A blockchain-based forensic model for financial crime investigation: the embezzlement scenario

Lamprini Zarpala1 · Fran Casino2,3

Received: 23 August 2020 / Accepted: 30 June 2021 / Published online: 15 July 2021
© The Author(s), under exclusive licence to Springer Nature Switzerland AG 2021

Abstract
The financial crime landscape is evolving along with the digitisation of financial services. Laws, regulations and forensic methodologies cannot efficiently cope with the growth pace of novel technologies, which translates into late adoption of measures and legal voids, providing a fruitful landscape for malicious actors. In this regard, the features offered by blockchain technology, such as immutability, verifiability, and authentication, enhance the robustness of financial forensics. This paper provides a taxonomy of the prevalent financial investigation techniques and a thorough state-of-the-art of blockchain-based digital forensic approaches. Moreover, we design and implement a forensic investigation framework based on standardised procedures and document the corresponding methodology for embezzlement scheme investigations. The feasibility and adaptability of our approach can be extended and embrace all types of fraud investigations and regular internal audits. We provide a functional Ethereum-based implementation, and we integrate standardised forensic flows and chain of custody preservation mechanisms. Finally, we discuss the challenges of the symbiotic relationship between blockchain and financial investigations, along with the managerial implication and future research directions.

Keywords Fraud detection · Blockchain · Chain of custody · Embezzlement · Digital forensics

JEL Classification K42 · K41 · M42 · G21

All authors equally contributed to this work.

Fran Casino
francasino@unipi.gr

Lamprini Zarpala
zarpala@unipi.gr

1 Department of Banking and Financial Management, Piraeus University, Piraeus, Greece
2 Department of Informatics, Piraeus University, Piraeus, Greece
3 Athena Research Center, Athens, Greece
1 Introduction

The impact of fraud and economic crime on all organizations worldwide still reaches high-record levels. The most frequently committed fraud scheme is asset misappropriation, where an employee is stealing or misusing organizational resources (Association of Certified Fraud Examiners 2020b). A provocative question arising when it comes to fighting fraud is about the deployed technologies during the investigation.

Data acquisition is one of the most critical steps during forensic investigations. This is interpreted as maintaining a chain of custody for data and performing data integrity validation to ensure tamper-proofness (Delena D. Spann 2014; Gottschalk and Gottschalk 2018). Advanced analytic techniques, such as machine learning, cognitive computing, and, in general, automated data processing methods, are some of the trends in forensics in the financial services sector.

In this work, we choose a real-world embezzlement scenario and apply the forensic-by-design architecture of blockchain to validate the audit trail’s integrity. To uncover embezzlement schemes, investigators have developed a hypothesis about the sequence of events and applied specific fraud analytic tools presented in Section 2.1. The results from the data forensics analysis and the other sources of documentation such as hard copies and CCTV tapes are stored in the audit trail, supporting the hypothesis in potential litigation proceedings (Association of Certified Fraud Examiners 2020a; Guide 2012; Delena D. Spann 2014).

The sequence of custody, control, transfer, and disposition of the audit trail of evidence is called chain of custody. The chain of custody indicates who had access to records and thus the degree of difficulty in manipulation. It assures that evidence is not damaged or altered in any way since gaps in the chain may illustrate mishandling of evidence which leads to damaging the case (Darrell D. Dorrell 2012). The importance of chain of custody is highlighted when the fraud investigator has to perform one of the most challenging tasks to put financial information in simple terms to be understandable from decision-makers (senior management, prosecutor, etc.). The collection, examination, analysis, interpretation, and presentation of digital evidence shapes investigations are crucial in proving embezzlement cases where digital evidence is prevalent because the employee under investigation may be well aware of the bank’s systems, procedures, and control gaps. In this regard, recent work in the digital forensic community has established reliable scientific methodologies and common standards in its workflows (Biasiotti et al. 2018; Gobler 2010). However, it still faces many challenges due to the volatile and malleable nature of the evidence and the continuous advances in technology that introduce new attack vectors (Huang et al. 2018; Casino et al. 2020).

In parallel to the digitization of financial services, blockchain technology (Nakamoto 2008) has experienced a wide adoption due to the myriad of possibilities and applications that it enables (Casino et al. 2019; Crosby et al. 2016). Setting aside

---

1 Financial forensics is a methodology which combines investigation and auditing skills to identify evidence for a potentially fraudulent activity that might end up in litigation. Fraudulent activities might derive either from within or outside the organization.

2 It is the misappropriation of funds that have been entrusted to an employee for care or management.
the different categorizations of blockchain in terms of applications and consensus algorithms (i.e. the methodology to reach an agreement between the different participants of the blockchain network to validate a transaction), they offer different features, such as auditability, security, decentralization and transparency (Xu et al. 2019; Casino et al. 2019). In addition, blockchains also provide immutability (Politou et al. 2019; Casino et al. 2020), which is an interesting feature, yet poses significant challenges to principles such as the right to be forgotten or the EU General Data Protection Regulation Directive (GDPR) (Politou et al. 2018).

Blockchain applications in the financial context are already a fact (Guo and Liang 2016; Peters and Panayi 2016; Casino et al. 2019). Nevertheless, blockchain capabilities can also be used maliciously to enable cryptocurrency fraud scams such as investment and Ponzi schemes, embezzlement, phishing, and ransomware (AICPA 2020). Therefore, investing efforts to prosecute fraud as well as its prevention in both traditional and next generation systems is mandatory. In this regard, the literature is still scarce in blockchain-based methods oriented to fraud prevention (Wolvertone and Lee 2019; Joshi et al. 2019). Promising research lines such as crypto de-anonymization methods have the potential to enable successful investigations and prosecutions (ShenTu and Yu 2015), yet such solutions have many constraints, as well as not being feasible in cryptocurrencies such as Monero.

Based on the above requirements, it is apparent that the blockchain features may enhance forensic procedures (Al-Khateeb et al. 2019). For instance, the immutability of blockchain can guarantee the verifiability of the chain of custody of evidences and provide an auditable trail of events. The latter is mandatory to be presented as a solid proof in a courtroom.

1.1 Motivation and contribution

The amount of cyber challenges faced by the financial sector requires cooperation between different entities and actors both at national and international levels. In this regard, several cybersecurity initiatives in the finance sector are being pushed by organizations such as ENISA (Naydenov and Theocharidou 2021) to establish a standard and fertile ground in such a critical sector. Therefore, the work presented in this paper contributes to reinforcing key dimensions such as information sharing and capacity building, awareness and training, standardization and certification, and research and innovation.

In this paper, we address the relevance of blockchain technology and its inherent features for the management of evidence in forensic investigations. We are concerned with a case study that occurs within a financial institution. This type of fraud is also known as bank fraud. According to the Basel Committee on Banking Supervision, there are different kinds of fraud: internal/occupational frauds or external frauds. In this context, we will examine occupation fraud as an embezzlement scheme for unauthorised withdrawals. The detection method used is a review of the source documentation that might confirm or refute the allegation of embezzlement. In addition, we provide a taxonomy of the financial investigation techniques, and comprehensive overview of the state of the art in blockchain forensics, and we
propose a blockchain-based architecture for embezzlement’ fraudulent activities enabling sound preservation of the chain of custody. This architecture and the forensic flows are implemented according to well-known standards and guidelines, such as the ones described in Section 3.3. Moreover, we provide an implementation based on Ethereum and smart contracts to preserve the chain of custody as well as the trail of events. Overall, our solution enables various features and benefits, such as integrity verification, tamper-proof, and future enhancement of similar investigations. Therefore, approaches such as the one proposed in this work aim to close the gap between the technicalities of financial investigations and legal procedures, enhancing the robustness of the current state of practice. In addition, we discuss several measures to improve the adaptability of our system towards similar crimes, and we provide a fertile ground for further research.

