uncover. It is hard for a company to recover from data breaches, reputation wise. Consumers will be less likely to trust you with their data if they are part of your data breach. Companies that are proactively protecting their company data and consumer data increase their reputation. Due to all of this, companies have to be more self-aware as to what they have to do to do better in their cybersecurity. They also have to know the benefits of investing in their cyber security.

The cyberattacks on blockchain technology have shown that this technology is no exception when it comes to cyber-attacks. However, through Blockchain 1.0–3.0 all cyberattacks have resulted in enhancements to the bitcoin technology. Blockchain 1.0, involving Bitcoin for example is not a perfectly fungible system, because some coins may be linked to accounts that are used for fraudulent activities. But as systems develop newer systems can address these concerns by introducing "mixer" networks to hide the transaction history (Zhang & Jacobsen, 2018). While Hyperledger fabric since built on later technologies, includes such built-in enhancements (see Hasanova et al., 2019, pp. 13–14, for a detailed description of how this technology can include specific security flaws) it still requires moderate attention based on the risk profile, initial security concerns, and other vulnerabilities identified at the point of engagement and that it may not be indestructible (Brett, 2018; Hasanova et al., 2019, p. 14).

2.3.1. *Cybersecurity lessons from the Department of Homeland Security (DHS)*

Since the internet, and all of the uses of it, have become such integral parts of everyone's daily social life, and professional life, and has risen to somewhat a basic need for the modern day person, having the government looking for security guidelines for cyberspace is crucial for the future. Given these challenges discussed above in the literature review section, many companies, institutions, and governments are attempting to develop their new plan for cybersecurity or ways to ensure cyber security for the next coming generation. The DHS for the United States has come up with their set of guidelines for the upcoming years, with their five-year cybersecurity plan. This plan provides the Department with a framework to execute our cybersecurity responsibilities during the next five years to keep pace with the evolving cyber risk landscape by (a) reducing vulnerabilities and building resilience; (b) countering malicious actors in cyberspace; (c) responding to incidents; and (d) making the cyber ecosystem more secure and resilient. The DHS identified five separate pillars that show how they would approach their cybersecurity Risk Management Approach. Within these five pillars they have set up seven goals throughout. The department is working to ensure the availability of critical national function to foster efficiency, innovation, trustworthy communication, and economic prosperity in ways consistent with our national values and that protect privacy and civil liberties (DHS, p. 3).

The first pillar is *Risk identification*. The DHS will be assessing the evolving cybersecurity risks. Through this, the department states that they must be "Understanding trends in threats, vulnerabilities, interdependencies, and potential consequences over time will allow DHS to prioritize our protective, investigative, and response activities, and to plan and budget appropriately." (DHS, 2018, p. 7). This will allow the department to understand the national risks we have to cybersecurity. It allows them to begin to adjust their program and different policies over the next five years to adjust for the evolving technologies, such as blockchain and the artificial intelligence (AI), that are being shifted more into mainstream use every year. The second pillar is named *Vulnerability reduction*. This pillar has the goal to protect the federal government information systems (DHS, 2018). Through this goal, the department would be able to increase their own cybersecurity for federal agencies through different practices, with the end goal being an overall greater level of security. Implementing framework for their process is key to ensuring the success of the project. The department will also track the performance of the next goals by tracking the use of their tools and services within their initial framework.

The third goal for the government is *to protect their critical infrastructure.* To do this, they lay out an objective to "improve cybersecurity capabilities and resources available to sector specific agencies, regulators, and policymakers." (DHS, 2018, p. 14). This will allow for each of the sectors under the department to be aware of the risk they will face to their cyber network. Given this, the sectors would be self-sufficient and maintain their own policies to support their risk management. The remainder of the goals for the DHS are listed as "Prevent and disrupt criminal use of cyberspace, respond effectively to Cyber Incidents, Strengthen the security and reliability of the Cyber Ecosystem, and Improve management of DHS cybersecurity activities" (DHS, 2018).

The DHS lays out plans to achieve these goals, and how they will effectively be able to complete their goals. Similarly, businesses should be proactive and should also be

looking to lay out plans of how their cybersecurity should be of a top pray for them, and how they will be able to protect their assets under the blockchain technologies and set up preventive measures. Blockchain technologies will surely, amid not entirely, alleviate the cybersecurity attacks while at the same time provide anonymity, and data integrity (Yli-Huumo, Ko, Choi, Park, & Smolander, 2016). In other words, Blockchain technologies can very well become a company's successful security framework.

2.4. *Blockchain as a cybersecurity framework*

Blockchain is emerging as one of the more reliable and powerful technologies for cyber security. The normal of today, which we have been doing for years now, is that when dealing with information exchange or the transfer of money and assets through online transactions via the internet, it will be going through a trusted intermediary. The intermediaries are responsible for ensuring the secure exchange and are then also liable for any problems that may occur during the transaction, including security breaches. Through the use of blockchain, the need for these central authorities between two parties is made obsolete because of being able to use Blockchain incorruptible, reliable, and decentralized public ledger (Puthal, 2018, p. 18). The use of blockchain technology here allows for people not to have to rely on outside third parties to ensure the safety of their transactions, or other dangers in their interactions with other parties.

