The Application of Blockchain to the Chain Of Custody of Judicial Evidence

H. Beatriz P. de Gallo
Faculty of Engineering
Universidad Católica de Salta
Salta, Argentina
bgallo@ucasal.edu.ar

Oscar Carlos Medina
Faculty of Engineering
Universidad Tecnológica Nacional
Córdoba, Argentina
omedina@frc.utn.edu.ar

John Grover Dorado
Faculty of Engineering
Universidad Católica de Salta
Salta, Argentina
jdorado@ucasal.edu.ar

José Aráoz Fleming
Faculty of Engineering
Universidad Católica de Salta
Salta, Argentina
jdaraoz@ucasal.edu.ar

Carlos Párraga
Faculty of Engineering
Universidad Católica de Salta
Salta, Argentina
cdparraga@ucasal.edu.ar

Enzo Ruben Notario
Faculty of Engineering
Universidad Católica de Salta
Salta, Argentina
ernotario@ucasal.edu.ar

Ernesto Sanchez
Faculty of Engineering
Universidad Católica de Salta
Salta, Argentina
esanchez@ucasal.edu.ar

***Abstract*— This article explores the application of Blockchain technology to the Chain of Custody of Judicial Evidence. The admissibility of evidence –considering the integrity, confidentiality, and reliability of an item of evidence in a trial– is fundamentally important to administer justice. The objective set in this paper is to define an architectural model for the implementation of smart contracts for the safe recording of the Chain of Custody of Judicial Evidence, taking advantage of the traceability and security features of Blockchain technology, and avoiding the risks of non-admissibility of evidence to which the current Chain of Custody Records are exposed. The conceptual model is described, but the implementation of this methodology is still being developed.**

Keywords—Blockchain, Chain of Custody, Judicial Evidence, Smart Contract, Traceability

I. INTRODUCTION

The evidence or proof validly presented in a judicial process is fundamentally important, as they are the most objective and concrete way of obtaining fair sentences. Therefore, it is necessary to resort to safe procedures for the correct handling of the evidence. Blockchain technology is useful and adequate to create a careful and meticulous record of the people who handle the evidence and contribute to the "admissibility of evidence" in a judicial process.

To conduct this research, a review of relevant publications was carried out. These works can be used as a basis to work on the most important aspects of the application of Blockchain in the field of Justice.

The objective of this work is to develop an architectural model that allows the implementation of smart contracts for the safe recording of events in the Chain of Custody of Judicial Evidence. The results obtained in the design and development of the conceptual model are described. However, the implementation phase of the proposed methodology has not been completed yet.

This paper is organized as follows: Section II describes the relevant characteristics of the Chain of Custody and Blockchain technology. Section III discusses the state of the art about the connection between Blockchain and judicial processes, and, more specifically, the Chain of Custody. Section IV describes a methodology for Blockchain Architecture Modeling, and Section V explains the use case valid for the Argentinian legal system. Finally, Section VI describes the conclusions of this work.

II. FRAMEWORK

This section describes the judicial procedure known as Chain of Custody, especially its characteristics, problems, and other elements relevant to this work. Then, there is a description of Blockchain technology and its characteristics that make it relevant in relation to the Chain of Custody.

A. The Chain of Custody of Judicial Evidence

The evidence validly presented in a judicial process is fundamentally important since it represents a concrete and objective source of information to pronounce appropriate sentences. So, the evidence admissibility –with its principles of integrity, confidentiality, and reliability– is essential to administer justice.

These characteristics of the judicial evidence are entered in a recording procedure called Chain of Custody, which is used for establishing the traceability of the evidence at all times. The Chain of Custody allows to identify where the evidence is, why it is at a certain place, and who is responsible for it. It is common to find paper-based records of the Chain of Custody, but there are a few cases of digital records. In this regard, [1] and [2] point

Research Council of the Catholic University of Salta (Argentine).

out the advantages of developing a computer system that includes agile technologies for the quick identification of evidence (Quick Response codes and barcodes), incorporates relational databases that support the actions performed on the evidence. Moreover, [3] refers to the challenge that digital evidence represents for justice, and proposes Blockchain as a tool to establish the traceability of the events related to the evidence.

