



# Eternity Wall

Riccardo Casatta e Valerio Vaccaro

Oltre i Bitcoin - OpenTimestamps: dal timbro postale alla blockchain

14 Maggio 2018

# Agenda

- Chi siamo e cosa facciamo
- Notarizzazione e OpenTimestamps
  - Introduzione a Bitcoin
- Casi d'uso
- Demo



# Chi siamo?

EW nasce nel 2015 per:

- scrittura di informazioni sulla blockchain
- voglia di sperimentare
- applicazioni non finanziarie su blockchain

Sviluppo app e sito per registrare messaggi sulla blockchain **immutabili ed incensurabili**.

[www.eternitywall.it](http://www.eternitywall.it)



 Eternity Wall - <https://eternitywall.com>

Brooke @bitcoincmom · 10 lug 2014  
Awww, my husband sent me a love note through the blockchain. For posterity.  
[blockchain.info/address/16wMx1...](https://blockchain.info/address/16wMx1...)

3 23

Riccardo Casatta @RCasatta · 11 lug 2014  
@bitcoincmom really nice :) but that annotation is saved on [blockchain.info](https://blockchain.info) site, not in the blockchain

1 1

Brooke @bitcoincmom · 11 lug 2014  
@RCasatta good point :)

PREFERITO  
1

12:46 - 11 lug 2014 - Dettagli

Nascondi



- 12 giugno 2017 4.45 GMT  
Today is my birthday! -- Efe :)
- 11 giugno 2017 16.04 GMT  
test
- 11 giugno 2017 0.41 GMT  
Enri & Andre si sono amati
- 10 giugno 2017 11.04 GMT  
NA-AT FAD Tech Alfredo
- 10 giugno 2017 8.35 GMT  
NA-AT FAD Tech
- 9 giugno 2017 14.40 GMT  
Hi there! What's up?
- 8 giugno 2017 1.37 GMT  
GisSkyne@R 8 giugno 2017 1.37 GMT  
Marlene
- 8 giugno 2017 11.22 GMT  
Ced F. (FR) was here. 2382EUR
- 7 giugno 2017 11.22 GMT  
Joshua Crooks △ Semper Fratres
- 6 giugno 2017 4.43 GMT  
türkçe de olsun aq
- 5 giugno 2017 8.00  
Joshua Crooks , Sean Nelson
- 4 giugno 2017 11.08  
test
- 4 giugno 2017 11.08  
You are on my mind 24/7

# Chi siamo?

Ma come sfruttare queste competenze in ambito business? Quali informazioni rilevanti per il business possono essere memorizzati su blockchain?



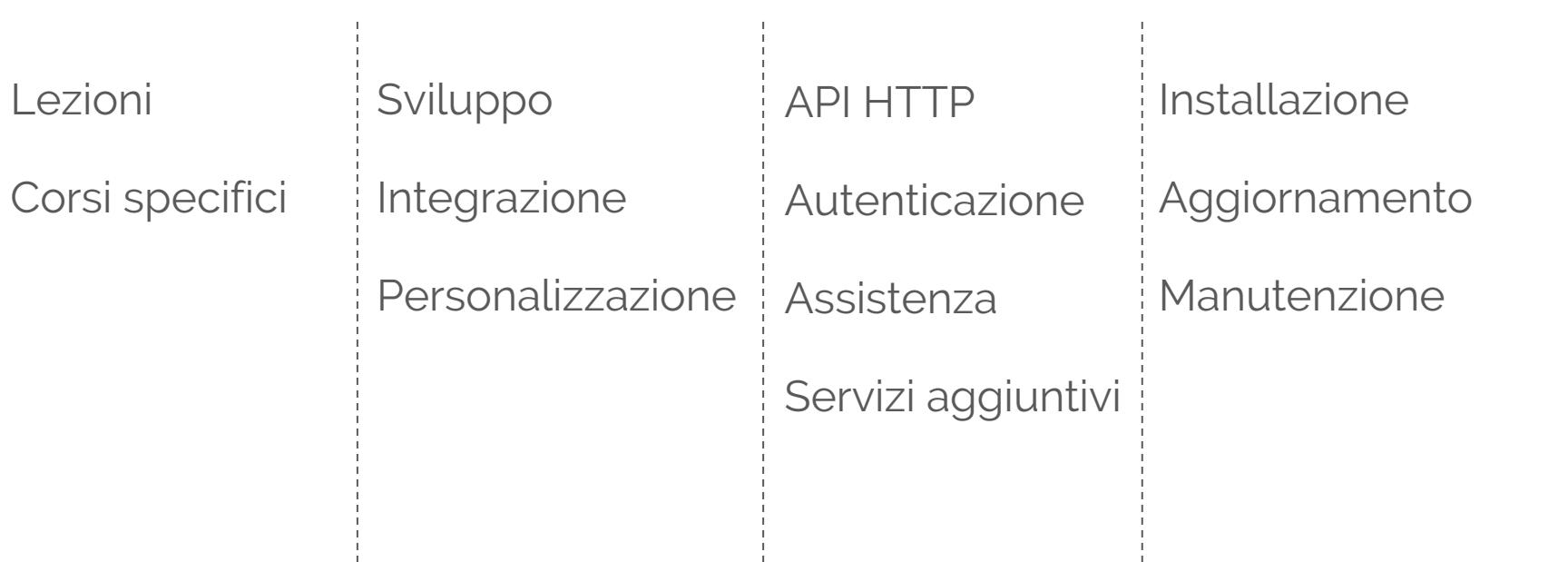
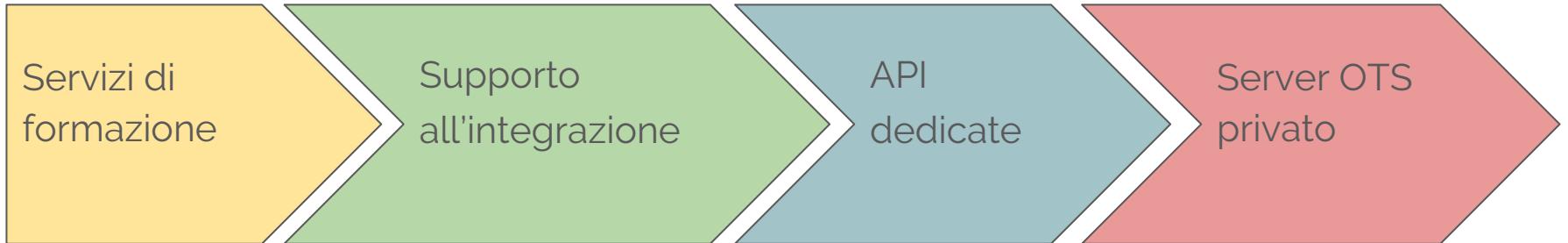
Necessità di attribuire una data certa ad un documento.



Nascita protocollo **OpenTimestamps**  
<https://opentimestamps.org>



# Business model



# Timestamping o marcatura temporale



- Il primo e più comune esempio è il **timbro postale**
  - Alice scrive a Bob, la data della comunicazione è apposta da terzi, nè Alice nè Bob possono contraffarlo facilmente
  - Attenzione: deve essere apposto sul documento e non sulla busta!
- Per importanti documenti deve essere posta da pubblico ufficiale, il notaio
  - Ad esempio per il rogito della casa

E per i documenti digitali?

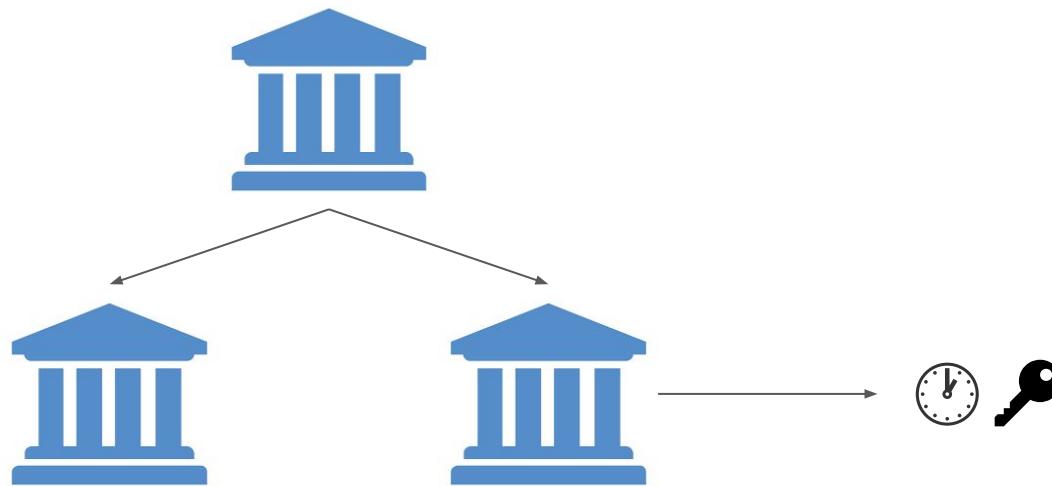
# Agenda

- Chi siamo e cosa facciamo
- Notarizzazione e OpenTimestamps
  - Introduzione a Bitcoin
- Casi d'uso
- Demo



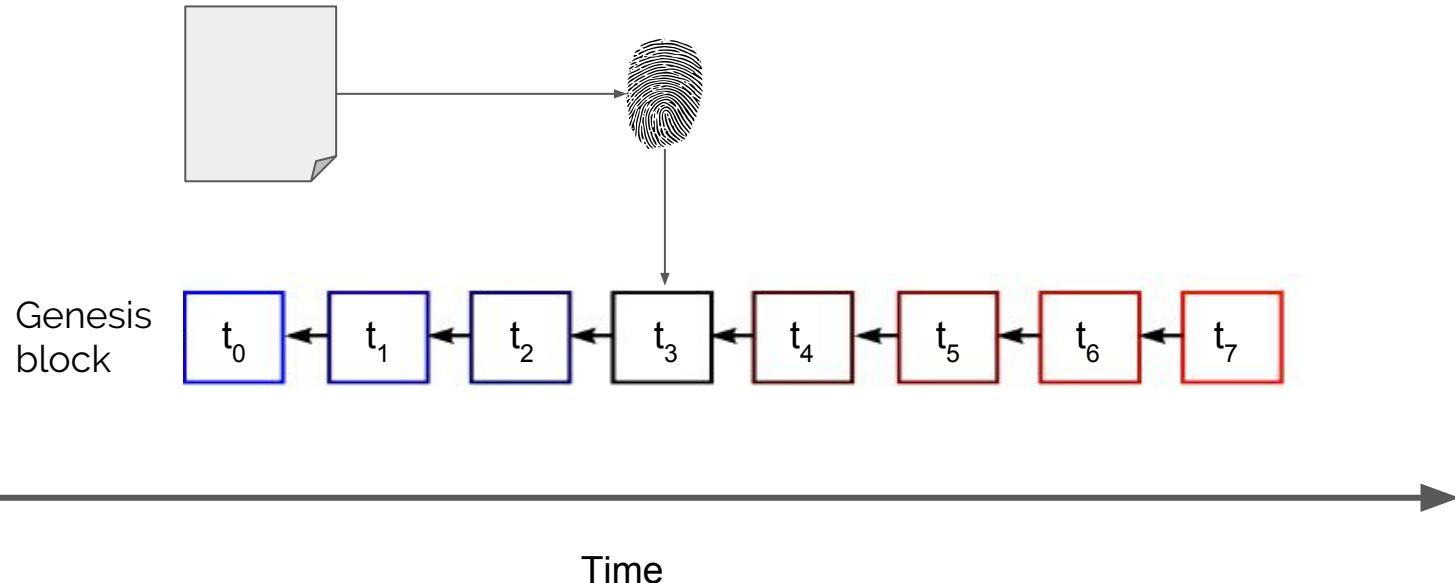
# Marcatura temporale certificata

- Basata su firma digitale
- Basata su certification authority
  - Ad esempio la PEC



