SoK: Blockchain Solutions for Forensics

Thomas K. Dasaklis, Fran Casino,
and Constantinos Patsakis

2.1 INTRODUCTION

The undergoing digitization of information-intensive processes has a radical impact on our daily lives. Digitization affects almost all aspects of our lives from how we work to how we interact and communicate with each other. As a result, a myriad of devices is involved in almost every possible aspect of our daily lives. For instance, a smartphone may contain data with different levels of sensitivity (text messages, emails, financial transactions, etc.) which provide background information on its owner and his/her social connections. Digitization, however, comes at a cost. Financial frauds, intellectual property infringements, industrial espionage and digital terrorist networks are just a few among the various faces of

T. K. Dasaklis (✉)
Department of Informatics, University of Piraeus, Pireas, Greece
e-mail: dasaklis@unipi.gr

F. Casino · C. Patsakis
Department of Informatics, University of Piraeus, Pireas, Greece

Athena Research Center, Athens, Greece
e-mail: francasino@unipi.gr; kpatsak@unipi.gr

cybercriminal behaviour. In the event of such deviant behaviour, digital evidence may be the only evidence of a case. Hence, digital evidence forms an integral part of the overall criminal investigation process.

Although the digital forensics community has established reliable scientific methodologies and common standards in its workflows, 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. Moreover, most of the criminal activity on the Internet is transnational, generating cross-jurisdiction problems of cooperation and information exchange that can be alleviated by common standards and protocols. Several challenges have been identified in the literature regarding the development of robust digital forensics approaches. In [19], the authors identify four broad categories of challenges in digital forensics: (a) technical challenges, (b) legal systems and/or law enforcement challenges, (c) personnel-related challenges, and (d) operational challenges. Another major issue that directly impacts digital forensics is the ever-increasing volume of potential evidence generated along with the growing number of devices used [34]. Some domain-specific challenges are worth mentioning. For example, in the case of cloud forensics, identifying useful network events and recording the minimum representative attributes for each event remain a significant challenge [30]. Lack of international collaboration and legislative frameworks in cross-nation data access/exchange and the increased number of mobile devices accessing the cloud are also significant challenges in cloud forensics [37]. Arguably the most critical problem in digital forensics is the validity and trustworthiness of the evidence itself (safeguarding the chain of custody for the data related to a case), particularly when multiple stakeholders are involved in the overall forensics process.

2.1.1   *Blockchain as a Game Changer in Digital Forensics*

Blockchain, a novel disruptive technology, has emerged the past few years, enabling the development of a wide range of applications [8]. In principle, a blockchain can be considered a distributed append-only data structure which stores states efficiently and in a transparent way. While the initial concept of Nakamoto was to store transactions of bitcoins in a way that prevents double-spending [28], the created structure has many appealing properties. Setting aside the different "flavours" that blockchains have, they offer auditability, robustness and security. Blockchains also provide

immutability to a large extent [31], posing significant challenges to the implementation of the right to be forgotten principle, as defined in the EU General Data Protection Regulation Directive (GDPR) [32].

Based on the above, it is apparent that the blockchain properties constitute a very promising baseline for forensics [1]. More precisely, during a forensic investigation, all the involved investigators would like to store their findings in an immutable way so that they cannot be altered and be brought to a court of law. Similarly, blockchains provide transparency and auditability, which is a requirement for the chain of custody of the corresponding evidence. In this regard, in the past few years, several researchers have investigated these opportunities and proposed blockchain-based solutions for forensics. While the field is rather recent, we argue that in the coming years blockchain solutions for managing forensics will become a default. This survey performs an in-depth analysis of the needs and gaps of the field and the different approaches in the literature. Therefore, we set the landscape and facilitate the design of the new solutions.

2.1.2   *Goal and Plan of the Chapter*

In this chapter, we analyse the current state of blockchain-based forensic methods applied in different fields. First, we provide a comprehensive classification and the main features of the state-of-the-art solutions, which are retrieved using a sound bibliographic analysis approach. Next, we analyse how blockchain's features can enhance digital forensics. Finally, we discuss the limitations and the main challenges that are at the intersection of both fields.