The European Union fosters its own project on this subject called LOCARD Project [4], which provides a collaborative and distributed platform to make the recording, analysis, and custody of any type of digital evidence automatic, so that it can be used as valid evidence in court. One of the key factors in this project is the use of Blockchain technology, which, thanks to the data immutability, ensures that the recorded evidence has not been manipulated or forged. This adds a new characteristic to the probationary quality of the evidence in a police or judicial process. Obviously, this recording system can also be applied to material evidence.

The main objective of the Chain of Custody is the constant monitoring of the evidence to ensure that there has been no falsification that could cast doubts on its admissibility as legal evidence. To accomplish this, it is necessary to have safe and reliable techniques for recording each action performed on the evidence, from the moment it is collected to its final storage.

The Chain of Custody involves a series of stages. The first stage begins with the collection of the evidence; it is followed by other different stages depending on the type of evidence that is being handled, and it concludes with its final storage in a Judicial Warehouse. All these stages must be recorded in the Chain of Custody, indicating the person in charge of handling the evidence in each stage, the dates and the conditions of the evidence delivered. Each judicial institution applies a valid procedure to maintain the Chain of Custody and provides sample forms to record the evidence. The procedure explored in this work and the evidence recording form used are the ones established for criminal proceedings by the Public Prosecutor's Office of Argentina [5]. Nevertheless, the proposal of this work can be implemented in other fields (labor, commercial, etc.).

B. Blockchain Technology

The Blockchain technology proposed by Nakamoto [6] has certain characteristics that make it relevant considering the safe tools that can be applied in the field of justice.

Blockchain can be briefly described as a chain of blocks linked by hash pointers, which make a decentralized and distributed network of different members and their transactions. It is a digital ledger. Each member is a node in the network and keeps a copy of the entire ledger. Also, a secure verification system called consensus protocol is used. It does not require the participation of trusted third parties. It has three basic technical principles: a) the replication of the ledger with the record of all the transactions among the members of the network; b) the use of cryptography to ensure the security and privacy of the transactions and to confirm the members' identity; and c) a consensus protocol to establish the rules that regulate the incorporation of new blocks or the modification of the existing ones.

There are very interesting studies about the implementation of Blockchain in non-business environments. In [7], the cases described belong to the fields of Cryptocurrencies, E-Government, Healthcare, Supply Chain, Energy and Banking. Although its application is a challenge in every aspect (security, privacy, latency, and computational cost), Blockchain-based smart contracts are very useful in non-traditional fields such as insurance services, the automotive industry, construction companies and educational institutions, among others. In [8], there is an analysis of an ethical perspective of Blockchain in which the moral dimensions (favorable and unfavorable) of the application of this technology to business are analyzed. What is interesting from this research is the description of the decentralized, democratic, and unmediated nature of Blockchain. Thanks to these characteristics, Blockchain does not originate power asymmetries between the contracting parties. This generates a model of equality and objectivity that is very useful in the field of justice, promoting fairness in the way the evidence is handled.

III. STATE OF THE ART

There are several investigations that address the application of Blockchain in Justice. Here is a brief summary of those relevant to this work.

In [9], the researchers propose the application of Blockchain for the safe storage of records of the access to the judicial information system with the assistance of auditors. The "JusticeChain" project proposes a reliable architectural model based on Hyperledger Fabric with two elements: a blockchain for the system records or logs, and a blockchain for the auditing processes used to examine who has access to the system and how. This model is very useful in institutions where the information system is managed by third parties and there are other interested parties with different roles and levels of trust, as in the case of the Portuguese justice. Research [10] addresses an interesting discussion about the use of Blockchain in dispute resolution processes, also called "judicial mediation". Also, a decentralized justice model that integrates Blockchain, Collective Collaboration and Game Theory is analyzed to find more efficient dispute resolution models that combine the interests of all the parties in safe and impartial conditions.