# Marcatura temporale decentralizzata

Utilizza la blockchain in luogo della terza parte



# Introduzione a Bitcoin

## Bitcoin: A Peer-to-Peer Electronic Cash System

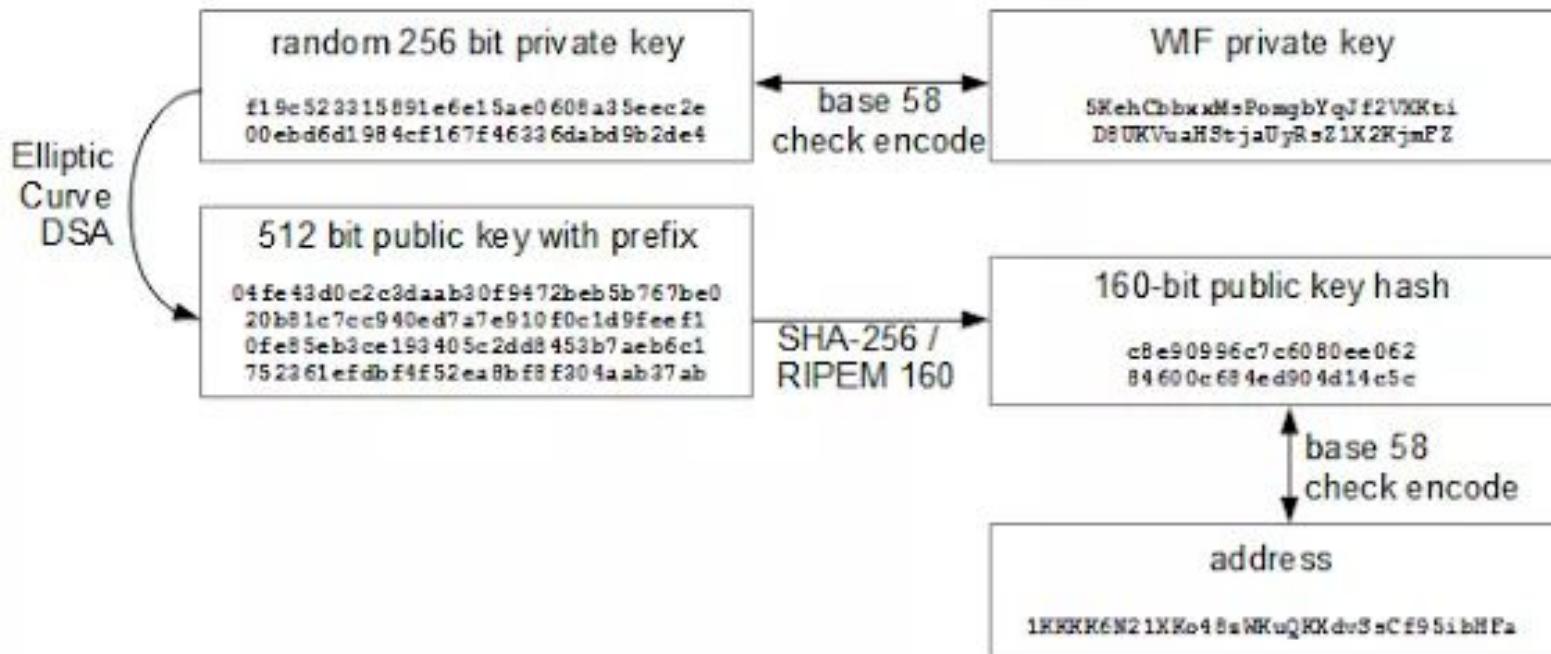
Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.



# Introduzione a Bitcoin: chiavi ed indirizzi

## Bitcoin Keys



# Introduzione a Bitcoin: blocchi e transazioni

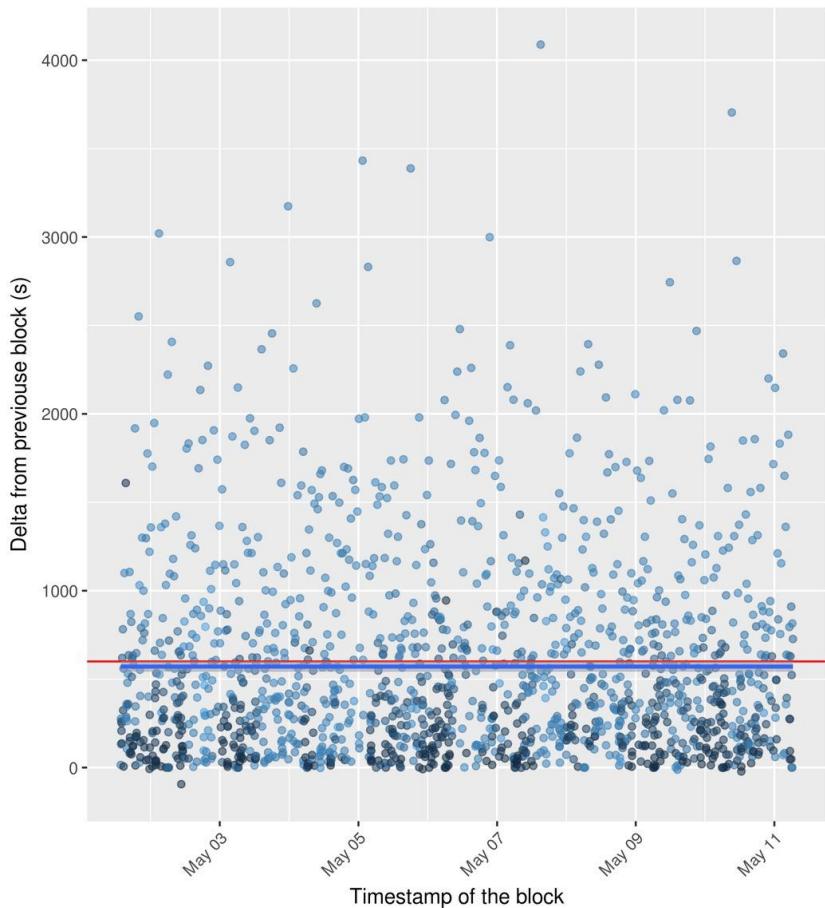
version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c8170100000000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	

version	01 00 00 00
input count	01
input	previous output hash (reversed) 48 4d 40 d4 5b 9e a0 d6 52 fc a8 25 8a b7 ca a4 25 41 6f b5 0c d7 32 c8 b4 81
	previous output index 00 00 00 00
	script length
	scriptSig script containing signature
	sequence ff ff ff ff
output count	01
output	value 62 64 01 00 00 00 00 00 00
	script length
	scriptPubKey script containing destination address
block lock time	00 00 00 00