To the best of our knowledge, this is the first work that provides a blockchain-based forensic sound procedure for embezzlement and an implementation based on smart contracts. Even though we use the embezzlement scenario to illustrate the forensic procedure, our high-level architecture can be extended in all fraud investigations and also in regular internal audits.

2 Related works

2.1 Financial investigation techniques

We analysed the state of the art of financial investigation techniques and tools and leveraged a taxonomy of the different families of methods that can be used according to the elements and actors under investigation. Figure 1 provides an overview of the taxonomy and the most relevant techniques related to the effective design of fraud detection.

Fraud-related technical literature incorporates in the design of detective controls the importance of red flags for perpetrator’s behaviour, which can validate the predictive theory (Gullkvist and Jokipii 2013). In the embezzlement case, and in asset misappropriation in general, the detective controls rotate around employee’s financial status, consumption habits, egocentric behaviour analysis, performance evaluation, adherence to vacation policies, job dissatisfaction (Singleton and Singleton 2010).

To detect deviations and specific behaviour in documents and social networks (Yoo and Gretzel 2009), fraud investigators use techniques of sentiment analysis (Goel and Uzuner 2016) augmented with graph analysis (Pourhabibi et al. 2020) to discover the degree of connectivity between individuals. Graph analysis is also used to evaluate the performance of a small subset of transactions and to identify the accounts involved in a cross-channel transaction. The latter cannot be identified with classical statistical source-account profiling (Molloy et al. 2017).

The visual analysis category mainly refers to the graphical representation of numerical and categorical data, usually in form of diagrams or plots (e.g. bar, radial, box plots, heat maps), and 3D visualizations. This is a well-known approach for fraud detection used by investigators to speed up manual analysis of.
data since this approach enhances its readability (Leite et al. 2018). An essential aspect of visual analysis is the interaction of such systems, letting investigators select, explore, and filter the visualized data.

Statistical and data analytics are leveraged with an extensive set of techniques (Kobayashi et al. 2011; Bănărescu 2015) which aim to detect anomalies in data. These anomalies could indicate customers’ abnormal behavior (e.g. frequency and amount of regular transactions, changes in geography, and outlier detection) (Cliff and Wall-Parker 2017; Ngai et al. 2011).

Artificial intelligence is widely used in the finance field to detect fraud schemes such as embezzlement (Choi and Lee 2018; Awoyemi et al. 2017). One of the main approaches is leveraging pattern recognition by using machine learning techniques (both supervised and unsupervised) to classify data according to some criteria (e.g., identify multiple transactions at a customers’ account in quick succession) (Sadgali et al. 2019) and to predict the occurrence of fraud through the use of neural networks, Bayesian learning, decision trees and association rules (Cerullo and Cerullo 1999a, b). Similarly, clustering algorithms are used to explore how data are related and find further insights. Other approaches also
include rule-based expert systems and process mining models which can extract and detect further data patterns (Omair and Alturki 2020).

Finally, in parallel to the aforementioned techniques, text analysis is another relevant source of evidence. Due to the modus operandi of the malicious actors, the use of natural language processing to detect authorship of documents (De Vel et al. 2001; Green and Sheppard 2013), including the use of specific keywords to tag specific transactions or operations, can help in the detection of embezzlement (Markowitz and Hancock 2014). Moreover, automated systems to detect forged documents and signatures (Gideon et al. 2018) are critical in this context.

For our analysis, we reviewed prior researches related to embezzlement schemes from the finance-related literature. Nevertheless, the existing literature gives little attention to the embezzlement schemes performed within financial institutions. Embezzlement schemes are more likely to be realised in situations when either the separation of duties or the relevant audit trails are weak or nonexistent. One of the most common types of banking fraud is the unauthorized withdrawals from customer accounts (Association of Certified Fraud Examiners 2020a) and may take various forms. For instance, it could be stealing money from customers by providing encoded deposit slips (Manning 2011) or borrowing from today’s account’s receivable and replace them with tomorrow’s receipts. In all cases, a scheme to be successful requires the creation of false data, reports, or data entries (Bologna 1995). The aforementioned tools and techniques can be applied to detect embezzlement schemes. Yet, one of the main challenges in the financial sector is accommodating such solutions to each organization’s systems. Moreover, as stated in Section 1.1, there are several challenges in terms of interoperability, training, policies and regulations, and standardization, that prevent the creation of common frameworks to exploit the full potential of such techniques.

### 2.2 Blockchain forensics

Despite the suitability of blockchain towards preserving a trail of events in an immutable and verifiable manner, only recently authors have started to explore it.

To retrieve the relevant literature in blockchain, we queried the Scopus database by using the keywords “blockchain” and “forensics”, and we located further studies by means of the snowball effect (i.e. additional literature referenced by the articles found in the initial search). In total, 28 articles were selected according to a specific criteria (i.e. we peer-reviewed and excluded some papers based on their structural quality, language, and subject area). Next, we performed a keyword-based and topic classification, depicted in Fig. 2. Therefore, we identified eight different blockchain forensic application topics which span from 2018 to June 2020, being the most populated the ones related with data management, IoT, and cloud.

In the context of cloud forensics, a framework to enable fast incident response was proposed in Ricci et al. (2019). In Zhang et al. (2018), the authors created a collaboration and evidence management framework to improve the coordination of investigations when different stakeholders are involved. In the case of Rane and
Dixit (2019) and Duy et al. (2019), authors focused in logging-as-a-service tools for securely storing and processing logs while coping with issues of multi-stakeholder collusion, and the integrity and confidentiality of logs. In this context, security and robust access mechanisms are mandatory, as discussed in Pourvahab and Ekbatani-fard (2019).

The works classified in data management topic present different models for data processing based on scalable solutions such as permissioned blockchains (Gopalan et al. 2019; Lone and Mir 2019; Xiong and Du 2019) and blockchains using lightweight consensus mechanisms (Tian et al. 2019). Other relevant features showcased by authors are the verifiability of the trail of events (Weilbach and Motara 2019; Bonomi et al. 2020) and the classification of the evidence in terms of features, enabling further data processing (Billard 2018).

The evidence collected from IoT devices and the interactions between different stakeholders are one of the main features studied in the literature (Brotsis et al. 2019; Hossain et al. 2018; Ryu et al. 2019; Li et al. 2019). In addition, privacy-preserving identity management (Le et al. 2018) is a mandatory feature to be considered in such context.

The blockchain-based mobile forensic research focuses on applications and malware detection. In this regard, authors propose the use of consortium blockchains to detect malware and based on statistical analysis of each application’s feature (Gu et al. 2018; Homayoun et al. 2019).

The multimedia forensic topic includes works related with processing and storing CCTV video evidence (Kerr et al. 2018), the multimedia evidence captured by smartphones (Samanta and Jain 2018) and image-based provenance and integrity (Zou et al. 2019).

In the healthcare context, the work presented in Malamas et al. (2019) proposes a blockchain-enabled authorization framework for managing both the Internet of Medical Things (IoMT) devices and healthcare stakeholders. Smart grid forensics and its relevance is discussed in Kotsiuba et al. (2018). Moreover, the authors showcase the benefits of blockchain towards enhancing energy optimization, security and managerial tasks.

Transportation forensics has captured the interest of researchers due to its timely relevance due to its seamless relationship with emerging technologies such as self-driving automation, IoT-based sensing, and 5G communication networks (Patsakis et al. 2019). Nevertheless, such novel frameworks and the adoption of new data privacy frameworks (like the GDPR) call for the development of sound forensic mechanisms to analyze traffic accidents and protect users’ sensitive data. For instance, in Billard and Bartonolomei (2019), the author proposes a system to manage user’s requests and their compliance with legal frameworks.