Regarding Blockchain and the Chain of Custody, several investigations of interest were found. In [11], the authors developed a prototype based on Ethereum for the recording of evidence related to forensics. This research is relevant to this work, since it provides details of an architectural model that could be useful for the design of our solution.

The research conducted in [12] supports the implementation of Blockchain in criminal investigation, especially to the Chain of Custody, and emphasizes the importance knowing this technology, mainly for the justice and the police force. According to this proposal, Blockchain allows to: a) ensure compliance with the principles of digital investigation; b) make multidirectional investigations easier; c) improve the collection of digital evidence with safe methods; and d) develop new solutions for the digital forensic challenges that may arise. These considerations encourage the idea of applying Blockchain in a model focused on people.

Research [13] presents a protocol for the Chain of Custody of digital evidence based on the BLS signature (verifiable random function) to choose a group leader from a random number. The protocol has two elements: a private key generator (which provides new keys for users in a new case) and a user management feature. Something innovative that the protocol includes is its algorithms for three actions that can be performed on the evidence: the visualization, creation and transfer. The research concludes with a reference to the security and performance analysis of the protocol. Although, from a technical point of view, the protocol guarantees the conditions required for the handling of the evidence, it does not include express references to the legal processes involved.

Research [14] proposes a test to confirm whether Blockchain can be applied to the Chain of Custody of digital evidence. This test has six questions about the requirements it should meet: 1) Are there any requirements for storing the state of the evidence? 2) Are there multiple participants in the system? 3) Are trusted third parties given access online? 4) Are all the participants in the system known? 5) Are all the participants in the system trustworthy? and 6) Are there any public verification requirements? The answers to these questions will help us decide whether or not it is possible to apply Blockchain to the Chain of Custody process. The research project finishes with a proposed model based on five elements: the participants, a Front-End developed with Hyperledger Fabric and Hyperledger Composer, the main modules for the interaction in the Blockchain network, a P2P network with consensus protocols, and a distributed warehouse database. The questions to establish the viability of Blockchain and the proposed model are relevant to this research. Also, other considerations in this article relating to procedural law are taken into account for this work.

IV. METHODOLOGY FOR THE BLOCKCHAIN ARCHITECTURAL MODEL

From the five patterns of business models proposed by [15], we considered the Blockchain pattern applied to cryptography-based security for the protection of intangible assets. This is the case of the Chain of Custody records. This model includes technical characteristics of Blockchain and elements of the business model that make it useful to this case. Moreover, it promotes users' secure authentication, regardless of whether they are legal entities or individuals. These users are the ones who provide the assets. Also, additional technological solutions are used; these have security features that make it possible to use services that previously required physical authentication.

Thus, there exist some components that link Blockchain technology with the business model. They form the basis of the architectural that is intended to be modeled in this work. These elements are the following: a) the definition of the business model; b) the identification of the main activities; c) the assets included in the contract; d) the identification of the participants, who are the core of the business model; e) the identification of the states that represent the dynamics of the business model; and f) innovation applied to the business model.

V. DIGITAL RECORD OF THE CHAIN OF CUSTODY OF JUDICIAL EVIDENCE

In order to create a smart contract to record the Chain of Custody of judicial evidence, a first conceptual version of the contract is formulated, highlighting its basic components:

A. The Business Model:

The procedure used for the Chain of Custody is the one established by the Public Prosecutor's Office of Argentina [5]. Moreover, the evidence record form that it provides is also used, applying the necessary modifications to the names of the participants and the activities. Fig. 1 shows this procedure.