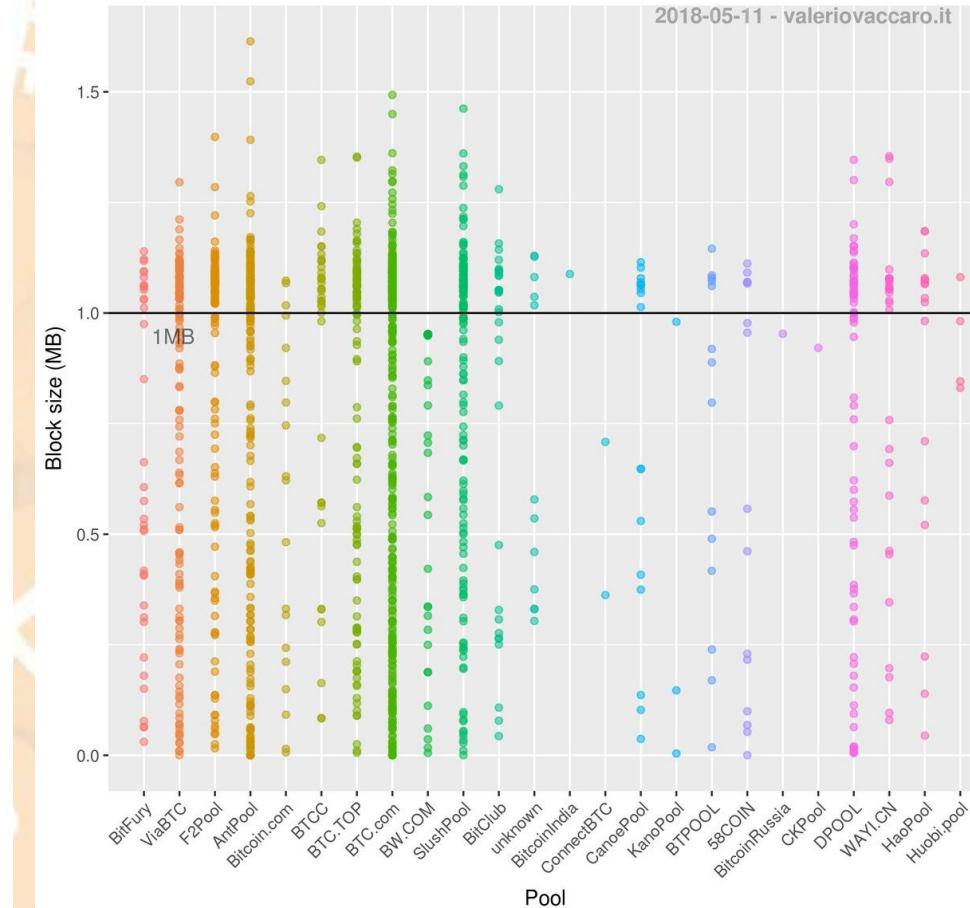


# Introduzione a Bitcoin: velocità e spazio

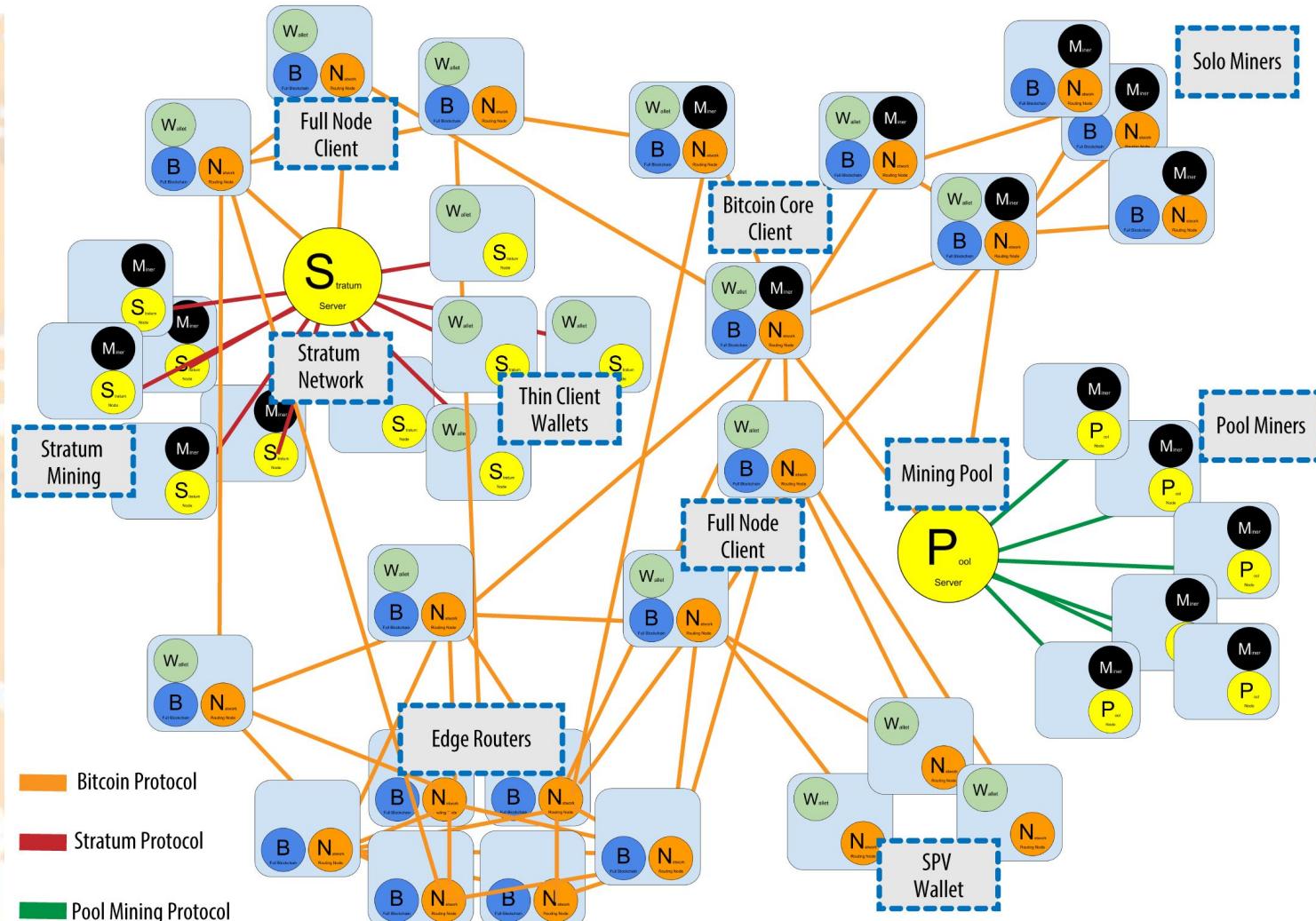
Block delay in 10 days



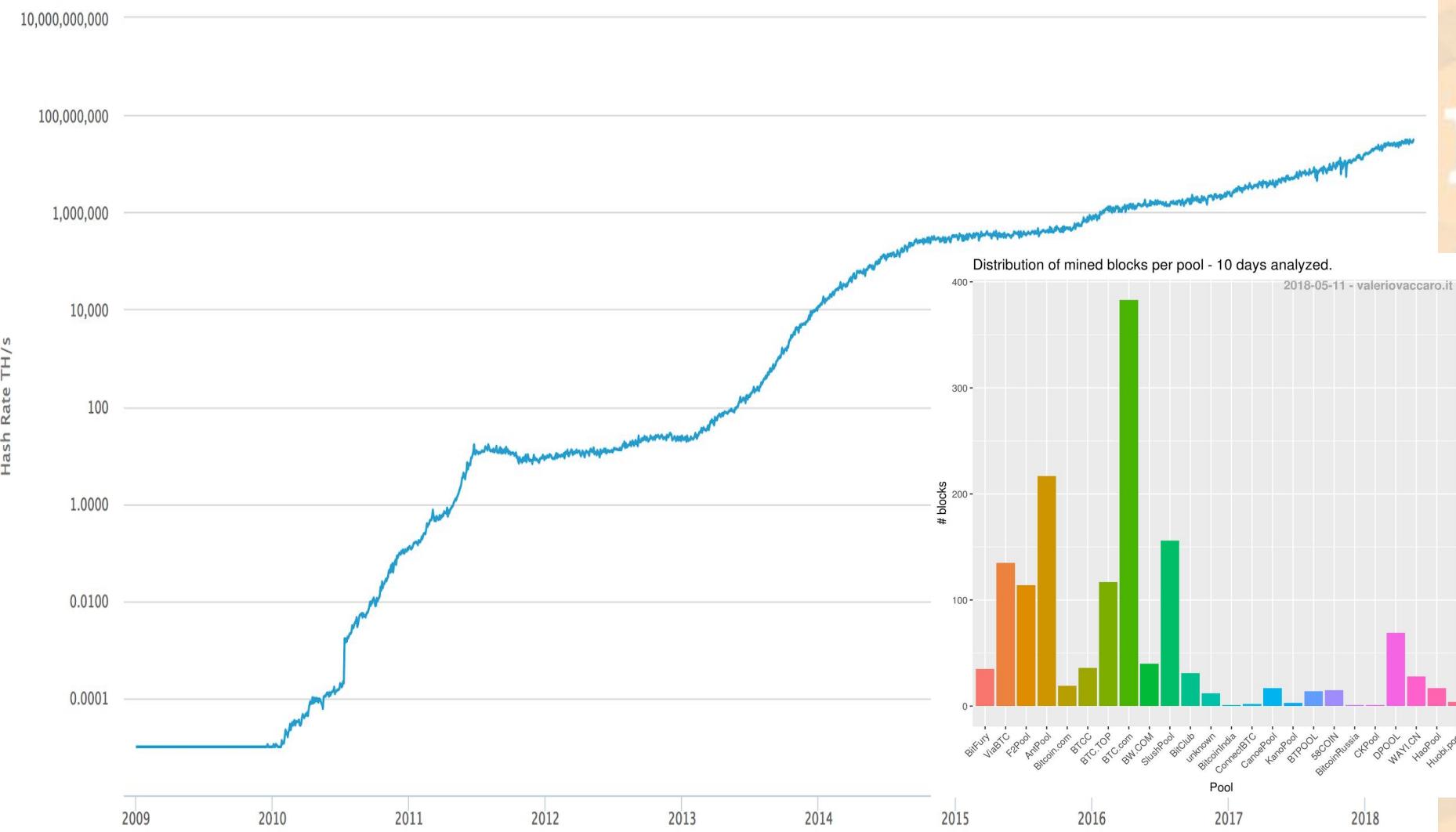
Distribution of blocks per pool - 10 days analyzed.



# Introduzione a Bitcoin: architettura della rete



# Introduzione a Bitcoin: mining



# Differenza fra trusted e trustless timestamping

Nel modello basato su terze parti, cosa succede se una chiave viene compromessa?

Basta revocare il relativo certificato, da quel momento in poi tutte le marcature temporali sono considerate invalide



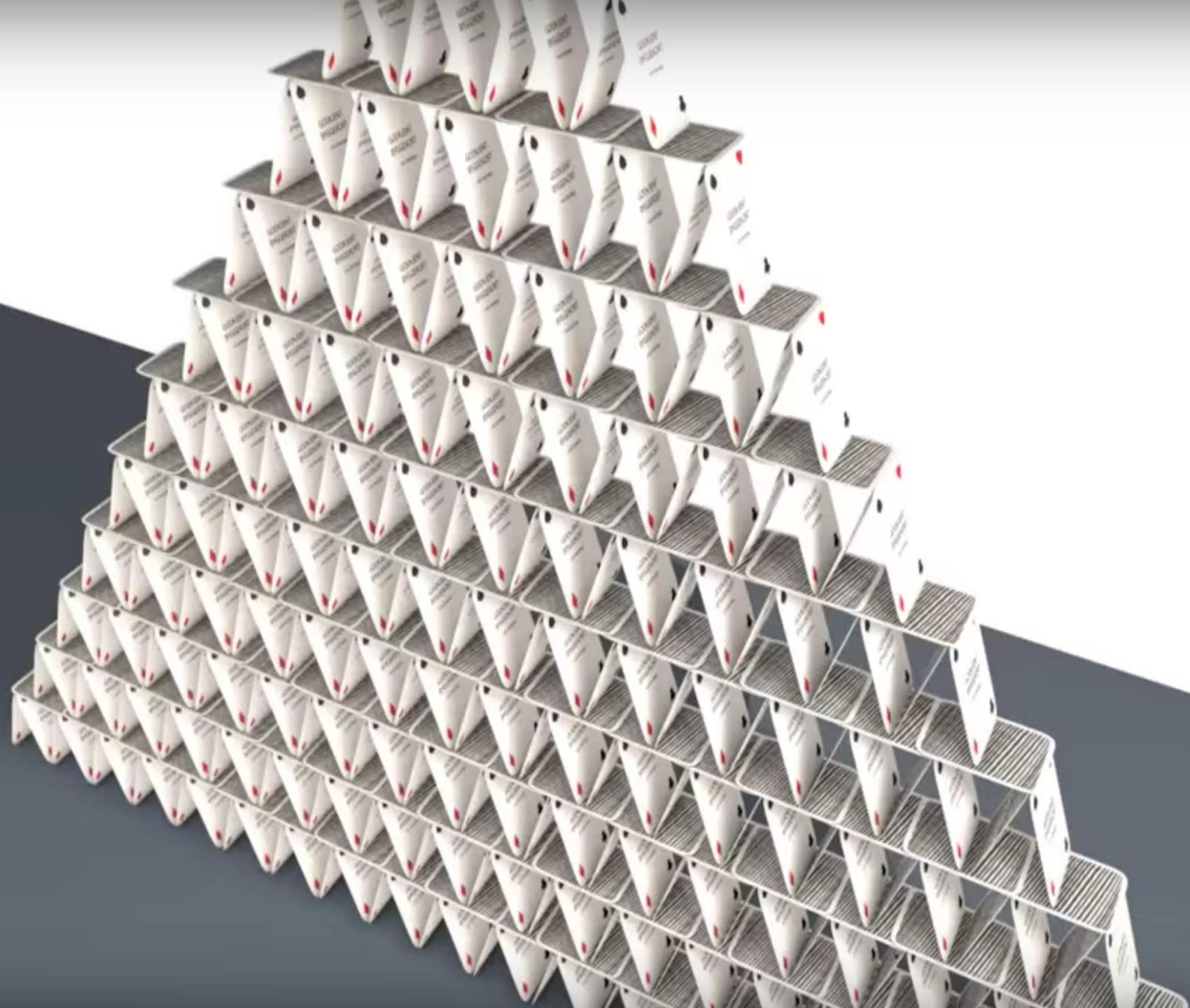
# Differenza fra trusted e trustless timestamping

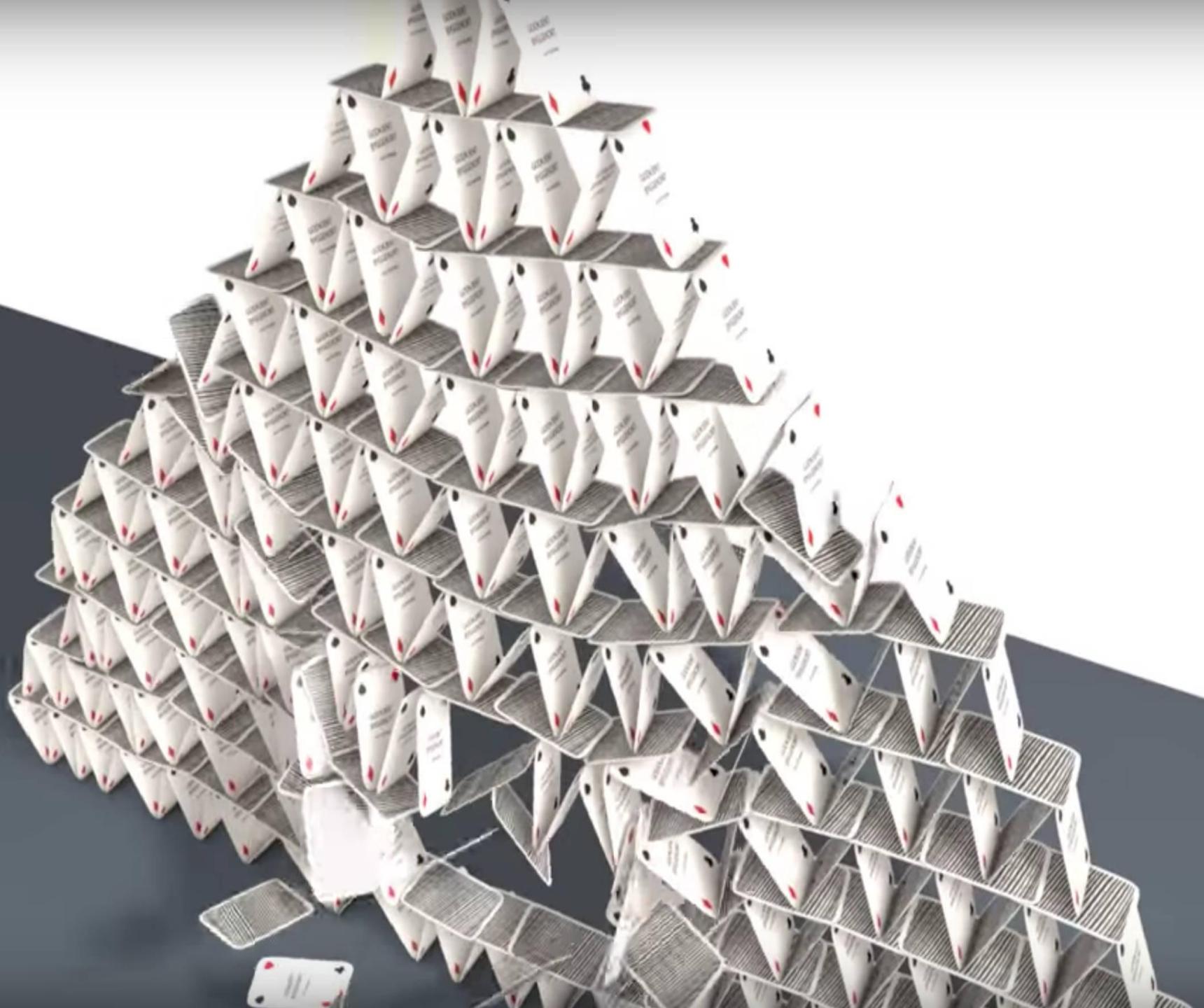
Nel modello basato su terze parti, cosa succede se una chiave viene compromessa?

