Blockchain-Based Chain of Custody for Digital Evidence with Hyperledger Fabric

1st Leandro Loffi
Department of Post-Graduate Program in Computer Science
Federal University of Santa Catarina (UFSC)
PO Box 476 - 88040-970 - Florianópolis - SC - Brazil
leandro.loffi@posgrad.ufsc.br
0000-0003-3725-7427

2nd Gerson Luiz Camillo
Department of Post-Graduate Program in Computer Science
Federal University of Santa Catarina (UFSC)
PO Box 476 - 88040-970 - Florianópolis - SC - Brazil
gerson.camillo@ufsc.br
0000-0003-2268-3722

3rd Carla Merkle Westphall
Department of Post-Graduate Program in Computer Science
Federal University of Santa Catarina (UFSC)
PO Box 476 - 88040-970 - Florianópolis - SC - Brazil
carla.merkle.westphall@ufsc.br
0000-0002-5391-7942

4th Carlos Becker Westphall
Department of Post-Graduate Program in Computer Science
Federal University of Santa Catarina (UFSC)
PO Box 476 - 88040-970 - Florianópolis - SC - Brazil
carlos.westphall@ufsc.br
0000-0002-5391-7942

***Abstract*—The increasing presence of digital evidence in legal, criminal, and civil cases requires adaptations to traditional chain-of-custody processes to ensure the integrity of this evidence. This work proposes the use of blockchain technology, specifically through Hyperledger Fabric, to strengthen the chain of custody for digital evidence. The developed solution employs smart contracts to immutably record each stage of evidence handling, from collection to transfer of custody, ensuring data authenticity, integrity, and traceability. Our implementation demonstrates that blockchain technology can significantly reduce the risk of evidence tampering, improve process efficiency, and facilitate audits, thereby contributing to greater reliability in the presentation of evidence during judicial proceedings.**

***Index Terms*—Chain of Custody, Blockchain, Hyperledger Fabric, Digital Evidence**

I. Introduction

Digital information is pervasive in our lives and businesses, significantly impacting how data is created, stored, and shared. In the judicial context, such data are increasingly present in criminal and civil proceedings and are referred to as digital evidence when linked to an investigation case [1], [2].

The chain of custody is part of the digital evidence collection phase in criminal or civil investigations and consists of a series of procedures aimed at ensuring the integrity of evidence in judicial processes [3]. These actions are performed sequentially to guarantee that the collected evidence remains unaltered, preventing compromise in legal proceedings. In summary, the chain of custody is a process designed to document the chronological history of digital evidence, ensuring its traceability [4].

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001, and Federal University of Santa Catarina.

The data that must be recorded in a chain of custody should answer a set of questions known as the 5WH (5W and 1H), that is, five W questions (*Who, What, When, Where, and Why*) and one H question (*How*) [5], [6]. The data and information to answer these questions should be recorded in the chain of custody. Below is the list of questions with their meanings [7]:

- **Who** had contact with, handled, or discovered the evidence;
- **What** alterations or procedures were performed on the evidence;
- **When** the evidence was discovered, accessed, examined, or transferred;
- **Where** the discovery, collection, examination, and storage of evidence took place;
- **Why** the evidence was collected, that is, the motivation and, if possible, the authority determining the collection; and
- **How** the circumstances of the discovery, collection, examination, and storage of evidence occurred.

Metadata (data about data) stored in a digital chain of custody must ensure certain security properties, as defined by Bonomi, Casini, and Ciccotelli [8]: integrity, traceability, authentication, verifiability, and security (proof of alterations). In this context, blockchain becomes essential, enhancing security through encryption and methods such as hash functions, enabling the chaining of information and, being decentralized, ensuring data consistency [9], [10].

When discussing blockchain, security, and chain of custody, one observes a harmony among them, as the chain of custody is directly linked to the security of digital evidence. Therefore, blockchain and its technologies emerge as effective solutions to address common problems in the traditional chain of

custody [11].

This leads to the research problem: *How can blockchain technology be applied to strengthen the integrity of the chain of custody of digital evidence, reducing the risk of tampering and ensuring the chronological accuracy of data presented in judicial proceedings?* Therefore, this article aims to identify how blockchain can assist in ensuring the integrity of evidence in criminal and civil proceedings.

