heg

Haute école de gestion
Genève

IARIA

Dismissing Poisoned Digital Evidence from Blockchain of Custody

David Billard

David.Billard@hesge.ch

The Fifth International Conference on Cyber-Technologies and Cyber-Systems
October 25, 2020 to October 29, 2020 - Nice, France

Your presenter

- ✓ **Sworn expert to the French and Swiss courts and accredited to the International Criminal Court**
- ✓ **Associate-professor at the University of Applied Sciences in Geneva (Switzerland)**
- ✓ **Lecturer at the Stocholm University (Sweden) and Lausanne (Switzerland)**
- ✓ **Co-founder and former associate of LERTI, a private digital forensic lab**

Forensic Science

- **A science by itself, for serving fight against crime**
- **Study of traces**
  - Detection, observation, collection
  - Identification, individualisation and authentication
  - Determining probative value of evidence
- **And links among traces**
  - Processing a (criminal) case
  - Detecting series
  - Understanding phenomenons and structures

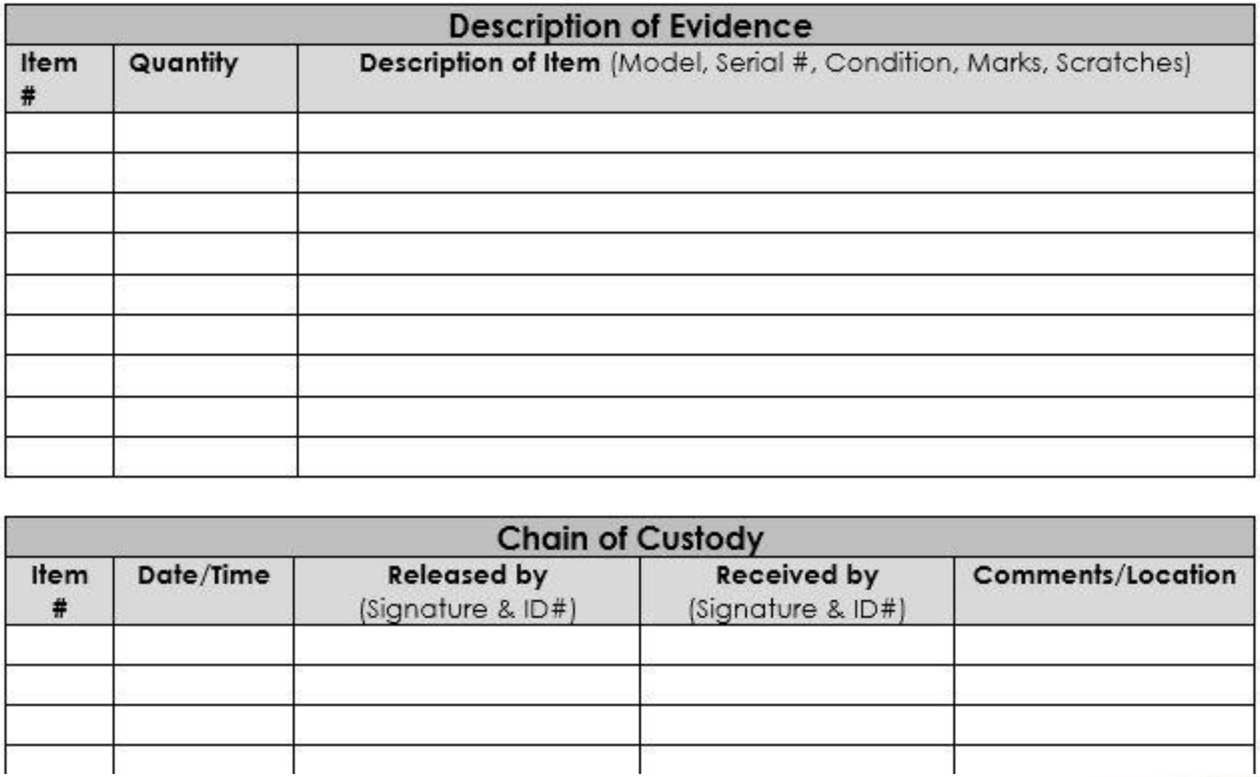
Chain of custody (chain of evidence)

- ✓ ***Chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence.***

- ➢ ***Used in criminal cases, civil litigation, arbitration***

- ➢ ***But also in supply chain management, financial audit, etc.***

Chain of custody



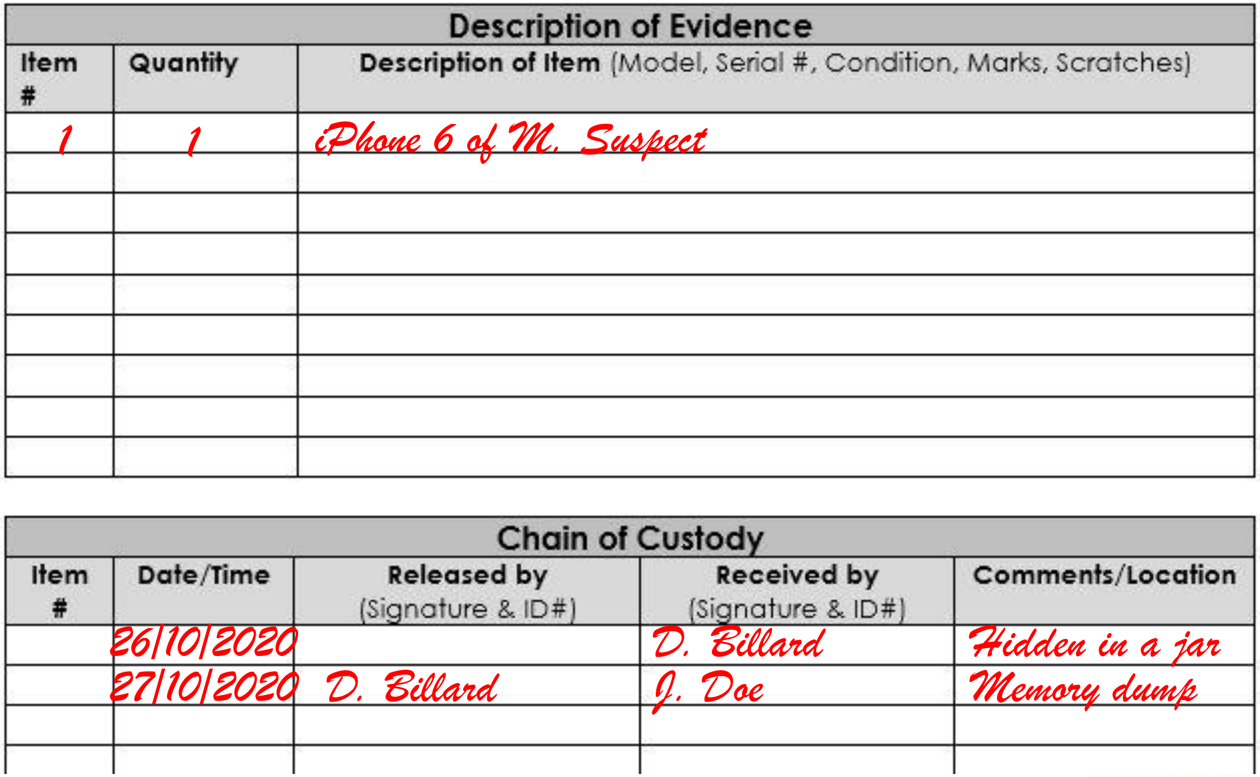
Description of Evidence		
Item #	Quantity	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	Date/Time	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	Comments/Location

