mapub.org/mapss

MAP Social Sciences

Volume 3 / Issue 1

MAP Social Sciences (MAPSS) is an international, multi-disciplinary, peer-reviewed journal published two times a year by **MAP** - *Multidisciplinary Academic Publishing*. The journal is a platform for publication of advanced academic research in the field of social sciences.

E-ISSN: **2744-2454**

REVIEW PAPER

GOVERNANCE IMPLICATIONS OF APPLYING INTERNAL AUDITING STANDARDS TO BLOCKCHAIN-BASED DECENTRALIZED AUTONOMOUS ORGANIZATIONS (DAOS)

Miloš Lončarević[1], **Goran Kozina**[2]

[1]***University of Applied Sciences Burgenland***, *Eisenstadt, Austria*
[2]***University North***, *Varazdin, Croatia*

Correspondence concerning this article should be addressed to Miloš Lončarević, University of Applied Sciences Burgenland, Eisenstadt, Austria. E-mail: 2219001040@fh-burgenland.at

ABSTRACT

The research paper discusses governance implications, benefits, and challenges of applying internationally recognized internal auditing standards to the newly emerging Decentralized Autonomous Organizations (DAOs) that have quickly gained traction in the past years and are currently totaling market capitalizations of more than USD 20 billion globally. It is analyzed how standards established for traditional centralized organizations are compatible with a decentralized, often anonymous organization that makes decisions democratically based on majority votes while most operations are conducted autonomously subject to pre-defined self-executing smart contracts. After the technological attributes of blockchains, smart contracts, DAOs and other general considerations are determined, each IIA standard is applied separately and results are drawn from a qualitative analysis. The publication contains the major conclusions from a literature analysis followed by a summary of conceptual obstacles to complying with the standards in case of selecting a DAO as an organizational form which could make their overall legality impossible in a context where the implementation of an IA function is mandatory. Additionally, it is summarized how choosing a DAO can contribute and/or challenge compliance with the standards while giving a glimpse into what internal auditing could look like in the future.

Keywords: Blockchain, Decentralized Autonomous Organization, DAO, Governance, Internal Audit, Standards

MAP Multidisciplinary Academic Publishing

MAP SOCIAL SCIENCES

Volume 3 / Issue 1

ISSN: 2744-2454/ © 2023 The Authors. Published by **MAP** - *Multidisciplinary Academic Publishing.*

Article Submitted: **10 March 2023**
Article Accepted: **29 May 2023**
Article Published: **31 May 2023**

https://doi.org/10.53880/2744-2454.2023.3.1.51

MAP SOCIAL SCIENCES Volume 3 / Issue 1

HOW TO CITE THIS ARTICLE
Lončarević M., Kozina G. (2023). **Governance Implications of Applying Internal Auditing Standards to Blockchain-based Decentralized Autonomous Organizations (DAOs)**. MAP Social Sciences, 3(1), 51-64. doi: https://doi.org/10.53880/2744-2454.2023.3.1.51

Social Sciences
by MAP - Multidisciplinary Academic Publishing

GOVERNANCE IMPLICATIONS OF APPLYING INTERNAL AUDITING STANDARDS TO BLOCKCHAIN-BASED DECENTRALIZED AUTONOMOUS ORGANIZATIONS (DAOS)

Miloš Lončarević and Goran Kozina

I. INTRODUCTION

Internal audit (IA) is seen as a trusted partner by management and other stakeholders including their owners. Based on a study conducted with more than 300 experts in Austria about ¾ not only believe that organizations with IA functions are more trustworthy but about the same number of people believed that it should be mandatory for large-sized organizations. IA functions take on the new role of consulting decision-making bodies in times of emerging technologies especially since currently the largest exposure of Austrian companies is seen to be in IT security (PC Concordia, 2021). Internal auditors' jobs are shifting from mere assurance providing functions to risk and opportunity consultants. Moreover, their business case of representing a modern IA profession should contain the ability to respond to rapidly changing and unpredictable market demands including the emergence and rapid growth of blockchain (BC; see Pugliese, p. 1-3, 2021). In view of the progress regarding artificial intelligence (AI), internet of things (IoT) as well as the distributed ledger technology (DLT) in combination with highly automated directive and preventive controls, IA will need to become inventive and proactive in a world where traditional assurance tasks can be performed exponentially faster in combination with a significantly reduced audit risk.

Organizations and individuals have adopted cryptocurrencies or the blockchain technology in general at an uncontrollably fast pace. The capitalization for publicly traded crypto tokens was believed to be valued at USD 1.21 trillion in April 2023 (Coinmarketcap, 2023) and internal auditors must adapt and be knowledgeable about implications and risks in that regard especially once decision-makers decide to incorporate one of the facets into the business strategy. But even if they do not, the internal control systems must be established in a way in which contemporary risks like ransomware and crypto-jacking are considered (see Audit & Risk, p. 8, 2018). Not only should auditors be aware of risks and implications but also how the technology could affect their very own work. Traditional auditing tasks like performing account reconciliations, reviewing the compliance with policies etc. may be substituted by the technology through autonomous and continuous checks based on smart contracts and a set of automated and preventive controls. It has therefore been suggested that besides middlemen like banks and notaries, internal auditors could become obsolete in the future as well (see Peterson, p. 68, 2018). Auditing firms are already framing a new role that makes auditors validate "the new computerized validators", i.e. go one step back and review design and codes of auditing protocols and controls (see Rapaport, 2018). Overall, IA needs to be involved very early and auditors must educate themselves about the subject to stay on top of leading their organizations into the unknown. This is especially relevant because IA professionals rate their own preparedness relating to the adoption and use of enabling technologies as low (see Protiviti, 2021).

A considerable number of companies decided to engage in various types of blockchain (BC) projects starting from accepting Bitcoin as a payment method on to having part of their supply chain processes on a consortium blockchain to increase security and efficiency. IA should engage in the implementation stage to address their governance, risk, and control view for consideration because adjustments to the BC setup are difficult to execute once the system is up and running (see Chalker, 2018). Use cases vary greatly from fintech, gov-tech, insur-tech, law-tech over P2P energy trade, auction houses, online exchanges, complex data warehouses and thousands of others (see e.g. Innovation Eye, 2021) while senior executives globally make BC and digital asset investments a top-five priority (see McCollum, 2020). But there are not just organizations that are highly involved in blockchains and smart contracts. There are some projects that primarily exist on a blockchain and their business is organized through many layers of smart contracts agreed upon by majority vote of the token-holders. This type of organization is called a Decentralized Autonomous Organization (DAO). It is often geographically scattered, enjoys high anonymity, and has reduced human involvement. Protocols for autonomously executed processes are decided upon by the crowds instead of appointed managers. The number of DAOs has increased by 3,200% in 2021 only and the market capitalization of publicly traded DAO tokens is valued to be at USD 20.7 billion in April 2023 (see Yaffe-Bellany, 2022, see also Coinmarketcap, 2023). In 2021 and 2022 the US states of Wyoming, Tennessee, and Vermont were among the first movers to recognize the potential and legalize DAOs as a form of LLC that can be registered and multiple projects have been incorporated since then (see Lom & Browndorf, 2021, see also Gilbert, 2022). However, because the technology and its impacts on organizational forms is still new, there is still a gray area regarding the applicability of laws, regulations, and standards. Some law experts argue that because of the openly tradeable tokens that in their totality depict the organizations ownership, DAOs should be classified as public-

ly traded companies (see Hanzl, p. 296-297, 2019). Not only in this case but also for certain industries there is a mandate to establish a standard abiding internal auditing function. Some of those laws and policies include the Listed Company Manual of the NYSE, the Minimum Requirements for Risk Management Directive in Germany (MaRisk), the Banking Law in Austria (BWG), several Public Corporate Governance Codices of EU countries, and others.

