Crypto Asset Lab

Blockchain beyond Monetary Application

Timestamping

Paolo Mazzocchi

Milan, June 5, 2019

Digital Gold Institute

Università degli Studi di Milano Bicocca

Blockchain Beyond Bitcoin

"There is no blockchain without bitcoin
There is blockchain beyond bitcoin"

Andreas Antonopoulos

speaker, educator, and one of the world's foremost bitcoin and open blockchain experts

Blockchain Graffiti

- Bitcoin Script operator *OP_RETURN* can be used to write 80 bytes of arbitrary data in the blockchain using a bitcoin transaction
- E.g. Eternity Wall offers the possibility to "write" a message on the Bitcoin blockchain:

Timestamp

- A timestamp demonstrates that a document existed in a specific status prior to a given point in time, providing a relevant document with a certain sure date, e.g. postmark

- Law requires dates to be certified by public officials and notary services

- For digital documents, timestamping is based on the digital signature of a Certification Authority (CA)

Hash Function

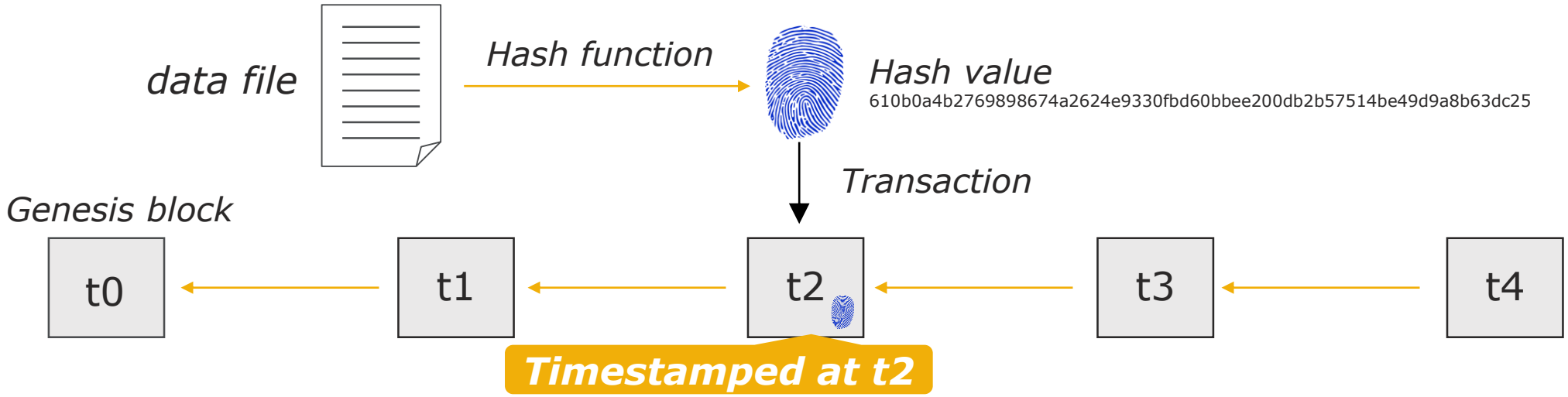
Map input data of **arbitrary length** to an output set of hash values, i.e. output data of a **fixed length**

Non-invertible	*Collision-resistant*	*Random oracle model*
		
input data cannot be recovered from the output	computationally unfeasible to find 2 inputs that produce the same output	the hash value is so unpredictable to appear as if it was chosen uniformly at random

Consequently, the resulting hash value:

- **does not reveal input data**
- **is a reliably unique identifier** for its input data: it can be considered its unique digital fingerprint
- has large differences for small differences in the input data

Blockchain Timestamping Process



- Digital data can be securely timestamped though the attestation of its hash value in a blockchain transaction
- The transaction extends its native blockchain timestamping to the included hash value, therefore proving its existence at a given point in time
- Timestamping immutability is **secured by the amount of computational effort** accumulated by the blockchain after the inclusion of the hash value in a block. Indeed, the more blocks are added to the chain after a given block, the more computationally intensive is tampering with the data of that block

