Auditing with Smart Contracts

Andrea M. Rozario. Rutgers Business School. New Jersey aochoa@scarletmail.rutgers.edu

Miklos A. Vasarhelyi. Rutgers Business School. New Jersey miklosv@business.rutgers.edu

Abstract. Blockchain-based smart contracts are emerging as a disruptive force that may change the way financial statement audits are performed and delivered. With their potential ability to autonomously execute audit procedures on behalf of the auditor and disclose the results of these audit procedures, blockchain-based smart contracts have the potential to improve audit quality and meet the information demands of various vested parties for more timely and transparent audit reporting. This paper proposes the application of smart contracts to auditing as an enabler for improved audit data analytics and close to real-time audit reporting.

Keywords: Smart Contracts, Blockchain, Audit Data Analytics

1. INTRODUCTION

Digital transformations and the preponderance of large volumes of data have forced businesses to adapt to an electronic world and modify their business practices (IAASB, 2016; PCAOB, 2016). Disruptive technologies such as deep

learning, along with Big Data (Vasarhelyi et al., 2015) are increasingly changing the type of information that is collected, how that information is analyzed, and disseminated. For example, deep learning models that incorporate textual data from social media posts can assist in the prediction of reputational risk (Forbes, 2016). More recently, smart contracts enabled by blockchain technology have demonstrated the potential to transform supply chain and financial industry business practices.

With its cryptographic and consensus mechanisms that secure the integrity of transactions, blockchain demonstrates great potential as a tamper-proof audit trail. Fused with smart contracts (Szabo, 1994; Szabo, 1997), which are computer programs that perform a task on behalf of a human user, blockchain can significantly alter existing business practices. Essentially, blockchain enabled smart contracts can generate agile supply chains and financial organizations by automatically monitoring and executing the terms of bills of lading and financial derivatives (Mainelli and Smith, 2015; Vaziri, 2016; Yermack, 2017). Given these recent digital transformations, it is important for the auditing profession to consider the impact of blockchain-based smart contracts. Hence, a natural research question that emerges is the extent to which the auditing profession will be disrupted by these technologies. In particular, this research study attempts to examine if blockchain enabled smart contracts have the potential to help auditors deliver improved audits.

Business organizations have been proactive regarding exponential changes in technology. However, the same premise does not apply to the external auditing profession. Pressured by rapidly changing business practices, the external auditing community, standard-setters, regulators, and academics have created initiatives aimed at examining the impact of sophisticated audit analytics in financial statement audits; these initiatives include the Data Analytics Working Group (IAASB, 2017) and the Rutgers and AICPA data analytics initiative (AICPA, 2017). Though the external audit paradigm has witnessed significant transformations in the last three decades (Mathews, 2006; PCAOB, 2017), with the recent requirement to report Critical Audit Matters (CAMs) as its last major transformation, it is clear that the external audit profession substantially lags in technological innovation. Increases in volume, velocity, and variety of data and

rapidly evolving technologies raise the question of the relevance and applicability of the traditional audit model (Appelbaum et al., 2017; Badertscher et al., 2017).

This research study makes several important contributions. First, it contributes to the emerging literature on audit data analytics (ADA) by proposing a new generation of audit analytic tools, smart audit procedures, which are enabled by blockchain technology. Second, this study presents a discussion regarding the effect of smart audit procedures on audit quality and the public interest thus helping initiate the debate on the role of emerging technologies in the audit process. Finally, this study contributes to the literature by providing direction for future research with respect to the evolution of the external auditing paradigm.

The next sections of this paper are organized as follows. Section 2 suggests the evolution of the auditing paradigm with blockchain and smart contracts. Section 3 describes the origins of smart contracts and their relevance to auditing. Section 4 illustrates the execution of a smart contract and introduces smart audit procedures. Section 5 proposes smart audit procedures as the next generation of ADA. Section 6 highlights some challenges related to the application of blockchain and smart contracts to auditing and suggests avenues for future research. Finally, Section 7 concludes the paper.

2. EVOLVING AUDITING WITH BLOCKCHAIN AND SMART CONTRACTS

Current audit methodologies prescribe 1) sampling of transactions to collect audit evidence about the risk of material misstatement, 2) a backward-looking audit approach, and 3) an annual, point in time, audit opinion. In a modern economy where databases store thousands of daily transactions that may be exposed to cybersecurity attacks, it is essential for the traditional audit model to evolve as financial statement audits progressively become automated and of predictive nature.

Consequently, it is vital for external auditors to consider the impact of sophisticated audit analytics as well as other emerging technologies including smart contracts and blockchain in order for them to remain relevant and continue to add value to the public by delivering high quality audits in a largely complex ecosystem. As business organizations continue to adopt blockchain and smart contracts to improve business process efficiencies (Tapscott and Tapscott, 2016),

it is important for external auditors to understand the opportunities and challenges that these technologies offer (Dai and Vasarhelyi, 2017; Rozario and Thomas, 2017).

Presently, auditors have the option to develop data analytic tools in-house, or purchase data analytic tools from audit software vendors such as IDEA or ACL, however, these data analytic tools exist in different platforms including proprietary audit firm platforms, and vendor platforms. Additionally, the integration of several audit analytic tools would be necessary to meet vested parties' demands for more timely audit reporting and transparency (Romero et al., 2012; No and Vasarhelyi, 2017). As a result, although these audit analytic tools could be uploaded to the cloud by the auditor and made publicly available to vested parties, saving the results of audit procedures to the cloud on a close to real-time basis could prove to be an onerous audit task. As the planning of an audit requires several cost benefit assessments including the accounts that should be examined, the nature, timing, and extent of audit procedures (Louwers et al., 2013; Badertscher et al., 2017), it is probable that moving towards a cloud enabled audit analytic tool reporting ecosystem would not be feasible from a cost-benefit stance.

Given the inherent complexities of adapting existing technologies to reflect a proactive and more transparent audit model, it is essential to consider the implications of smart contract based audit analytics (hereafter smart audit procedures). Essentially, smart contracts deployed on a blockchain that is created by the external auditor can facilitate the execution of audit procedures and at the same time, provide close to real-time audit reporting and more transparency to stakeholders (Rozario and Thomas, 2017). Henceforth, the conceptualization of smart contracts is expanded to include smart audit procedures that assist external auditors in delivering more efficient and effective audits.

