Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 192 (2021) 2779–2788

Procedia Computer Science

www.elsevier.com/locate/procedia

25th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems

# The Application of Blockchain of Custody in Criminal Investigation Process

Fu-Ching Tsai*

*Department of Criminal Investigation, Central Police University, Taoyuan City 33304, Taiwan*

**Abstract**

With the advancing technologies become tools for illicit activities and avoid detection, digital forensics is necessary for law enforcement in modern criminal investigations. In order to maintain the integrity and authenticity of the evidence, a chain of custody is essential for the successful prosecution of criminals in court. However, it is a great challenge to manage the preservation and collection of digital evidence because of its fragile and volatile in nature. Blockchain has been proposed as a promising and reliable technology to provide immutability and traceability of digital content, however, the applications of blockchain to the law enforcement agencies (LEAs) requires special attention to the security issue. In this research, we proposed a blockchain of custody framework to facilitate the security and transparency of digital evidence in criminal investigation process. The framework is implement on Ethereum smart contract to support authenticity and integrity of digital evidence in preliminary investigation, case management and court phases. We also propose the role of investigator to leverage access control in evidence creation, transferring and modification. The corresponding actions with judicial process is simulated using private ethereum blockchain. The experimental results indicate that the proposed framework can prevent digital evidence been tampered or contaminated and assure its legal defensibility with rigorous privilege management. Moreover, by successfully synchronizing digital evidence transactions to multiple nodes ensures the accountability of evidence data for every involved law enforcement agency.



*Keywords:* Blockchain; Smart Contract; Digital evidence; Chain of Custody

* Corresponding author. Tel.: +886-3-3282321; fax: +886-3-328.4118
*E-mail address:* fctsai@mail.cpu.edu.tw


10.1016/j.procs.2021.09.048

## 1. Introduction

Given the current popularity of 3C products, modern technologies are commonly used to commit more sophisticated crimes. Therefore, how to properly collect digital evidence plays an important role in the criminal investigating tasks. The process of digital forensic begins from the scene and the proof of the case must be placed before the trier of fact for consideration. Due to the circumstantial and fragile nature of digital evidence, any unexpected alternation may cause the great damage and impede their reliability. More importantly, the subtle changes, whether it is man-made, accidents or nature disasters in the digital form are difficult to detect and easily ignored by forensic officers.

Chain of custody is crucial to declare the authentication of evidence and to convince the trier of fact. The traditional chain of custody is mainly operated by paper base systems. The police officers or people who take charge of the evidence provide their signature to ensure the reliable of the data when delivering the items to the next stage. Further, by tracking the well documented chronological delivery route allowing the trier of fact to trace and identify the factuality of evidence regardless of different organizations involved in the whole transmitting process. However, the paper-based chain of custody is solid inadequate to guarantee the provenance and integrity of digital evidence [1]. Crime facts which stored or transmitted in digital form suffers from the challenges due to the speed, anonymity and the volatile nature of digital evidence. While traditional paper-based chain of custody requires long period of time and huge human resources to demonstrate the legality at court, the tedious and time consuming process may lose the opportunity to solve the case by fast examining the digital evidence. Thus, developing a framework to deliver and preserve digital evidence more efficiently is an important issue in forensic field.

Blockchain has features include decentralization, integrity, traceability and consistency, which are also required by traditional chain of custody . Moreover, smart contract development in blockchain contributes the access control mechanism to distinguish the rights between dispatch officer and other general staff on handling the digital evidence. Building a precise access control framework is essential in judicial procedures to avoid evidence destruction and privacy violation. In this study, we propose a blockchain of custody framework that combines various privilege design of smart contract to identify different roles in judicial procedures . The framework is composed of three phases, which are preliminary investigation, case management and court phase. In preliminary investigation phase, the dispatched law enforcement officers are allowed to upload digital evidence hash value to the blockchain. In case management phase, the relevant personnel acquire different permissions according to the design of smart contract. Finally, in court phase, the trier of fact can verify the integrity of evidence by comparing hash value with the previous calculated value. The reminder of this paper is organized as follows: Section 2 provides a review of blockchain and smart contract in digital forensic applications. Section 3 describes our proposed blockchain of custody architecture and privilege design based on smart contract principles. Section 4 demonstrate the implementing process and system outcomes. Finally, the last section concludes the paper, and makes some suggestions for future work.

