Forensic Science International: Digital Investigation 32 (2020) 300911

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

DFRWS 2020 EU — Proceedings of the Seventh Annual DFRWS Europe

Tainted Digital Evidence and Privacy Protection in Blockchain-Based Systems

David Billard. *HES-SO, University of Applied Sciences in Geneva, Switzerland*
E-mail address: David.Billard@hesge.ch

Extended abstract

This paper focuses on an often-forgotten aspect of digital evidence handling, when a court dismisses an evidence from a trial. Multiple reasons can lead to dismiss an evidence: it can be challenged by a party during an investigation or in front of the court, or simply dropped by the prosecutor.

Of course, different countries apply different laws, but let's take a simple example, that is quite universal. Bob is suspected to hold illegal child pornography material. A warrant is issued and a police search is conducted at Bob's house. During the search, a hard drive is seized and following the police procedure, the hard drive is registered and a chain of custody is initiated. Since this police body is a modern one, the hard drive is also registered into the blockchain-based evidence inventory software.

Digital forensics experts examine the drive and find connections with Alice, who seems deeply involved in child pornography. A police search is therefore triggered on Alice and a USB stick with a lot of inculpatory evidence is found at Alice's home. As required by the procedure, the USB stick is registered into the same blockchain-based software.

Much later in the investigation, a defense lawyer raises the legality of the first police search on serious grounds. The court follows the motion and the first police search is dismissed. Since the second police search is a direct offspring of the first, it is also dismissed from the case.

Now let's examine the same case, when a blockchain is used to implement a chain of custody [1], [2]. The digital evidence found at Alice's and Bob's are stored in the ledger, but there is no mechanism to delete a digital evidence from the ledger, since it is precisely built to forbid any alteration, deletion or cancellation.

In the absence of such mechanism, having this unique blockchain structure available, there are at least two possible options in order to dismiss transactions.

The first one is to delete the whole blockchain and to issue a new blockchain, without the dismissed evidence. In practice, it means to start from the root block and re-issue all the subsequent transactions (excepted the transactions linked to the dismissed evidence of course). Although it is theoretically doable, it means a huge effort of transaction and block validation, involving voting algorithms, and keeping track of all the blockchain intra references. The reader can already notice that the computational complexity is quite significant.

The second option is to issue undo-transactions whose purpose is to indicate that the referenced transaction is void and cannot be used anymore. It means that the blockchain contains two categories of transactions: (1) the transactions for registering evidence and (2) the undo-transactions for dismissing evidence.

This technique of using undo-transactions is widely used, since a long time, in DataBase Management Systems (DBMS) for recovery or rollback purposes[3]. Unfortunately, while it is well suited for DBMS, it brings some issues in blockchain-based systems.

The major issue concerns the verification of the transaction validation. In order for a user to check if a transaction is valid, the user will have to verify if the chain of hashes and signatures has not been broken since a particular point in time (usually the begin of the blockchain). This check means that the transaction has been correctly entered into the system and has been validated following the rules.

But this check does not prove that the transaction is valid from a legal point of view: the evidence linked to the transaction may have been dismissed later. Therefore, the check process must continue until either: (1) it finds the undo-transaction, then the transaction is not legally valid or (2) it reaches the end of the blockchain, then the transaction is legally valid. The reader will notice that the computational complexity of this check is significantly higher than the single transaction verification protocol usually observed in blockchain.

Both solutions are unsatisfactory and we devised a solution where an additional layer of software, *AccessTX*, provides access to the blockchain. Let's name the chain of custody blockchain *InventoryTX*. The additional layer, controlling access to InventoryTX, will first check if a transaction is either legally dismissed or valid, before granting access. After the check is done, the transaction will be validated through the normal processing of the blockchain *InventoryTX*.

In order to check the legal validity of a transaction, the access control will also use a blockchain, named *InvalidatedTX*. The payload of every transaction in InvalidatedTX contains the transaction ID related to a tainted evidence. It is desirable that each transaction in InvalidatedTX is signed by the jurisdiction issuing the removal of the tainted evidence.

The validation of each invalidating transaction is processed as in a normal blockchain, since the root of InvalidatedTX. Only the nature of the invalidating transaction differentiates it from a traditional blockchain.