A privacy-preserving framework is also proposed in Kevin and David (2019), this time for managing sensitive navigation data while ensuring user’s anonymity. In Cebe et al. (2018), the authors propose a blockchain-based forensics system that enables traceable and privacy-aware post-accident analysis with minimal requirements in storage and processing. In Patsakis et al. (2019) a blockchain-based framework is proposed for keeping logs of all hardware profile changes and updates in a vehicle.
Fig. 2 Summary of blockchain forensic topics and the number of publications per year.
Finally, we analysed the maturity of the literature according to their development stage in Table 1. In general, we may observe that the majority of solutions are in an early stage and thus, more efforts need to be devoted to this research field to exploit all the potential of blockchain. A more detailed exploration of the blockchain forensics literature can be found in Dasaklis et al. (2020).

2.3 Forensic models

Despite that one of the main issues in the digital forensics research field is the standardisation of procedures according to each topic or context (Garfinkel 2010), there exist several well-known forensic guidelines and models (Kyei et al. 2013; Kent et al. 2006; INTERPOL 2019), which are summarised in Table 2. Moreover, a review of the international development of forensic standards, such as ISO/IEC 27043:2015, can be found in Wilson-Wilde (2018) and Antwi-Boasiako and Venter (2017).

In general, the procedures summarised in Table 2 have a common hierarchical structure, which can be divided in the steps described in Table 3. Note that, evidence custody changes as well as evidence destruction are two relevant steps that, although not mapped in the high level description provided in Table 3, are included in our system implementation.

3 Methods

In the following sections, we will describe the case study and the actors involved, our blockchain-based forensic architecture, and the forensic methodology applied to such case.

3.1 A case study for an embezzlement scheme.

Let Malory be a malicious bank employee who worked at Golden Bank in Albany, Oregon for 15 years. In addition, Malory was promoted to the Head Teller position in the Central Branch 5 years ago. He was living beyond means; driving a expensive car and being the owner of an expensive home. As he was working for many years in the same branch, he had developed a good relationship with affluent clients of the branch that where living abroad.

Within such period, the Branch Manager received an oral complaint by the client Alice, who was contesting the balance recorded in the passbook of his saving account. The Branch Manager tried to trail the vouchers of his last transactions but were missing from the physical record. The responsibility of the missing vouchers lied to Malory. The Branch manager, informed the Internal Audit Department of the bank to investigate the case.

The investigation’s result was that Malory had embezzled 500,000 US$ from a network of 10 clients with similar profile characteristics to Alice (elderly customers...
These clients were served in the branch that Malory was a Head teller. Malory tap into customers’ saving accounts to wire funds without authorization for 5 years and proceeded unauthorized withdrawals. Malory used the cancel transaction field as a markdown for the embezzled money on each account, so as to keep track what needs to be returned to each account before the client appeared in the branch.

Figure 3 presents part of Malory’s scheme for a selected sample of three clients. In this case, Malory has embezzled a total amount of 300 $ by performing unauthorized transactions among clients disrespecting the bank’s procedures. The next paragraphs describe explicitly 3 days where Malory acted on behalf of clients and for his own interest.

In Day 1, Malory being alone in the cash desk of the bank’s branch performed an unauthorised cash withdrawal of 700 $ from the banking account of Alice. A minute after he performs an unauthorised cash deposit in the banking account of Bob. From these two transactions he puts 200$ in his wallet from the cash difference in the bank’s ledger. The only evidence from this irregular behaviour is tracked in the CCTV surveillance system, since the physical vouchers linked to unauthorised transactions are lost. At this point of time, Alice has a debit balance of 700 $ and Bob a credit balance of 500 $.

Next, in Day 2, Malory performs an unauthorised cash withdrawal of 500$ from the banking account of Bob, and credits Claire’s saving account with an equal amount. At the end of the day, Bob’s balance becomes zero while Claire’s balance is credited with 500 $. Similar to Day 1, the only evidence from this irregular behaviour is tracked in the CCTV surveillance system.

A day later, Malory performs an unauthorised withdrawal from the account of Claire of 400$ and deposits back to client Alice an amount of 300$ keeping for himself 100$. At this point Claire’s account has a credit balance of 100$ and Alice’s account has a debit balance of 400$. Same as above, no voucher bears clients’
Table 2 Most well-known forensic models and guidelines

| Name                                         | Year  | Reference                        |
|----------------------------------------------|-------|----------------------------------|
| Digital Forensic Investigation Model         | 2001  | Kruse and Heiser (2001)          |
| Digital Forensic Research Workshop          | 2001  | Palmer et al. (2001)             |
| Abstract Digital Forensic Model              | 2002  | Reith et al. (2002)              |
| Integrated Digital Investigation Model       | 2004  | Carrier and Spafford (2003)      |
| Enhanced Digital Investigation Process Model | 2004  | Baryamureeba and Tushabe (2004)  |
| Extended Model of Cybercrime Investigation  | 2004  | Ciardhuán (2004)                 |
| NIST Guide to Integrating Forensic Techniques into Incident Response | 2006  | Kent et al. (2006)               |
| Digital Forensic Model for Digital Forensic Investigation | 2011  | Ademu et al. (2011)              |
| International Organization for Standardization ISO/IEC 27043:2015 | 2015  | ISO (2015)                       |
| INTERPOL Guidelines for Digital Forensics Laboratories | 2019  | INTERPOL (2019)                  |
| ENFSI Guidelines                             | 2016-2020 | European Network of Forensic Science Institutes (2020) |
signatures and the only evidence that can track his irregular behaviour is the daily CCTV recording.

### Table 3 Main steps in a digital forensic investigation model

| Forensic Step          | Description                                                                                                                                 |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Identification         | Assess the purpose and context of the investigation. Initialize and allocate the resources required for the investigation, such as policies, procedures and personnel. |
| Collection & Acquisition | The seizure, storage and preservation of digital evidence. Although this two steps need to be strictly differentiated in the physical forensics context, we consider a more relaxed approach in the digital context, since most of times data will be directly collected in a digital form. |
| Analysis               | The identification of tools and methods to process the evidence and the analysis of the outcomes obtained                                    |
| Reporting & Discovery  | The proper presentation of the reports and information obtained during the investigation to be disclosed or shared with the corresponding entities. |

3 The testimony is recorded as a written agreement between Malory and two investigators (signed by each of them).

4 A hard copy of the report is distributed internally to Senior management, HR department, and legal department (i.e., these actors are defined later in this section). The recipients sign a mail record which is then archived in the physical folder of the case.

#### 3.2 Actors involved

The main actors involved during the investigation of the above embezzlement scheme are presented in Fig. 4. Now, we will describe how each actor is involved in the chain of custody.

Firstly, the branch archived the written complain of the client contesting the balance recorded in the passbook of his saving account. It was also responsible for the archiving of original vouchers related to the transactions signed by each customer and for the historic record of CCTV material.

The Internal Audit received the written declaration of the complaint through the internal mail of the bank and e-mail communication. Original hard copies of the complaint are stored in a separate physical folder linked to Malory’s case. The physical folder is scanned at the end of the case and archived in a shared folder with authorized accesses. This folder also includes hard copies linked to the fraud hypothesis (CCTV files, original vouchers, signatures’ specimen etc), the signed testimony3 of Maroly. The signed report released with investigation results4. Digital documentation from detective tools mentioned in 2.1 is archived in the local server of the department, and only authorized users may have access. For the investigation’s purposes, the Internal Audit interacts with the bank’s IT department, Surveillance Department, the Branch, and Human Resources (HR) Department.

IT Department assists Internal Audit by providing data from the database of core banking system. The data are sent via e-mail usually as an excel file concerning
transactions and daily journal of entries of Malory. Also, when Internal Audit needs to trace additional CCTV files, it collaborates with Surveillance Department. The latter delivers any CCTV files upon request through USB. Each employee has a physical record with personal information archived in HR Department. This information distributed to investigators through emails. Also, it is responsible for the archiving of disciplinary board’s proceedings.