To address this problem, a literature review was conducted, contributing to a better understanding of the breach of the chain of custody—when any alteration occurs in the evidence before, during, or after forensic analysis. This also involves the path of data and documents, the identification of the history and chronology of the chain of custody, which guarantee the authenticity of the traces presented in court.

In light of this, it becomes necessary to study, analyze, and possibly apply blockchain as support to assist in the custody of evidence, eliminating doubts and risks of tampering [12], [13]. With blockchain, it is possible to trace a reliable path and history, as well as properly handle information, ensuring the chronological correctness of the manipulated data [14], [15].

The principal innovation of this research is the practical integration of blockchain technology—specifically Hyperledger Fabric—to strengthen the digital evidence chain of custody. Departing from purely theoretical models, this study offers a fully operational implementation that utilizes smart contracts to immutably record every phase of evidence handling, from initial acquisition through subsequent custody transfers.

II. Related Work

Several studies have explored the use of blockchain technology as a tool to ensure the integrity of the chain of custody in digital forensic contexts. This section presents a review of relevant works, highlighting contributions, challenges, and gaps in the practical application of this technology.

Machin Guardia [16], in his thesis, explores the applicability of blockchain in forensic custody, highlighting the importance of its application to ensure the validity of evidence in judicial proceedings. The author describes how the implementation of the chain of custody can be efficient and secure, standardizing communication between the entities involved and preventing external alterations to the process. Additionally, he suggests that his Chain of Custody (CoC) solution can reduce the resources needed to protect information against modifications by users or attackers.

In the same context, Hermeiro [17] emphasizes the importance of the hash code in preserving the chain of custody of digital evidence. Any alteration in the original code would generate a noticeable modification, breaking the chain of custody and invalidating the evidence. The author highlights the hash code as a guarantee of security and integrity and suggests that the introduction of blockchain technology could further strengthen the chain of custody, preserving and authenticating digital evidence in judicial proceedings.

Medina [18] addresses the challenges of implementing blockchain with the goal of ensuring the integrity and reliability of evidence, recognizing the complexity due to the need to work with data security and integrity. He proposes the use of permissioned blockchain and smart contracts to track changes in evidence ownership throughout its lifecycle, highlighting the potential of this technology to simplify evidence tracking effectively and accurately.

Khan et al. [14] point out the difficulties in the field of digital forensic analysis, especially due to the volatility of information and the ease with which data can be transferred to other jurisdictions. Therefore, they highlight the need to ensure the integrity and confidentiality of digital evidence.

Ali et al. [19] present the use of a forensic chain prototype based on Hyperledger Composer with the aim of preserving the obtained data, contributing to the discussion on practical implementations of blockchain in the chain of custody.

Some works centralize the CoC process around specific cases, supporting all phases of the forensic process up to the preparation of the final report [10], [20]–[22]. Others focus on handling individual digital traces, aiming to ensure the integrity and immutability of data from different sources [11], [23].

Regarding the complete management of the chain of custody, there are comprehensive proposals that cover all phases of the forensic process and meet security requirements [3], [10], [20], [22], [24]–[29].

Despite the advances, significant gaps are identified in the literature. One of them is the lack of practical implementation or evaluation in real environments in many articles. For example, Sathyaprakasan et al. [30] and Chen et al. [21] developed frameworks but did not conduct experiments or simulations to validate the feasibility and performance of their proposals, raising questions about their applicability in the real world.

Another challenge is the need for complete traceability of the chain of custody without compromising the privacy of the parties involved. Proposals like that of Zhang et al. [9], which offer traceability, provide promising solutions, but the cryptographic complexity can hinder large-scale implementation.

Transactional costs and performance remain challenges, especially in public blockchains [22], [28]. The use of permissioned blockchains partially solves this issue but brings challenges in terms of interoperability and access control between different platforms.

In summary, although the literature presents several proposals for applying blockchain in the chain of custody, significant challenges remain to be overcome, including practical implementation, management of cryptographic complexities, ensuring confidentiality and privacy, and issues of performance and interoperability.

III. Proposed Solution

Considering the ease with which evidence can be tampered with during custody, it becomes necessary to have a solution that ensures the authenticity, integrity, confidentiality, and security of such artifacts in cases of legal infractions.