Given the concerns for cybersecurity in the future and the plans that the United States Government is looking to implement over the next five years, companies may turn to blockchain to use as part of their security framework. While there is no consensus on the exact amount of how much should companies invest into cybersecurity some industry experts suggest that robust investments in cybersecurity should not fall below three percent of a company's total capital expenditures (Carfagno, 2019). Companies should treat their cybersecurity policies and technologies like they do any investment, meaning fluid, long-term, performance-driven, and with quantifiable goals. Cybersecurity is something that can be developed in the future for companies because of the implementation of blockchain technologies. "Blockchain is touted as a technology that can provide a robust and strong cybersecurity solution and high level of privacy protection … " (Kshetri, 2017, p. 1). As pointed out before, the overall security of blockchain is significantly higher than existing remedies, investing towards blockchain technologies should be an important strategic move for a company.

The blockchain is a safe alternative to allowing these transactions to occur while at the same time cutting out the middle company. This is because the blockchain general ledger database is a tamper proof, secure, and permanent record of the business between the two parties (Li, Jiang, Chen, Luo, & Wen, 2017). Once the transaction is approved by the participants in the exchange, it is added to the blockchain, and it cannot be edited, altered, or removed without the approval of the all parties in the chain. The blockchain is an irreversible system. By using blockchain, it not only reduces the cost of business but also eliminates the possibility of loss information because of a single point of failure by one of the parties involved, since the ledger is constantly synchronized across all of the participants (Puthal, 2018, p. 19). This is exactly why the blockchain is such an incredible technology for cyber security and reliability when it comes to replacing the current status quo for transactions.

The blockchain is able to ensure privacy and protection at all times. As noted in his article, Puthal (2018) states that an industry must be analyzed and make sure that blockchain would be the proper technology to be put in use. He suggests that only under the following situations should organizations consider the idea of deploying a blockchain based security situation. The first one is where people will rely on an outside third party for transactions. The second, involves the third party not being able to be trusted, while authenticity of the transactions would be a concern. The third has that the validation of the transactions remains a top priority for the firm, and the fourth concerns that the company cares more about the data integrity rather than the confidentiality of the information (Puthal, 2018, p. 21). Knowing the uses that this technology would have inside the functions it could have allow it to be known as an effective platform for cybersecurity in these aspects.

According to the McKinsey industry-by-industry 2018 analysis, the highest feasibility blockchain can have is on the financial sector; technology, media and telecom; public sector; property; insurance; utilities; transport and logistics with highest impact in areas of financial, public sector and healthcare (Carson, Romanelli, Walsh, & Zhumaev, 2018). Viriyasitavat, Da Xu, Bi, and Pungpapong (2019) also show how blockchain has the potential to revolutionize business processes in the areas of banking, insurance, digital supply chain, energy management, healthcare, voting, and recruitment. Blockchain technologies can improve business processes due to persistency, validity, and auditability (Viriyasitavat & Hoonsopon, 2019). Although most large businesses consider blockchain as a reality, many of them question the blockchain as a pragmatic solution for improvement of their business processes. The main reasons for business management do not invest in blockchain technologies are the cost and complexity of implementation. This skepticism can also be due to the problems regarding time inconsistency and bias that may occur in existing blockchain consensus mechanisms. However, Viriyasitavat and Hoonsopon (2019) suggest solutions such as using Practical Byzantine Fault Tolerance (PBFT) with smart contracts can overcome the issue of time inconsistency and consensus in business processes.

Blockchain technology is developing fast and in various directions, but there is not enough practice history of making relative to business decisions for executives. One of the areas where blockchain technology will be used in business is its adaption into the management of supply chains that makes the transaction easier, secure and accurate for reporting purpose. Similarly, in accounting, blockchain can be used in these situations to ensure the privacy and security of the system. With the way blockchain works, it is possible to improve security of both forward and backward linkages in supply chains. Every part of the supply chain is traceable and the sources of insecurity pinpointed quite easily. Knowing the use of blockchains public availability, it can be inferred that it could easily be used to effectively track down recalled products more efficiently than the current process that companies use when a product seems to be liable to problems with viruses. If a product is released and it is then discovered that that product is liable to malware attacks, having the blockchain as part of your supply chain would allow for you to easily track where all of those products went and where they are located, allowing for your company to easily erase them from the market, thus, ending that cyber-attack. Supply chain could be a heavily impacted industry for their cybersecurity from blockchain. Many of the major security issues that are within a supply chain can be handled because of implementing blockchain

strategies. With this as an example, it shows what blockchain is able to do as a security framework being used to its potential.

