



Eternity Wall

Valerio Vaccaro

8° Pavia Blockchain Group Meetup

9 Luglio 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

The screenshot shows a timeline of messages on the Eternity Wall platform. At the top, a message from Giacomo Zucco dated 14 gennaio 2016 18:59 says: "A lot of anon love messages, here's the FIRST signed one! LOVE YOU MIR!". Below it, a message from HostFat dated 13 gennaio 2016 2.02 says: "Look at my tentacles!". A central message from Eternity Wall dated 12 gennaio 2016 14:28 says: "Signed messages are now public!". Other messages visible include ones from Brooke (@bitcoinnmom) and Riccardo Casatta (@RCasatta).

The screenshot shows the Eternity Wall mobile application. The main screen displays a timeline of messages. At the top, a message from Brooke (@bitcoinnmom) dated 10 lug 2014 says: "Awww, my husband sent me a love note through the blockchain. For posterity. blockchain.info/address/16wMx1...". Below it, a message from Riccardo Casatta (@RCasatta) dated 11 lug 2014 says: "@bitcoinnmom really nice :) but that annotation is saved on blockchain.info site, not in the blockchain". Another message from Brooke (@bitcoinnmom) dated 11 lug 2014 says: "@RCasatta good point :)".



Chi siamo?

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



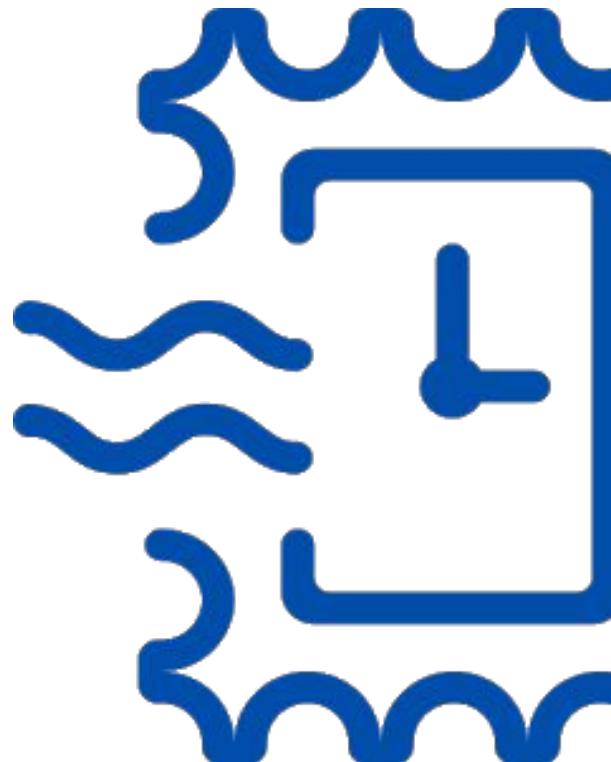
Necessità di attribuire una data certa ad un documento.



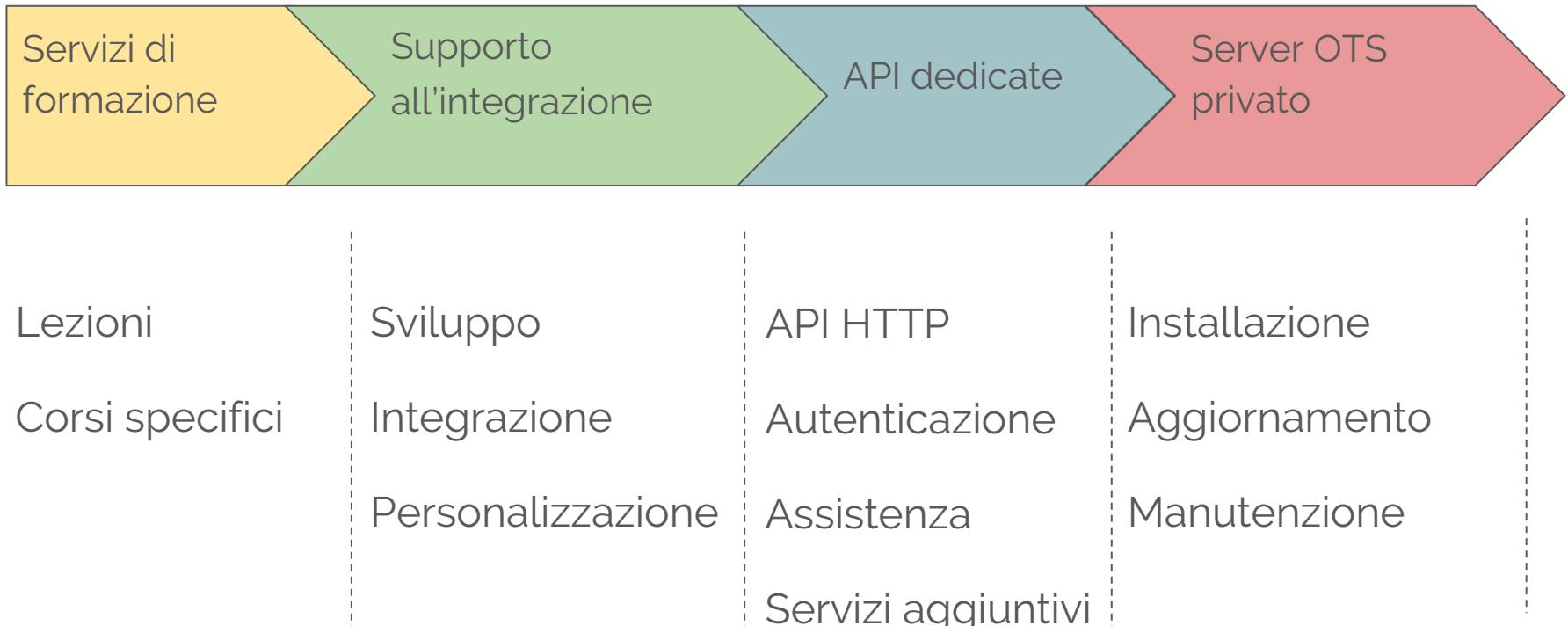
Nascita protocollo **OpenTimestamps**
<https://opentimestamps.org>