Smart audit procedures are autonomous audit procedures, including autonomous internal control tests (hereafter smart control tests) and autonomous analytical procedures (hereafter smart analytical procedures), that are deployed on the external auditor blockchain. The deployment of smart audit procedures on the distributed blockchain ledger would lead to close to real-time audit reporting for several stakeholders such as key investors, suppliers, audit inspectors, the SEC, and the audit committee. Since the blockchain provides a platform for the

execution of smart audit procedures and close to real-time audit reporting, these novel audit procedures have great potential to enhance audit quality by enabling auditors to more efficiently execute audit procedures, and as a result, allocate more resources to higher risk areas. Finally, as smart audit procedures would be distributed to the participating nodes on the auditor's blockchain on a close to real-time basis, they would help meet the needs for more transparency and timelier audit reporting.

3. SMART CONTRACTS BACKGROUND AND RELEVANCE TO AUDITING

Smart contracts were first introduced by Szabo (1994) as a "computerized transaction protocol that executes the terms of a contract," including the enforcement, verification, and performance stages of the contracting process. Szabo describes smart contracts using a vending machine example to describe their operationalization in the real world, see Figure 1 for an illustration of Szabo's example.

3.1 Vending Machine Smart Contract

A vending machine is a smart contract between a customer and a vendor and is designed to accept a set of inputs based on pre-defined rules and dispense outputs, that is, transfer ownership, if those rules are met. A customer would enter a specified amount of money and select a product. In this case, the customer would enter $5.00 to buy a bag of chips that costs $3.00. The smart contract would then activate and search for the product and its respective price. If the product is found and the price is equal to or less than the monetary amount that was provided by the customer, the smart contract would transfer ownership of the product by releasing the product to the customer and returning the differential for the price of the product and the amount provided by the user, if the money provided by the customer exceeds the price of the selected product. Consequently, the vending machine releases a bag of chips and change of $2.00 to the customer and the transaction between the vendor and the customer is settled. If the product is not found, or if the money provided by the user is not sufficient to purchase the product, the transaction cannot be completed.
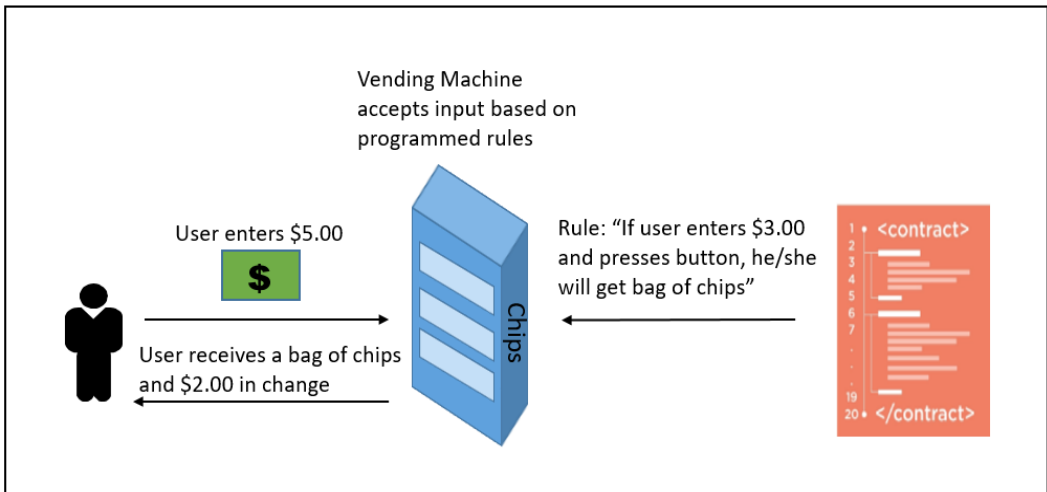
Figure 1. Vending Machine Example of Smart Contract

3.2 Revival of Smart Contract: Blockchain Smart Contract

Though an innovation in the early 1990s, smart contracts did not thrive during that period as an authorized trusting third party was necessary to monitor the terms and the execution of the encoded contracts, which poses the risk that a contracting party may not meet its contractual obligations (Kiviat, 2015). With blockchain technology, the execution of smart contracts becomes feasible as the oversight responsibilities are distributed to the participating nodes (Buterin, 2014; Dai and Vasarhelyi, 2017). Pre-defined business logic can be agreed upon by contractual parties, programmed, and stored on the blockchain ledger. Then, blockchain users would activate the smart contract by sending data to it, the smart contract would then verify the information received is within the boundaries of the pre-defined rules and release an output, such as payment for goods. If conditions are not met, the output is not released and an error message, indicating that the transaction could not be completed, is displayed. The status of the smart contract would be visible to the contracting parties on the blockchain, thus mitigating the risk of a counterparty defaulting.

Taken together, the benefits of smart contracts on the blockchain include 1) disintermediation, as it is not necessary to preemptively select a trusting central authority; 2) trust in a trustless environment because information is encrypted and visible by parties on the blockchain; 3) mitigation of the risk of fraud or human

error[1], because smart contracts perform precise calculations and 4) process efficiency as smart contracts are self-executing.

Consequently, smart contracts are simply software agents that automatically execute tasks on the blockchain based on pre-defined conditions that imitate the actions of a human user (Nwana and Ndumu, 1999; Vasarhelyi and Hoitash, 2005). Software agent research predated smart contracts and the blockchain as it emerged in the 1980's (Nwana and Ndumu, 1999) with the purpose of developing computer programs that assist the human user in the monitoring of events or performance of tasks (Maes, 1994). As a result, it is natural to extend the definition of smart contracts to represent a variety of computer programs that contain pre-defined rules and execute tasks, based on those rules.

While there are general applications of blockchain smart contracts including the automatic settlement of financial derivatives and secure transfer of property titles (DeCovny, 2015; Fanning and Centers, 2016), applications to the auditing domain remain unexplored. Applied to the external auditing domain, the definition of blockchain smart contracts is expanded to include smart audit procedures (e.g. the analyses of audit evidence) that are autonomously executed on behalf of the auditor for the purpose of improving audit efficiency, effectiveness, and meeting the informational needs of various stakeholders for timelier, and more transparent audit reporting. Figure 2 depicts the aforementioned links between software agents, smart contracts, and smart audit procedures.

