Three lines model paradigm shift: a blockchain-based control framework

Nathalie Brender and Marion Gauthier
Department of Business Economics, Geneva School of Business Administration, HES-SO, University of Applied Sciences and Arts Western Switzerland, Carouge, Switzerland, and
Jean-Henry Morin and Arber Salihi
Institute of Information Service Science, University of Geneva, Geneva, Switzerland

Received 12 July 2022
Revised 24 January 2023
Accepted 20 April 2023

Abstract

Purpose – While the three lines model (TLM) provides an organizational structure to execute risk and control duties, research and practice show limitations in the model's implementation. These limitations result in governance issues. Such issues, together with control weaknesses, could be addressed by leveraging properties of distribution, transparency, and immutability of blockchain technology. To this end, in this paper the authors propose a conceptual control framework based on blockchain technology to augment control practice.

Design/methodology/approach – The design of the resulting blockchain-based control framework (BBCF) and its prototype, based on the design science research methodology (DSRM), is presented and discussed in terms of the potential impact in the context of the identified problems within the TLM.

Findings – One potential outcome of BBCF could 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. In a larger context of improving governance practices, the BBCF could set the path for a more inclusive and participatory interaction between the different governance actors of an organization.

Research limitations/implications – However, this assumes that blockchain is more widely adopted despite its complexity and rigidity.

Practical implications – BBCF covering both a conceptual model design and a reference implementation provides an innovation in audit and control. BBCF could include all relevant stakeholders who have an interest in corporate governance and control activities, including the regulators.

The authors acknowledge that this research was supported by the Swiss National Science Foundation (SNSF), Project #100018_172834. The authors also want to note that this work benefited from the helpful comments and suggestions from Prof. Jee-Hae Lim and the two anonymous reviewers from Hawaii Accounting Research Conference 2022 where the work was presented in January 2022.

Funding statement: This research was supported by the Swiss National Science Foundation (SNF), Project # 100018_172834.

Data availability statement: The Proof-of-Concept (POC) underlying code is available at https://github.com/asalihi/blockchain-abstraction-framework.

Ethics approval statement: All of the participants met and interviewed for our research project participated in our study in a free and consenting manner.

Conflict of interest disclosure: None of the four authors have any potential conflict of interest pertaining to this submission.

Journal of Applied Accounting Research
Vol. 25 No. 1, 2024
pp. 149-170
Emerald Publishing Limited
0967-5426
DOI 10.1108/JAAR-06-2022-0143

Originality/value – 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 Audit, Internal control, Lines of defense, Blockchain

Paper type Research paper

1. Introduction

In 2013, the Institute of Internal Auditors (IIA) proposed an enterprise risk management (ERM) oversight model called the three lines of defense model (TLDM) (IIA, 2013). This model provides organizations with a structure to execute risk management and control activities in a way that minimizes the likelihood of both operational risk gaps and significant control breakdowns. It has been widely adopted by organizations (Arndorfer and Minto, 2015; Lyons, 2015; Vousinas, 2019) and has become a required organizational model by banking regulators and the Basel Committee on Banking Supervision in regulated financial institutions (Arndorfer and Minto, 2015; Bantleon *et al.*, 2020).

In 2020, the IIA updated the TLDM, now called the Three Lines Model (TLM) to clarify the different types of relationships among the roles and lines, highlighting the need for communication, cooperation, and collaboration among the different activities to create and protect value for the shareholders (IIA, 2020). The model is graphically depicted in Figure 1.

(1) The **governing body (e.g., the board of directors)** is accountable for an organization's governance. It delegates responsibility and provides resources for management to achieve the objectives of the organization, and oversees it to ensure that the actions taken are aligned with shareholders' interests.

(2) **Management** is responsible for achieving an organization's objectives. It consists of the following:

- **The first line (L1)** owns and manages risks and controls. It focuses on delivering products or services to clients of the organization.

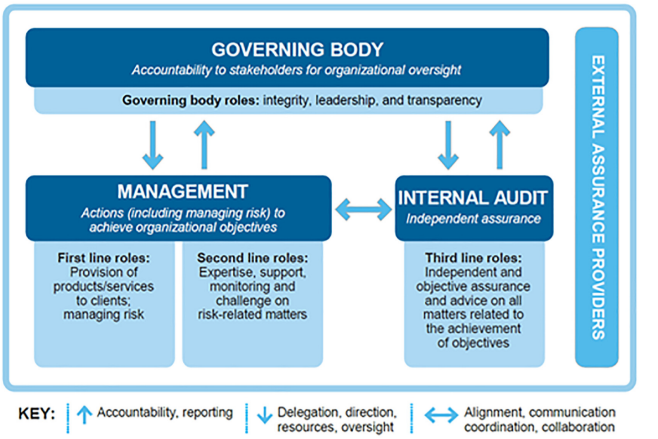


Figure 1.
The three lines model

Source(s): Figure 1 created by the IIA's Three Lines Model, July 2020

- **The second line (L2)** monitors risk and controls in support of management. It includes activities focused on risk-related matters such as compliance, internal control, management control, and IT security.

(3) **The third line (L3)** is the internal audit function. It monitors the effectiveness of the other lines, provides independent and objective assurance and advice on the adequacy of governance and risk management, including fraud risk. It communicates its findings to management and reports them to the governing body.

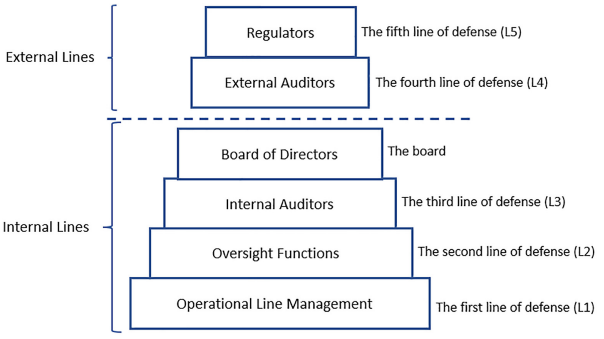
(4) **External Assurance Providers (L4)** are usually the external auditors (EA). They provide an independent assessment of the compliance with regulatory requirements. They are sometimes called the fourth line of defense (Arndorfer and Minto, 2015; Klotz, 2015; Vousinas, 2019).

Several researchers propose **regulators** as another line of defense, called the **fifth line (L5)**, especially in regulated industries such as banks and insurance (Arndorfer and Minto, 2015; Klotz, 2015; Vousinas, 2019).

Integrating all these elements, the TLM may be presented as follows (see Figure 2):

Even though research and practice show that the model is "simple, easy to communicate and understand" (IIA, 2013), its implementation may not be straightforward. It is common for investigations in large-scale corporate failure to identify problems within the implementation of the TLM in the organization(s) concerned as a significant contributing factor (Bantleon *et al.*, 2020; Lyons, 2019; Roussy and Rodrigue, 2018).