After reviewing Blockchain for its uses within cyber security, it can easily be attributed that it would be useful for use in the profession of accounting. Proper accounting requires secure recording and ensuring that proper procedures are being used. Blockchain will be such a large part of accounting because while it maintains the key uses it shows when being used for higher level of cybersecurity, these uses are also adapted into the accounting industry. The Blockchain also essentially is just another large accounting ledger system. When businesses have the ability of recording their transactions directly to the shared blockchain that is synchronized on a real time basis with the other participants in the blockchain, a requirement for double entry accounting goes away. Due to the development of Blockchain technology, and its implementation, processes of generating and examining annual financial statements have become irrelevant. Blockchain can be effectively introduced in accounting within recording and reporting transactions and different financial statements, as well as many other uses of its technologies.

3. Blockchain's use in financial accounting- an in-depth look

Accounting is an industry that is being impacted daily by the use of new technologies. Companies will begin to have to make adjustments to adhere to these changes. Blockchain, is one of the main technologies that is primed to change the accounting industry (Dai & Vasarhelyi, 2017; Karajovic, Kim, & Laskowski, 2017; Kwilinski, 2019). Accountants and companies will have to work to implement this into their daily functions and use.

> Blockchain records and validates information in a decentralized way, and the entire process does not require any authority intermediaries, and the technology guarantees the information to be transparent, secure, tamper-proof, and reliable through the distributed ledger technology, hash chaining and PoW mechanism. As a result, the blockchain technology has great potential of enhancing the trust between market participants. (Yu, Lin, & Tang, 2018, p. 3)

Allowing the blockchain to be used in this function will allow it to make its first crucial changes to accounting, by allowing for financial information to be more "transparent, secure, permanent, and immutable". This is exactly what users of company financial information want and need to perform their daily tasks, and succeed at their jobs. As stated, accountants are trying to ensure that the financial information for their company is able to be precise, and without error. This is why the information that is produced and tracked by internal accounting departments for companies, is audited by the outside independent third party accounting firm. Blockchain technology checks off many goals that auditors, and other accountants seek for, to have a successful year in their information and numbers.

The reliability of this information confirmed after the audit is guaranteed to an extent, but it can never be completely confirmed that it is impeccably correct, beyond error. This is why audits are given certain levels of risk grades when completed, with an opinion from the independent auditor. The process that blockchain creates for finance departments for companies would allow for the companies implementing these goals to gain trust in the public eye, with the idea of confirmed accurate numbers,

without error or the chance to fail. Using Blockchain does not stop only at the use of recording or posting your financial data for the public. Since the information is posted to the public blockchain, that means anyone is able to become further nodes on the blockchain. This anyone, includes the auditors and lawyers, who could give further explanation on the information provided, and other types of investors would be able to do further research to make better investment decisions and develop greater strategies with their use of the blockchain. Firms would be posting source documents for the statements and balance sheets, and the information will then be generated into those different statements and ledgers through smart contracts (Yu et al., 2018, p. 5).

Most of the early adopters of smart contracts and blockchain started to explore use which will lower operational costs related to the transaction processing and also improving data accuracy through increased trust between parties (KPMG, 2019). One specific area getting attention is the use of smart contracts, which execute automatically upon achievement of specific contractual criteria. For example, in 2017 AXA launched "Fizzy," an automated parametric insurance platform for delayed flights. This system recorded information on customers' purchased flight delay insurance using a smart contract and connects to global air traffic databases to monitor flight statuses (AXA, 2019). If the policyholder experiences a flight delay of 2 or more hours, the smart contract triggers the mechanism for payment upon receipt of flight confirmation by the holder, and then Fizzy automatically pays the customer. This system diminishes the hassle of filling out forms or having to deal with the time to process the claim. This being true, allows for the users of a public blockchain to see what type of account procedures the company is using. This look into the typical very behind the scenes aspect of accounting, will allow for fundamental changes to the way information is presented and disclosed in financial accounting. "Using blockchain in financial accounting means there will be thousands of backups once it is posted on the public blockchain and all transactions are visible to all members of the network" (Yu et al., 2018, p. 7). This will make the process of accounting and reporting more transparent and traceable. This information will be able to be verified through all the different nodes of the chain.

Similarly, the automatic generation aspect of the blockchain also allows processes to be done more timely as well. "In 2016, ICICI Bank executed pilot transaction in international trade finance and remittance on blockchain network with emirates NBD … announced that it has successfully executed transactions in international trade finance and remittance in real time using blockchain technology … " (Khandelwal, 2019, p. 2). This proves that the idea of blockchain in accounting can actually exist and be real, and work. The bank was able to use blockchain to do applications that would normally take a few days to complete in the matter of moments because of the speed blockchain technology works and processes its information at. This allows for the concept of a digital accounting system to exist, and gives a platform for many other banks and other companies to potentially work off of, to gain a successful model for themselves.