From ***https://www.nist.gov/***

Chain of custody

From https://www.nist.gov/



Description of Evidence

Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)
1	1	iPhone 6 of M. Suspect

Chain of Custody

Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location
	26/10/2020		D. Billard	Hidden in a jar
	27/10/2020	D. Billard	J. Doe	Memory dump

Chain of custody for digital evidence

- **Physical items can be bagged**
- **Difficult for digital assets**
- **Use of blockchain**
- **Permissioned blockchain**

Permissioned v/s permissionless blockchains

Permissioned blockchain uses an access control layer to:

- **Control network access**
- **Control who can validate transaction/blocks**

Permissionless blockchain uses pseudonymat and consensus algorithm:

- **Bitcoin with Proof of Work**
- **Ethereum with Proof of Stake**
- **Hyperledger with practical Byzantine Fault Tolerance**

A small scenario

Police searches Ms Marple's home.

Ms Marple is suspected to host a suspected man running from the police.

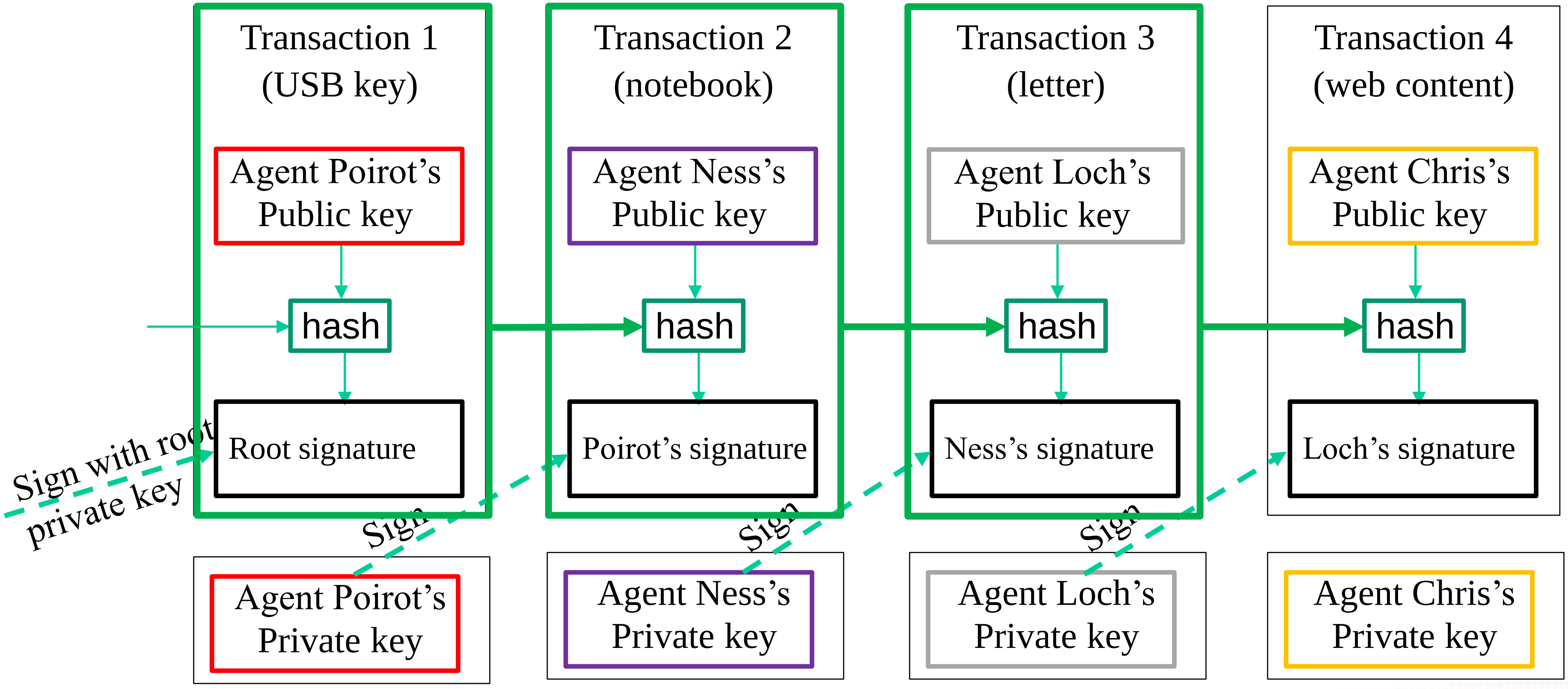
3 evidence items are found at her home:

- ✓ **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.**

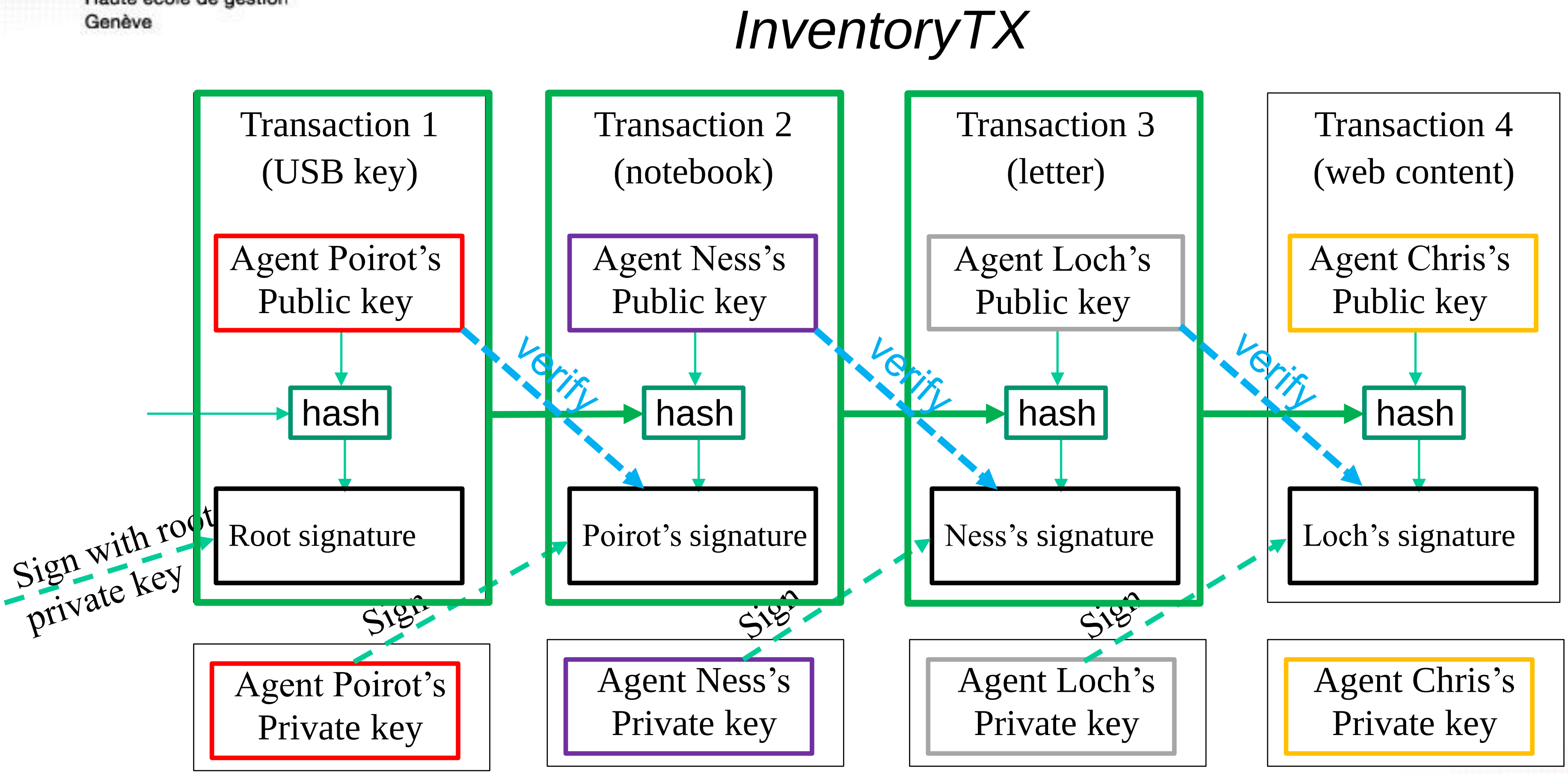
Later, the web site is investigated by agent Chris and it contains drug recipes.

How these 4 evidences are recorded

InventoryTX



How these 4 evidences are recorded



Transaction validation

Transactions validated by authorized law enforcement

Or

Tribunal officials

Since it is permissioned blockchain

→ No need of proof of work

→ No need of proof of stake

Further in the investigation

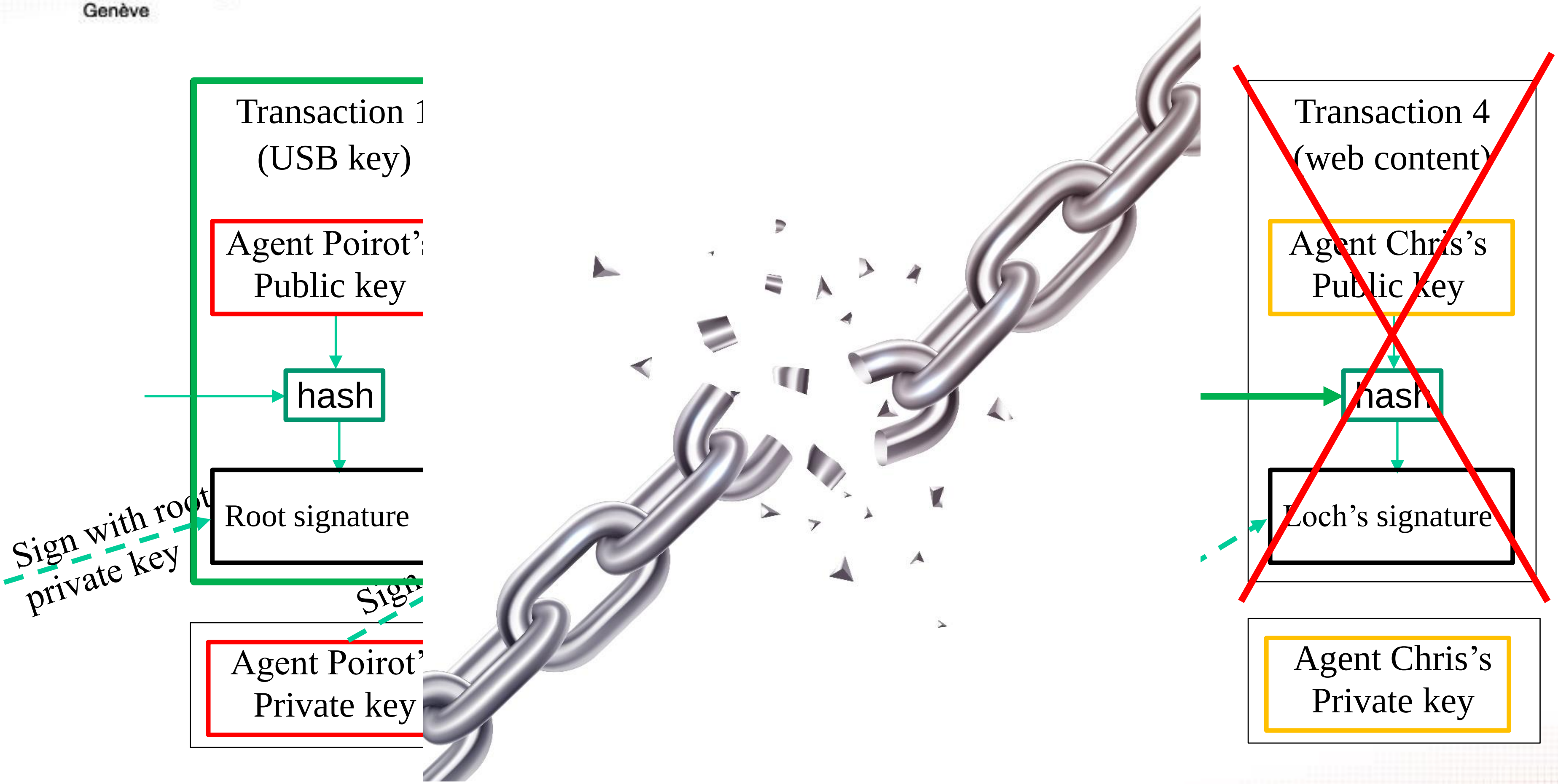
Defense argues that pornographic material and drug recipes are not the subject of the search and should be dismissed