When the investigation’s report is issued, Senior Management receives it. Its role is to decide and approve any disciplinary and litigation actions. Decisions and approvals are documented and archived. If the decision involves litigation actions then Legal Department undergoes the submission to a prosecuting authority.

At last, the Prosecutor receives a structured package including the disciplinary board’s decision, the findings’ report and a copy of physical evidence and proceeds to further legal actions.

### 3.3 Forensic Procedure

In the case of chain of custody and trail of events preservation, we need to ensure that our system enables features such as integrity, traceability, authentication, verifiability and security (Bonomi et al. 2020; Tian et al. 2019). In this regard, Table 4 provides a description of each feature and how our blockchain-based system enables it.

In addition, Fig. 5 summarises the main tasks performed in each investigation phase according to our case scenario, and their corresponding relationship with the forensic flow. We included the process defined in ISO 27043:2015 (ISO 2015), as well as each step defined in the guidelines to plan and prepare for incident response (ISO/IEC 27035-2:2016 (International Organization for Standardization 2016)), the guidelines for the identification, collection, acquisition and preservation of digital evidence (ISO/IEC 27037:2012 (International Organization for Standardization 2012)) and the guidelines for interpretation and analysis of digital evidence (ISO/IEC 27042:2015 (International Organization for Standardization 2015)). Therefore, we mapped the different steps of the investigation as defined in our method. Note that we included the prevention layer in our design, which details will be later discussed in Section 5. Therefore, after reporting the incident and initiating the investigation, the evidence collection and forensic analysis is summarised in following steps:

1. Collection and analysis of the investigated accounts (including saving accounts of clients and their correlation with employees’ accounts).
2. Analysis of the daily transactions recorded in the journal of entries of Malory (i.e. extractions from core banking system).
3. Reconcile the time of transactions appearing in the journal entry with the CCTV time.
4. Review of CCTV files in order to trace the physical presence of the client and the suspect.
5. Collection of the testimony of the suspect(s) in signed hardcopy.
For an investigation to be sound, all the forensic steps need to be provable and, in the case of evidence analysis, results need to be reproducible. In the case of internal audits, a malicious investigator could tamper evidence or the analysis performed on data to hide proofs. Therefore, a robust forensic procedure is required to guarantee that evidence is collected in a sound manner and it is not tampered during the analysis. Moreover, each forensic action has to be paired with an individual. The aforementioned requirements can be accomplished by means of the blockchain-based forensic architecture described in the next section.

### 3.4 Blockchain-based Forensic Architecture

In this section, we describe our blockchain-based forensic architecture. In our setup, we assume that the system is implemented in the context of a secure laboratory/investigation facility according to a set of policies and regulations. Note that, since each region and country may apply different policies, we leave their definition and discussion as a future research line. Nevertheless, our system can accommodate more functionalities in the smart contract definition, as well as higher layer control systems and application programming interfaces (APIs).

Considering the previously stated forensic flows and the characteristics of the embezzlement scenario, the architecture of our method is depicted in Fig. 6. Different policies and regulations will be applied at each level identified in Fig. 5, so that, e.g. the identity management, including roles and permissions, will be defined by the corresponding authorities according to each jurisdiction. Moreover, the forensic
Fig. 4. Actors involved in the embezzlement scheme.
guidelines and standards, as well as the underlying blockchain technology to be used and the definition of the smart contracts are also tied to the same principle.

The first step involves the case creation. In this regard, a case can be registered due to a citizen’s testimony (we include in this definition any individual that wants to report a crime) or directly by a prosecutor (or an investigator with enough clearance to open a case) who observed suspicious behaviour. Next, evidences are collected and analysed by using the appropriate forensic tools. The description of each action (e.g. storing an evidence and analysing an evidence) may have a description file associated with JSON or CSV format, to ease further searches and classifications. We assume that secure and private storage is used to preserve the evidences, but other platforms such as cloud-based storage or decentralized storage systems such as the Inter-Planetary File System (IPFS) (Benet 2014) can be used if data are properly protected/encrypted (i.e. following the definitions set out in information security standards like ISO/IEC 27001 (Ganji et al. 2019) or other national IT-security guidelines). More concretely, depending on the approach selected by the investigators, the hashes of the evidence can point to an IPFS address or record the SHA-256 hash of the evidence, the latter being the prevalent method in most threat intelligence platforms, such as Virustotal5 or MalwareBazaar6. Therefore, our proposed system enables the extraction of the hashes of an investigation via a set of smart contract functions, as later described in Section 4, enabling investigators to use such intelligence services (e.g. by using their APIs to upload the evidence or by a hash query) to retrieve additional intelligence. Despite its practicality, an automated methodology to integrate a query system for each intelligence platform requires different configurations and is left to future work.

Finally, when the investigation concludes, all the data can be collected and presented in court.

The aforementioned interactions are mapped into a smart contract and therefore stored permanently in the blockchain. The latter guarantees the verifiability of the investigation due to the blockchain’s immutability, as well as the preservation of the chain of custody, as mentioned early in Table 4. Therefore, the investigation can be audited to certify that any evidence was tampered during the investigation, guaranteeing the soundness of the different forensic procedures. In addition, our approach is designed to be accommodated and in other digital investigation contexts apart from embezzlement, enhancing its adaptability to internal audits.

Concerning the identity management scheme, we argue that due to each organisation’s specific regulatory requirements and policies, which may entail further definitions, agreements and developments, the definition of such scheme falls out of the scope of this paper. Therefore, we consider the identity management module as a black box in our architecture to apply standard and validated mechanisms. For instance, further than the MetaMask7 web3 plugin used in our testing setup to manage the wallets and operating the smart contracts through our web interface, other blockchain-based identity management systems could be applied in this layer.

---

5 https://www.virustotal.com/
6 https://bazaar.abuse.ch/
7 http://metamask.io/
Blockchain circumvents the boundary-based digital identity problem by delivering a secure solution without the need for a trusted, central authority managing access permissions through smart contracts. Since blockchain is considered one of the main enablers of self-sovereign identities, alongside with verifiable credentials and decentralised identifiers, there are multiple examples of privacy-preserving blockchain-based identity management systems and already functional projects (Jacobo-vitz 2016; Dunphy and Petitcolas 2018; Zhu and Badr 2018) that could be adopted for our forensic platform. In this regard, some approaches enabling multi-authority attribute-based access control with smart contracts have been presented in the literature (Guo et al. 2019a, b), as well as approaches implementing multi-blockchain approaches for fine-grained access control (Malamas et al. 2020). In addition, FIDO-based authentication mechanisms could also be used to enable higher security standards (Morii et al. 2017; Lyastani et al. 2020), including biometric access control, cryptographically secure credentials, and passwordless authentication.

4 Experiments and integration details

The interactions between the different actors of the system and the forensic events have been implemented by means of a smart contract, and different tests have been performed in a local private blockchain to showcase the feasibility and performance of the proposed method. More specifically, an Ethereum-based blockchain using node\(^8\) and ganache-cli\(^9\) was created, and truffle\(^10\) was used to code and deploy a fully functional smart contract. Moreover, a graphical interface was developed to query and insert information stored in the blockchain by using

| Feature               | Description                                                                 |
|-----------------------|-----------------------------------------------------------------------------|
| Integrity             | The events data as well as evidences cannot be altered or corrupted during the transferring and during analysis due to the use of hashes. |
| Traceability          | The events and evidences can be traced from their creation till their destruction since every interaction is stored in an immutable ledger. |
| Authentication        | All the actors and entities are unique and provide an irrefutable proof of identity due to the use of asymmetric cryptography. |
| Non-repudiation       | Each action can be related with its author, enabling strong accountability guarantees. |
| Verifiability         | The transactions and interactions can be verified by the corresponding actors. This verification can be performed in real time. |
| Security              | Only actors with clearance can add content or access to it. A robust underlying consensus mechanism ensures that the transactions are signed in a cryptographically secure way. |

---

\(^8\) https://nodejs.org/

\(^9\) https://github.com/trufflesuite/ganache-cli

\(^10\) http://truffleframework.com
Fig. 5 Embezzlement Forensic investigation main phases according to standardised procedures (top) and the corresponding actions performed in our case study (bottom)
node package manager npm\textsuperscript{11}, which also retrieves the corresponding hash of the directory of a specific investigation and its link to the IPFS (Benet 2014), along with other detailed information. Therefore, the information of a specific investigation (or a set of them) is graphically depicted for the user, as well as the option to store a new event, as seen in Figs. 7 and 8, respectively.