Khandelwal (2019) performs a SWOT analysis of Blockchain in Accounting and Finance in his recent paper. Some of the strengths and opportunities he lists are: increased efficiency, cost effective, governance and trust with consensus-based transactions, digitalization of accounting system, boost up employment, and records of issues and trading shares (Khandelwal, 2019, p. 7). His example of ICICI Bank proves that the accounting system's efficiency has increased with the use of blockchain

technology. Because blockchain technology reduces intermediaries and uses less space it increased cost effectiveness, also due to reduced transaction costs. Since most parties have to agree when a change is made or data must be added to the blockchain, this creates a more honest system. This allows for any questionable changes to be immediately reviewed by the parties involved. This is a highlight again of the blockchains security level for company. Blockchain is the alternative to traditional accounting methods.

This view above is not without criticism. For example, Rückeshäuse in a 2017 study suggest to reconsider this view. Her paper suggests that blockchain based accounting, using current proof of work systems may impede the management to use internal and external control system and hence may lead the way to more accounting scandals. While this perspective defies why blockchain technologies are used in the first place, we still need more use of blockchain technology and more research on such unethical decision making issues.

Blockchain technologies allow the profession to move further into a technology filled and digital future at a great pace. Blockchain obviously allows IT professionals and finance professionals to work together to reach a common goal within a blockchain based system. This makes for companies to hire more of these workers. The execution of the sale and trading of shares on blockchain allow for transparency in ownership of shares. It also allows for a cheaper process of trading, and more true numbers based on the real time results blockchain would be able to report to signal to investors of the firm about the health of their stock. Investors would have more information than given by traditional audits, and auditors would be able to provide even further information while also confirming the successfulness of the blockchain being used by the company. Blockchain will alter the auditing profession, but in many successful ways.

3.1. *Auditing with blockchain*

Other technologies and industry automation are accelerating auditing processes. During an Audit, accounting records are examined by external auditors on behalf of investors to provide reasonable assurance as to their accuracy and integrity and to ensure compliance with accounting regulations. Financial Audits can be time consuming, expensive, and laborious, often requiring manual reviews of systems and obtaining paper documentation, and confirmation from external sources. Blockchain would be able to reduce this reliance on manual tasks and the duplication of records. If Blockchain is going to be used as a platform for accounting, then it would have to be able to be audited, and professionals would need to develop ways to audit the system. In the paper, "Designing and Auditing Accounting Systems Based on Blockchain and Distributed Ledger Principles", Appelbaum and Nehmer describes a process that is used when auditing a Distributed Ledger Technology (DLT). He describes that DLTs have seven core components. The components are listed as:

1. There is no trusted third party required instead, the network is peer-to-peer.
2. New transactions are time stamped and hashed onto an on-going chain of transactions.
3. The hash algorithm is designed to provide a proof-of-work.
4. The record, the hashed chain of transactions, cannot be changed without redoing the proof-of-work.

5. The proof-of-work is accomplished by a pool of CPUs from the peer-to-peer network through computation.
6. The longest chain (block of transactions) includes the latest transaction and requires the most CPU work to create the hash, therefore it takes the most time, to date, to compute the hash.
7. The system works as long as the majority of peer-to-peer nodes are not cooperating to subvert the chain since they represent the majority of the computing power and so can compute the hash faster than any other group. (Appelbaum & Nehmer, 2017, p. 4)

When examining transactions of a blockchain system in this context, auditors will come across the issues of data reliability, data security, and transaction transparency. "Data reliability pertains to the performance principle requirement that auditors obtain sufficient appropriate evidence about whether material misstatements exist, through designing and implementing appropriate audit tasks." (Appelbaum & Nehmer, 2017, p. 6). Reliable evidence is evidence that is able to be trusted, and understood by the auditor. Highly reliable evidence is usually collected and confirmed by external sources through the use of invoices, confirmations, or analyst reports to name a few. The information on the blockchain for the company, to this extent, is an external source for the company. Auditors would need evidence of proper governance of the peer network and the blockchain itself, and will then be able to confirm the reliability of the blockchain evidence. This will lead to all evidence stemming from the blockchain being deemed reliable and useful for the company audit. Data security provides assurance that the data has been protected from fraud and is free of any wrongful manipulations. A blockchain can provide the evidence is secure given its use of the non-alterable transaction trail along the nodes of the chain. Thirdly, using a blockchain in the design of a transaction processing system improves the data transparency by providing that record of the series of blocks and showing the process of how that block came to be within the "hashing system" that Appelbaum and Nehmer (2017) described in the core components.