Every year, the PCAOB releases a staff inspection brief about the current year's inspections highlighting audit areas where audit firms were deficient. These areas include internal control over financial reporting, validation of fair value estimates, and responding to risks over material misstatements (PCAOB, 2017). Applied to auditing, the benefits of smart audit procedures are imminent as they can help reduce the expectation gap that currently exists between the procedures auditors perform versus those procedures audit inspectors and regulators expect them to perform.

---

[1] Although smart contracts mitigate the risk of fraud or human error, anecdotal evidence such as the failure of the DAO (https://www.coindesk.com/understanding-dao-hack-journalists/) suggests that smart contracts can be circumvented as a result of erroneous code, as a result, this is a challenge that must be considered in the implementation of smart contracts.
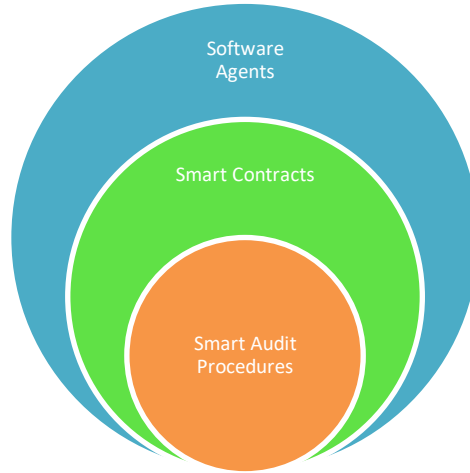
Figure 2. Linkage of Software Agents to Smart Audit Procedures

On the external auditor blockchain the audit firm's data science team can develop smart audit procedures based on the audit procedures that are agreed upon with the audit inspector. Essentially, these smart audit procedures would be vetted by the inspector to reduce the expectation gap, while at the same time enabling proactive audit inspections[2]. Once consensus is reached, smart audit procedures would be loaded to the blockchain and the external auditor would invoke those procedures by sending relevant audit evidence to them. The smart audit procedures and their results would be visible by the external auditor, as the owner of the audit blockchain, and the audit inspector.

Equally important, vested parties including the SEC, key investors, and the audit committee could have limited access to review the aggregated results of smart audit procedures, with an emphasis on any error messages (red flags) that may be indicative of notable items (Alles, et al., 2006; Issa and Kogan, 2014); hence, reducing the expectation gap between auditors and financial statement users in a close to the event, modern economy. Additionally, reviewing the results of smart audit procedures would enable the SEC to follow a proactive approach by monitoring audit clients that may require inspection or by identifying potential indicators that may signal an economic crisis. Collectively, the deployment of smart audit procedures on the blockchain has the potential to improve audit quality and meet the demands of various parties.

---

[2] With blockchain based smart audit procedures, both auditors and regulators have the opportunity to proactively address areas where audit firms have been deficient.

4. THE OPERATIONALIZATION AND VERSATILITY OF BLOCKCHAIN SMART CONTRACTS

As discussed in the preceding section, there are numerous applications of blockchain smart contracts. The Ethereum blockchain platform (Buterin, 2014) represents one of the several platforms that facilitate the development and execution of a variety of smart contracts, referred to as decentralized applications (dapps). These 'dapps' range from simple smart contracts, such as the exchange of digital value, to more complex smart contracts, such as a distributed autonomous organization (DAO) (PwC, 2016).

Sending a bitcoin, or ether, on the blockchain is an example of a simple smart contract as predefined rules that ensure the validity of the transaction are executed on the blockchain. Blockchain smart contract use cases have emerged in the manufacturing industry[3]. A blockchain smart contract between a vendor and a customer would include computer code that reflects the shipping terms of a contract and enforces the adequate transfer and ownership of the goods. Fused with the Internet of Things, blockchain smart contracts for manufacturing are also capable of continuously monitoring the location and temperature of the goods.

Finally, the long-term vision for blockchain smart contracts comprises the development of distributed and decentralized autonomous organizations (DAOs) that operate in an entirely automated manner (Jarvenpaa and Teigland 2017; Swan 2015; Benkler 2006). These DAOs would represent a new type of organizationas they are enabled by the Internet (Brafman and Beckstrom, 2006) but are also autonomous as a result of converting business logic to computer protocol. In auditing, blockchain smart contracts can be used to autonomously execute internal control tests and analytical procedures. Smart contracts on the blockchain are versatile and can be applied to business as well as auditing processes that are formalizable.

4.1 Blockchain Smart Contract for Manufacturing

Figure 3 illustrates an example of a blockchain smart contract for manufacturing to demonstrate their applicability. Understanding the operationalization of smart contracts that have been successfully implemented can guide the discussion

---

[3] Refer to the following links for examples of use cases of blockchain smart contracts with IoT in the manufacturing industry: http://www.gazelle.in/BCSCM.pdf, https://www.chainofthings.com/news/2016/11/23/smart-bol-reducing-contractual-enforcement-costs.

concerning the application of smart audit procedures. A supplier and a buyer agree upon contractual terms including the price, quantity, product description, shipping and payment conditions. These terms would be programmed as business logic and deployed on the blockchain. The blockchain offers the buyer the opportunity to find the smart contract and check the status of the transactions that pass through the smart contract and be able to verify the quality and location of the goods. If there is a violation to one rule, or several rules, embedded in the smart contract, an error message is triggered, and the transaction cannot be completed. This violation would have to be addressed by a human user, presumably an internal auditor or business process owner, to verify the legitimacy of the transaction. Alternatively, the violation could be addressed by an automated procedure that handles smart contract violations. Otherwise, if there are no violations, the contract self-settles once the goods reach their destination and payment is satisfied.
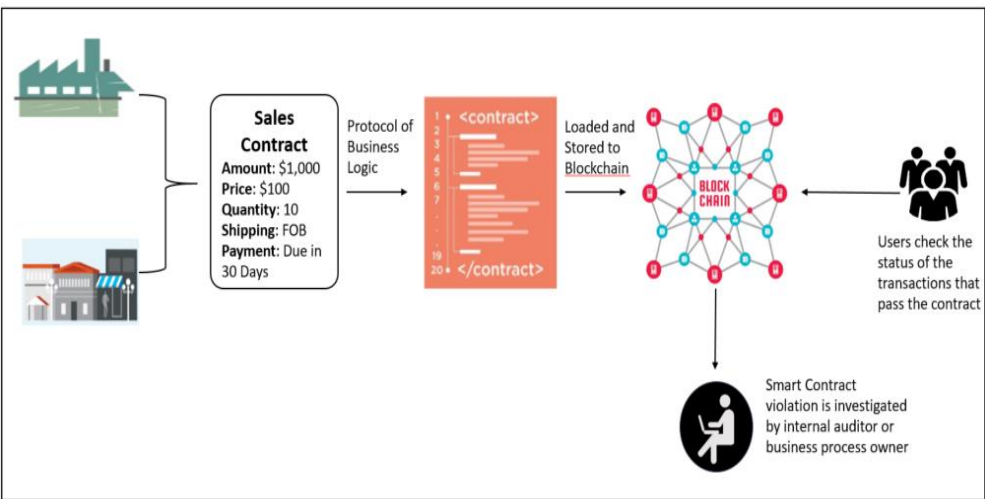