We have selected Ethereum due to its robust consensus mechanism as well as its smart contract framework (i.e. we use solidity 0.5.0, which prevents vulnerabilities such as \textit{uninitialized storage pointer} and \textit{erroneous visibility}). For more information about the security of Ethereum and its smart contract framework, we refer the interested reader to Xiao et al. (2020) and Chen et al. (2019), respectively.

For the sake of completeness, a detailed description of the functions implemented in the smart contract is provided in Table 5. As an additional feature, every time the information of the smart contract is updated, a \textit{trigger} function is called, which can be used as an alert. Therefore, the investigators will be able to check in real time the information about a given investigation using the \textit{get/retrieve} functions implemented in the smart contract for verification or managerial purposes.

A link between the smart contract’s functions and the forensic procedures is summarised in Table 6. In the case of custody change procedures, the involved actors will be stored in the corresponding list of owners of the evidence along with a timestamp. Moreover, a new event can be created with an evidence pointing to the same hash, yet with a new creation date to grasp the import of such evidence. In the case of the destruction of an evidence, this procedure will change the status of the evidence to \textit{deleted}. In the latter case, the deletion of a file in a local storage is an easy task, yet the complete erasure of the content in e.g. IPFS can only be made feasible through novel mechanisms (Politou et al. 2020), since IPFS does not implement an erasure protocol at the time of writing (Allen et al. 2020; Casino et al. 2020). In the case of blockchain, the problem is exacerbated due to its inherent immutability (Politou et al. 2018, 2019; Deuber et al. 2019), and the best solution is to minimise the direct storage of data (i.e. only pointers and hashes).

In addition to the benefits enabled by the smart contracts, it is essential to guarantee the privacy of the transactions and the involved actors. Therefore, the contents can be modified only by participants with specific roles (each function is implemented with concrete permissions, e.g. using the \textit{require} clause of solidity and variables such as \textit{msg:sender} to check account authenticity), thus enabling secure access control. For example, prosecutors will be able to open and close investigations, but investigators will be able only to add new events to a specific investigation. In our setup, read-only functions and variables can be checked by public users. Nevertheless, more sophisticated access control, policies and data protection measures can be implemented by the users of the platform according to their specific needs.

\textsuperscript{11} \url{https://nodejs.org/en/knowledge/getting-started/npm/what-is-npm/}
Fig. 6 Overview of the different levels of the system
The transactions tested in the developed private blockchain (e.g. deployment of the smart contract, adding a new case and adding a new event) are performed in the order of milliseconds, and thus, our approach enables real-time interactions. The implementations as well as the graphical interface web service are available on GitHub12.

5 Discussion

In this section, we discuss both the benefits and the challenges to be overcome in the blockchain digital forensics field. Moreover, we provide a granular analysis of such challenges across the different topics explored in this work, namely, digital forensics, blockchain, and finance related crimes.

According to the challenges extracted from our literature review, we identified several mechanisms that could be used to prevent/minimise financial fraud in institutions and their corresponding context of application in Table 7. As it can be observed, training on anti-fraud and incorporating higher security standards are necessary to help employees in their daily activities. In addition, executive personnel should implement more comprehensive and transparent managerial practices to avoid the possibility of obscure and unethical activities. Finally, communication, networking and risk assessment are crucial to improving the information flows between all the actors involved.

Blockchain and its benefits to a myriad of application scenarios have been thoroughly discussed in the past (Casino et al. 2019; Kuo et al. 2017; Ølnes et al. 2017; Zheng et al. 2018). Features such as immutability, verifiability, auditability, security were enhanced by the automation provided by smart contracts. For example, the existence of an event at an specific time (e.g. the existence of a file, a good, a token or any kind of asset) can be verified in a matter of milliseconds, due to the self-executing capabilities and the real time synchronization of the information in the blockchain. The latter enables proof-of-existence when paired with the use of hashes, which can be used to guarantee the trail of events as well as the proper preservation of the chain of custody in the digital forensics context.

In addition, the benefits go further beyond the provision of a solid proof in court, since the knowledge an evidence gathered in a case can be correlated in the future to reduce the time required to find a vulnerability or speed up cybercrime investigations. This is particularly relevant in the finance context, where all background and identification information can be stored. For instance, the Know your Customer (KYC) can be processed easier and faster during investigations and be secured against any internal fraudulent activities. On top of that, the application of smart contracts could prevent efforts for forgery and counterfeit documents. Therefore, the use of blockchain and its data mining capabilities will foster collaboration between different entities to share information and enable the early detection of embezzlement schemes. Moreover, evidences and reports can provide valuable input for the

12 https://github.com/francasino/financial_forensics
**EMBEZZLEMENT DIGITAL FORENSICS**

**Blockchain Query**

| #  | Name                  | Description                                      | Responsible | Investigators | Events | Date Created   | Status | Global ID     | Pedigree Hash                                                                 |
|----|-----------------------|--------------------------------------------------|-------------|---------------|--------|----------------|--------|---------------|--------------------------------------------------------------------------------|
| 1  | Embezzlement Bank 1   | Investigation for embezzlement in a Greek Bank    | Hellenic Police | 2             | 1      | Tue Nov 12 2019 | true   | HP000001      | "QmY8xHZlhfFDjD6tMa37siU3SPTW9phFnoX8ozJzq6Y1W4"                             |
| 2  | Money Laundering User A | Investigation for money laundering suspect A | Interpol    | 1             | 1      | Sat Nov 16 2019 | true   | INTAAA2934   | "QmW5oPVT68thUL3y8svree9JnqjqhQn5jkeoQkwwF"                                 |
| 3  | Embezzlement Bank 2   | Investigation for embezzlement in an European Bank | Europol  | 1             | 1      | Sun Nov 24 2019 | true   | EUPfn398g    | "QmNbrXGoudvUGV31mMYTpx3Dc4E4Ca48M5KnmpgKzV8V5oz"                           |

**Fig. 7** Example of the outcome of a query by searching all cases and their corresponding IPFS links
Fig. 8  A detail of the form user to insert a new event to the system
Table 5: Main characteristics and permissions of the functions implemented in the smart contract. The permissions column states which functions are public (P) or restricted (R) only for specific users related to a case.