## 2. Literature review

### *2.1. Digital evidence and chain of custody*

The chain of custody refers to the process of recording the state of evidence in chronological order during the investigation. According to the U.S. National Institute of Justice (NIJ) defines chain of custody as “a process used to maintain and document the chronological history of the evidence” [1]. The chain of custody plays a pivotal role throughout the investigation. The integrity of the evidence must be maintained according to the first discovery, until later submitted to the court. If the process of supervision is contaminated, the hard-earned evidence will not be accepted. Therefore, the chain of custody must document evidence at any stage of the investigation process, from the acquisition, collection, evidence analysis, and the units that deliver the evidence to the laboratory, as well as the information of time, place, cause and manner of use of the evidence [5].

In the modern digital age, with the increasing of cybercrime activities, the complexity of digital evidence makes it harder to create and maintain a reliable chain of custody. Compared to traditional evidence, digital evidence has many unique characteristics, such as easy to be copied, transmitted, modified and contaminated. Since most valuable data in a digital form are time sensitive, recording timestamps becomes a critical factor to govern the proof of facts in a legal proceeding. In addition, modern criminals are often dominated by cross-border organizations. They often utilize the

conflicts over prescriptive jurisdiction in different countries to avoid law enforcement investigation. Thus, developing a blockchain of custody framework which supports cross-border criminal intelligence sharing and collaboration is the trend to fight against crime internationally [5].

### *2.2. Blockchain technology*

The birth of the blockchain subverts the traditional trading model and develops new applications in different industries. Regardless of how the blockchain evolves, its operating principles are similar. The followings are three fundamental concepts of blockchain theory.

- Peer-to-peer (P2P) architecture: The blockchain itself is a distributed database in which participants of each node can trade digital assets and store transaction records through the P2P network .

- The blockchain stores messages in a timestamp and transaction verification manner [2]. Transaction records are stored in "blocks". Each block contains hash values, timestamps, and transaction messages, each of which contains a different nonce to calculate the new hash value. The newly generated block will be added to the previous blockchain through transaction verification, so as to link a long chain of data blocks.

- A consensus mechanism with rules and security: Both parties trading on the node achieve security by using public and private key encryption and digital signature algorithms. And each participating node can verify each event together. When a transaction enters the P2P network, the node first verifies whether the transaction is legal. If the node agrees on its legitimacy, they will confirm the transaction and place it in a block. This new block will be added to the previous blockchain and combined into a longer chain. In this way, the latest block keeps the latest state of the chain shared .

Blockchain stores all transactions in distributed blocks which means all nodes in the network are in possession of a copy of complete transaction data. For ensuring consistent data among all nodes, block data needs to be synchronized with the blockchain copy stored by the validator nodes. Therefore, even if a node suffered from hacker attacks, it will not affect the operation of the entire chain.

### *2.3. Ethereum and smart contracts*

Ethereum is one of the most important application based on blockchain technology. Despite as the well-known cryptocurrency, Ethereum also supports cross platform deployment which makes the use of blockchain more flexible and extensive [37]. The smart contract is a high level computer language deployed at Ethereum to encode business logic. Smart contract contains information about the transaction which can store the participants' agreement on the condition, and the changes involved in the contract are automatically made when the conditions are met. A smart contract can be defined as “a mechanism involving digit assets and participants”, in which some or all of the parties invest and redistribute assets through the nodes in the network to verify the contract content [3]. Smart contract can be flexible design and development, through the use of automated programs to perform a variety of industries, such as finance, insurance, medical services, making the blockchain of more diverse applications .

In order to implement user defined business logic in Ethereum, ethereum virtual machine (EVM) is adopted as an isolated runtime environment for smart contract. Although the hardware and software environment of each node is different, the EVM is able to compile down various smart contract down to bytecode and deploy to Ethereum to ensure that each node has the same execution environment. The objective of isolated environment of EVM is also designed to secure the network from malicious attacks, such as infinite loop or access operating system resources. The EVM is designed as a sandbox and is an execution environment that is isolated from the operating system. In EVM, smart contracts cannot access file systems, networks, or other programs in operating system but can only access other smart contracts. All smart contracts are executed synchronously with other nodes in the EVM. In order to ensure proper allocation of resources for the EVM, each instruction executed by the EVM has a cost which is measured in units of Gas. The more operating instructions will cost more Gas and meanwhile this mechanism also ensures that the system is not attacked by the network denial of service. As a result, Gas not only encourages developers to write streamlined,

high-quality code, but also ensures that miners performing the requested operations receive compensation for their contribution .