Basta revocare il relativo certificato, da quel momento in poi tutte le marcature temporali sono considerate invalide

## Errato

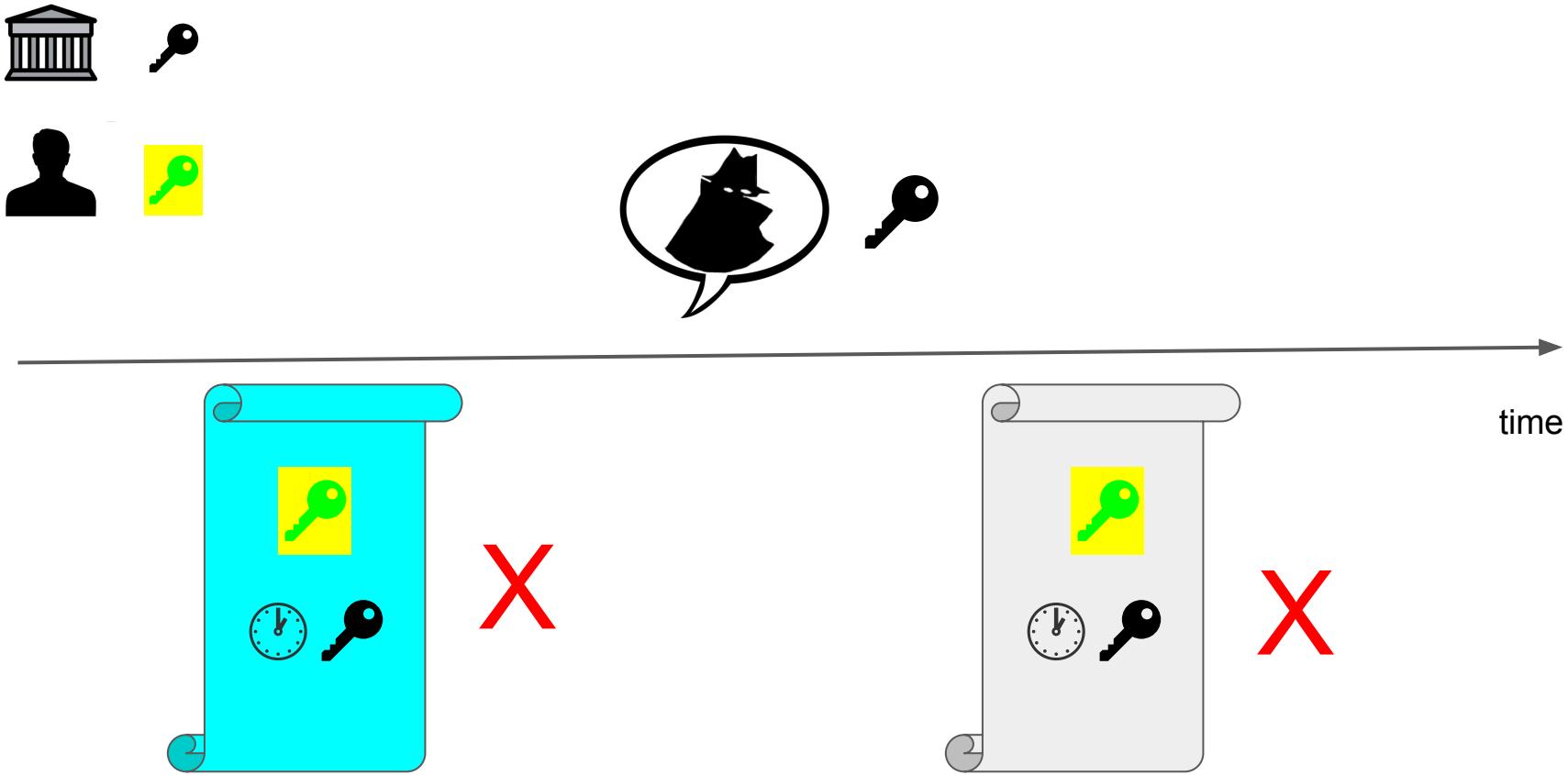
**Ogni** marcatura temporale mai creata da quel certificato deve essere considerata inattendibile, poiché chi possiede la chiave può semplicemente firmare date passate



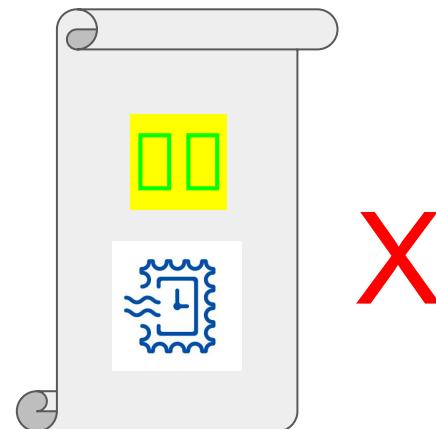
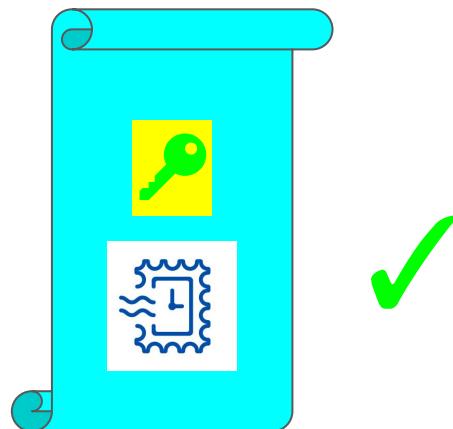




# Marcatura temporale basata su firma digitale



# Firma digitale con marcatura temporale trustless



time

# Blockchain pubblica o privata?

- Ai fini della marcatura temporale, utilizzare una blockchain privata non è differente dall'utilizzare la marcatura temporale basata su terze parti fidate.
- Utilizzare una blockchain pubblica per la marcatura temporale significa un cambio di paradigma, una rivoluzione del sistema esistente con vantaggi sia in termini di sicurezza che di costi.

# Timestamping and proof of publication

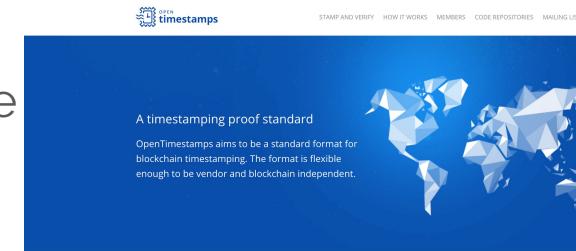
- Timestamping
  - An external viewer **could not** see all the element of the set
    - If someone timestamp two different version of a document, the rest of the world cannot see it
- Proof of publication
  - An external viewer **could** see all the element of the set
    - Prevent double spend!
    - Bitcoin UTXO (Unspent Transaction Output)
    - Very Expensive!



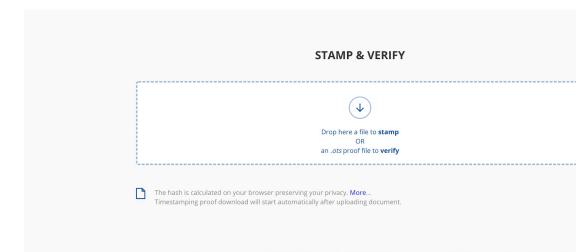
# OpenTimestamps

OpenTimestamps è un protocollo standard per la notarizzazione di qualsiasi informazione digitale con le seguenti caratteristiche:

- **Trust** - OTS usa la blockchain bitcoin risultando decentralizzato, pubblicamente verificabile e rimuovendo la necessità di una certification authority,
- **Cost** - OTS può condensare un numero illimitato di timestamps in una singola transazione,
- **Convenience** - OTS genera un timestamp verificabile direttamente da una terza parte in un solo secondo.

