Published in Proceedings of the Hawai'i Accounting Research Conference (HARC) 2022, 3-5 January, Honolulu, Hawaii, USA, which should be cited to refer to this work.

Augmenting Audit and Control: a Blockchain Based Control Framework (BBCF)

Abstract

Audit and control have become key elements of sound corporate governance. While the Three Lines Model (TLM) provides an organizational structure to execute risk and control duties, research and practice show that this model also has limits even when integrated within proper Enterprise Risk Management (ERM) and Internal Control (IC) frameworks. Such control weaknesses could be addressed by leveraging properties of distribution, transparency, and immutability of blockchain technology. To this end, this paper proposes a conceptual control framework based on blockchain technology to augment common control practice with more trustworthy and accountable blockchain based control patterns. The design of the resulting Blockchain Based Control Framework (BBCF) and its prototype are presented and discussed in terms of potential impact in the context of the identified limits and in particular with respect to COSO, the TLM and risks in general. The contribution intends to serve both as a starting point for discussing the evolution of audit and control practice based on blockchain technology, as well as an initial actionable prototype for experimentation and further development.

Keywords: Auditing, Internal Controls, Lines of Defense, Blockchain

1 Introduction

Every organization sets objectives to achieve. While pursuing those objectives, an organization will face events and circumstances that may threaten their achievement (COSO, 2017). The Committee of Sponsoring Organizations of the Treadway Commission (COSO), whose principal mission is to develop frameworks and guidance on enterprise risk management, internal control, and fraud deterrence to improve organizational performance and governance, released two main frameworks: the Enterprise Risk Management (ERM) – Integrated Framework to effectively identify, assess, and manage risks (Lyons, 2015) and the Internal Control (IC) – Integrated Framework to provide companies with a methodology and some tools to ensure organizational objectives relating to operations, reporting and compliance are achieved. As explained by the COSO, even though those two publications have different focus, they are related. Indeed, internal control, whose main purpose is to mitigate risks, is part of an ERM system which is a broader system that addresses other topics such as strategy-setting, governance, communication with stakeholders, and performance measurement (COSO, 2020).

Nowadays, both frameworks are widely used by organizations, and the IC Integrated Framework is even considered as the standard for the design, operation and assessment of internal control systems related to operations, compliance, and financial reporting (COSO; Martin et al. 2014). It consists of five interrelated components (control environment, risk assessment, control activities, information & communication, monitoring activities) across three categories of objectives (operations, reporting and compliance) that are derived from the way management runs an enterprise and are integrated with management process. The

definition provided by COSO – IC Integrated Framework of the five components of the framework is provided in Appendix A – COSO Definition (COSO, 2013).

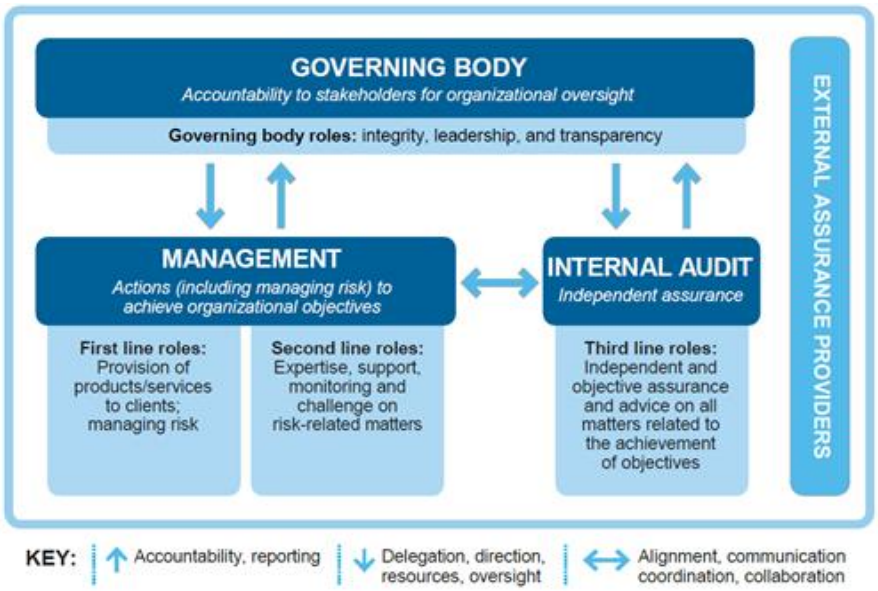
COSO defines internal control as "a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations" (COSO, 2013).

The financial crisis of 2008 has shown, however, that having an ERM system and internal controls in place are not enough to manage risks properly and effectively. Indeed, at that time, financial institutions had been among the earliest adopters of the COSO ERM framework and were supposed to have the most mature and sophisticated ERM programs in place (Lyons, 2015). Some researchers (Lyons, 2015; Davies & Zhivitskaya, 2018; Arndorfer & Minto, 2015) suggest that one of the various causes of the 2008 financial crisis was the governance model of those financial firms and the disengagement of their Board of Directors ("the board"), representing the shareholders' interests. To enable the achievement of their objectives, organizations actually need effective structure and processes to not only manage risk but also support strong governance.

Risk governance refers to the architecture within which the ERM system operates in an organization and how it identifies, measures, and manages risks at the organization-wide scale. The board is ultimately responsible for the governance of the ERM system and should therefore ensure that executive management maintains a sound ERM system, including internal controls, to safeguard stakeholder interests and the organization's assets. In order to do so, the board should ensure that there is a comprehensive and robust ERM oversight system in place (Lyons, 2015). In this context, the Institute of Internal Auditors (IIA) published in 2013 a position paper on an ERM oversight model called the Three Lines of Defense Model (TLDM) (IIA, 2013). This model has been widely adopted by organizations (Lyons, 2015; Dogas, 2016; Arndorfer & Minto, 2015; Vousinas, 2019; Potter & Tuburen, 2016, Bank of England 2015), and has become a required organizational model by banking regulators and the Basel Committee on Banking Supervision in regulated financial institutions (Arndorfer & Minto, 2015; Banteleon, et al. 2020).

An ERM oversight model should provide a clear structure of responsibility and accountability for organizations' ERM systems and processes (Lyons, 2015). As such, the TLDM addresses how specific duties related to risk management and internal control could be assigned and coordinated within an organization (IIA, 2015). In 2020, to address the emergence of new risks and the growing complexity of organizations, the IIA has updated the TLDM and has renamed it "the Three Lines Model" (TLM) (IIA, 2020). This updated model clarifies the different types of relationships among the different roles and among the different lines. It also highlights the need of communication, cooperation and collaboration among the different activities to create and protect value for the shareholders. The model is graphically depicted in Figure *1*.

Figure 1: The Three Lines Model



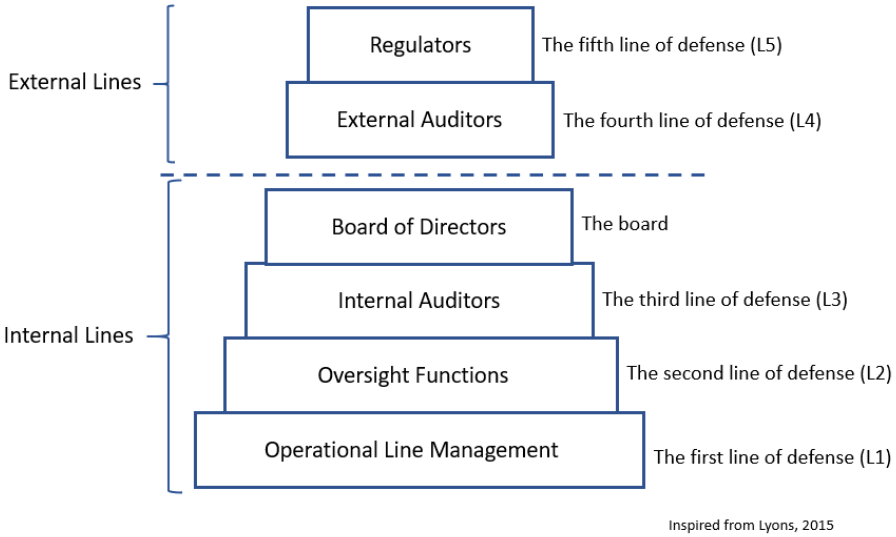
Source: The IIA's Three Lines Model, page 4, July 2020.

- The **governing body (e.g., the board)** is ultimately accountable for an organization's governance. It delegates responsibility and provides resources to management to achieve the objectives of the organization; and at the same time, it oversees management, including risk management and the performance of internal control system, to ensure that actions taken are aligned with shareholders' interests.
  For the first time, in its 2020 publication, the IIA noted that the "governing body roles" also constitute a "line", which was already suggested by some researchers (Lyons, 2019; Leech & Hanlon, 2016) but without naming it as such in its model (see Figure *1*).
- **Management** is responsible for achieving an organization's objectives. It comprises both the first and the second lines' roles:
  - **The first line (L1)**: owns and manages risk and controls. It includes both "front and back office" activities and focuses on delivering products or services to clients of the organization and can therefore be seen as the "operational line management" (Lyons, 2015).
  - **The second line (L2)**: monitors and assists risk and controls in support of management. It includes complementary activities focused on risk-related matters such as compliance with laws, regulation, internal control, IT security, quality assurance which Lyons (2015) calls the "tactical oversight functions".
- **The third line (L3)**: is usually represented by the internal audit function. It monitors the effectiveness of the other lines of defense, provides independent and objective assurance and advice on the adequacy of governance and risk management. It is responsible for the coordination tasks (IIA, 2017), communicates its findings to management and reports them to the governing body.
- **External Assurance Providers (L4)**: is usually represented by the external auditors. They provide an autonomous assessment of the first two lines where this is relevant to the audit of the organization's financial reporting and to compliance with regulatory

requirements. Some researchers present the external auditors as a line of defense which they call “the fourth line” (Arndorfer & Minto, 2015; Klotz, 2015; Vousinas, 2019).

We also noted that several researchers propose the **Regulator** as another line of defense, sometimes called the **fifth line of defense (L5)**, especially in regulated industries such as banks and insurance (Arndorfer & Minto, 2015; Klotz, 2015; Vousinas, 2019).
Integrating all those elements, The Line of Defense Model could also be presented as follow:

Figure 2: The Line of Defense Model



From a theoretical point of view, the TLM can be understood as an organizational framework that helps to reduce potential information asymmetries in the context of the principal-agent theory. Thus, the different lines of defense reduce the information asymmetries between the principals and agents throughout the different hierarchy levels and minimize the risks of discretionary decisions from the agents (Banteleon, et al. 2020). It also provides an organizational structure to execute risk and control duties in a way to minimize the likelihood of both risk gaps and significant control breakdowns. However, research and practice show that this model, even when integrated within an ERM framework and an IC framework such as COSO, has several limits. It is common for investigations into the cause of large-scale corporate failure to identify the lines of defense weaknesses in the organization(s) concerned as being a significant contributing factor (Lyons, 2019). Among those weaknesses, as reported in the literature (Decaux & Sarens, 2015; KPMG, 2012; Roussy & Rodrigue, 2018; Sarens, Decaux & Lenz, 2012; Lyons, 2019; Suk-Young Chwe, 2000; UK Parliament, 2013; Davies & Zhivitskaya, Banteleon et al., 2020, Luburic 2017; Udding 2016; EY, 2013), we find:

- lack of coordination among lines,
- siloed risk functions,
- ambiguous responsibilities,
- redundant controls,

- assurance gap,
- lack of first line accountability,
- static model with a dynamic environment,
- inconsistent and multiple reporting,
- assurance fatigue,
- lack of quality information on risk to the board,
- inadequate or inconsistent reporting.