Blockchain Timestamping

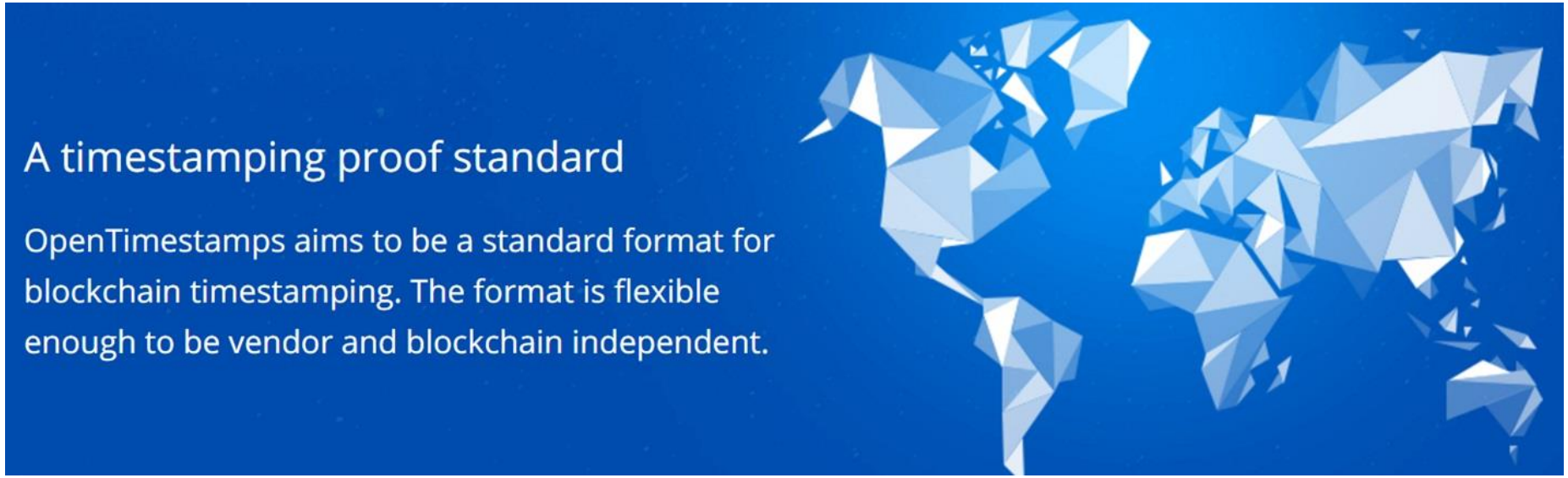
Pros

- Digital public proof, easily auditable by everyone
- The proof cannot be faked, manipulated, or removed
- A Blockchain Certification Authority cannot be bribed
- Can be used along with regulatory timestamping prescription

Cons

- Not efficient (one transaction per document)
- Lack of standardization

The OpenTimestamps Standard



- Define a set of operations for creating **provable blockchain timestamps** and later independently verifying them
- **vendor-independent**
- **blockchain-agnostic**
- **free public open-source**

https://petertodd.org/2016/opentimestamps-announcement

The OpenTimestamps Standard

Trust Minimization

OpenTimestamps uses decentralized, publicly auditable, blockchains, **removing the need for trusted authorities**; its architecture is designed to support multiple, cross-checked, notarization methods

Scalability

OpenTimestamps scales indefinitely, allowing timestamps to be created for free by combining an **unlimited number of timestamps into one blockchain transaction** by leveraging Merkle-tree

Convenience

There are multiple public OpenTimestamps **calendar servers**, free to use without any registration that can create a third-party-verifiable timestamp in about a second; you don’t need to wait for a blockchain confirmation

OpenTimestamps: Trust Minimization

OpenTimestamps attestation proofs can be verified independently from any server, vendor, or centralized infrastructure, simply using a local copy of the blockchain (e.g. a Bitcoin full node)

