

# Blockchain beyond Monetary Application

Timestamping

*Paolo Mazzocchi*  
*Milan, June 5, 2019*

# 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:



The screenshot shows the Eternity Wall website interface. At the top left is the logo, which consists of two interlocking circles in blue and black. To the right of the logo is the text "Eternity Wall" in a large, black, sans-serif font. Below the logo and title is the text "Messages lasting forever" with a small upward-pointing triangle. A light gray box contains the following text: "Messages written on the wall are embedded in the blockchain, the public registry underneath [bitcoin](#). There are almost 100 thousands copies of this ledger all around the world and soon it will also be in space. Even if this site goes down or disappears, your message is guaranteed to persist for generations to come." Below this text are three categories, each with an icon and a description: "For love" with a heart icon and the description "Publicly declare your love for someone"; "In memory" with a book icon and the description "Memorialize an event or a person"; and "For fun" with a megaphone icon and the description "Just say hello to the entire world". The background of the website is a warm, orange-toned image of a mountain range.

# 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*



input data cannot be recovered  
from the output

*Collision-resistant*



computationally unfeasible to  
find 2 inputs that produce the  
same output

*Random oracle model*

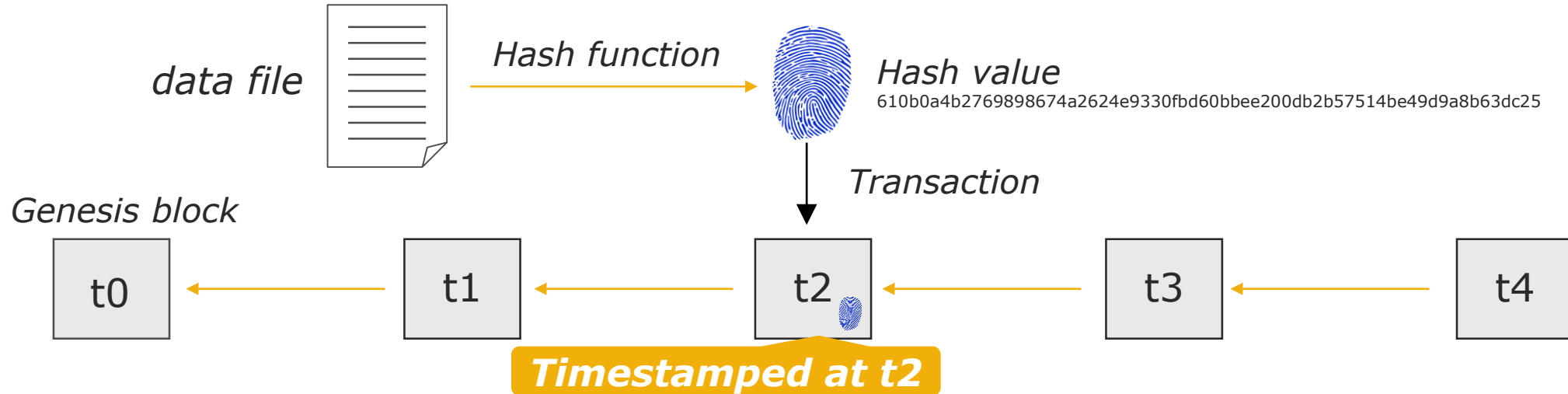


the hash value is so  
unpredictable to appear as if it  
was chosen uniformly at random

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 through 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



## A timestamping proof standard

OpenTimestamps aims to be a standard format for blockchain timestamping. The format is flexible enough to be vendor and blockchain independent.