Because of the strict governance requirements in the internal auditing standards and the complex conceptual setup of DAO-IT-governance, it is the goal of this research to determine obstacles to complying with any governance related internal auditing standards. Should this be the case, full DAOs may not only be operating in a gray area but it would be impossible to incorporate them in a context where implementing an IA function is mandatory. Because all standards are applied and evaluated in depth, not only obstacles are determined but also benefits and challenges regarding standard compliance are described. By conducting this research, we want to contribute findings for law/standards makers on the one hand and blockchain developers on the other by adding to a scientifically underexplored but highly exposed area of emerging technology. Additionally, the findings could be used as part of the mandatory internal and external quality assessments described in the IIA standards 1311 and 1312. Lastly, the sum of content provided ought to give an overall look into what internal auditing could look like in the future (see Loncarevic, 2023).

To be able to understand the implications of applying standards developed for traditional centralized organizations to the new concept of DAOs, it is essential to briefly provide an overview of the key functionalities of smart contracts and DAOs.

II. FUNDAMENTALS OF SMART CONTRACTS & DAOs

While the concept of digital smart contracts (SCs) is not new, the blockchain technology gave them a new twist. They self-conclude based on conditions agreed-upon by two or more parties. Complex types of agreements can now be prepared and executed including, for example, payments that are only triggered once pre-defined arrangements were met, and no third party needs to be involved because the blockchain serves as a transparent intermediary. The transactions carved into the blockchain are essentially immutable and therefore the need for trust is not required (see Alharby & van Moorsel, p. 127, 2017; see also Diederich, p. 166-169, 2016).

An example for a smart contract would be an agreement between an airline and a customer that provides partial refunds automatically if the plane departs later than four hours. Another one could be a billing agreement between a rent-a-car firm and their customers whereby payments are triggered gradually once a certain mileage was reached or some time has expired. A smart contract between a wholesaler and their preferred deliverer may only self-conclude once verifiable conditions of delivery to the customer were met. All these agreements are subject to information on-chain and off-chain. This is provided by the means of oracles, which provide the trigger to conclude the contract or not (see also Alharby & van Moorsel, p. 128, 2017; see also Mou, 2020). In the above-mentioned examples, the contract parties may agree on oracles such as a trusted source for time, departure boards from airports, mileage of a car plugged to an API transmitting values to the SC, track-and-trace functionalities of postage firms, various types of sensors etc. Note that oracles can be setup improperly, have inbuilt errors, or may be manipulated. Once an SC has concluded, it is difficult to undo the transactions. The program of the Ethereum blockchain is known to be catered to support advanced SC functions (see Alharby & van Moorsel, p. 128, 2017). Because of the complex code of an SC, its contents are not always verifiable by the individuals engaging in it and discussions over whether the actual agreement trumps the underlying code or vice versa have been going on at a legal and an ethical level (see Diederich, p. 169, 2016).

Smart contracts can be grouped and layered into more complex interdependent processes and governances forged into an autonomously executing project. Ownership of the project is shared by individuals buying into the business' ecosystem through providing a financial contribution and receiving ownership tokens that enable them to vote for or against changes to that project. This type of setup is called a Decentralized Autonomous Organization or simply DAO. The entire project reduces human involvement to proposals that participants can submit and decentralized votes based on the token-share owned by an individual (see Buterin, p. 13, 2014, see also Murray et al, p. 623, 2021). In such a setup there is no central management, but the totality of token-holders also represents the executive management through majority vote. Thereby the network avoids the principal-agent problem through direct incentivization concepts (see Murray et al, p. 623, 2021). The protocol must disincentivize not playing by the rules and be transparently followable by investors/owners. If the DAO is set-up and managed well, it can allow for more decen-

tralized execution of duties and less discriminatory engagements of participants in comparison to traditional centralized organizations (see Voshmgir, p. 104-105, 2019).

However, DAOs have shown to have a tendency for limited voter participation due to the effort required to work through proposals and make informed decisions. Also, corporate and tax law remain a gray area for this type of organization (see Chohan, p. 3, 2017). Beside the most common perceived drawbacks blockchains are known for, including tax evasion, terrorism and shady business financing, the energy consumption of certain consensus mechanisms etc. DAOs in particular may have some additional implications and risks worth mentioning. Majority voting may lead to mediocre outcomes because the lowest common denominator is chosen given a certain range. Changes are difficult to execute once majority votes have already happened and management decisions are made very slowly. Developers and proposal makers have disproportionately more implicated power over the ecosystem (see Kaal, p. 21-29, 2021). In a majority robs minority attack, a collective of investors holding 51% of the blockchain's native tokens may direct all funds including that of the minority to their own wallets (see Jentzsch, p. 2-3, 2016). New security issues may arise due to the code that are difficult to manage and can have a potentially fatal impact. One example is the original DAO-project called "the DAO" whereby a loophole in the code was exploited to drain USD 50 million. This had such a massive impact, that disagreements over how to proceed in the matter led to a hard fork in the utility blockchain Ethereum (see Voshmgir, p. 107, 2019; see also Konashevych, 2021 & Chohan, p. 2, 2017).

Despite and sometimes because of these drawbacks and risks, more elaborated DAOs are emerging, and their overall numbers and capitalization are rising (see Coinmarketcap, 2023). Because of the new legalization wave in the Unites States, more use cases have emerged for purposes like investments, decentralized finance, charity, fundraising and other projects. According to the NYT in 2021 there have been already 4,000 DAOs whose tokens rose 3,200 per cent in comparison to the year before (see Lipton & Livni, 2022). Considering the increased clarity brought about by new legislation it is only a matter of time before all requirements regarding internal auditing will be formalized. The next section will show the results of the literature analysis conducted regarding governance implications of internal auditing in DAOs (see Loncarevic, 2023).