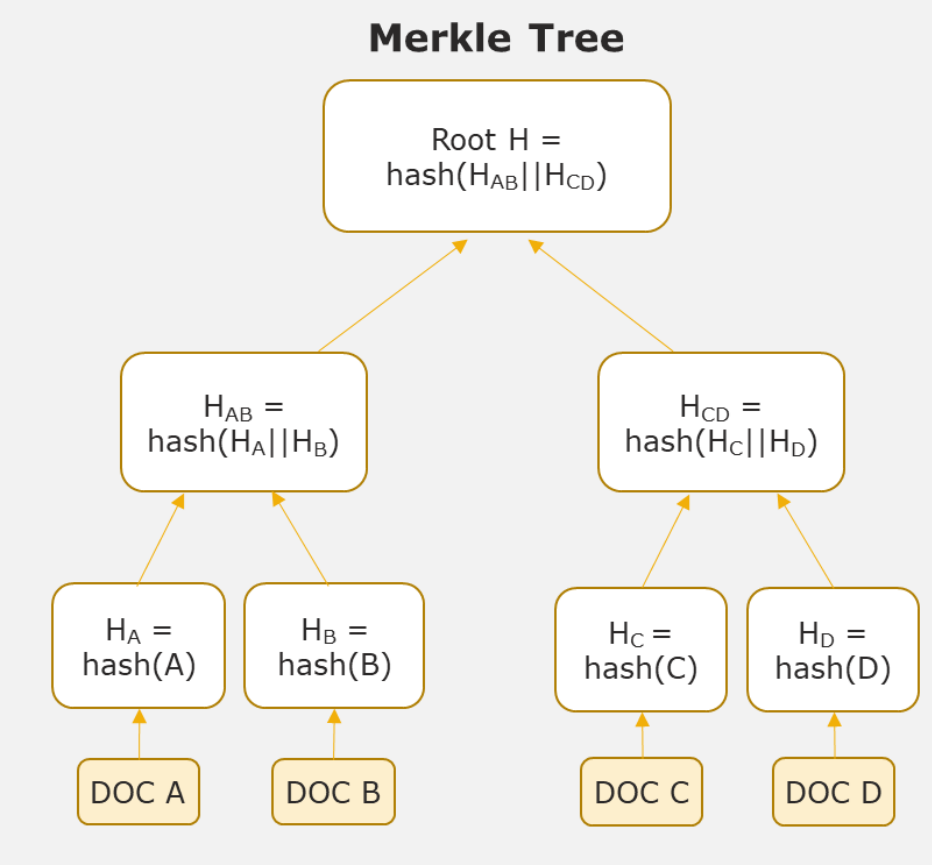
- Distributed, decentralized, independent, uncensorable, cross-jurisdictional
- Third party auditable, suitable for regulatory prescriptions

OpenTimestamps: Scalability

A single blockchain transaction **timestamps an unlimited number of documents**

An OpenTimestamps *calendar server* provides *"aggregation before attestation"*:

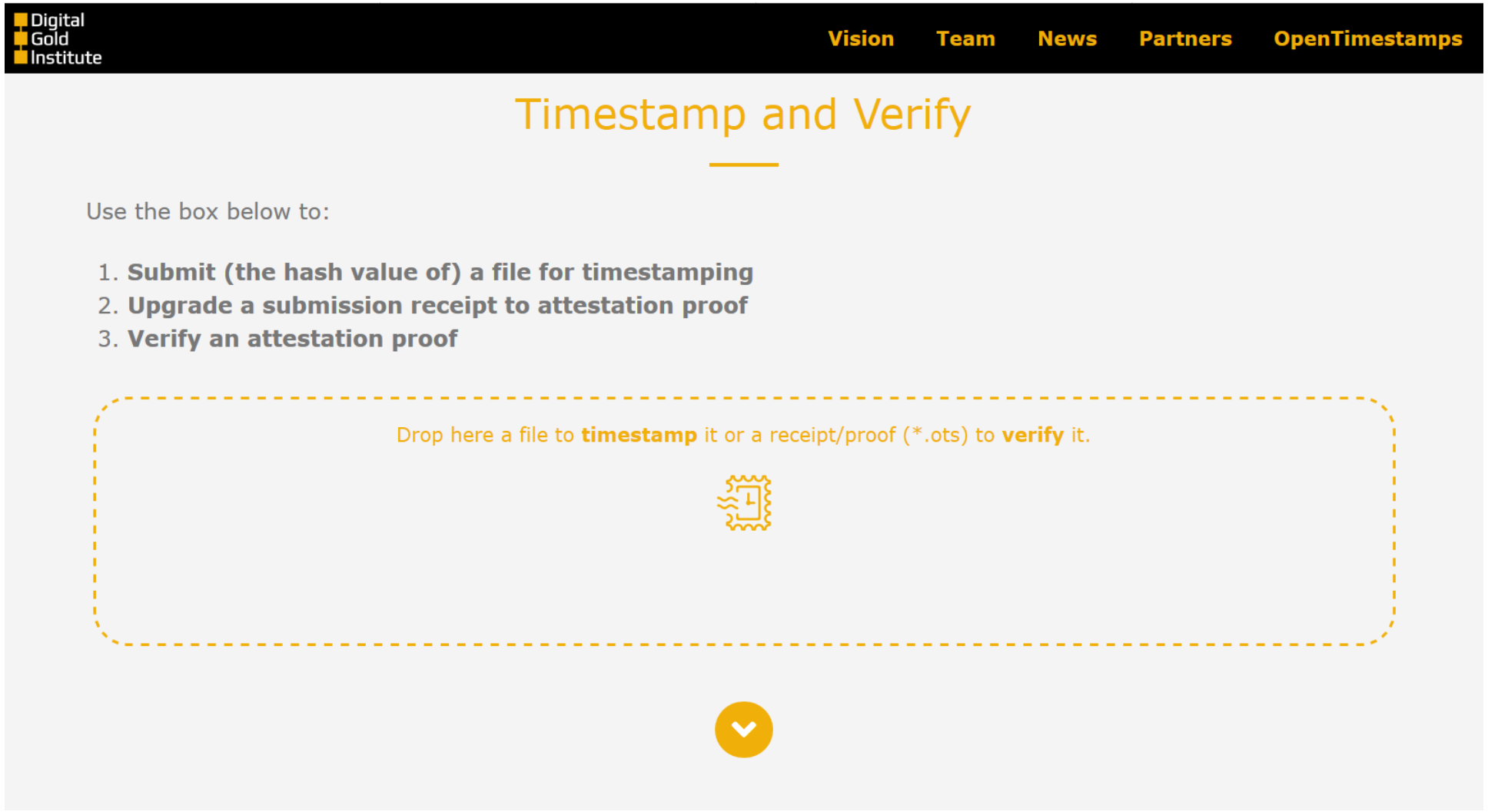
1. aggregation of multiple (hash values of different) documents in a **single Merkle tree** data structure
2. attestation of the Merkle tree root in a **single blockchain transaction**, achieving implicit attestation of all documents included in the tree



OpenTimestamps: Convenience

- While anyone can timestamp with permissionless blockchain(s) by paying the transaction fees (using the OpenTimestamps protocol or any alternative approach), there are multiple **public** OpenTimestamps **calendar servers**, **free to use** without any registration or API key (e.g. https://btc.ots.dgi.io)
- A single calendar server can offer its services to **multiple remote** OpenTimestamps clients
- Verifiable timestamp are created almost instantly
- The public free OpenTimestamps calendar servers use Bitcoin as timestamp notary, i.e. they make the Bitcoin transactions that will ultimately attest hash values in the Bitcoin blockchain

OpenTimestamps with Digital Gold Institute



https://www.dgi.io/ots/

Warnings (1/3)

- Attestation proofs can be verified independently from any OpenTimestamps server or facility. The same is not true for the submission receipt, which can only be upgraded to proof using the OpenTimestamps calendar(s) used for submission

- The user is responsible to store both the stamped document (which has never been shared with the OpenTimestamps servers) and its attestation proof (which technically might be stored by the OpenTimestamps servers)

Warnings (2/3)

While the OpenTimestamps protocol is blockchain agnostic, a timestamp is **as reliable as the used blockchain**:

- very reliable when using Bitcoin because that blockchain is secured by huge computational power (proof-of-work)
- much less reliable with other public permissionless blockchains
- when used with a private permissioned blockchain its reliability depends on the trustworthiness of the chain governance: in this case a traditional certification authority is probably better

Warnings (3/3)

It is worth mentioning that timestamping (using the OpenTimestamps protocol or any alternative approach):