Figure 3. Depiction of smart contract for sales between buyer and supplier

4.2 Blockchain Smart Contract for Auditing

Similarly, in auditing the external auditor and inspector would agree upon the pre-defined audit procedures to address the risk that goods that are shipped are not accurately recorded. These predefined procedures would be decomposed into 'IF-THEN' rules by the audit firm, for example, and embedded into a smart analytical procedure that is loaded to the external auditor blockchain and pre-approved by both the audit firm and the inspector (Rozario and Thomas, 2017).

A description of a smart analytical procedure to address this risk is depicted in Figure 4 and would consist of 1) a rule to predict current weekly sales based on a

trained multivariate regression model that incorporates financial and non-financial parameters including, weekly sales, location, and temperature data from prior weeks. The multivariate regression model would be re-trained and re-tested as more data would be collected each time the auditor calls the smart procedure; 2) the predicted sales from the multivariate regression can then be used as a benchmark to compare current actual sales (Yoon, 2016). 'IF-THEN' logic can express that if current actual sales are equal to, less than, or greater than, up to 5% of overall materiality, then no further audit procedures are required and the auditor is able to quantify the risk of material misstatement for the revenue account. If the input, that is, actual sales, does not match the programmed rules, an error message would be displayed indicating that further investigation is necessary.

The external auditor can then propose alternatives for the processing of these error messages. The first alternative entails generating a follow-up smart audit procedure that interacts with the aforementioned smart analytical procedure. The rules programmed into this follow-up smart audit test would include rules that reflect risk filters that segregate those transactions with errors that would require the auditor's attention. An 'IF-THEN' condition indicating whether sales increased asa result of seasonality, for example, would discriminate those sales transactions that increased for legitimate reasons compared to those transactions that increased for unverifiable and potentially fraudulent or erroneous reasons that would of course, require investigation by the external auditor.

On the other hand, the processing of error messages is not required to be autonomous, hence, the external auditor could opt to manually check those transactions that were flagged by the smart analytical procedure, although this may result in the problem of exceptional exceptions that is already evident with more sophisticated analytical tools that are executed outside of the blockchain (Issa and Kogan, 2014). On the external auditor blockchain the audit inspector has the ability to inspect the results of the aforementioned smart analytical procedure proactively as they can access the smart audit procedure and the status of the transactions that pass the procedure close to real-time. Moreover, the SEC, key investors, and the audit committee can view the results of this procedure and make an assessment for revenue[4], if there are no additional procedures required,

---

[4] The revenue assessment for transaction-level data on the blockchain for example, could take the form of an audit review, certification, or seal of approval (No and Vasarhelyi, 2017).

or make a preliminary assessment in the scenario that errors messages have to be processed.
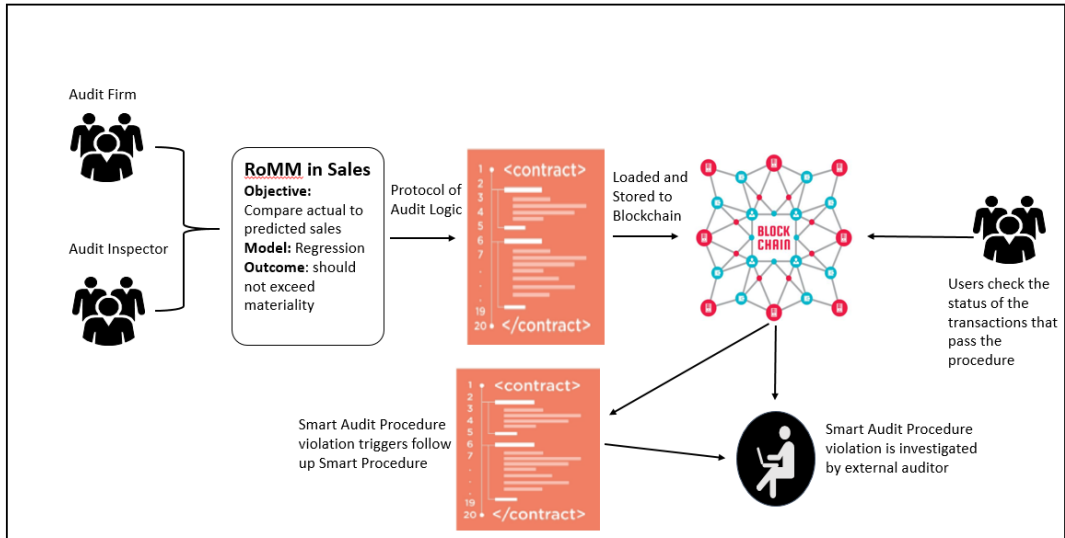

Figure 4. Depiction of smart audit procedure for addressing the risk of material misstatement in sales

An illustration of a smart analytical procedure was described above, however, it is important to note that simpler, yet new smart audit procedures can be developed. For instance, since blockchain enables the secure tracking and monitoring of various IoT devices, the audit firm can design an internal control test to verify the actual location of the goods and compare that to the expected location of the goods (Dai and Vasarhelyi, 2017; Rozario and Thomas, 2017) to assess the risk that goods may be shipped to the incorrect location. Since business organizations have begun to explore the synergies of blockchain and IoT (IBM, 2017), it is reasonable to infer that auditors would have to design new audit procedures that would help them assess the risk of material misstatement more precisely.