Based on the design science research methodology (DSRM) as defined by Vaishnavi and Kuechler (2015), in this paper we propose an approach supported by a conceptual framework [1] that leverages several features of blockchain technology [2] intended to strengthen the TLM. As presented in Table 1, DSRM consists of five phases for the design and evaluation of artifacts that can take the form of concepts, models, methods, and instantiations (Hevner *et al.*, 2004; March and Smith, 1995) intended to solve identified organizational problems (Hevner *et al.*, 2004). In the table, the arrows on the left represent iterations that are an important aspect of DSRM (Geerts, 2011). As Hevner *et al.* (2004) illustrate, evaluation provides feedback information on the designed artifact and a better understanding of the problem, leading to new iterations in the design process (Geerts, 2011). In our case, we organized regular meetings with a group of five experts based on their knowledge and strong interest in blockchain, risk management, and control activities: a financial audit director, an IT audit partner, a



Source(s): Figure 2 created by authors and inspired from the work of Lyons, 2015

Figure 2.
The five lines model

Principal Activities of DSR	Blockchain – Based Control Framework
Awareness of Problem	The Three Lines of Defense Model (TLDM) may not be properly implemented resulting in recurring problems accross organizations.
Suggestion	The objective is to see whether the characteristics of the blockchain technology can help avoiding the recurring problems arising from improper TLDM implemenation and ensure the proper implementation of the model.
Development	A framework combining blockchain technology with a business process conformance checker has been conceptualized, and developped under the form of a Proof-of-Concept (POC).
Evaluation	The Framework has been presented to 15 external auditors (working mainly for the Big 4, IT auditors and Financial auditors with different levels of responsibility, ranging from manager to partner), 11 Directors of internal audit departments of larger organizations (corporation or state-related), 3 internal audit Senior Managers, 1 Director of risks and internal control, and 7 innovation experts (Big 4) who were also presented with a semi- structured questionnaire. The analysis of the answers received is the basis for the evaluation of the conceptual model which fells into the descriptive method type as defined by Peffers et al. (2008). One of the Big 4 is also supporting us in identifying a relevant process (Product warranty and non-financial data reporting process) and a relevant company (SOX vs non-SOX) that would be willing to deploy the POC and test it live.
Conclusion	The results of the overall project will be shared with the scientific community to motivate future research and with the professional community (enterprises and external assurance providers) for potential adoption.

Table 1.
DSR activities

Source(s): Table created by author

blockchain specialist, a senior executive, and a legal specialist. We used their feedback to better understand the issues and consequently update the model. All of them had participated in a previous research project aimed at assessing blockchain's impact on the audit and control professions.

Pries-Heje *et al.* (2008) explain that in the context of socio-technical research, as it is the case here, the environment plays a determining role in the evaluation phase where a purely technical and rational evaluation would not grasp the human determination of the value of an artifact. Therefore, to evaluate the blockchain based control framework (BBCF), we presented it to 37 potential users mostly located in Switzerland, with three located in Europe. In each session, we presented BBCF and conducted semi-structured interviews to discuss each interviewee's observations on the solution and how it would impact their work if in use. We use this qualitative evaluation of BBCF in section 4 to discuss its potential benefits and limits.

The remainder of this paper is structured as follows. Section 2 presents blockchain. Section 3 describes the conceptual model and its objectives. Section 4 presents and discusses the evaluation of BBCF. In Section 5, we conclude the paper.

2. Blockchain technology

A blockchain is a decentralized architecture relying on a network of computers called nodes (Orcutt, 2019) to validate transactions for a unified ledger. How transactions are verified,

validated, and added to the ledger is based on a blockchain protocol that 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 (Zhang *et al.*, 2017).

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

(1) **Public** or **permissionless blockchain**, where everyone can transact and maintain the ledger according to the rules. It allows transactions between any party without the intervention of a centralized intermediary (Zhang *et al.*, 2017). Thus, Bitcoin functions as a secure peer-to-peer payment system (Rozario and Thomas, 2019).

(2) **Permissioned blockchain**, where participants must be granted access to be part of the network. In this architecture, a control layer runs on top of the blockchain and governs the actions performed by the allowed participants (Iredaleon, 2019). There are two subtypes of permissioned blockchains:

- **Private blockchain**, where participants are limited to one organization (e.g., Private Ethereum). For example, an enterprise can decide to use a private blockchain to secure settlement of cross-company transactions.
- A **consortium**, where participants are from multiple organizations. For example, Contour is a coalition of banks and companies whose goal is to reduce the time it takes to execute the entire process of a 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. Blockchain also allows the use of smart contracts – programs that execute code as soon as predefined conditions are met. Thus, smart contracts can help two or more parties to collaborate without intermediaries and make such a collaboration transparent, foolproof, and irreversible. In this regard, blockchain can help businesses design applications and conduct transactions that are simultaneously self-executing and autonomous (DuPont and Maurer, 2015). Thus, blockchain has gained the attention of companies that are launching pilot projects for business applications (Stratopoulos *et al.*, 2020) in sectors such as healthcare, supply chain management, market monitoring, smart energy, and copyright protection (Rozario and Thomas, 2019).

Specific to the audit and control community, blockchain can provide tamper-proof audit trails, an immutable ledger, and the opportunity to test full populations of transactions, possibly in real-time (Dai and Vasarhelyi, 2017; Zhang *et al.*, 2017). Thus, it has gained the attention of the Big 4 (Deloitte, EY, KPMG, PwC). Each of them has dedicated employees leading 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 audit and other control activities are performed. Some researchers even suggest that blockchain could replace audit functions (Pimentel and Boulianne, 2020; Dermirkan *et al.*, 2020). Other researchers and audit practitioners take a more critical look at the technology (Sargent, 2022) and point out that even if trust is naturally addressed by blockchain, there will always be levels where this will not be the case (Hardjono and Maler, 2017). These levels of trust include business, sociological, and legal. Blockchain can be seen as a distributed platform where information is stored in a transparent way; however, at no time is the content analyzed, except through specific functions implemented through smart contracts. Moreover, as with any new technology, blockchain is not immune to fraudulent entries and may be prone to malicious attack (Oladejo and Jack, 2020). Thus, on the one hand, in an open transaction environment

where information about the transactions is available to others, organizations might be tempted to put illusory or misleading data on a public chain to influence the behavior of other enterprises trying to gain business intelligence (O'Leary, 2017). On the other hand, even permissioned blockchains, where a central authority preselects trusted parties, can suffer from collusion between participants to report false transactions (Demirkan *et al.*, 2020; Dai *et al.*, 2017; Dai and Vasarhelyi, 2017; Kokina *et al.*, 2017; Sheldon, 2018). Indeed, transparency and visibility do not make transactions correct, authorized or complete (O'Leary, 2017; Sargent, 2022). Hamm (2018), a member of the Public Company Accounting Oversight Board, declared that "blockchain does not magically make information contained within it inherently trustworthy. Events recorded in the chain are not necessarily accurate and complete. Recording a transaction on a blockchain does not alleviate the risk that the transaction is unauthorized, fraudulent, or illegal (. . .)." Because blockchain consensus verification is not audit evidence (Sargent, 2022), and because blockchain technology cannot guarantee the correctness of source documents (Oladejo and Jack, 2020) companies still need to enact controls prior to what gets "on chain" (Sheldon, 2019; Kokina *et al.*, 2017; O'Leary, 2017) and auditors still need to bridge the digital and the physical world to ensure that transactions are correct, complete, and have economic substance.

On top of these challenges, other impediments exist to blockchain-wide adoption. Blockchain infrastructure has several technical problems that need to be addressed:

(1) Interoperability and compatibility issues with Enterprise Information Systems (EIS) (e.g., Enterprise Resources Planning (ERP)) (Kacina *et al.*, 2017).

(2) Scalability issues – a system's ability to operate properly under heavy loads – typically a larger size or volume (Rouse, 2006). As blockchain contains the full history of all transactions across all participants, its size continues to grow indefinitely (Lu *et al.*, 2018).

(3) Efficiency issues – because of its infrastructure design, the number of transactions transmitted, received, and validated over the network is small compared to other existing centralized infrastructures.

Notwithstanding these technical difficulties, blockchain offers interesting properties, as described above, that may facilitate the work of the different lines and provide increased levels of assurance for organizations to better keep risks under control and achieve increased maturity in governance.

3. Framework presentation

In this section, we first introduce BBCF, and then present a potential application by showing how a warranty process could run within the framework.