The rest of the chapter is organized as follows: Sect. 2.2 describes the research methodology used and the main quantitative literature findings. Next, Sect. 2.3 provides a topic classification of the blockchain-based digital forensics methods and a qualitative analysis of their features. Thereafter, Sect. 2.4 provides a discussion of the main limitations of blockchain technologies and the challenges to be faced by next-generation digital forensics solutions. Finally, the chapter offers some final remarks in Sect. 2.5.

2.2   METHODOLOGY

To survey the available blockchain-based forensics approaches, we have used a sound methodological framework. In particular, we performed a systematic search during November 2019 without time-frame restrictions.

Table 2.1 Year-based and source-type classification of the available literature

Publication type	Publication year	
	2018	2019
Journal articles	2	8
Serials	–	4
Conference proceedings	4	6

We used the Scopus scientific database as our primary source for identifying relevant literature. We used a predefined set of keywords for searching within the titles of all the available Scopus papers (the terms used included the words "blockchain" and "forensics"). To locate additional studies, we used the so-called snowball effect (additional literature was retrieved based on references of key articles found in the initial phase of our search). We excluded some papers based on certain exclusion criteria (relevant to document type, language and subject area). In total, 24 articles were selected for analysis. For the thematic content analysis of the selected literature, we used a qualitative analysis software (MAXQDA11). Finally, we adopted various qualitative analysis methods (i.e. narrative synthesis and thematic analysis) for the classification and synthesis of the extracted data. We present the results of our analysis in Sect. 2.3.

There exist some bibliographic analysis results worth mentioning. As seen in Table 2.1, the available blockchain-enabled forensics literature spans only 2 years (2018 and 2019). Therefore, it is not until very recently that the scientific community has focused on blockchain technology as a viable solution for establishing robust forensics mechanisms. Regarding the type of publications, there seems to be an even allocation between conference proceeding papers and articles published in international journals.

2.3   Classification of the Available Blockchain-Based Forensics Literature

In this section, we thoroughly analyse the literature and provide a topic-based classification (see Fig. 2.1). Next, we identify the main features and solutions proposed by each method in Table 2.2 and discuss them in the following paragraphs.
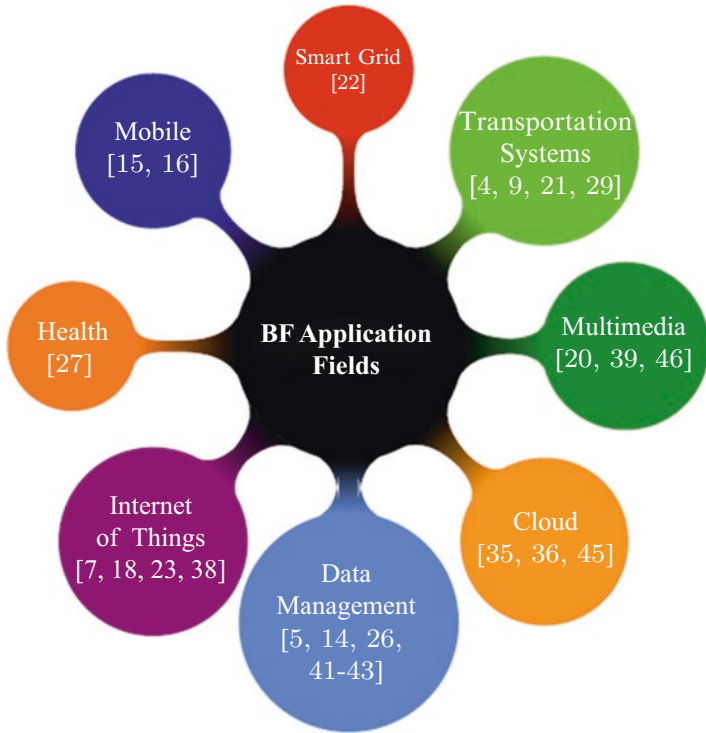
Fig. 2.1 Mind map abstraction the blockchain forensics research topics. The size of each topic has been weighted according to the number of contributions

2.3.1   Cloud Forensics

Cloud security threats remain a significant challenge nowadays. Cloud forensics, an umbrella term covering issues of cloud computing and digital forensics, may assist in investigating cloud environments and quickly respond to and report cloud security incidents [36]. Cloud forensics call for multiparty collaboration due to the multitude of stakeholders engaged. To this end, blockchain technology may enhance the collection of digital evidence in cloud environments and further improve different stakeholder coordination [45]. Another critical aspect of cloud forensics may refer to logs management. In particular, secure preservation and investigation of the various logs are essential elements of cloud forensics. However, due to