5. SMART AUDIT PROCEDURES: AUDIT DATA ANALYTICS 3.0

The emergence of new technologies including the rise of the Internet and electronic commerce, machine learning models that learn from magnitudes of Big Data, and presently blockchain and smart contracts has resulted in debates among various stakeholders concerning the role of technology into the audit model (IAASB, 2016; PCAOB, 2016). Vasarhelyi and Halper (1991) first designed and implemented continuous auditing applications at AT&T Bell labs. Several years

later, this research area gained significant traction with the implementation of continuous control monitoring (Alles et al., 2006), continuous data assurance (Kogan, et al., 2014), continuous risk monitoring and assessment (Moon, 2016) and continuous auditing in XML and ERP (Murthy and Groomer, 2004; Kuhn and Sutton, 2010).

The case studies to demonstrate the practical applications of the use of technology in auditing were limited to the internal audit sector since they are less bound by restrictive statutory requirements (Kuenkaikaew and Vasarhelyi, 2013). However, as technologies continue to develop at an exponential rate, it is logical for the external auditing profession to respond to such changes in order to remain relevant in a modern and digitally-enabled world. Taken together, it is vital to consider the transformation of the traditional external auditing model in light of technological change.

The traditional external auditing model that enables auditors to draw conclusions regarding the underlying information on the audit client's financial statements is comprised of analytical procedures for risk assessment, procedures to test the operating effectiveness of internal controls, and substantive procedures, including substantive analytical procedures and tests of details (Louwers et al., 2013). DA (data analytics) permeates the traditional audit model, in fact, it is difficult to envision a financial statement audit that does not use DA (Stewart, 2015).

5.1 ADA 1.0 & ADA 2.0

Given that data analytics is a salient component of the external audit model, it is of interest to divide this construct into taxonomies that reflect its potential evolution. At present, external auditors perform DA procedures such as scanning, trend, or ratio analysis (Stewart, 2015); these are simple DAs and were initially introduced around the 1980s when the AICPA issued guidance for analytical procedures (AICPA, 1989). Hence, it is logical to infer that this is the first generation of audit data analytics, ADA 1.0. As technology progressed and computing power increased, audit software vendors including, IDEA and ACL, which primarily serve the internal auditing sector, began to develop audit analytic tools that improved the auditing process by enabling auditors to examine complete populations of data with increased frequency and little human intervention. These auditing tools range from simple learning algorithms to more sophisticated

statistical and machine learning models and comprise the second generation of audit data analytics, ADA 2.0. Today, the external auditing profession is slowly, but steadily evolving from ADA 1.0 to ADA 2.0 (Appelbaum et al., 2017).

5.2 ADA 3.0

With blockchain smart contracts, ADA advances to its next natural progression, ADA 3.0. Essentially, the blockchain platform facilitates the deployment of smart audit procedures that autonomously execute predictive models, identify notable items, and deliver close to real-time audit reporting on behalf of the external auditor. Smart audit procedures have the potential to improve audit quality and mitigate the expectation gap between auditors and stakeholders. When auditing using smart audit procedures, there are two perspectives that should be considered: 1) the audit risks these procedures are designed to respond to, that is, the audit client's business risks, and 2) quality control processes for these procedures (i.e. their reliability).

With respect to the first implication, blockchain and smart contracts business practices for audit clients create new audit risks, consequently, smart audit procedures would be designed to respond to existing audit risks and new risks that emerge as a result of these new business practices. Secondly, the development of data analytic tools should be validated ex-ante and ex-post to assess their reliability (IAASB, 2016). Smart audit procedures and other tools that interact with these procedures, such as the blockchain deployed by the external auditor, and oracles[5] that interact with the external auditor's blockchain, should be verified to ensure they are operating as intended. Collectively, the risk response schemata of smart audit procedures and the protocol validation of smart audit procedures are important considerations.

5.3 Responding to Audit Risks

Smart audit procedures that help auditors assess audit risks comprise smart analytical procedures and smart internal control tests that autonomously execute audit objectives on behalf of the external auditor. Table 1 describes significant audit risks that pertain to the revenue process. Audit risks are categorized as existing risks, for those risks that exist in revenue regardless of the system that

---

[5] Oracles are the interface between smart contracts and the outside world (Bartoletti and Pompianu, 2017), they store data that resides outside of the blockchain and that interacts with blockchain smart contracts.

captures revenue transactions, and new risks, for those risks that emerge as a result of blockchain and smart contracts adoption by audit clients.

For the risk of entering fictitious, unauthorized, or erroneous sales contracts, auditors presently select a sample of sales contracts and manually review the terms of these contracts. Alternatively, auditors can use NLP (natural language processing) and deep learning software to automatically review the terms of contracts for the complete sales contract population (Yan, 2017). The results of this procedure is aggregated along with the results of other procedures to arrive at a qualitative audit opinion about the reasonableness of the underlying financial information on the client's financial statements. However, as financial statement users, and regulators have different information needs (Romero et al., 2012), blockchain smart audit procedures have immense potential to not only assist the external auditor in improving audit quality but also meet the various information needs of different parties that expand beyond a qualitative audit opinion.

	Audit Risk	**Smart Audit Procedure**	**Traditional Audit Procedure**
Existing	Fictitious, unauthorized, or erroneous sales contracts are entered into the system	Dual-purpose Smart Audit Procedure is configured to **autonomously** match key provisions in initial client smart contract code to key provisions in client smart contract code for the period under audit	Auditor selects a sample of PDF client sales contracts and examines key contract provisions
		Dual-purpose Smart Audit Procedure is configured to **autonomously** match client smart-contract customer name to client blockchain active digital wallets	
		Smart Internal Control Test is configured to **autonomously** match the access level of customer nodes (i.e. send transactions) on client blockchain	

	Goods shipped are not recorded completely, or accurately	Smart Analytic is configured to **autonomously** learn and predict sales using financial and non-financial data and compare to actuals	Auditor performs analytical procedure to calculate sales based on price and quantity. This benchmark is used to compare to actuals
		Follow up Smart Analytic Procedure is configured to **autonomously** process error alerts identified in the first analytic	Auditor follows up and investigates notable items that are greater than, or below, benchmark
	Cash receipts are not accurately recorded or posted in the correct period	Not applicable as client blockchain ledger reconciles every sales transaction	Auditor selects sample of cash receipts balance and requests confirmation from external party
New	Client blockchain may not have a robust mechanism in place to assure data integrity	Smart Internal Control Test is configured to **autonomously** validate consensus mechanism on client blockchain	
		Smart Internal Control Test is configured to **autonomously** verify that no participant in client blockchain controls more than 51% of computing power	
	Client blockchain may post unauthorized transactions	Smart Internal Control Test is configured to **autonomously** verify active participants on client blockchain have authorized access	
	Client smart contracts may be created arbitrarily and without authorization	Smart Internal Control Test is configured to **autonomously** match number ofinitial client smart contracts to number of client smart contracts for the period under audit. For those contracts that are not matched, verify that they were created with proper authorization and for legitimate reasons	