III. LITERATURE ANALYSIS

In the literature section it was our goal to establish the current state of scientific literature in relation to internal auditing and DAOs, and more specifically, to any governance implications of merging the two areas of interests. Several databases and online catalogues were searched in consideration of narrow parameters and keywords. Note that in a separate publication all operations related implications were discussed, and the underlying dissertation was written due to the very fact that currently there has not yet been any research conducted concerning the combination in question (see Loncarevic, 2023). To yield relevant results, nevertheless, some overall aspects like auditing in blockchains and smart contracts as well as governance implications in DAOs were researched to add foundations to the respective section regarding the application of governance related internal auditing standards. Mind that the technology of blockchain is only approximately 15 years old and blockchain-based smart contracts are an even younger phenomenon. Knowledge building in the area has not always happened to the highest scientific standards but were rather a learning-by-doing process. Much of the knowledge initially came from blogposts whereby the author was in some cases (in line with many of the enthusiasts) anonymous and credentials, sources, or peer-reviews could not be validated. Only in recent years has the scientific community caught up to a certain extent and a summary of the most important findings from the literature analysis is listed below (see Loncarevic, 2023).

A. General Governance Implications of Blockchains and DAOs

Making use of the blockchain technology will have governance implication on any venture in one way or another. Should a company engage in a consortium blockchain it will have some shared governance over the blockchain and may not always be able to influence everything happening on the blockchain. What is often mentioned for DAOs as the most evident governance change, in comparison to traditional centralized organizations, is the supposed ridding of the principal-agent problem. Managers are sometimes incentivized to make suboptimal decisions for short-term gains to increase their own bonus. Conflicts of interests may arise if the incentives are not aligned (see Chedrawi, 2018; see also Yermack, p. 25-26, 2017). The decisions made on the blockchain have a bigger backing from the owners but as established above it may be slower, more uninformed, and mediocre.

Often the governance of a DAO is mistaken for the consensus mechanism of the underlying blockchain while the actual governance entails a lot more (see Rikken et al, p. 405, 2019). The governance of a DAO may be established as part of the BC code and additional smart contracts. In a perfect full DAO each token-holder has equal rights in the ecosystem. In some cases, additional roles and responsibilities may be defined like for voting-delegates, trusted funds-custodians, or even auditors. Apart from all agreements on-chain a lot of the governance can and will happen off-chain. This is because some debating and decision-making is happening more efficiently off-chain. More prominent and active members of the DAO may have additional implied power in the project potentially leading to counter-governance (see Rikken et al, p. 404, 2019; see also Ferguson et al, p. 6-8, 2020).

Risks to a DAOs governance include so called "whales" who have disproportionate large amounts of tokens in a proof-of-stake consensus mechanism or individuals with large CPU-mining power in a proof-of-work consensus mechanism that can steer the organization in an undesirable way for all participants. The above-mentioned 51% attacks and hard forks can also pose a threat to the success of a company with this organizational form. Due to mob justice, decisions in DAOs are often made based on herd-majority voting instead of rationale while individuals not equipped to make well-founded strategic decisions have the same decision-making power as those who do (see Rikken et al, p. 409-411, 2019).

Per design a DAO does not make any exclusions based on nationality, gender, ethnicity, age, or other backgrounds. On the other hand, there could be different views on what the corporate culture should look like and geographic preferences e.g. regarding risk appetite may lead to clashes in the ecosystem (see Rikken et al, p. 411-413, 2019). The anonymity aspect of the project also means that the real force behind individuals' decisions during voting is unknown. A competitor could cast votes not in the interest of the DAO or retrieve sensitive information. For accountability reasons it is likely that participants may have to identify themselves and link driver's IDs, perform some type of video-face-verification etc. (see Beck et al, p. 1028- 1029, 2018).

Mini et al. differentiate between "Establishing Algorithmic Organization" and "Taming Algorithmic Power" as two forces facing each other. The first strives toward full autonomy and trustlessness even resolving disputes between participants while the latter still puts human decision-making and control/superiority over the code into the center (see Mini et al, p. 9-12, 2021). It is worth noting that the project stands and falls with the strength of the protocol. Changes to the established governance are difficult to process at a later point in time. Moreover, the coordination and negotiation of smart contracts is time-consuming and still gives a lot of power to coders (see Beck et al, p. 1029-1030, 2018).

IT governance is a dominating force that has recently emerged with the computerization of business administration. In blockchains not only roles and responsibility are defined and assigned to nodes and private keys, but other aspects must be considered too. Once new nodes are added to the ecosystem, large transaction loads and queueing difficulties may arise. Auditors must test respective policies and procedures as well as data throughput and hardware related issues (see Lineros, p. 50, 2021). Other IT-related controls include those of data-storage, private key management, disaster recovery and business continuity management (see Lineros, p. 50-51, 2021).

B. Considerations for Internal Control Systems

If the expertise for securing an adequate internal control system for a DAO's/blockchain's business venture cannot be generated in house it must be provided by financial services firms and consulting agencies to combat not only established but also new risks. For an adequate governance issues like encoded segregation of duties, asset custody, as well as data verification and other aspects must be considered. The automation of controls may tempt to transfer all validation and auditing tasks to the machine which brings certain audit risk that can fully derail a business venture (see Smith, p. 143-144, 2019). Any set of preventive, directive, and otherwise automated control can only serve to assist in business administration but should be verified ongoingly because even the best protocol may have flaws. In fact, the literature suggests that auditors may focus their work on providing assurance on the design of otherwise automated controls and similar setups, which is something that is already happening on a large scale in environments with sophisticated ERP-systems.

Some fundamental conditions mentioned by Smith are that BC may not be mistaken for an accounting tool but as the distributed ledger technology that it is. The use of a blockchain does not mean that a business venture cannot be hacked. It simply means that some risk is eliminated or transferred while a new set of risks needs to be tended to. Not for every business case using a BC will be

the best choice considering the inherent costs as well as the usability. Lastly, being engaged in BC does not necessarily mean engaging in the use of cryptocurrencies, which often entails confusion once the topic of BC comes up (see Smith, p. 146-147, 2019). There is also a general perception that BC using organizations are somewhat riskier and control risks are increased in audit engagements. The lack of auditing standards may thereby diminish the benefits of a BC control system (see Dyball & Seethamraju, p. 613, 2021).

The roles and responsibilities regarding the management of smart contracts but also the internal control system in blockchains should be clearly defined, which may prove difficult in a fully decentralized environment. This becomes easier in permissioned blockchains where all participants are known to each other. Additionally, stakeholders of the blockchains must consider the cultural impact of using a blockchain, the transparency, potential anonymity, the way of decision-making, and many other aspects. The core values may vary greatly in comparison to a traditional centralized organization (see Vincent & Barkhi, p. 66-70, 2021). If internal auditors want to have an impact of governance, risk, and internal controls, they should be involved during the planning and implementation stage of the blockchain project (Vigliotti & Jones, p. 121-131, 2020; see also Loncarevic, 2023).

