The International Journal of Digital Accounting Research
Vol. 21, 2021, pp. 155-181
ISSN: 2340-5058

On the impact of smart contracts on auditing

Javier De Andrés. University of Oviedo. Spain jdandres@uniovi.es

Pedro Lorca. University of Oviedo. Spain plorca@uniovi.es

Abstract. The use of smart contracts has grown exponentially over the last few years. This is a phenomenon associated with the development of other technologies, such as the blockchain and the Internet of Things (IoT). Smart contracts run in a decentralized way on the blockchain and are self-executing. This is a source of advantages in business operations, but there are also some limitations and drawbacks. Regulatory issues are also of key importance, as the legal frameworks differ across countries. Smart contracts are likely to have an impact on external auditing, as external auditors will have to adapt their capabilities and procedures to an environment where many companies use this technology. But smart contracts may also be used to define a framework which ensures continuous audit reports and direct access of authorized stakeholders to the results of audit procedures. Conversely, internal auditing will also experiment changes, both caused by a series of new risks that will have to be adequately addressed and new tools to monitor business operations. In addition, some promising research opportunities arise, both in the IT, the Legal and the Business field.

Keywords: Smart contracts, external auditing, internal auditing.

1. INTRODUCTION

The smart contract concept was formalized more than 30 years ago by Nick Szabo, who defined smart contracts as “computerized transaction protocols that execute terms of a contract” (Szabo, 1996). This original concept has evolved since then due to the advances in information technologies. Nowadays, certain developments

Submitted April 2021
Accepted June 2021

DOI: 10.4192/1577-8517-v21_6

such as the blockchain and the Internet of Things (IoT) allow a wider implementation of smart contracts. Blockchain ensures security and transparency of all records. This benefit can be reinforced when the company extensively uses IoT devices so the verification of compliance with contracts can be done in an automatic way. So, smart contracts are an important element in the development of Industry 4.0 initiatives. In the long term, smart contracts may eventually contribute to the development of distributed and decentralized autonomous organizations (DAOs), which are entities completely operating in an autonomous way (Jarvenpaa & Teigland, 2017).

Due to such advantages, the global market of smart contracts is expected to exceed $ 200 million by 2025 (marketsandresearch.biz, 2020). However, its use also involves risks. For example, a study by Chen et al. (2018) reports the use of smart contracts to defraud significant amounts through Ponzi schemes. Smart contracts have also been used in honeypot frauds (Torres & Steichen, 2019) as well as for cyberattacks, including the stealing of digital currency (Apostolaki et al., 2017).

All this may have a substantial impact on auditing, both external and internal. First, the external auditors of an organization that extensively uses smart contracts must address some issues. Among these, we can highlight the readability of the code and the assessment of the new risks of a smart contract ecosystem. However, some auditing tasks can be either automated or are not needed anymore (i.e. external confirmations). But the impact of smart contracts on external auditing is not limited to the need for addressing the features of the new business environment, as smart contracts can be a tool to redefine the external audit framework. Some proposals outline the capabilities of smart contracts to store audit evidence which contributes to satisfying the information needs of different stakeholders, thus reducing the audit expectations gap.

Conversely, smart contracts also cause an impact on internal auditing. New risks arise and others will be mitigated / eliminated due to the autonomous execution, forge resistance, transparency, and other capabilities of this technology. In this regard, the key importance of security issues must be highlighted. But smart contracts can be also used to replace / improve existing internal auditing procedures. As an increasing number of companies engage in Industry 4.0 initiatives, IoT devices are more common, and this fosters the use of smart contracts in internal auditing processes. Another favouring factor that can be mentioned is the increasing need for companies to check the compliance with a growing body of health / food / environmental regulations.

In recent years the Big Four accounting firms have been researching and investing resources on blockchain (Bonyuet, 2020). Deloitte was the first Big Four firm to become involved with this technology, with the development of its first blockchain lab in Dublin. PwC is partnering with Northern Trust, a leading global asset management firm, to enable real-time audits via Blockchain and therefore, ensuring transparency in all transactions. PwC has also released a cryptocurrency auditing solution to meet the needs of firms engaged in cryptocurrency transactions. Likewise, in April 2018, Ernst & Young (EY) released Blockchain Analyzer, which allows capture of the entire transaction data from a firm's multiple blockchain ledgers. In March 2019, EY launched Crypto-Asset Accounting and Tax (CAAT) software to assist US firms to report their crypto asset transaction when filing their tax returns.

However, the use of this technology in auditing also has limitations. First, smart contracts cannot be applied to every area of auditing and every sector of activity, as some tasks still need a significant amount of human intervention. Second, there are also technical issues to solve. Among them we can highlight the problems related to net traffic in an IoT environment and privacy issues. Finally, more regulation is still needed, both general regulation governing the lifecycle of a smart contract and a framework for the use of smart contracts to store / access audit evidence. All these areas constitute gaps in the literature that could eventually be addressed by future research efforts.

In addition, and to the extent we know, there are no prior papers that provide a comprehensive overview of the current and future trends of the use of smart contracts in auditing. This is the main objective of the present research. We detail the current and future impact on both internal and external auditing of the diffusion of the smart contract technology. These effects go beyond the technical / operational aspects and will have organizational implications as well as change the auditing profession. We also outline the main research opportunities that arise, including those belonging to the IT, the Legal and the Business fields.

The remainder of the paper is structured as follows: section 2 provides a brief introduction to the blockchain-based smart contracts technology, the most used platforms, and the main regulations. Legal issues on smart contracts are discussed in Section 3. Section 4 comments on the effects of smart contracts on external auditing, addressing both the issues that arise when auditing an organization that uses smart contracts and smart contracts as a tool for external auditors. Section 5 discusses the impact of smart contracts on internal auditing. Again, we consider both the internal control and other internal auditing questions for an organization that extensively uses smart contracts and some possibilities to improve internal auditing processes. In section 6 new research opportunities are presented. Finally, section 7 contains a summary and the main conclusions of this research.

2. SMART CONTRACTS: STATE-OF-THE-ART

The idea of smart contracts is not new as it was proposed before the emergence of blockchain and other distributed ledger technologies (DLT). In this way, early definitions such as those from Szabo consider smart contracts just as “automated contracts” without referring to any implementation issue. However, the blockchain offers a distributed infrastructure which fosters the creation and use of smart contracts, as it ensures integrity and security. To do this, it operates without a trusted third party. An introduction to blockchain and a brief discussion of its application to Accounting can be found in Dai and Vasarhelyi (2017), and a description of the lifecycle of a blockchain-based smart contract can be seen in Rozario and Vasarhelyi (2018), Zheng et al. (2020) and Hewa et al. (2021), among others.