The court follows this request.

Judges Roy and Prince have to delete transactions 2 & 4

But how, since the blockchain cannot be tampered with?

What we cannot do



Transaction 1
(USB key)

Agent Poirot's
Public key

hash

Root signature

Sign with root
private key

Sign

Agent Poirot'
Private key

Transaction 4
(web content)

Agent Chris's
Public key

hash

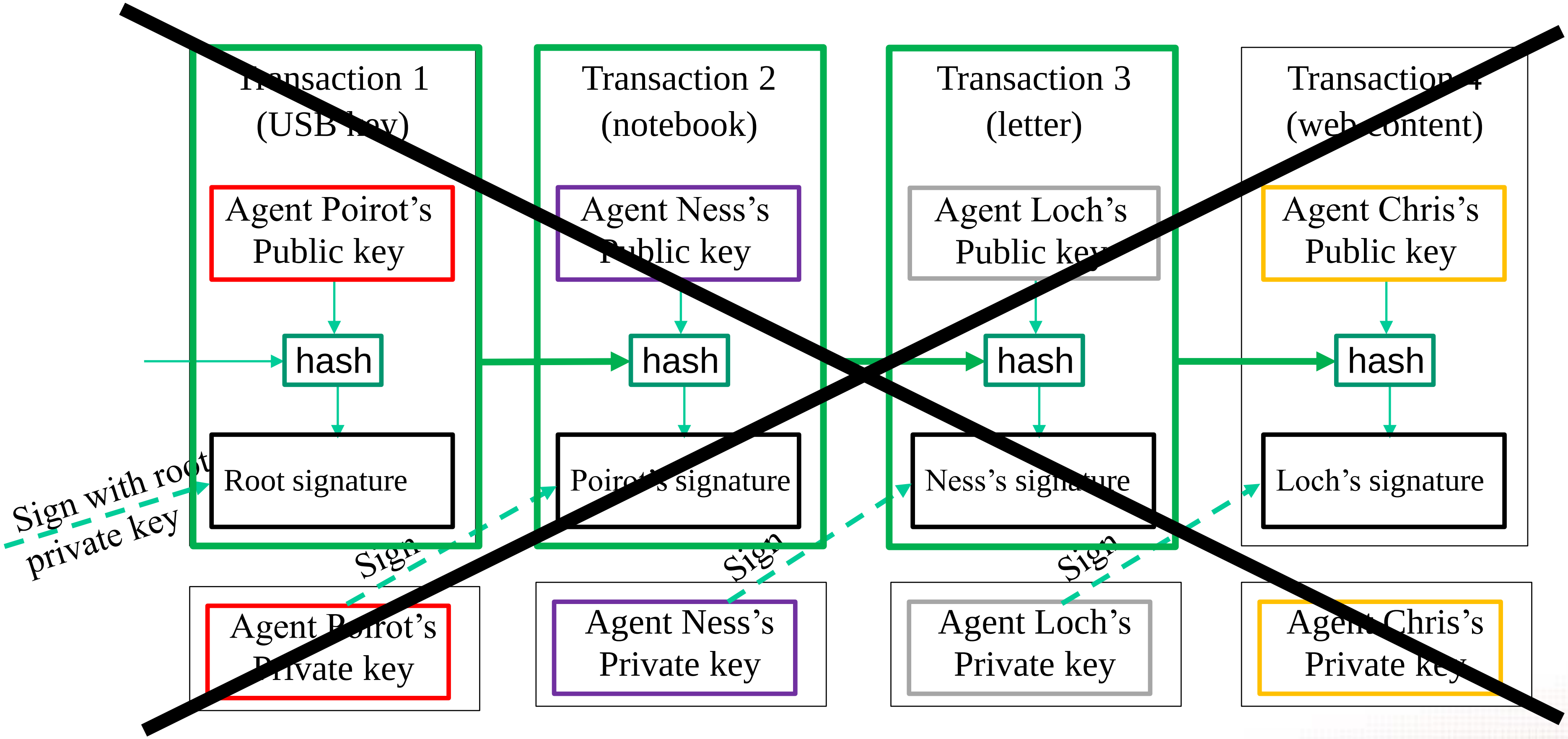
Loch's signature

Agent Chris's
Private key

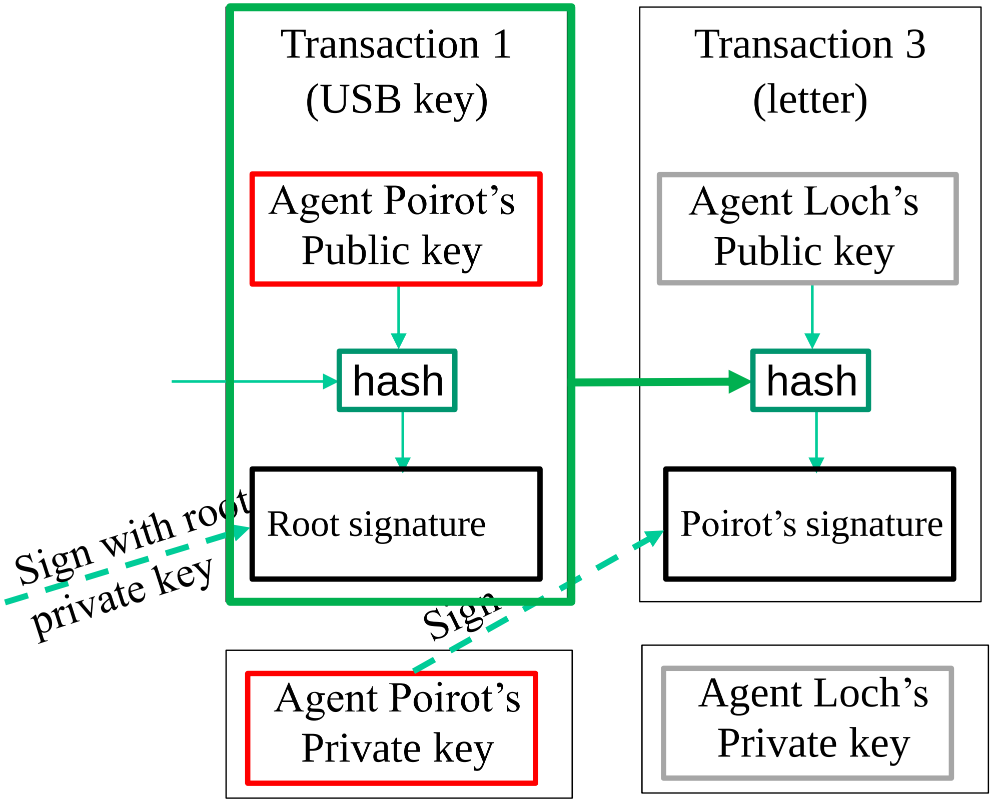