C. Implications for the Audit Committee

By the example of consortium blockchains it was shown, that the way audit committees receive and process reports changes substantially. In traditional centralized organizations the AC selects an external auditor, establishes the fee structures, and liaises with management and auditors. The AC will have to make sure the required expertise is available in view of governance, risk, and controls (GRC). But in a consortium the participating parties may have differing approaches to GRC and the weakness of one entity might affect the entire ecosystem. Auditors from one centralized entity may not have all required rights to validate all aspects of the blockchain. It is therefore advisable to consider establishing an audit setup on the consortium blockchain level rather than at the individual organizational one. Independent auditors may be involved to make sure each entity receives only reports from their sphere based on a need-to-know principle (see Smith & Castonguay, p. 129, 2020). This example shows that different layers of governance for ventures including a blockchain may apply that can sometimes mismatch. Likewise in a DAO the governance of the utility blockchain can have an impact on the native blockchain and vice versa as was shown in the example of "the DAO" (see Loncarevic, 2023).

D. Crowdauditing and Trusted Audit with Untrusted Auditors

If internal auditors are appointed, according to DAO principles some form of centralization may emerge which goes against the nature of full decentralization and democratization. Individuals could have too much of an impact and steer the project into a direction that is not in the best interest of the majority of token owners. To combat this issue Chen et al proposed a concept called "crowdauditing" and/or "trusted auditing with untrusted auditors". Well-designed smart contracts provide incentivization for participation in the DAO's auditing arrangement. Every individual can for example stake their tokens to join a pool of auditors. Additional requirements can be determined by the token-holders. Through an unbiased selection mechanism an auditor gets appointed and through the consideration of the Nash equilibrium point the personal benefits are maxed out to provide the best auditing work. After completion of the audit work, a second smart contract contains the evaluation of the audit reports integrity and quality. Based on the outcome the auditor's reputation gets updated which influences the possibility of getting selected as an auditor in the DAO again (see Chen et al, p. 6215-6236, 2021). The approach provides a model that attempts to preserve as much of decentralization and anonymity as possible. However, it also entails some challenges including the fact that early on bad apples may be selected, which can pose a threat to the business' success. Moreover, if an auditor performed well on one type of audit it does not guarantee that they will perform well in a different domain too. Among other potential drawbacks and open questions, it is still unclear how the system can be manipulated, how audit work is evaluated, and what kind of costs this approach involves.

E. Audit Nodes on a Blockchain

Another dimension that could influence the governance of the blockchain or a DAO are the number and the type of nodes involved in the endeavor. To obtain an understanding of the most common node types in blockchains, refer for example to Müller, 2021, Frankenfield, 2021, Seth, 2021, or Voshmgir, 2019 from the reference list. Another still uncommon type of node that could possibly complete the set, are audit nodes. Based on the pre-defined program of the blockchain they can have a variety of functions. Light nodes may connect to trusted audit nodes to validate that certain checks

according to the standards were performed (see Lemieux, p. 126, 2016). Audit nodes can also have information regarding ownership of data or about sensitive information including identities of participants. To protect the data certain information can be fragmented and transferred to different audit nodes (see Chen & Reiser, p. 95, 2017). It is important to note that the term audit node in this context may be confusing because in the mentioned examples the nodes have a specified automated function according to the protocol rather than providing user rights to the node owner in order to access and audit transactions manually.

IV. METHODOLOGY

The summary of the literature analysis conducted above shows some of the more relevant findings used as part of the qualitative and exploratory research in the next section. To address the research problem of whether and how governance related internal auditing standards can be applied to the DAO context, all conceptual attributes of a DAO were established. The common body of knowledge for the functionality and the literary basis of the DAO were defined and the analysis was conducted based on well-known frameworks for scientific literature analysis (see Vom Brocke et al, p. 3, 2009; see also Snyder, 2019). In the next step the IIA's International Standards for the Professional Practice of Internal Auditing (simply referred to as "the standards") were chosen as a reliable set of standards for parameters to be translated into the unique context of the DAO to establish organizational, technological, or any other governance related obstacles regarding the compliance with each individual sub-standard. Because each of them are screened for implications, not only obstacles but also benefits and challenges regarding compliance are identified and summarized as part of the paper. The standards were established and are regularly amended by the IIA, which has 210,000 members globally and the internal auditing standards are recognized universally (see theiia.org, 2022). A similar approach to that of Vincent and Barkhi (2021) and Burns et al (2020) was selected whereby an established framework (COSO) was applied to the context of the blockchain in general and implications, benefits, and challenges were identified. In this early stage of blockchain research exploratory methods are required to establish the foundation for quantitative work especially when tools established for the known type of organizations are applied to new, almost futuristic concepts and technologies (see Loncarevic, 2023).

V. FINDINGS

The following chapter shows the summary of major results regarding conceptual obstacles, benefits, and challenges in terms of the compliance with governance related internal auditing standards. IA has been around for a lot longer than DAOs which is why we can rely on a substantial amount of research and subject books. Before the respective issues are described, we elaborate on what the standard looks like for traditional centralized organizations to set the known basics before deriving implications.

A. Conceptual Obstacles

The below-mentioned implications prove to be most likely obstacles to fully complying with internal auditing standards. It does not necessarily mean that this list is complete and additionally, it cannot be ruled out that through giving up some anonymity, decentralization, or other characteristic of a DAO in combination with a well-established protocol an expert could conclude that standard compliance is possible. We rather show the biggest gaps related to established auditing standards in combination with the theoretical concept of a full and pure DAO.

i. Purpose, Authority, and Responsibility

In a traditional organization an IA function will need full backing from the top as well as the authority to perform their duties. The tone-at-the-top and the management style will decide what role the IA function will take up in the respective organization. Access rights and responsibilities must be established in an effective way and the purpose must be made known to stakeholders of the organization. The backing of the management will have a direct impact on the quality of the results from IA work (see IIA A, p. I-27, 2017). The internal audit charter is the central document containing the above-mentioned parameters and can be seen as a type of IA constitution. Other handbooks, processes, workflows etc. will directly be based on that charter. It is prepared and reviewed by the chief audit executive (CAE) and presented to senior management for approval. It includes specifics regarding mission and scope of work, accountability, independence, responsibility, authority, and more (see IIA B, p. 2-8, 2017).

In a DAO the senior management's role would be taken by the collective of token holders and the audit charter could be defined in the protocol while certain auditing tasks could be agreed-upon as part of smart contracts in an op-

erative sense. The audit charter would need to be submitted as a formal proposal to the token-holders. Whoever does not agree with a majority vote on the audit charter, can withdraw their funds and/or fork off. A major obstacle would be that the standards require the establishment of the role of a CAE. This in combination with the mentioned authority would pose a major point of centralization giving them more factual as well as implied power which goes against the idea of a full DAO. Selecting a CAE includes very strict vetting of candidates e.g. for conflicts of interest, trustworthiness, work experience, education, and other characteristics. Should a fully anonymized setup be selected for a DAO, this could become a difficult exercise, especially considering that all token-holders would need to perform their own due diligence if the selection process is not delegated. The latter would again entail more centralization, which may not be preferred by investors specifically choosing a DAO to invest in because of its conceptual benefits. Should the DAO setup allow for audit delegates who make decisions on behalf of the owners, all roles and responsibilities would have to be defined as part of the AC and the DAO protocol. As you will see in the next sub-section, the fact that each token-holder represents a fraction of management can lead to independence and objectivity issues especially if internal auditors hold and are paid in native tokens. If they do not, it would need to be clarified by what standard they are internal as compared to external auditors.