This paper intends to contribute to the resolution of most of the weaknesses identified within the TLM by proposing a conceptual framework based on a new and growing technology, namely, blockchain technology. The development of this framework called "Blockchain Based Control Framework" ("BBCF") and its associated prototype to showcase the potential impact of blockchain on audit and control activities are part of a Swiss National Science Foundation (SNF) research grant[1]. To develop our framework, we used the Design Science Research Methodology (DSRM) developed by Peffers et al. (2008). DSRM consists of six activities: (1) problem identification and motivation, (2) definition of the objectives of a solution, (3) design and development, (4) demonstration, (5) evaluation and (6) communication. The objectives of Design Science Research (DSR) are to create and evaluate IT artifacts intended to solve identified organizational problems (Hevner et al., 2004) or improve the way they are solved. Those artifacts can be concepts, models, methods, and instantiations (Hevner et al., 2004; March & Smith, 1995). Not all six activities need to be included in a single proposal of research as DSR expands to fit research projects which can span many researchers, articles, and decades of development (Appelbaum & Nehmer, 2017).

Table *1* below describes how we have used the six DSR activities to organize our research project. The arrows on the left side of the table represent iterations which are an important part of DSRM (Geerts, 2011). Hevner et al. (2004) illustrate it with their build-and-evaluate loop: evaluation provides feedback information on the designed artifact and a better understanding of the problem, leading to new iterations of the design process (Geerts, 2011). In our case, we have organized several presentations to the same group of experts – which includes financial and IT auditors, blockchain specialists, L1 and L2 representatives – and have used their feedback to better understand the issues and consequently update our model to make it more relevant.

This paper focuses on the first three activities of the DSRM, that is to say problem identification and motivation, definition of the objectives of a solution and design and development. Currently focusing on the development phase of our IT artifact, the evaluation will lead to results to be reported in a future article.

[1] Research grant information anonymized for peer review.

Table 1: DSR Activities

Principal Activities of DSR	Blockchain – Based Control Framework
Problem Identification and Motivation	Even the companies where the TLM has been deployed in combination with COSO ERM and COSO IC face risk oversight issues.
Definition of the Objectives of the Solution	The objective is to see whether the characteristics of the blockchain technology can strengthen the control environment for each line of the TLM and decrease the audit risk.
Design and Development of an Artifact	A framework combining blockchain technology with a business process conformance checker has been conceptualized, and is currently developped under the form of a Proof-of-Concept (POC).
Demonstration of the Solution	Two processes called « reference processes » will be designed to cover several situations (e.g., with and without the use of smart contracts, with manual control performed outside of the framework, with automatic control performed by another IT system that communicates the results to BBCF, etc.). Those processes will be used within the framework, and the outcome will be presented to a pool of experts to demonstrate how the framework solves one or more problems identified.
Evaluation	Metrics will be developped to measure how well the framework addresses the problems identified, and how the outcome of the POC meets the objectives defined (step 2 above). The pool of experts' feedbacks received at the demonstration (step 4 above) will also be taken into account for revising the framework's objectives and design.
Communication of the Results	When the POC will have been tested, the results will be shared with the scientific community to motivate future research and with the professional community (enterprises and external assurance providers) for potential adoption.

Inspired by Geerts, 2011

The remainder of this paper is structured as follows: In the second section we present the blockchain technology, its main characteristics, and limitations. The third section describes the conceptual model and its objectives. In the fourth section we discuss the expected benefits and limits of our framework. Finally, to conclude, we summarize future work on applying blockchain technology to the control environment.

2 Blockchain technology

A blockchain is a decentralized architecture relying on a network of computers called nodes (Alexander, 2019; Orcutt, 2019) to validate transactions to the ledger. The way transactions are verified, validated, and added in the ledger is based on a blockchain protocol which uses cryptography and consensus algorithms to secure the network. Once verified and validated according to the protocol, transactions are grouped together into blocks that are timestamped (Orcutt, 2019) and chronologically added to the chain of previous blocks. All transaction records are kept in the blockchain and are shared with the entire network, thereby ensuring transparency, immutability, decentralization, and robustness (Casino et al., 2019; Zhang et al., 2017).

Depending on the structure and participants, blockchain can be categorized into:

- **Public** or **permissionless blockchain** where everyone can transact and maintain the ledger as per the rules. It allows transactions between any party without the intervention of a centralized intermediary (Zhang et al., 2017).

Bitcoin, for example, is a public blockchain. It was the first publicly known application of blockchain technology, and it functions as a secure peer-to-peer payment system (Rozario & Thomas, 2019).

- **Permissioned blockchain** where participants must be granted access to be part of the network. In this type of architecture, a control layer runs on top of the blockchain and governs the actions performed by the allowed participants (Iredaleon, 2019). There are several subtypes of permissioned blockchains:
    - **Private blockchain** where participants are limited to one organization. Private Ethereum is an example of private blockchain. An enterprise can decide to use a private blockchain to secure settlement of cross-company transactions, enhance real-time access to data, or use smart contracts to speed up some clearing processes.
    - **Consortium** where participants are from multiple organizations. For example, Volton in the trade finance sector is a coalition of over 50 banks and companies whose goal is to reduce the time it takes to execute the entire process of paper-based letter of credit.

Within a blockchain, rules and procedures can be embedded at the transaction level, which can contribute to standardizing process activities. This technology also allows the use of smart contracts, which are programs that execute what is written in their code as soon as certain conditions are met. Thus, smart contracts can help two or more parties to collaborate without intermediary and make transactions transparent, foolproof, fast, and irreversible.

When combined with smart contracts, blockchain technology can autonomously execute tasks on behalf of human users (Szabo, 1997; Rozario & Thomas, 2019). In this regard, blockchain can help businesses to design applications and conduct transactions that are simultaneously self-executing and autonomous (DuPont & Maurer, 2015). Therefore, blockchain has gained the attention from business entities that are launching pilot projects for business application (Stratopoulos et al., 2020) in several sectors such as healthcare, supply chain management, market monitoring, smart energy, and copyright protection (Rozario et al., 2019; Xu et al., 2019).

As blockchain can also provide tamper-proof audit trails, it is gaining attention from the audit and control community. Indeed, each one of the Big Four (Deloitte, Ernst & Young, KPMG, PricewaterhouseCoopers) has dedicated employees to lead research programs on this technology to anticipate its potential impacts on the profession. Because of its key characteristics – transparency, traceability, immutability, and decentralization – blockchain is expected to change how audits and other control activities are performed. As blockchain allows entities to make digital interactions and to record any transactions, assets, or documents in a way that is transparent, secure, auditable, efficient, and highly resistant to interruptions (Schatsky & Muraskin, 2015), it should facilitate access to data. Accountable internal control results could be saved on the blockchain and could therefore be accessible by the "internal lines of defense". This should increase the coordination among those lines, improve the first line accountability, and at the same time reduce the likelihood of having redundant controls. This kind of environment should also facilitate the completion of internal and external audits. Direct

access to the blockchain could even be granted to the "external lines of defense", being the financial auditors and the regulators (Roberts, 2017), which would enable real-time auditing (MacManus, 2017; Schmitz & Leoni, 2019).

Even though blockchain offers many features, we have to notice that today several impediments exist to its wide adoption. Firstly, several technical challenges need to be addressed. The blockchain infrastructures have interoperability and compatibility issues with ERP, which often include several functional modules such as for accounting, controlling, logistics, manufacturing, warehousing, and procurement (Kacina et al., 2017).

Another key technical challenge is scalability, which is a system's ability to operate properly under heavy loads – typically, larger size or volume (Rouse, 2006). As blockchain contains the full history of all transactions across all participants, its size continues to grow indefinitely, which represents an issue (Lu et al., 2018). Moreover, because of its infrastructure design, the number of transactions transmitted, received, and validated over the network is small compared to other existing centralized infrastructures.

The other main impediment to blockchain is technical complexity integrating components (e.g., consensus algorithms and cryptography) that require technical understanding. This complexity translates into end users finding blockchain hard to understand (Marr, 2018; Price, 2019) whereas, as explained by the COSO, it is crucial, including for the board, to know how blockchain works to be able to evaluate, prepare for, and manage blockchain's impact on internal control and the organization as a whole (COSO, 2020).

Notwithstanding these technical difficulties, blockchain offers interesting properties (as described above) that may contribute to facilitating the work of the different lines, including the work of the external auditors, and to provide increased levels of assurance in order for organizations to better keep risks under control.

3 Conceptual Model Presentation

In this section, we will introduce our Blockchain Based Control Framework, where the blockchain technology is used as a support to the internal control system. We will first introduce each element of the framework, and then present how these elements work together.