So, in many recent definitions, both academic and legal, the blockchain is a requisite for the existence of a smart contract. For example, Ante (2021) defines it as “a script that is anchored on a blockchain or similar distributed infrastructure”. In a similar vein, the legislation of the US state of Arizona, which was a pioneer in the regulation of smart contracts, states that it is an “event driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger that can take custody over and instruct transfer of assets on that ledger” (State of Arizona, Bill HB 2417, 2017).

Smart contracts involve a creation phase, followed by deployment, execution and completion phases (figure 1). First phase is similar to the development of any other software product. However, the latter three phases involve recording transactions in the blockchain, which remain immutable, and any modification means the creation of a new contract. In smart contracts it is of special importance the definition of oracles, which are the interfaces between the smart contract and the outside world (Bartoletti & Pompianu, 2017). They store data that reside outside of the blockchain and are used to determine the outcome of the smart contract.

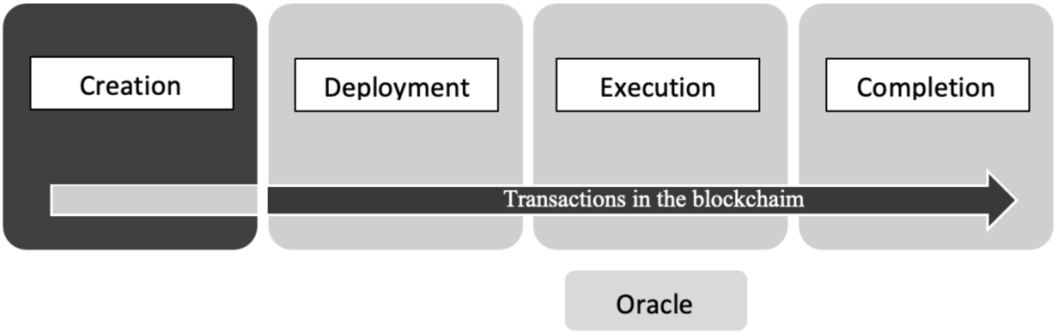

Figure 1. Phases in smart contracts

Currently, there are several platforms that can be used for smart contracts. Among them, we can highlight Hyperledger Fabric, Corda, Stellar, Rootstock, Eos, Waves, New Economy Movement (NEM) and Ethereum. All of them have different characteristics in terms of execution environment, supported languages, data model, consensus algorithms, permissions needed and other features. The most popular is Ethereum, with an associated cryptocurrency which is the second in market capitalization after Bitcoin[1]. Ethereum supports a series of programming languages, namely Solidity, Yul, LLL (Low-level Lisp-like Language), and others, which allow the deployment of a wide variety of user applications. The programs are compiled into a bytecode and then loaded to the Ethereum Virtual Machine (EVM) and run. The EVM is a distributed runtime environment and the users have to buy gas (the unit of account in the EVM) to reward the miners in order to have the program stored in the Ethereum blockchain and executed. The total cost depends on (a) the gas amount (gas cost in Ethereum terminology), which in turn depends on the computation and storage resources needed for the program, and (b) the gas price, which is the amount of the Ethereum cryptocurrency (Ether) to be paid per unit of gas. So, if the user wants their program to be executed faster, a higher gas price should be offered. A detailed review of Ethereum and the rest of platforms can be seen in Wang et al. (2018) and Zheng et al. (2020).

Smart contracts can facilitate safe and trusted business activities by providing automated transactions without the supervision of an external financial system such

[1] https://coinmarketcap.com

as banks, courts, or notaries. These transactions are traceable, transparent, and irreversible (Singh et al., 2020). Then, the use of smart contracts is a source of advantages in business operations. First, it is possible to achieve efficiency gains, as they allow time savings, and a more efficient corporate governance, among other benefits (Angelo et al., 2019). Second, cost reductions can be achieved. For example, contract drafting can be cheaper, and the costs caused by the ambiguities of written language can be avoided (Sklaroff, 2017). Although the implementation of a blockchain involves fixed costs, their impact can be mitigated through adjustments in the strategy of the firm (De Giovanni, 2020). This is because transactions using blockchain/smart contracts add value for clients, as they perceive less risk. So, companies have the possibility to adjust their pricing policies as customers may be willing to pay higher prices for the goods/services purchased. Third, smart contracts allow autonomy, understood as freedom from state intervention (Raskin, 2017). Finally, they emanate a disintermediation which can offer automated consumer protection, shifting it from courts (Fairfield, 2014).

Therefore, new proposals are presented for use in different business areas. For example, Han et al. (2020) proposed a smart contract architecture for decentralized energy trading and management based on blockchains that is able to achieve an efficient and effective transaction with multi-player participation. Ahmadisheykhsarmast and Sonmez (2020) developed a novel smart contract payment security system for eliminating or reducing payment issues in the construction sector. In connection to this, Prause (2019) argues that smart-contract applications linked to smart supply chain management, IoT and Industry 4.0 can provide solutions to critical challenges in the area of smart manufacturing and logistics.

However, smart contracts also have some limitations and issues that should eventually be addressed. First, efficiency gains may not be achieved in sectors which are not characterized by standardized contractual terms and recurrent operations (Madir, 2018), and sometimes contracts imply general principles and terms which are not easily translated into digital form (Tjong Tin Tai, 2018). As examples of this, we can highlight the rendering of certain complex services (i.e. employment). Furthermore, contractual terms can be intentionally left vague because of an unwillingness to invest resources in negotiations or drafting. The ambiguity of provisions in contracts may also reflect the stronger position of one of the parties. In addition, in some sectors contracts may be only a formality while the "real" agreement is reflected in the ongoing commercial relationship (Mik, 2017).

Second, cost reductions may not occur as cost savings may be outweighed by implementation costs (Ferreira, 2021). Furthermore, the automated execution of smart contracts does not eliminate the potential for a dispute that requires judicial intervention (Mik, 2017), and this means a limitation to the autonomy benefit. This may be exacerbated by the fact that judges may struggle to regard programming code within a smart contract as legally 'certain' (Giancaspro, 2017). Third, the disintermediation and automation, rather than increase consumer protection, may reverse the burden of proof, causing a disadvantage to consumers (Ferreira, 2021). Fourth, it is difficult to ensure the contractual capacity of the parties to the contract. In a smart contract the parties may not know each other, and it could be the case that one of them does not have the capacity to contract. For example, there is a very real risk that a party who has attained the age of majority may inadvertently contract with a minor cloaked by the anonymity of the Internet (Giancaspro, 2017). Fifth, scalability problems may arise. Scalability is the measure of a system's ability to increase or decrease in performance and cost in response to changes in application and system processing demands. Blockchain networks have a scalability problem in terms of their limitations in the number of transactions they can process. Public blockchains such as Ethereum and Bitcoin suffer from this problem as the Ethereum network can process approximately 15–25 transactions per second, while Bitcoin's maximum throughput is 3.3–7 transactions per second (Croman et al., 2017). In contrast, traditional centralized financial systems such as VISA can process over 1700 transactions per second. Hence, in order to compete with such centralized financial systems blockchains need to be scalable both in terms of handling network load and processing transactions (Singh et al., 2020).