During the engagement, the auditor needs all of this audit evidence. The evidence describes so far is any of the information used by the audit team to come to their final decision about the engagement, and giving the audit opinion. The procedures that are used to reach this opinion are an inspection of Records, inspection of Tangible assets, observation, inquiry, confirmation, recalculation, re-performance, and analytical procedures. In a blockchain, the continuous information collecting environment, these procedures are made more efficient by replacing the typical methods with blockchain related methods. As an example, for confirmation, a traditional auditor would verify account balances using confirmation letters from banks, while a blockchain auditor would only have to link the data streams within the blockchain (Appelbaum & Nehmer, 2017, p. 8). These sources of documentation would already be participating in the accounts receivable of the blockchain. This already reduces the high amount of burdens an auditor would have during this process. A second example would be in the inspection of record or documents. Traditionally, the audit team would pull different samples and then trace or match them to their sources. A blockchain audit would be able to evaluation the entire dataset in a ERP using the blockchain technology. The auditor is able to inspect documents that support the configuration of the peer network operating the DLT process, providing evidence that Appelbaum's first component is in place. Blockchain proves that audits would be made easier for engagement teams that would be assigned for that client that uses a DLT.

At the first level, it is shown that Blockchain transactions provide perfect audit evidence, being that the evidence is "difficult to alter, credible, complete, obvious, and with evidence of approvals." (Appelbaum & Nehmer, 2017, p. 12). There are concerns, though, moving forward into the future for auditors and blockchains, the origin of the blockchain must always be questioned, which will come from outside the technology itself. The auditors must also ensure that the peer network is not in collusion to subvert the chain. Auditors must be aware of this risk when conducting their inspection. Given all of the factors regarding the audit, blockchain is still an incredible change to business, the integration of the technology within an auditing process will most likely be gradually adopted over time, and not a huge change all at once, disrupting the profession.

Overall, while blockchain technology presents opportunities for accounting by making in more accurate, transparent, and traceable it presents challenges to the traditional accounting approaches, such as auditing, since conducting a standard point-in time forensic retrospective auditing will be ineffective and inefficient with the use of a system that has full integrity (Smith, 2017). This also presents new opportunities in the auditing profession since auditing of transactions will require a more real time auditing practice. Given everything we discussed, it can be confirmed that Blockchain will eventually change the traditional auditor role in major ways.

3.2. *Big data in accounting and blockchain*

An addition in the future of accounting is how Big Data is being implemented into current business practices. While blockchain is increasingly being added to businesses, this will call for more and more accurate data management. This is where blockchain and big data will be connected. Using Blockchain will allow for accountants to properly organize all of the new information that Big Data causes them to have to access and review as part of their job. Organizations are moving forward into the age of big data which is going to be known as a "high volume, high velocity, and high variety" with the ability to heavily improve overall decision making (Rezaee & Wang, 2019, p. 87). Companies are already establishing roles into their staff that are improving their ability into being able to take advantage of Big Data. Big data affects accounting in many different ways. It will be able to improve different factors of managerial and financial accounting, and also different financial reporting practices, as well as the profession of auditing.

Big Data can contribute to the development of different control systems, as well as different ways to effectively develop a budget for a company within managerial accounting. Using Big Data can also improve the quality of financial report information, allowing it to be linked easier to its base documents. This will improve transparency, and allow for easier and more efficient decision making. Big data also affects forensic accounting. These accountants are facing large pools of information.

> Auditors are now facing the challenge of huge amounts of both structured (e.g. general ledger or transaction data) and unstructured data (e.g. email, voice or free- text fields in a database, Wi-Fi sensors, electronics tags, etc.), together with an increasing amount of nontraditional data sources such as third-party watch lists, news media, free-text payment descriptions, email communications, and social media. (Rezaee, Wang, & Lam, 2018, p. 43)

Since auditors need to review all of the documents required for the company audit, big data allows for them to easily reach this goal for the client. Data analytics sue Big Data, and has been able to transform all of the unstructured data into useful, and relevant information that auditors and forensic accountants can use to perform their jobs at a higher rate of ability. With information coming from all over the place, big data allows for accounting firms to reduce the costs of their audits, while also increasing the efficiency of them. This allows for firms to stand out and compete for bigger and better clients, allowing the audit profession to grow and for firms to become more and more profitable.

In sum, while blockchain technology will enable more use of Big Data, Big Data itself will also bring changes to accounting standards. This is because accounting standards in the age of big data will give users more responsibility for demanding available data. The profession hence, will require employees who are savvy in Big Data techniques, tools, and procedures. Moreover, it is important that future accounting standards balance the need for disclosure with the need for the protection of sensitive data. This should necessitate closer interaction with accounting professionals with the policy makers regarding the use of Big Data as well as blockchain technologies. Regarding this last point, we suggest that future research and practice should also foster more multidisciplinary collaborations to address meaningful questions and issues that arose from using blockchain technologies (Risius & Spohrer, 2017).