## 3. The blockchain of custody framework

This research utilizes blockchain technology to support digital forensic tasks with regarding to preliminary investigation phase, case management phase and court phase. The timestamps and hash values in the blockchain can ensure that each block is added sequentially to a chain and its content can be traced. The immutability of blockchain is the key feature to keep the distributed ledger unchanged. Accordingly, we adopted the immutable feature of blockchain to facilitate the reliability of digital evidence and provide effective audit trail capabilities. The proposed framework demonstrates the transparent process of handling digital evidence from crime scene to court and makes it corruption-free. An overview of proposed framework is shown in Fig 1. Three main phases, preliminary investigation phase, case management phase and court phase, are discussed in the following subsections.

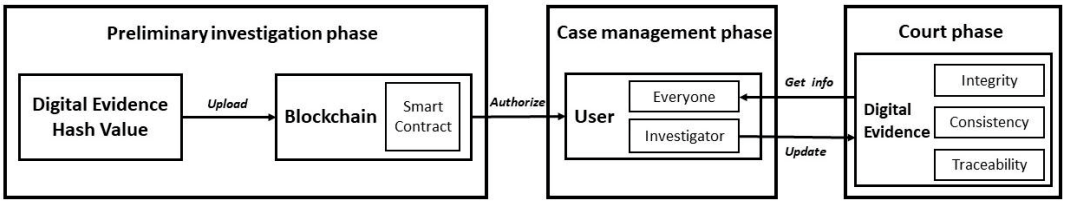


Fig. 1. Digital evidence blockchain of custody flow chart

### *3.1. Preliminary investigation phase*

The procedure for establishing chain of custody start with the crime scene. Therefore, the immutability of digital evidence should be applied whenever an investigator takes custody of evidence at a crime scene. With implementing blockchain in chain of custody, digital evidence from the scene should be collected by dispatched officers and turned into hash values followed by upload to digital evidence blockchain of custody. The law enforcement officer who get authorization to conduct the investigation from the decision maker is allowed to upload hash value. The mechanism for delegate authorization is implemented by smart contract. When the investigator has been verified as the person who takes charge of the crime case, the smart contract allows the authorized account to upload, modify, query the hash value of the digital evidence and record trace its transformation status on blockchain.

### *3.2. Case management phase*

Case management phase in criminal investigation process is designed to provide a comprehensive solution for achieving, transferring, sharing and cooperating between law enforcement agencies (LEAs). Despite the common superior or subordinate criminal case transformation between LEAs in a single country, modern cross-border crimes, such as fraud, money laundry and drug trafficking, also require case transfer to conduct further investigation. Although criminal intelligence sharing is critical, privilege segmentation and control is also a major concern for criminal case management due to secreting nature of privacy. Thus, smart contract is applied to provide concise access control among various LEAs.

The account which established in this phase can be divided into investigators and general user. As far as our knowledge, the role of investigator which is necessary for law enforcement applications has not been discussed in previous researches. Investigators who are responsible for a specific criminal case can create digital evidence hash and upload to the blockchain while general users can only query the hash value and the information of the digital evidence. When the criminal case needs to be transferred to a new custodian, the timestamps and the new custodian will be recorded through the smart contract. Since digital evidence should not be deleted if the crime case has already

gone through the judicial process, we remove the delete function which is commonly provide in previous business blockchain model and propose the modify function to keep every action that has been applied on the digital evidence [4].

### *3.3. Court phase*

The most important task of blockchain in the court is to convince the trier of fact that digital evidence has not been tampered. When the authorized user, such as investigator, lawyers, prosecutors and judges, set the query request to blockchain, the smart contract will demonstrate the hash value of digital evidence in each prior phases so as to explain the items are properly handled and legally considered as evidence in court. Since we provide modify function instead delete function, the sequence of custody can demonstrate the integrity, consistence and traceability of digital evidence. Therefore, the trier of fact is able to recognize the legal fact of digital evidence basically depend on the hash comparison results. If the hash values of current evidence items in the court match the hash value of the one which been uploaded at the crime scene in preliminary investigation phase, then we can treat the digital content in the court is identical with the original one. Thus, by applying the blockchain on digital evidence management provides a mechanism to identify the integrity of digital content but not focus on the traditional proof of delivery when transferring substantial digital evidence, such as USB drive. This benefit is more important in cross-border criminal investigation when it is almost impossible to spent a lot of time and effort to deliver the substantial digital evidence to various countries and take turns to analyze it.