- 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

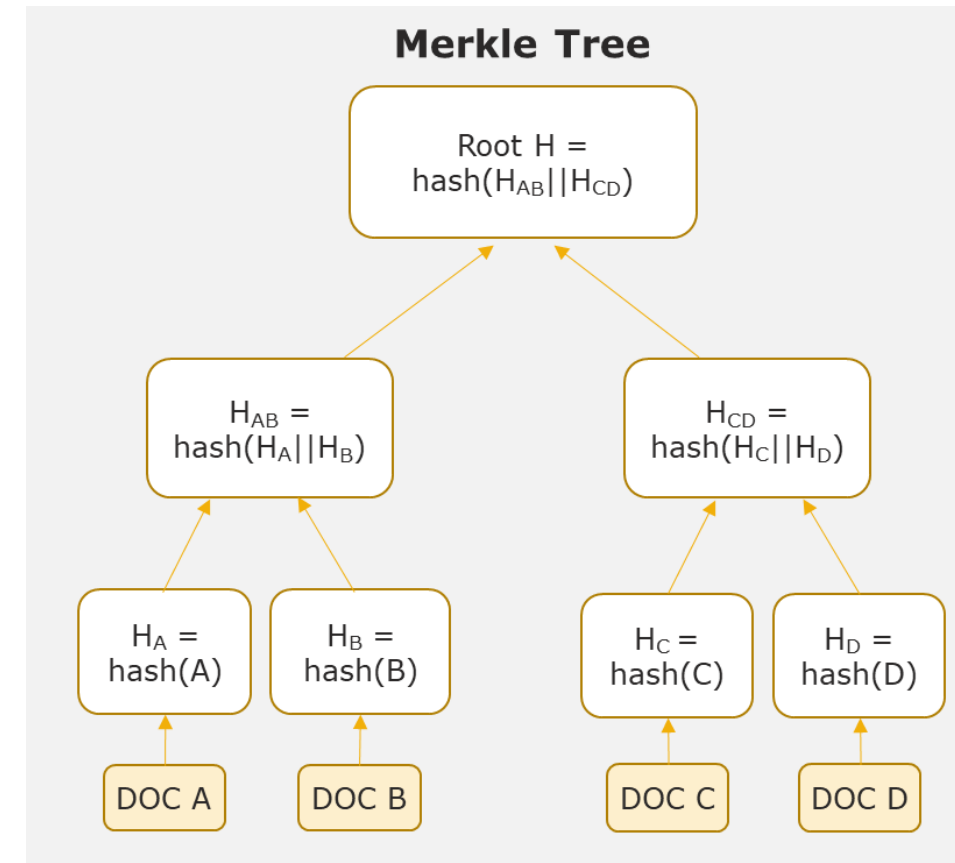


# OpenTimestamps: Scalability

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

## Timestamp and Verify

Use the box below to:

1. **Submit (the hash value of) a file for timestamping**
2. **Upgrade a submission receipt to attestation proof**
3. **Verify an attestation proof**

Drop here a file to **timestamp** it or a receipt/proof (\*.ots) to **verify** it.