| Code | Function                  | Input                                                   | Output | Permissions | Description                                           |
|------|---------------------------|---------------------------------------------------------|--------|-------------|-------------------------------------------------------|
| f1   | constructor               | void                                                    | na     | na          | creates the smart contract                           |
| f2   | addCase                   | String name, String description, String responsible, String globalID, timestamp, hash | void   | R           | adds a new case to the system                        |
| f3   | updateCaseDescription     | Uint caseID, string description                         | void   | R           | updates a case description                            |
| f4   | updateCaseStatus          | Uint caseID, string status                             | void   | R           | updates a case status                                 |
| f5   | updateResponsible         | Uint caseID, address responsible                       | void   | R           | updates the responsible of a case                     |
| f6   | addInvestigatorCase       | Uint caseID, address investigator                      | void   | R           | adds a new investigator to a case                     |
| f7   | getNumberOfCases          | void                                                    | Uint   | P           | returns the global number of cases                   |
| f8   | getCase                   | Uint caseID                                             | Object | P           | returns a case object and its information              |
| f9   | getCaseGlobalID           | Uint caseID                                             | String | P           | returns the global ID of a case                       |
| f10  | getNumberOfInvestigators  | Uint caseID                                             | Uint   | P           | returns the number of investigators assigned to a case |
| f11  | getCaseHash               | Uint caseID                                             | hash   | P           | returns the hash pointer with information of a case   |
| f12  | addEvent                  | Uint caseID, string type, String description, String status, hash, timestamp | void   | R           | adds a new event to a case                            |
| f13  | updateEventStatus         | Uint eventID, string status                             | void   | R           | updates an event/evidence status                     |
| f14  | getNumberOfEventsCase     | Uint caseID                                             | Uint   | P           | returns the number of events of a case                |
| f15  | getEventsCase             | Uint caseID                                             | Object | P           | returns the set of events related to a case           |
| f16  | getGlobalNumberOfEvents   | void                                                    | Unit   | P           | returns global number of registered events           |
| f17  | getEvent                  | Uint eventID                                            | Object | P           | returns an event object                              |
| f18  | getEventHash              | Uint eventID                                            | Hash   | P           | returns the hash of a specific event                  |
| f19  | triggers                  | void                                                    | void   | P           | trigger functions to update the status of the smart contract |
elaboration of AI models with which increase the rate of embezzlement detection, since embezzlement schemes sometimes last for more than 5 years.

As discussed in (Chang et al. 2020), the authors identified several critical success factors for adopting blockchain technology in the finance sector. In general, robust and efficient blockchain implementations are critical to guarantee the required infrastructure to leverage financial services. The latter, paired with well-trained teams and robust security and privacy guarantees, will close the gap for the adoption of blockchain in finance. Other crucial aspects are reputation and community building and mechanisms to guarantee upgraded, long-term products and services. Another relevant aspect that hinders blockchain adoption is the lack of global regulations (Ali et al. 2020), due to highly regulated industries paired with complex jurisdictional and legal frameworks. In addition, underdeveloped countries with insufficient technological infrastructure, and an unclear privacy management and data governance are also delaying blockchain’s adoption (Kim and Kang 2017). The latter is translated into a lack of interoperable solutions and reactive behaviours displayed by regulators, which are always a step behind novel trends and opportunities.

The proper use and adoption of blockchain and showcasing its potential is vital. We believe that systems like the one proposed in this paper reinforce the trust in blockchain and close the gap between the financial sector and blockchain, not only in the context of digital investigation but as a potential tool to leverage better services backed with solid regulatory frameworks supporting them.

Despite the aforementioned benefits, blockchain is not a panacea. There are still many challenges to overcome, such as the issues related with standardization of the procedures related with digital crime prosecution. The latter includes cross border investigations, data storage and data sharing policies, and the management of personal data. Note that the storage of personal data in a blockchain contradicts the GDPR and the right to be forgotten (Politou et al. 2018, 2019) due to immutability. Therefore, despite the unarguable benefits of the immutability property, the capability of sharing an asset perpetually can be used with malicious ends as already seen in the literature (Li et al. 2020; Conti et al. 2018; Patsakis et al. 2020). Moreover, this issue is not only affecting blockchain but also decentralised permanent storage solutions, due to the lack of effective erasure mechanisms (Casino et al. 2020). We believe the controlled erasure of data in blockchain, as well as similar systems, will be a relevant research area in the near future and some authors are already

| Forensic embezzlement procedure | Code |
|----------------------------------|------|
| Register new case                | f1, f2, f3 |
| Evidence management              | f12, f13 |
| Evidence analysis                | f8, f11, f12, f17, f18 |
| Analysis & Report                | f8, f9, f10, f11, f14, f15, f18 |
| Admin & Statistics               | f4, f13, f5, f6, f7, f9, f10, f14, f15, f14, f17, f19 |
investigating it (Politou et al. 2019; Radinger-Peer and Kolm 2020; Deuber et al. 2019; Xu et al. 2020).

Another relevant flaw of blockchain is its scalability, which varies according to the volume of transactions, verifiers/miners, consensus mechanism and other features. In this regard, it is well-known that private flavours of blockchain are the most suitable for most of applications, yet their scalability when the number of users and interactions grow also suffers performance issues (Dinh et al. 2017; Pongnumkul et al. 2017; Dong et al. 2019; Politou et al. 2020).

In our implementation, we minimise the amount of data stored in the blockchain by using hashes. Nevertheless, our testing protocol focused on the underlying functionalities to showcase the feasibility of robust digital investigation and verifiable chain of custody. Therefore, the implementation of an advanced identity management system and the required policy definitions to overcome the issues of cross border investigations are not covered in this paper, and are left for future research.

The key benefit from the managerial perspective of our proposed architecture is that it can eliminate operational risk and costs associated with investigation procedures. In particular, it can accelerate investigations by facilitating the reconciliation of evidence in a verifiable and auditable manner, increasing the possibility of identifying perpetrators and reducing fraud management and recovery costs. It enables senior management to have direct access to fraud risk exposure, reporting, and monitoring and gain a comprehensive view of all investigative information improving their decision-making analysis to impose sanctions and proceed to litigation actions. Moreover, the proposed architecture can be adopted for the audit trail of regularly planned internal audits.

Based on the same methodological steps, the auditors can store their evidence from their audit trails to better monitor their follow-up actions. Thus, regular internal audits can rip the benefits of this architecture and deliver efficient outcomes to the management. Blockchain adoption might have a double effect on the internal audit department since it can reduce operational costs associated with the streamlining of auditing and investigative procedures.

Table 7 Prevention mechanisms and their corresponding application level

| Mechanism                                                                 | Level affected |
|---------------------------------------------------------------------------|----------------|
| Training on anti-fraud and appropriate behavioural conduct                | Workers        |
| Efficient networking and communication strategies                          | All            |
| Transparent managerial practices                                           | Executives     |
| Risk assessment to both internal and external fraud                       | All            |
| Integration of security and AI experts in the organization charts         | Workers        |
| Audit controls and appropriate resources                                  | All            |
6 Conclusions

In this paper, we recall the negative impact of financial crimes on society, focusing on embezzlement scenarios. We provide a thorough state-of-the-art of blockchain-based digital forensic approaches, increasing their relevance in such investigations due to their inherent features. Next, we propose a functional implementation of a forensically sound flow to investigate financial crimes based on Ethereum, and we test it with a real-world embezzlement use case. The outcomes showed that our proposal empowers integrity verification, tamper-proofness, and adaptability towards other fraud and financial crimes.

Despite the benefits of our approach, we leveraged a profound analysis of the literature, identifying the fundamental challenges for adopting blockchain and the financial sector and proposing some strategies to overcome them. Moreover, we discussed further benefits of our approach and how it enhances some of the features required for closing the gap between blockchain and the financial sector.

Among the most important aspects of blockchain integration in financial investigations - and internal audits - are the guarantee of invariable evidence and the streamlining of auditing and investigation procedures. The management of a financial institution may reduce several operational costs associated with the fraud incident and its investigation. The whole framework facilitates the interaction of interdisciplinary resources securely and confidentially and provides a comprehensive overview of each organization’s management related to monitoring and reporting fraud risk exposure. Future work will focus on increasing the adaptability of the scheme by enabling other functionalities and the migration to other blockchain systems. Moreover, we aim to provide a robust identification mechanism to enable secure and private cross-border investigations.