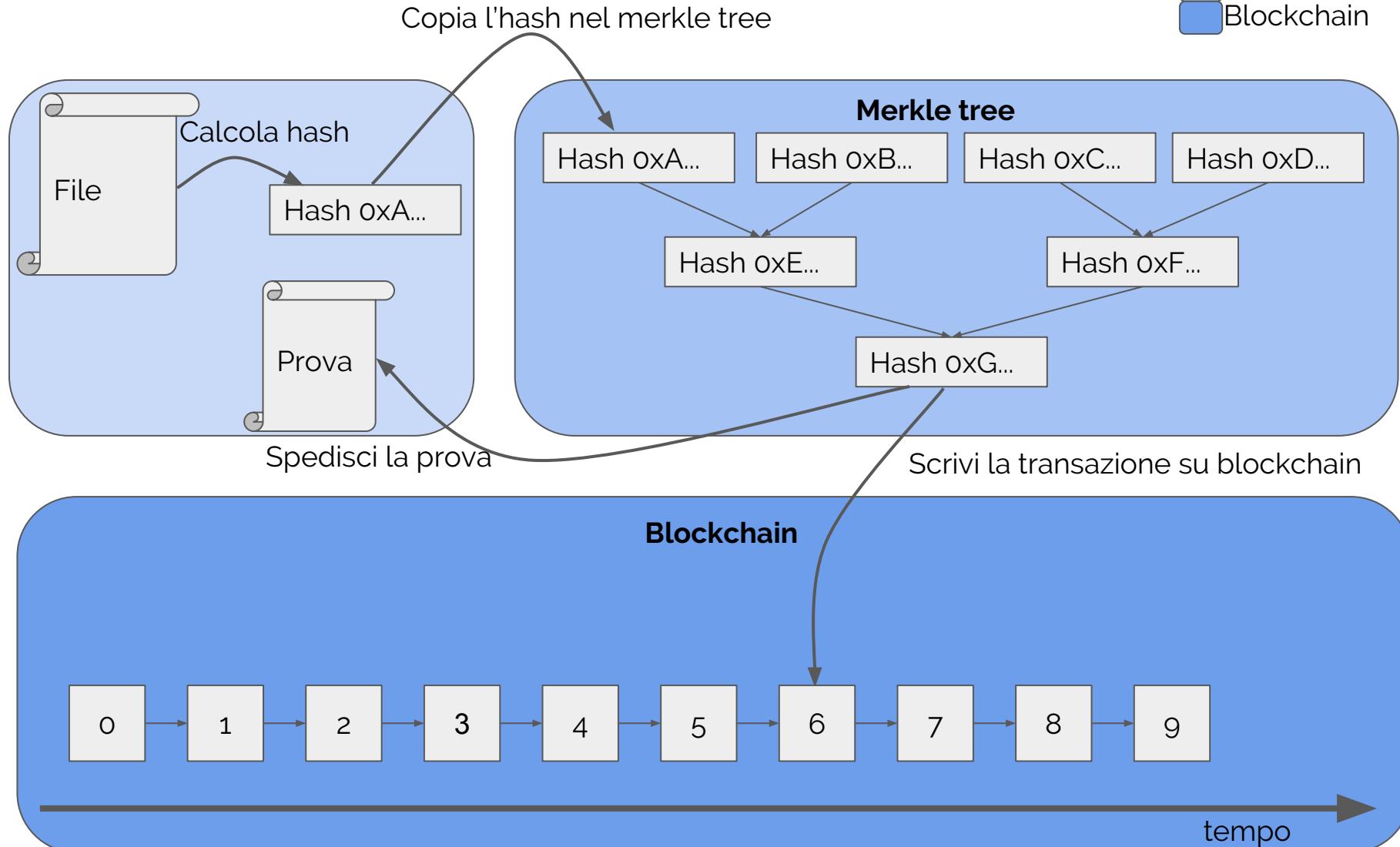


<https://opentimestamps.org>

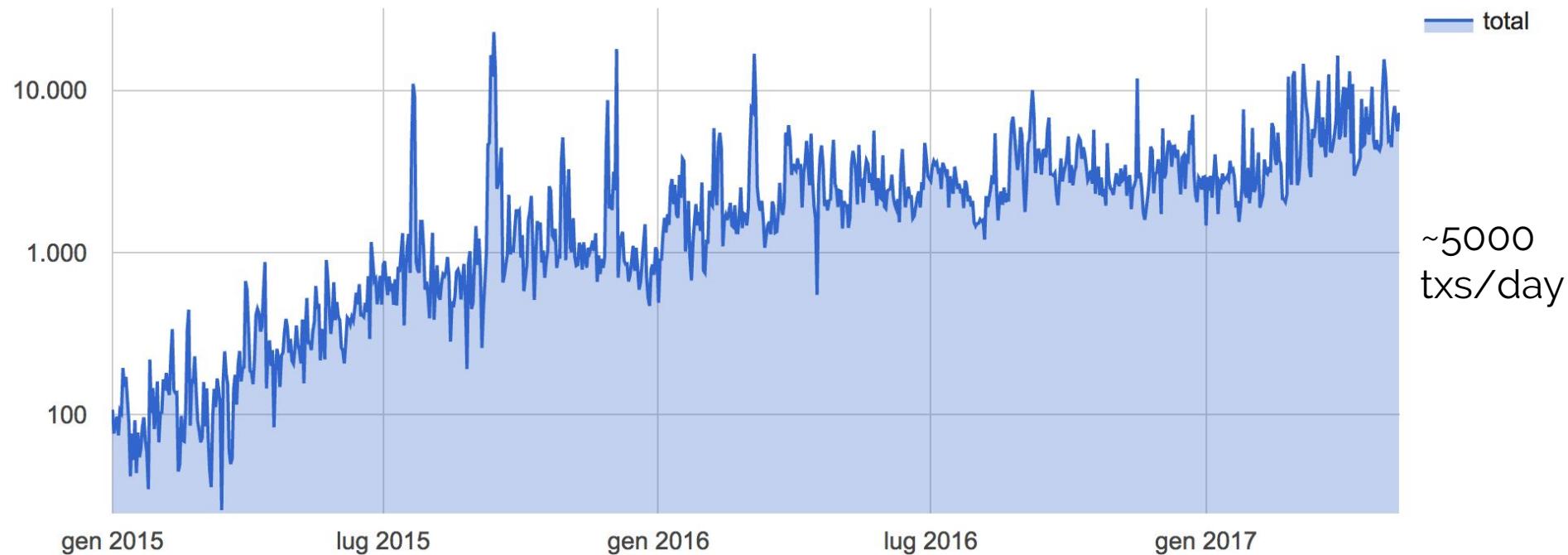


# OpenTimestamps

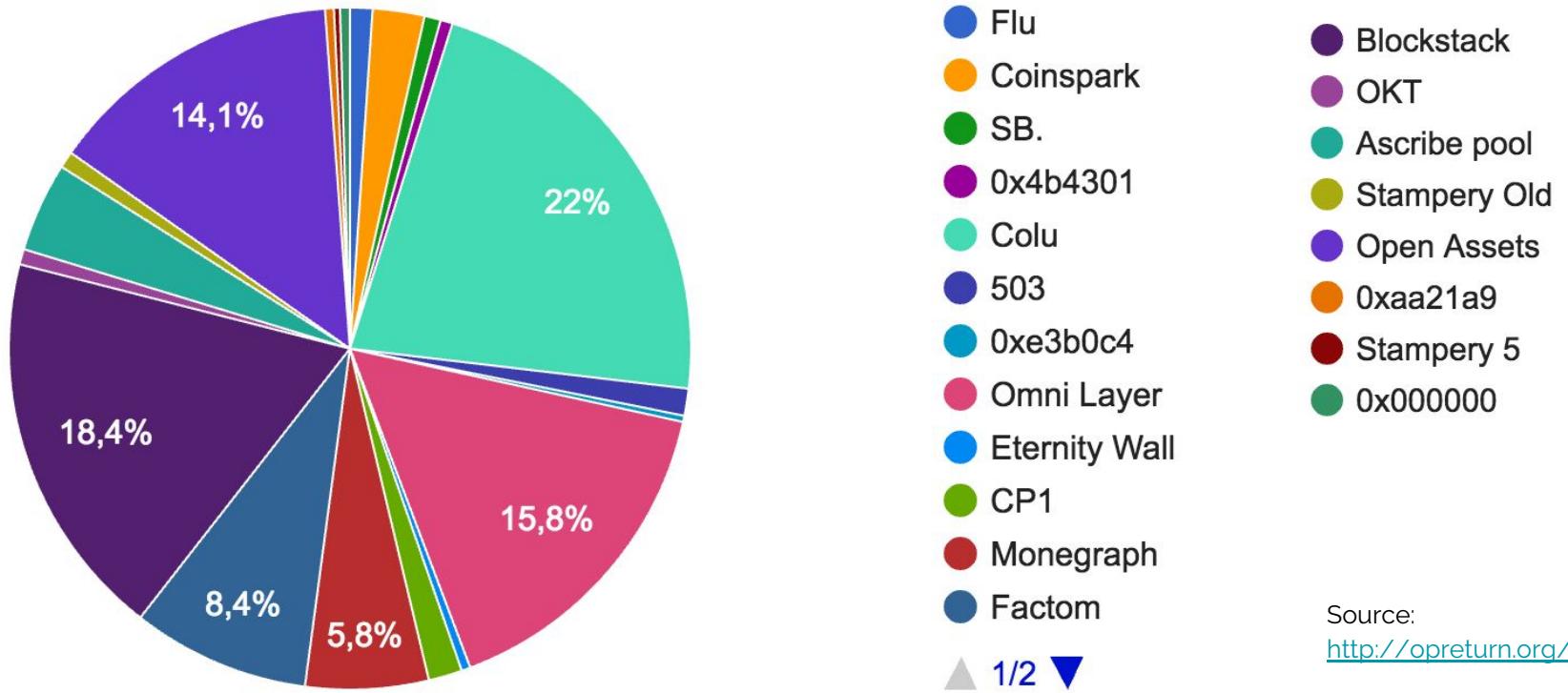
Client  
Calendar server  
Blockchain



# OP\_RETURN tx per giorno



# Utilizzo di OP\_RETURN



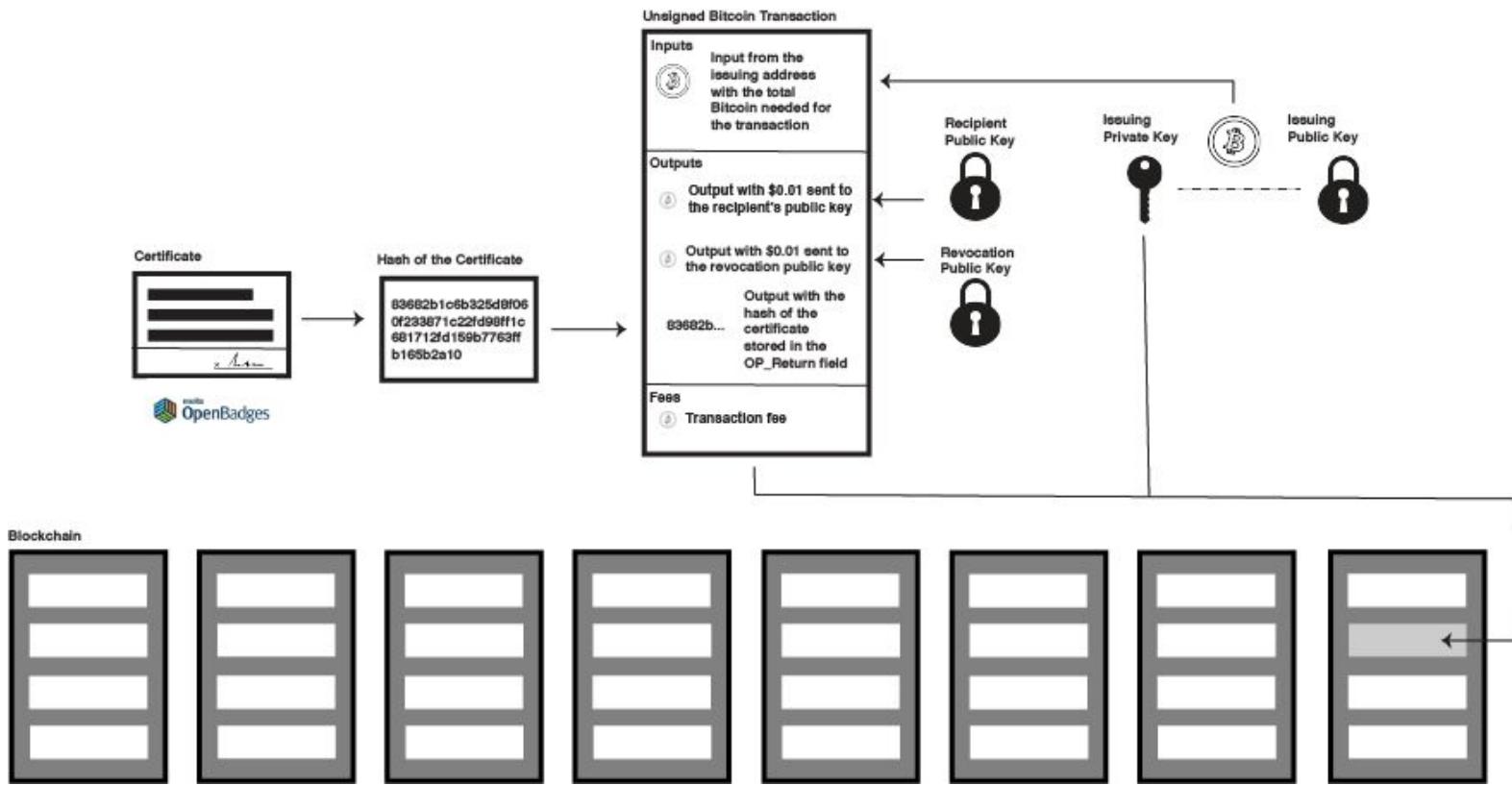
# Utilizzo di OP\_RETURN

~30% per timestamping

~2000 tx/giorno =~ 2000 \$/giorno



# One-certificate-one-transaction



# One-certificate-one-transaction

3000 degrees/year \* 40 exam/year \* 40000 universities ≈ ...



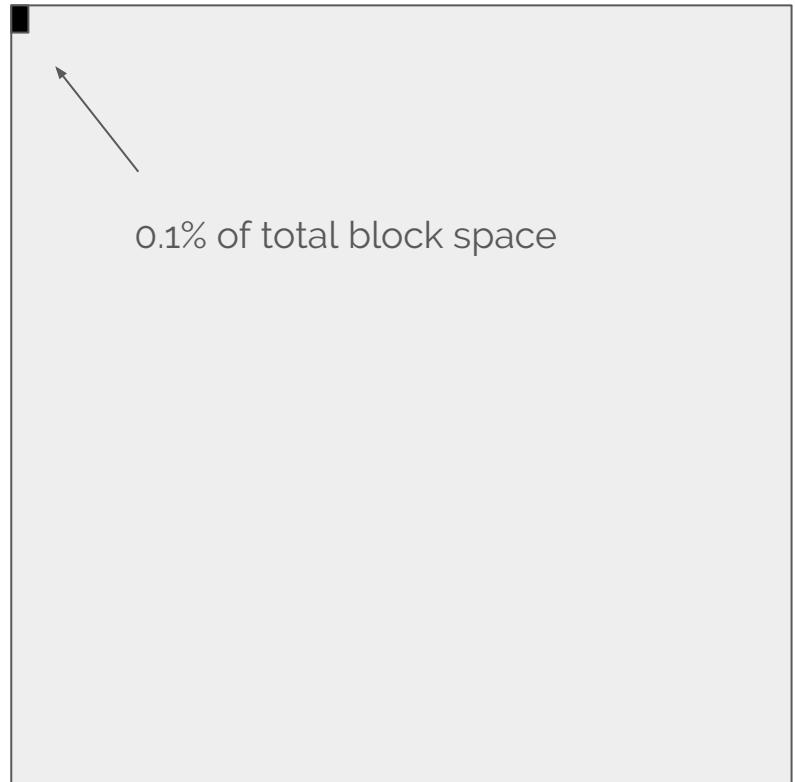
# One-certificate-one-transaction

3000 degrees/year \* 40 exam/year \* 40000 universities ≈ ...