# 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

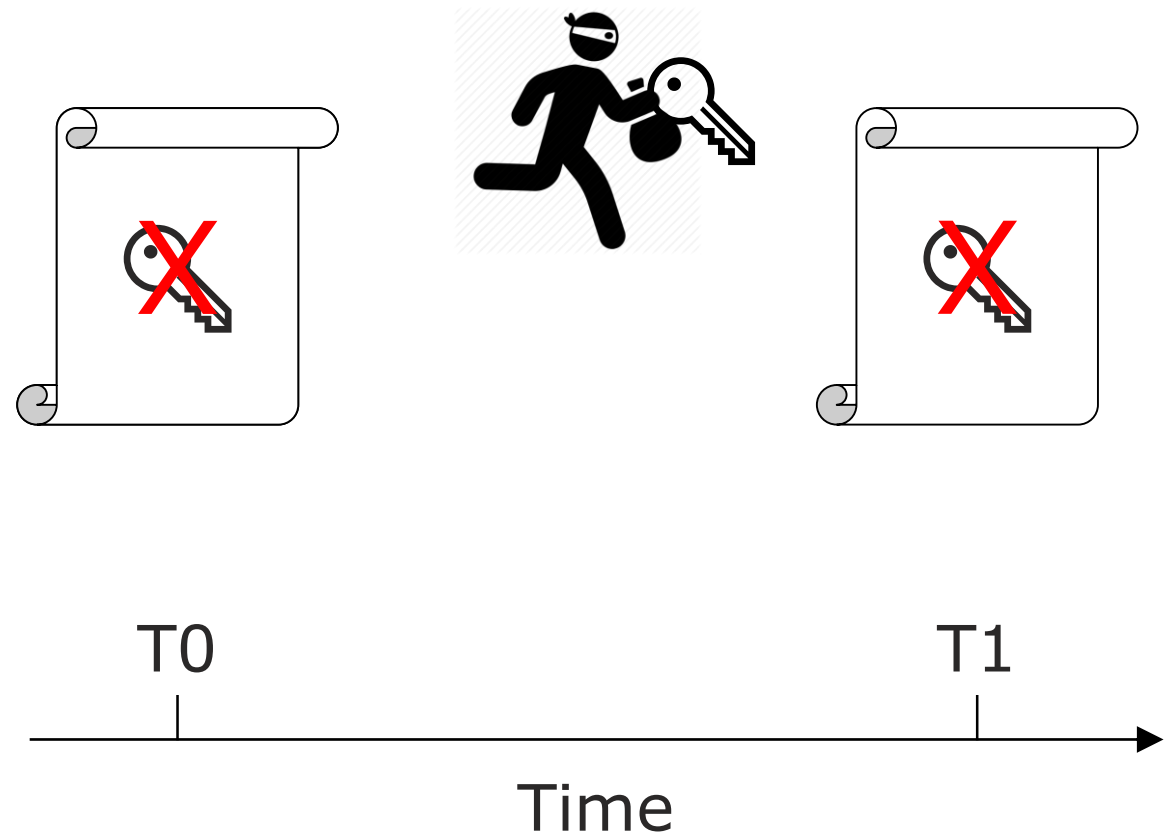


# Use Case 1: Digital Signature without Timestamping

- 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

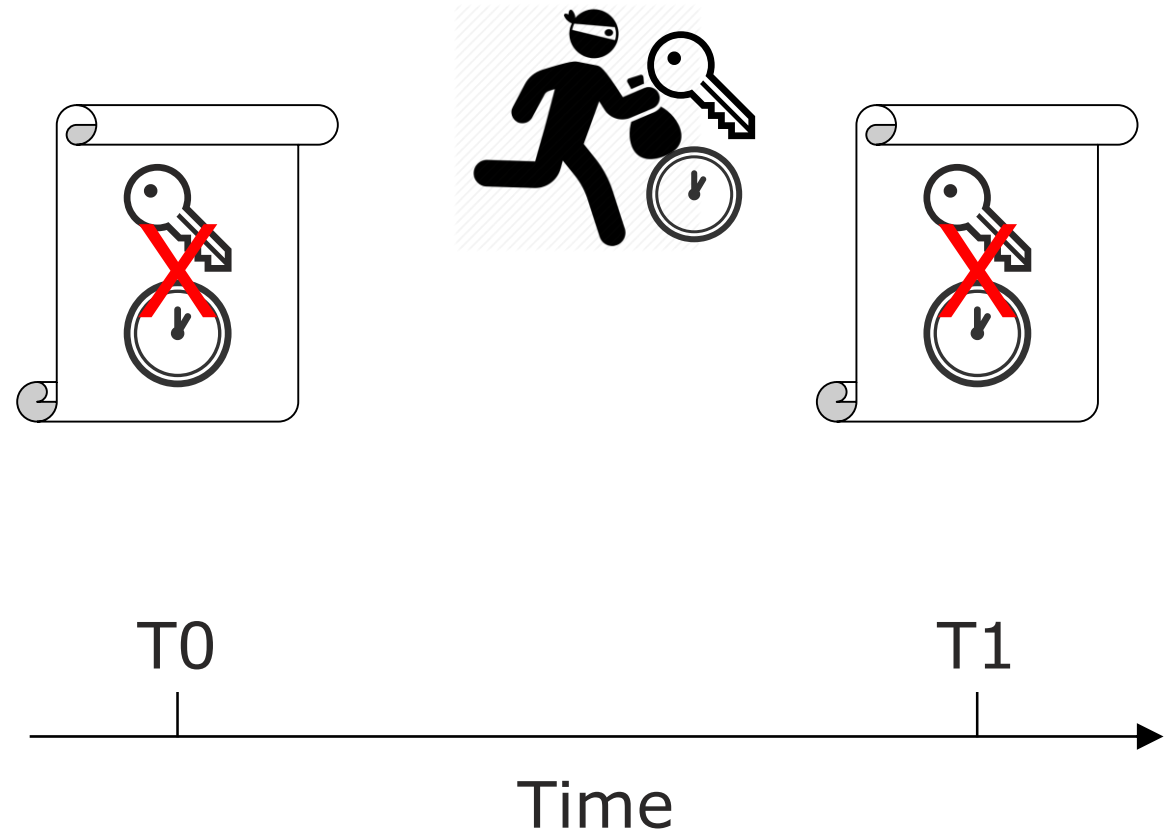
**WRONG!!**

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



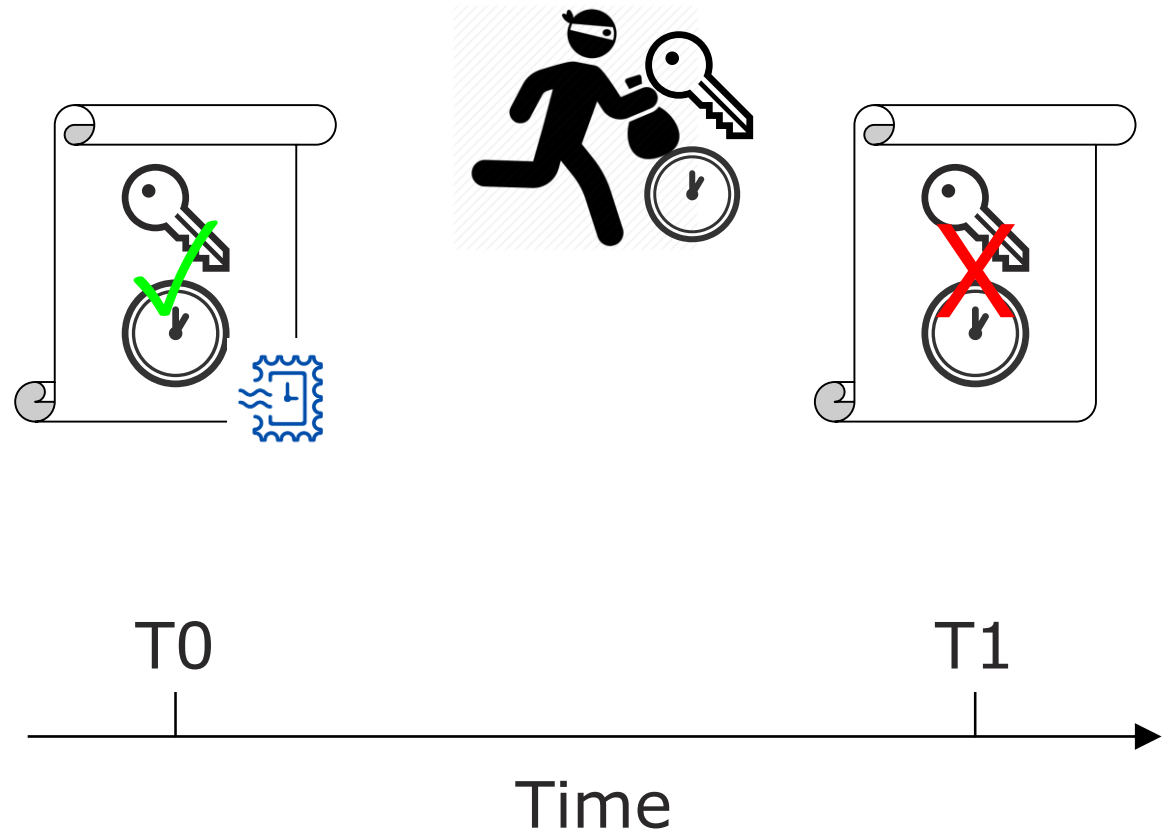
# Use Case 1: Digital Signature with Timestamping

- 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?



# 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

The image shows two overlapping web page screenshots. The top one is from Coindesk, featuring a dark header with the logo and navigation links for Blockchain 101, Technology, Markets, Business, Data & Research, and Events. Below the header is a yellow banner with the text 'Stay Up to Date on Crypto & Blockchain With Our Suite of Newsletters. Subscr'. The main content area has a background image of a stock market board with silhouettes of people. The bottom screenshot is from Deloitte, showing a search bar with the text 'Cerca' and a magnifying glass icon. The Deloitte logo is on the left, and navigation links for 'About Deloitte', 'Location: Italia', 'Servizi', 'Industries', and 'Carriere' are on the right. The main content area features a large blue globe graphic. Below the globe, the article title 'L'integrità dei dati di trading' is visible, along with a brief description: 'Deloitte ed Eternity Wall utilizzano un protocollo di notarizzazione su blockchain'. A link for 'Explore Content' and 'English version' is also present.