Table 2.2 Description of the features of the available blockchain-based forensic schemes

Refs.	Application domain	Problem addressed	Blockchain-enabled forensic features	Implementation
[35]	Cloud forensics	Integrity of logs, multi-stakeholder collusion	Secure logging as-a-service for cloud environment, integrity, confidentiality and immutability of logs	Yes
[36]	Cloud forensics	Multi-location storage of forensic evidence, multiple stakeholders engaged	Data encryption, distributed storage	No
[45]	Cloud forensics	Multiparty cooperation, trustworthiness of records among stakeholders	Chain of custody, proof of existence, privacy and anti-tampering preservation for process records	Yes
[33]	Cloud forensics	Multi-stakeholder collusion, security and access control, multiparty cooperation, trustworthiness of records among stakeholders	Integrity, chain of custody, data encryption, secure access control	Yes
[13]	Cloud/ network forensics	Multiparty cooperation, trustworthiness of records among stakeholders, SDN log recording	Chain of custody, proof of existence, privacy and anti-tampering preservation for process records	Yes
[5]	Data management forensics	Validity of the digital evidence	Weighted digital evidence, digital evidence inventory, categorization according to each evidence relevance, assignment of confidence rating	No
[6]	Data management forensics	Integrity and validity of electronic evidence and ownership	Chain of custody, tracking of the stakeholders involved, credibility of the data provided	Yes

(*continued*)

Table 2.2 (continued)

Refs.	Application domain	Problem addressed	Blockchain-enabled forensic features	Implementation
[14]	Data management forensics	Integrity and validity of electronic evidence	Chain of custody, tracking of the stakeholders involved, credibility of the data provided	No
[26]	Data management forensics	Integrity and authenticity of digital evidence, authenticity and legality of processes and procedures used to gather and transfer the evidence	Chain of custody, safeguarding the integrity and tamper-resistance of digital forensics	Yes
[41]	Data management forensics	Tampering with evidence, data privacy issues, sensitive information leakages	Lightweight, scalable secure digital evidence framework, multi-signature schemes for evidence submission and retrieval	Yes
[42]	Data management forensics	Proof of existence of digital evidence	Tamper-proof chronology by means of OpenTimestamps	No
[43]	Data management forensics	Trust and security issues as derived by current centralized data management schemes	Electronic evidence preservation, different evidence access rights, data security protection, information integrity guarantees, traceability	No
[27]	Healthcare forensics	Different access levels (to both health data and devices), health data privacy	Log audit trails for integrity and provenance guarantees, health data privacy, fine-grained access	Yes
[7]	IoT forensics	Collection and preservation of evidence regarding alleged malicious behaviour in IoT networks	Private forensic data/metadata evidence collection, integrity, authentication, and non-repudiation of the data collected	No

(*continued*)

Table 2.2 (continued)

Refs.	Application domain	Problem addressed	Blockchain-enabled forensic features	Implementation
[18]	IoT forensics	Multiple IoT stakeholders, multiparty access to digital evidence	Integrity, confidentiality, anonymity, authenticity and non-repudiation	No
[23]	IoT forensics	Traceability, integrity and provenance of the evidence is limited due to the resource-constraint nature of IoT devices	Integrity, authenticity, non-repudiation, identity privacy, end-to-end forensic life cycle	No
[38]	IoT forensics	Heterogeneity and distribution characteristics of the IoT environment	Chain of custody for all the IoT-related forensics processes, security and data integrity, multiparty verification of the IoT-related forensics processes	Partial
[24]	IoT forensics	Traceability, integrity and provenance of the evidence	Security and data integrity, multiparty verification of the IoT-related forensics processes and evidences	Partial
[15]	Mobile forensics	Current limitations of static-based and dynamic-based code analysis tools (code obfuscation, encryption, malware in different families with various features)	Consortium blockchain framework to store and classify android malware, classification of different malware families	Partial
[16]	Mobile forensics	Tracking and recording of a very wide range of existing malicious programs, current limitations of static-based and dynamic-based code analysis tools	Enhanced malware detection features based on the usage of both private and consortium blockchain	No