B. Activities:

These are the key activities that must be duly recorded in the Chain of Custody:

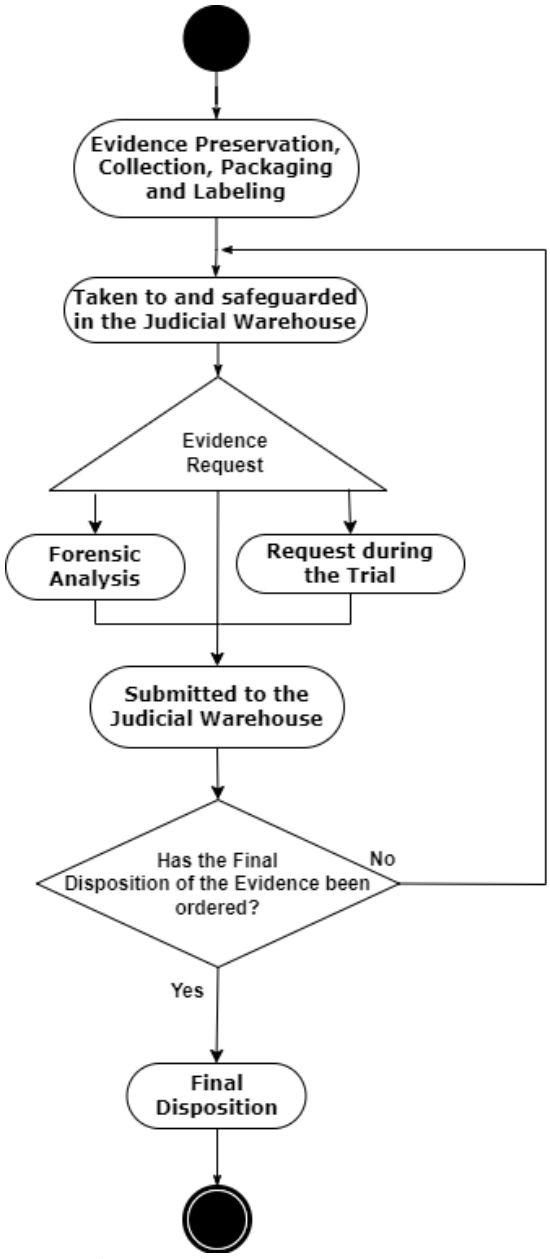

Figure 1: Chain of Custody of the Judicial Evidence

- Preservation, Collection, Packaging and Labeling of the Evidence: these actions are performed by the police officer or person in charge of safeguarding the evidence at the crime scene. In the case of digital evidence, it is the forensic expert who gathes the evidence from the electronic devices provided by one of the parties.
  Here, the collection process must follow all the rigorous steps required by the Chain of Custody.
- Analysis of the Evidence: it is the main activity performed by the Forensic Analyst. The technical conclusions that will be drawn in the production of the expert report are the result of this activity.
- Reception and Custody of the Evidence at the Judicial Warehouse: in addition to verifying the label and packaging of the evidence delivered, the person in charge of the judicial warehouse is responsible for safeguarding the evidence based on its type and nature, and ensuring its integrity, authenticity and origin.
- Request at the Trial: sometimes it is necessary, upon the prosecutors' and parties' request (and with the Judge's authorization), to present the evidence during the trial. For this, the corresponding request must be made and the requirements for the delivery of the evidence must be met.
- Final Disposition of the Evidence: once the evidence has been fully analyzed and its permanent custody is no longer necessary, the judge must decide on its final disposition. They can decide either to destroy it or to deliver it to the original owner.

C. Assets represented in the contract:

For the purposes of this paper, the record form included in [5] will be used as described on pages 55 to 57 of that document. The elements represented in the contract are the following:

- Identification of the Chain of Custody Record: it consists in a QR code with access to evidence identification data. Its elements are these:
  - A unique identifier of the evidence;
  - A description of the item of evidence;
  - The geographical location where the evidence was collected;
  - The people involved; and
  - A timestamp
- Record of the Evidence Handling:
  - Type of handling: evidence finding, collection, packaging, request, delivery or transfer.
  - Acting person: with a QR code, it is possible to have access to identification details (name and surname, ID number, job position, signature).
  - Descriptive data about the evidence handling: specific information about each action is given.