## 4. System design

We demonstrate the implementation process of the digital evidence blockchain of custody system in this section. First, we introduce the hardware and software construction used in system development, then introduces the implementation steps of the system, and finally shows the development results of the system.

### *4.1. The environment of system development*

The developing environment of this study can be divided into the hardware equipment required for the execution system, and the software used in the implementation process. The detailed specifications are shown in Table 1. Node A and B represent the role of administrator and general user on Ethereum, respectively. We simulate an Ethereum private chain which composed with Node A and B with Geth, the command line interface for implementing a full Ethereum node in GO. The smart contract is compiled online by Remix with the Solidity language, then deployed to the private chain. The contract function can be viewed and tested through the interface provided by the Ethereum wallet. The purpose of implementing Geth to set up a Ethereum private chain is to conduct the operations which defined in the smart contract at the Ethereum node, explain the digital evidence can be successfully transferred among various organizations and be free from tampering as well.

Table 1. System development software and hardware configuration

| Hardware | Configuration |
|---|---|
| Node A：Acer Swift 1 | CPU : Intel Celeron N4100<br>RAM : 4GB<br>Disk : 128GB<br>OS : Windows 10 64bit Home Edition |
| Node B：ACPI x64-base PC | CPU : Intel Core i5-7400<br>RAM : 16GB<br>Disk : 1TB<br>OS : Windows 7 64bit Home Edition |
| **Software** | **Configuration** |
| Blockchain | Ethereum Geth v1.8.23 (private chain) |
| Smart contract | Solidity 0.4.22 |
| Program Compiler | Remix Ethereum IDE |
| Ethereum Wallet | Ethereum Wallet V0.10.0 |

### *4.2. Role design*

We design four roles, which are administrator, owner, creator and investigator, in this research to support modern criminal investigations involve in blockchain of custody for handling digital evidence. The architecture of role relations is shown in Fig 2. Since the architecture of this research is based on private Ethereum blockchain, an authorized department is necessary to create accounts for every blockchain user. Thus, the administrator's main task is to establish the account for the users . We design SetMember() function for administrator allowing to create different privilege level of users.

The investigator may combine with two roles, namely creator and owner. The investigator with the role of creator, who is responsible for the crime case, has the right to establish hash value of digital evidence by using CreateEvidence() function. By considering the crime cases are usually transferred to different LEAs, the investigator with the role of owner can use the Transfer() function to hand over the custody to another investigator. Once the custody has been transferred, the role of owner will be also transferred to the next custodian and the former custodian is no longer have the role of owner. The general user only has the function of viewing digital evidence information. An overview of different roles and corresponding functions is shown in Table 2.