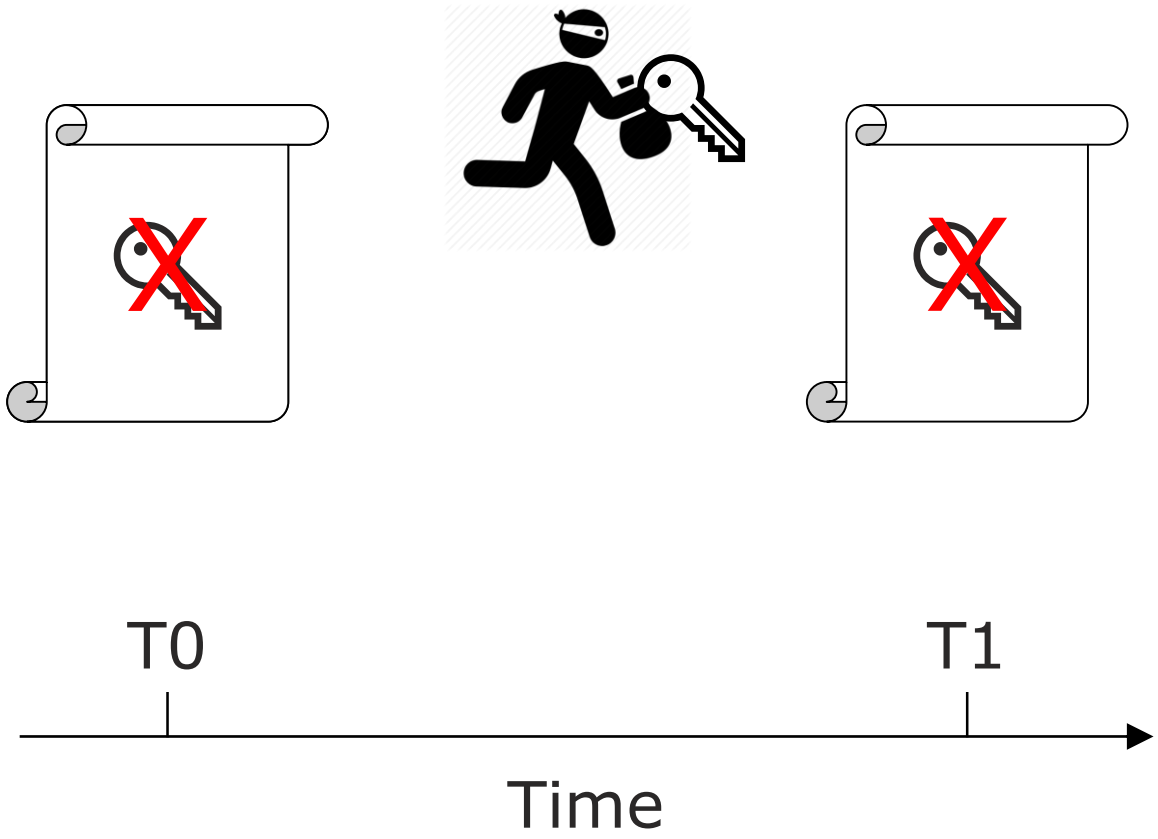
- **can be selectively revealed** to show convenient evidence and hiding inconvenient evidence (e.g. timestamping a bet on a given outcome and its opposite, later revealing only the realized one)
- **does not prove authorship** (that should be proved with a digital signature)
- **can be repudiate** if not digitally signed
- **does not ensure veracity**, validity, correctness, or accuracy of the timestamped document

Use Case 1: Digital Signature without Timestamping

- What if a signing private key is stolen?
- The key revocation certificate is issued to signal that signatures *after* the theft should be considered invalid