80MB blocks!

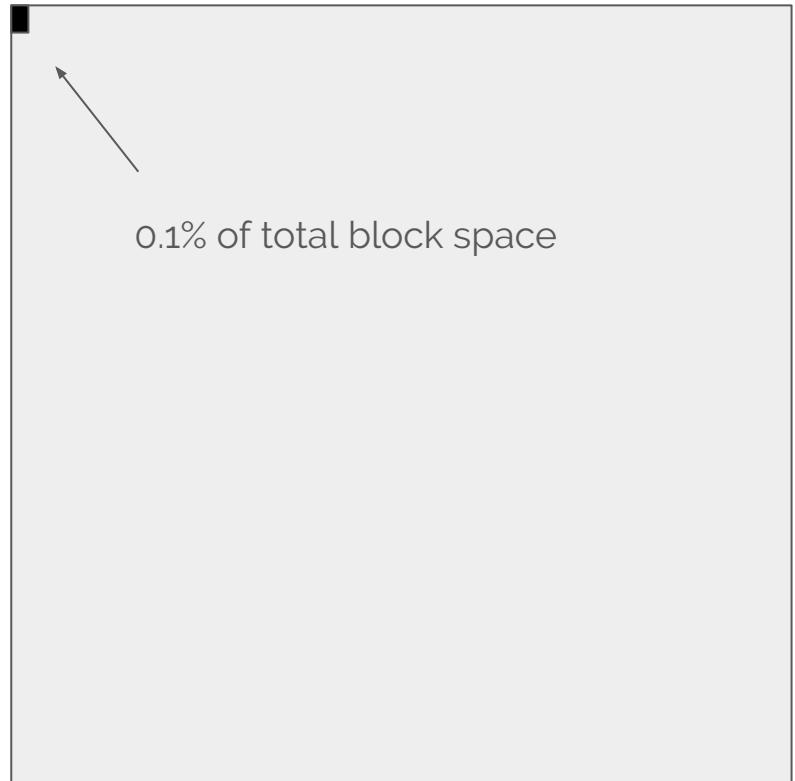
# OpenTimestamps goal

- ≈ 144 tx/day for global timestamping
- For maximum precision
- Less cost, 1/10 than now
- 0.1% of block



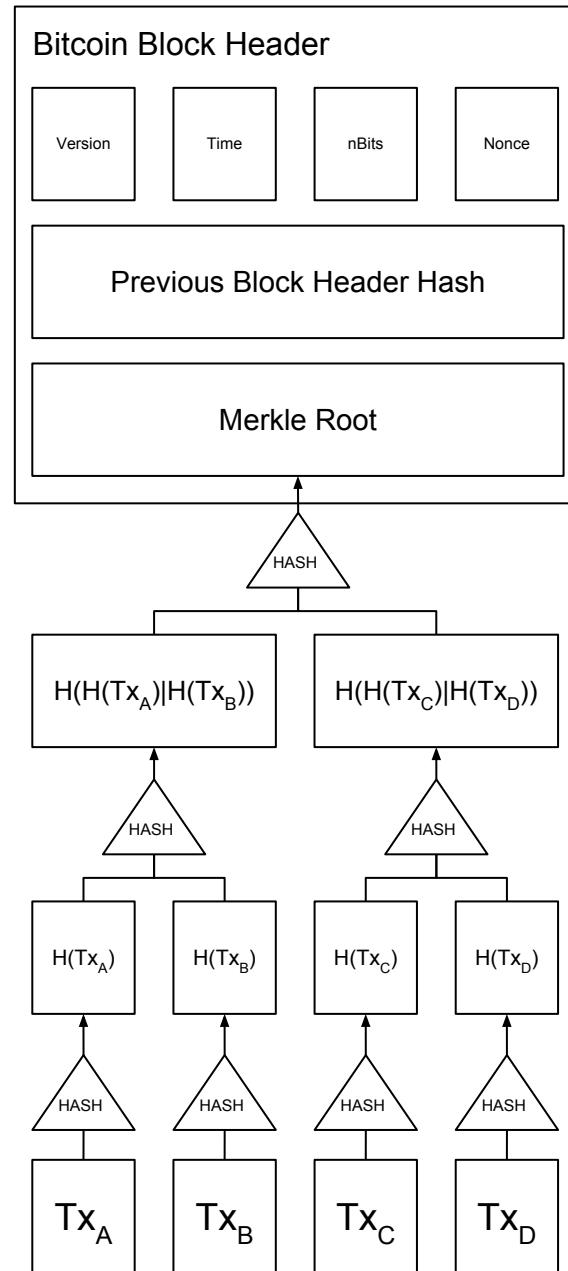
# OpenTimestamps goal

- ≈ 144 tx/day for global timestamping
- For maximum precision
- Less cost, 1/10 than now
- 0.1% of block
- 0% ? -> Sign to Contract R&D