Acknowledgements This work was supported by the European Commission under the Horizon 2020 Programme (H2020), as part of the project LOCARD (https://locard.eu) (Grant Agreement no. 832735) and YAKSHA, (https://project-yaksha.eu/project/) (Grant Agreement no 780498).

References

Ademu, I. O., et al. (2011). A new approach of digital forensic model for digital forensic investigation. International Journal of Advanced Computer Science and Applications, 2(12), 175–178.
AICPA (2020) Cyber criminals are finding ways to steal your digital dollars. https://blog.aicpa.org/2020/05/cyber-criminals-are-finding-ways-to-steal-your-digital-dollars.html.
Ali, O., Ally, M., Clutterbuck, Dwivedi, Y. (2020). The state of play of blockchain technology in the financial services sector: A systematic literature review. International Journal of Information Management, 54, pp. 102199.
Al-Khateeb H, et al. (2019). Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger. In: Advanced Sciences and Technologies for Security Applications, Springer, Cham, pp. 149–168.
Allen S. et al. (2020) IPFS Release v0.6.0. https://github.com/ipfs/go-ipfs/releases, Accessed 1 July 2020.
Antwi-Boasiako, A., & Venter, H. (2017). A model for digital evidence admissibility assessment. In G. Peterson & S. Shenoi (Eds.), Advances in Digital Forensics XIII (pp. 23–38). Cham: Springer International Publishing.
Association of Certified Fraud Examiners (2020a) Fraud examiners manual.
Association of Certified Fraud Examiners (2020b) Report To the Nations 2020 Global Study on Occupational Fraud and Abuse.
Awoyemi, J. O., Adetunmbi, A. O., & Oluwatade, S. A. (2017). Credit card fraud detection using machine learning techniques: A comparative analysis. In: 2017 International Conference on Computing Networking and Informatics (ICCNI), IEEE, pp. 1–9.
Bănărescu, A. (2015). Detecting and preventing fraud with data analytics. Procedia Economics and Finance, 32, 1827–1836.
Baryamureeba, V., & Tushabe, F. (2004). The enhanced digital investigation process model. Digital Investigation, pp. 1–9.
Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. arXiv:1407.3561.
Biasiotti, M. A., et al. (2018). Handling and Exchanging Electronic Evidence Across Europe, (Vol. 39). New York: Springer.
Billard, D. (2018). Weighted forensics evidence using blockchain. In: Proceedings of the 2018 International Conference on Computing and Data Engineering, ACM, New York, NY, USA, ICCDE pp. 57–61.
Billard, D., & Bartolomei, B. (2019). Digital Forensics and Privacy-by-Design: Example in a Blockchain-Based Dynamic Navigation System. Annual Privacy Forum, Springer, Cham.
Bologna, G. J. (1995). Understanding and detecting computer-related embezzlement. Edpacs, 23(3), 1.
Bonomi, S., et al. (2020). B-coc: A blockchain-based chain of custody for evidences management in digital forensics. arXiv:1807.10359.
Brotsis, S., et al. (2019). Blockchain solutions for forensic evidence preservation in iot environments. In: 2019 IEEE Conference on Network Softwarization (NetSoft), pp. 110–114.
Carrier, B., & Spafford, E. H. (2003). Getting physical with the investigative process. International Journal of Digital Evidence, Fall 2003.
Casino, F., et al. (2019). A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics, 36 55–81.
Casino, F., et al. (2020). Immutability and decentralized storage: An analysis of emerging threats. IEEE Access, 8 4737–4744.
Cebe, M., et al. (2018). Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles. IEEE Communications Magazine, 56(10), 50–57.
Cerullo, M. J., & Cerullo, V. (1999). Using neural networks to predict financial reporting fraud: Part 1. Computer Fraud and Security, 5 14–17.
Cerullo, M. J., & Cerullo, V. (1999). Using neural networks to predict financial reporting fraud: Part 2. Computer Fraud and Security, 6 14–17.
Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How blockchain can impact financial services - the overview, challenges and recommendations from expert interviewees. Technological Forecasting and Social Change, 158, pp. 120166.
Chen H, et al. (2019). A survey on ethereum systems security: Vulnerabilities, attacks and defenses. arXiv:1908.04507.
Choi, D., & Lee, K. (2018). An artificial intelligence approach to financial fraud detection under iot environment: A survey and implementation. Security and Communication Networks, vol. 2018, 5483472, p. 15.
Ciardhuain, S. O. (2004). An extended model of cybercrime investigations. International Journal of Digital Evidence, 3(1), 1–22.
Cliff, G., & Wall-Parker, A. (2017). Statistical analysis of white-collar crime. In: Oxford Research Encyclopedia of Criminology and Criminal Justice.
Conti, M., et al. (2018). A survey on security and privacy issues of bitcoin. IEEE Communications Surveys & Tutorials, 20(4), 3416–3452.
Crosby, M., et al. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6–10), 71.
Darrell, D., & Dorrell, G. A. G. (2012). Financial Forensics Body of Knowledge. Hoboken: John Wiley & Sons Inc.
Dasaklis, T.K. et al. (2021), Sok: Blockchain solutions for forensics. Technology Development for Security Practitioners, Springer, Cham, pp. 21–40.
De Vell, O., Anderson, A., Corney, M., & Mohay, G. (2001). Mining e-mail content for author identification forensics. ACM Sigmod Record, 30(4), 55–64.
Delena, D. Spamm. (2014). Fraud Analytics: Strategies and Methods for Detection and Prevention. John Wiley & Sons.
Deuber D, et al. (2019). Redactable blockchain in the permissionless setting. In: 2019 IEEE Symposium on Security and Privacy (SP), IEEE, pp 124–138.

Dinh, T.T.A. et al. (2017). Blockbench: A framework for analyzing private blockchains. In: Proceedings of the 2017 ACM International Conference on Management of Data, pp. 1085–1100.

Dong, Z. et al. (2019). Dagbench: A performance evaluation framework for dag distributed ledgers. In: 2019 IEEE 12th International Conference on Cloud Computing (CLOUD), IEEE, pp. 264–271.

Dunphy, P., & Petitcolas, F. A. P. (2018). A first look at identity management schemes on the blockchain. IEEE Security Privacy, 16(4), 20–29

Duy, P. et al. (2019). Sdnlog-foren: Ensuring the integrity and tamper resistance of log files for sdn forensics using blockchain. In: Proceedings - 2019 6th NAFOSTED Conference on Information and Computer Science, NICS 2019, pp. 416–421.

European Network of Forensic Science Institutes (2020) Forensic guidelines. http://enfsi.eu/documents/forensic-guidelines/

Ganji, D., et al. (2019). Approaches to develop and implement iso/iec 27001 standard-information security management systems: A systematic literature review. International Journal on Advances in Software, 12(3 & 4).

Garfinkel, S.L. (2010). Digital forensics research: The next 10 years. Digital Investigation 7, pp. S64–S73.

Gideon, S. J., Kandulna, A., Kujur, A. A., Diana, A., & Raimond, K. (2018). Handwritten signature forgery detection using convolutional neural networks. Procedia Computer Science, 143 978–987.

Gobler, M. (2010). Digital forensic standards: International progress. In: South African Information Security Multi-Conference, SAISM 2010, Port Elizabeth, South Africa, May 17-18, 2010. Proceedings, pp. 261–271.

Goel, S., & Uzuner, O. (2016). Do Sentiments Matter in Fraud Detection? Estimating Semantic Orientation of Annual Reports. Intelligent Systems in Accounting, Finance and Management, 23(3), 215–239.

Gopalan, S.H., et al. (2019). Digital forensics using blockchain. International Journal of Recent Technology and Engineering, 8(2), 182–184.

Gottschalk, P. (2018). Internal Investigation Approaches. Investigating White-Collar Crime. Springer, Cham, pp. 57–72.