	Client smart contracts that are outdated may be used in conjunction with replacement (substitute)client smart contracts	Smart Internal Control Test is configured to **autonomously** match client smart contracts that should be inactive to client smart contracts that are actually inactive	

Table 1. Smart Audit Procedures for Financial Statement Audit of Revenue

With smart audit procedures, the auditor can address the first audit risk by invoking a smart internal control test that matches the key contract terms from the period the client sales smart contracts were initially loaded to the client sales smart contracts code for the current period under audit. This smart procedure can be invoked by the auditor by sending client sales smart contract data to it; the results of these audit procedures can then be viewed by the parties on the external auditor's blockchain, depending on their information needs, close to real-time. For example, key suppliers would benefit from verifying that the audit client's contracts with key customers have not changed; the audit inspector would benefit from monitoring audit evidence that pass smart audit procedures and being able to develop an expectation for items that the external auditor should further investigate prior to the completion of the audit, that expectation can then be compared to actual items that were investigated by the auditor. Additionally, this audit procedure serves as a dual-purpose procedure as it collects audit evidence about the existence and values of these contracts.

Assuring the client's blockchain and smart contract protocol is operating as intended are new audit risks that emerge as a result of using this technology and thus creates the demand for a new type of IT audit. The blockchain's infrastructure of immutability and decentralization certainly helps external auditors address the risk of inaccurate cash receipts. Thus, if the blockchain protocol IT audit asserts the consensus mechanism is appropriate, and that no client blockchain participants control more than 51% of the blockchain, then external customer confirmations are not necessary as the blockchain reconciles each payment that is received by the customer. External confirmations become irrelevant in a blockchain ecosystem that operates effectively as auditors have the ability to obtain the hash for a particular transaction of interest to verify its

existence, occurrence, and valuation. As a result, blockchain protocol that has been validated offers transaction-level confirmations.

From a client smart contract perspective, the auditor would have to consider the risks that contracts may be arbitrarily created without proper authorization and that outdated contracts are not being used by the client. Taken together, smart audit procedures that address financial statement account level risks, blockchain system,and client smart contracts risks have the potential to improve audit quality and meet the information needs of various parties.

The risks and respective procedures in Table 1 parallel a blockchain smart audit procedure model to envision the evolution of the audit model given blockchain and smart contract technologies, however, it is important to emphasize that not all components of financial statement audits would be moved to blockchain smart audit procedures. Audit areas that relate to accounting complexities such as the valuation of fair value investments, or the tax provision, would be performed outside of the external auditor's blockchain. Thus, a holistic audit model would consist of a hybrid of blockchain smart audit procedures and outside of the blockchain audit procedures (Rozario and Thomas, 2017).

5.4 Validation of External Auditor Blockchain, Smart Audit Procedures, and Oracles

Establishing quality control procedures over data analytic tools has been emphasized by standard-setters and regulators (IAASB, 2016). Using blockchain with smart audit procedures and oracles as tools to audit financials statements requires specific validation checks that would enable auditors to rely on these technologies. Table 2 describes validation checks that would be required to achieve reliance on each of the aforementioned audit data analytic tools. For the external auditor blockchain, assurance over the consensus protocol, authorized node access, and security of private keys for digital wallets are validation checks that would be necessary to have reliance over blockchain and smart contracts technologies.

For smart audit procedures, assuring the protocol cannot be circumvented, i.e. that a blockchain participant cannot arbitrarily send and post audit evidence that does not conform to the logic in smart procedures, is paramount.   Similarly, assuring the interaction among smart audit procedures is appropriate (i.e. results

of smart analytic triggers follow-up smart analytic procedure as needed), that error alerts are created for auditors when audit logic is not conformed to, and that smart audit procedures are not created unless approved by both the audit firm and the audit inspector, is equally important. Finally, the provenance of oracles that interact with blockchain smart contracts should be verified.

ADA Tools	Validation Checks
External Auditor Blockchain	Assure verification (consensus) protocol for the validation of data that is posted to blockchain smart audit procedures agree to the conditions defined by primary blockchain participants, i.e. the audit inspector and the external auditor. Assure authorized participants have appropriate access to create smart audit procedures (external auditor), vet smart audit procedures (audit inspector), post audit evidence to the blockchain (external auditor), and limited, read-only, access to view results of audit procedures (investors, SEC, audit committee). Assure that only authorized users that are part of the external auditor's blockchain have secure access to private keys for their respective digital wallets. Assure audit evidence sent by external auditor is sent to regulator digital wallet address.
Smart Audit Procedures	Assure embedded audit logic cannot be circumvented by rogue participants. Assure smart audit procedures can be created only by the external auditor and approved by the audit inspector. Assure that external auditors do not send audit evidence to existing smart audit procedures with erroneous protocol and which are replaced by new smart audit procedures (since blockchain smart audit procedures cannot be retroactively revised). Assure smart audit procedures that have flagged errors invoke the correct follow-up smart procedures to process those errors. Assure that follow-up smart procedures create error alerts for auditors.

	Assure that smart audit procedures are not created unless approved by both the audit firm and audit inspector for legitimate reasons.
External Auditor Oracles	Assure the security and integrity of data stored in oracles, including the provenance of the systems outside of the blockchain that interact with oracles.
	Assure the data per the oracles reconciles to the data loaded and sent to blockchain smart contracts.