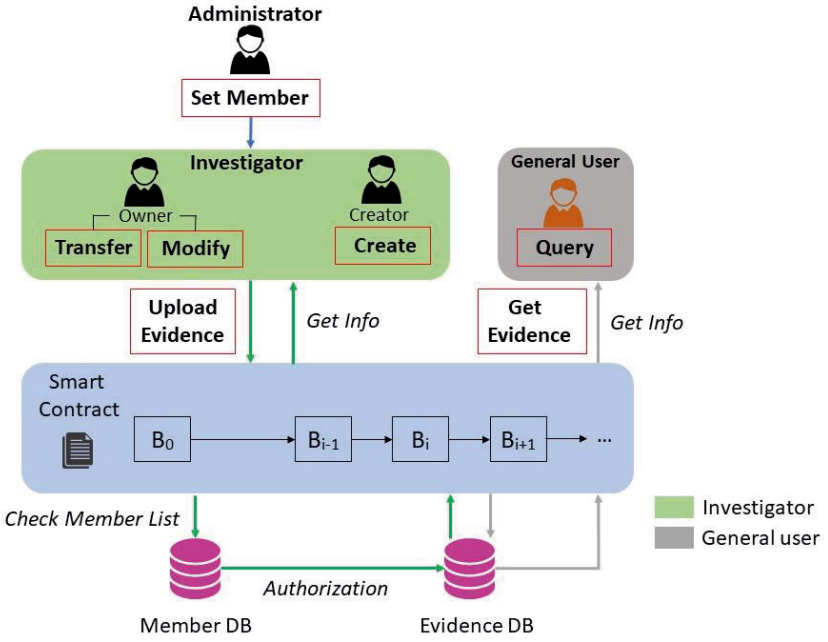


Fig. 2. The blockchain of custody framework

Table 2. Smart contract function design

| Role | Funtion | Description |
|---|---|---|
| Administrator | SetMember() | The account which can deploy the smart contract and is responsible for setting a list of members to distinguish between investigators or general users. |
| Creator | CreateEvidence() | The account that can creat the digital evidence hash value and case description to the blockchain. |
| Owner | Transfer()<br>ModifyEvidence() | The account which holds the digital evidence and case custodian. The account can transfer the custodian and modify the case description. |
| General user | GetEvidence() | The account which can sent a query to retrieve digital evidence hash value and other relevant case description. |

### *4.3. Experimental results*

This section describes the detailed design of blockchain of custody operations regarding to preliminary investigation, case management and court phases. In first part, we demonstrate privilege assignment, case transfer and legality of evidence procedures through 8 steps. Further, we discuss the security implications of smart contracts in blockchain of custody applications.

#### *4.3.1. Functionality*

For achieving various law enforcement requirements in digital evidence management, we illustrate the functionality of blockchain for not only maintaining the integrity of the digital evidence but also supporting effective proof of delivery. Table 3 demonstrates the 8 steps of operation in terms of three phases to realize the concept of blockchain of custody. The preliminary investigation phase consists of 3 steps. In step 1, the administrator assign the role of investigator to Node A via SetMember() function. When the identity of Node A becomes an investigator, Node A can create the digital evidence hash value and make the description of the crime case. The content of the crime case can

be uploaded to the blockchain using CreateEvidence() function. Once the digital evidence been uploaded in step 2, Node A also possess the role of creator and owner. In step 3, Node B as a general user can only execute GetEvidence() function to retrieve relevant information of digital evidence. These 3 steps of operation in preliminary phase explain the actions of blockchain of custody at crime scene.

As for case management phase, digital evidence transfer and modify are demonstrated from step 4 to step 7. Since a crime case shouldn't be transferred to a general user, in step 4, Node B should be assigned as an investigator by utilizing SetMember() before crime case transferring. In step 5, the crime case is transferred from Node A to Node B by conducting Transfer() function. As mentioned before, the role of owner is also transferred to Node B in the same step. In step 6, we demonstrate the crime case and the role of owner can both be transferred back to the previous custodian. With regard to the professional and legal responsibility of the first digital evidence examiner at the crime scene, we define that the ModifyEvidence() function should be conducted by the investigator who possess the role of both creator and owner.

The design of ModifyEvidence() function reflect the trend toward encouraging digital evidence creator to attain the court for enhancing probative value of the evidence. Therefore, in step 7, Node A with the role of creator, owner and investigator can proceed ModifyEvidence() function. Finally, in the court phase, Node A and B can verify the hash value of digital evidence, list of transferred custodians and timestamps of each step in this research.

Table 3. The demonstration of 8 steps of judicial process

| Phase | Step | Operation of node A | Role of Node A | Operation of node B | Role of Node B |
|---|---|---|---|---|---|
| Preliminary investigation phase | 1 | SetMember(Node A) | Investigator | — | General user |
| | 2 | CreateEvidence() | Investigator<br>Creator<br>Owner | — | General user |
| | 3 | — | Investigator<br>Creator<br>Owner | GetEvidence() | General user |
| Case management phase | 4 | SetMember(Node B) | Investigator<br>Creator<br>Owner | — | Investigator |
| | 5 | Transfer(Node B) | Investigator<br>Creator | — | Investigator<br>Owner |
| | 6 | — | Investigator<br>Creator<br>Owner | Transfer(Node A) | Investigator |
| | 7 | ModifyEvidence() | Investigator<br>Creator<br>Owner | — | Investigator |
| Court phase | 8 | Get Evidence | Investigator<br>Creator<br>Owner | Get Evidence | Investigator |

*4.3.2. Security assessment*

Preventing digital evidence been tampered or contaminated is crucial to assure its legal defensibility. We analyze the proposed blockchain of custody framework in respect of security to further demonstrate the judicial procedures from the crime scene investigation to court proceeding. In the preliminary investigation phase, the administrator can effectively distinguish the difference between law enforcement officer and general user by assigning the role of investigator to the account who is responsible for the crime case. Only the role of investigator is allowed to create digital evidence on the blockchain. This mechanism not only prevents the growth of occupied block caused by uploading irrelevant data from unauthorized users, but also keep from destroying the content of crime case by anonymous users. In the case management phase, the role of owner is essential for crime case transfer. The crime case can only be transferred to investigators but not general users. In addition, when crime case is transferred from one to another account, the role of owner will also be transferred to the new custodian. The design of allowing only one owner in the blockchain prevents the evidence ownership conflict while multiple investigators claim requesting evidence transferred simultaneously.