Finally, it is noticeable that the diffusion of smart contracts poses technical challenges both at the stages of creation (readability, functional issues), deployment (contract correctness, dynamic control flow), execution (execution efficiency and computation overhead on blockchain, among others) and completion (privacy and security, among others) (Zheng et al., 2020, Sookhak et al., 2021). In this regard, all digital technologies are vulnerable to attacks from cybercriminals, and smart contracts are no exception. Cybercrime generates very high costs for businesses and national economies. As business transactions increase through digital technologies and huge volumes of personal and financial information are digitized, the risk of security breaches increases exponentially. The use of smart contracts necessarily involves the digitization of the entire transaction between the parties, which could expose them to an increased risk of sensitive information being compromised (Giancaspro, 2017).

To sum up, Macrinici et al. (2018) explored the literature on the subject of problems and their solutions of smart contracts applied to blockchain platforms. They performed a classification of problems in accordance with the taxonomy of vulnerabilities established by Atzei et al. (2017), and three categories of problems were identified:

- The blockchain mechanism category. It refers to consensus mechanism, sacrificed performance for scalability, unpredictable state, randomness generation, timestamp dependency, lack of reimbursement and unilateral abortion.
- The contract source code category. It comprises lack of privacy (preserving privacy), call to the unknown, exception disorder, gasless send (out of gas exception), type casts mismatch and re-entrancy.
- The virtual machine category. It concerns programming smart contracts, stack overflow and cryptocurrency transfer loss.

Although the problems are many, the fact is that the technologies themselves may provide solutions to them.

3. LEGAL ISSUES ON SMART CONTRACTS

As several authors state (Ante, 2021), both the term smart and the term contract may be misleading, since a smart contract consists of dumb computer code and it is not guaranteed that it represents a legally binding construct. So, regulations have been passed and a legal debate has aroused. A priori, it would be easy to assume that smart contracts would be treated like any other legal contract. However, a brief examination of their nature and the various established principles of contract law shows that there are likely to be some theoretical and practical difficulties and inconsistencies (Giancaspro, 2017). The legal validity of contracts concluded by electronic means has been the subject of analysis in recent years. In many legal systems, contracts were required to be in writing, otherwise the contract would be null and void or subject to invalidity (De Graaf, 2019).

Legislative response has not been homogeneous depending on the country, and even inside certain countries different regulations coexist. This is the case of the USA, where some states have passed comprehensive regulations (New York, Nevada, Wyoming) and some others have codified limited aspects of the use of smart contracts (Delaware, Arizona, Tennessee, Arkansas, North Dakota). In contrast, many USA states have limited their response to the creation of task forces to explore the issues and opportunities offered by this technological development, and are waiting for federal regulations which are of application at the national level. Some authors (Arcari, 2019, Grenon, 2019) are of the opinion that USA regulations of smart contracts are mainly promotions of particular jurisdictions and may have unforeseeable effects due to the immaturity of the technology.

In the case of the European Union attempts were made to remove barriers as well as to facilitate electronic contracting. The E-Commerce Directive (art. 9, paragraph 1) obliges the Member States to “ensure that their legal system allows contracts to be concluded by electronic means” and that “the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means” (De Graaf, 2019). However, for the specific case of smart contracts it has been officially recognized in a Report that there is not a clear legal framework (European Parliament 2020). This Report also recommends that the future Digital Services Act, which is intended to upgrade the rules governing digital services in the EU, should, among other questions, determine the requirements for a smart contract to be considered as legally valid. In the absence of an EU legal framework, some countries have passed specific regulation. We can mention the cases of Malta, which in 2018 passed the Innovative Technology Arrangements and Services (ITAS) Act, Italy, where according to Law No. 12/2019 smart contracts are considered valid when they comply with the requirements of the Agenzia per l’Italia Digital (AgID), and especially Estonia, a country with an outstanding level of digital infrastructure and innovative concepts such as the Estonian digital identity or an e-residency that grants its holder a number of rights. However, some others (i.e. France, Spain, among others) have not and therefore smart contracts are regulated by e-business laws and general commercial law. It is noticeable that blockchain regulation across the EU is still mostly related to Initial Coin Offerings (ICOs) and cryptocurrencies rather than to smart contracts. As the European Securities and Markets Authority (ESMA) points out, stronger regulatory efforts are needed in order to achieve a level playing field across the EU and prevent consumers being exposed to substantial risks.

For the case of common law countries, we can highlight a report issued by the UK Jurisdiction Task Force (2019) on the status of cryptoassets, DLTs and smart contracts. It concludes that smart contracts can be implemented and interpreted under the current legal framework and the contract law doctrine. Some other authors (Vos, 2019) also state that in common law countries commercial law has enough flexibility to support smart contracts and other technological innovations. In accordance with this line of thought many countries, and not only those having common law systems, have not yet passed any specific regulation on smart contracts. Among these, we must highlight the cases of China and Japan, the most developed countries that, to date, have remained silent on this issue.

However, the legal debate cannot be considered to be over. For example, McJohn and McJohn (2017) point out that in the case a smart contract is created by artificial intelligence, under the legal framework of many countries it could not be considered as a legal contract, since the machines have no will and therefore cannot generate any agreement, thus generating a legal uncertainty.

So, there are also reasons that support a specific regulation. This is the path followed by some Eastern European countries (i.e. Russia and Belarus). However, as Ferreira (2021) notes, smart contract regulations rarely go beyond the definition of what is considered a smart contract. In addition, different definitions and regulations may prove to be problematic for the blockchain industry which is inherently cross-border. Moreover, and regarding to procedural issues, we must underline that whereas error correction with traditional non-digital contracts is relatively straightforward, the same cannot be said of smart contracts. This may present something of a logistical nightmare for courts trying to apply traditional contract law principle to rectify errors with a smart contract (Giancaspro, 2017). Therefore, some authors (Savelyev, 2017) have suggested as an alternative to traditional enforcement practices and judicial prosecution the consideration of the state as a superuser with extra powers.

Finally, the role of financial professionals and commercial lawyers will change. The very premise of smart contracting is disintermediated automation; the contract between the parties executes itself and no trusted intermediary is needed to affect the exchange of consideration between the parties. The intermediary in most non-digital commercial transactions is a financial or legal person or authority. But in a digital environment, the traditional functions of many financial professionals and commercial lawyers can now be performed directly by smart contracts, putting their roles at risk. Nevertheless, there will still be a place in the world for lawyers and other professionals who are deeply embedded in our global economies and who think in a way that computers simply cannot (Giancaspro, 2017).

4. EFFECT OF SMART CONTRACTS ON EXTERNAL AUDITING

As indicated in the introduction, smart contracts are exponentially adopted by business organizations and other entities, and this poses new challenges to auditing. Furthermore, they can be used by external auditors as a tool to assist in auditing all type of organizations (Roszkowska, 2021).