3.3. *Blockchain to enhance regulation and avoid financial misconduct*

An issue that arises in business is the financial misconduct. This misconduct can stem from the unethical practices by a company or by the firm and auditors that are in charge of ensuring that there is not misconduct occurring. Misconduct does happen, and when it does, it is up to different boards and different societies to ensure that the person that was caught is disciplined in the correct ways. This is one of the challenges in the accounting profession. Being able to share the cases of misconduct across the various different governing boards that need to be aware of these instances. These various boards can consist of the board of accountancy for each state in the United States, but also the Internal Revenue Service, Securities and Exchange Commission, and the Public Company Accounting Oversight Board. If one of these groups identifies a misconduct, it would be of high interest for the other groups to know about it and be able to identify for their use and tracking as well. A recent study found that these parties vary in their level of reporting misconduct to a central authority, the AICPA. (Sheldon, 2018, p. A27). This means that there are major concerns of a low level of communication across different states. What would then stop someone caught of financial misconduct from moving to a different area of the country and being able to work in financial information again. This is where the use of blockchain would be able to assist in this field of accounting.

Blockchain would be able to allow these groups to achieve a higher real time reporting and sharing of the misconduct data. It offers the solution of "aggregating misconduct issues without relying on a central party or an authority to serve as the clearinghouse" (Sheldon, 2018, p. A28). If everyone registered to the AICPA is issued a unique ID code, thus allowing every CPA to create an account and register

to an Accounting Blockchain. Having this access, and having the major constituents, the groups mentioned before, join the blockchain, and record the instances of financial misconduct to the CPAs unique ID. This would allow for a system that is updated in real time, because of blockchain technology, that is available to everyone based on the public domain access of the server. All of the parties involved would have the crystal clear transparency to see any misconducts linked to different IDs. There is almost little to no cost to this service, and allows for an efficient process that protects business as a whole. The only cost would be to setup and maintain the blockchain, which could be divided equally by all the parties that are currently monitoring misconduct, and this would be a cheaper and more efficient way to do so anyhow. This type of work would allow for the accounting profession to move forward to a place of protection and validation for the business world.

4. Discussion and conclusion

Overall, the existing research on blockchain and its use in business, specifically in accounting area, though limited, still gives us insights about the future of blockchain technology and its use in accounting area. It is certain that Blockchain effectively change the way accounting, and all of its different fields be impacted. It is a difficult task to try and interpret what Blockchain will do in the future generations because of the never ending development of the technology. "In the near future, blockchain will have the ability to integrate and to interoperate IoT, Artificial Intelligence (AI), and other emerging technologies to provide higher quality services for society" (Lu, 2018a, p. 235). The technologies named here, are ones that are for certain to be already impacting accounting, if not, in the near future will be impacting heavily for many different companies and firms. As we have shown in previous sections of this paper, blockchain technology will impact accounting not only its use and its benefits, but also in auditing, Big Data, and policy making areas. The typical accounting job will be on the task to face an abundance of changes in the future years because of all of these emerging technologies, and these changes are disruptive yet open to many potential opportunities in the profession.

Blockchain can effectively be a very impactful new part of Accounting and overall business environment in many different ways. Specifically, though, keying in on the way that blockchain has a very high level of security, allows it to be a potential major impact in the cyber security system of a company in business or accounting. Therefore, we also show that firms need to take into account primary actions in order to ensure a healthy and secure future for blockchain accounting from cybercrimes. These actions can range from, but not limited to:

- The assessment of the current features and capabilities of the blockchain accounting infrastructure at different levels of networking, internet, database, and data management must be done at both public and private level blockchain ledgers.
- There is a model containing three primary components of cyber security and is proposed by the CIA, commonly known as security triad model. The three main components of cyber security are therefore Confidentiality, integrity and availability. All the three domains of network security are needed to be accessed to get an overall idea about the maturity level of blockchain accounting.

- All the new systems and software that must be designed in the context of blockchain technology must be tested based on three A's of authentication, authorization and auditing (Piscini, 2017)

As suggested by the information provided in this paper, blockchain technology has promising uses for not only a security system in the future with growing threats to cybersecurity, but also as part of an accounting system based on its ability to be secure and transparent, decentralized, and providing trust in a financial world. As accounting profession being in the center of the ethical, proper and successful business environment, blockchain will provide sustainable environment for everyone. Blockchain as a whole, will allow for a more transparent financial based system. However, we also suggest that future research and practice should also foster more multidisciplinary collaborations to address meaningful questions and issues that arose from using blockchain technologies and management analytics (Risius & Spohrer, 2017).

Allowing blockchain to become a bigger part of company's financial base system will be a move that many will come to do, and a move that will prove increased efficiencies, security, and cost reductions for those that are on the right side of it. Government, institutions, companies and all other stakeholders should focus on cybersecurity investments strategies and their applications in accounting.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Sebahattin Demirkan http://orcid.org/0000-0002-9987-4853
Irem Demirkan http://orcid.org/0000-0003-3888-9071

References

Al-Jaroodi, J., & Mohamed, N. (2019). Blockchain in industries: A survey. *IEEE Access*, *7*, 36500–36515.