3.1 BBCF overview

Within BBCF, blockchain is used as a support for the internal control system. Its purpose is not to replace an existing Enterprise Information System (EIS) nor the internal control in place; instead, it provides an additional component that will support the current systems and practice in place. BBCF should be implemented to exist alongside and be interfaced with existing legacy and EIS. The main objectives of the framework are to:

(1) Monitor processes;

(2) Automatically and systematically record 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, and to provide easier access to the transaction underlying the evidence (potential audit trail);

(3) Provide a single and real-time view of process advancement and control results to the different lines, which should help in building stronger linkages and more robust engagement between lines, especially between the first and second lines;

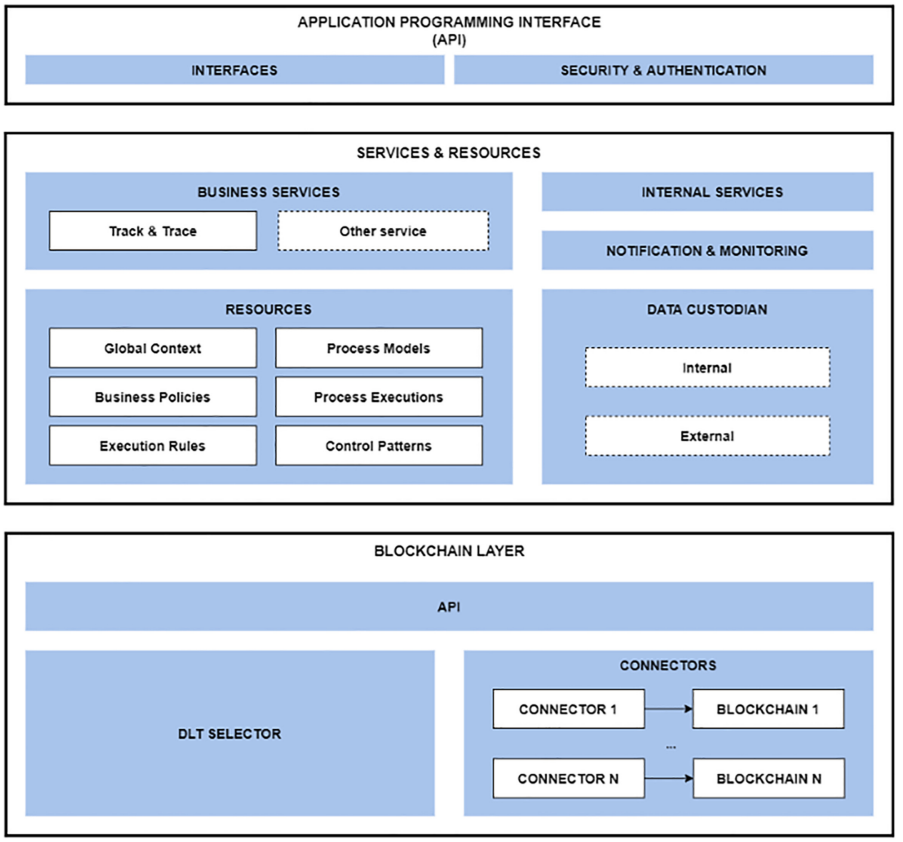
(4) Propose embedded controls on a blockchain in the form of smart contracts for those companies wishing to redesign or shift some of their processes and related controls;

(5) Notify process deviation or control failure for investigation and correction;

(6) Provide meaningful and timely reporting to the management and the board.

To fulfill these objectives, BBCF relies on the design graphically presented in Figure 3. Each component is described in Appendix 1 – BBCF Presentation.

BBCF consists of three layers. The top layer provides an interface to allow end users to interact with the framework services of the middle layer.



Source(s): Figure 3 created by authors

Figure 3.
BBCF overview

The middle layer exposes a set of services for business-oriented activities that need to rely on blockchain through the underlying abstraction layer. Two main services, "Track & Trace" and "Monitoring & Notification," are proposed and briefly described below.

The lower layer serves as a technology agnostic blockchain abstraction providing an interface to different blockchain-based platforms through connectors.

The two main services proposed by BBCF are "Track & Trace" (T&T), a conformance checker, and "Monitoring & Notification" (M&N), a notification service. T&T's goal is to verify integrity in the execution of registered processes, and the conditions associated with controls and standard tasks. M&N focusses on execution of actions and notifications. In practice, each time a process execution is subject to update, T&T:

(1) Proceeds to the update of the process execution state if both the integrity of the process and the conditions of controls are verified.

(2) Records a trace on a blockchain, whose content is the context related to process execution and the results of the verification (related to process integrity, control conditions as well as underlying evidence if needed).

(3) Informs the M&N service of the results of the operations carried out so that M&N can:

- Execute the appropriate actions specified for the control or standard task concerned with the update request. These actions can be executed either independently as the result of the checks, or in the case of success only, or in the case of problem only.
- Send automatic notification when a violation of the model has been detected or at least one condition has failed, independently of the actions entered when the process was created and handled in (a).
- If specified in the setup, stop the process so that no further steps can occur until a manual intervention is performed to correct the violation (e.g., for critical processes, super key controls, or when a key control does not have a compensating control).

To enforce strong integrity of operations and data, and thus to avoid scenarios involving malfunctions or fraud, T&T records traces on blockchain-based platforms when a process is created or deactivated, or when a process execution is activated, terminated, or canceled.

Ultimately, each trace can act as audit evidence because it allows the verification of the integrity of the original resources used to perform an update of a process execution or describe a process model or a process execution itself. In addition, thanks to audit traces registered by the BBCF itself, anyone can verify that there are as many traces reflecting the different service calls made to the API than traces reflecting the execution results of the aforesaid services. Thus, it is possible to verify the completeness of traces for processes, but also process executions and their progress. This could be particularly useful for L3 and L4 to spot issues and assess risky areas.

Depending on the company's governance, technology maturity levels, and its internal control requirements, BBCF can be deployed with an active or a passive use of service, and different levels of blockchain use. There are three predefined levels for the possible deployment of BBCF: Level I – passive use of both blockchain and services; Level II – passive use of blockchain and active use of services; and Level III – active use of both blockchain and services.

(1) Level I (Passive use of both blockchain and services): Trace only

In level I, T&T is used to save (a) provided data on a data custodian and (b) an associated trace containing the fingerprint of the data on a blockchain. It is also used to verify the

integrity of the data being stored on data custodians. An internal mapping between the stored data and the trace is registered within the platform to allow retrieval of both at any time. In general, the data would reflect the execution result of tasks performed either manually or within an IT system such as an ERP. In practice, this level ensures the integrity of stored information thanks to the traces recorded on a blockchain. Such information can later be used by appropriate parties to perform audit procedures. At the control level, the way BBCF works can be represented in the operation flow below (Figure 4).

(2) Level II (Passive use of blockchain, active use of services): Trace and Execution Rules

Within this level, controls are still performed off-chain. However, control data is provided to T&T to perform appropriate verifications. Such verifications include validation of process integrity and of control conditions or standard tasks that have been performed and for which progress should be recorded. At the control level, the way BBCF works can be represented in the high-level operation flow below (Figure 5).