In this context, the use of blockchain technology emerges as a useful method to guarantee the veracity of digital evidence.

It allows for securing, encrypting, and storing data so that it cannot be tampered with or illegally accessed without permission.

In this work, Hyperledger Fabric is utilized with the aim of controlling access to stored data through encrypted access keys, as well as monitoring who accessed them and what actions were taken with these data.

The blockchain was implemented using the JavaScript programming language, a specific chaincode, a gateway and a frontend for connection and visualization were developed.

Interaction with the blockchain occurs via an API. The front-end was developed using Svelte and Vite. It allows users to create new items, list all items, and transfer custody. These operations are performed via HTTP requests to the Node.js server using the `fetch` API.

The back-end (`app.js`) processes the requests made by the front-end, using Express.js to define the endpoints that the requests access. When one of these requests is received, `app.js` processes it and interacts with the Hyperledger Fabric network to execute the corresponding commands. The results are returned to the front-end in JSON format.

There is also the smart contract (`assetTransfer.js`), which is the code that defines the transactions that can be performed on Hyperledger. This contract contains the necessary functions that the back-end calls in response to the front-end requests, which are:

- `InitLedger`: Initializes with a set of items within the blockchain to demonstrate the start, as shown in Figure 1.
- `GetAllAssets`: Reads all items present in the chaincode, as shown in Figure 2.
- `CreateAsset`: Responsible for adding a new item with its respective attributes, as shown in Figure 3.
- `UpdateAsset`: Allows you to change all Asset items, but the change status remains stored, as shown in Figure 4.
- `TransferAsset`: Responsible for transferring custody of a given item with id, as shown Figure 5.

```
async InitLedger(ctx) {
    const assets = [
        {
            ID: '1',
            Who: 'Gerson',
            What: 'Storage HD-500GB',
            When: '2024-12-04T12:00:00Z',
            Where: 'Korea',
            Why: 'Evidence collection',
            How: 'Forensic Method',
        },
    ];

    for (const asset of assets) {
        asset.docType = 'asset';
        await ctx.stub.putState(asset.ID, Buffer.from
        (stringify(sortKeysRecursive(asset))));
    }
}
```

Fig. 1. InitLedger.

To run the blockchain, you need to initialize Hyperledger with a network, have `Node.js`, `Express.js`, and svelte

```
async GetAllAssets(ctx) {
    const allResults = [];
    const iterator = await ctx.stub.getStateByRange('', '');
    let result = await iterator.next();
    while (!result.done) {
        const strValue = Buffer.from(result.value.value.
        toString()).toString('utf8');
        let record;
        try {
            record = JSON.parse(strValue);
        } catch (err) {
            console.log(err);
            record = strValue;
        }
        allResults.push(record);
        result = await iterator.next();
    }
    return JSON.stringify(allResults);
}
```

Fig. 2. GetAllAssets.

```
async CreateAsset(ctx, id, who, what, when, where, why, how){
    const exists = await this.AssetExists(ctx, id);
    if (exists) {
        throw new Error(`The asset ${id} already exists`);
    }

    const asset = { ID: id, Who: who, What: what, When: when,
    Where: where, Why: why, How: how };
    await ctx.stub.putState(id, Buffer.from(stringify
    (sortKeysRecursive(asset))));
    return JSON.stringify(asset);
}
```

Fig. 3. CreateAsset.

```
async UpdateAsset(ctx, id, who, what, when, where, why, how){
    const exists = await this.AssetExists(ctx, id);
    if (!exists) {
        throw new Error(`The asset ${id} does not exist`);
    }

    const updatedAsset = { ID: id, Who: who, What: what,
    When: when, Where: where, Why: why, How: how };
    await ctx.stub.putState(id, Buffer.from(stringify
    (sortKeysRecursive(updatedAsset))));
    return JSON.stringify(updatedAsset);
}
```

Fig. 4. UpdateAsset.

```
async TransferAsset(ctx, id, newOwner, when) {
    const exists = await this.AssetExists(ctx, id);
    if (!exists) {
      throw new Error(`The asset ${id} does not exist`);
    }

    const assetJSON = await ctx.stub.getState(id);
    const asset = JSON.parse(assetJSON.toString());

    asset.Who = newOwner;
    asset.When = when;

    await ctx.stub.putState(id, Buffer.from(stringify
    (sortKeysRecursive(asset))));
    return JSON.stringify(asset);
}
```

Fig. 5. TransferAsset.

installed. The `Node.js` API can be accessed on port 3000,

and svelte on port 5173.