D. . Participants:

As it is essential that the evidence remains inalterable, it is especially important to identify the people who handle it. Four (4) main users can be identified:

- Evidence Custodian: this is the worker or officer who first comes into contact with the evidence and is responsible for its classification, protection, preservation and packaging.
- Forensic Analyst: this is not necessarily the same person who acts as the Evidence Collector. Their task is to examine the evidence to decide whether it is relevant to the case and to find circumstantial information, based on the items subject to examination requested by the Judge.
- Judicial Officers: the judges and the prosecutors are authorized to use the evidence during the trial, notwithstanding the parties' right to oppose the reception of the evidence.
- Judicial Warehouse Staff: it is the technical personnel responsible for the custody of the evidence at the warehouse..

E. Business Model Phases:

There are four phases in the business model: a) The record of the Chain of Custody; b) The record of the delivery of the evidence to the appropriate person; c) The record of the evidence safekeeping in the warehouse; and d) The record of the final disposition of the evidence.

F. Innovation in the current process:

The application of security technologies is of utmost importance when it comes to preserving evidence, ensuring its admissibility in a judicial proceeding. From this approach, the possible elements that can be innovated in the Chain of Custody are the following:

- Based on the research done to date, there are not any applications developed on Blockchain technology to have been successfully implemented in the Chain of Custody of any type of evidence (material or digital) in the Argentine Justice, so this in a new process in the Argentine judicial context.
- We suggest the implementation of a digital data record because, until now, data have only been recorded manually. For this, it will be necessary to develop applications that are appropriate for the evidence handling in all criminal proceedings, so this record can be applied to other courts.
- The relation between the Chain of Custody Record and other information systems used for record management in the legal system will bring important benefits that will make its strategic, administrative and operational management easier.
- It is possible to prepare statistical and/or analytical reports on evidence and its uses.
- There are other technologies that can reinforce the Blockchain security, such as the user's digital signature and biometric identification. Also, agile technologies for the identification and traceability of evidence (QR and bar code) can be used.
- It is advisable to conveniently redesign the Chain of Custody model to include digital evidence, as the current model is mostly used for biological material evidence.

G. Considerations about technology, Blockchain network and contract programming language:

As this system is restricted to the people involved in a court case, a private Blockchain network is proposed only for users whose identity is known. For data storage, a private Ethereum network is proposed, as it represents an industry standard, and with the new Proof of Stake consensus protocol, it would be more efficient and eco-friendlier.

The data recovery will be made by a back-end smart contract (developed in Solidity) and a front-end application based on 3.0 technologies, as they have a versatile user interface and are widely accepted in the community.

Fig. 2 shows the participants, the business model states, and the processes involved in the conceptual model of the record of the Chain of Custody that is proposed. To date, this project shows the resulting conceptual model that will be used to develop the application prototype before its final version. We suggest that expert users use it in real cases in order to validate it. The project is currently in process, with the participation of researchers from the areas of computer science, criminology, and law, which allows a multidisciplinary approach in the development of the prototype and its final application.

VI. CONCLUSIONS

Blockchain technology is highly suitable to keep records of the Chain of Custody. The security, privacy, traceability, and consensus features of Blockchain reinforce the integrity, confidentiality and availability required for judicial evidence.

The proposed model for the DIGITAL RECORD OF THE CHAIN OF CUSTODY OF JUDICIAL EVIDENCE must continue to be developed until it can be implemented with a prototype. Also, it will certainly be adjusted as the necessary cycles are completed.

Before its implementation, it will be necessary to study the research cited in the state of the art in detail in order to adapt the model to the experiences shared by those authors.

Although the architectural model was based on the Public Prosecutor's Office of Argentina's federal proceedings, there are some minor procedural changes that should be applied when considering the different province's jurisdictions.

In addition, the functional structures and technological infrastructure available in each of them are very different.

This means that, when looking for a use case that is technically and operationally viable, the model will require a systematic process of validation and adjustment carried out by forensic experts and important judicial officers.