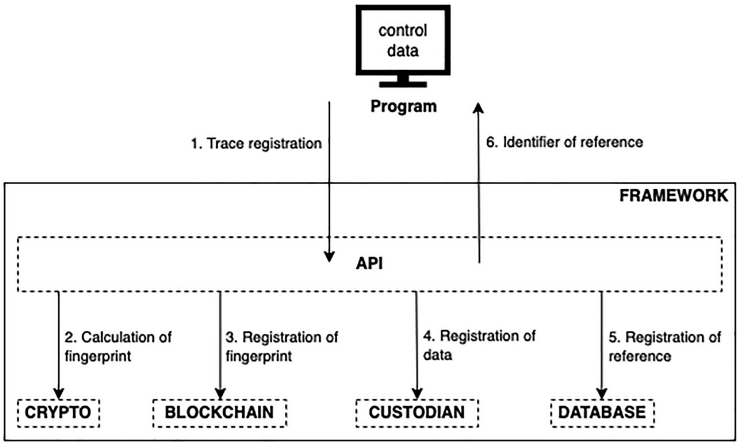
(3) Level III (Active use of both blockchain and services):Smart contracts

Here, controls are performed on-chain through the use of smart contracts. At the control level, the way BBCF works using smart contracts can be represented in the operation flow below (Figure 6).

BBCF can be deployed either within a single company where the different departments and even the different subsidiaries can share near real-time data and access them (i.e., for transfer pricing) or by a consortium where external parties involved in a given process share data. In the following section, we use the product warranty process where several companies are involved as a use case to illustrate how BBCF works.

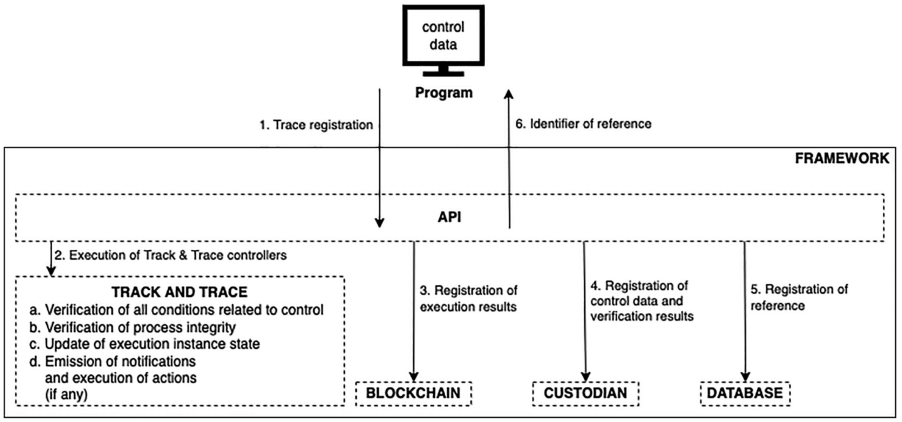
3.2 Use case – product warranty

We now present a hypothetical case where BBCF is deployed by a watch company to manage its warranty claim process. Claim processes usually exist in companies that produce goods and devices. It involves several participants:



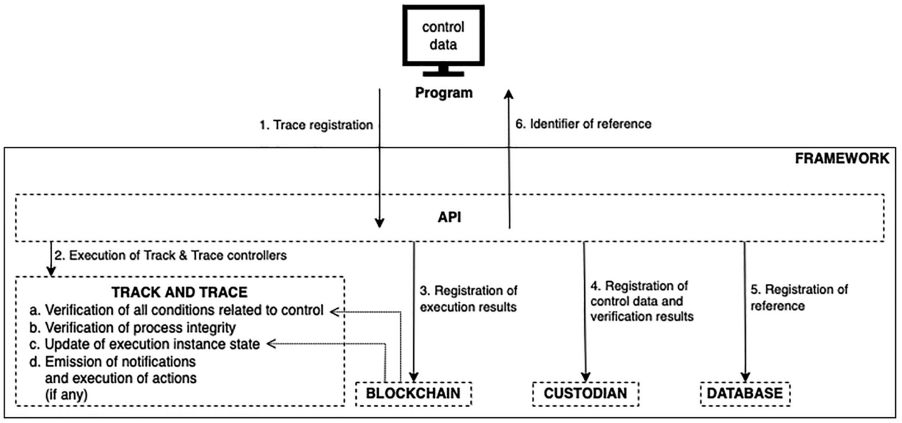
Source(s): Figure 4 created by authors

Figure 4.
BBCF deployment – Level I



Source(s): Figure 5 created by authors

Figure 5.
BBCF deployment -Level II



Source(s): Figure 6 created by authors

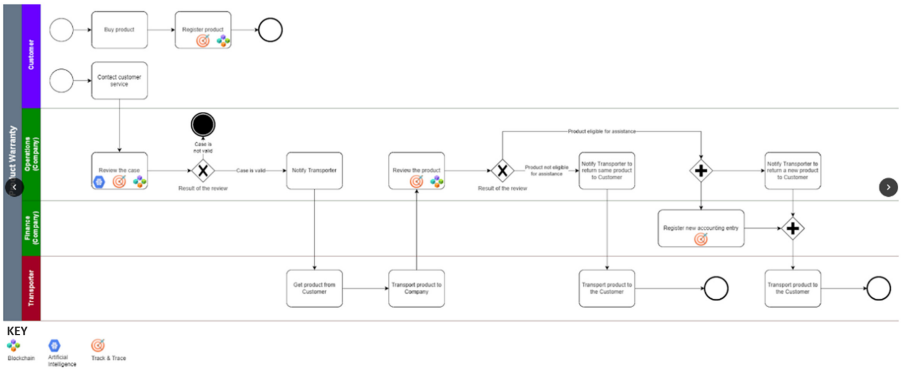
Figure 6.
BBCF deployment -Level III

(1) The manufacturer (in our case it owns BBCF), makes watches, issues, and manages the product warranty process (including repair, replacement, or reimbursement for a product). This process poses several issues: It is time consuming and costly as it implies both sharing information and coordinating with several internal departments – including production, warehousing, logistics, or finance – which can result in data entry errors, and sharing of information and coordination with external parties such as transporters, customers, etc. It is prone to fraudulent claims that can be authorized and result in additional charges for the manufacturers.

(2) The transporter, who collects products from clients and delivers repaired or new products.

(3) The customer.

The flowchart below shows how the warranty process would run within BBCF (Figure 7).



Source(s): Figure 7 created by authors

Figure 7.
Warranty process running through BBCF

In this case, the use of BBCF Level III – active use of both services and blockchain – would standardize and accelerate the process. As soon as the customer provides the required information online via a questionnaire, conditions set into the warranty contract and translated into a smart contract are verified. If they are met, the process is automatically executed (inform the transporter to collect the watch, ensure the availability of the parts to allow the repair, inform the repair/production department, book the accounting entry, inform finance, etc.). The automation of the process would reduce human intervention and therefore limit the risk of data error or data redundancy, increasing data accuracy. This would therefore provide shared trust in the data especially as they are immutable, transparent, and accessible to all the parties involved. It would also positively impact the different lines at the manufacturer level. L1 would keep track of the number of claims and their related costs on a real time basis. L2 would easily assess the data to evaluate the financial impact. L3 could more easily assess the effectiveness of the process as flaws would be automatically identified by T&T and reported in a timely way by M&N. L4 could easily verify the amount reported in the financial statements. Overall, the process of completion would be more efficient, and the different parties would have up-to-date and trustworthy information.

4. BBCF evaluation and discussion

The conceptual framework described in this paper combines the use of blockchain technology with a business process conformance checker to reinforce the organizational structure and governance, strengthen its control environment, and facilitate the audits performed by both internal and external auditors, and even regulators. To our knowledge, the use of blockchain coupled with a conformance checker has not yet been developed and published.

