Tainted digital evidence and privacy protection in blockchain-based systems

Abstract

Your law enforcement officer introduces a digital evidence into the chain of custody blockchain. The court invalidates this evidence and all the attached evidence. We show how to dismiss this tainted evidence from a blockchain which by default does not allow for alteration, deletion or cancellation.

Instead of modifying the structure of the blockchain or its purpose, we prevent a user to access tainted evidence.

Let’s name the evidence blockchain InventoryTX. We propose to add an additional blockchain structure, InvalidatedTX, that records the invalidated transactions, and a controlling structure AccessTX which is the access point to InventoryTX. In order to access a transaction from the InventoryTX blockchain, the request goes through the AccessTX access point that first parses the InvalidatedTX blockchain. The cost for parsing InvalidatedTX is $O(m)$ where $m$ is the number of invalidated transactions. In usual cases, $m$ will be close to zero, thus the search overhead will be insignificant. When a transaction is returned from the InventoryTX blockchain, it has the properties inherited from being in a blockchain, and the additional property that the transaction is legally sound and has not been voided.

Example

Transaction 2 is invalidated by Judge Roy and Transaction 4 is invalidated by Judge Prince

Conclusion

In this paper, we presented a cost-effective solution for obliterating blockchain transactions from a case, in the presence of tainted evidence. Our solution for dismissing tainted evidence does 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.