4.1. Auditing an organization with smart contracts

Smart contracts are suitable to have a significant impact on auditing, as they constitute supporting evidence of accounting records. So, they should be analyzed by auditors, just as ordinary written contracts.

In this regard, it is noticeable that the lack of readability of smart contracts can make them opaque to external auditors. Zhou et al. (2018) estimated that for more than 77% of smart contracts only the compiled code is available, but not the source code. To address this issue, a number of technical solutions have been proposed, including reverse engineering tools (Zhou et al., 2018), semi-automated translation systems (Frantz & Nowostawski, 2016), the use of programming languages that do not require compilation (Ciatto et al., 2018) and the definition of specific programming languages to make the execution of a smart contract human-readable (Kasampalis et al., 2018). In addition, some authors (De Graaf, 2019) propose the passing of laws enabling third party auditors to ensure the readability and reliability of the smart contracts code.

Furthermore, the extensive use of blockchain-based smart contracts in business operations leads to new risks which should be monitored by the external auditor in the evaluation of the strength of the internal control of the audited firm (Rozario &

Vasarhelyi, 2018). Among these, we can highlight the following: (a) blockchain may not guarantee data integrity, (b) unauthorized transactions may be posted to the blockchain, (c) smart contracts may be created without authorization, and (d) outdated smart contracts may be still active. These new risks require the implementation of additional audit procedures. In consequence, auditors need to have multidisciplinary teams composed of professionals with blockchain expertise.

However, as smart contracts are code which is machine-readable, and accounting records are also in digital form, some auditing tasks could be automated, thus reducing costs and time. For example, for smart contracts-based operations external confirmations are not needed as auditors can verify their occurrence and details.

In order to ease automation, it could be of great utility to have a definition of standard templates for smart contracts, which cover the most common business operations. In this regard, we can highlight some projects which are intended to contribute to this goal. OpenLaw[2] allows the automatic creation of Ethereum-based smart contracts to be embedded in legal agreements. In a similar way, Accord Project[3], provides open source common formats for smart contracts, thus enabling the reuse of agreement templates.

But once there are technological developments that provide useful standards, it would be of particular importance that such standardization efforts should be fostered by Public Bodies. For example, by establishing that certain types of smart contract in certain sectors (i.e.: financial, insurance) shall follow a mandatory format. In this way, it could be ensured that a “critical mass” is reached, thus ensuring wide diffusion and knowledge. In connection to this, we must mention that in another process of standardization related to digital accounting, which is the use of eXtensible Businees Reporting Language (XBRL), the diffusion of the standard was fostered by an external factor, the regulatory agencies, rather than by companies being aware of their advantages (Bonsón et al., 2009). Regulators made the greatest effort to promote the use of XBRL, mainly through the introduction of compulsory XBRL formats for financial statements.

[2] https://www.openlaw.io/

[3] https://accordproject.org/

4.2. The use of smart contracts for external auditing

Smart contracts deployed on a blockchain can be used to execute audit procedures in an automatic manner, thus providing close to real-time audit reporting (Rozario and Thomas, 2019). This is an evolution of the concept of continuous auditing, as introduced by Vasarhelyi and Halper (1991), among others. The main advantage of audit tools based on smart contracts is that a number of stakeholders may have limited (or total) access to the results of audit procedures. Among these, we can highlight key investors, audit commissions of companies, audit inspectors, securities commissions and bodies in charge of prudential supervision. This would eventually increase audit quality, reduce the audit expectations gap and help supervisory bodies to follow a more proactive strategy (Rozario & Vasarhelyi, 2018).

Although both internal control tests and audit analytical procedures can be implemented in a smart contract, it should be borne in mind that not all stages of external auditing are suitable to be implemented using this technology. Areas that involve accounting complexities such as for example fair value valuation or tax provisions should remain outside of the external auditor blockchain. So, the audit model would consist of a hybrid of smart contracts and external procedures (Rozario & Thomas, 2019).

Another issue to be solved is that for a wide application of this paradigm government bodies in charge of external audit regulation should issue regulatory technical standards about, for example, allowed platforms and languages, or the pieces of audit evidence that should eventually be released to the different stakeholders. In this regard, we must take into account that due to its relative novelty, the maturity of smart contracts technology is not very high. Moreover, a distributed audit architecture involves some risks, i.e. the forging of audit records (Zou et al., 2020). So, a feasible approach could be to delay regulations until consensus is reached about industry standards and the most relevant technical problems are solved.

In sum, the diffusion of smart contracts, either in audited companies or as a relevant part of the auditing parading, will mean that auditors' digital skills must be upgraded to deal with this new situation. In order to be able to perform this task, accountants and auditors will need to acquire technical understanding of, for instance, blockchain-based smart contract solutions and associated technologies such as artificial intelligence (Schmitz & Leoni, 2019). Eventually, this may lead to an increase of the level of interdisciplinarity of the auditing teams, which should use IT professionals much more frequently than now. In addition, as McGregor and Carpenter indicate (2020), another consequence of this is that smart contracts, as well as other emerging technologies, may attract non-audit firms to the industry, demanding a broadening of auditors 'skills, and therefore changing the structure of the audit market.

5. EFFECT OF SMART CONTRACTS ON INTERNAL AUDITING

Similar to external auditing, changes have to be made in the internal auditing processes of companies using smart contracts, but they are also a useful tool for internal auditing.

5.1. Internal auditing in an organization with smart contracts

Despite their advantages, smart contracts are also a source of threats to security and privacy, as most commonly used blockchain platforms lack mechanisms to preserve privacy, which may be eventually exploited by attackers. Thus, they constitute an issue in order to assure the internal control of firms. Some technical solutions have also been proposed to address privacy and security issues, including compilers with cryptographical protocols (Kosba et al., 2016), distributing blockchain data in different nodes (Shrobe et al., 2018), and adjusting the routing policies to prevent blockchain messages being intercepted (Apostolaki et al., 2019). As a way to overcome the reliability of network storage, Xu et al. (2020) propose a decentralized arbitrable remote data auditing scheme for network storage service based on blockchain techniques through smart contracts.

Another issue is that contract correctness should be carefully examined before deployment, as once the contract is in the blockchain, revision is not possible. A significant source of risk is the lack of knowledge of programmers about the business and legal aspects which determine the high-level workflows. This may lead to smart contracts which are technically correct but do not implement the required business logic (Almakhour, 2020).

In connection with this, functional correctness, that is, that the contract complies with the specifications provided by its designers, is of special importance. Some tools have been designed for the automatic detection of functional problems, and the most elaborated ones involve the use of machine learning techniques (Liu et al., 2018). There are also some frameworks for the formal (mathematical) verification of the correctness of smart contracts, and the most relevant are discussed in the work of Almakhour et al. (2020).