Table 2.2 (continued)

Refs.	Application domain	Problem addressed	Blockchain-enabled forensic features	Implementation
[20]	Multimedia forensics	Integrity and legal authenticity of video data produced as evidence in legal proceedings, privacy concerns of video data gathered by CCTV installations	Trustworthy evidence protection in distributed network environment, video data integrity (link to the primary video stream and its creation)	Yes
[39]	Multimedia forensics	Civilians/journalists who need to protect their identity while ensuring that the evidence they collect are forensically sound	Integrity and spatiotemporal properties of digital evidence	Yes
[46]	Multimedia forensics	Photo-faking, photo owners have limited control over their photos after uploading them on the Internet due to lack of copyright protection mechanisms	Customized access control rules, photo-tracing, creation of copyright-protected photos (resolving copyright dispute problems)	Yes
[22]	Smart grid forensics	Smart grid security, intrusion detection	Ensure the integrity of smart energy transaction platforms, keeping log information for effectively investigate cybercrimes and predict system failures	No
[4]	Transportation forensics	Contradictory use of personal data, privacy, multiple stakeholders involved	Integrity, veracity, authenticity, non-repudiation and identity privacy of vehicle-related data voluntarily and spontaneous release of data for forensic purposes	No

(*continued*)

Table 2.2 (continued)

Refs.	Application domain	Problem addressed	Blockchain-enabled forensic features	Implementation
[9]	Transportation forensics	Transportation data is overwritten shortly, no available system for integrating data from the various stakeholders involved (data from other vehicles, road conditions, manufacturers, and maintenance centres), only third-party solutions exist for vehicular forensics (such as surveillance cameras and eyewitnesses)	Lightweight privacy-aware blockchain framework to manage the collected vehicle-related data (maintenance information/history, car diagnosis reports)	No
[21]	Transportation forensics	Data privacy concerns (GPS sensitive info) due to third-party usage	Legal authority may run forensic analysis without unnecessary violation of the user anonymity and privacy	No
[29]	Transportation forensics	Unauthorized changes in vehicle hardware profiles, multiple stakeholders involved	Logs of all hardware profile changes are kept on blockchain, provision of customized access (only authenticated changes are allowed)	Yes

the inherent uncertainties of cloud environment, several difficulties exist concerning the collection of authentic logs from a cloud environment while preserving integrity and confidentiality. Blockchain technology may be used as a logging-as-a-service tool for securely storing and processing logs while coping with issues of multi-stakeholder collusion and the integrity and confidentiality of logs [13, 35].

2.3.2   *Data Management Forensics*

The works classified in data management include these proposing novel models for data processing and chain of custody preservation

methodologies. The use of permissioned blockchains [14, 26, 43] is stated as a measure to enhance scalability, as well as the use of lightweight consensus mechanisms [41]. Advanced evidence collection and feature classification [5], as well as the relevance of the timeline of events [6, 42], are other features discussed by authors. However, the main drawback of the proposed solutions is that they only offer architectural designs and they do not provide full exploitation of blockchain, with only a few of them offering practical implementations [6, 26, 41].

2.3.3   *Healthcare Forensics*

With the prevalence of new regulatory frameworks brought forward (like the EU GDPR directive), healthcare organizations have started taking necessary steps towards protecting themselves against costly breaches of patients' sensitive information and further safeguarding their reputation. To this end, forensics may be a valuable ally for addressing litigation risks when it comes to data breaches and unauthorized access to medical data from both outside attacks or internal misuse [10]. Access control management is an essential feature of patient data protection. In [27], the authors propose a blockchain-enabled authorization framework for managing both the Internet of Medical Things (IoMT) devices and healthcare stakeholders. The proposed framework provides fine-grained access to patient health data and preserves the chain of custody of all logs by offering audit trails for integrity and provenance guarantees.

2.3.4   *IoT Forensics*

IoT forensics includes the study of IoT devices, their systems and interrelations between different parts of their ecosystems. In this regard, the result of our literature review showed that there is a relevant interest in IoT forensics in the blockchain. We observed that evidence collected from IoT devices and interactions between the different actors (e.g. through privacy-preserving identity management techniques) are the most relevant features studied in the literature [7, 18, 38]. Moreover, proper identity management and privacy preservation is also a mandatory requirement in such context [23]. Nevertheless, current solutions are not mature enough, since authors only proposed architectures and flows, except for [23], which only provided transaction performance tests.