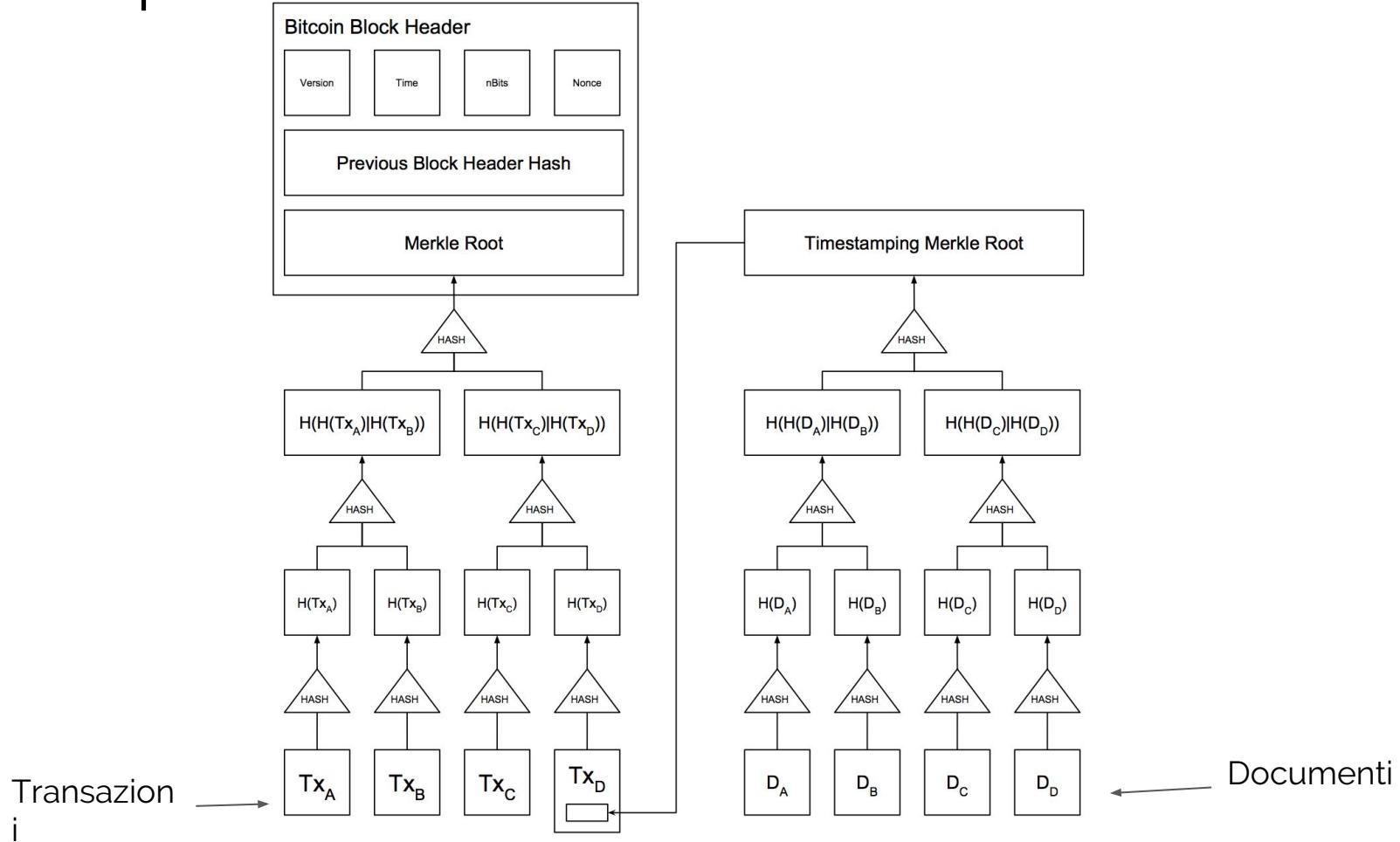


0.1% of total block space

# Aggregating Timestamps



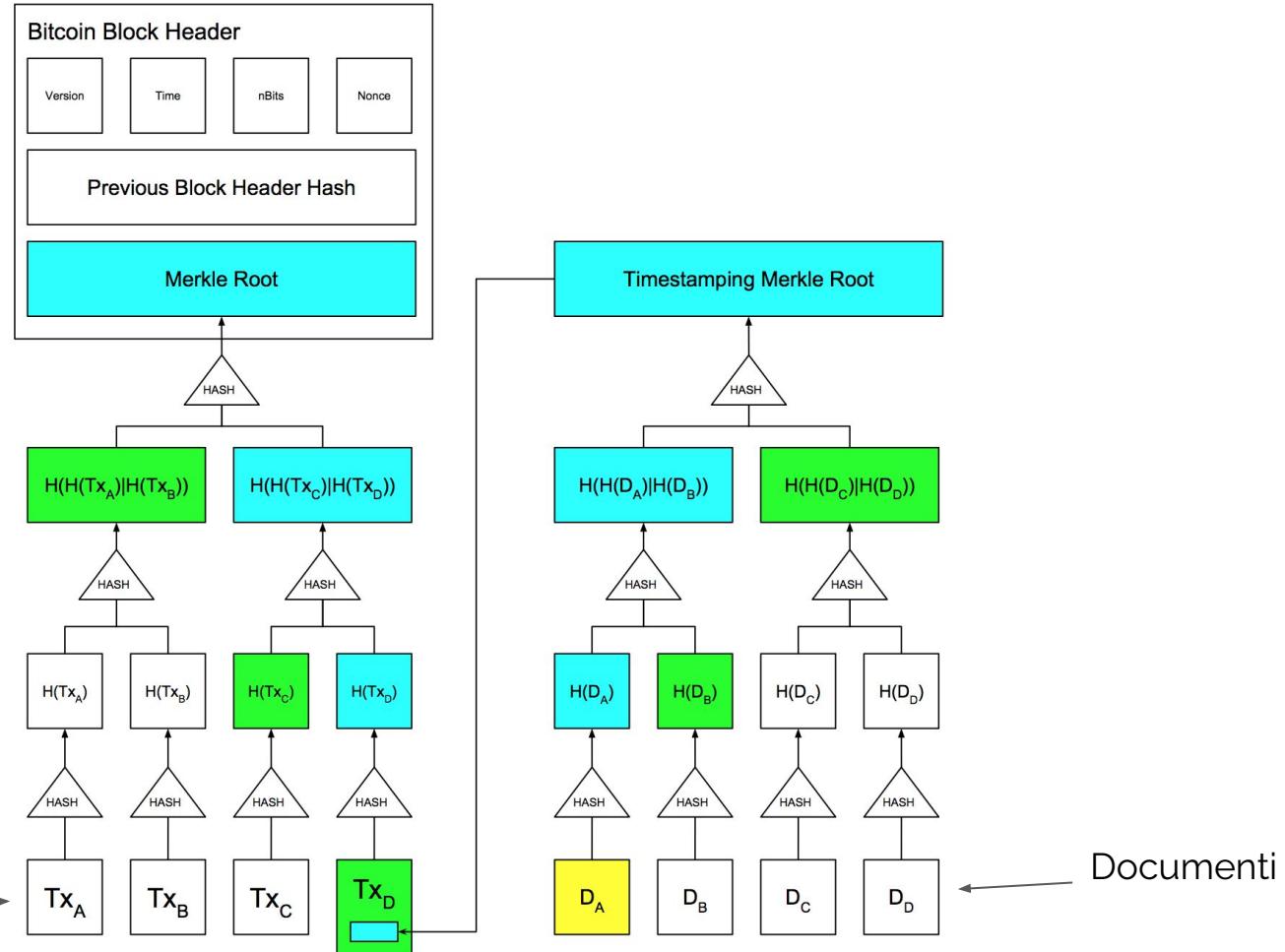
# Aggregating Timestamps



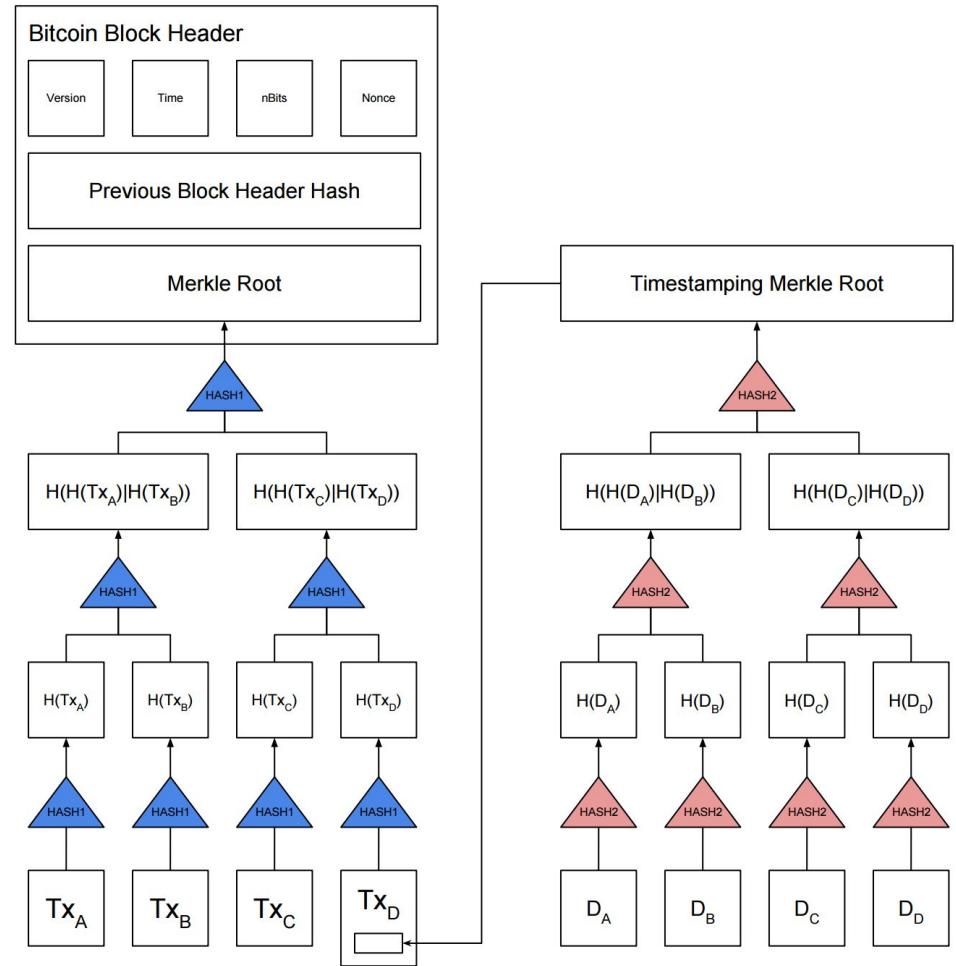
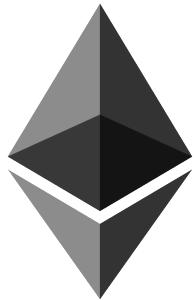
# Aggregating Timestamps

✓ scalability &  
independence

Transazion  
i



# OpenTimestamps is flexible



# Scenari di utilizzo

- **Scenario regolatorio**

Creazione di prove di integrità dei dati e timestamping compatibili con le richieste regolatorie (es. Dodd-Frank), i dati sono integri secondo le direttive?

- **Autenticità dei documenti**

Il documento in mio possesso è l'originale oppure è stato manomesso?

- **Sicurezza chiavi private**

Un timestamp sicuro consente di distinguere i documenti firmati oltre un certo evento (es. furto della chiave, compromissione dei server, ...), i miei documenti sono stati firmati prima che mi venisse rubata la chiave?

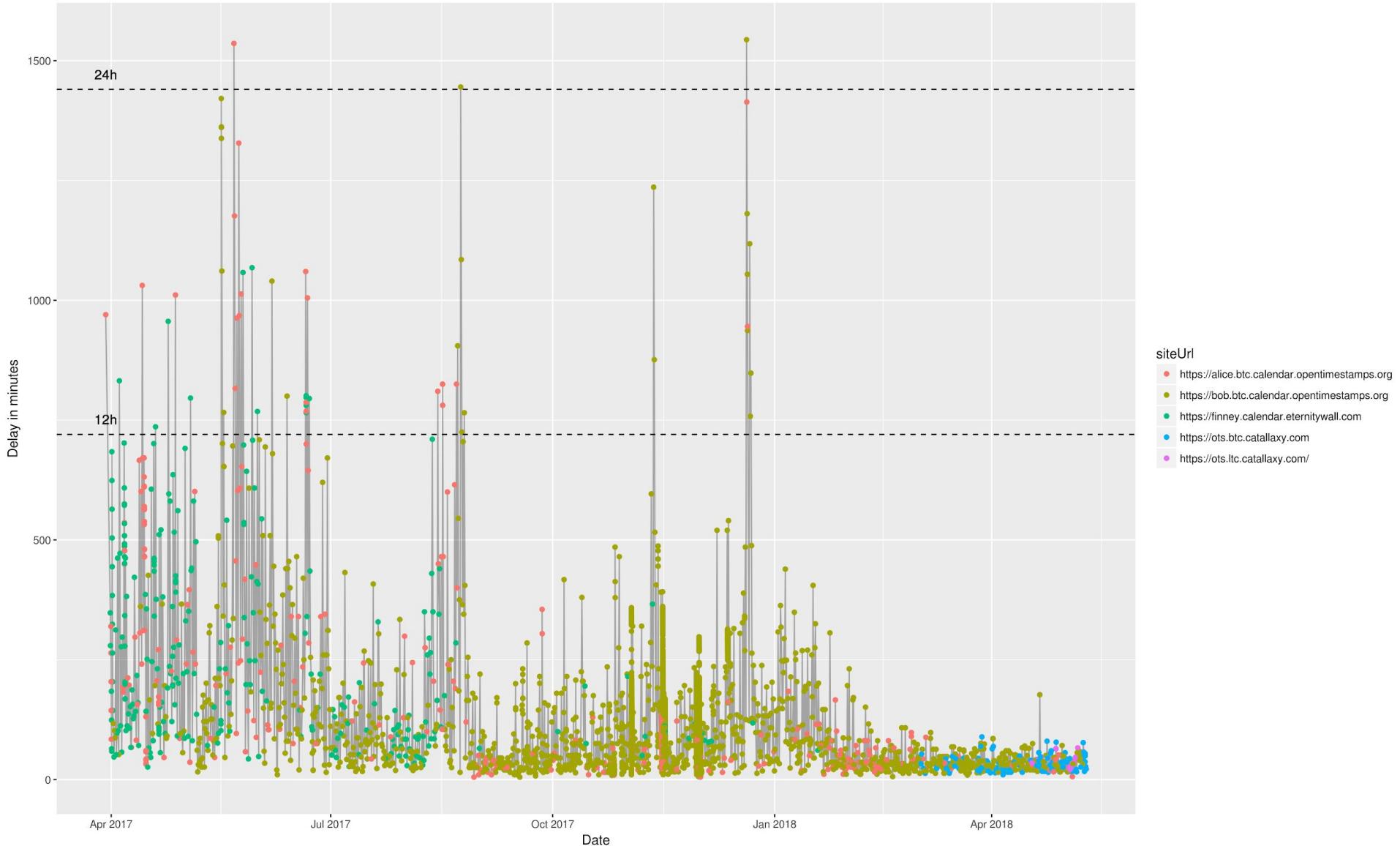
- **Integrità dei record**

I miei dati sono proprio quelli che avevo immesso oppure hanno subito dei cambiamenti e delle manomissioni?



# Performances

Minimum delay in the OTS servers



# Software

Tutto il software di OpenTimestamps è open source e già disponibile su github.

<https://github.com/opentimestamps>

Client e Server sono disponibili per installazioni personali e sono già sviluppate le librerie per:

- Python
- Javascript
- Java
- Rust
- Node-RED

Esistono dei **server pubblici e gratuiti** che consentono di essere già operativi! Da ora!

The screenshot shows a timestamping interface with a dark blue header containing the OpenTimestamps logo and navigation links. Below the header is a timestamp card with the ID "58061bedef2a684c72cdff0774c4a0903d27c077e00513a48838ce7c9c7686f". The card includes a "DOWNLOAD THIS TIMESTAMP" button. A legend at the top right defines icons for Bitcoin Attestation (green), Pending (orange), Unknown Attestation (grey), Comments (purple), and Fork (blue). The main area lists timestamp entries with their hashes, types (append, sha256, fork), and content snippets.

Type	Hash	Content Snippet
append(7a69b9...)	58061bedef2a684c72cdff0774c4a0903d27c077e00513a48838ce7c9c7686f	c961e8c08453c
sha256()	ad418752e5b26f6187a132e31b6e56d3c169751ae3913fe35d7f5f17a70c9a7722987	
Fork		Fork in 2 paths
append(ja7bc9a...)	1 ad418752e5b26f6187a132e31b6e56d3c169751ae3913fe35d7f5f17a70c9a7722987	
sha256()	1 bdfc05aa2a2ea17c02be3c45f51a843de93d9f1a72442a3fa0491fcfa0fa5dad5c575ab1	505c29e1e21e9802e523fb1359778c32993d64fa0d4a949fbed
append(l8a5dad...)	1 bdfc05aa2a2ea17c02be3c45f51a843de93d9f1a72442a3fa0491fcfa0fa5dad5c575ab1	3ef693712ef1b0200d1c9484d2eff0f5240573a23b3e51387ca0235916ef9d2
sha256()	1 3ef693712ef1b0200d1c9484d2eff0f5240573a23b3e51387ca0235916ef9d2	3ef693712ef1b0200d1c9484d2eff0f5240573a23b3e51387ca0235916ef9d2
append(l40b8de...)	1 3ef693712ef1b0200d1c9484d2eff0f5240573a23b3e51387ca0235916ef9d2	3ef693712ef1b0200d1c9484d2eff0f5240573a23b3e51387ca0235916ef9d2
sha256()	1 654a6f5083d6e08734f897ae0cae352d07f12bbf50a740373b305ecea866	5620e62c28b
prepend(l59371d...)	1 593714ca54a6f5083d6e08734f897ae0cae352d07f12bbf50a740373b305ecea866	
append(l0817a...)	1 593714ca54a6f5083d6e08734f897ae0cae352d07f12bbf50a740373b305ecea866	
Pending Attestation		Pending attestation: server <a href="http://alice.btc.calendar.opentimestamps.org">http://alice.btc.calendar.opentimestamps.org</a>
sha256()	1 bb175cc748172f48626c0f8900d1404051892ce7570c7819cc3f5cc912da	
append(l4ed4b...)	1 bb175cc748172f48626c0f8900d1404051892ce7570c7819cc3f5cc912da	Deeb81f6e4db090c8e473f3ee457e637fbfa059d4a86d
sha256()	1 e485d9c45942d52d1f8bec3aae328f...5b5e57b7968950778464e888e93887198760677256	
prepend(l9344c...)	1 d9344c932a12d1f8bec3aae328f...5b5e57b7968950778464e888e93887198760677256	5b5e57b7968950778464e888e93887198760677256
sha256()	1 e1a849ace1f06e8814fe3ff3e625e08944e683f63536d657344666a091c	
append(l0deb...)	1 e1a849ace1f06e8814fe3ff3e625e08944e683f63536d657344666a091c	1.4513e05b79794c...0027a3a4781e747e7f59577b564e4878a
sha256()	1 7b354f045f246d070655999de9d451a2632209d966ac51d761c1b2b504070eef283d59d	
append(l9ee28...)	1 7b354f045f246d070655999de9d451a2632209d966ac51d761c1b2b504070eef283d59d	9ea177126389148d2f63705ac541a24e12104e3638282
sha256()	1 4ba7d5a93c30df2c5b21bab37ed1ac723548983f9d539a9441cac243a2af3e78936370dc	
append(l5983...)	1 4ba7d5a93c30df2c5b21bab37ed1ac723548983f9d539a9441cac243a2af3e78936370dc	a816dc268bf1c07c16e7132488a4d65a3a0cbce089731410
sha256()	1 550939ad487c4993702b2e316ca6f90d6a0ff350e965380d913f64513c35	
prepend(l3f209c7...)	1 3f20c70401083997c02191d213939f7718a5f2e242y86b1f3166871e924045959bad1487c	499a73e8016537054e070e64201068814b16874a
sha256()	1 df7209222c0600a4f013eb3f01653707b54ed5a070ee64a251068814b16874a	
prepend(l3485...)	1 de3485d64b64f4ea8c099997515a3312e43a5cc5ca15b426728ef88de8446e0df720992c060	
sha256()	1 96fd49f3c49b3a5272dc99f4839e828412af2a5a4bd88e1dfa959b04313	