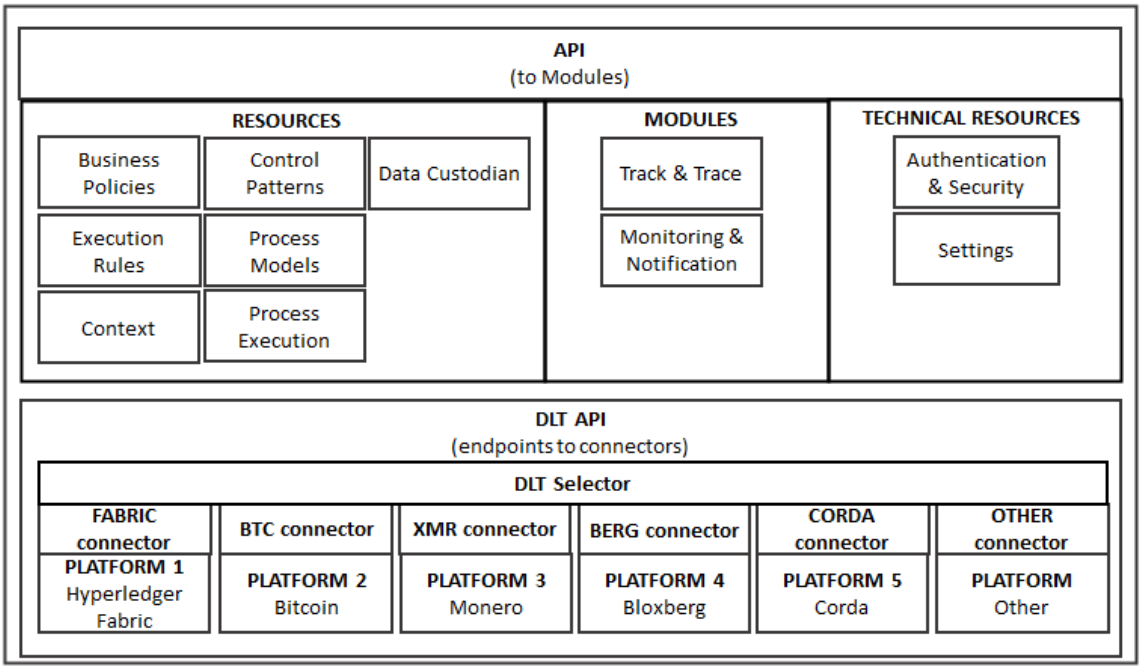
The main purpose of the framework is to address the weaknesses identified from the literature and summarized in the introduction by:

- monitoring processes,
- automatically recording on a blockchain a trace of each control performed (automatic and manual controls) and its results (passed or failed), as well as its remediation if any,
- proposing embedded controls on a blockchain under the form of smart contracts for those companies that wish to build their entire internal control system, or transition part of it using blockchain technology,
- notifying process deviation or control failure for investigation and correction,
- improving coordination among lines,
- clarifying controls and risks ownership to increase each line's accountability,
- avoiding redundant controls, which would help reducing some of the assurance fatigue,
- providing a real-time overview of process advancement and control results,

- providing meaningful and timely reporting to allow the board and executive management to oversee risks,
- improving the audit trail reliability,
- decreasing the extent of tests of details performed by the external auditors.

To fulfill those objectives, the BBCF relies on a tentative design graphically presented in Figure *3*. It is composed of two layers. The lower layer serves as an interface to the different Distributed Ledger Technology (DLT) platforms through connectors. The higher layer exposes a more business-oriented interface as a generic abstraction of specific technical DLT details.

Figure 3: Blockchain Based Control Framework Overview



A - API (Application Programming Interface): is an IT solution that allows applications to communicate and exchange services or data with each other. For example, each time an employee will want to access any resources or modules of the framework, s/he will do it via the API. The access to the API and therefore to the overall framework will be limited using access controls based on the segregation of duties (SOD) matrix where specific duties will have to be separated (e.g., the ability to authorize blockchain transactions and the ability to record transactions within the entity's general ledger, or the ability to authorize and execute changes to the blockchain). Access rights in a blockchain environment is particularly important both in a private and a consortium setups because information saved onto a blockchain is immutable and the effects of inappropriate access issues can become shared issues across companies on a blockchain (COSO, 2020). Proper access rights depending on business requirements will have to be managed accordingly within the framework.

B - Resources: represent all the data used by the modules to execute their applications. Each element of resources is presented below.

a) Business Policies: represent general guidelines set by top management. They are documents that reflect the entity's objectives and organization and are part of the entity's control environment. They define the responsibilities for each line of defense and therefore provide information used to setup the framework. Examples of a business policy would be a Code of Conduct governing the behavior of parties within a blockchain and establishing guidelines for addressing noncompliance, or a mechanism to (1) validate each member of a blockchain consortium commitment to ethics and integrity and (2) enforce accountability with the code of conduct and report/address/remediate any deviations (COSO, 2020). One could even have a Due Diligence Policy establishing guidelines and criteria for determining parties with whom the organization will transact and parties to which the organization will grant access to a blockchain (COSO, 2020).

b) Context: This element encompasses the meta parameters, structuring information, global variables for execution, and rules applying to the stakeholders – namely L1, L2, L3, the board, the external auditors, the regulators, the entity's clients, and suppliers. Examples of information used in this element would be the mapping of the relationship between the entity and its stakeholders, the rules defining how the external auditors can access the data custodian, the contact information of a supplier, etc. This element should be the responsibility of L2.

c) Data Custodian: It oversees the safe custody, transport, storage, and retrieval of data. Moreover, as some modules of the framework allow to produce traces which are registered on a blockchain, and at the same time store the related information on the data custodian, we have setup a mapping to retrieve the data associated with a trace when needed. Data custodian can be internally managed, in that case the framework itself is the custodian, or it can be externally managed by a third party. This element should be the responsibility of L2, and more precisely of Information Security.

d) Execution Rules: They cover controls rules and notification rules. For example, for a reconciliation, a control rule would stipulate that a comparison of two or more sets of records should result in a match, while a notification rule would stipulate that if the sets of data do not reconcile a notification would be sent to the control owner and to L2 for follow-up and resolution. This element should be the responsibility of L2.

e) Control Patterns: We established our controls classification as the COSO framework does not provide a complete list of internal control activities. To do so, we examined the controls that were implemented in 4 distinct business processes – Know Your Customers (KYC), Couponing, Compliance, and Program Change Management – from 4 companies in 4 different industries (banking, food processing, auditing, and a large manufacturing company). These 4 processes served as reference processes for the project. The control listing of 2 of the Big Four were reviewed in parallel. This work helped us to identify 10 different controls that are recurrent across any organization's processes: Review, Authorization, Approval, Performance Planning, Evaluation, Reconciliation, Segregation of Duties, Physical Control over Assets, IT General Control, and IT Application Control. Each control activity is defined in Appendix B – List of Internal Control Activities.

- Control is defined as a process (COSO, 2013). A process is a series of actions or steps taken in order to achieve a particular end; therefore, a control is a recurring activity with a start,

one or several operations and an outcome. Based on this observation, it appeared that we could use the software design pattern framework to create what we call "control patterns" in order to:

- standardize and streamline internal control activities – which would improve control design[2], and
- automatize and operate as much as possible those controls onto a blockchain which would improve control effectiveness.

A description of each control pattern is provided in Appendix C – Control Patterns. Each pattern follows the inputs / operations / outputs model.

We have mapped the 10 controls to COSO objectives (effectiveness and efficiency of operations, accuracy of financial reporting, compliance with applicable laws and regulations, and fraud prevention) (COSO, 2020), and to management assertions. Management assertions are the implicit or explicit claims and representations made by management regarding the recognition, measurement and presentation of assets, liabilities, equity, income, expenses and disclosures while preparing the financial statements in accordance with the applicable financial reporting framework. The list and definition of management assertions is provided in Appendix D – Management Assertions, and the mapping among controls, COSO objectives and management assertions is provided in Appendix E – Mapping.

By associating control patterns to COSO objectives and to management' assertions, we provide management with some sort of predefined control activities that can be used in any process depending on the control objectives that have been assigned to mitigate the risks. Thus, each control pattern can be seen as a building block which can be combined with other(s) building block(s) to fulfill one or some COSO objectives and one or some management assertions. These building blocks can be combined with underlying blockchain technologies in accordance with the level of maturity of blockchain use within the organization. The organization would then have a workbench of "ready-to-use" blockchain-based controls that can be used in any of its business processes to keep risks under control. Within our framework, a control can be:

- manually performed outside of the platform. In this case, the control owner (L1) records a trace in a blockchain of the control performed in a blockchain using the Track & Trace module described below.
- automatically performed outside of the platform by another system such as an ERM. In this case, a trace of the control performed is automatically registered in the blockchain.
- fully supported by the platform. For example, a reconciliation performed thanks to a smart contract whose trace of performance is automatically recorded by the module Track & Trace in the blockchain.

Control Patterns should be the responsibility of L1, as specified by the LDM.

f) Process Models: This resource includes new processes, updated processes, and deactivated processes. Each process will include several steps that will be tagged as "control" or "task". Examples of process models would be a KYC process implemented by a bank, a "couponing" process where a company issued coupons that customers can use to get a discount,

[2] Using patterns, the control "reconciliation" for example encompasses a regular accounting reconciliation between a sub-ledger and the general ledger, a 3-way match, and controls over data transfer to and from the blockchain to the entity's general ledger system and other off-chain systems.

a “change request management” process to plan, implement and evaluate changes to a system, etc.

L2 should be responsible for this element of the framework and more precisely should be responsible for:

- Writing, in collaboration with L1, the entity’s processes,
- Managing the process update,
- Ensuring the right version of the process is saved and used within the framework in the module Track & Trace described below,
- Identifying, in collaboration with L1, the risks within each process,
- Ensuring, in collaboration with L1, that each risk within a process is properly mitigated by one or several controls.

g) Process Execution: A process can be executed several times a day (e.g., KYC), or several times a year (e.g., couponing, change request management). For each process recorded within Track & Trace (see description of Track & Trace below), it is possible to define a context relative to an execution instance of a specific version of such process. This context gathers the traces recorded as the tasks of the process are executed automatically within the company's information system or manually by the employees. L1 should be responsible for this element of the framework and must ensure that processes are performed in accordance with the process model.

C - Modules: They represent the two main functionalities of the BBCF. Each module is presented below.

a) Track & Trace: This module is a conformance checker. It checks whether the data (controls and tasks performed) entered into BBCF conforms to information stored in Control Patterns and Process Model. As such, the Track & Trace module:

- allows to create, update and deactivate processes, and to automatically setup dependence trees to order steps and controls of a process based on the model of such process. This information is then stored within the resource Process Model,
- ensures that the steps of a process are performed in the right order (according to the dependence tree),
- ensures that all the controls pertaining to a process are properly performed (according to Process Model and Control Patterns),
- leaves a trace on blockchain for each activation and deactivation of a process,
- leaves a trace on blockchain for each activation, deactivation, deviation, or cancellation of an execution instance,
- leaves a trace on blockchain for each control performed and its outcome (passed or failed),
- leaves a trace on blockchain for a task if requested in the process set-up. Indeed, while creating a process within Track & Trace, a task can be tagged to leave a trace,
- informs the module Monitoring & Notification when flaws are detected (a flaw could be that a violation of the model has been detected, a control has failed or has been performed at an inappropriate time, etc.),
- allows to retrieve traces saved on blockchain and the underlying data using the data custodian.

A trace is a set of information recorded by the platform internally or on a blockchain. Each trace reflects the completion of an action (e.g., the creation of an execution instance) or the occurrence of an event (e.g., a violation of a process model detected by the Track & Trace module during an attempt to add an execution instance update, or a deficiency during control performance). Each trace can act as audit evidence as it allows retrieval of original resources used to perform the control or registered during task completion.

The framework allows to check that there are as many traces reflecting the different service calls made to the API than traces reflecting the execution results of aforesaid services. In the case of Track & Trace, it would be possible to verify completeness of traces for processes (creation and deactivation) but also execution instances (by verifying that for any call made to Track & Trace, there is a trace reflecting the creation, start, stop or update of an instance).

L1 and L2 should be responsible of this module. L3 and the external auditors could be interested in the module activity to spot issues and assess risky areas.

b) Monitoring & Notification: This module has two functions: it follows activities (progress of execution instance and controls performance) and sends activity reports to the desired group(s) of person(s).