Figure 6 shows the main screen with the blockchain functionalities. Figure 7 shows the screen for creating an asset. Figure 8 shows the display screen for all assets. Figure 9 shows the asset custody transfer screen.

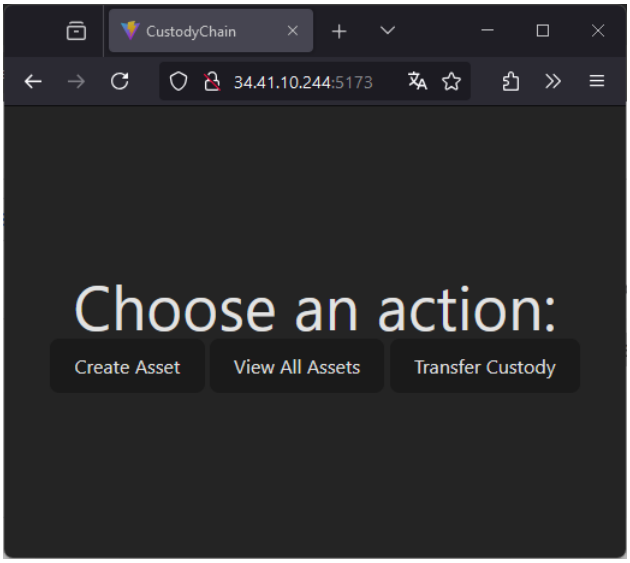

Fig. 6. Screen with blockchain functionalities.

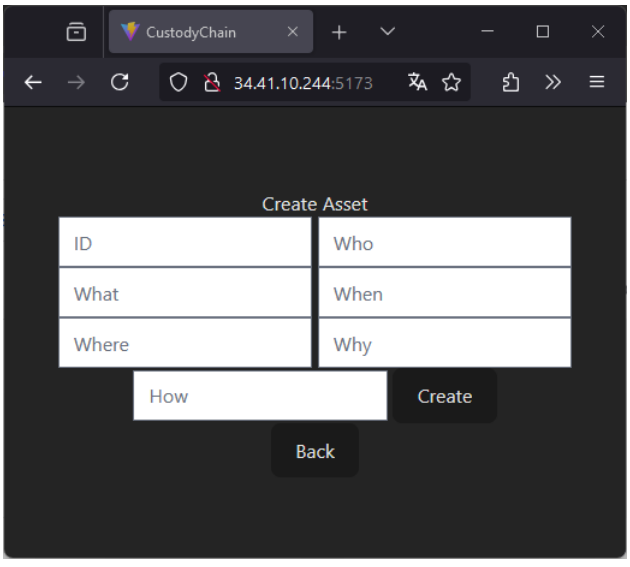

Fig. 7. Asset creation screen.

All the requirements and files needed to make it work are available on https://github.com/leandroloffi/CustodyChain.

IV. Results

During the execution of the Hyperledger network, the period between three and two minutes corresponds to the network's activation phase. After this initial interval, once the runtime falls below two minutes, the network is fully operational,

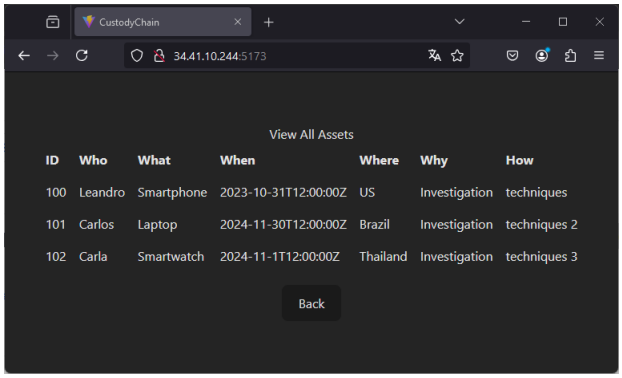

Fig. 8. All Assets screen.