To evaluate BBCF, we met with thirty-seven potential users representing the different lines of defense. Twelve of them had participated in 2017–2018 in a research project whose aim was to assess blockchain's potential impact on the audit and control professions. For this study, we reached out to all interviewees, and twelve of them agreed to participate in the project. They provided us with the contacts of other professionals among whom ten agreed to be interviewed. To identify the fifteen remaining participants, we used social network media to find senior representatives of the different lines of defense working in organizations based in Switzerland. We note that even though we reached out to representatives of L1, none of them agreed to participate in our study due to lack of time, interest, or knowledge of blockchain.

Therefore, all the lines of defense were represented except the first line. This represents a limit of our study. The categorization of the interviewees among the different lines of defense is presented in Table 2, below.

Based on a standardized interview guide, we conducted semi-structured interviews that lasted one hour on average and were transcribed using handwritten notes. They were conducted either at the workplace of the interviewees or remotely using a videoconferencing software.

The interviews were conducted in two sequences. First, a member of the research team presented BBCF. Then, based on the interview guide, the researcher asked questions relating to three themes. The first theme focused on the interviewees' knowledge of blockchain and their experience with it. The second theme focused on the review and assessment of internal control systems, notably the audit performed by internal and external auditors. The third theme concerned the evaluation of BBCF and the interviewees' assessment on how it would impact their practice if in use.

We analyzed the data collected using the content analysis method. According to Evrard *et al.* (2003), it involves analyzing the content of an interview, which can be either non-directive or semi-directive (as in our case), using a set of techniques such as thematic analysis or syntactic and lexical analysis. Based on the notes taken during the interviews, we analyzed the data in two stages. The first stage consisted of a vertical analysis carried out within the interviews, and interview by interview, while the second stage consisted of a horizontal analysis of all the interviews theme by theme. This method allowed us to look for the meaning, relevance, and occurrence of themes from one interviewee to another. We analyzed the content of the interviews using a coding technique that divided the relevant content of the notes taken into different topic categories. Two members of the research team conducted the coding and discussed the results in accordance with the methods proposed by Strauss and Corbin (1998). The notes taken during the interviews were inductively coded to develop a list of categories per topic with descriptions. Then, the codes were compared to check and discuss their reliability. One of the authors made the necessary adjustments to the category list and codes and re-coded all interview notes based on the revised category list and coding manual. The following discussion presents the results of the analysis of the interviewees' evaluation of BBCF.

4.1 The positive impact of BBCF's

Several interviewees highlighted that one of BBCF's values is to provide one source of information. BBCF allows the assertion of process steps and control executions, and it allows all blockchain participants to retrieve information on an as-needed basis, including evidence of transaction and control details (results and supporting data) while having access to the audit trail.

Many interviewees also noted that as controls saved on blockchain are time-stamped and signed, it allows them, when cross-checked with the segregation of duties matrix, to quickly

Table 2. Categorization of interviewees

Categorization of interviewees	%
L1	0
L2	19
L3	33
L4 IT	30
L4 Financial	18
Total	100

Source(s): Table created by author

identify anomalies and deviations, and therefore to investigate them specifically to assess whether they are justified deviations or true exceptions. Thanks to this functionality, several interviewees think that some of the audit procedures should change. Thus, auditors should be able to focus on understanding the spotted deviations instead of performing random tests of details. Level II of deployment seems to be particularly interesting for most of the interviewees, who explained that this level provides more confidence in the reliability of the internal control system ("data are accurate and real"), as it can spot and report anomalies in a timely manner, or it can even stop processes from moving forward in case of a major violation of process execution or control execution rules. In this context, many interviewees think that auditors will have to do more IT general controls to assess whether the framework is reliable. They also expect that if BBCF works as intended, the number of tests of details should decrease.

Several EAs also reported that with the use of BBCF, they expect journal entry (JE) testing for detecting fraud to change significantly. Indeed, if the platform is reliable, and if BBCF is audited in the first year and then reviewed for changes year over year, the risk of fraud should decrease. Consequently, the auditors will be able to define more relevant tests to detect fraud rather than testing fifty JEs when thousands of them are registered during the year and when the parameters for selecting those JE, as explained by one financial audit manager, are not always relevant nor well understood by auditors. Many interviewed auditors expect that if their clients were to use BBCF, they would most probably move toward a continuous audit practice as they would be able to access reliable data at any time and from anywhere. Several of them speculated that some audit procedures will no longer be performed, leaving room for them to focus on higher value-added work where their professional judgment is required.

A few interviewees highlighted that the use of smart contracts is the ultimate control setup because, if properly coded, no deviation or exception is possible. Indeed, if the entity decides to use smart contracts (Level III of deployment) to execute controls, human intervention is minimized, which limits the risk of error and increases the reliability and security of the controls. In such a set-up, BBCF could become an element in a fraud prevention system where mechanisms are put in place to stop fraud or anomalies from occurring (Estévez *et al.*, 2006).

Some interviewees also noted that the immutability of the data is a real benefit of BBCF. Once saved onto a blockchain, information cannot be modified. Therefore, in the context of BBCF, once controls and processes are executed and a trace of those controls and processes have been saved onto a blockchain, auditors have the guarantee that no change has happened since their execution. The interviewees explained that getting irrefutable records from BBCF increases their confidence in the audited data. This finding confirms the results summarized in Sargent's structured literature review (2022) on blockchain within the audit environment.

Some interviewees think that BBCF will bring efficiency within the internal control system in several ways. First, T&T ensures process integrity by monitoring both the order of execution for the different steps and the performance of planned controls according to their execution rules. Any deviation is therefore reported on a real-time basis and can be corrected in a timelier way. Second, T&T helps to systemize processes and controls, increasing control efficiency. Lastly, the possibility of creating exception reports using near real-time data tailored to meet each line's specific needs as part of a dedicated value-added service increases the agility of the business environment.

Some interviewees also think that BBCF should bring efficiency to their work, which is aligned with what other researchers have reported (Sargent, 2022). Thus, some of them expect that in the first year of BBCF deployment the IT audit workload will increase as they will have to audit the whole architecture. However, in the following years, they expect a decrease of the overall workload as the IT auditors will only have to ensure that the platform has not changed, allowing the EAs to rely on the information it provides, which will ultimately decrease the number of tests of details performed.

As presented above, the interviewees expect several positive impacts from BBCF; however, they also pointed out several limitations as discussed below.

4.2 The limits of BBCF

Almost all interviewees reported that BBCF brings a high level of rigidity whereas systems, processes, and controls change quite often. We noted that, on the one hand, many EA are in favor of this rigidity. Indeed, it should systematize processes and controls and therefore facilitate their work while increasing the confidence in the data and the assurance they provide. On the other hand, almost all the internal auditors (IA) warned that, even though enforcing processes and controls can be appreciable for the "controllers" (L2, L3, L4), it is inefficient for the "doers" (L1) as their activity could potentially stop several times; one of BBCF's functionalities is to stop the process in case of a major violation until a manual intervention is performed to correct it. According to the IA interviewed, the L1 teams would suffer this rigidity, and it could even decrease the overall productivity of the business.

Many interviewees also highlighted the fact that BBCF requires a high level of maintenance because controls and processes must be documented and up to date. This raised two concerns: First, it seems that BBCF is suitable for larger organizations where most controls are already documented and automatic. Some interviewees even think that BBCF is best for companies in highly regulated industries – such as pharmaceuticals or companies that need to comply with the Sarbanes–Oxley law. Second, BBCF seems to be an expensive solution to maintain but also complex to integrate within the existing IT environment.