We propose the ModifyEvidence() function in this research to replace DeleteEvidence() function in previous researches to ensure the integrity and authenticity of digital evidence during the entire judicial process. Once the digital evidence is uploaded, deleting evidence is prohibited for providing more comprehensive audit trail which may subsequently be relied upon in court. The ModifyEvidence() function is used to update case description so as to provide valuable information for further investigation. And since the investigator who upload the hash has overall responsibility to testify the evidence in court, the account which possesses both the role of investigator and creator is allowed to execute ModifyEvidence() function to modify the content of case description. The rigorous principle of ModifyEvidence() reflect the high standard requirement of security in law enforcement applications. It is worth noting that ModifyEvidence() function can merely modify the content of crime case description. All evidence hash which been uploaded to blockchain cannot be changed in all circumstances.

## 5. Conclusions

With the emerging technology trend, the dramatic increase of digital evidence has a great impact on criminal investigation. Since digital evidence is vulnerable in nature, how to maintain the integrity and authenticity of digital evidence become a crucial task. In this study, we propose a blockchain of custody framework which supports evidence

collection and transferring in a lawful manner. In order to distinguish different level of authorization to access sensitive crime cases, we design the role of investigator to encompass various criminal investigation actions. The combinations of creator and owner with the role of investigator make evidence collecting and transferring more rigorous and ensure the integrity and authenticity of digital evidence during the entire judicial process. The framework is implemented on Ethereum blockchain with smart contract. The experimental results show that the proposed model can validate the immutability of evidence data and facilitate crime case sharing more effectively. Future research directions may include exploring more roles involved in criminal investigation and considering the scalability issue when deploying the proposed framework in a wider range of applications.

## Acknowledgements

This research was supported by the Ministry of Science and Technology of the Republic of China under the Grants (MOST 109-2410-H-015-007 –) and partially supported by the Executive Yuan of the Republic of China under the Grants Forward looking Infrastructure Development Program (Digital Infrastructure-Information Security Project-110).

## References

[1] Giova, G. (2011) "Improving chain of custody in forensic investigation of electronic digital systems." *International Journal of Computer Science and Network Security* **11 (1)**: 1-9.
[2] Xu, X, Weber I, Staples M, et al. (2017) A taxonomy of blockchain-based systems for architecture design. In: *2017 IEEE international conference on software architecture (ICSA)* 243-252. IEEE.
[3] Du, X, Le-Khac N-A and Scanlon M. (2017) "Evaluation of digital forensic process models with respect to digital forensics as a service." *arXiv preprint arXiv:170801730*.
[4] Prayudi, Y and Sn A. (2015) "Digital chain of custody: State of the art." *International Journal of Computer Applications* **114 (5)**: 1-9.
[5] Nakamoto, S. (2008) "Bitcoin: A peer-to-peer electronic cash system." *Bitcoin–URL: https://bitcoin org/bitcoin pdf*.
[6] Lone, AH and Mir RN. (2018) "Forensic-chain: ethereum blockchain based digital forensics chain of custody." *Sci Pract Cyber Secur J* **1 (2)**: 21-27.
[7] Pilkington, M. (2016) "11 Blockchain technology: principles and applications." *Research handbook on digital transformations* **225**: 225-253.
[8] Buterin, V. (2014) "A next-generation smart contract and decentralized application platform." *white paper* **3 (37)**.
[9] Ølnes, S, Ubacht J and Janssen M. (2017) "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing." *Government Information Quarterly* **34 (3)**: 355-364.
[10] Swan, M. (2015) *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.
[11] Wohrer, M and Zdun U. (2018) Smart contracts: security patterns in the ethereum ecosystem and solidity. In: *International Workshop on Blockchain Oriented Software Engineering (IWBOSE)* 2-8. IEEE.
[12] Bonomi, S, Casini M and Ciccotelli C. (2018) "B-coc: A blockchain-based chain of custody for evidences management in digital forensics." *arXiv preprint arXiv:180710359*.