Even if the smart contract is functionally correct, significant problems can arise during its execution. For example, smart contracts may interact with other contracts, originating unpredicted transfers of funds and other undesired effects. This may also constitute a significant risk, which could be monitored using statistical procedures (Charlier et al., 2017). In connection with this, we can highlight the proposal of Hu et al. (2021), which successfully used machine learning methods to identify anomalous behavior of smart contracts.

Another source of risk is originated by the process of obtaining real-world information needed for the execution of a smart contract, which is gathered by a suitable oracle. Trustworthiness of oracles remain a challenge for a wider development of the smart contracts market. In this regard, some solutions have been proposed, from which we can highlight the use of decentralized voting schemes (Adler et al., 2018).

Internal control of smart contracts is even more important if we consider that a significant number of businesses are adopting Industry 4.0 initiatives. This means that the use of IoT devices is growing exponentially, and this also fosters the use of smart contracts. This is because there are a number of fields where this technology can be applied to IoT devices. Among these, we can mention scalable resource sharing, decentralization of data storage, operation of unmanned aerial vehicles (UAVs) and other autonomous vehicles, scalable connectivity in a smart city environment and edge computing, among others. A review of the smart contract application to IoT devices in business can be seen in Fotiou and Polyzos (2018) and Hewa et al. (2021).

The consequence of all this is that companies must establish organizational procedures and policies to guarantee an adequate internal control for the specific case of smart contracts, as more units inside the firm are involved in their creation and deployment. Such procedures and policies should also be reviewed by the external auditor, as part of the internal control assessment which is conducted during the external audit process.

5.2. The use of smart contracts for internal auditing

Blockchain-based smart contracts can also be used to execute internal control tests in an automatic manner, as well as to implement security policies which reduce the need for periodical checking.

A main area where smart contracts can replace traditional procedures is the addressing of security issues. First, we can highlight several proposals for auditing the management of access control through smart contracts (Outchakoucht et al., 2017, Cruz et al., 2018). These methods are an alternative to centralized security policies. We can also mention the work of Di Francesco Maesa et al. (2019), which is a proposal for the use of smart contracts to make the systems to control the access to digital resources auditable. This work also considers the scenario where the resources to be protected are smart contracts as well.

Security issues are even more important in an IoT environment, due to the high volume of net traffic and the low computational capabilities of many devices. Lone and Naaz (2021) review a number of technical solutions that use smart contracts which are mostly aimed at monitoring and addressing security weaknesses of IoTs when compared to general Internet connection. The majority of the proposals use the Ethereum platform. As these authors evidence, the most commonly addressed topics are access control and authentication. However, there are also technical solutions proposed for integrity preservation, authorization, or non-repudiation, among others.

However, as Dorri et al. (2019) outline, there is also an important question that should be addressed, which is that the IoT context may be incompatible with the high resource-demanding and network traffic of the most popular smart contracts platforms. So, scalable and lightweight platforms should be developed in order to use this approach with devices which have very limited computational capabilities.

Another area where internal audit is of key importance is cloud services. As relevant applications of smart contracts for internal auditing we can mention the works of Wang et al. (2020) and Yuan et al. (2020) which propose their use to audit the integrity of cloud-stored data, and the one by Xiong and Xiong (2020), to control the risk of data being sold. Cloud services can also be used to store IoT data and, in this regard, we can mention the proposal of Fan et al. (2020) to detect the existence of malicious behavior with regard to cloud-stored industrial IoT data. It is also relevant to consider the work by Tapas et al. (2020) which consists of a model for the independent audit of IoT-cloud resources in a smart cities' environment.

Another area where smart contracts can be used to reduce the cost of robust audits is logistics management. Supply chain compliance is a key requirement for a number of goods where traceability must be ensured (i.e. food, gemstones, among others). In this regard, we can mention some smart contract-based proposals aimed at ensuring the traceability of industrial components (Dietrich et al., 2020). As Wang et al. (2018) note, the implications of the application of smart contracts to logistics go beyond efficiency/costs and will have a socio-economic impact, which will even affect the structures of firms. However, the mentioned authors stress that there are also technical challenges, mainly related to the connectivity of the systems with the real world, which should be solved to take full advantage of the capabilities of this technology.

In connection with logistics, smart contracts can also be used to implement internal audit systems to comply with environmental regulations. This is because, to a certain extent, some aspects of environmental regulations are closely related to logistics, for example, those related to waste management and transport. Furthermore, others are direct application of certain IoT devices. An example of this is the model proposed in Dai et al. (2019) for the continuous audit of the performance on the control of air pollution. Nevertheless, as Hewa et al. (2021) indicate, there are still a number of research opportunities in this field which have not been fully exploited (i.e., the use of AI systems in combination with smart contracts).

6. NEW RESEARCH OPPORTUNITIES

In recent years, the number of research work on smart contracts has increased exponentially. This is because it is a topic with interesting practical implications. However, due to the novelty of this technology some avenues of research regarding the field of auditing, both external and internal, remain unexploited. As many papers show (Dai et al., 2019; Fan et al., 2020; Roszkowska, 2021) a literature gap still exists. The following are examples of research topics that are still unexploited:

- The study of how smart contracts deployed on a blockchain can be used to execute audit procedures automatically.
- Based on the former, the design of audit tools based on smart contracts.

- The analysis of the implementation of additional audit procedures to address the new risks that emerge because of the diffusion of smart contracts.
- The determination of the optimal composition of multidisciplinary audit teams for a smart contracts environment.
- The study and prescription of the role of public bodies in the quest for standardization.
- The determination of the optimal boundaries of the regulation, regarding, for example, the platforms and languages allowed, or the pieces of audit evidence that should eventually be delivered to the different stakeholders.
- The determination of the most adequate procedures and policies to ensure internal control for the specific case of smart contracts, as more organizational units within a firm are involved in their creation and deployment.
- The study of the impact on auditing profession (new job profiles, in-house training, etc.) caused by the diffusion of smart contracts.
- The proposal of procedures and strategies to build interdisciplinary auditing teams that include IT professionals.

In addition, we must bear in mind that smart contracts are a technological innovation which, apart from addressing new risks, is supposed to replace procedures which are done with older technologies. So, some other research opportunities arise:

- The determination of the reasons for the adoption, as it may be influenced by size, profitability (which may determine the resources a firm has to make IT investments), and other factors.
- The assessment of the effect of the adoption on performance, in order to test whether the implementation is successful. In other words, whether the benefits outweigh the costs.

Furthermore, another issue which may constitute an avenue for further research about smart contracts is to conduct technology acceptance studies. As smart contracts are a rather immature technology, no robust methodologies have been applied yet, and we can only mention the preliminary results of

Ahmadisheykhsarmast and Sonmez (2020) which indicate that a significant number of users are opposed / have reservations to the use of smart contracts to manage payments.