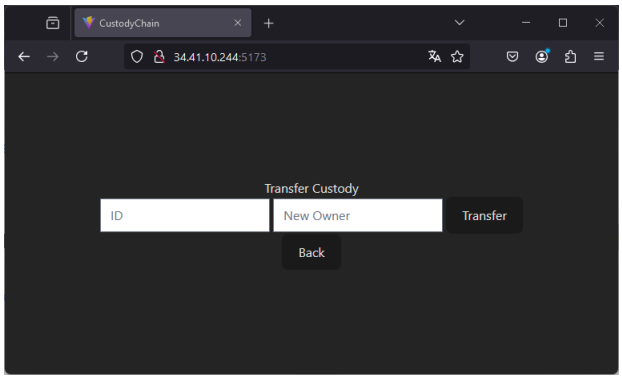

Fig. 9. Transfer Custody screen.

and the designated functions are actively running. At this stage, the memory usage stabilizes, exhibiting an increase of approximately 0.3 GB compared to baseline conditions. The network traffic exhibits fluctuations that only become discernible during the network activation phase, as illustrated in Figure 10 and Figure 11.

The implemented blockchain ensures data security by using various internal functionalities to record each movement of the evidence under custody. Thus, any movement of the custodial object is recorded on the blockchain, as well as any changes in custodian.

In this way, the chronological accuracy of the data is ensured, since when a block is added to the blockchain, it cannot be altered without all the other blocks also being modified.

Moreover, as it is a blockchain, the inserted records cannot be altered, as they are maintained on multiple computers distributed across a network, which ensures the integrity of the information and protects the evidence against tampering.

Given this characteristic of immutability of records on the blockchain, there is a significant reduction in the risk of tampering with the custodial evidence, thus ensuring greater reliability in using the evidence as procedural proofs.

Another benefit is the possibility of tracking the movements of evidence within the chain of custody, ensuring transparency

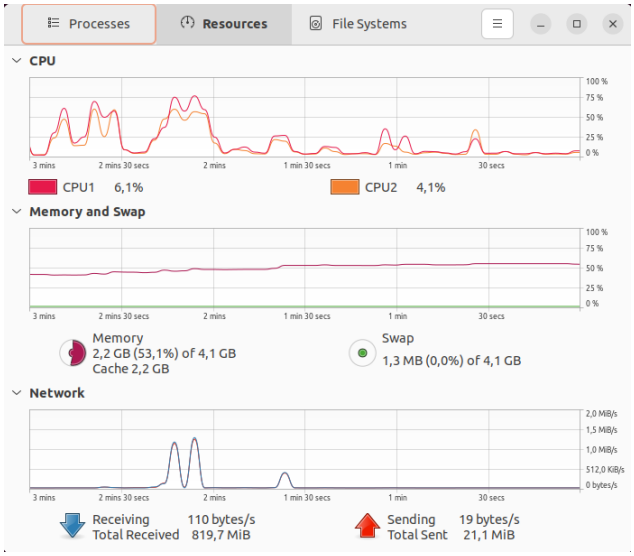

Fig. 10. Running blockchain performance.

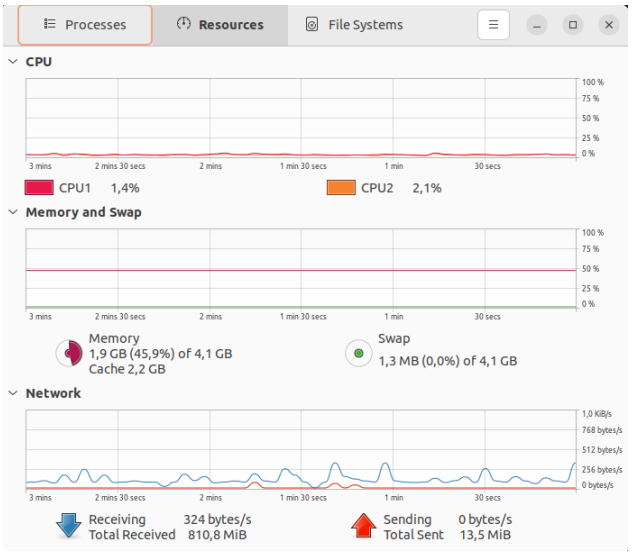

Fig. 11. Blockchain performance with downgraded network.

and facilitating any eventual audit in case of judicial challenge.