The audit charter would need to consider on-chain and off-chain subjects because the responsibility of IA does not end with the blockchain and the smart contracts. If the work of CAE and auditors is remunerated as part of smart contracts, not only will the completion of off-chain work be difficult to verify since effective oracles, that need to be audited themselves, must be in place. In general, it will be difficult to avoid double-governance in a DAO which could affect IA work too (see Loncarevic, 2023).

Related standard: 1000 - Purpose, Authority, and Responsibility

ii. Independence and Objectivity

One of the first things for entrants to the audit profession to learn is that internal auditing retains their professionalism and image from the stakeholders through holding the standard of organizational independence and personal objectivity prominently up high. Independence means that decision-makers provide organizational pre-conditions for the CAE to report their results directly to the executive management and board (or sub-committee) without the interference of a filtering entity in between. Process independence is also covered under the major standard which means that IA should not be included in regular operations or at least in the few cases where it is inevitable safeguards must be provided. Objectivity means that you should and cannot properly audit an area that you recently worked in, where a spouse or close friend works, or have any other conflict of interest. Internal auditors should even refrain from activities that give the impression that their expert opinion could be influenced. To combat impartiality, auditors should ongoingly consider any conflicts of interests and validate both independence and objectivity constantly (see Bünis & Gossens, p. 36-40, 2016; see also Eulerich, p. 5-6, 2018).

As we will see in section "C. Benefits" the setup of a DAO may bring advantages due to the fact that autonomous audit procedures do not have a conflict-of-interest in operations although the individuals designing the procedures and controls could have them. Also reporting lines are transparently pre-defined and stakeholders can verify the on-chain independence of a hypothetical internal audit function. However, the fully decentralized setup of a DAO brings certain obstacles to the table in terms of complying with independence and objectivity related standards. The first one, is that the CAE needs direct access to senior management and the board. There is, however, no CAE but also no board that they could direct their auditing results to. If the CAE forwards audit reports to the full population of token-holders, they would also transmit high risk findings to a large anonymous crowd with unknown intentions and loyalties. A loophole in the code discovered by IA and transmitted to all token-holders could quickly be exploited by some individuals. Moreover, there needs to be an entity that can receive confidential reports on behalf of token-holders, evaluate them, and make final decisions regarding a potential implementation of audit recommendations. For objectivity reasons IA must not submit formal proposals to token-holders since they would not be impartial at the time of a follow-up audit. A pre-appointed audit committee could instruct certain developers to draft solutions for identified audit objectives through the definition of smart contracts. However, not only would this lead to centralization at more than one instance but also the setup would not work in a fully anonymous environment. Token-holders on the other hand as co-owners of the DAO would require certain confidential documentation to evaluate the audit committee's or delegate's work, which again poses the threat of exposing high risks to unknown individuals.

Another major obstacle in a full DAO is uncertainty regarding conflicts-of-interests of auditors. While anonymity and geographic dispersion aids in the fact that there is naturally (presumably) less acquaintance between the participants and therefore fewer incentivization for an auditor to not report a discovery because someone close was involved. Meanwhile, the real loyalty and conflicts-of-interests off-chain are a black box to the endeavor, meaning that objectivity is difficult to verify. Real loyalties of auditors are unknown and if the incentivization structure as part of the smart contracts is not sophisticated, the anonymous auditor may decide to opt for exploiting a discovered loophole themselves because it is more lucrative, and the consequences are negligible. It is furthermore difficult to establish that an auditor does not own the DAOs native tokens, engages in votes, and therefore participates in managing activities producing another conflict of interest. Therefore, IA standards regarding independence and objectivity may be difficult to comply with in a fully decentralized and anonymous DAO (see Loncarevic, 2023).

Related standard: 1100 - Independence and Objectivity

iii. Reporting and Acceptance of Risks

There are various other potential obstacles to full compliance with IA standards and some of those arise in operational auditing areas, which is elaborated on specifically in a second research paper. Therefore, all operational auditing implications from audit planning through engagement planning, to conducting the audit, and others were considered only to the level where it affects governance issues. Since the cumulation of the audit work is to be found in the main deliverable – the audit report – the most important governance aspects of the audit work itself is summarized in this section. Audit reports in practice vary regarding content, layout, length, detail etc. but generally include objectives, scope, and results as minimum requirements to provide recommendations for future improvements. In general, the look of the audit deliverable will depend on the organizations' decision makers' preferences, i.e. that of senior management and the board (see Eulerich, p. 272- 274, 2018). For the overall report but also for individual findings certain risk classification categories may be used that could also give an indicator of who should address those findings (see Bünis & Gossens, p. 157-160, 2016). Audit reports are disseminated to only a small number of individuals who are knowledgeable and involved in the area in question to prevent malicious use of the information.

Internal audit will determine an implementation coordinator, often a local manager from the audited area, and set implementation deadlines. Communication between IA and these coordinators can have a big impact on the result of the implementation work. After the deadline has passed at the latest, IA usually conducts some type of follow-up activity to evaluate if and how recommendations were implemented by the entity in question. Should the auditee not agree with a certain recommendation or risk assessment and decide to refuse implementation, IA will have to evaluate the concerns brought forward. Should they remain with their position regarding the addressing of open and unaddressed risks, the matter gets escalated to senior managers who will make final decisions on how the situation should be handled. They can either accept the risk (and take the responsibility), urge the auditee to implement the recommendation, or take some different type of action. Either way the follow-up procedure may then be closed (see Bünis & Gossens, p. 161-163, 2016; see also Eulerich, p. 275-279, 2018). Note that for example cost-driven managers with a larger risk appetite are more likely to accept certain risks and vice versa. Therefore, the degree of influence and value added an IA department can provide will also depend on risk appetite, strategy, and corporate culture.

In a DAO taking into consideration the token-holders' preferences regarding audit reporting can be difficult. In a different publication regarding operational obstacles to complying with IA standards in DAOs, we have already established that rectifying errors and omissions in reports, which is a mandatory sub-standard of internal auditing, can be difficult once smart contracts have been concluded and certain information is already engraved into the (almost) immutable blockchain. Also, auditors are not incentivized to do so if the remuneration was already paid out and their reputation could be influenced. Additionally, from a governance perspective, it would be difficult to establish the right reporting lines in a DAO. It is unclear who the auditee is in the first place, who can be assigned an implementation coordinator, and how their participation in the audit and implementation phase is incentivized. As mentioned before, it is not in the best interest of a DAO to provide sensitive information regarding potentially fatal risks to a large pool of anonymous token-holders. Some of them may be competitors who might use the information in a way that is not in the best interest of the DAO. Others could directly exploit identified loopholes. A greater obstacle is that even in the case where a DAO has defined delegates who autonomously handle these matters in a smaller circle e.g. by having an

audit committee, a steering committee, or IT development committee, the period between making a formal proposal to amend a code to address a coding error and the time the proposal was passed by majority vote, could be long enough for one individual from the crowd of token-holders to e.g. drain funds. Mind that this is not only an unacceptable drawback but it would also mean that DAO enthusiasts would have to concede in favor of substantially more centralization points, which many may not support.