An example might be the best way to illustrate the different components of the proposed solution. We suppose the police searches Ms Marple's home. This woman is suspected to host a suspected man running from the police. Three evidence items are found at her home:

- Agent Poirot found a USB key with the searched man identity documents and 1000 bitcoins;
- Agent Ness found a notebook with pornographic contents and a hyperlink to a web server;
- Agent Loch found a love letter from the suspected man to Ms Marple.

Later, the web site is investigated by agent Chris and it contains drug recipes. The *InventoryTX* blockchain is built and has the look of Fig. 1. The reader will notice that it is a generic representation of a blockchain and that different authors in the literature may have additional features.

https://doi.org/10.1016/j.fsidi.2020.300911

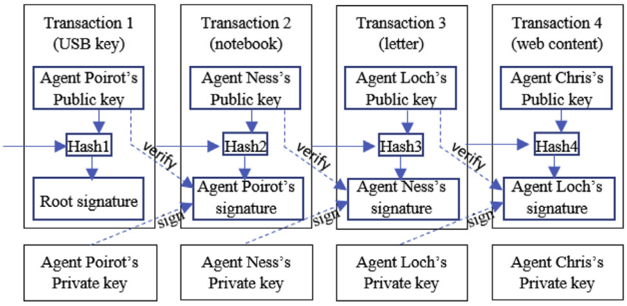

Fig. 1. InventoryTX for the Marple case.

We suppose that, in our fictious example, the defense argues that pornographic materials and drug recipes are not the subject of the search and should be dismissed. The court follows this request and judges Roy and Prince update the *InvalidatedTX* blockchain which is depicted in Fig. 2.

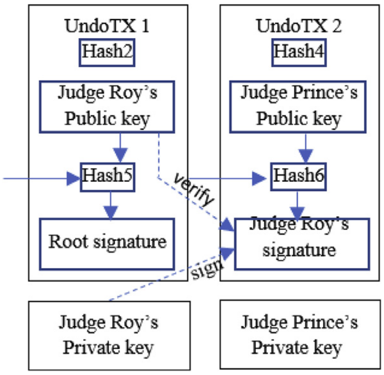

Fig. 2. *InvalidatedTX* for the Marple case.

When parties will access the evidence stored into the *InventoryTX*, the system will first look up in the *InvalidatedTX* to verify if the transaction concerning the evidence is legally sound. Three scenarii are then possible:

- If the transaction hash is absent from *InvalidatedTX*, and present in *InventoryTX* then the system will serve the transaction payload, which is usually a reference to a safe storage entity holding the evidence content, or description.
- If the transaction hash is absent from *InvalidatedTX*, and also absent from *InventoryTX* then the system will raise a "`Transaction not found`" exception.
- If the transaction hash is present in *InvalidatedTX* then the system will raise a "`Transaction invalidated by court order #xxx`" exception.

This system possesses the advantage of being very lightweight. In the absence of dismissed evidence, the cost for the lookup is in O(1), since *InvalidatedTX* is empty. In the presence of dismissed evidence, the cost for the lookup is in O(m) were m is the total number of dismissed evidence records.

Our solution for dismissing tainted evidence do not erase the fact that the evidence was once part of the procedure, but it will prevent the use of this evidence by the parties. We believe that this algorithm will help in the adoption of blockchain solutions by providing more flexibility in the evidence management. Besides, this solution works with a majority of blockchain implementation because it does not modify the blockchain structure.

Furthermore, evidence data is separated from the blockchain transaction's payload, that holds only metadata.

References

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

[2] H. Al-Khateeb, G. Epiphaniou, and H. Daly, "Blockchain for Modern Digital Forensics: The Chain-of-Custody as a Distributed Ledger," in *Blockchain and Clinical Trial: Securing Patient Data*, H. Jahankhani, S. Kendzierskyj, A. Jamal, G. Epiphaniou, and H. Al-Khateeb, Eds. Cham: Springer International Publishing, 2019, pp. 149–168.

[3] J. Gray and A. Reuter, *Transaction Processing: Concepts and Techniques*. Morgan Kaufmann Publishers Inc., 1992.