Based on information received from Track & Trace, this module can notify the desired group(s) of person(s) (e.g., the control owner, L2, L3, the board, external auditors, or any other groups) when an issue has been detected. As notifications and reports can be tailored, all the lines of defense, the board of directors and the external auditors can be interested in this module and ask for specific information.

D - Technical Resources: represents internal data that are used by the framework to ensure its proper functioning and integrity. The two elements of Technical Resources are presented below.

a) Authentication & Security: protects the global API, handles the verification of user rights and privileges, handles the security related to blockchain platforms and users in coordination with the DLT layer, and so on. L2 and more precisely the Information Systems team should be responsible for Authentication & Security.

b) Settings: covers all the technical parameters that ensure the proper functioning of the framework, such as server addresses and ports of the modules, database configuration, blockchain key management, etc. L2 and more precisely the Information Systems team should be responsible for Settings.

E - DLT Selector: is a functionality exposed by the DLT API allowing to choose the blockchain platform where the trace will be saved according to a set of technical rules and parameters. The framework uses several blockchains because each blockchain platform has its own specificities (e.g., organizational structure, source of participants, transaction costs, etc.), and depending on the entity's needs (data confidentiality, data accessibility, data management costs, etc.), the DLT Selector would automatically select the blockchain where the trace will be saved. L2 and more precisely the Information Systems team should be responsible for DLT Selector.

In Appendix G – Description of the Main Activities of the Framework, we provide a table listing the main activities exposed to the users of the framework and a description of what these activities are about. Also, for each activity, we define the different operations made by the framework by specifying the modules involved, the steps executed within them and, each time, the inputs processed by such modules and the outputs they produce.

It is worth noting that, depending on entities, the framework can be deployed with different levels of use of services and blockchain support:

- Level I (Passive) – Trace only: The framework is used only to save traces on blockchain. These traces represent tasks performed either manually or within other IT systems such as an ERP.

- Level II (Active) – Trace and Execution Rules: Within this level, the platform is used to save traces related to either one control pattern executed individually or one task of a registered process inside Track & Trace. The registration of such traces can be subject to rules imposed by Track & Trace (i.e., compliance with the process model) or by specific policies (e.g., an execution rule that enforces a result of execution for a pattern control in order to mark it as successful).

- Level III (Active, on chain) – Smart contracts: Here, smart contracts are implemented and used as much as possible to execute logic related to registered control patterns.

For all these levels, monitoring and notification strategies can be defined. Reporting can also be set up within levels II and III.

4 Discussion

The conceptual framework described in this paper combines the use of an emerging and growing technology – namely, blockchain – with a business process conformance checker to reinforce the organizational structure and governance of an organization, strengthen its control environment, and facilitate the audits performed by both internal and external auditors, and even regulators. From our knowledge, the use of blockchain coupled with a conformance checker has not been developed and published yet. Only attempts to show full on-chain execution have been considered, for example by Weber et al. (Weber et al., 2016), Carminati et al. (Carminati, Ferrari, et al., 2018; Carminati, Rondanini, et al., 2018), and López- Pintado et al. (López-Pintado, Dumas, et al., 2019; López-Pintado, García-Bañuelos, et al., 2019). Any company can use this framework and implement it in accordance with its governance and technology maturity levels as well as internal control requirements.

We are currently developing the Proof of Concept (POC) of our model and will therefore be able to evaluate its impacts as recommended by the DSRM (Sedbrook and Newmark, 2008). Once ready, the POC will be presented to the group of experts we have been working with to get their feedback. The magnitude of the blockchain's potential impacts on internal control may vary depending on how it can be coupled with other technologies and how it is used (either as a private ledger only or within a consortium). Nonetheless, we expect our model to significantly contribute to the strengthening of internal control systems and facilitate auditing practice by

positively impacting the 5 components of the COSO framework, the 3 objectives of COSO IC and the lines of defense. We have also identified some risks and limitations that we present below.

A – Impacts on the five components of the COSO framework

a) The control environment should be strengthened in several ways.

The internal control structure of the organization will be more easily understandable as people in charge of performing controls are clearly identified within the framework (assignment of responsibilities), which also promotes accountability.

The module "Track & Trace" will not only provide the latest process description but also ensure that processes are properly followed by monitoring both the order of execution of the different steps they include and the performance of planned controls according to their definition. Moreover, the trace of a control performed and saved in blockchain will provide an irrefutable record (i.e., a person or an organization will not be able to deny or contest their role in authorizing/sending a message or record).

If the entity decides to use smart contracts (Level III of our framework deployment), human intervention will be minimized. This will limit the risks of errors and at the same time increase the reliability and security of the controls executed through smart contracts.

Lastly, reports on internal controls can be sent to the BOD on a regular basis using near real-time information, which will help carry out its governance oversight responsibility.

b) The risk assessment should be more dynamic.

Indeed, our framework will be able to identify on a real-time basis controls that are either deficient or not performed and notify the appropriate functions. The possibility to create ad hoc reports using near real-time data tailored to meet each line's specific needs will increase the business environment agility. Improper or deficient processes and controls will be highlighted in near real-time, allowing the Management and the BOD to timely respond to the risks identified, and assess whether the specific objectives for operations/reporting/compliance are met and take appropriate actions if deemed necessary.

Within the Level III of BBCF' deployment, smart contracts represent an important part of the risk mitigation tool set. In fact, their use minimizes human intervention, which should result in less operational errors, thus reducing the risk of loss, and the opportunities to perpetrate fraud. Moreover, controls executed within smart contracts are more reliable and secure, which should impact the risk assessment performed by management.

c) Control activities should be reinforced at the different levels of the entity and at the various stages within business processes, which should contribute to better mitigating risks.

First, the framework will increase the visibility of control results which will be accessible near real-time by all parties to the transactions, allowing timely remediation when necessary. Second, it will increase the traceability of processes steps, controls performed and their results, which will improve the audit trail. The use of blockchain will also help maintaining record integrity.

Lastly, as explained above, when properly designed and implemented, smart contracts enable control activities making controls more reliable and secure, and minimize both human error and opportunities for fraud, thus reducing the overall risk.

d) The internal and external communication should improve as the flow of information should be eased.

The possibility to have ad hoc and near real-time reports will improve both internal and external communication. Indeed, reports geared toward management allow timely decisions, and when tailored for external users, they create new ways to communicate financial results and information to stakeholders.

Moreover, as the framework relies on blockchain technology, it will, from an internal and external communication standpoint, (1) increase the visibility of information, (2) promote the availability of data that is accessible, accurate, consistent, current, retained, and timely, and (3) increase the level of confidence in the entity's production and publication of information.

e) As monitoring will be embedded into the framework, the related activities should be systematized.

As information is collected or aggregated onto blockchain on a near real-time basis, the Monitoring & Notification module will catch problems closer to the occurrence of a deficiency, minimizing exposure and speeding remediation, and will communicate ad hoc reports on a regular basis to management and BOD. The framework also offers the possibility to generate the balance score cards or indicators based on the pre-defined reports.

B – Impacts on the three objectives of the COSO IC framework

We also expect our BBCF to positively impact the three objectives of the COSO Internal Control framework. Indeed, the BBCF should:

a) allow some efficiency and effectiveness gains at the operational level

Indeed, Track & Trace allows to ensure that processes are properly performed and that the traces of controls or process steps and related supporting data are easily accessible within the blockchain which provides evidence of transaction. Moreover, the framework facilitates monitoring activities as reports can be created on a regular basis (near real-time), on any topics, and in extensive details (creation/deactivation of a process, start and stop of a specific execution instance, and success/error of a control). Deviations can therefore be detected and addressed timelier. We expect our framework to contribute to streamlining processes by establishing coping mechanisms when deviations are identified. For example, processes could be stopped when the deviation is related to a key control in absence of a compensating control, continued with trace registration and notification emission when the compensating control is executed successfully, or continue with a trace and a notification when the deviation relates to a standard control. The use of smart contracts can also be a means of effectively and efficiently conducting global business as they allow to minimize human interventions, which should result in less operational and transactional errors and less opportunities for fraud.

b) improve financial reporting reliability, timeliness, and transparency

Indeed, the framework allows to ensure that the reporting process is performed as it should. It also provides the evidence that the controls are made, and that control failures are addressed timely and remediations also produce an immutable trace. As those evidences are saved onto the blockchain, they are accessible by all the blockchain participants and they cannot be modified, which creates the means to enhance the availability of the information to support the financial books and records and speed up both the financial reporting and the auditing process, which in turn allows to communicate the financial information to key stakeholders faster.

The resort to smart contracts would also imply fewer human interventions and therefore should result in less reporting errors. Moreover, as transactions can be processed and recorded almost simultaneously, the risk of booking error should decrease.

c) provide evidence of compliance with laws and regulations

Our framework provides both evidence that regulated processes (such as KYC) are performed as they should, and evidence of control performed and related results to ensure adherence to laws and regulations. Moreover, the possibility to ensure compliance through smart contracts also guarantees adherence to law and to regulations.

C – Impacts of the framework on the Three Lines Model

The BBCF should also help the different lines as well as the BOD and the external assurance providers with their attributes and responsibilities. Based on the recommendations provided by the Institute of Internal Auditors in their updated document on the Three Lines Model, we expect the following impacts.

The BBCF should allow the BOD to clearly delegates responsibility as each participant's roles, rights, and attributes:

- will be defined within the framework through two of the elements of resources – the Business Policy and the Context (as described above);
- will be translated into the API access rights, and the identification of the process owners and the control owners in the Process Model (as described above).

Moreover, the possibility to tailor reports should:

- help the BOD with their duty to oversight the entity including risk management, and more particularly the internal controls by providing real-time information. Those reports should help the BOD to assess the internal control's effectiveness and, by extension, the organization's risk exposure.
- allow the BOD to timely and regularly communicate in a transparent way to the stakeholders whether the entity is achieving its objectives. Indeed, the data used to generate the reports could be directly accessible by the stakeholders (depending on the type of blockchain – public or consortium), which in turn should increase the BOD's accountability and the stakeholders' confidence.

The combination of the different modules (Track & Trace, Monitoring & Notification) should support L1 in its duty to establish and maintain appropriate structures and processes for the management of operations and risks. Moreover, using near real-time information on process flows and control results, L1 should be able to assess the risk exposure of the organization and its compliance with internal and external policies and laws, and to timely adjust the operations

when necessary. L1 should also be able to ensure that the current resource allocation allows the entity to reach its objectives and to adjust when necessary. Thus, L1 would be able to assess whether the processes in place are effective, and work with L2 when this is not the case as explained further below. Moreover, the fact that control owners, control doers, control reviewers and process owners are clearly identified should increase each employee's accountability, which in turn should positively impact the entity's processes and controls effectiveness. L1, L2, L3 and the BOD could have access to the same data and to the same reports, which would promote transparency and deeper conversations on the entity's monitoring and strategy.