Designed by macrovector / Freepik

Haute école de gestion
Genève

Voiding the whole chain



Beginning anew



Other solution

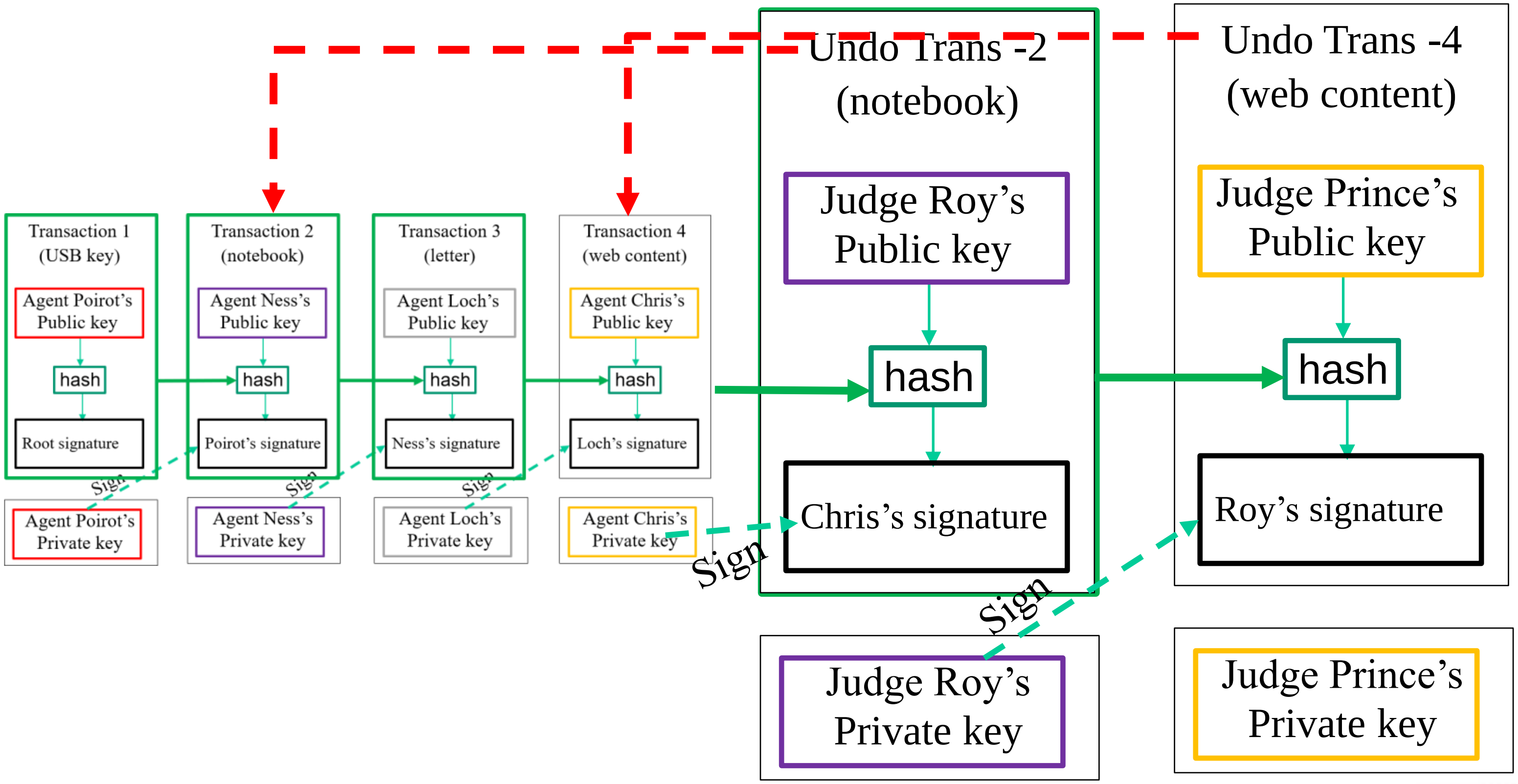
By restarting anew, we loose the fact that two evidences have been dismissed by a court order

All the validators must validate again

A query for a dismissed transaction will return a general error

Let’s try undo-transactions (DBMS-like)

Undo transactions



Transaction legal state

Given a transaction Id, how do we now if it is legally valid?