Andersen, N. (2016). *Block chain technology: A game changer in accounting*. Deloitte, March.

Appelbaum, D., & Nehmer, R. (2017). *Designing and auditing accounting systems based on blockchain and distributed ledger principles*. Montclair, NJ: Feliciano School of Business.

AXA. (2019). AXA goes blockchain with Fizzy. Retrieved from https://www.axa.com/en/newsroom/news/axa-goes-blockchain-with-fizzy

Barzilay, O. (2017). *3 ways blockchain is revolutionizing cybersecurity*. Retrieved from www.forbes.com: https://www.forbes.com/sites/omribarzilay/2017/08/21/3-ways-blockchain-is-revolutionizing-cybersecurity/#77dc34b12334

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

Brett, C. (2018, October 11). Blockchain disadvantages: 10 possible reasons not to enthuse -. *Enterprise Times*. Retrieved from https://www.enterprisetimes.co.uk/2018/10/15/blockchain-disadvantages-10-possible-reasons-not-to-enthuse/

Byström, H. (2019). Blockchains, real-time accounting, and the future of credit risk modeling. *Ledger*, *4*.

Cachin, C. (2016). Architecture of the hyperledger blockchain fabric. In *Workshop on distributed cryptocurrencies and consensus ledgers* (Vol. 310, p. 4).

Carfagno, D. (2019, September 4). How much should your company invest in cybersecurity? Retrieved from http://www.blackstratus.com/how-much-should-your-company-invest-in-cybersecurity/

Carson, B., Romanelli, G., Walsh, P., & Zhumaev, A. (2018). Blockchain beyond the hype: What is the strategic business value? Retrieved from https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value

Coyne, J. G., & McMickle, P. L. (2017). Can Blockchains serve an accounting purpose? *Journal of Emerging Technologies in Accounting*, *14*(2), 101–111.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), 71.

Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems*, *31*(3), 5–21.

Deloitte. (2016a). Blockchain – enigma. paradox. Opportunity. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-ukblockchain-full-report.pdf

Deloitte. (2016b). Blockchain: A game changer for audit processes? Retrieved from https://www2.deloitte.com/mt/en/pages/audit/articles/mt-blockchain-a-game-changer-foraudit.html

Deloitte. (2016c). Blockchain technology a game-changer in accounting? Retrieved from https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A%20game-changer%20in%20accounting.pdf

Deloitte. (2017). Blockchain technology and its potential in taxes, Retrieved from https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Reports/pl_Blockchaintechnology-and-its-potential-in-taxes-2017-EN.PDF

DHS. (2018, 15 April). U.S. Department of Homeland Security cybersecurity strategy. *U.S. Department of Homeland Security Cybersecurity Strategy*.

Dogo, E. M., Nwulu, N. I., Olaniyi, O. M., Aigbavboa, C. O., & Nkonyana, T. (2018). Blockchain 3.0: Towards a secure ballotcoin democracy through a digitized public ledger in developing countries. *i-Manager's Journal on Digital Signal Processing*, *6*(2), 24.

Donaldson, C., & Osei-Bryson, K.-M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*. doi:10.1016/j.ijinfomgt.2019.102056

Freeze, D. (2018). Global ransomware damage costs predicted to hit $11.5 billion by 2019. Retrieved from https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/

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

Gautham. (2017). *The "Big Four" audit firms and their contribution to blockchain technology – Newsbtc*.

Gordon, L. A., Loeb, M. P., Sohail, T., Tseng, C.-Y., & Zhou, L. (2008). Cybersecurity, capital allocations and management control systems. *European Accounting Review*, *17*(2), 215–241.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in cybersecurity: Insights from the Gordon-Loeb model. *Journal of Information Security*, *7*(2), 49–59.

Hasanova, H., Baek, U. J., Shin, M. G., Cho, K., & Kim, M. S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management*, *29*(2), e2060.

Hassani, H., Huang, X., & Silva, E. (2018). Banking with blockchain-ed big data. *Journal of Management Analytics*, *5*(4), 256–275.

Higginson, M., Hilal, A., & Yoguc, E. (2019, June). Blockchain and Retail Banking: Making the Connection. *McKinsey & Company*. Retrieved from www.mckinsey.com/industries/financial-services/our-insights/blockchain-and-retail-banking-making-the-connection

IBM. (n.d.). Cost of a data breach report. IBM Security. Retrieved from https://databreachcalculator.mybluemix.net

Karajovic, M., Kim, H. M., & Laskowski, M. (2017). Thinking outside the block: Projected phases of blockchain integration in the accounting industry. *Australian Accounting Review*, doi:10.1111/auar.12280

Kaushal, M., & Tyle, S. (2016, July 29). The blockchain: What it is and why it matters. Retrieved from https://www.brookings.edu/blog/techtank/2015/01/13/the-blockchain-what-it-is-and-why-it-matters/

Khandelwal, S. (2019). Blockchain Technology: Heart of digital financial infrastructure for managing trust and governance system. *Available at SSRN 3308578*.