Table 2. Validation checks for data analytic tools in a blockchain smart audit procedure environment

6. PENDING CHALLENGES

The future of auditing was discussed by envisioning financial statements audits that benefit from blockchain smart audit procedures. Certainly, there will be challenges to overcome in the adoption of the hybrid audit model, such challenges relate to:1) current statutory requirements that require an annual and aggregate qualitative audit opinion, 2) challenges over the security and privacy of the external auditor blockchain and smart audit procedures, 3) challenges regarding the scalability of the blockchain and flexibility of smart audit procedures, and 4) challenges over the impact of smart audit procedures on auditor judgment. While blockchain and smart contracts technology will change the way financial statement audits are performed and delivered, the external audit profession would thrive by applying such technologies. Several blockchain smart audit procedures were proposed, yet a number of issues pertinent to the challenges mentioned warrant further research:

Current Statutory Requirements

- Is qualitative assurance relevant when results of smart audit procedures can be quantified?
- Should audit reviews, certifications, or seals of approval replace the annual audit opinion?
- How should statutory requirements change to encourage a close to real-time, and transactional level, audit reporting?
- Would the materiality concept change as companies shift towards a hybrid audit model?

- Would external auditors provide assurance over underlying information that makes up financial statements and the blockchain smart contract system?
- What are the IT risks and IT risk responses in blockchain smart contract systems that external auditors should address?

Security and Privacy of Blockchain and Smart Audit Procedures

- How to limit access to the results of smart audit procedures to cater to different information needs?
- Which audit objectives would remain off the blockchain and which would shift to smart audit procedures?
- Should client confidential information be loaded to the blockchain?

Scalability and Flexibility

- How should audit firms address erroneous code in smart audit procedures?
- How often should smart audit procedures be executed?
- How to process non-compliance alerts (error messages) from smart audit procedures?
- How should auditors manage outdated smart audit procedures?
- Should auditors store smart audit procedures workpapers in the same, or a different external auditor blockchain?

Impact on Auditor Judgment

- Do smart audit procedures and blockchain enhance auditors' professional skepticism?
- Do smart audit procedures and blockchain cause auditors to overrely on these technologies?

7. CONCLUSION

Given recent debates about the relevancy of the audit profession in a rapidly changing business world, it is important for audit firms, regulators, academics, and standard-setters to remain informed about recent technological developments that have the potential to disrupt business ecosystems and consequently, the audit ecosystem. The numerous initiatives on the impact of new technologies on financial statement audits suggest that external auditors are proactively making an effort to respond to a digital and modern economy. Moving towards a hybrid audit

model that includes blockchain smart audit procedures can enhance audit quality, cater to the information demands of different stakeholders, and thus parallel a digital business world.

This paper proposed a new type of ADA enabled by blockchain and smart contracts, smart audit procedures. Smart audit procedureswould be the next generation of ADA, ADA 3.0, and have the potential to change the way financial statement audits are performed and delivered. However, before smart audit procedures become feasible, there are challenges that should not be neglected, including challenges related to current regulatory requirements and challenges related to disruptive technologies that remain in early stages of adoption.

While the application and challenges of smart contracts to auditing were described, this study can be expanded in several ways. First, validating the audit client's blockchain is paramount and would give rise to a new type of blockchain IT audit. The aspect of auditing a business entity's blockchain was briefly considered as it is beyond the scope of this paper. Second, the conceptualization of an external auditor blockchain assumes that a permissioned blockchain is implemented. This study can be extended by examining the implications of performing smart audit procedures on a permissionless blockchain that is available to the general public and crosses transnational boundaries.

8. REFERENCES

ALLES, M.; BRENNAN, G.; KOGAN, A.; VASARHELYI, M. A. (2006): "Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens", International Journal of Accounting Information Systems, vol. 7, n. 2: 137-161. https://doi.org/ 10.1016/j.accinf. 2005.10.004

AICPA (1989): Analytical Procedures, AU Section 320, New York, NY. https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/download abledocuments/au-00329.pdf

AICPA (2017): Rutgers AICPA Data Analytics Research Initiative. https:// www.aicpa.org/interestareas/frc/assuranceadvisoryservices/radarprojects.html

APPELBAUM, D.; KOGAN, A.; VASARHELYI, M. A. (2017): "Big Data and analytics in the modern audit engagement: Research needs", Auditing: A Journal of Practice and Theory: November 2017, vol. 36, n. 4: 1-27. https://doi. org/10.2308/ajpt-51684

BADERTSCHER, B. A.; KIM, J.; KINNEY W.; OWENS, E. L. (2017): "Audit Procedures and Financial Statement Quality: The Positive Effects of Negative Assurance", Working Paper.

BARTOLETTI, M.; POMPIANU, L. (2017): "An empirical analysis of smart contracts: platforms, applications, and design patterns". https://arxiv.org/pdf/ 1703.06322.pdf. https://doi.org/10.1007/978-3-319-70278-0_31

BENKLER, Y. (2007): "The wealth of networks: How social production transforms markets and freedom", The Yale Law Journal, vol. 116, n. 7: 1472. https://doi.org/10.2307/20455766

BRAFMAN, O.; BECKSTROM, R. A. (2006): The starfish and the spider: The unstoppable power of leaderless organizations, Penguin.

BUTERIN, V. (2014): "A next-generation smart contract and decentralized application platform", White paper.

DAI, J.; VASARHELYI, M. A. (2017): "Towards Blockchain-based Accounting and Assurance", Journal of Information Systems: Fall 2017, vol. 31, n. 3: 5-21. https://doi.org/10.2308/isys-51804

DECOVNY, S. (2015): "Chips Off the Old Blockchain", CFA Institute Magazine, vol. 26, n. 6: 24-25. https://doi.org/10.2469/cfm.v26.n6.8

FANNING, K.; CENTERS, D. P. (2016): "Blockchain and Its Coming Impact on FinancialServices", Journal of Corporate Accounting & Finance, vol. 27, n. 5: 53-57.onlinelibrary.wiley.com/doi/10.1002/jcaf.22179/pdf

FORBES (2016): "Thirteen Companies that Use Deep Learning to Produce ActionableResults".https://www.forbes.com/sites/kevinmurnane/2016/04/01/thirteen-companies-that-use-deep-learning-to-produce-actionable-results/#59f0590633b8

IBM (2017): "Implementing Blockchain for Cognitive IoT Applications". https://www.ibm.com/developerworks/cloud/library/cl-blockchain-for-cognitive-iot-apps-trs/cl-blockchain-for-cognitive-iot-apps-trs-pdf.pdf

IAASB (2016): Exploring the Growing Use of Technology in the Audit, with a Focus on Data Analytics. New York, NY: IFAC.