7. SUMMARY AND CONCLUSIONS

Smart contract is an old concept that has evolved in recent years thanks to the latest advances in technology, particularly blockchain and the IoT. They currently enable automated commercial transactions which are also secure, traceable, transparent, irreversible and trusted. In addition, there is no need for supervision by an external system such as banks, courts or notaries. Therefore, the use of smart contracts can be a source of advantages in business transactions: efficiency gains, cost reductions, autonomy and automated consumer protection.

However, smart contracts have also some drawbacks: efficiency gains may not be achieved in certain sectors and the implementation costs may be significant. Furthermore, the disintermediation and automation, rather than increase consumer protection, may reverse the burden of proof. In addition, difficulties may arise to ensure the contractual capacity of the parties, as well as scalability problems and vulnerability to attacks from cybercriminals.

The fact that smart contracts are a recent technology raises legal issues. As a result, national laws provide different solutions. However, there is a lack of uniformity between the different national regulations. Since smart contracts are not limited by borders, a harmonization effort at the international level would be desirable.

Smart contracts are suitable to have a significant impact on external auditing, as they can constitute supporting evidence of accounting records. So, they should be analyzed by auditors, just as ordinary written contracts. As smart contracts are code which is machine-readable, and accounting records are also in digital form, some auditing tasks could be automated, thus reducing costs and time. To facilitate automation, the definition of uniform templates for smart contracts, covering the most common business operations, would be very useful. This would require a collaboration effort that involves several Public Bodies. In addition, smart contracts can be used by external auditors to execute audit procedures automatically, thus providing near real-time reports, and allowing the possibility to grant certain stakeholders access to the results of audit work.

Smart contracts are also likely to have an impact on internal auditing. First, changes need to be made to the internal audit processes of companies using smart contracts. New organizational policies and additional audit procedures must be set to ensure an adequate internal control and the mitigation of the new risks that arise (privacy and security threats, functional correctness issues, and others). To cope with this complexity, internal auditors must rely on multidisciplinary teams composed of professionals with IT and business expertise. But, on the other hand, blockchain-based smart contracts can also be used to automatically run internal control tests, as well as to implement security policies that reduce the need for periodic checks.

Finally, we must underline that the diffusion of smart contracts in business is creating new research opportunities which may have an impact on its application to auditing. These avenues of research belong both to the IT field (i.e. design of tools and frameworks), to the Legal field (i.e. optimal extent of the regulation) and to the Business field (i.e. design of organizational policies, factors for the adoption and economic effects).

8. REFERENCES

Adler, J., Berryhill, R., Veneris, A., Poulos, Z., Veira, N., &Kastania, A. (2018). Astraea: A decentralized blockchain oracle. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). https://doi.org/10.1109/cybermatics_2018.2018.00207

Ahmadisheykhsarmast, S., & Sonmez, R. (2020). A smart contract system for security of payment of construction contracts. *Automation in Construction*, 120, 1-13. https://doi.org/10.1201/9780429324932-17

Almakhour, M., Sliman, L., Samhat, A.E., & Mellouk, A. (2020). Verification of smart contracts: A survey. *Pervasive and Mobile Computing,* 67, 1-19. https://doi.org/10.1016/j.pmcj.2020.101227

Angelo, M. D., Soare, A., & Salzer, G. (2019). Smart contracts in view of the civil code. Proceedings of the 34th ACM/SIGAPP symposium on applied computing. https://publik.tuwien.ac.at/files/publik_278278.pdf. Accessed 1 February 2021. https://doi.org/10.1145/3297280.3297321

Ante, L. (2021). Smart contracts on the blockchain – A bibliometric analysis and review. *Telematics and Informatics,* forthcoming. https://doi.org/10.2139/ssrn.3576393

Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking bitcoin: Routing attacks on cryptocurrencies. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP), 375–392. https://doi.org/10.1109/sp.2017.29

Apostolaki, M., Marti, G., Müller, J., & Vanbever, L. (2019). SABRE: Protecting bitcoin against routing attacks. In Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 201924-27 February 2019, San Diego, CA, USA, 1-15. https://doi.org/10.14722/ndss.2019.23252

Arcari, J. (2019). Decoding smart contracts: Technology, legitimacy, & legislative uniformity. *Fordham Journal of Corporate and Financial Law*, 24(92), 363.

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts SoK. Proceedings of the 6th International Conference on Principles of Security and Trust, 10204, April, 164-186. https://doi.org/10.1007/978-3-662-54455-6_8

Bartoletti M., & Pompianu L. (2017). An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns. In Brenner M. et al. (eds.) Financial Cryptography and Data Security. FC 2017. *Lecture Notes in Computer Science*, 10323, 494-509. https://doi.org/10.1007/978-3-319-70278-0_31

Bonsón, E., Cortijo, V., & Escobar, T. (2009). A Delphi Investigation to Explain the Voluntary Adoption of XBRL. *The International Journal of Digital Accounting Research*, 9, 193-205. https://doi.org/10.1016/j.accinf.2008.10.002

Bonyuet, D. (2020). Overview and Impact of Blockchain on Auditing. *The International Journal of Digital Accounting Research*, 20, 31-43. https://doi.org/10.4192/1577-8517-v20_2

Charlier, J., Lagraa, S., State, R., & François, J. (2017). Profiling smart contracts interactions tensor decomposition and graph mining. In Proceedings of the Second Workshop on MIning DAta for Financial Applications, MIDAS 2017, 31–42.

Chen, W., Zheng, Z., Cui, J., Ngai, E., Zheng, P., & Zhou, Y. (2018). Detecting ponzi schemes on ethereum: Towards healthier blockchain technology. In Proceedings of the 2018 World Wide Web Conference on World Wide Web, International World Wide Web Conferences Steering Committee, 1409–1418. https://doi.org/10.1145/3178876.3186046

Ciatto, G., Calegari, R., Mariani, S., Denti, E., & Omicini, A. (2018). From the Blockchain to Logic Programming and Back: Research Perspectives. Proceedings of the 19th Workshop “From Objects to Agents” (WOA), 69-74.