2.3.5   *Mobile Forensics*

Mobile forensics includes the analysis of digital and physical evidence provided by smartphone devices and similar ones (i.e. these sharing similar architectural bodies and underlying operating systems, such as tablets or other handheld devices). Nevertheless, the identified blockchain-based forensic research mainly focuses on applications and malware detection. More concretely, authors propose the use of consortium blockchains and focus on malware detection and statistical analysis based on each application feature [15, 16]. Therefore, more work needs to be provided in this field, with special regard to hardware inclusion and holistic systems definition, as well as usable implementations.

2.3.6   *Multimedia Forensics*

Multimedia forensics employs various scientific techniques for examining a multimedia file (audio, video and/or image) concerning its (a) integrity (establish the linkage between a multimedia output and its source identification) and (b) authenticity (check for the veracity of the multimedia output). For example, in [20], a blockchain-based approach is proposed for cataloguing CCTV video evidence. The authors provide a functional implementation of the blockchain-based system that manages high volumes of CCTV evidence. In [39] the authors present E-Witness, a system that uses blockchain technology for safeguarding the integrity and spatiotemporal characteristics of digital evidence captured by smartphones. To verify the integrity and spatiotemporal claims of the evidence, the proposed system uses hashes of pictures/videos along with location certificates stored in the blockchain. A blockchain-based photo forensics scheme is presented in [46]. The proposed Ethereum-based scheme resolves photos' veracity issues like photo-faking, photo-tracing and copyright dispute problems.

2.3.7   *Smart Grid Forensics*

Smart grids offer significant improvements in terms of resources utilization in current electricity supply networks. Smart grids embrace digital communications technologies, smart metering, intelligent appliances and energy-efficient resources for better matching energy supply and demand. Like other cyberphysical systems, however, smart grids are vulnerable to

cyberattacks, and intrusion detection might prove extremely important. In [22] the theoretical underpinnings of blockchain technology and its importance in smart grids forensics are discussed. The authors highlight how blockchain can enhance features such as energy optimization, system performance, managerial tasks and security of smart grids. Finally, the authors discuss the opportunities/open issues in the topic.

2.3.8   *Intelligent Transportation Systems Forensics*

Intelligent transportation systems (ITS) embrace a range of technological novelties like advanced sensing and control and IoT applications for improving safety, efficiency and services provision of both vehicles and road transport networks. However, the increased automation of ITS (e.g. self-driving cars) and the adoption of new data privacy frameworks (like the GDPR) call for the development of sound forensic mechanisms to analyse traffic accidents and protecting users' sensitive data. In [4], a blockchain-enabled system is proposed for managing users' requests (car navigation) and relevant data that fully complies with data privacy and protection legal frameworks. In [9], the authors propose a blockchain-based forensics system that enables the trustless, traceable and privacy-aware post-accident analysis with minimal requirements in storage and processing. A blockchain framework is proposed in [21] for managing sensitive navigation data (GPS position) within a fixed geographic zone while ensuring user anonymity. Cybersecurity threats may also prove critical in the context of current ITS. In [29] a blockchain-based framework is proposed for keeping logs of all hardware profile changes in a vehicle. Based on the inherent characteristics of blockchain technology, the proposed framework only allows authenticated changes, subject to user, time, geospatial and contextual constraints, as defined by automotive manufacturers.

2.4   Discussion

In what follows, we describe the main limitations of blockchain technology and some strategies to overcome them. Moreover, we provide a detailed analysis of actual and future challenges of digital forensics and discuss possible countermeasures.

2.4.1   Limitations in Blockchain

The suitability of blockchain is a topic that has been extensively discussed in the literature [8, 11]. In this regard, the challenges to be faced by different blockchain technologies vary depending on their type and application scenario. For example, public blockchains face limitations such as scalability, performance and cost issues. In this regard, public blockchains are nowadays mainly used for cryptocurrencies and to commit small pieces of data (i.e. hashes) for verifiability purposes [44]. In the case of private blockchains, the performance and scalability challenges are overcome due to the use of more efficient consensus mechanisms and a reduced number of participants.

