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 incriminatory 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 transaction. The reader will notice that the computational complexity of this check is significantly higher than the single transaction verification protocol usually observed in blockchain. As a result, the transaction is dismissed from the blockchain.

The major issue concerns the verification of the transaction validation. In order for a user to check if a transaction is valid, they 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, as it is processed as a legal transaction. This is the case when the transaction is linked to a valid evidence. The reader will notice that it is a generic representation of a blockchain validation protocol.

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 contains a chain of custody 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.
We suppose that, in our fictional 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.

![Diagram](image1)

**Fig. 1.** InventoryTX 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 scenarios 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**