Croman K. Decker, Ch., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E.G., Song, D., & Wattenhofer, R. (2016). On Scaling Decentralized Blockchains. In: Clark J., Meiklejohn S., Ryan P., Wallach D., Brenner M., Rohloff K. (eds) Financial Cryptography and Data Security. FC 2016. *Lecture Notes in Computer*

Science, 9604. Springer, Berlin, Heidelberg, 106-125. https://doi.org/10.1007/978-3-662-53357-4_8

Cruz, J.P., Kaji, Y., & Yanai, N. (2018). RBAC-SC: role-based access control using smart contract. *IEEE Access*, 6, 12240–12251. https://doi.org/10.1109/access.2018.2812844

Dai, J., Vasarhelyi, M.A. (2017). Toward Blockchain-Based Accounting and Assurance. *Journal of Information Systems*, 31(3), 5-21. https://doi.org/10.2308/isys-51804

Dai J., He, N., & Yu, H. (2019). Utilizing Blockchain and Smart Contracts to Enable Audit 4.0: From the Perspective of Accountability Audit of Air Pollution Control in China. *Journal of Emerging Technologies in Accounting*, 16 (2), 23–41. https://doi.org/10.2308/jeta-52482

De Graaf, T.J. (2019). From old to new: From internet to smart contracts and from people to smart contracts. *Computer Law & Security Review*, 35(5), 1-11. https://doi.org/10.1016/j.clsr.2019.04.005

De Giovanni, P. (2020). Blockchain and smart contracts in supply chain management: A game theoretic model. *International Journal of Production Economics*, 228, 107855. https://doi.org/10.1016/j.ijpe.2020.107855

Di Francesco Maesa, D., Paolo Mori, P., & Ricci, L. (2019). A blockchain based approach for the definition of auditable Access Control systems. *Computers & Security*, 84, 93-119. https://doi.org/10.1016/j.cose.2019.03.016

Dietrich, F., Palm, D., & Louw, L. (2020). Smart contract based framework to increase transparency of manufacturing networks, 30th CIRP Design, 278-283. https://doi.org/10.1016/j.procir.2020.02.177

Dorri, A., Kanhere, S.S., Jurdak, R., & Gauravaram, P. (2019). LSB: A Lightweight Scalable Blockchain for IoT Security and Privacy. *Journal of Parallel and Distributed Computing*, 134, 180-197. https://doi.org/10.1016/j.jpdc.2019.08.005

European Parliament. (2020). Draft report with recommendations to the commission on a digital services act: Adapting commercial and civil law rules for commercial entities operating online. Committee on Legal Affairs, 2020/2019(INL).

European Securities and Markets Authority (ESMA) (2019). Advice. Initial Coin Offerings and Crypto-Assets. Report nº. ESMA50-157-1391. Available at https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf Accessed 1 February 2021

Fairfield, J. (2014). Smart contracts, Bitcoin bots, and consumer protection. *Washington and Lee Law Review*, 71, 35-50.

Fan, K., Bao, Z., Liu, M., Vasilakos, A.V., & Shie, W. (2020). Dredas: Decentralized, reliable and efficient remote outsourced data auditing scheme with blockchain smart contract for industrial IoT. *Future Generation Computer Systems*, 110, 665-674. https://doi.org/10.1016/j.future.2019.10.014

Ferreira, A. (2021). Regulating smart contracts: Legal revolution or simply evolution? *Telecommunications Policy*, 45, 1-16. https://doi.org/10.1016/j.telpol.2020.102081

Fotiou, N., & Polyzos, G.C. (2018). Smart Contracts for the Internet of Things: Opportunities and Challenges. Proceedings of the 2018 European Conference on Networks and Communications (EuCNC). https://doi.org/10.1109/EuCNC.2018.8443212

Frantz, C.K., & Nowostawski, M. (2016). From institutions to code: towards automated generation of smart contracts. Proceedings of IEEE International Workshops on Foundations and Applications of Self Systems, 210–215. https://doi.org/10.1109/fas-w.2016.53

Giancaspro, M. (2017). Is a 'smart contract' really a smart idea? Insights from a legal perspective. *Computer Law & Security Review*, 33(6), 825-835. https://doi.org/10.1016/j.clsr.2017.05.007

Grenon, S. (2019). Codifying code? Evaluating US smart contract legislation. International Bar Association. Available at www.ibanet.org Accessed 1 February 2021.

Han, D., Zang., Ch., Pin, J., & Yan, Z. (2020). Smart contract architecture for decentralized energy trading and management based on blockchains, *Energy*, 199, 117-417. https://doi.org/10.1016/j.energy.2020.117417

Hewa, T., Ylianttila, M., & Liyanage, M. (2021). Survey on Blockchain based Smart Contracts: Applications, Opportunities and Challenges. *Journal of Network and Computer Applications*, 177(1), 1-39. https://doi.org/10.1016/j.jnca.2020.102857

Hu, T., Liu, X., Chen, T., Zhang, X., Huang, X., Niu, W., Lu, J., Zhou, K., & Liu, Y. (2021). Transaction-based classification and detection approach for Ethereum smart contract. *Information Processing & Management*, 58(2), 1-19. https://doi.org/10.1016/ j.ipm.2020.102462

Jarvenpaa, S., & Teigland R. (2017). Trust in digital environments: From the sharing economy to decentralized autonomous organizations. Proceedings of the 50th Hawaii International Conference on System Sciences, 5812-5816.

Kasampalis, T. Guth, D. Moore, B., Serbanuta, T., Serbanuta, V., Filaretti, D., Rosu, G., & Johnson, R. (2018). IELE: An Intermediate-Level Blockchain Language Designed and Implemented Using Formal Semantics, Technical Report, available at https://www.ideals.illinois.edu/handle/2142/100319. Accessed 1 February 2021. https://doi.org/10.1007/978-3-030-30942-8_35

Kosba, A., Miller, A., Shi, E., & Wen, Z. (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. Proceedings of the 2016 IEEE Symposium on Security and Privacy, 839-858. https://doi.org/10.1109/SP.2016.55

Liu, H., Liu, C., Zhao, W., Jiang, Y., & Sun, J. (2018). S-gram: towards semanticaware security auditing for Ethereum smart contracts. In Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering, 814–819. https://doi.org/10.1145/3238147.3240728

Lone, A.H., & Naaz, R. (2021). Applicability of Blockchain smart contracts in securing Internet and IoT: A systematic literature review. *Computer Science Review*, 39, 1-13. https://doi.org/10.1016/j.cosrev.2020.100360

Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics*, 35, 2337-2354. http://doi.org/10.1016/j.tele.2018.10.004

Madir, J. (2018). Smart contracts: (How) do they fit under existing legal frameworks? https://doi.org/10.2139/ssrn.3301463

Marketsandresearch.biz. (2020). Global smart contracts market 2020 by company, regions, type and application. Forecast to 2025, available at: https://www.marketsandresearch.biz/report/35413/global-smart-contracts-market-2020-by-company-regions-type-and-application-forecast-to-2025 Accessed 1 February 2021.

McGregor, D., & Carpenter, R. (2020). Potential threats for the auditing profession, audit firms and audit processes inherent in using emerging technology. Business and Management Review, 11(02), 45-54. http://doi.org/10.24052/BMR/V11NU02/ART-06

McJohn, S.M., & McJohn, I. (2017). The Commercial Law of Bitcoin and Blockchain Transactions. *Uniform Commercial Code Law Journal*, 16(13), 1-23.