If we are presented with transaction 2, we have to go to undo-transaction -2 to discover it is no longer valid

For each transaction T all the blockchain is parsed:

From beginning to T: T is technically valid

From T to end (or –T): T is legally valid or dismissed

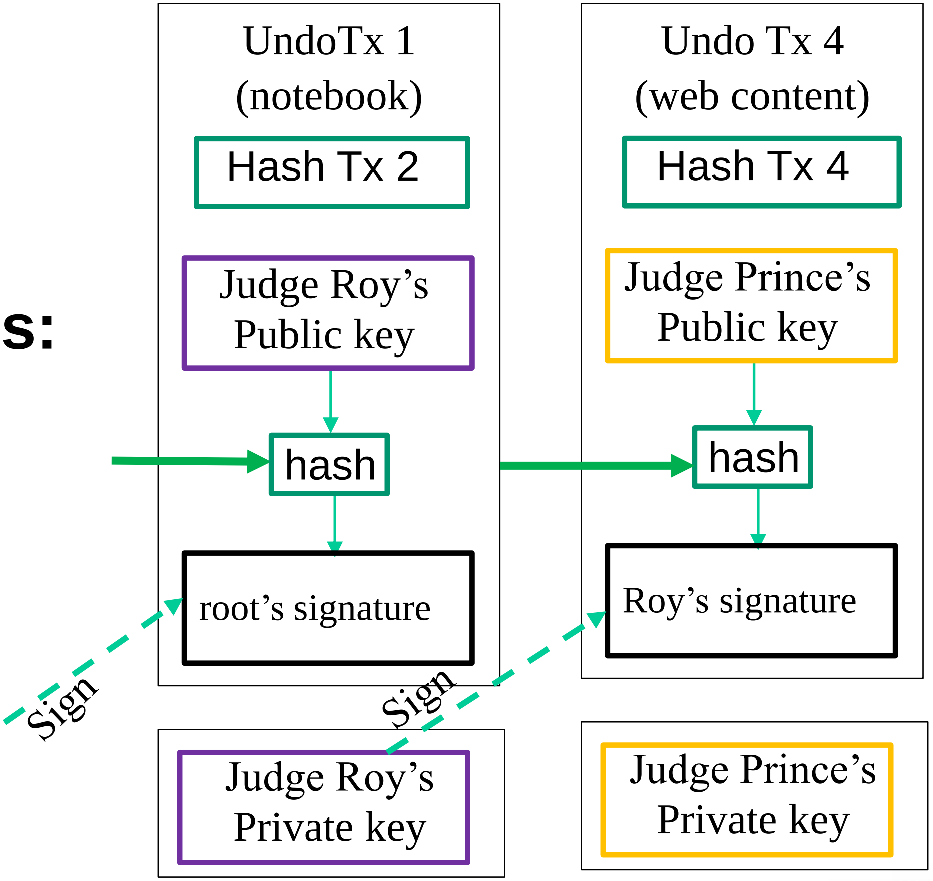
Complexity is O(n^2)

Our solution

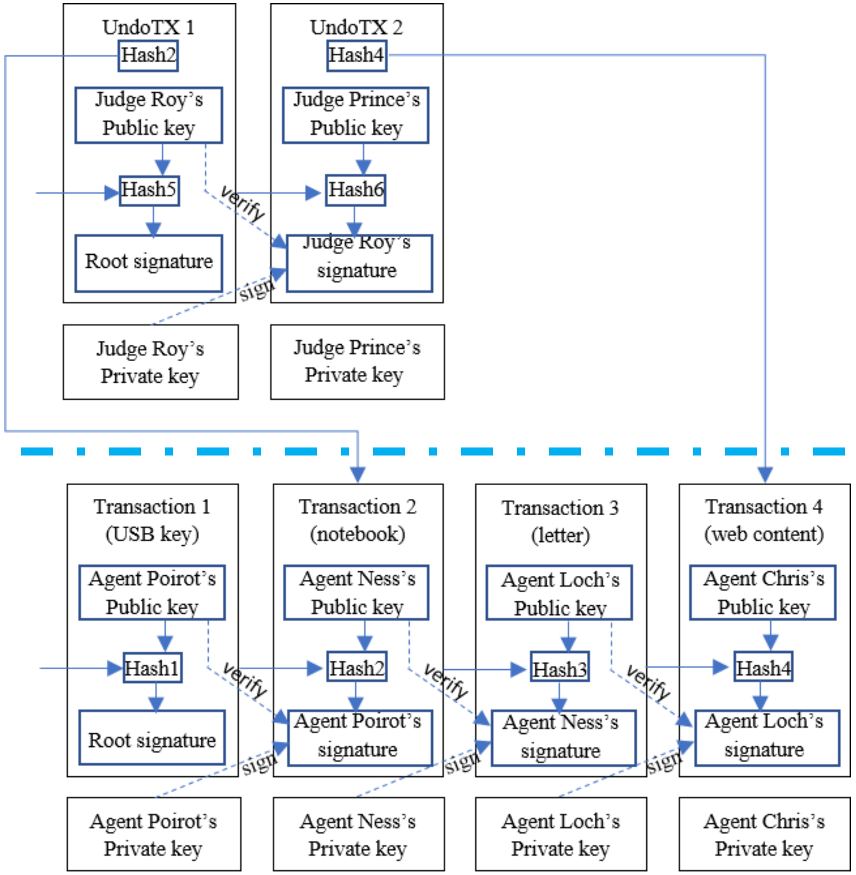
Building an additional blockchain recording dismissed transactions:

InvalidatedTX

Stores only dismissed evidence



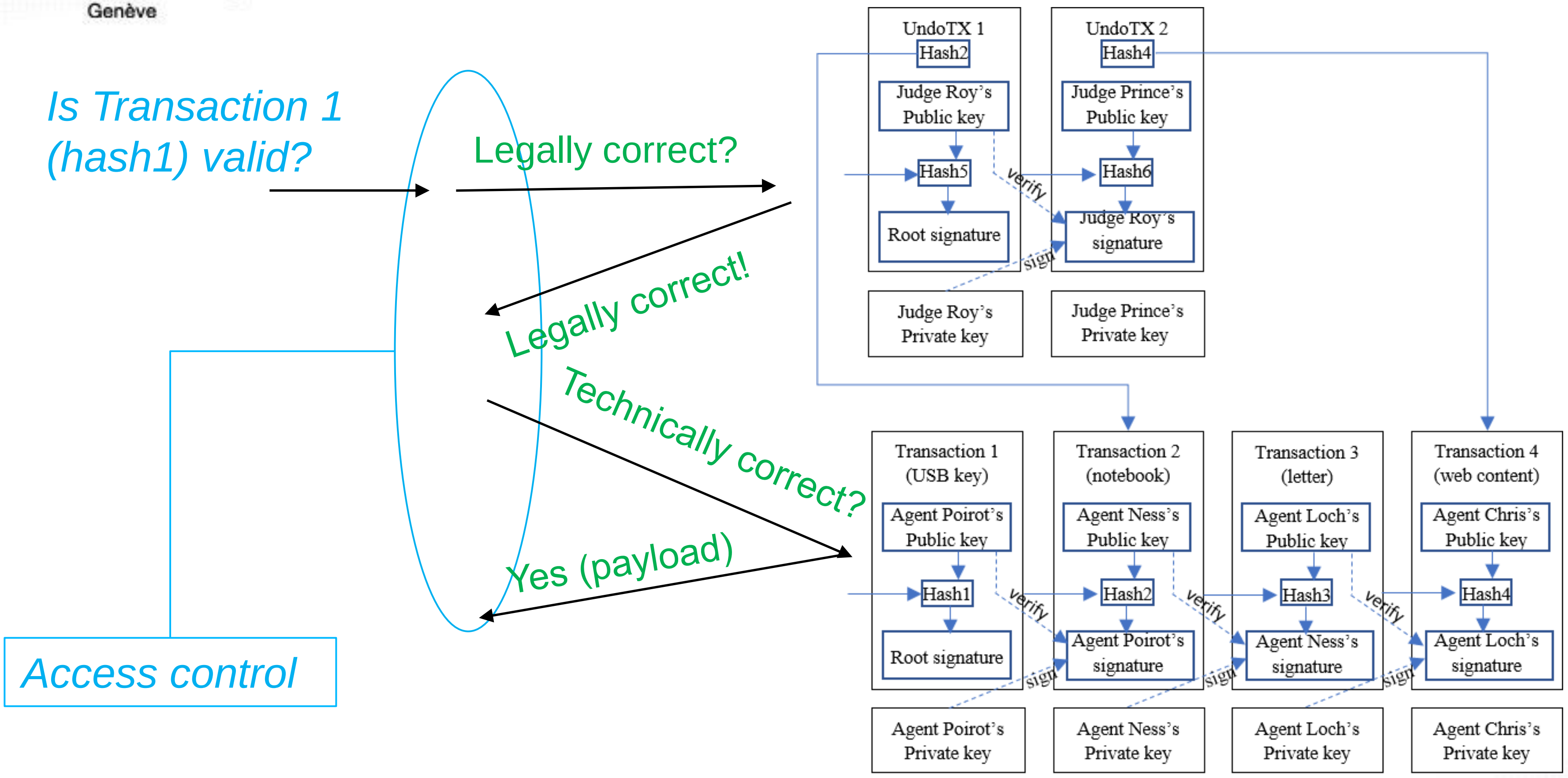
The whole blockchain picture



InvalidatedTX

InventoryTX

The whole picture



Is Transaction 1 (hash1) valid?

Legally correct?

Legally correct!

Technically correct?

Yes (payload)