It was also observed that the implementation of blockchain can make the chain of custody procedure more efficient, as it automates the transfer stage between custodians without the need for physical document signatures, which also reduces costs.

One of the key strengths of our article is its emphasis on practical application. By utilizing a variety of tools, we empirically demonstrate the feasibility of conducting the proposed practical demonstration. This hands-on approach not only validates our theoretical concepts but also showcases their applicability in real-world scenarios, thereby bridging the gap between theory and practice.

V. Conclusion

In this article, we sought to understand how blockchain technology can be applied to strengthen the integrity of the chain of custody of forensic evidence, reducing the risk of tampering and ensuring the chronological accuracy of data presented in judicial proceedings.

After conducting a survey of relevant information through the analysis of related works, we chose to use a blockchain based on Hyperledger Fabric to control the movements of evidence within a proposed chain of custody.

Several benefits were observed with the implementation of blockchain in the chain of custody, such as data security and integrity, guarantee of chronological accuracy, and reduction of the risk of evidence tampering through the immutability of records on the blockchain. It was also found that blockchain facilitates audits through the ability to track movements made, in addition to making the chain of custody more efficient.

Finally, possible future applications of blockchain technology in the forensic area were identified, such as automation through smart contracts, aiming to facilitate the automatic transfer of custody based on predefined conditions, and integration with IoT to physically track evidence and ensure its integrity from the collection site to final storage.

As future work, it is proposed to translate the solution into other languages, in addition to developing an improvement for other functions in the front-end to search for chain of custody cases from different institutions, in addition to developing a specific network for each case.

References

[1] A. Espindula, Perícia criminal e cível: uma visão geral para peritos e usuários da perícia, 4th Edition, Editora Millenium, Campinas, SP, 2013.

[2] V. P. Stumvoll, Criminalística, 7th Edition, Editora Millenium, Campinas, SP, 2019.

[3] H. M. Elgohary, S. M. Darwish, S. M. Elkaffas, Improving Uncertainty in Chain of Custody for Image Forensics Investigation Applications, IEEE Access 10 (2022) 14669–14679. doi:10.1109/ACCESS.2022.3147809.

[4] A. Araujo, M. Monteiro, L. A. Martins, Informática forense, 1st Edition, Vol. 2, Editora Leud, São Paulo, 2018.

[5] T. F. Gayed, H. Lounis, M. Bari, Cyber Forensics: Representing and (Im)Proving the Chain of Custody Using the Semantic Web, in: COGNITIVE 2012: The Fourth International Conference on Advanced Cognitive Technologies and Applications, Citeseer, 2012, pp. 19–23.

[6] J. Ćosić, Z. Ćosić, M. Bača, An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence, Journal of Information and Organizational Sciences 35 (1) (2011) 1–13.

[7] ABNT - Associação Brasileira de Normas Técnicas, ABNT NBR ISO/IEC 27037, Rio de Janeiro, RJ (2013).

[8] S. Bonomi, M. Casini, C. Ciccotelli, B-CoC: A Blockchain-Based Chain of Custody for Evidences Management in Digital Forensics, in: International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2019), Vol. 71 of Open Access Series in Informatics (OASIcs), Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2020, pp. 12:1–12:15. doi:10.4230/OASIcs.Tokenomics.2019.12.

[9] Y. Zhang, H. Lei, B. Wang, Q. Wang, N. Lu, W. Shi, B. Chen, Q. Yue, Traceable ring signature schemes based on SM2 digital signature algorithm and its applications in the data sharing scheme, Frontiers of Computer Science 18 (2) (2024) 182815.

[10] A. J. Akbarfam, M. Heidaripour, H. Maleki, G. Dorai, G. Agrawal, ForensiBlock: A Provenance-Driven Blockchain Framework for Data Forensics and Auditability, in: 2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 2023, pp. 136–145. doi:10.1109/TPS-ISA58951.2023.00025.