<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 guarantees the validity of degrees and certificates on the Blockchain



The screenshot shows the website of the University of Milano-Bicocca. The header includes the university logo and navigation links such as 'dipartimenti', 'biblioteca', 'comunicazione', 'dove siamo', 'lavora con noi', 'rubrica', 'CERCA', and 'accedi a...'. Below the header, there are navigation tabs for 'ATENEI', 'DIDATTICA', 'RICERCA', 'INTERNAZIONALIZZAZIONE', and 'SERVIZI'. A secondary navigation bar contains 'FUTURI STUDENTI', 'STUDENTI IMMATRICOLATI', 'STUDENTI INTERNAZIONALI', 'DOPO LA LAUREA', and 'ALUMNI'. The main content area displays a news article titled 'Milano-Bicocca, certificati di laurea garantiti con un clic' dated Wednesday, January 23, 2019. The article text states: 'Garantire l'autenticità del proprio titolo di laurea con un clic. E, dall'altra parte, poterne verificare la validità all'istante sul web, senza passare da richieste agli atenei e trafile burocratiche. L'Università di Milano-Bicocca ha introdotto un sistema informatico di blockchain, l'ultima frontiera in termini di sicurezza virtuale, per garantire agli studenti la validità e l'integrità di documenti e certificati ufficiali sul web. Sviluppata insieme al consorzio interuniversitario Cineca, la nuova tecnologia permette di emettere documenti digitali certificati, assicurando che non siano manipolabili o falsificabili. Uno strumento moderno, gratuito, semplice e immediato, utilizzabile ovunque nel mondo, grazie al quale gli studenti possono garantire l'autenticità e integrità dei loro titoli di laurea a potenziali datori di lavoro. Alle aziende e agli imprenditori basterà un clic per verificarne la validità, senza doverne fare richiesta agli atenei. Il nuovo sistema di certificazione, tra i primi in Italia e già attivo, verrà presentato durante il convegno "La certificazione blockchain nell'education", in programma venerdì 25 gennaio, dalle 14 alle 18, presso l'Auditorium Guido Martinotti (Edificio U12, via Vizzola 5, Milano), con interventi di esperti, docenti e ricercatori universitari. L'evento è promosso dall'Università di Milano-Bicocca insieme al consorzio Cineca e all'Università degli Studi di Padova, dove pure sarà avviato l'innovativo sistema di certificazione.'

<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



The screenshot shows a webpage from Agenda Digitale EU. The header includes the site name and a search icon. The main content area features a breadcrumb trail 'Home > Documenti Digitali', a share count of '613 condivisioni', and social media sharing icons for Facebook, Google+, LinkedIn, Twitter, Email, and a link icon. The article text discusses the legal implications of the DL Semplificazioni law, highlighting Italy's position as a leader in blockchain and distributed ledger technologies. The date '07 Feb 2019' is displayed at the bottom of the article snippet.

Agenda   Al via la blockchain revolution: ecco cosa po

Home > Documenti Digitali

613 condivisioni      

Passato il DL Semplificazioni, l'Italia si pone all'avanguardia su blockchain e tecnologie a registri distribuiti con una normativa che ha la stessa valenza rivoluzionaria per i documenti informatici della prima legge Bassanini. Ecco cosa si potrà fare senza intermediari con i registri distribuiti e gli smart contracts

07 Feb 2019

<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

The logo for Crypto Asset Lab features the text 'Crypto Asset Lab' in a bold, black, sans-serif font. To the left of the text is a yellow, 3D wireframe cube. To the right of the text is a vertical stack of three yellow squares, each connected to the one below it by a thin vertical line.

---

 Digital  
Gold  
Institute

UNIVERSITÀ DEGLI STUDI  
DI MILANO  
 BICOCCA

 [cryptoassetlab@unimib.it](mailto:cryptoassetlab@unimib.it)

 [cryptoassetlab.diseade.unimib.it](https://cryptoassetlab.diseade.unimib.it)

 [@CryptoAssetLab](https://twitter.com/CryptoAssetLab)

 [@CryptoAssetLab](https://facebook.com/CryptoAssetLab)

 [Crypto Asset Lab](https://linkedin.com/company/CryptoAssetLab)

*Nothing in this document constitutes an offer to buy or sell, or a solicitation of an offer to buy or sell, any financial instruments. It is not intended to represent the conclusive terms and conditions of any security or transaction, nor to notify you of any possible risks, direct or indirect, in undertaking such a transaction. No entity in Crypto Asset Lab shall be responsible for any loss whatsoever sustained by any person who relies on this document.*

*Nessun contenuto presente in questo documento costituisce e deve essere inteso come offerta all'acquisto o alla vendita o sollecitazione all'investimento in relazione a strumenti finanziari e non è inteso a rappresentare i termini e le condizioni definitivi di ogni strumento finanziario ovvero di ogni offerta avente ad oggetto strumenti finanziari, nè i rischi diretti od indiretti connessi alla stessa offerta. Nessuna entità del Crypto Asset Lab è responsabile delle perdite sostenute da una persona che si affida a questo documento.*