Furthermore, some participants emphasized that BBCF requires the implementation of additional sets of controls to address new risks. The data provided to BBCF or retrieved by one of the services proposed by the platform will have to be verified to ensure its integrity and validity. These additional controls are key, especially as the blockchain is not intended to validate the incoming data but to preserve its integrity once recorded. As expressed by some of the interviewees, IT auditors will need to assess the information systems that generate the flow of data drawing on BBCF. Some interviewees noted that although several 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 would provide greater confidence in the operations performed and the results obtained for audit and control purposes. This is even more important in an environment where blockchain is used to share data with stakeholders outside the company such as suppliers and customers. Drawing on this point, some interviewees pointed out that data management could be another type of issue as BBCF is intended to handle a large amount of data. Thus, they were concerned by the data sharing implied using blockchain technology especially when it is used as a consortium, and more particularly by the confidentiality of the data that would be saved onto a blockchain, which indeed seems to be a problem as shown by Wang *et al.* (2019). Some participants also pointed out that most companies want to provide their EAs only with the minimum necessary data that have been reviewed and internally validated beforehand; however, if granted access to BBCF, EAs could potentially access not only data that would not have been internally validated beforehand but also access the entire set of data. This last point, as a few interviewees explained, represents the risk that auditors find more anomalies. Their point is that if EAs were granted access to BBCF they could look at any kind of data and they would necessarily find more issues. Moreover, in this set-up the auditees would lose some controls over their data as they would not be able to restrict access by the auditors because, to perform their duty, auditors are supposed to have access to all information – books/records/minutes of meetings and requested information from officer – relevant to their audits.

In addition, a few interviewees pointed out that the possibility of using smart contracts represents a risk. They are immutable programs, so if they contain an error and start to

produce undesirable or wrong output, there is no way back. Therefore, it seems crucial to ensure that a smart contract does what it is intended to do before implementing it. In particular, the auditors mentioned that smart contracts should be audited prior to their inclusion on a blockchain to reduce such risk.

A few interviewees pointed out that the current functionalities of BBCF do not allow tracing a transaction to the financial statements. They asked whether such a reconciliation (from the control going through BBCF to the financial statements) would be possible as it would facilitate the completeness test and the fraud risk assessment. All transactions that go through BBCF should end up in a booking entry and therefore in the accounting balances, and it should be possible for all transactions making up the accounting balances to trace back to a trace of control saved onto a blockchain.

Based on the analysis of the interviewees' assessment of BBCF, we can also infer that the deployment of this framework would impact the TLM in several ways as described below.

4.3 BBCF's potential impacts on the TLM

The design and characteristics of BBCF should enforce a proper implementation of the TLM, allow a better distribution of the workload between the different lines of defense as reported by a few interviewees, and as such help to solve some of the problems identified within this model. Indeed, as the framework is based on blockchain, it inherently creates distributed trust within the different lines, allowing management to focus on building stronger linkages, and more robust engagement especially between the first and second lines (Hoefer *et al.*, 2020). Moreover, as the same data are accessible at any time by the different lines and as exceptions are automatically reported on a near real-time basis, it enables a "collaborative compliance" (Morin, 2014) where each line is aware of the inherent check mechanism. As a result, each line does what it is expected to do, which increases each line's accountability and motivation to perform its duties and facilitates coordination. In turn, this results in a more efficient internal control system with effective processes and proper reporting in place.

Furthermore, the combination of T&T and M&N modules support L1 in its duty of establishing and maintaining appropriate structures and processes for the management of operations and risks. However, it seems that, as highlighted by several interviewees, BBCF is not suitable for smaller organizations where most controls are manual. In such a context, L1 would have to log the controls manually and save the supporting documents into BBCF. This extra step could be cumbersome and, demotivating, and could be a source of errors. As such, BBCF deployment would most probably require some process reengineering to automatize controls, properly identify the controls and tasks that need to be recorded into a blockchain and properly identify the super key controls that would necessitate the process to be stopped when major anomalies or deviations are detected.

Using near real-time information on process flows and control results, L1 will be able to assess the organization's compliance with internal and external policies and laws, adjust operations in a timely way when necessary, and assess the processes' effectiveness. In addition, the fact that control owners, control doers, control reviewers, and process owners are clearly identified increases each employee's accountability, which in turn positively impacts the entity's processes and controls effectiveness. L1, L2, L3, and the BOD have access to the same data and to the same reports, which promotes transparency and deeper conversations on the entity's monitoring and strategy.

Furthermore, as BBCF provides near real-time information on operations' compliance with the entity's processes and on internal control outcomes (pass or fail), L2 can monitor and assess the adequacy and effectiveness of the risk mitigation practice within the organization more easily and in a more timely way. BBCF allows L2 to understand better where the failures are coming from – that is, 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. It also allows L2 to analyze the reasons for these failures, and therefore look for ways to avoid them and improve the entity's processes and controls.

BBCF enhances L3's work in several ways. First, it facilitates the IAs' evaluation of the internal control environment by pinpointing deficient processes and deficient controls. IAs can focus on areas where the achievement of organizational objectives is at risk – for example, a loss of efficiency and/or effectiveness, a deviation from internal policy or even laws, or potential reporting errors, and reduce random tests of details, and thus focus their efforts on providing management and the BOD with best practices and recommendations for improvement. Second, IAs can perform their reviews and audits more rapidly as information is readily available. Indeed, they can directly access the data without asking L1 for information, which increases their 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 visibility and offers evidence of provenance with an audit trail. The traces guarantee the authenticity and immutability of audit evidence. The near real-time characteristic of the information helps the auditor perform their work in a timelier way and to assess whether recommendations have been put in place. These attributes allow L3 to assume a central role in the risk management system which was already put forward by Vinnari and Skærbæk (2014) as with the use of BBCF they can 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 information and therefore increase the efficiency of the auditing process while maintaining the auditors' independence, EAs are granted read-only access to BBCF on a need-to-be basis.

Most of the EAs interviewed explained that the overall risk rating of a client using a blockchain based internal control system would rise significantly. In fact, blockchain is a new and complex technology for which there is no auditing protocol. As such, the deployment of BBCF would most probably increase the IT audit workload as the IT auditors would have to understand and audit it to assess the reliability of the systems (including both the interfaces connecting BBCF with existing systems, and the blockchains integrated within the framework) and determine whether they can rely on the information provided. BBCF would therefore impact the overall audit approach in several ways. First, as part of a risk-based financial audit, the auditors must obtain an understanding of the client's business environment and its internal control to assess the entity's audit risk (c.f. International Standard of Auditing 315), therefore, the audit team will need to include EAs who understand the blockchain and IT auditors who have the experience of auditing it. Second, as the auditors will be able to access the different processes saved into 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), they will quickly assess the overall operating effectiveness of the control environment, determine the risky areas, and identify controls that need to be investigated further. This should reduce the amount of substantive work performed by the EAs who will be able to focus their tests of details on risky accounts and transactions. Thus, BBCF would most probably decrease the amount of work performed by EAs, but increase the work performed by the IT auditors and increase temporarily the overall audit fees as the audit teams would require special skill sets.

5. Conclusion

In essence, this exploratory research has been motivated by the desire to propose a blockchain-based solution to strengthen companies' internal control systems. Covering both a conceptual model design and a reference implementation, BBCF provides an innovation for

auditing and control and thus fills a gap in the research literature by exploring how the blockchain technology itself could be used as an audit tool to find transactions that violate conditions and send notices of anomalies to auditors (Appelbaum and Nehmer, 2020) and to the other lines of defense.

BBCF consists of basic components that can be extended in terms of resources, modules, functionalities, rules, and connectors. Its aim is to reinforce the organizational structure and its governance, strengthen the control environment, and ease auditing practice, be it internal or external – even the regulator. Ultimately, BBCF could be extended to include all relevant stakeholders that have an interest in corporate governance and control activities. One major advantage of 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.