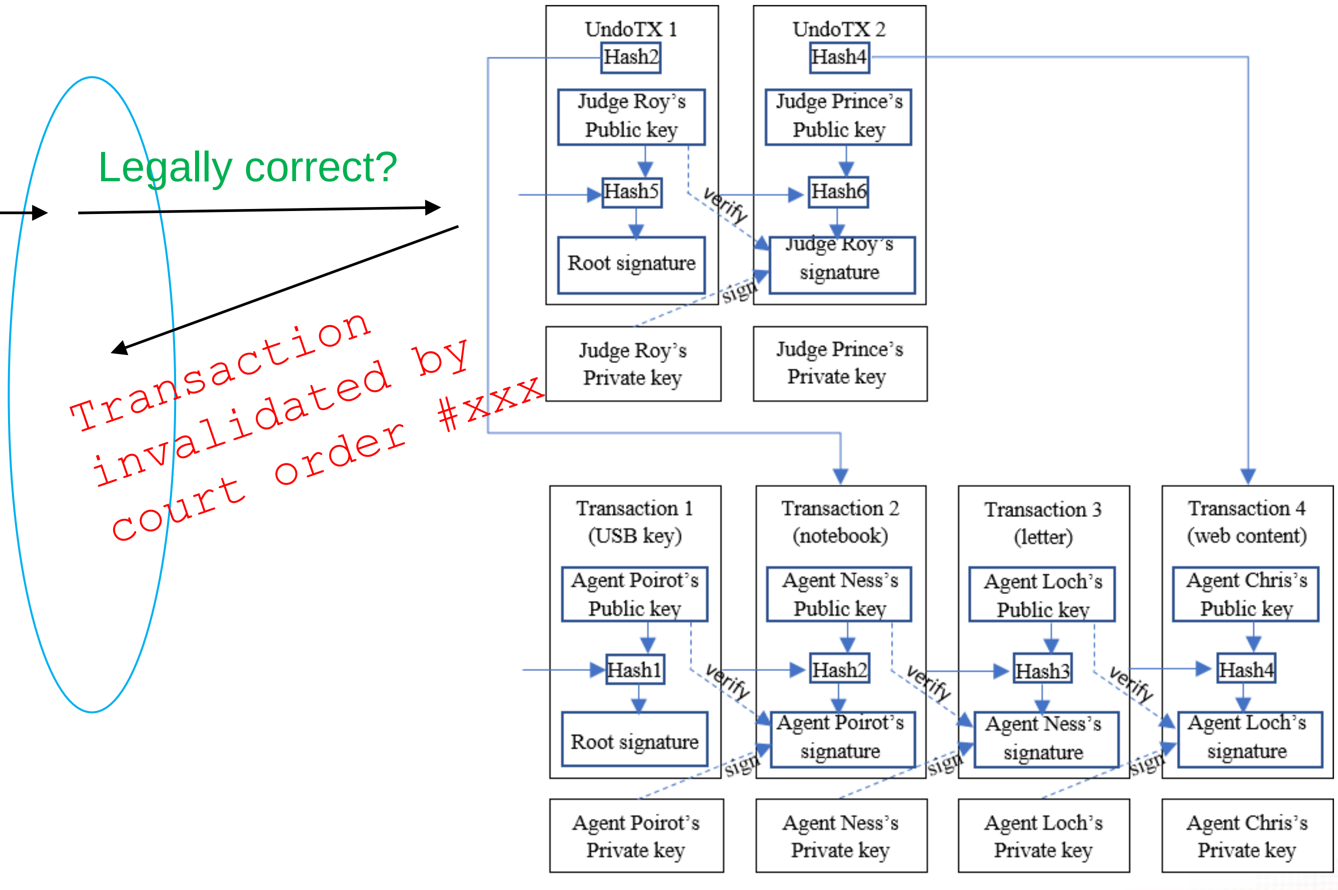
Access control

The whole picture

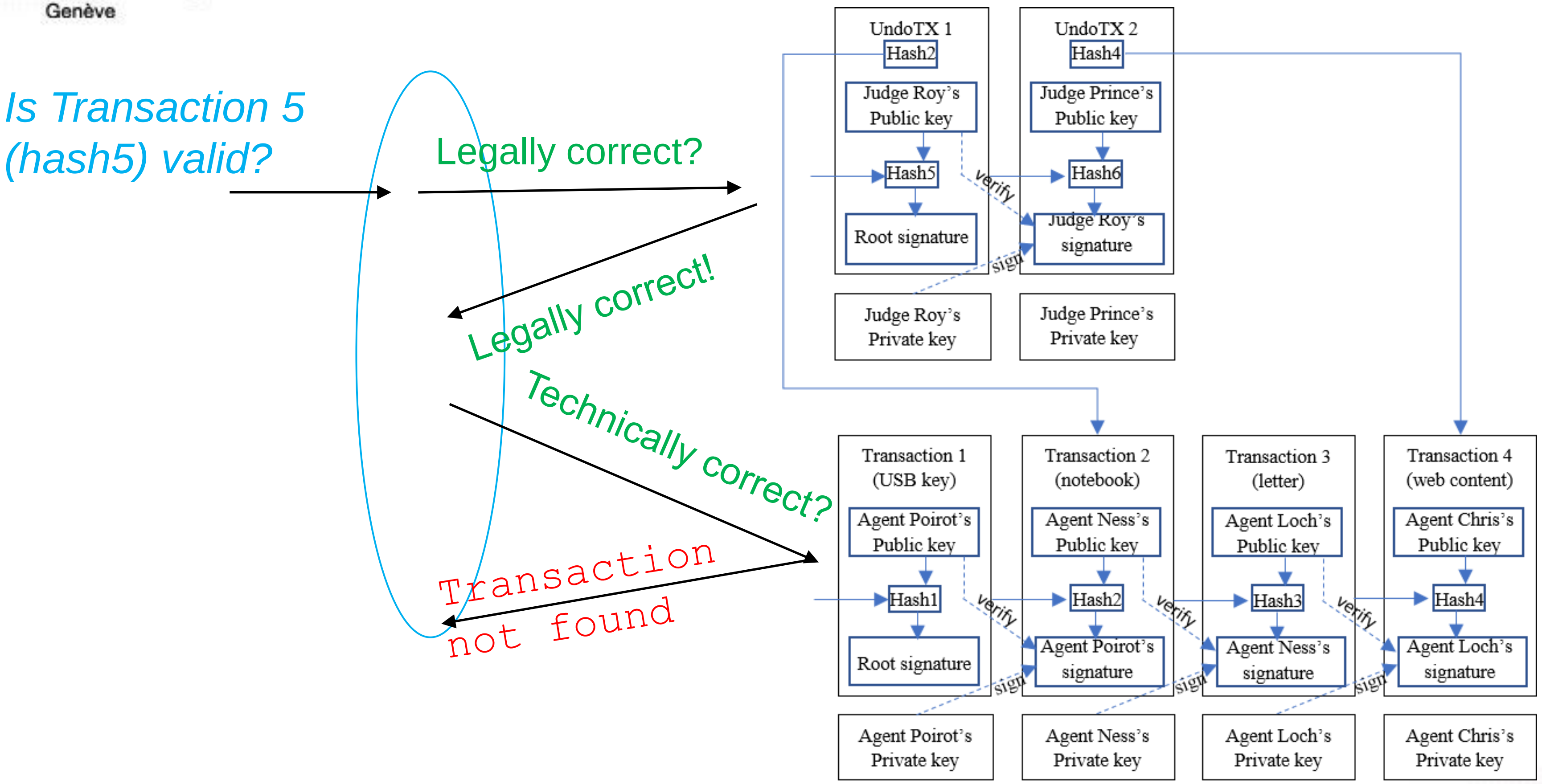
Is Transaction 2 (hash2) valid?

Legally correct?

Transaction invalidated by court order #xxx



The whole picture



Is Transaction 5 (hash5) valid?

Legally correct?

Legally correct!

Technically correct?

Transaction not found

The verification algorithm

```
if (hash(T) ∉ InvalidatedTX) then
 if (hash(T) ∈ InventoryTX) then
  return payload(T)
 else
  return “Transaction not found”
else
 return “Transaction invalidated by court order #xxx”
```

Complexity:

- ***O(m),*** **m = number of Tx in InvalidatedTX, possibly 0**
- ***O(n)*****, n = number of Tx in InventoryTX < T**
- ***O(m+n)***

The fact that T has been dismissed is recorded

Poisonous evidence

In our example, only two evidences were dismissed.
But what if the house search itself is dismissed?
→ In turn, all the related evidences should be dismissed

The search is poisoned and in turn poison the evidences

But not always true (law is not always straightforward)

Cannot automate the dismissal with an algorithmic search & dismiss

Privacy protection

Payload not part of the transaction

Only a reference to a safe storage

Deleting a transaction:

```
For each transaction T
  If EvidenceID(T) = EvidenceID then
    Add a new transaction to InvalidatedTX
    Erase safe storage content
```

Atomic action

Conclusion

Our solution helps in the management of tainted digital evidence in criminal investigations

- **By removing the dismissed transactions in a linear complexity**
- **By keeping the fact that evidences have been dissmissed**
- **While providing privacy protection over sensible data**

Two blockchain layers with an access control