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.

KPMG. (2019). Blockchain in insurance. Retrieved from https://home.kpmg/xx/en/home/insights/2018/09/blockchain-in-insurance-fs.html

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, *41*(10), 1027–1038.

Kwilinski, A. (2019). Implementation of blockchain technology in accounting sphere. *Academy of Accounting and Financial Studies Journal*, *23*, 2.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*, doi:10.1016/j.future.2017.08.020

Lu, Y. (2018a). Blockchain and the related issues: A review of current research topics. *Journal of Management Analytics*, *5*(4), 231–255.

Lu, Y. (2018b). Blockchain: A survey on functions, applications and open issues. *Journal of Industrial Integration and Management*, *3*(4), 1850015.

Lu, Y. (2018c). Cybersecurity research: A review of current research topics. *Journal of Industrial Integration and Management*, *3*(4), 1850014.

Orcutt, M. (2018). How secure is blockchain really? Retrieved from https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/

Perera, S., Nanayakkara, S., Rodrigo, M. N. N., Senaratne, S., & Weinand, R. (2020). Blockchain technology: Is it hype or real in the construction industry? *Journal of Industrial Information Integration*, *17*, Article 100125. doi:10.1016/j.jii.2020.100125

Piscini, E. D. D. (2017). *Blockchain & cyber security. Let's Discuss*. Retrieved from www2.deloitte.com:https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf

Puthal, D. (2018). The blockchain as a decentralized security framework [future directions]. *IEEE Consumer Electronics Magazine*, *7*(2), 18–21. doi:10.1109/mce.2017.2776459

Rezaee, Z., & Wang, J. (2019). Relevance of big data to forensic accounting practice and education. *Managerial Auditing Journal*, *34*(3), 268–288.

Rezaee, Z., Wang, J., & Lam, B. (2018). Toward the integration of big data into forensic accounting education. *Journal of Forensic and Investigative Accounting*, *10*(1), 87–99.

Risius, M., & Spohrer, K. (2017). A blockchain research framework. *Business & Information Systems Engineering*, *59*(6), 385–409.

Rosic, A. (2019, November 15). What is blockchain technology? A step-by-step guide for beginners. Blockgeeks. Retrieved from https://blockgeeks.com/guides/what-isQ29 blockchain-technology

Rückeshäuser, N. (2017). Do we really want blockchain-based accounting? Decentralized consensus as enabler of management override of internal controls. In J. M. Leimeister & W. Brenner (Hrsg.), *Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017)* (pp. 16–30). St. Gallen, S.

Sheldon, M. D. (2018). Using blockchain to aggregate and share misconduct issues across the accounting profession. *Current Issues in Auditing*, *12*(2), A27–A35. doi:10.2308/ciia-52184

Singh, S., & Singh, N. (2016). Blockchain: Future of financial and cyber security. *2nd international conference on contemporary computing and informatics (IC3I)*. doi:10.1109/ic3i.2016.7918009

Smith, A. M. (2017). Auditing blockchain: A new frontier. Pricewaterhouse coopers. Retrieved from https://www.pwc.com/us/en/industries/financial-services/research-institute/blog/blockchain-audit-a-michael-smith.html

Statistics: The average cost of a malware attack on a company is $2.4 million. (2019). Retrieved from https://www.vumetric.com/statistics/the-average-cost-of-a-malware-attack-on-a-company-is-2-4-million/

Tung, K. (2019). AI, the internet of legal things, and lawyers. *Journal of Management Analytics*, *6*(4), 390–403.
Viriyasitavat, W., Da Xu, L., Bi, Z., & Pungpapong, V. (2019). Blockchain and internet of things for modern business process in digital economy—the state of the art. *IEEE Transactions on Computational Social Systems*, *6*(6), 1420–1432.
Viriyasitavat, W., & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*, *13*, 32–39.
Voices – Blockchain, accounting and audit: What accountants need to know. (n.d.). Retrieved from https://www.cpa.com/media-coverage/voices-blockchain-accounting-and-audit-what-accountants-need-know
Walch, A. (2016). The bitcoin blockchain as financial market infrastructure: A consideration of operational risk. *18 NYU Journal of Legislation and Public Policy 837*.
Watson, L. A., & Mishler, C. (2017). Get ready for blockchain: Should management accountants add blockchain technology to their professional vocabulary? *Strategic Finance*, *98*(7), 62–64.
Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. *PLoS ONE*, *11*(10), e0163477. doi:10.1371/journal.pone.0163477
Yu, T., Lin, S., & Tang, Q. (2018). Blockchain: Introduction and Application in Financial Accounting. Available at SSRN 3258504.
Zhang, K., & Jacobsen, H. A. (2018). Towards dependable, scalable, and pervasive distributed ledgers with blockchains. In *ICDCS* (pp. 1337–1346).