One potential outcome of using a blockchain-based internal control system may 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, EAs may perform more real-time audits and thus become partners in the business process re-engineering, and decisions related to audit and control. In the larger context of improving governance practices, including promoting transparency and ensuring the smooth and continuous circulation of information, blockchain-based internal control systems such as BBCF could set a path for a more inclusive and participative interaction between the different governance actors of an organization. The three lines of defense, the BOD, the EAs, and the regulator could all 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. 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 – as a private ledger only, within a consortium or as a publicly accessible ledger. Experts from the auditing and accounting fields suggest that such an approach could significantly contribute to the strengthening of internal control systems and facilitate auditing practice by positively impacting the work that the lines of defense perform. Beyond internal control reinforcement, BBCF could enable a different governance structure in which the actors are more connected. It may increase 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 and the functions of the internal and external auditors.

However, the integration of such a framework would require organizations to fundamentally change several practices that are well established to date. These organizations will have to (re)define their data management including redefining their accessibility and sharing while deploying an adequate level of protection. Moreover, with the current set-up of BBCF, we assume that the T&T and M&N modules work properly in terms of linking with the existing information system, and that organizations will be willing to increase their level of confidence in their internal control system, by rebound easing the work of auditors. We also assume that companies adopt blockchain, which promotes collaboration within and between organizations. However, it is possible that the business community and more particularly the audit and control practice fully reject the use of this technology.

There are still several issues that need to be addressed for blockchain to become mature and sustainable. First, because of its technical components (e.g., consensus algorithms and cryptography), blockchain is considered to be a complex technology which is hard to understand (Marr, 2018; Price, 2019) and therefore hard to use; However, it is crucial, including for the board, to understand how blockchain works to be able to evaluate, prepare for, and manage its impact on the organization, including the internal control system (COSO, 2020). Second, standards and regulations are still lacking, adding real uncertainty for companies as to the viability of including blockchain within existing EIS. Lastly, the use of

blockchain, because of its immutable character, implies a greater rigidity in transactions and their records, but this rigidity will only be accepted if the positive impacts of blockchain surpass it. Therefore, it seems that further empirical studies are necessary to better grasp the whole impact of the technology on organizations, and their readiness to deploy it.

Notes

1. The development of the framework and the related prototypes are part of a Swiss National Foundation (SNF) research grant anonymized for peer review.
2. In this article the terms "blockchain", "blockchain technology" and "distributed ledger technology" are used interchangeably.

References

Appelbaum, D. and Nehmer, R.A. (2020), "Auditing cloud-based blockchain accounting systems", *Information Systems Journal*, Vol. 34 No. 2, pp. 5-21, doi: 10.2308/isys-52660.

Arndorfer, I. and Minto, A. (2015), "Financial Stability Institute Occasional Paper No. 11, the 'four lines of defense model' for financial institutions", available at: http://www.bis.org/fsi/fsipapers11.pdf

Bantleon, U., d'Arcy, A., Eulerich, M., Hucke, A., Pedell, B. and Ratzinger-Sakel, N.V. (2020), "Coordination challenges in implementing the three lines of defense model", *International Journal of Auditing*, Vol. 25 No. 1, pp. 59-74.

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

Dai, J. and Vasarhelyi, M.A. (2017), "Toward blockchain-based accounting and assurance", *Journal of Information System*, Vol. 31 No. 3, pp. 5-21, doi: 10.2308/isys-51804.

Dai, J., Yunsen, W. and Vasarhelyi, M.A. (2017), "Blockchain: an emerging solution for fraud prevention", *CPA Journal*, Vol. 87, p. 12.

Demirkan, S., Demirkan, I. and McKee, A. (2020), "Blockchain technology in the future of business cyber security and accounting", *Journal of Managerial Analytics*, Vol. 7 No. 2, pp. 189-208, doi: 10.1080/23270012.2020.1731721.

DuPont, Q. and Maurer, B. (2015), *Ledgers and Law in the Blockchain*, King's Review, 23.

Estévez, P.A., Held, C.M. and Perez, C.A. (2006), "Subscription fraud prevention in telecommunications using fuzzy rules and neural networks", *Expert Systems with Applications*, Vol. 31 No. 2, pp. 337-344, doi: 10.1016/j.eswa.2005.09.028.

Evrard, Y., Pras, B. and Roux, E. (2003), *Market : Etudes et recherche en marketing*, 3rd ed., Dunod, Paris.

Geerts, G.L. (2011), "A design science research methodology and its application to accounting information systems research", *International Journal of Accounting Information Systems*, Vol. 12 No. 2, pp. 142-151.

Hamm, K.M. (2018), "Mexican mangos, diamonds, cargo shipping containers, Oh My! What auditors need to know about blockchain and other emerging technologies: a regulator's perspective", *Speech at the 43rd World Continuous Auditing & Reporting Symposium*.

Hardjono, T. and Maler, E. (2017), "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, A.R., March, S.T., Park, J. and Ram, S. (2004), "Design science in information systems research", *MIS Q*, Vol. 28 No. 1, pp. 75-105.

Hoefer, E., Cooke, M. and Curry, T. (2020), "Three lines of defense-Failed promises and what comes next, Financial Regulatory Forum, Reuters", available at: https://www.reuters.com/article/bc-finreg-risk-management-three-lines-of-idUSKBN25Z2FN

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) (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

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

Kacina, J., Harler, M. and 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'", *Trends in the World Economy*, Vol. 7, pp. 53-68.

Kokina, J., Mancha, R. and Pachamanova, D. (2017), "Blockchain: emergent industry adoption and implications for accounting", *Journal of Emerging Technologies in Accounting*, Vol. 14 No. 2, pp. 91-100, doi: 10.2308/jeta-51911.

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

Lyons, S. (2015), "Enterprise risk management and the five lines of corporate defense", *The Journal of Enterprise Risk Management*, Vol. 1 No. 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 ed., CRC Press, an Auerbach Book, Taylor & Francis Group, ISBN 9781498742283,SSRN, available at: https://ssrn.com/abstract=3447760

March, S.T. and Smith, G. (1995), "Design and natural science research on information technology", *Decision Support Systems*, Vol. 15 No. 4, pp. 251-266.

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/

Morin, J.H. (2014), La responsabilité numérique: Restaurer la confiance à l'aire du numérique. ISBN: 978-2-916571-78-2.

Oladejo, M.T. and Jack, L. (2020), "Fraud prevention and detection in a blockchain technology environment: challenges posed to forensic accountants", *International Journal of Economics and Accounting*, Vol. 9 No. 4, pp. 315-335.

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/

O'Leary, D.E. (2017), "Configuring blockchain architectures for transaction information in blockchain consortiums: the case of accounting and supply chain systems", *Intell Syst Account Finance Manage*, Vol. 24 No. 4, pp. 138-147, doi: 10.1002/isaf.1417.

Pimentel, E. and Boulianne, E. (2020), "Blockchain in accounting research and practice: current trends and future opportunities", *Accounting Perspectives*, Vol. 19 No. 4, p. 325, doi: 10.1111/1911-3838.12239.

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

Pries-Heje, J., Baskerville, R. and Venable, J.R. (2008), "Strategies for design science research evaluation", *ECIS 2008 Proceedings*, 87, available at: https://aisel.aisnet.org/ecis2008/87

Rouse, M. (2006), "Scalability definition", available at: https://searchdatacenter.techtarget.com/definition/scalability

Roussy, M. and 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*, Vol. 151, pp. 853-869.

Rozario, A.M. and Thomas, C. (2019), "Reengineering the audit with blockchain and smart contracts", *Journal of Emerging Technologies in Accounting*, Vol. 16 No. 1, pp. 21-35.