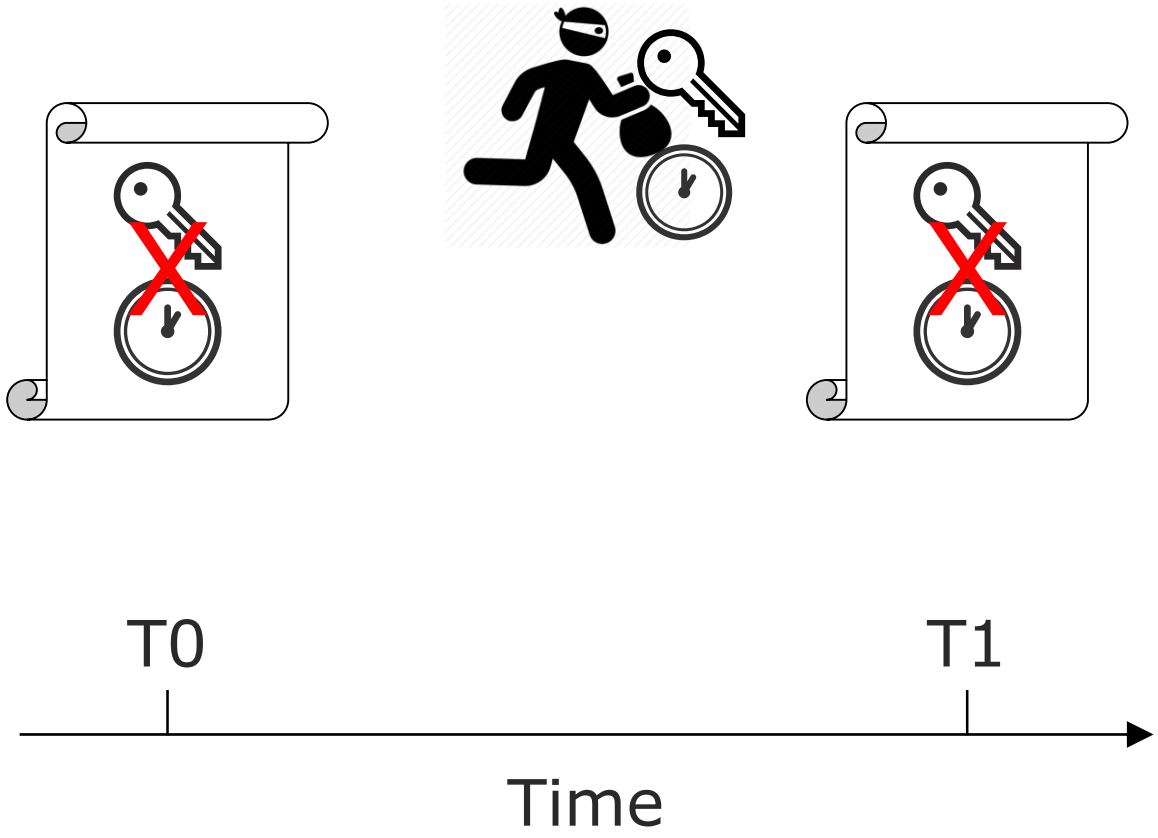
WRONG!!

- Every signature performed with that key should be considered invalid because the thief can backdate documents



Use Case 1: Digital Signature with Timestamping

- Traditional timestamping relies on a third-party central authority signing with its private key
- What if the timestamper's private key is stolen?
- Every timestamp created by that key must be considered invalid because the thief can backdate timestamps



Use Case 1: Digital Signature with Blockchain Timestamping

- Blockchain notarization is an effective hardening approach
- What if the traditional timestamper's private key is stolen?

Blockchain timestamps cannot be backdated!