As the framework provides near real-time information on operations' compliance with the entity's processes and on internal control outcomes (pass or fail), L2 should be able to timely and more easily monitor and assess the adequacy and effectiveness of the risk mitigation practice within the organization. The framework would also allow L2 to better understand where the failures are coming from (e.g., by identifying the processes that are not performed properly, the employees who do not perform their tasks properly or the controls that fail on a recurring basis), analyze the reasons of these failures, and therefore look for ways to avoid those failures and improve the entity's processes and controls.

The BBCF will enhance L3's work in several ways. First, it will facilitate the internal auditors' evaluation of the internal control environment as the framework will pinpoint deficient processes and deficient controls. As such, the internal audit team will be able to focus on areas where the achievement of organizational objectives is at risk (loss of efficiency and/or effectiveness, deviation with internal policy or even laws, potential reporting errors) and provide Management and the BOD with best practices and recommendations for improvement. Second, L3 should be able to perform their reviews and audits more rapidly as information is readily available. Indeed, data is directly accessible by the internal auditors without asking information to L1, which increases L3 independence from Management. Moreover, the fact that the data is less likely to be lost when entered or aggregated within a common and comprehensive digital ledger increases the visibility and offers supplemental provenance evidence (audit trail). The traces also guarantee authenticity and immutability of audit evidence. The near real-time characteristic of the information should also help the auditor to timelier perform their work and assess whether recommendations have been put in place. All those attributes allow L3 to report up-to-date information to the BOD and Management on the adequacy and effectiveness of governance and risk management (including internal control).

We assume that to ease the access to the information and therefore increase the audit process efficiency while maintaining the auditors' independence, L4 would be granted read-only access to the framework. The external auditors would perform an IT audit of the BBCF to assess the reliability of the systems, including the blockchain platforms integrated within the framework, and determine whether they can rely on the information it provides. In that case, our framework would impact the overall audit approach. Indeed, as part of a risk-based financial audit, the auditors are required to obtain an understanding of the client's business environment and its internal control to assess the entity's audit risk (ISA 315). The auditors would be able to access the different processes saved into the BBCF and obtain several kinds of reports (e.g., summary of all controls performed, summary of all failed controls and possible remediation, summary of

all process deviations, L3 reports), which would allow the auditors to get an overview of the control environment and determine the risky areas. Based on that information, the auditors would determine the controls that need to be further investigated, assess the overall operating effectiveness of internal controls, and most probably reduce the amount of substantive work, which could be readily performed as all the transaction and their supportive documents would be saved onto the framework with an immutable trace, and directly accessible by the auditors.

D – Limitations and Risks

Even if blockchain represents a clear opportunity to rethink business processes and collaboration between organizations, there are still a number of issues to be addressed for this technology to become mature and sustainable.

First, as Hardjono and Maler point out, even if trust is naturally addressed by blockchain, there will always be levels where this will not be the case (Hardjono & Maler, 2017). These levels of trust include notably business trust, sociological trust and legal trust. Indeed, blockchain can be seen as a distributed platform where information is stored in a transparent way. At no time is the content analyzed, except through specific functions implemented by smart contracts, and which reflect business, societal or legal considerations.

Second, limitations also exist in a pure technical point of view. These limitations come from the fact that the technology is still new and therefore unstable, but also from the complex nature of the components it includes. Swan defines at least seven of such technical issues, even if there are probably more (Swan, 2015).

On top of these technical limitations, the lack of standards and regulation add real uncertainty for companies as to the viability of including blockchain within there is. This is especially true for audit and control professions (Boillet, 2017).

Finally, it should be noted that these problems have a perverse effect, since they all lead to additional issues. Indeed, because blockchain is a new, complex and still unstable technology, there is a lack of understanding of its foundations, a lack of political will for its legal framework and a reluctance to consider any reform of existing business processes (Hileman & Rauchs, 2017).

To address all these risks, one solution could be the establishment of a framework for risk and requirements management, as proposed by Drljevic et al. (Drljevic et al., 2020).

All those points translate into several risks within our framework, one of them being the possibility of using smart contracts within the Level III of BBCF' deployment. Indeed, the design and implementation of smart contracts represent a risk. As they are immutable programs, if they contain an error and start to produce undesirable or wrong output, there is no way back. Therefore, it is crucial to ensure that a smart contract does what it is intended to do the way it is intended to before implementing it. One might consider having such smart contracts being audited prior to their inclusion on the blockchain to reduce such risk.

It is also important to note that although a number of security elements are enforced, it is essential to have a set of controls and measures in place to ensure the ongoing integrity of the platform and its modules. A controlled, monitored and restricted access environment provides greater confidence in the operations performed and the results produced for audit and control

purposes. This is even more important in an environment where blockchain is used to share data with stakeholders outside of the company such as suppliers and customers.

In essence, this exploratory research has been motivated by the desire to propose a first solution to the business. The BBCF is composed of basic bricks that can be extended in terms of resources, modules, functionalities, rules, and connectors. The integration of the BBCF will require organizations to (re)define where their data are and how the different bricks relate to their information system. It is currently assumed that Track & Trace and Monitoring & Notification modules work properly in terms of linking with the existing information system, and that organizations would be willing to increase their level of confidence in their internal control system, and by rebound easing the work of auditors. However, potentially, a systemic risk could be for the audit and control practice to fully reject the use of blockchain technology.

5 Conclusion

The BBCF provides innovation both in its conceptual model design and its implementation. It reinforces the organizational structure and governance of an organization, strengthens its control environment and eases the audit practice, be it internal or external. We can even imagine that regulators could be part of this framework. We believe that ultimately this framework could be extended to include all relevant stakeholders that have an interest in corporate governance and control activities. One force of the BBCF is that it can be applied within any company at any stage of its development, as it offers modularity and scalability, both in the deployment of its functionalities and the extent of the use of blockchain platforms. The evaluation of the POC will provide more concrete and precise insight about the impact of BBCF – particularly in terms of potential effectiveness and transparency gains – but also its limitations – probably related to technical constraints related to the different blockchain platforms used. One limitation of our work would probably be related to the fact that the BBCF may not be adopted and implemented by our business partners as such and will require further applied research to have it run live in companies.

One potential outcome would be to redefine the scope and boundaries of some of the activities in audit and control practices from a more static to a more dynamic and prospective role. For example, external auditors may perform more real time audits and thus become partners in the business design / process re-engineering and decisions related to audit and control. In addition, the control patterns enabled by blockchain may contribute to both redesign processes and offer a greater level of confidence in control execution.

In a larger context of improving governance practices, including promoting transparency and ensuring the smooth and continuous circulation of information, the BBCF could set the path for a more inclusive and participative interaction between the different governance actors of an organization. The three lines of defense, the BOD, the external auditors and the regulator could access the same information about control activities, reports and even specific balance score cards that could be derived from the results of these control activities. Beyond internal control reinforcement, the framework could institute a different governance structure, in which the actors are more connected, thus increasing the proximity of the BOD with the first and second lines of defense compared to current structures where the BOD has more contact with

executive management, in particular the CEO, the internal audit and external audit functions. This new kind of governance may reflect back to the blockchain foundations and philosophy.

Appendix A – COSO Definition

The definitions below are provided by COSO Internal Control - Integrated Framework (2013).

(1) **Control environment** – is a set of standards, processes and structures providing the basis for carrying out internal control across an organization.

(2) **Risk assessment** – is the basis to determine how risk will be managed.

(3) **Control activities** – represent the actions established through policies and procedures to mitigate risks. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations and business performance reviews. Segregation of duties is typically built into the selection and development of control activities.

(4) **Information and communication** – Internal communication is the means by which information necessary to carry out internal control responsibilities is disseminated throughout the organization, flowing up, down, and across the entity. External communication is twofold: it enables inbound communication of relevant external information and it provides information to external parties in response to requirements and expectations.

(5) **Monitoring** – represents the evaluations to ascertain whether each of the five components of internal control is present and functioning.

Appendix B – List of Internal Control Activities

Control Activity	Definition
Authorization	Authorization is the power granted to an employee to perform a task. It is a delegation of duties. Control activities in this category are designed to provide reasonable assurance that all transactions are within the limits set by policy to ensure the activity of the department is consistent with the entity's goals and objectives.
Approval	Approval is the formal confirmation or sanction of employee decisions, events or transactions, based on an independent review. It signifies that the approver has formally reviewed the supporting documentation and is satisfied the transaction is accurate and complies with applicable laws and regulations. Approvals are usually represented by a signature.
Performance Planning	Control activities in this category establish key performance indicators which will be used in the evaluation control.
Evaluation	Control activities in this category compare projected data with actual data to evaluate and understand the difference and decide whether further investigation and/or corrective actions are needed.
Review	Control activities in this category are designed to provide reasonable assurance that transactions have been reviewed for accuracy and completeness by a person different from the preparer.
Reconciliation	Control activities in this category are designed to provide reasonable assurance of the accuracy, validity and consistency of records (mostly financial) through periodic comparison of: - items from different systems or records, - source documents with data recorded in accounting information systems. Reconciliation also involves resolving any discrepancies that may have been discovered and ensuring that unauthorized changes have not occurred to transactions during their processing.
Segregation of Duties (SOD)	Control activities in this category require that more than one person be involved in completing a particular process so that an employee provides independent examination on the other person's performance. Therefore no one is in a position where s/he could both perpetuate and hide fraudulent activities through the manipulation of accounting records. There should be a separation of duties and responsibilities for initiating, authorizing, recording, reconciling and reviewing transactions and maintaining custody over records (Larry & Bradley, 1997).
Physical Controls over Assets	Control activities in this category are designed to provide reasonable assurance that assets are safeguarded and protected from loss or damage due to accident, natural disaster, negligence or intentional acts of fraud, theft or abuse. These controls may impose restrictions on access to buildings, specified office or factory areas or equipment, such as turnstiles at the entrance to the premises. They also include physical restraints, such as fixing non-current assets to prevent removal, and regular counts.

Information Technology General Controls (ITGC)	They represent the foundation of the IT control structure (Romney and Steinbart, 2009). They apply to all systems components, processes and data present in an organization or system environment. The objectives of these controls are to ensure the appropriate development and implementation of the applications, as well as the integrity of program, data files and computer operations. They help ensure the reliability of data generated by IT systems and support the assertion that systems operate as intended and that output is reliable. They apply to all systems, components, processes and data for a given organization or information technology environment. The objectives of ITGCs are to ensure the proper development and implementation of applications, as well as the integrity of programs, data files, and computer operations.
Information Technology Application Controls (ITAC)	These controls prevent, discover and rectify transactional errors and fraud. They are concerned with certainty, completeness, validity and authorization of the data entered into the system, processed, stored, sent to other systems and reported (Agyapong, 2017).