Furthermore, it is neither clear who the audit reports can be sent to and who will oversee implementing recommendations, nor who will be in charge once a dispute between IA and the auditee arises. There is no hierarchy where the issue could be escalated to and as established before, the ultimate instance of token-holders may not be a good point because of security reasons but also because the majority may not have the expertise or resources to make a sophisticated decision. The related standards may be one of the most difficult to comply with should a DAO be selected as an organizational form (see Loncarevic, 2023).

Related standards: 2400 - Communicating Results, 2500 - Monitoring Progress, 2600 - Communicating the Acceptance of Risks

B. Challenges

Choosing a DAO as an organizational form will impact standard compliance in different ways. In some cases, there are no hard conceptual obstacles to complying with them, but some unique aspects challenge it. That includes the fact that while governance may be transparently established as part of the protocol and the smart contracts there will be off-chain happenings that can pose the risk of double- or counter-governance that affects the DAO and its IA function. For standards regarding the audit charter this fact will need to be reflected in a way that smart contracts and oracles cannot always fully embrace. Anonymity proves to be a challenge for roles and responsibilities in an IA function. DAOs are also prone to implied governance, i.e. individuals who are more prominent in the project and can influence the voting process to a certain degree. Mob democracy, herd majority, whales of the DAO, as well as hard forks add additional governance challenges to the DAO as a whole. As the example of "the DAO" has shown, the governance of the utility blockchain can influence the governance of the native token and vice versa which can limit auditor authority.

Trusted auditing/crowd auditing, as proposed in the literature analysis section, entails other challenges like establishing appropriate oracles for smart audit procedures and validating an auditor's expertise for each new audit subject. The trial-and-error strategy used as part of that concept could be risky in the initial stages and having alternating auditors would mean losing organizational experts.

Any arrangements made through smart contracts would need to be made between the CAE and the majority of token-holders if no different arrangement is made as part of the program. However, involving the token-holders can be a time- and resource-consuming process whereas we have also established that they do not always have the capacity to make the most adequate decisions. If, for example, a smart contract is set up for an audit engagement of the purchasing practice of the DAO, the IA employee in charge would need to define individual auditing tasks and oracles that provide profound evidence that audit work was performed in an appropriate manner. In this case it would be difficult for a token-holder to understand the meaning and implications of each of these smart contracts. If the protocol allows for the CAE to establish SCs with individual auditors, it will limit the power of the collective and lead to a centralized type of organization. Not all audit work can be quantified and if remuneration is tied to quantifiable input data, auditors are incentivized to push the least number of buttons to trigger payment. This would massively increase audit risk and lower audit quality. Take for example the task of performing a risk assessment for each subject in the audit universe. If the smart contract self-concludes once each item has a risk rating, auditors are incentivized to guess and enter random numbers instead of putting the effort into performing sophisticated risk analyses.

In this very computerized environment, the smart contracts themselves pose a control risk and would need separate audit activities to validate the proper setup of the agreement and the oracles. This does not only increase audit cost massively but also gives developers more power shifting some of the implied governance rule to them. Performing changes to audit assignments and scope or the rectification of errors and omissions may not only be difficult on the blockchain/concluded SC, but auditors are also disincentivized to execute them. Corporate culture, ethics, tone-at-the-top and other factors varying to a large extent in a geographically dispersed project can affect the harmony and success of the venture and increase the risk of hard forks further. To see a more elaborate list of

challenges to complying with IA standards in a DAO context also refer to the dissertation this research paper is based on (see Loncarevic, 2023).

C. Benefits

The flipside to the obstacles and challenges regarding standard compliance are various new ways the technological features can contribute to it. All the audit evidence is transparently documented on an immutable blockchain. Additionally, all governance related issues including access rights, reporting channels, authority etc. are defined as part of majority consensus agreements. In addition to audit evidence, also auditor work may be timestamped and documented for an independent review e.g. as part of the quality assurance and improvement program. The performed audit procedures are known and can be coordinated with other stakeholders including external audit, compliance, the fraud department etc. more easily. The CAE as well as auditors are incentivized to perform their duties timely and in a way that is pre-defined in the smart contract to trigger remuneration. While this is more an operational aspect, it is still worth mentioning that IA will be able to test full populations more efficiently instead of just a number of samples through automation.

In a DAO, there is no hierarchy and no discrimination against any of the participants based on ethnicity, gender, age, disability etc. The voting rights are simply determined by the number of tokens you own. Diverse participants in a DAO with diverse backgrounds can contribute to global and local risks while providing their unique expertise and preferences regarding risk appetite and the steering of the project. All decision-making is transparent and there is no principal-agent problem in theory because the collective of management is incentivized to maximize their own shareholder value. Conflicts of interests may also be removed in that regard also because there may be no hesitance to openly report audit issues related to the sphere of a well-known co-worker in an anonymous context. The design therefore appears to be more objective also because the code could transparently exclude auditing rights for auditors whose private key was involved in the transactions at question. The system could allow for smart contracts that narrowly define the sensitive data auditors are allowed to review based on a need-to-know principle and access is timestamped and documented. The other side of the coin shows that the audit charter can guarantee the access for IA and no discussions with auditees are required.

The reporting process would be timelier, in some cases even in real time, and the protocol could define automated dissemination based on certain characteristics, e.g. the risk rating of an observation. The technological features of the blockchain provide improved opportunities for continuous audit activities and mass data analytics. The falsification of audit evidence is more difficult reducing some of the audit risk. Generally, the lack of hierarchy means there may be fewer instances trying to interfere with reporting, improving compliance with standards regarding organizational independence. Despite token-holder voting having its drawbacks, all IA assignments have a larger backing from the DAO project owners. Moreover, sophisticated incentive schemes in smart contracts can align the interests of token-holders and internal auditors. This aspect can also be used to incentivize optimal and timely implementation of audit recommendations. Decisions on risk acceptance of decision-makers is transparently documented on the BC. Should IA represent one form of partial centralization in a DAO as part of e.g. an audit committee, it may have the opportunity to strengthen its standing in the project and avoid being sidelined. A more complete list of benefits can be viewed in the underlying dissertation (see Loncarevic, 2023).