[11] S. Li, T. Qin, G. Min, Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems, IEEE Transactions on Computational Social Systems 6 (6) (2019) 1433–1441. doi:10.1109/TCSS.2019.2927431.

[12] D. Rodeck, B. Curry, What is blockchain, Forbes (2022).

[13] J. M. Ramos, R. H. Cabral, Percepções de colaboradores de certificação digitalacerca das influências da criação de uma identidade digital baseada em blockchain no comércio de certificados digitais, PERCEPÇÕES DE COLABORADORES DE CERTIFICAÇÃO DIGITALACERCA DAS INFLUÊNCIAS DA CRIAÇÃO DE UMA IDENTIDADE DIGITAL BASEADA EM BLOCKCHAIN NO COMÉRCIO DE CERTIFICADOS DIGITAIS (2021).

[14] A. A. Khan, M. Uddin, A. A. Shaikh, A. A. Laghari, A. E. Rajput, Mf-ledger: blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture, IEEE Access 9 (2021) 103637–103650.

[15] R. Sobti, G. Geetha, Cryptographic hash functions: a review, International Journal of Computer Science Issues (IJCSI) 9 (2) (2012) 461.

[16] D. Machín Guardia, et al., Blockchain para la cadena de custodia en análisis forense (2020).

[17] A. C. C. Hermeiro, A cadeia de custódia da prova digital: O uso da tecnologia blockchain como forma de preservação, Master's thesis (2023).

[18] G. A. Medina, Os desafios e avanços para implementação da tecnologia de blockchain na cadeia de custódia das provas no brasil (2021).

[19] M. Ali, A. Ismail, H. Elgohary, S. Darwish, S. Mesbah, A procedure for tracing chain of custody in digital image forensics: A paradigm based on grey hash and blockchain, Symmetry 14 (2) (2022) 334.

[20] P. Black, I. Gondal, R. Brooks, L. Yu, AFES: An Advanced Forensic Evidence System, in: 2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW), 2021, pp. 67–74. doi:10.1109/EDOCW52865.2021.00034.

[21] S. Chen, C. Zhao, L. Huang, J. Yuan, M. Liu, Study and implementation on the application of blockchain in electronic evidence generation, Forensic Science International: Digital Investigation 35 (2020) 301001.

[22] M. Li, C. Lal, M. Conti, D. Hu, LEChain: A blockchain-based lawful evidence management scheme for digital forensics, Future Generation Computer Systems 115 (2021) 406–420.

[23] K. Awuson-David, T. Al-Hadhrami, M. Alazab, N. Shah, A. Shalaginov, BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem, Future Generation Computer Systems 122 (2021) 1–13.

[24] M. Li, Y. Chen, C. Lal, M. Conti, M. Alazab, D. Hu, Eunomia: Anonymous and Secure Vehicular Digital Forensics Based on Blockchain, IEEE Transactions on Dependable and Secure Computing 20 (1) (2023) 225–241. doi:10.1109/TDSC.2021.3130583.

[25] M. Li, J. Weng, J.-N. Liu, X. Lin, C. Obimbo, Toward Vehicular Digital Forensics From Decentralized Trust: An Accountable, Privacy-Preserving, and Secure Realization, IEEE Internet of Things Journal 9 (9) (2022) 7009–7024. doi:10.1109/JIOT.2021.3116957.

[26] A. H. Lone, R. N. Mir, Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer, Digital investigation 28 (2019) 44–55.

[27] M. Lusetti, L. Salsi, A. Dallatana, A blockchain based solution for the custody of digital files in forensic medicine, Forensic Science International: Digital Investigation 35 (2020) 301017.

[28] A. O. Philip, R. K. Saravanaguru, Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era, Journal of King Saud University-Computer and Information Sciences 34 (7) (2022) 4031–4046.

[29] Sakshi, A. Malik, A. K. Sharma, Blockchain-based digital chain of custody multimedia evidence preservation framework for internet-of-things, Journal of Information Security and Applications 77 (2023) 103579.

[30] R. Sathyaprakasan, P. Govindan, S. Alvi, L. Sadath, S. Philip, N. Singh, An Implementation of Blockchain Technology in Forensic Evidence Management, in: 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2021, pp. 208–212. doi:10.1109/ICCIKE51210.2021.9410791.