Appendix C – Control Patterns

Table 2: Control patterns

Control #	Control type	Inputs	Actions	Outputs
1	Review	- Information - Reviewer ID - Authentication	- Review of information	- Signature of reviewer - Date - OK or NOT OK
2	Authorization	- Information (on activity/transaction) - Information (on the entity's policy) - SOD matrix - Reviewer ID - Authentication	- Compare activity/transaction with entity's policy and/or SOD matrix - Authorize activity/transaction	- Signature of reviewer - Date - OK or NOT OK
3	Approval	- Information (on transaction and laws/regulations) - Reviewer ID - Authentication	- Compare transaction with laws/regulation - Approve transaction	- Signature of reviewer - Date - OK or NOT OK
4	Performance Planning	- Documents (these documents include key performance indicators and ones necessary to establish the development plan – the "plan")	- Establish key performance indicators data (the "plan")	- Signatures of Management - Documents (with the "plan")

5	Evaluation	- Documents • The plan • Actual results for the key performance indicators or "Actual" • Variation threshold per key performance indicator.	- Compare "plan" to "actual" for each key performance indicator - Perform investigations (when variation is not within the authorized variation threshold)	- Signature of Reviewer - Document (evaluation) - Date - OK or NOT OK
6	Reconciliation	- Documents	- Compare referential value within several documents - Perform investigation and resolve issues (if there is no match)	- OK (if for all documents, referential values are found and similar) / NOT OK (for at least one document, one or more Referential values differ)
7	Segregation of Duties (SOD)	This control is represented by the SOD matrix. This internal control translates into 3 sub-controls described in rows 7a, 7b and 7c.		
7a	Verification of initiator and approver for a transaction/event	- Document (containing information on transaction/event) - Initiator - Approver - SOD matrix	- Compare initiator and approver with SOD matrix	- OK/NOT OK
7b	Access control	- Person - SOD matrix - Action (read, write, execute) - Resource	- Compare SOD, people access request and resource to ensure that the person has the right to perform the action on the resource based on SOD matrix	- GRANT/DENY

7c	Access Review	- Log (containing person, resource and action performed) - SOD matrix	- Compare log with SOD matrix	- OK/NOT OK
8	Physical Control over Assets	This internal control translates into 2 sub-controls described in rows 8a and 8b.		
8a	Physical access to assets	- Assets - Person - SOD Matrix	- Compare SOD, person access requests and assets to ensure the person is authorized to access the asset (building, cash, or any other physical assets)	- GRANT/DENY
8b	Physical surveillance over assets	- Assets	- Surveillance	- Document - File (e.g., video from camera surveillance)
9	IT General Controls	This translates into several sub-controls described in rows 9a, 9b, 9c, 9d, 9e and 9f.		
9a	Logical access controls over infrastructure, applications, and data	This is represented by the SOD matrix and the physical control over assets as described above.		
9b	System development life cycle controls	This translates into a process including several steps and several controls such as "Performance Planning", "Evaluation", "SOD", "Review", "Approval" and "Authorization". Therefore, these controls cannot become a single pattern.		

9c	Program change management controls	This translates into a process including several steps and several controls such as "Review", "Approval" and "Authorization". Therefore, these controls cannot become a single pattern.
9d	System and data backup and recovery controls	These are general controls which translate into back-up and recovery processes, both made of several steps. Therefore, they cannot become a single pattern.
9e	Computer operation controls	These general controls are made of input, process, and output computer controls, which cannot become a single pattern.
9f	Outsourced Service Providers	This type of controls translates into the ISAE 3402 report, which is an entire process by itself. As such, it cannot become a single pattern.
10	IT Application Control	This translates into several sub-controls such as completeness checks, validity checks, accuracy, identification, authentication, and authorization. As such, this type of control cannot translate into a single control pattern.

Table 3: Definitions of Inputs / Actions / Outputs

Inputs / Actions / Outputs		**Description**
Information	Document	Email, file or information stored in a database representing a payment, a journal entry, information contained in email, etc.
	Source	Document containing data used as referential values.
	Referential Value	Fields on document to be used as part of the control.
	Rule	Document materializing a rule (e.g., a list of documents to obtain to perform a reconciliation), a formula, a standard or a benchmark to comply with.
	Requirement	Specific type of rule: list of documents accepted or required to perform a control.
	Event	Data generated by a program following the completion of an action.
	Computation Input	Data used to perform a computation.
	Computation Results	Result being generated as an output of a given computation as part of the control.
	Formula	Mathematical formulas performed as part of a process.
	Proof	Document supporting a conclusion.
	Resource	IT applications.

	Non-Persistent Data	Data being generated by a program and subject to further processing before being persisted.
Action	Access	Access to information (read-only).
	Block	Refusal of access or change of information.
	Filter	Selection of a needed set of information.
	Compare	Comparison of information from different sources to ensure they are the same.
	Transfer	Information being sent from one actor to another.
	Update	Change of existing information with new one (read and write).
	Write (Establish)	Creation of information.
	Authorize	To formally review documents to ensure that the transaction is within the limits ($ value) set by policy.
	Approve	To formally review documents and to ensure that the transaction is accurate and complies with applicable laws and regulations.
	Sign	Sign a document physically or electronically.

Appendix D – Management Assertions

Assertion	Definition
Over transactions (sales, purchases, wages) for the period under audit	
Occurrence	The transactions and events that have been recorded or disclosed have occurred and such transactions and events pertain to the entity.
Completeness	All transactions that should have been recorded have been so and all related disclosures that should have been included in the financial statements have been included.
Accuracy	Amounts and other data relating to recorded transactions and events have been recorded appropriately and related disclosures have been appropriately measured and described.
Cut off	Transactions and events have been recorded in the correct accounting period.
Classification	Transactions and events have been recorded in the proper accounts.
Presentation	Transactions and events are appropriately aggregated or disaggregated and clearly described, and related disclosures are relevant and understandable in the context of the requirements of the applicable financial reporting framework.
Validity	All recorded transactions fairly represent the economic events that actually occurred, are lawful in nature and have been executed in accordance with management's general authorization.
Over account balances at the period end	
Existence	Assets, liabilities, and equity interests exist.
Rights & Obligations	The entity holds or controls the rights to assets and liabilities are the obligations of the entity.
Completeness	All assets, liabilities and equity interests that should have been recorded have been so and all related disclosures that should have been included in the financial statements have been included.
Accuracy / Valuation / Allocation	Assets, liabilities, and equity interests have been included in the financial statements at appropriate amounts. Any resulting valuation or allocation adjustments have been appropriately recorded and related disclosures have been appropriately measured and described.
Classification	Assets, liabilities, and equity interests have been recorded in the proper accounts.
Presentation	Assets, liabilities, and equity interests are appropriately aggregated or disaggregated and clearly described, and related disclosures are relevant and understandable in the context of the requirements of the applicable financial reporting framework.
Understandability	The information included in the financial statements has been appropriately presented and is clearly understandable.

Appendix E – Mapping

Control Activity	Management Assertions		COSO Objective
Reconciliation	Accuracy	Completeness	Financial Accuracy
	Occurrence	Cut-off	Fraud Deterrence
	Validity		
Authorization	Validity		Financial Accuracy
			Fraud Deterrence
Approval	Accuracy		Financial Accuracy
	Validity		Compliance
Review	Valuation	Cut-off	Financial Accuracy
	Accuracy	Classification	Fraud Deterrence
	Completeness	Understandability	Compliance
	Presentation	Rights & Obligations	
Performance Planning	Validity		Financial Accuracy
Evaluation	Valuation		Financial Accuracy
	Cut-off		Compliance
	Classification		
Segregation of Duties	Validity		Fraud Deterrence
Physical Control over Assets	Valuation	Cut-off	Financial Accuracy
	Existence		Fraud Deterrence
	Completeness		
Verification (confirmation / reperformance)	Valuation	Completeness	Financial Accuracy
	Existence	Accuracy	Fraud Deterrence
	Occurrence	Cut-off	
ITGC	Reliability		Financial Accuracy
	Integrity		Effectiveness
IT Application Controls	Completeness		Fraud Deterrence
	Validity		
	SOD		

Appendix F – Example of criteria defined in DLT selector

Criterion		Description
Enforcement	Date	Set of rules to compare the date when selection happens with reference dates. This criterion is useful only to select among multiple sets of criteria registered in database.
	Time	Set of rules to compare the time when selection happens with reference times. This criterion is useful only to select among multiple sets of criteria registered in database.
Platform	Instances	Selection of specific instances regardless of other provided rules
	Networks	Selection of instances of specific platforms regardless of other provided rules
Consensus	Algorithm	Algorithm used to establish consensus
	Type	Type of consensus amongst major categories of existing algorithms
	Energy-saving	Defines if the algorithm used for consensus requires huge energy consumption at network level
Contract	Support	Defines if the platform supports the use of smart contracts
	Completeness	This criterion focuses on platforms that use languages that allow Turing completeness
	Languages	List of one or more programming languages supported by a platform for smart contract development
Currency	Support	Defines if the platform uses a dedicated currency
Decentralization	Score	Describes how much the platform is decentralized (decentralization being defined following specified criteria)

Fees	Ranges	Set of ranges defining min and max values for fees being paid when a transaction is submitted on the network
	Category	Some predefined categories with specific min and max values can be specified
Finality	Delay	Delay observed between the submission of a transaction and its validation by the validators of the network
Governance	Type	Defines the governance used for the development of the network. Such governance can be managed by a commercial entity, a nonprofit organization or in a decentralized way.
	Open source	Such criterion defines if the development of the network is made open-source or not
Immutability	Type	Immutability within a platform can be definitive or probabilistic only
Lightnode	Support	Some platforms, especially public ones, can support light nodes where only part of the blockchain is hosted by the participants
Maturity	Score	Describes how much the platform is mature with respect to a set of defined criteria
Performance	Throughput	Defines a range of min and/or max transactions validated per second by the network
	Category	As per the fees, throughput can also be specified by using a set of predefined categories
Platform	Type	Specifies if the platform should be public or permissioned
Privacy	Participants	Defines if some enhanced measures are used within the platform to protect the identity of the participants
	Transactions	Same as for the participants, but here, we target the confidentiality of the transactions submitted
Scalability	Level	Defines if scalability should be minimal or well addressed

Security	Quantum-resistant	Defines if algorithms used for cryptographic operations are quantum-resistant or not
	Fault-tolerance	Defines the required percentage of honest validators to avoid double spending and other attacks
Tokenization	Support	Specifies if the platform supports the creation of tokens

NOTE: Each criterion is composed of a value, this value being specific to the criterion, and a weight, the weight being a number between 1 and 5 (1 when criterion denotes an undesired property, 5 when criterion denotes a required property). Also, multiple entries can be specified for a given criterion.