Moreover, the cost of memory, compared with public blockchain is negligible, yet off-chain data storage is a recommended strategy for most applications. Nevertheless, both public and private blockchains require the use of proper data management and architectural designs to provide security and privacy guarantees [25]. In this regard, the use of secure identity management systems [3], the proper analysis of the specific blockchain systems to be used [17] and a careful implementation development of smart contracts [2, 40] are mandatory.

2.4.2   Challenges in Blockchain Digital Forensics

We classified next-generation digital forensics' most relevant challenges in the following six domains:

Tokenization of Artefacts from Digital Evidence
Digital forensics imply the analysis of the digital evidence and the extraction of the corresponding knowledge regarding the events of a crime under investigation. However, this analysis is not performed by a single entity. For instance, an image of hard disk may contain different evidence that must be analysed by different people who will look into different parts. One person may study the log files, while another may investigate the file system and a third one might be needed to analyse a specific binary that requires reversing. Therefore, a single evidence is expected to be divided in an arbitrary amount of artefacts, each of which might have to be studied individually and from another person. Breaking down things and storing them in blockchains is not straightforward, and several existing solutions could be adopted (e.g. the use of tokens); however, the bulk

of them considers that the elements that something is decomposed to is predetermined. Despite the fact that some solutions for assigning tokens in blockchain for arbitrary decomposition of an object have been proposed in the supply chain field [12], storing tokenized artefacts in the blockchain during the course of a digital investigation remains a challenge.

Efficient Management of Data Volume in the Chain of Custody
One of the main concerns in digital forensics is the volume of data, since evidence may include thousands of multimedia files or log files per case. In this regard, although data storage of raw documents has to be provided for all cases, it should be based on off-chain technologies (e.g. IPFS, Storj). In this case, only hashes should be used in the blockchain (i.e. or meta-hashes if data are processed as blocks, to ease auditability).

Parse Forensic Sound Procedures in Blockchain Systems
Standard and sound forensic flows have to be provided, even when using blockchain as a platform to provide verifiability and chain of custody tamper-proof guarantees. Therefore, proper standardized flows and smart contracts that map the adequate functions have to be provided to enable final court validation as well as certification by digital forensic laboratories and law enforcement agencies.

Enable an Understandable Forensic Outcome/Reports
The use of blockchain provides a myriad of benefits, such as the efficient and verifiable provision of data flows. Still, the knowledge retrieving and report creation parts belong to a different stage. In this regard, even if automated, the reports and outcomes generated should be understandable in court. Therefore, even if blockchain facilitates this task, research efforts have to be done in this direction, providing a link between forensic sound procedures and their proper explanation.

Interoperability and Cross-Border Jurisdictions The use of international standardized flows and proper data management and sharing agreements will enhance the fight of cybercrime. Nowadays, international collaborations already exist in the scope of the European Union.[1] Nevertheless,

---

[1] https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime/e-evidence_en

further development of blockchain-based solutions[2] will serve as a ground truth platform for standardized solutions, enabling international interoperability.

Timeline of Events and Chronology
The relevance of data acquisition and timeline of events in digital forensics is key to identify patterns and relate similar cases, since the knowledge generated by forensic investigations has to be used in the future to prevent or minimize them. Therefore, the proper reporting and evidence collection procedures have to be done respecting the timeline of events.

Blockchain can provide proof of existence due to its immutability, which, combined with the use of block timestamps and hashes, can guarantee that evidence was collected at a specific moment and they have not been modified.

2.5   Conclusions

Digitization comes with a myriad of novel opportunities and services. Nevertheless, this heterogeneous landscape is also becoming a profitable playground for malicious users, which are continuously increasing the dynamism and complexity of cybercriminal activities. In this regard, digital forensics needs to be rapidly updated to deal with a set of multidisciplinary challenges, ranging from the advances in information and communication technologies, to jurisdictional and interoperability restrictions. To this end, we believe that digital forensics can be benefited from the widespread adoption of blockchain technology and its inherent characteristics.

In this chapter, we presented a literature review of the current blockchain-based forensic solutions and classified them according to their features as well as their application field. Thereafter, we identified the benefits and limitations of blockchain-based forensics and outlined the main challenges to be overcome in the future, providing a fertile ground for research.