Green RM, Sheppard JW (2013) Comparing frequency-and style-based features for twitter author identification. In: The Twenty-Sixth International FLAIRS Conference, pp. 1–6.

Gu, J., et al. (2018). Consortium blockchain-based malware detection in mobile devices. IEEE Access, 6 12118–12128.

Pedneault, S. (2010). Preventing and detecting employee theft and embezzlement: A practical guide Vol. 5. John Wiley & Sons.

Gullkvist, B., & Jokipi, A. (2013). Perceived importance of red flags across fraud types. Critical Perspectives on Accounting, 24(1), 44–61.

Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. Financial Innovation, 2(1), 24.

Guo H, Meamari E, & Shen, C.C. (2019a). Multi-authority attribute-based access control with smart contract. In: Proceedings of the 2019 International Conference on Blockchain Technology, pp. 6–11.

Guo, R., Shi, H., Zheng, D., Jing, C., Zhuang, C., & Wang, Z. (2019b). Flexible and efficient blockchain-based abe scheme with multi-authority for medical on demand in telemedicine system. IEEE Access, 7 88012–88025.

Homayoun, S., et al. (2019). A blockchain-based framework for detecting malicious mobile applications in app stores. In IEEE Canadian Conference of Electrical and Computer Engineering (CCECE). pp. 1–4.

Hossain, M.M, et al. (2018). Probe-IoT: A public digital ledger based forensic investigation framework for IoT. In IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 1–2.

Huang, K., et al. (2018). Systematically understanding the cyber attack business: A survey. ACM Computing Surveys (CSUR), 51(4), 1–36.

International Organization for Standardization (2012). Guidelines for identification, collection, acquisition and preservation of digital evidence. https://www.iso.org/standard/44381.html.

International Organization for Standardization (2015). Guidelines for the analysis and interpretation of digital evidence. https://www.iso.org/standard/44406.html.

International Organization for Standardization (2016). Guidelines to plan and prepare for incident response. https://www.iso.org/standard/62071.html.
INTERPOL. (2019). Global guidelines for digital forensics laboratories. Global Complex for Innovation: Tech. rep.
ISO (2015) ISO/IEC 27043:2015 Information technology. Security techniques. Incident investigation principles and processes. Tech. Rep. 1, ISO, Central Secretariat.
Jacobovitz, O. (2016). Blockchain for identity management. The Lynne and William Frankel Center for Computer Science Department of Computer Science Ben-Gurion University, Beer Sheva, Israel, pp. 1–19.
Joshi, P., et al. (2019). A blockchain based framework for fraud detection. In: 2019 Conference on Next Generation Computing Applications (NextComp), pp. 1–5.
Kent, K., et al. (2006). Sp 800-86: guide to integrating forensic techniques into incident response.
Kerr, M., et al. (2018). A blockchain implementation for the cataloguing of cctv video evidence. In: 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), pp. 1–6.
Kevin, D., & David, B. (2019) HACIT2: A privacy preserving, region based and blockchain application for dynamic navigation and forensics in VANET, International Conference on Ad Hoc Networks. Springer, Cham, pp. 225–236.
Kim, K., & Kang, T. (2017). Does technology against corruption always lead to benefit? The Potential Risks and Challenges of the Blockchain Technology, OECD Global Anti-Corruption & Integrity Forum, pp. 12–15.
Kobayashi, H., Mark, B. L., & Turin, W. (2011). Probability, random processes, and statistical analysis: applications to communications, signal processing, queueing theory and mathematical finance. Cambridge: Cambridge University Press.
Kotsiuba, I., et al. (2018). Blockchain evolution: from bitcoin to forensic in smart grids. In: 2018 IEEE International Conference on Big Data (Big Data), IEEE, pp. 3100–3106.
Kruse, W. G., & Heiser J. G. (2001). Computer forensics: incident response essentials. Pearson Education.
Kuo, T. T., et al. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211–1220.
Kyei, K., et al. (2013). A review and comparative study of digital forensic investigation models. In M. Rogers & K. C. Seigfried-Spellar (Eds.), Digital Forensics and Cyber Crime (pp. 314–327). Berlin Heidelberg: Springer.
Le D.P., et al. (2018). Biff: a blockchain-based iot forensics framework with identity privacy. In: TENCON 2018 IEEE Region 10 Conference, IEEE, pp. 2372–2377.
Leite, R. A., Gschwandtner, T., Miksch, S., Gstrein, E., & Kuntsler, J. (2018). Visual analytics for event detection: Focusing on fraud. Visual Informatics, 2(4), 198–212.
Li, S., et al. (2019). Blockchain-based digital forensics investigation framework in the internet of things and social systems. IEEE Transactions on Computational Social Systems, 6(6), 1433–1441.
Li, X., et al. (2020). A survey on the security of blockchain systems. Future Generation Computer Systems, 107 841–853.
Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digital Investigation, 28, 44–55.
Lyastani, S.G., Schilling, M., Neumayr, M., Backes, M., Bugiel, S. (2020). Is fido2 the kingslayer of user authentication? a comparative usability study of fido2 passwordless authentication. In: 2020 IEEE Symposium on Security and Privacy (SP), IEEE, pp. 268–285.
Malamas V, et al. (2019) A Forensics-by-Design Management Framework for Medical Devices Based on Blockchain. In: 2019 IEEE World Congress on Services (SERVICES), IEEE, vol 2642, pp. 35–40.
Malamas, V., Kotzanikolaou, P., Dasaklis, T. K., & Burmester, M. (2020). A hierarchical multi blockchain for fine grained access to medical data. IEEE Access, 8 134393–134412
Manning, G. A., & EA CFE. (1999). Financial investigation and forensic accounting. CRC Press.
Markowitz, D. M., & Hancock, J. T. (2014). Linguistic traces of a scientific fraud: The case of diederik stapel. PloS one, 9(8), e105937.
Molloy, I., Chari, S., Finkler, U., Wiggerman, M., Jonker, C., Habbeck, T., et al. (2017). Graph analytics for real-time scoring of cross-channel transactional fraud. In J. Grossklags & B. Preneel (Eds.), Financial Cryptography and Data Security (pp. 22–40). Berlin Heidelberg: Springer.
Morii, M., Tanioka, H., Ohira, K., Sano, M., Seki, Y., Matsuura, K., Ueta, T. (2017). Research on integrated authentication using passwordless authentication method. In: IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), IEEE, vol 1, pp. 682–685.
Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
Wolverton, R., & Lee, J. (2019). Blockchain Versus Financial Statement Fraud. AICPA: Tech. rep. https://future.aicpa.org/professional-insights/download/blockchain-versus-financial-statement-fraud.

Xiao, Y., et al. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, 22(2), 1432-1465.

Xiong Y, Du J (2019) Electronic evidence preservation model based on blockchain. In: Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, ACM, pp. 1–5.

Xu, M., et al. (2019). A systematic review of blockchain. *Financial Innovation*, 5(1), 27.

Xu, J., et al. (2020). An identity management and authentication scheme based on redactable blockchain for mobile networks. *IEEE Transactions on Vehicular Technology*, 69(6), 6688–6698.

Yoo KH, Gretzel U (2009). Comparison of deceptive and truthful travel reviews. In: Information and communication technologies in tourism 2009, Springer, pp. 37–47.

Zhang, Y., et al. (2018). A blockchain-based process provenance for cloud forensics. In: 2017 3rd IEEE International Conference on Computer and Communications (ICCC), IEEE, pp. 2470–2473.

Zheng, Z., et al. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4), 352–375.

Zhu, X., & Badr, Y. (2018). Identity management systems for the internet of things: A survey towards blockchain solutions. *Sensors*, 18(12), 4215.

Zou, R., et al. (2019). Blockchain-based photo forensics with permissible transformations. *Computers and Security*, 87 101567.

**Publisher’s Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.