Appendix G – Description of the Main Activities of the Framework

Activity	Description	Inputs/Outputs	Modules involved & Main operations executed
Framework Initialization (FI)	Parameterization operations of the platform and all its modules for later use	INPUTS Configuration (authentication rules, notification rules, control patterns, etc.) OUTPUTS Platform configured	API (service call) + All modules being configured (configuration is made depending on provided parameters)
Process Initialization (PI)	Registration of a new process	INPUTS Process ID, process model OUTPUTS OK (success) / NOT OK (failure)	API (service call)
		INPUTS Process ID, process model OUTPUTS Dependence tree, signature	TRACK & TRACE - Verification of the conformity of submitted model and definition of dependencies between tasks (dependence tree) - Signature of provided data to ensure integrity
		INPUTS Process ID, signature	BLOCKCHAIN - Creation of a new trace containing signature data

		OUTPUTS OK (success) / NOT OK (failure)	
		INPUTS Process ID, process model, signature OUTPUTS OK (success) / NOT OK (failure)	CUSTODIAN - Storage of data related to process version within the custodian
Instance Initialization (II)	Registration of a new execution instance tied to a registered process to follow up the registration of traces representing executed tasks	INPUTS Instance ID, process ID, data (if any) OUTPUTS OK (success) / NOT OK (failure)	API (service call)
		INPUTS Instance ID, process ID, data (if any) OUTPUTS Instance ID, signature, state, context	TRACK & TRACE - Retrieval of parent process - Verification of its signature to assert integrity - Signature for the provided data of instance to ensure integrity - Initialization of the context to allow future registration of traces
		INPUTS Instance ID, signature OUTPUTS OK (success) / NOT OK (failure)	BLOCKCHAIN - Creation of a new trace containing signature data
		INPUTS Instance ID, signature, state, context	CUSTODIAN - Storage of data related to instance within

		OUTPUTS OK (success) / NOT OK (failure)	the custodian
Trace Registration (TR)	Registration of a trace related to the execution of a task or a control within an execution instance of a process. NOTE: Only pre-selected key tasks and controls can be subject to trace registration.	INPUTS Instance ID, task ID (relative to the process model), business data or control results (if any) OUTPUTS OK (success) / NOT OK (failure)	API (service call)
		INPUTS Instance ID, task ID OUTPUTS Context updated, trace (if OK) / NOT OK (error)	TRACK & TRACE - Retrieval of the instance from the custodian. - Retrieval of the information for the process related to the instance (model, signature, etc.). - Verification of the signatures of both the instance and the parent process to ensure that no violation of integrity occurred. - Verification of the context of instance with respect to the dependence tree of the process model. - If task is a control, verification of conditions associated to it. There are four possible outcomes for the last two operations:

			1. violation of integrity (the task cannot be registered according to the dependence tree and based on the current state of the execution instance) 2. deviation created or already existing 3. task is a control that does not violate the integrity of the instance, but its conditions are not met 4. trace corresponds to a task that can be executed without violating integrity and local conditions provided (if task is a control) The instance is updated only in the second (if deviation is authorized) and the last cases, as progress is made. In any case, a trace is registered for audit purposes (this trace specifies a violation of integrity in case 1, a failure of verification of the provided conditions in case 3, and an authorized update in cases 2 and 4).
		INPUTS Trace (reflecting the outcome of the analysis of context with respect to the dependence tree) OUTPUTS OK (success) / NOT OK (failure)	BLOCKCHAIN - Creation of a new trace containing the signature of the trace generated by TRACK & TRACE NOTE: This trace contains, amongst other things, the hash of multiple information such as the signature of the instance, the task identifier, a timestamp, a hash of the data provided during the API call, etc., to ensure no manipulation after its registration.

		INPUTS Context updated, trace generated OUTPUTS OK (success) / NOT OK (failure)	CUSTODIAN - Update of the context tied to the instance and the trace itself generated by TRACK & TRACE
Version Update (VU)	Registration of a new process version	OPERATIONS ARE SIMILAR TO THE ONES OF PROCESS INITIALIZATION Indeed, an update generates a whole new entry with its own set of execution instances, so that all previous versions can still be managed independently, and such that no alteration of recorded history is made.	
Process Deactivation (PD)	Deactivation of a process	INPUTS Process ID OUTPUTS OK (success) / NOT OK (failure)	API (service call)
		INPUTS Process ID OUTPUTS OK (success) / NOT OK (failure)	TRACK & TRACE - Retrieval of process and modification of its state to reflect its deactivation - Retrieval of all running execution instances and modification of their state to reflect their deactivation
		INPUTS Process ID, execution instance ID (for all instances that were running) OUTPUTS OK (success) / NOT OK (failure)	BLOCKCHAIN - For the process itself and all running execution instances that were still running, registration of a specific trace on blockchain to reflect the deactivation

		INPUTS Process ID, execution instance ID (for all instances that were running), traces (one per instance and one for the process itself) OUTPUTS OK (success) / NOT OK (failure)	CUSTODIAN - Registration of the generated traces by TRACK & TRACE - Update of the context itself for given instances - Update of the process entry
Instance Deactivation (ID)	Deactivation of an instance	OPERATIONS ARE SIMILAR TO THE ONES OF PROCESS DEACTIVATION In fact, when PD is called, for all running instances, ID is called as part of the whole execution. Here, deactivation means change of the state and context, and registration of a trace reflecting the deactivation.	
Control Execution (CE)	Execution of a control based on list of control patterns and outside any context handled by Track & Trace (i.e., outside a specific process)	INPUTS Control pattern ID, execution ID, data (depends on control pattern) OUTPUTS OK (success) / NOT OK (failure)	API (service call)
		INPUTS Control pattern ID, execution ID, data (depends on control pattern) OUTPUTS Trace	CONTROL MANAGER - Retrieval of execution rules needed for the execution of the control, if any - Execution of the control (the notion of execution here depends on the pattern) - Generation of a trace representing the result of execution (either success or failure)

		INPUTS Trace (reflecting the outcome of the execution of the control) OUTPUTS OK (success) / NOT OK (failure)	BLOCKCHAIN - Registration of the generated trace by CONTROL MANAGER
		INPUTS Control pattern ID, execution ID, data, trace OUTPUTS OK (success) / NOT OK (failure)	CUSTODIAN - Registration of the generated trace along with the other data tied to the control
Process Audit (PA)	Retrieval of data and/or trace related to a process for further audit	INPUTS Process ID AND/OR instance ID AND/OR trace ID OUTPUTS Data (depends on what is being retrieved)	API (service call)
		INPUTS Process ID AND/OR instance ID AND/OR trace ID OUTPUTS Data (depends on what is being retrieved)	TRACK & TRACE (as coordinator of specified operations) - Retrieval of the desired information from CUSTODIAN - Retrieval of the desired information from BLOCKCHAIN
Control Audit (CA)	Retrieval of data and/or trace related to a control execution for further audit	INPUTS (Control pattern ID AND/OR filters) OR Control execution ID	API (service call)

	NOTE: Here, controls being executed within a context tied to a process registered in Track & Trace are not concerned.	OUTPUTS Data (depends on what is being retrieved) NOTE: Filters allow to retrieve only specific control execution, e.g., only successful ones or executions that occurred before / after / between date(s).	
		INPUTS (Control pattern ID AND/OR filters) OR Control execution ID OUTPUTS Data (depends on what is being retrieved)	CONTROL MANAGER (as coordinator of specified operations) - Retrieval of all executed controls and execution of filters OR retrieval of specific control (if single execution set as input) - Retrieval of associated data from BLOCKCHAIN
Notification Rule Registration (NRR)	Registration of a new notification rule	INPUTS Notification rule OUTPUTS OK (success) / NOT OK (failure)	API (service call)
		INPUTS Notification rule OUTPUTS OK (success) / NOT OK (failure)	NOTIFICATION MANAGER - Verification of the rule (events, conditions and actions)

		INPUTS Notification rule OUTPUTS OK (success) / NOT OK (failure)	CUSTODIAN - Registration of the notification rule
Notification Rule Execution (NRE)	Execution of registered notification rules NOTE: NRE is executed for each activity, and at each stage. For the sake of brevity, the steps related to NRE are described only once.	INPUTS All notification rules OUTPUTS OK (success) / NOT OK (failure)	NOTIFICATION MANAGER - Verification of candidate rules (i.e., ones that match the event that occurred at each main operation executed) - Send to the module which generated the event the list of conditions, if any, to verify it (as each module is responsible of conditions tied to a rule related to an event it produces) - Execute the list of actions specified for all rules whose event matches the one generated and whose list of conditions is valid

References

Alexander, A. (2019). "Unlocking new potential: The various applications of blockchain mean this young technology will bring big opportunities to the accounting profession". *Accounting Today*, Vol. 33, Issue 12.

Appelbaum, D.A., Nehmer, R. (2017). Using drones in internal and external audits: An exploratory framework. *Journal of Emerging Technologies in Accounting 14(1)*. DOI: 10.2308/jeta-51704

Arndorfer, I., & Minto, A. (2015). Financial Stability Institute Occasional Paper No. 11, The "four lines of defence model" for financial institutions. Available at: http://www.bis.org/fsi/fsipapers11.pdf

Bank of England (2015). Fair and effective markets review. Available at: https://www.bankofengland.co.uk/report/2015/fair-and-effective-markets-review---final-report

Bantleon, U., D'Arcy, A., Eulerich, M., Hucke, A., Pedell, B., Ratzinger-Sakel, N. (2020). Coordination Challenge in implementing the three lines of defense model. *International Journal of Auditing 1-16.*

Beasly, M., Carcello, J., Hermanson, D. (2001). 10 audit deficiencies. Journal of Accountancy. Available at: https://www.journalofaccountancy.com/issues/2001/apr/top10auditdeficiencies.html

Boillet, J. (2017, August 17). Is audit ready for blockchain? *Accounting Today*. Available at: https://www.accountingtoday.com/opinion/is-audit-ready-for-blockchain

Carminati, B., Ferrari, E., & Rondanini, C. (2018). Blockchain as a Platform for Secure Inter-Organizational Business Processes. *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, 122–129. Available at: https://doi.org/10.1109/CIC.2018.00027

Carminati, B., Rondanini, C., & Ferrari, E. (2018). Confidential Business Process Execution on Blockchain. *2018 IEEE International Conference on Web Services (ICWS)*, 58–65. Available at: https://doi.org/10.1109/ICWS.2018.00015

Casino, F., Dasaklis, T.K., Patsakis, C. (2019). A systematic literature review of blockchain-based application: Current Status, classification, and open issues. *Telematics and Informatics, Vol. 36, pp.55-81.*

Committee of Sponsoring Organization of the Treadway Commission (2021). Available at: https://www.coso.org/Pages/default.aspx

Committee of Sponsoring Organization of the Treadway Commission (2020). Blockchain and internal control: the COSO perspective. Available at: https://www.coso.org/Documents/Blockchain-and-Internal-Control-The-COSO-Perspective-Guidance.pdf

Committee of Sponsoring Organization of the Treadway Commission (2017). Enterprise Risk Management, Integrating with Strategy and Performance. Available at: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

Committee of Sponsoring Organization of the Treadway Commission (2013). Internal Control Integrated Framework. Available at: https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf

Davies, H., Zhivitskaya,M. (2018). Three lines of defense: A robust organizing framework, or just lines in the sand? *Global Policy, Vol. 9, Supplement 1*.