Future work will focus on developing a blockchain-based forensic framework which enables the collection of heterogeneous digital evidence as well as forensic procedures in a standardized manner. To this end, we will study the tokenization of digital forensic evidences to provide a common layer of abstraction for different categories of cybercrime.

---

[2] https://locard.eu/

BIBLIOGRAPHY

1. Al-Khateeb, H., Epiphaniou, G., & Daly, H. (2019). Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger. In *Advanced Sciences and Technologies for Security Applications* (pp. 149–168).

2. Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on ethereum smart contracts (sok). In *International Conference on Principles of Security and Trust* (pp. 164–186). Berlin: Springer.

3. Bernal Bernabe, J., Canovas, J. L., Hernandez-Ramos, J. L., Torres Moreno, R., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access, 7*, 164908–164940.

4. Billard, D., & Bartolomei, B. (2019). Digital forensics and privacy-by-design: Example in a Blockchain-based dynamic navigation system. In *Annual Privacy Forum* (pp. 151–160). Cham: Springer.

5. Billard, D. (2018). Weighted forensics evidence using blockchain. In *Proceedings of the 2018 International Conference on Computing and Data Engineering* (pp. 57–61). New York: ICCDE 2018, ACM. https://doi.org/10.1145/3219788.3219792.

6. Bonomi, S., Casini, M., & Ciccotelli, C. (2020). B-coc: A blockchain-based chain of custody for evidences management in digital forensics. In *OpenAccess Series in Informatics, 71*.

7. Brotsis, S., Kolokotronis, N., Limniotis, K., Shiaeles, S., Kavallieros, D., Bellini, E., & Pavue, C. (2019). Blockchain solutions for forensic evidence preservation in iot environments. In *2019 IEEE Conference on Network Softwarization (NetSoft)* (pp. 110–114). IEEE.

8. Casino, F., Dasaklis, T. K., & Patsakis, C. (2018). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36*, 55–81.

9. Cebe, M., Erdin, E., Akkaya, K., Aksu, H., & Uluagac, S. (2018). Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. *IEEE Communications Magazine, 56*(10), 50–57.

10. Chernyshev, M., Zeadally, S., & Baig, Z. (2019). Healthcare data breaches: Implications for digital forensic readiness. *Journal of Medical Systems, 43*(1), 1–12.

11. Chowdhury, M. J. M., Ferdous, M. S., Biswas, K., Chowdhury, N., Kayes, A. S. M., Alazab, M., & Watters, P. (2019). A comparative analysis of distributed ledger technology platforms. *IEEE Access, 7*, 167930–167943.

12. Dasaklis, T., et al. (2019). A framework for supply chain traceability based on blockchain tokens. In *International Conference on Business Process Management.* Cham: Springer.

13. Duy, P., Do Hoang, H., Thu Hien, D., Ba Khanh, N., & Pham, V.H. (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.

14. Gopalan, S. H., Suba, S. A., Ashmithashree, C., Gayathri, A., & Jebin Andrews, V. (2019). Digital forensics using blockchain. *International Journal of Recent Technology and Engineering, 8*(2 Special Issue 11), 182–184.

15. Gu, J., Sun, B., Du, X., Wang, J., Zhuang, Y., & Wang, Z. (2018). Consortium blockchain-based malware detection in mobile devices. *IEEE Access, 6*, 12118–12128.

16. Homayoun, S., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2019). A blockchain- based framework for detecting malicious mobile applications in App stores. In *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)* (pp. 1–4). IEEE.

17. Homoliak, I., Venugopalan, S., Hum, Q., Reijsbergen, D., Schumi, R., & Szalachowski, P. (2019). The security reference architecture for blockchains: Towards a standardized model for studying vulnerabilities, threats, and defenses. *arXiv.* https://doi.org/10.1109/COMST.2020.3033665.

18. Hossain, M. M., Hasan, R., & Zawoad, S. (2018). Probe-IoT: A public digital ledger based forensic investigation framework for IoT. In *INFOCOM Workshops* (pp. 1–2).

19. Karie, N. M., & Venter, H. S. (2015). Taxonomy of challenges for digital forensics. *Journal of Forensic Sciences, 60*(4), 885–893.

20. Kerr, M., Han, F. V., & Schyndel, R. (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).

21. Kevin, D., & David, B. (2019). HACIT2: A privacy preserving, region based and blockchain application for dynamic navigation and forensics in VANET. In *International Conference on Ad Hoc Networks* (pp. 225–236). Cham: Springer.