Mik, E. (2017). Smart contracts: terminology, technical limitations and real world complexity. *Law, Innovation and Technology*, 9(2), 269-300. https://doi.org/10.1080/17579961.2017.1378468

Outchakoucht, A., Hamza, E., & Leroy, J.P. (2017). Dynamic access control policy based on blockchain and machine learning for the internet of things. *International Journal of Advanced Computer Science Applications*, 8(7), 417-424. http://doi.org/10.14569/IJACSA.2017.080757

Prause, G. (2019). Smart Contracts for Smart Supply Chains. *IFAC PapersOnLine* 52(13), 2501-2506. https://doi.org/10.1016/j.ifacol.2019.11.582

Raskin, M. (2017). The law and legality of smart contracts. *Georgetown Law Technology Review*, 1(2), 305-341. https://georgetownlawtechreview.org/wp-content/uploads/2017/05/Raskin-1-GEO.-L.-TECH.-REV.-305-.pdf Accessed 1 February 2021.

Reppublica Italiana (2019). Legge 11 febbraio, n. 12 Conversione in legge, con modificazioni, del decreto-legge 14 dicembre 2018, n. 135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione. (19G00017) (GU Serie Generale n.36 del 12-02-2019).

Republic of Malta (2018). Act No. XXXIII: Innovative Technology Arrangements and Services Act. Available at https://legislation.mt/eli/cap/592/eng/pdf Accessed 1 February 2021.

Roszkowska, P. (2021). Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments. *Journal of Accounting & Organizational Change,* 17(2), 164-196. http://doi.org/10.1108/jaoc-09-2019-0098

Rozario, A., & Thomas, C. (2019). Reengineering the Audit with Blockchain and Smart Contracts. *Journal of Emerging Technologies in Accounting,* 16(1), 21-35. https://doi.org/10.2308/jeta-52432

Rozario, A., & Vasarhelyi, M. (2018). Auditing with Smart Contracts. *The International Journal of Digital Accounting Research* 18(1), 1-27. http://doi.org/10.4192/1577-8517-v18_1

Savelyev, A. (2017). Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, 26(2), 116-134. https://doi.org/10.1080/13600834.2017.1301036

Schmitz, J., & Leoni, G. (2019). Accounting and Auditing at the Time of Blockchain Technology: A Research Agenda. *Australian Accounting Review*, 29(2), 331-342. https://doi.org/10.1111/auar.12286

Sklaroff, J.M. (2017). Smart contracts and the cost of inflexibility. *University of Pennsylvania Law Review*, 166, 263-303. https://scholarship.law.upenn.edu/prize_papers/9/ Accessed 1 February 2021.

Shrobe, H., Shrier, D.L., & Pentland, A. (2018). Enigma: Decentralized computation platform with guaranteed privacy. In *New Solutions for Cybersecurity,* MIT Press, 425-454.

Singh, A., Parizi, R.M., Zhang, Q., Choo, K.R., & Dehghantanha, A. (2020). Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. *Computers & Security,* 88, 101654. 10.1016/j.cose.2019.101654

Sookhak, M., Reza, M., Nader, J., Safa, S., & Yud, F.R. (2021). Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues. *Journal of Network and Computer Applications,* 178, 1-22. https://doi.org/10.1016/j.jnca.2020.102950

State of Arizona (2017). Bill HB 2417 amending Section 44-7003, Arizona Revised Statutes; amending title 44, chapter 26, Arizona Revised Statutes, by adding article 5; relating to electronic transactions, available at https://www.azleg.gov/legtext/53leg/1r/bills/hb2417p.pdf Accessed 1 February 2021.

Szabo, N. (1996). Smart contracts: building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought*, 16, 18, p-2.

Tapas, N., Longo, F., Merlino, G., & Puliafito, A. (2020). Experimenting with smart contracts for access control and delegation in IoT. *Future Generation Computer Systems*, 111, 324-338. 10.1016/j.future.2020.04.020

Tjong Tjin Tai, E. (2018). Force majeure and excuses in smart contracts. *European Review of Private Law*, 6, 787–904.

Torres, C.F., & Steichen, M. (2019). The art of the scam: Demystifying honeypots in ethereum smart contracts, *Proceedings of the 28th USENIX Security Symposium*. August 14–16, Santa Clara, CA, USA, 1591-1607.

UK Jurisdiction Taskforce. (2019). Legal statement on cryptoassets and smart contracts, available at https://technation.io/about-us/lawtech-panel Accessed 1 February 2021.

Vasarhelyi, M.A., & Halper, F.B. (1991). The continuous audit of online systems. *Auditing: A Journal of Practice and Theory*, 10(1), 110-125.

Vos, G. (2019). The launch of the legal statement on the status of cryptoassets and smart contracts, available at https://www.judiciary.uk/wp-content/uploads/2019/11/LegalStatementLaunch.GV_.2-1.pdf Accessed 1 February 2021.

Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., & Wang, F.Y. (2018). An overview of smart contract: architecture, applications, and future trends. In: 2018 IEEE Intelligent Vehicles Symposium, IV, IEEE, 108–113. 10.1109/IVS.2018.8500488

Wang, H., Qin, H., Zhao, M., Wei, X., Shen, H., & Susilo, W. (2020). Blockchain-based fair payment smart contract for public cloud storage auditing. *Information Sciences*, 519, 348-362. http://doi.org/10.1016/j.ins.2020.01.051

Xiong, W., & Xiong, L. (2020). Data resource protection based on smart contract. *Computers & Security*, 98, 1-16. 10.1016/j.cose.2020.102004

Xu, Y., Ren, J., Zhang, Y., Zhang, C., Shen, B., & Zhang, Y. (2020). Blockchain Empowered Arbitrable Data Auditing Scheme for Network Storage as a Service. *IEEE Transactions on Services Computing*, 13(2), 289-300. http://doi.org/10.1109/TSC.2019.2953033

Yuan, H., Chen, X., Wang, J., Yuan, J., Yan, H., & Susilo, W. (2020). Blockchain-based public auditing and secure deduplication with fair arbitration. *Information Sciences*, 541, 409-425. http://doi.org/10.1016/j.ins.2020.07.005

Zheng, Z., Xie, S., Dai, H., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, 105, 475–491. https://doi.org/10.1016/j.future.2019.12.019

Zhou, Y., Kumar, D., Bakshi, S., Mason, J., Miller, A., & Bailey, M. (2018). Erays: reverse engineering ethereum’s opaque smart contracts. In: *SEC'18: Proceedings of the 27th USENIX Conference on Security Symposium,* 18, 1371–1385.

Zou X., Deng, X., Wu, T.Y., & Chen, C.M. (2020). A Collusion Attack on Identity-Based Public Auditing Scheme via Blockchain. In Pan JS., Li J., Tsai PW., Jain L. (eds) *Advances in Intelligent Information Hiding and Multimedia Signal Processing. Smart Innovation, Systems and Technologies*, vol. 156. Springer, 97-105. https://doi.org/10.1007/978-981-13-9714-1_12