Decaux, L., & Sarens, G. (2015). Implementing combined assurance: insights from multiple case studies. *Managerial Auditing Journal, 30, 56–79.*

Drljevic, N., Aranda, D. A., & Stantchev, V. (2020). Perspectives on risks and standards that affect the requirements engineering of blockchain technology. Computer Standards & Interfaces, 69, 103409. Available at: https://doi.org/10.1016/j.csi.2019.103409

DuPont, Q., Maurer, B. (2015). "Ledgers and law in the blockchain". *King's Review magazine*.

EY. (2013). Maximizing value from your lines of defense. A pragmatic approach to establishing and optimizing your LOD model. Insights on governance, risk and compliance.

Gamma, E., Helm, R., Johnson, R., Vlissides, J., (1995). Design patterns: Elements of reusable object-oriented software. Pearson Education, UK.

Geerts G (2011) A design science research methodology and its application to accounting information systems research, *International Journal of Accounting Information Systems.*

Giroux, G., Cassell, C. (2011). Changing audit risk characteristics in the public client market, *Research in Accounting Regulation, 23 (2) (2011), pp. 177-183.*

Hardjono, T., & Maler, E. (2017, June 5). *Kantara Initiative Releases First Blockchain Report Addressing Privacy Protection and Personal Data – Kantara Initiative*. Available at: https://kantarainitiative.org/kantara-initiative-releases-first-blockchain-report-addressing-privacy-protection-and-personal-data/

Hevner AR, March ST, Park J, Ram S. Design science in information systems research. *MIS Q 2004;28(1):75-105.*

Hileman, G., & Rauchs, M. (2017). *2017 Global Blockchain Benchmarking Study* (SSRN Scholarly Paper ID 3040224; Issue ID 3040224). Social Science Research Network. Available at: https://papers.ssrn.com/abstract=3040224

Institute of Chartered Accountants in England and Wales (ICAEW), (2015). Documenting and testing internal controls: issues that continue to challenge auditors. Available at: https://www.icaew.com/-/media/corporate/files/technical/iaa/documenting-and-testing-internal-controls---issues-that-continue-to-challenge-auditors.ashx?la=en

Institute of Internal Auditor (IIA), (2013). The three lines of defense in effective risk management and control. Position paper. Available at: https://global.theiia.org/standards-guidance/recommended-guidance/Pages/The-Three-Lines-of-Defense-in-Effective-Risk-Management-and-Control.aspx

Institute of Internal Auditor (IIA), (2015). Leveraging COSO across the three lines of defense.

Institute of Internal Auditor (IIA), (2020). The IIA's three lines model. An update of the three lines of defense. Available at: https://na.theiia.org/about-ia/PublicDocuments/Three-Lines-Model-Updated.pdf

International Auditing and Assurance Standards Board, (2009). "ISA 315: Identifying and assessing the risks of material misstatement through understanding the entity and its environment."

Iredaleon, G., (2019) Introduction to permissioned blockchains. Available at: https://101blockchains.com/permissioned-blockchain/

Kacina, J., Harler, M., Rajnic, M. (2017). The blockchain for business. Available at: https://www.sophiatx.com/storage/web/SophiaTX_Whitepaper_v1.9.pdf

Klotz, M., (2015). Implementing Corporate Governance with the "Lines of Defense Model". Global Economy at the crossroads - Trends in the world economy (pp. 53-68), Chap. 4. *Szczecin University Press*.

KPMG. (2012). The Convergence Evolution: Global Survey into the Integration of Governance, Risk and Compliance, in cooperation with Economist Intelligence Unit, KPMG, Switzerland.

Kwakye, E. Agyapong (2017). Internal Control Activities as a Tool for Financial Management in the Public Sector: A Case Study of Ghana Post Company Limited *Journal for the Advancement of Developing Economies, 2017 Volume 6 Issue 1*, pp43-77, ISSN: 2161-8216

Larry, E.R., Bradley, J.S. (1997). Auditing; Concepts for changing environment, 2nd Ed. U.S.A. Harcourt Brace College Publishers.

Leech, T., Hanlon, C. (2016). Three lines of defense versus five lines of assurance: Elevating the role of the board and CEO in risk governance. T*he Handbook of Board Governance: A Comprehensive Guide for Public, Private and Not for Profit Board Members (pp.335-355).* DOI: 10.1002/9781119245445.ch17

López-Pintado, O., Dumas, M., García-Bañuelos, L., & Weber, I. (2019). Interpreted Execution of Business Process Models on Blockchain. *ArXiv:1906.01420 [Cs]*. Available at: http://arxiv.org/abs/1906.01420

López-Pintado, O., García-Bañuelos, L., Dumas, M., Weber, I., & Ponomarev, A. (2019). CATERPILLAR: A Business Process Execution Engine on the Ethereum Blockchain. *ArXiv:1808.03517 [Cs]*. Available at: http://arxiv.org/abs/1808.03517

Lu, Q., Xu, X., Liu, Y. (2018). Design Pattern as a service for blockchain applications. Conference paper DOI:10.1109/ICDMW.20178.00025

Luburic, R. (2017). Strengthening the Three Lines of Defence in Terms of More Efficient Operational Risk Management in Central Banks. *Journal of Central Banking Theory and Practice, 6, 29–53.*

Lyons, S., (2015). Enterprise risk management and the five lines of corporate defense. *The Journal of Enterprise Risk Management, Vol.1, Issue 1*.

Lyons, S. (2019). Oversight and the Five Lines of Corporate Defense. Corporate Defense and the Value Preservation Imperative: Bulletproof Your Corporate Defense Program, 1st Edition, CRC Press, An Auerbach Book, Taylor & Francis Group, ISBN 9781498742283, Available at SSRN: https://ssrn.com/abstract=3447760

MacManus, E. (2017). "The audit of the future". *EY financial services thought gallery*. Available at: https://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2017/04/Audit-of-the-Future-Accountancy-Ireland.pdf

March, ST., Smith, G. (1995) Design and natural science research on information technology. Decision Support Systems;15(4):251–66.

Marr, B. (2018). "The 5 big problems with blockchain everyone should be aware of." *Forbes*. Available at: https://www.forbes.com/sites/bernardmarr/2018/02/19/the-5-big-problems-with-blockchain-everyone-should-be-aware-of/

Martin, K., Sanders, E., Scalan, G. (2014). The potential impact of COSO internal control integrated framework revision on internal audit structured SOX work programs. *Research in Accounting Regulation*, 26 (1) (2014), pp. 110-117

Orcutt, M. (2019). "Once hailed as unhackable, blockchains are now getting hacked". MIT Technology Review. Available at: https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/

Peffers, K., Tuunanen, T., Rothenberger, MA., Chatterjee, S. (2008) A design science research methodology for information systems research. Journal of Management Information Systems;24(3):45–77.

Potter, P., Tuburen, M. (2016). The 3 lines of defense for risk management. *Risk Management, vol. 63, no. 5*.

Price, S. (2019). "Connecting the 'average' user: 'User Experience in Blockchain." *Medium*, Available at: https://medium.com/@Price_Steven/connecting-the-average-user-user-experience-in-blockchain-dad84d66c763

Roberts, M. (2017). "Utilizing blockchain in your development". *Qualcomm.* Available at: https://www.qualcomm.com/news/onq/2017/12/19 /utilizing-blockchain-your-development

Romney, M., Steinbart, P. (2009). Accounting information systems, 11th Ed. New Jersey, Pearson Prentice Hall.

Roussy, M., Rodrigue, M. (2018). Internal Audit: Is the 'Third Line of Defense' Effective as a Form of Governance? An Exploratory Study of the Impression Management Techniques Chief Audit Executives Use in Their Annual Accountability to the Audit Committee. *Journal of Business Ethics, 151, 853–869.*

Rozari, A.M., Thomas, C. (2019). Reengineering the Audit with Blockchain and Smart Contracts. *Journal of Emerging Technologies in Accounting (2019) 16 (1): 21–35.*

Sarens, G., Decaux, L., & Lenz, R. (2012). Combined assurance: Case studies on a holistic approach to organizational governance. Altamonte Springs/- Fl: The Institute of Internal Auditors Research Foundation.

Schatsky, D., Muraskin, C. (2015). "Beyond bitcoin, blockchain is coming to disrupt your industry". *Deloitte Insight*.

Schmitz, J., Leoni G. (2019). "Accounting and auditing at the time of blockchain technology: A research agenda". *Australian Accounting Review*, Vol. 29(89, 2).

Sedbrook, T., Newmark, RI. (2008) Automating REA policy level specifications with semantic web technologies. Journal of Information Systems;22(2):249–77.

Simon, H. (1969) The sciences of the artificial. Cambridge MA: MIT Press

Stratopoulos, T., Wang, V., Ye, J., (2020). Blockchain Technology Adoption. Available at SSRN: https://ssrn.com/abstract=3188470 or http://dx.doi.org/10.2V139/ssrn.3188470

Suk-Young Chwe, M. (2000). Communication and Coordination in Social Networks. T*he Review of Economic Studies, 67, 1–16.*

Swan, M. (2015). *Blockchain: Blueprint for a new economy* (First edition, First edition) [Computer software]. O'Reilly. Available at: http://shop.oreilly.com/product/0636920037040.do

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday, 2(9).* Available at: https://doi.org/10.5210/fm.v2i9.548

Udding, A. (2016). Three lines of defence: a panacea? Available at: https://axveco.com/three-lines-of-defence-a-panacea/

UK Parliament. (2013). Report of the Parliamentary Commission on Banking Standards. Volume I: Summary, and Conclusions and Recommendations, HL Paper 27-I HC 175-I, London.

Van Der Aalst, W., Van Hee, K., Van der Werf, J.M., Kumar, A., Verdonk, M. (2011) Conceptual model for online auditing. *Decision Support Systems* 50 (2011), pp. 636-647

Vincent, N.E., Skjellum, A., Medury, S., (2020). Blockchain architecture: A design that helps CPA firms leverage the technology. *International Journal of Accounting Information Systems 38.*

Vousinas, G.L. (2019). Beyond the three-lines-of-defense. The five lines of defense model for financial institutions. Available at:

https://www.academia.edu/41222014/Beyond_the_three_lines_of_defense_The_five_lines_of_defense_model_for_financial_institutions

Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A., & Mendling, J. (2016). Untrusted Business Process Monitoring and Execution Using Blockchain. In M. La Rosa, P. Loos, & O. Pastor (Eds.), *Business Process Management* (Vol. 9850, pp. 329–347). Springer International Publishing. Available at: https://doi.org/10.1007/978-3-319-45348-4_19

Xu, M., Chen, X., Kou, G. (2019). "A systematic review of blockchain". *Financial Innovation*, Vol 5, pp. 5-27. Available at: DOI: 10.1186/s40854-019-0147-z.

Zhang, P., White, J., Schmidt, D., Lenz, G. (2017). Applying software patterns to address interoperability in BC-based healthcare apps. Available at: https://arxiv.org/abs/1706.03700