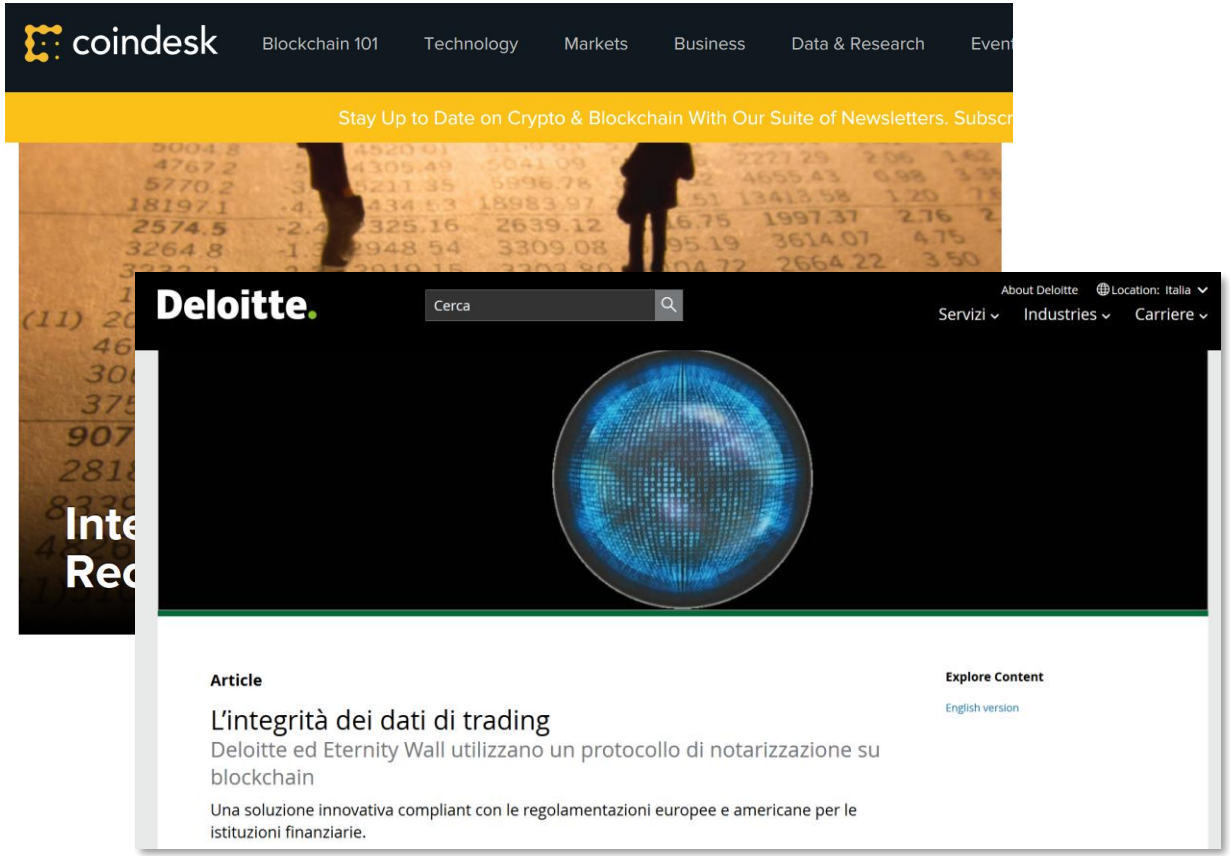
Use Case 2: Timestamp Internet

- OpenTimestamps is used to timestamp the whole Internet Archive https://archive.org/
- This has been possible thanks to the high scalability of the OpenTimestamps protocol
- For the first time historical archived data cannot be altered without being noticed

http://nova.ilsole24ore.com/progetti/la-blockchain-da-il-tempo-al-web/

Use Case 3: Regulatory Compliance

- Broker-dealers have started using notarization to satisfy the regulatory prescriptions for storing required records exclusively in non-rewriteable and non-erasable electronic storage media.
- WORM (write once read many) optical media has been used so far, but it is quite impractical, especially for large data set
- Compliance can be achieved anchoring rewritable data sources to the blockchain, providing accurate and secure time-stamping resilient to manipulation



http://www.coindesk.com/intesa-sanpaolo-trade-data-bitcoin-blockchain/
https://www2.deloitte.com/it/it/pages/financial-services/articles/l_integrita-dei-dati-di-trading---deloitte-italy---financial-ser.html

Use Case 4: Publicly Verifiable Certificates

It is easy to verify documents:

- signed by the issuer
- timestamped on blockchain

- It would be easy to provide public web-portals for drag-and-drop verification
- University of Milano-Bicocca guarantee the validity of degrees and certificates on the Blockchain

https://www.unimib.it/comunicati/milano-bicocca-certificati-laurea-garantiti-clic

Blockchain Certification: the Italian Law

- The “DL Semplificazioni” recognizes the legal validity of the blockchain timestamping
- AGID will have to provide technical specification

https://www.agendadigitale.eu/documenti/al-via-la-blockchain-revolution-ecco-tutte-le-novita-e-cosa-si-potra-fare/

Takeaways

- Blockchain timestamping is the decentralized digital alternative to traditional certification authorities
- The OpenTimestamps standard is trust-minimizing, scalable, and convenient
- Timestamping provides only proof of existence at a given date; it does not convey authorship, non-repudiation, veracity, guaranteed origin, etc.
- Most of the time, timestamping only makes sense if coupled with digital signature or alternative authorship proofs
- Centralized timestamping on private permissioned blockchain is no different from traditional Certification Authority
- For a decentralized timestamp to be reliable, it must use bitcoin

Crypto Asset Lab

Digital Gold Institute

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

cryptoassetlab@unimib.it cryptoassetlab.diseade.unimib.it @CryptoAssetLab @CryptoAssetLab Crypto Asset Lab