Sargent, C.S. (2022), "Replacing financial audits with blockchain: the verification issue", *Journal of Computer Information Systems*, Vol. 62 No. 6, pp. 1145-1153, 9p, doi: 10.1080/08874417.2021.1992805.

Sheldon, M.D. (2018), "Using blockchain to aggregate and share misconduct issues across the accounting profession", *Current Issues in Auditing*, Vol. 12 No. 2, pp. A27-A35, 1 September, doi: 10.2308/ciia-52184.

Sheldon, M.D. (2019), "A primer for information technology general control considerations on a private and permissioned blockchain audit", *Current Issues in Auditing*, Vol. 13 No. 1, pp. A15-A29, doi: 10.2308/ciia-52356.

Stratopoulos, T., Wang, V. and Ye, J. (2020), "Blockchain technology adoption", SSRN, available at: https://ssrn.com/abstract=3188470 or http://dx.doi.org/10.2V139/ssrn.3188470.

Strauss, A. and Corbin, J. (1998), *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, Sage Publications, Thousand Oaks, CA.

Vaishnavi, V.K. and Kuechler, W. (2015), *Design Science Research Methods and Patterns: Innovating Information and Communication Technology*, CRC Press.

Vinnari, E. and Skærbæk, P. (2014), "The uncertainties of risk management: a field study on risk management internal audit practices in a Finnish municipality", *Accounting, Auditing & Accountability Journal*, Vol. 27 No. 3, pp. 489-526, doi: 10.1108/AAAJ-09-2012-1106.

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

Wang, L., Shen, X., Li, J., Shao, J. and Yang, Y. (2019), "Cryptographic primitives in blockchains", *Journal of Network and Computer Applications*, Vol. 127, pp. 43-58, doi: 10.1016/j.jnca.2018.11.003.

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

Further reading

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

Appendix
BBCF Presentation

(1) The **Application Programming Interface (API)** is embedded in a dedicated layer that is responsible for exposing the various services and operations related to blockchain found in the underlying layers. Since the API represents the entry point for BBCF, it is essential that logic related to authentication and access control by end-users is implemented.

(2) **Services and resources** contain all the services exposed to end-users, as well as the internal operations that support the functioning of the platform, and the data related to them (i.e., Resources).

- **Resources** represent all the data generated and used by the services as part of the operations they execute. This module includes the following elements:

- **Global context** encompasses the meta parameters, structuring information, global variables for execution, and rules applying to the stakeholders (L1, L2, L3, the board, the EAs, the regulators, the entity's clients, and suppliers).

  - **Business policies** represent general guidelines set by top management that are part of the entity's control environment, that reflect the entity's objectives, and that define the responsibilities of each line of defense (and that therefore provide information used to set up BBCF).
  - **Execution rules** 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.
  - **Process models** include all running and deactivated processes managed by the T&T service. Each process includes all the different steps to be executed (either control or standard task) to fulfill a business scenario (e.g., financial reporting, couponing, etc.). It requires that the entity's processes and related risks be documented and up to date.
  - **Process execution** as a process can be executed several times a day or several times a year, it is possible to define different contexts related to specific execution instances of a given process version. These contexts gather multiple information such as the traces recorded on blockchain-based platforms as the tasks of the process are executed within the company's information system or manually by the employees.

- **Business services** present all the services that are exposed to end-users and to applications interacting with the framework. One implementation of such services is T&T, used to follow the execution of processes and controls. It is possible to extend the framework by adding more services.

  - **Track and trace (T&T)** is a conformance checker whose goal is to verify the integrity of the execution of registered processes, and the conditions associated with controls and standard tasks. In practice, T&T provides two levels of operation as described below. When the active mode of BBCF is used, T&T ensures process integrity by building a dependency tree representing the relations between steps of a given process and the overall order of such a process. Then, when a process execution should be updated, T&T uses the current state of the process execution, as well as the dependency tree, to verify whether progress is valid. As for the conditions associated with controls and standard tasks, T&T proceeds to the verification of each of them by calling internal functions responsible for the different categories of control conditions supported by BBCF.
  - **Monitoring and Notification (M&N)** is a notification service that can take the actions presented on pages 6 and 7 of this paper.

- **Internal services** represent those used by the platform to support its operations. These include services dedicated to authentication and security, as well as the management of settings.

- The **data custodian** oversees the safe custody, storage, and retrieval of data, especially ones described as resources. In practice, a data custodian can represent internal storage (in this case, BBCF itself acts as a custodian) or external storage managed by a third party (e.g., a cloud provider).

As some modules of BBCF allow the generation of traces registered on a blockchain, the framework includes a mapping table where each data stored on a data custodian is directly linked to its related trace published on the blockchain. Using such a table, one could thus retrieve all the necessary information to perform appropriate audits.

(3) The **Blockchain layer** serves as an abstraction interface to the different blockchains integrated within BBCF, using both a specific selector and connectors.

- The **DLT API** acts as a bridge between the whole layer and the upper parts of BBCF, and with its end-users. It redirects the calls to the DLT selector or the connectors accordingly.
- The **DLT selector** is a service allowing end-users to choose which blockchain to use for either submitting a transaction (e.g., recording a trace generated by T&T) or executing a smart contract. The selection of the most appropriate blockchain is made according to a set of technical and business rules reflecting the needs of the end-users and applications interacting with BBCF (e.g., data confidentiality, data accessibility, data management costs, performance, etc.).
- **Connectors** represent services acting as a bridge between the framework and blockchains. They translate operations defined by the framework (e.g., transaction submission or smart contract execution) to technical procedures specific to the network they represent. Any blockchain could be registered within BBCF as long as a specific connector is developed.

About the authors

Nathalie Brender, Associate Professor, holds a US CPA (Certified Public Accountant United States) and a PhD in risk governance of the Graduate Institute of International and Development Studies in Geneva. She teaches accounting, corporate finance, auditing, and risk management at the University of Applied Sciences Western Switzerland where she is also the Chair of the Business Economics Department and the former Director of the Certificate of Advanced Studies in Internal Audit. Previously, N. Brender was Senior Manager in internal and financial audit at Andersen and EY, and Financial Reporting Expert at STMicroelectronics. She is conducting research in the areas Blockchain impact on audit and control professions, and risk governance based on funding obtained from the Swiss National Science Foundation (SNSF). In 2014, she published a book entitled Global Risk Governance in Health. Nathalie Brender is the corresponding author and can be contacted at: nathalie.brender@hesge.ch

Marion Gauthier holds a US CPA (Certified Public Accountant United States) and a Master degree of Professional Accounting (MPAcc) from the University of Washington (USA). She works as a research fellow at the University of Applied Sciences Western Switzerland where she also taught a course on the International Financial Reporting Standards in 2016 and 2017. She previously worked as a Senior Internal Auditor at L'Occitane en Provence (Switzerland), Starbucks Coffee Company (US and the Netherlands), and as an External Auditor at Ernst and Young (US -Seattle).

Jean-Henry Morin, Associate Professor, DSI Visiting Research Fellow at University of Zurich, is Program Director of the Bachelor program in Information Systems and Services Science at the University of Geneva, CUI and an information security expert. Since 2014 he has been investigating blockchain technology and its relation to information security, rights and policy management with a particular interest on governance, risk and compliance. He currently supervises doctoral students doing research in the context of blockchain technology. He is the author of book on Digital Responsibility (Morin, 2014) and has published in international journals and conferences on security, Service Level Agreements (SLA), Internet of Things (IoT), Design Thinking, and Digital Rights Management.

Arber Salihi is a computer engineer graduated from INSA Lyon. He holds a PhD in Information Systems from the University of Geneva. Previously, he worked as a front-end developer for the Blue Brain Project (EPFL) and as a full stack developer at Bottomline Technologies.