22. Kotsiuba, I., Velykzhanin, A., Biloborodov, O., Skarga-Bandurova, I., Biloborodova, T., Yanovich, Y., & Zhygulin, V. (2018). Blockchain evolution: From bitcoin to forensic in smart grids. In *2018 IEEE International Conference on Big Data (Big Data)* (pp. 3100–3106). IEEE.

23. Le, D. P., Meng, H., Su, L., Yeo, S. L., & Thing, V. (2018). Biff: A blockchain-based iot forensics framework with identity privacy. In *TENCON 2018–2018 IEEE Region 10 Conference* (pp. 2372–2377). IEEE.

24. Li, S., Qin, T., & Min, G. (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.

25. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems, 107*, 841–853.

26. 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.

27. Malamas, V., Dasaklis, T., Kotzanikolaou, P., Burmester, M., & Katsikas, S. (2019). A forensics-by-design management framework for medical devices based on blockchain. In 2019 IEEE World Congress on Services (SERVICES) (Vol. 2642, pp. 35–40). IEEE.

28. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Manubot.

29. Patsakis, C., Dellios, K., De Fuentes, J. M., Casino, F., & Solanas, A. (2019). External monitoring changes in vehicle hardware profiles: Enhancing automotive cyber-security. *Journal of Hardware and Systems Security, 3*(3), 289–303.

30. Pilli, E. S., Joshi, R. C., & Niyogi, R. (2010). Network forensic frameworks: Survey and re-search challenges. *Digital Investigation, 7*(1–2), 14–27.

31. Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. *IEEE Transactions on Emerging Topics in Computing*, 1–1. https://doi.org/10.1109/TETC.2019.2949510.

32. Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the gdpr: Challenges and proposed solutions. *Journal of Cybersecurity, 4*(1), tyy001.

33. Pourvahab, M., & Ekbatanifard, G. (2019): Digital forensics architecture for evidence collection and provenance preservation in iaas cloud environment using sdn and blockchain technology. IEEE Access 7, 153349–153364.

34. Quick, D., & Choo, K. K. R. (2016). Big forensic data reduction: Digital forensic images and electronic evidence. *Cluster Computing, 19*(2), 723–740.

35. Rane, S., & Dixit, A. (2019). BlockSLaaS: Blockchain assisted secure logging-as-a-service for cloud forensics. In *International Conference on Security & Privacy* (pp. 77–88). Singapore: Springer.

36. Ricci, J., Baggili, I., & Breitinger, F. (2019). Blockchain-based distributed cloud storage digital forensics: Where's the beef? *IEEE Security and Privacy, 17*(1), 34–42.

37. Ruan, K., Carthy, J., Kechadi, T., & Baggili, I. (2013). Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digital Investigation, 10*(1), 34–43.

38. Ryu, J. H., Sharma, P. K., Jo, J. H., & Park, J. H. (2019). A blockchain-based decentralized efficient investigation framework for IoT digital forensics. *Journal of Supercomputing, 75*(8), 4372–4387.

39. Samanta, P., & Jain, S. (2018). E-Witness: Preserve and prove forensic soundness of digital evidence. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking* (pp. 832–834). ACM.

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

41. Tian, Z., Li, M., Qiu, M., Sun, Y., & Su, S. (2019). Block-DEF: A secure digital evidence framework using blockchain. *Information Sciences, 491*, 151–165.

42. Weilbach, W. T., & Motara, Y. M. (2019). Distributed ledger technology to support digital evidence integrity verification processes. In *International Information Security Conference* (pp. 1–15). Cham: Springer.

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

44. Yousaf, H., Kappos, G., & Meiklejohn, S. (2019). Tracing transactions across cryptocurrency ledgers. In *28th {USENIX} Security Symposium ({USENIX} Security 19)* (pp. 837–850).

45. Zhang, Y., Wu, S., Jin, B., & Du, J. (2017). A blockchain-based process provenance for cloud forensics. In *2017 3rd IEEE International Conference on Computer and Communications (ICCC)* (pp. 2470–2473). IEEE.

46. Zou, R., Lv, X., & Wang, B. (2019). Blockchain-based photo forensics with permissible trans-formations. *Computers and Security, 87*, 101567.