# Agenda

- Chi siamo e cosa facciamo
- Notarizzazione e OpenTimestamps
  - Introduzione a Bitcoin
- Casi d'uso
- Demo



# Un caso reale - Intesa San Paolo

Dodd-Frank, normativa americana e europea, richiede l'archiviazione dei dati relativi a transazioni finanziarie su dispositivi che soddisfano le proprietà:

- WORM Write Once Read Many
- Anti tamper



Gli approcci dei servizi di notarizzazione tradizionali si basano sulla fiducia di una terza parte, autorità di certificazione e firme digitali, e richiedono processi operativi complessi che implicano rischi e costi elevati.

Da questo **scenario regolatorio** è partito un progetto con Deloitte e Intesa San Paolo incentrato sul protocollo OpenTimestamps.

<https://ew.link/3qrs>

# Un caso reale - Intesa San Paolo

I dati di trading sono archiviati ad un dato istante e viene generato un codice non-reversibile (hash value) che rappresenta tutti i dati senza però la possibilità di ricostruzione dell'informazione completa.

Dagli hash sono generate delle impronte digitali e immutabili nel tempo registrate su blockchain al fine di:

- impedire la manomissione dei dati,
- attribuire un timestamp sicuro dato dalla blockchain.

I vantaggi di questa soluzione sono:

- indipendenza da qualunque fornitore e capacità di prova senza il coinvolgimento di terze parti,
- maggior sicurezza dei dati salvati,
- abbattimento dei costi per servizi di terze parti.

Svantaggi

- Impianto regolatorio

<https://ew.link/3qrs>

# The Internet Archive

Tutti i file dell'intero Internet Archive (per un totale di circa **750 milioni di elementi**) sono stati certificati in **una sola transazione** a dimostrare l'estrema **scalabilità** della soluzione.



Get timestamps for Internet Archive's collections

Example: NASA Apollo Program

Example: NASA Apollo Program

I file aggiunti all'internet archive vengono timestampati giornalmente ed è possibile reperire le prove tramite la pagina

<https://opentimestamps.org/internet-archive>

<https://ew.link/eyu1>

# Bollettino Argentino

Il Bollettino Ufficiale della Repubblica Argentina utilizza il protocollo OpenTimestamps per garantire l'**integrità** e la **datazione** dei comunicati emessi, dal sito web è possibile scaricare, oltre ai file PDF contenenti il testo del bollettino, i file OTS ovvero le ricevute ottenute con il protocollo Opentimestamps a garanzia della **trasparenza** del processo.

 Boletín Oficial  
de la República Argentina | LISTADO PDF/OTS

Fecha  FILTRAR 1 2 3 4 5 6 7 8 »

26-02-2018

Sección	PDF hash	Certificación	PDF	OTS
1	e87d91aa9df574ae2c696a65ddff34494a1aab50a32a07948b867755dd702257	26-02-2018 06:10:18		
2	4a0b9a31f1041d61f035c9300194ac62597596a5ed8f6938672f89973636e3d0	26-02-2018 07:00:09		
3	2c9955d95d12ba939ce86cf1efc416d239b3ff07185446adda92b99d1a38eea1	26-02-2018 07:00:10		
4	7c3983f83b55b2e1b8673bed04e882f9356065576b5815706495a374d7301723	26-02-2018 06:10:18		

23-02-2018

Sección	PDF hash	Certificación	PDF	OTS
1	dd95bf584feb5a4ee269337de993621966b7e8e5a62440135c0d0cb073ce8e5c	23-02-2018 06:18:28		
2	49431926b8414921bef5851c731bafaafcd158d05cd277b1c92d174bdff3cb300	23-02-2018 07:00:09		
3	6967b0c6e30496e4e81551b5e7708920d625be495bf044cd088866897bea836c	23-02-2018 07:00:10		

Le prove sono liberamente verificabili dal cittadino senza accedere ad altri servizi governativi.

<https://ew.link/7hkd>

# OTSPProofBot

**@otsproofbot** è un bot twitter che consente di salvare e timestampare ogni singolo tweet.

## OtsProofBot

[Follow @otsproofbot](#) 2,719 followers

Make Twitter immutable again!

At Mon Feb 26 14:37:31 +0000 2018 user [@tulipan81](#) wrote:

Tomorrow I will speak at "Casi d'uso a confronto: blockchain pubblica o privata?" about @eternitywall! Please @otsproofbot save this tweet

[Watch on Twitter](#)

Original JSON:

```
{"id": "968132927891623937", "user": "tulipan81", "text": "Tomorrow I will speak at \"Casi d'uso a confronto: blockchain pubblica o privata?\" about @eternitywall! Please @otsproofbot save this tweet", "timestamp": "Mon Feb 26 14:37:31 +0000 2018"}
```

SHA256:

```
c68e4b37b4a53b750881a8cf9f6367d9ebd27b64552ed6877b3bf0ddcd22cb52
```

**CHECK OTS PROOF**

Statistics: 1 tweets pending, 4367 confirmed; 52371 total views.

Based on [OpenTimestamps](#) protocol.



Tomorrow I will speak at "Casi d'uso a confronto: blockchain pubblica o privata?" about [@eternitywall!](#) Please [@otsproofbot](#) save this tweet

[Traduci dalla lingua originale: inglese](#)

15:37 - 26 feb 2018



Aggiungi altro Tweet



OtsProofBot @otsproofbot · 45 s

In risposta a [@tulipan81](#)

The message 'Tomorrow I will speak at "Casi...' was saved using OpenTimestamps services [otsproofbot.com:1880/otsproofbot?id...](#)

[Traduci dalla lingua originale: inglese](#)



Basta citarlo in un tweet per attivarlo, il bot autonomamente:

- salva il testo del tweet,
- crea una prova e
- risponde al tweet con un link alla prova generata,

<https://ew.link/y2ud>



Eternity Wall - <https://eternitywall.com>

# Agenda

- Chi siamo e cosa facciamo
- Notarizzazione e OpenTimestamps
  - Introduzione a Bitcoin
- Casi d'uso
- Demo





# Javascript lib stamp demo



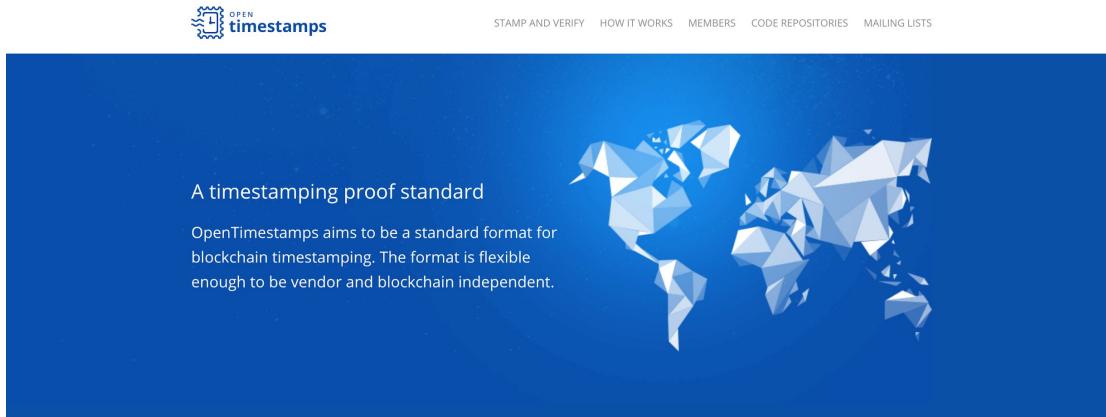
Attribution 3.0 Unported (CC BY 3.0)

```
$ npm install -g javascript-opentimestamps  
  
$ ots-cli.js stamp Presentazione-Blockchain-Devs-Milano.pdf  
  
The timestamp proof Presentazione-Blockchain-Devs-Milano.pdf.ots' has been  
created!  
  
$ ots-cli.js info Presentazione-Blockchain-Devs-Milano.pdf.ots  
  
...  
  
$ ots-cli.js upgrade Presentazione-Blockchain-Devs-Milano.pdf.ots  
  
$ ots-cli.js verify Presentazione-Blockchain-Devs-Milano.pdf.ots
```



Eternity Wall - <https://eternitywall.com> | OpenTimestamps - <https://opentimestamps.org> | Riccardo Casatta - @RCasatta

# Verifica online



#### STAMP & VERIFY

Use the in-browser stamper and verifier



#### HOW IT WORKS

Details on OpenTimestamps



#### MEMBERS

Companies using OpenTimestamps



#### CODE REPOSITORIES

OpenTimestamps repositories



#### MAILING LISTS

OpenTimestamps announcements



#### INTERNET ARCHIVE

OpenTimestamps proof for the Internet Archive

#### STAMP & VERIFY



Drop here a file to **stamp**  
OR  
an **.ots** proof file to **verify**



The hash is calculated on your browser preserving your privacy. [More...](#)  
Timestamping proof download will start automatically after uploading document.



Eternity Wall - <https://eternitywall.com>



# Agenda

- Chi siamo e cosa facciamo
- Notarizzazione e OpenTimestamps
  - Introduzione a Bitcoin
- Casi d'uso
- Demo



# API autenticate

In occasione di questo meetup forniamo una chiave per l'accesso gratuito alle API autenticate, **valido per un mese**.

Dettagli: <https://ew.link/zt3o>

Your public key is 1QKW5ANYnhdomA9Rz7QGmZxFcFdSsXMWMx

Your private key is

L3EZMZyzrbGjW9x5FWwBkJmerZCULyCHG8qmJCyNnxJc2zXSwGez

Esempio di chiamata:

```
$ npm install -g javascript-opentimestamps
$ echo "auth.calendar.eternitywall.com =
L3EZMZyzrbGjW9x5FWwBkJmerZCULyCHG8qmJCyNnxJc2zXSwGez">key.wif
$ ots-cli.js stamp -k key.wif Presentazione-Blockchain-Devs-Milano.ots
```





# Grazie

Riccardo Casatta & Valerio Vaccaro

[riccardo@eternitywall.com](mailto:riccardo@eternitywall.com) | [valerio@eternitywall.com](mailto:valerio@eternitywall.com)

- Presentazione: <https://ew.link/kj54>
- Marcatura temporale: <https://ew.link/rt32>