VI. CONCLUSION & FUTURE OUTLOOK

The results regarding the application of well-established governance-related internal auditing standards to blockchain-based DAOs, showed that there are some obstacles to fully complying with some of the standards, should a fully decentralized and anonymous DAO be selected as an organizational form. The standards require the appointing of a chief audit executive (CAE) which is an aspect that presents some form of centralization while independence and objectivity standards may be difficult to comply with conceptually in this type of setup. It is unclear who has the authority to perform audits and write reports but also who will be the recipient of the results. The collective of token-holders cannot be addressed with high-risk audit findings because one anonymous individual could exploit loopholes before they can be fixed. Moreover, conflicts of interests as well as true loyalties are difficult to discover while counter-governance off-chain can complicate all IT governance on-chain. Furthermore, it is not defined who the auditees are in the context and whether developers are incentivized to participate in the audit process, for example as interview partners providing key information on the genesis of business processes. Submitting proposals to fix high risks and loopholes provide enough time for individual participants to

exploit those weaknesses. The lack of hierarchy means that there is no adequate authority that can make decisions on risk acceptance in case of a dispute about an audit recommendation between the auditor and the auditee. These obstacles can lead to an IA function in a DAO generally not conforming with the standards. This means that DAOs in general could be barred from incorporating in industries and legislations where establishing a standard-abiding IA function is mandatory. Moreover, it was not only displayed that choosing a DAO as an organizational form has many benefits and challenges but will also lead to complying with the standards in a considerably different way.

The results address both standard and law-making bodies as well as DAO enthusiasts showing fundamental implications of combining the two vastly different concepts of IA and DAOs. There may be new standards required for emerging technologies that have the potential to address risks in a different way and some flexibility is required to provide a platform for transformative ideas like DAOs. Blockchain enthusiasts need to consider giving up some decentralization and anonymity to strengthen security and being able to run their business legally. Moreover, the research paper could point quality assessors of IAs in DAOs to weak spots and strengths. Most importantly, it shows that the role of IA will, like many other professions, be subject to substantial changes but may have the opportunity to become an important point of reference for managers and token-holders regarding new risks and opportunities of groundbreaking technologies (see Loncarevic, 2023).

VII. REFERENCES

Alharby, M./ van Moorsel, A. (2017): Blockchain-based Smart Contracts: A Systematic Mapping Study, Computer Science & Information Technology (CS & IT), pp. 125-140, Available Online: https://arxiv.org/ftp/arxiv/papers/1710/1710.06372.pdf, Accessed on: 12.03.2022

Audit & Risk (2018): Update – Cyber attacks grow more frequent and sophisticated, published in A&R Magazine Nov/2018, pp. 8-9

Beck, R./ Müller-Bloch, C./ King, J. (2018): Governance in the Blockchain Economy: A Framework and Research Agenda, Journal of the Association for Information Systems (2018) 19(10), pp. 1020-1034, doi: 10.17705/1jais.00518, ISSN 1536-9323

Bünis, M./ Gossens, T. (2016): Das 1x1 der Internen Revision, Bausteine eines erfolgreichen Revisionsprozesses, 2. Neu bearbeitete und erweiterte Auflage, Erich Schmidt Verlag, Berlin 2018, ISBN 978 3 503 17741 7, pp. 1-227

Burns, J./ Steele, A./ Cohen, E./ Ramamoorti, S. (2020): Blockchain and Internal Control – The COSO Perspective, pp. 1-32, Available Online: https://www.coso.org/Documents/Blockchain-and-Internal-Control-The-COSO-Perspective-Guidance.pdf, Accessed on: 20.03.2022

Buterin V. (2014): Ethereum: A next-generation smart contract and decentralized application platform, Available Online: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, Accessed on: 12.03.2022

Chalker, A. (2018): Why Internal Auditors Must Care About Blockchain, published on Protiviti.com, Available Online: https://blog.protiviti.com/2018/06/12/internal-auditors-must-care-blockchain/, Accessed on: 30.05.2022

Chedrawi, C. (2018): Audit in the Blockchain era within a principal-agent approach, Conference paper - Information and Communication Technologies in Organizations and Society (ICTO 2018)

Chen, H./ Zhou, H./ Yu, J./ Wu, K./ Liu, F./ Zhou, T./ Cai, Z. (2021): Trusted audit with untrusted auditors: A decentralized data integrity Crowdauditing approach based on blockchain, Int J Intell Syst. 2021;36, pp. 6213-6239. https://doi.org/10.1002/int.22548

Chen, L./ Reiser, H. (2017): Distributed Applications and Interoperable Systems, 17th IFIP WG 6.1 International Conference, DAIS 2017, Held as Part of the 12th International Federated Conference on Distributed Computing Techniques, DisCoTec 2017, Neuchâtel, Switzerland, June 19–22, 2017, Proceedings, Springer International Publishing, pp. 1-205

Chohan, U. (2017): The Decentralized Autonomous Organization and Governance Issues, pp. 1-6

Coinmarketcap (2023): Top DAO Tokens by Market Capitalization, published by Coinmarketcap.com, Available Online: https://coinmarketcap.com/view/dao/, Accessed on: 21.04.2023

Coinmarketcap (2023): Today's Cryptocurrency Prices by Market Cap, published by Coinmarketcap.com, Available Online: https://coinmarketcap.com/, Accessed on: 21.04.2023

Diederich, H. (2016): Ethereum – Blockchains, digital assets, smart contracts, decentralized autonomous organizations, Wildfire Publishing, ISBN 9781523930470, pp. 1-346

Dyball, M./ Seethamraju, R. (2021): The impact of client use of blockchain technology on audit risk and audit approach – An exploratory study, Int J Audit. 2021;25: pp. 602–615, Wiley, https://doi.org/10.1111/ijau.12238

Eulerich, M. (2018): Die Interne Revision, Theorie – Organisation – Best Practice, Erich Schmidt Verlag, Berlin 2018, ISBN 978-3-503-17693-9, pp. 1-498

Ferguson, C./ Buchanan, F./ Barnett, W. (2020): Influential Article Review - How the Bitcoin Caused the Emergence of Autonomous Organizations, American Journal of Management, 19(6), pp. 1-35

Frankenfield, J. (2021): Master Node, published on Investopedia.com, Available Online: https://www.investopedia.com/terms/m/master-node-cryptocurrency.asp, Accessed on: 12.03.2022

Gilbert, A. (2022): Decentralized Autonomous Organizations. The New LLCs?, published on Bloomberg Law, Available Online: https://news.bloomberglaw.com/banking-law/decentralized-autonomous-organizations-the-new-llcs, Accessed on: 10.09.2022

Hanzl, M. (2019): Decentralized Autonomous Organization (DAO) – Notwendigkeit eines neuen Gesellschaftstyps?, published in ÖJZ 2019/36, retrieved from the RDB Manz database, pp. 293-297

IIA A (2017): The IIA's CIA Learning System, Internal Audit Basics Part 1, published by the Intitute of Internal Auditors, pp. 1-1 – 1-302

IIA B (2017): Model Internal Audit Activity Charter, IPPF Supplemental Guidance, published by the IIA, Available Online: https://www.theiia.org/en/content/guidance/recommended/supplemental/practice-guides/model-internal-audit-activity-charter/, Accessed on 22.05.2022, pp. 2-8

Innovation Eye (2021): Blockchain Industry in the UK Landscape Overview 2021: Companies, Investors, Influencers and Trends, Available Online: https://analytics.dkv.global/Blockchain-in-the-UK-2021/Full-Report.pdf, Accessed on: 30.05.2022