IAASB (2017): Data Analytics. http://www.iaasb.org/projects/data-analytics

ISSA, H.; KOGAN, A. (2014): "A predictive ordered logistic regression model as a tool for quality review of control risk assessments", Journal of Information Systems, vol. 28, n. 2: 209-229. https://doi.org/10.2308/isys-50808

JARVENPAA, S.; TEIGLAND, R. (2017): "Introduction to Trust, Identity, and Trusted Systems in Digital Environments Minitrack", In Proceedings of the 50th Hawaii International Conference on System Sciences.

KIVIAT, T. I. (2015): "Beyond Bitcoin: Issues in Regulating Blockchain Transactions", DukeLaw Journal, vol. 65: 569-569.

KOGAN, A.; ALLES, M. G.; VASARHELYI, M. A.; WU, J. (2014): "Design and evaluation of a continuous data level auditing system", Auditing: A Journal of Practice & Theory, vol. 33, n.4: 221-245. https://doi.org/10.2308/ajpt-50844

KUENKAIKAEW, S.; VASARHELYI, M. A. (2013): "The Predictive Audit Framework",The International Journal of Digital Accounting Research, vol. 13, n. 2: 37-71. https://doi.org/10.4192/1577-8517-v13_2

KUHN, J. R.; SUTTON, S. G. (2010): "Continuous auditing in ERP system environments: The current state and future directions", Journal of Information Systems, vol. 24, n. 1: 91-112. https://doi.org/10.2308/jis.2010.24.1.91

LOUWERS, T. J.; RAMSAY, R. J.; SINASON, D. H.; STRAWSER, J. R.; THIBODEAU, J. C. (2013): Auditing and assurance services: McGraw-Hill/Irwin New York, NY.

MAES, P. (1994): "Agents that reduce work and information overload", Communications of the ACM, vol. 37, n. 7: 30-40. https://doi.org/10.1145/176789.176792

MAINELLI, M.; SMITH, M. (2015): "Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)", The Journal of Financial Perspectives, vol. 3, n.3: 38-69.

MATTHEWS, D. (2006): "From ticking to clicking: changes in auditing techniques in Britain from the 19th century to the present", The Accounting Historians Journal, vol. 33, n. 2: 63-102. https://doi.org/10.2308/0148-4184.33.2.63

MOON, D. (2016): Continuous risk monitoring and assessment: CRMA. Doctoral dissertation, Rutgers University-Graduate School-Newark.

MURTHY, U. S.; GROOMER, S. M. (2004): "A continuous auditing web services model for XML-based accounting systems", International Journal of Accounting Information Systems, vol. 5, n.2: 139-163. https://doi.org/10.1016/j.accinf.2004.01.007

NO, W. G.; VASARHELYI, M. A. (2017): "Cybersecurity and Continuous Assurance", Journal of Emerging Technologies in Accounting, vol. 14, n. 1: 1-12. https://doi.org/10.2308/jeta-10539

NWANA, H. S.; NDUMU, D. T. (1999): "A perspective on software agents research", The Knowledge Engineering Review, vol. 14, n. 2: 125-142. https://doi.org/10.1017/s0269888999142012

PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (2016): Audit Expectations Gap: A Framework for Regulatory Analysis. Washington, D.C: PCAOB. https://pcaobus.org/News/Speech/Pages/Franzel-speech-Institute-12-13-16.aspx

PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (2017): PCAOB Adopts New Standard to Enhance the Relevance and Usefulness of the Auditor's Report with Additional Information for Investors. Washington, D.C: PCAOB. https://pcaobus.org/News/Releases/Pages/auditors-report-standard-adop tion-6-1-17.aspx

PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (2017): Staff Inspection Brief. https://pcaobus.org/News/Releases/Pages/staff-inspection-brief-2017-issuers-8-30-17.aspx

PWC (2016): How Smart Contracts Automate Digital Business. http://usblogs.pwc.com/emerging-technology/how-smart-contracts-automate-digital-business/

ROMERO, S.; GAL, G.; MOCK, T. J.; VASARHELYI, M. A. (2012): "A measurement theory perspective on business measurement", Journal of Emerging Technologies in Accounting, vol. 9, n. 1: 1-24. https://doi.org/10.2308/jeta-50396

ROZARIO, A.; THOMAS, C. (2017): "Reshaping the Audit with Blockchain and Artificial Intelligence: An External Auditor Blockchain for Close to Real-Time Audit Reporting", Rutgers University Working Paper.

SZABO, N. (1994): "Smart contracts". http://www.fon.hum.uva.nl/rob/Courses/ InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh. net/smart.contracts.html

SZABO, N. (1997): "Formalizing and securing relationships on public networks". First Monday, vol. 2, n. 9. https://doi.org/10.5210/fm.v2i9.548

STEWART, T. (2015): Data analytics for financial-statement Audits, Chapter 5 in AICPA, Audit Analytics and Continuous Audit: Looking Toward the Future, American Institute Of Certified Public Accountants. New York, NY 2015

SWAN, M. (2015): Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.

TAPSCOTT, D.; TAPSCOTT, A. (2016): "Blockchain revolution", 1st ed. New York: Portfolio-Penguin.

VASARHELYI, M. A.; HALPER, F. B. (1991): "The continuous audit of online systems", In Auditing: A Journal of Practice and Theory.

VASARHELYI, M. A.; HOITASH, R. (2005): "Intelligent Software Agents In Accounting: an evolving scenario", The Evolving Paradigms of Artificial Intelligence and Expert Systems: An International View, 6.

VASARHELYI, M. A.; KOGAN, A.; TUTTLE, B. M. (2015): "Big data in accounting: An overview", Accounting Horizons, vol. 29, n. 2: 381-396. https://doi.org/10.2308/acch-51071

VAZIRI, A. (2016): "SMART BOL – Reducing Contractual Enforcement Costs". https://www.chainofthings.com/news/2016/11/23/smart-bol-reducing-contractual-enforcement-costs

YAN, Z. (2017): "Automate Contract Analysis in Auditing", Rutgers University Working Paper.

YOON, K. (2016): "Weather Variables as Audit Evidence", Doctoral dissertation – Chapter 4, Rutgers University-Graduate School-Newark.

YERMACK, D. (2017): "Corporate governance and blockchains", Review of Finance, vol. 21, n. 1: 7-31. https://doi.org/10.1093/rof/rfw074