The recording of the digital Chain of Custody represents an extra challenge due to the variety and typology of the materials that can be collected at the crime scene. In this sense, the use of electronic devices such as smartphones or computers, which act as silent witnesses, expands the criminal scenario from the material world to the virtual world, introducing the concept of "digital evidence warehouse", which could include Blockchain technology for its protection.

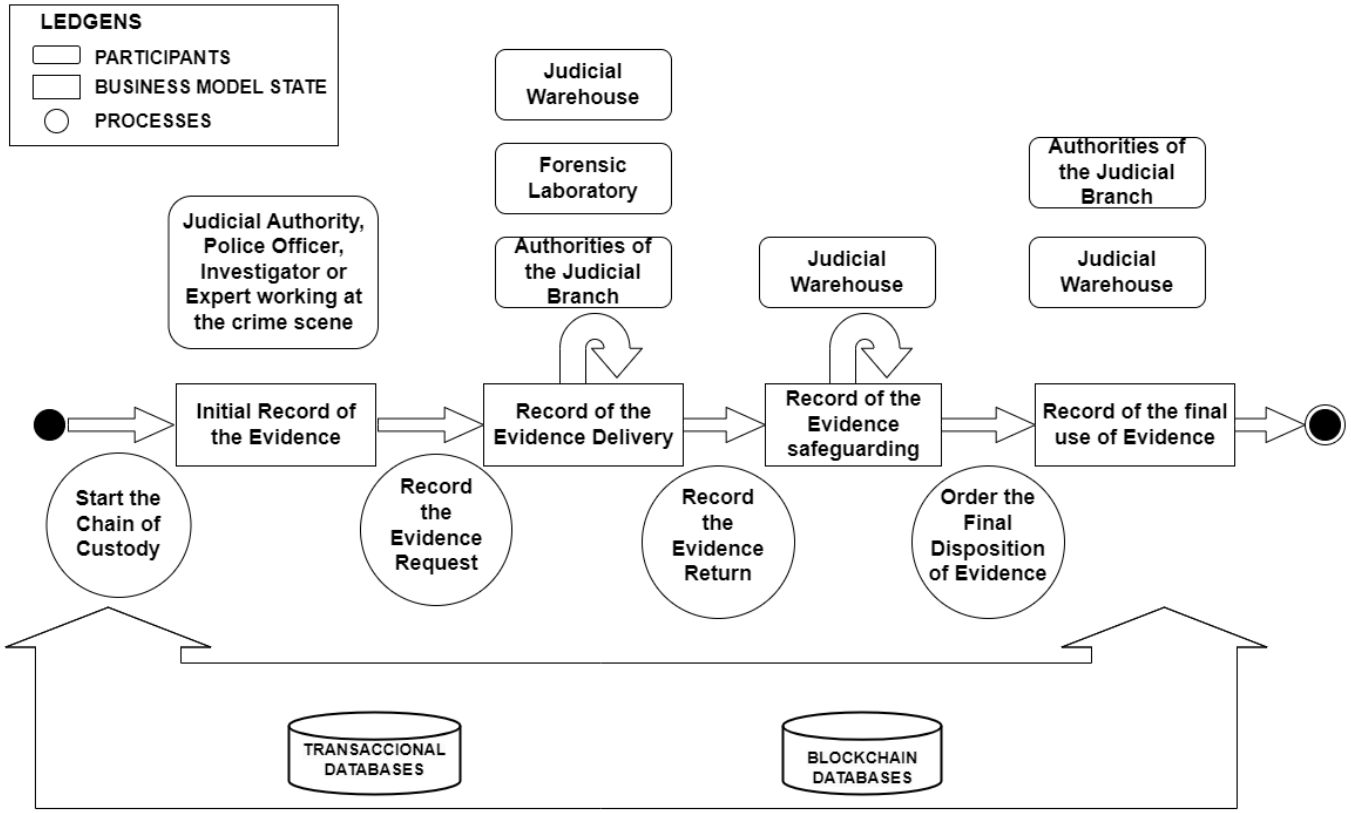

Figure 2: States and processes of the Business Model of the Chain of Custody

REFERENCIAS

[1] C. Aguiar Miranda, A. Montoya Moreno, and F. Rascon Figueroa, "Implementación de un software de registro de cadena de custodia. (Primera parte)," *Visión Criminológica-Criminalistica*, vol. 24, pp. 54–65, 2018.