Jentzsch, C. (2016): Decentralized Autonomous Organization to Automate Governance, pp. 1-31, Available Online: https://lawofthelevel.lexblogplatformthree.com/wp-content/uploads/sites/ 187/2017/07/WhitePaper-1.pdf, Accessed on: 12.03.2022

Kaal, W. (2021): Decentralized Autonomous Organizations – Internal Governance and External Legal Design, Electronic copy available at: https://ssrn.com/abstract=3652481, pp. 1-66

Konashevych, O. (2021): Takeaways: 5 years after The DAO crisis and Ethereum hard fork, published on cointelegraph.org, Available Online: https://cointelegraph.com/news/takeaways-5-years-after-the-dao-crisis-and-ethereum-hard-fork, Accessed on: 12.03.2022

Lemieux, V. (2016): Trusting records: is Blockchain technology the answer?, Records Management Journal, Vol. 26 No. 2, 2016, pp. 110-139, Emerald Group Publishing Limited, 0956-5698, DOI 10.1108/RMJ-12-2015-0042

Lineros, J. (2021): IT Governance Considerations for Permissioned Blockchains, Journal of Emerging Technologies in Accounting, American Accounting Association, Vol. 18, No. 1 DOI: 10.2308/JETA-19-12-01-49, Spring 2021, pp. 45–59

Lipton, E./ Livni, E. (2022): Reality Intrudes on a Utopian Crypto Vision, published on nytimes.com, Available Online: https://www.nytimes.com/2022/03/08/us/politics/cryptocurrency-dao.html, Accessed on: 12.03.2022

Lom, A./ Browndorf, R. (2021): Wyoming to Recognize DAOs as LLCs, Available Online: https://www.regulationtomorrow.com/us/wyoming-to-recognize-daos-as-llcs/, Accessed on: 12.03.2022

Loncarevic (2023): Internal Audit in the Age of Blockchain-based Decentralized Autonomous Organizations, University of Applied Sciences Burgenland & University North, Croatia

McCollum, T. (2020): Backing the Blockchain, Executives seek to grow value of digital assets, published as Online Exclusive for the IA Magazine

Mini, T./ Ellinger, E./ Gregory, R./ Widjaja, T. (2021): An Exploration of Governing via IT in Decentralized Autonomous Organizations, Forty-Second International Conference on Information Systems, Austin 2021, pp. 1-17

Mou, V. (2020): Blockchain Oracles Explained, published on binance.com, Available Online: https://academy.binance.com/en/articles/blockchain-oracles-explained, Accessed on: 12.03.2022

Müller, B. (2021): Arten von Knotenpunkten im Bitcoin-Netzwerk, published on wirtschaftszeit.at, Available Online: https://wirtschaftszeit.at/startseite-detail/article/arten-von-knotenpunkten-im-bitcoin-netzwerk, Accessed on: 12.03.2022

Murray, A./ Kuban, S./ Josefy, M. (2021): Contracting in the Smart Era: The Implications of Blockchain and Decentralized Autonomous Organizations for Contracting and Corporate Governance, Academy of Management Perspectives, Vol. 35, No. 4, pp. 622-641

PC Concordia (2021): Präsentation: 1. Österreichischer Revisions-Report – ein Land unter Interner Revision, published as a Youtube Video by Presseclub Concordia, Available Online: https://www.youtube.com/watch?v=g3KbdefdCAU, Accessed on 30.05.2022

Peterson, S. (2018): Embrace Change or Become Obsolete, published in Internal Auditor magazine, 04/2018, p. 68

Protiviti (2021): The Next-Generation Internal Audit Journey Needs to Begin Now, Assessing the Results of Protiviti's 2021 Next-Generation Internal Audit Survey, published online at Protiviti.com, pp. 1-38

Pugliese, A. (2021): CEO Message: Envisioning the Next 80 Years, published as an Online Exclusive of the Internal Audit Magazine, pp. 1-4

Rapaport, M. (2018): PwC Has an Answer for the Blockchain: Audit It, Accounting firm unveils new service for clients' use of blockchain, published on the WSJ Online, Available Online: https://www.wsj.com/articles/pwc-has-an-answer-for-the-blockchain-audit-it-1521194401, Accessed on: 30.05.2022

Rikken, O./ Janssen, M./ Kwee, Z. (2019): Governance challenges of blockchain and decentralized autonomous organizations, Information Polity 24 (2019), pp. 397–417, DOI 10.3233/IP-190154, IOS Press

Seth, S. (2021): How Do Cryptocurrency Mining Pools Work?, published on Investopedia.com, Available Online: https://www.investopedia.com/tech/how-do-mining-pools-work/, Accessed on: 12.03.2022

Smith, S. (2019): Blockchain, Artificial Intelligence and Financial Services: Implications and applications for finance and accounting professionals. Springer Nature, pp. 1-263

Smith, S./ Castonguay, J. (2020): Blockchain and Accounting Governance: Emerging Issues and Considerations for Accounting and Assurance Professionals, Journal of Emerging Technologies in Accounting, Vol. 17, No. 1, Spring 2020, pp. 119-131, American Accounting Association, DOI: 10.2308/jeta-52686

Snyder H. (2019): Literature review as a research methodology: An overview and guidelines, Journal of Business Research 104, pp. 333–339

Theiia.org (2022): About the Institute of Internal Auditors (IIA), Available Online: https://www.theiia.org/en/about-us/, Accessed on: 12.03.2022

The IIA (2017): International Standards for the Professional Practice of Internal Auditing (Standards), Available Online: https://www.theiia.org/en/standards/what-are-the-standards/mandatory-guidance/standards/, Accessed on: 12.03.2022

Vigliotti, M./ Jones, H. (2020): The Executive Guide to Blockchain – Using Smart Contracts and Digital Currencies in your Business, Springer Nature Switzerland AG, ISBN 978-3-030-21106-6, pp. 121-139

Vincent, N./ Barkhi, R. (2021): Evaluating Blockchain Using COSO, American Accounting Association, Current Issues in Auditing, Vol. 15, No. 1, pp. 57-71

Vom Brocke, J./ Simons, A./ Niehaves, B. / Riemer, K./ Plattfaut, R./ Cleven, A. (2009): Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Process, Conference Paper, pp. 1-14

Voshmgir, S. (2019): Token Economy – How Blockchains and Smart Contracts Revolutionize the Economy, 1st Edition, Blockchain Hub Berlin, ISBN: 978-3-9821038-2-2, pp. 1-310

Yaffe-Belany (2022): Reality Intrudes on a Utopian Crypto Vision & More Cryptocurrency News, published in the New York Times Online, Available Online: https://www.nytimes.com/2022/03/08/us/politics/cryptocurrency-dao.html, Accessed On: 02.06.2022

Yermick, D. (2017): Corporate Governance and Blockchains, Review of Finance, 2017, pp. 7–31, published by Oxford University Press on behalf of the European Finance Association. doi: 10.1093/rof/rfw074