[2] T. M. Palmbach, *Crime Scene Investigation and Examination: Chain of Evidence*, vol. 1. Elsevier Ltd., 2015. doi: 10.1016/B978-0-12-800034-2.00100-2.

[3] V. Torres Zúñiga, "Aplicaciones de la tecnología blockchain en el Área Forense," no. Mayo. 2019. [Online]. Available: https://www.researchgate.net/profile/V-Torres-Zuniga/publication/350850167_Aplicaciones_de_la_Tecnologia_Blockchain_en_el_Area_Forense/links/6075fd4e299bf1f56d560351/Aplicaciones-de-la-Tecnologia-Blockchain-en-el-Area-Forense.pdf

[4] P. López-Aguilar and A. Solanas, "An Effective Approach to the Cross-Border Exchange of Digital Evidence Using Blockchain," in *Applications in Electronics Pervading Industry, Environment and Society*, 2022, pp. 132–138.

[5] "Manual de Procedimientos del Sistema de Cadena de Custodia," 2015. [Online]. Available: https://www.mpf.gob.ar/capacitacion/files/2015/07/Cadena-de-Custodia.pdf

[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Decentralized Business Review*, p. 21260, 2008, [Online]. Available: https://www.debr.io/article/21260.pdf

[7] I. Konstantinidis, G. Siaminos, C. Timplalexis, P. Zervas, V. Peristeras, and S. Decker, *Blockchain for business applications: A systematic literature review*, vol. 320. Springer International Publishing, 2018. doi: 10.1007/978-3-319-93931-5_28.

[8] C. Dierksmeier and P. Seele, "Blockchain and business ethics," *Business Ethics*, vol. 29, no. 2, pp. 348–359, 2020, doi: 10.1111/beer.12259.

[9] R. Belchior, M. Correia, and A. Vasconcelos, "JusticeChain: Using blockchain to protect justice logs," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11877 LNCS, no. December 2020, pp. 318–325, 2019, doi: 10.1007/978-3-030-33246-4_21.

[10] Y. Aouidef, F. Ast, and B. Deffains, "Decentralized Justice: A Comparative Analysis of Blockchain Online Dispute Resolution Projects," *Frontiers in Blockchain*, vol. 4, no. March, pp. 1–8, 2021, doi: 10.3389/fbloc.2021.564551.

[11] S. Bonomi, M. Casini, and C. Ciccotelli, "B-CoC: A blockchain-based chain of custody for evidences management in digital forensics," *OpenAccess Series in Informatics*, vol. 71, 2020, doi: 10.4230/OASIcs.Tokenomics.2019.12.

[12] H. Al-Khateeb, G. Epiphaniou, and H. Daly, "Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger," *Advanced Sciences and Technologies for Security Applications*, pp. 149–168, 2019, doi: 10.1007/978-3-030-11289-9_7.

[13] W. Yan, J. Shen, Z. Cao, and X. Dong, "Blockchain Based Digital Evidence Chain of Custody," *ACM International Conference Proceeding Series*, pp. 19–23, 2020, doi: 10.1145/3390566.3391690.

[14] A. H. Lone and R. N. Mir, "Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer," *Digit Investig*, vol. 28, pp. 44–55, 2019, doi: 10.1016/j.diin.2019.01.002.

[15] J. Weking, M. Mandalenakis, A. Hein, S. Hermes, M. Böhm, and H. Krcmar, "The impact of blockchain technology on business models – a taxonomy and archetypal patterns," *Electronic Markets*, vol. 30, no. 2, pp. 285–305, 2020, doi: 10.1007/s12525-019-00386-3.