Eternity Wall - <https://eternitywall.com> | OpenTimestamps - <https://opentimestamps.org>



Business model



Timestamping o marcatura temporale



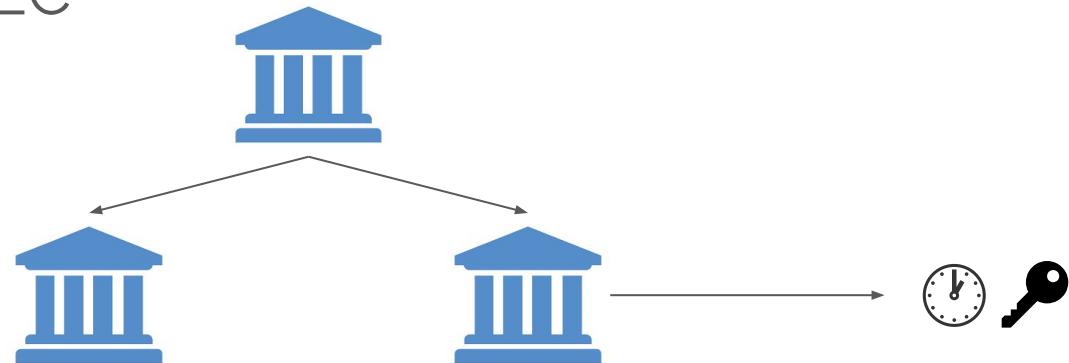
- Il primo e più comune esempio è il **timbro postale**
 - Alice scrive a Bob, la data della comunicazione è apposta da terzi, né Alice né Bob possono contraffarlo facilmente
 - Attenzione: deve essere apposto sul documento e non sulla busta!
- Per importanti documenti deve essere posta da pubblico ufficiale,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

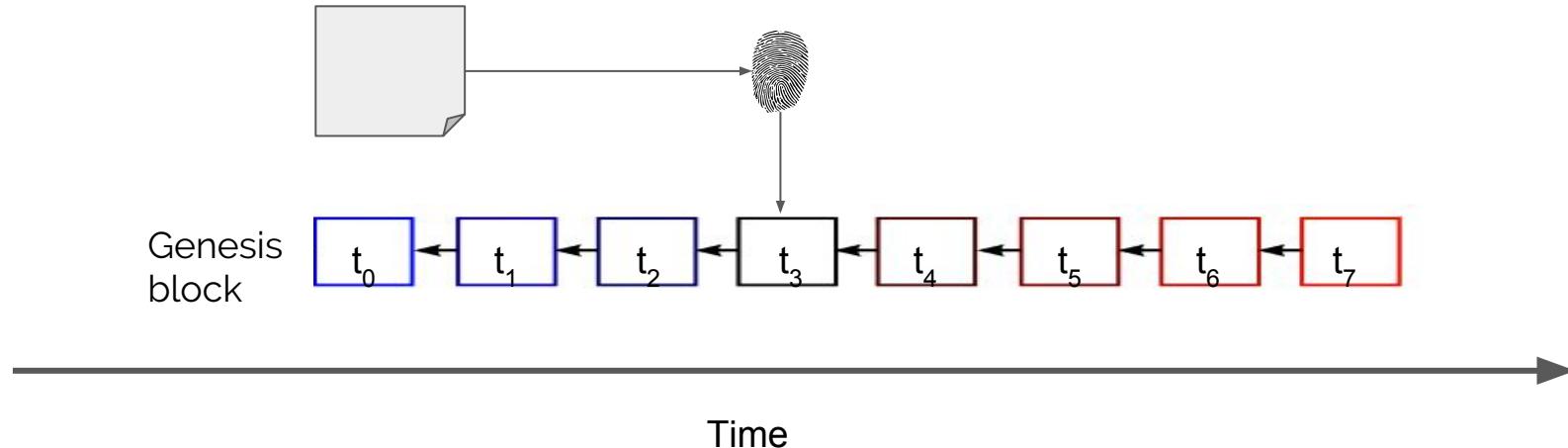
Marcatura temporale certificata

- 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

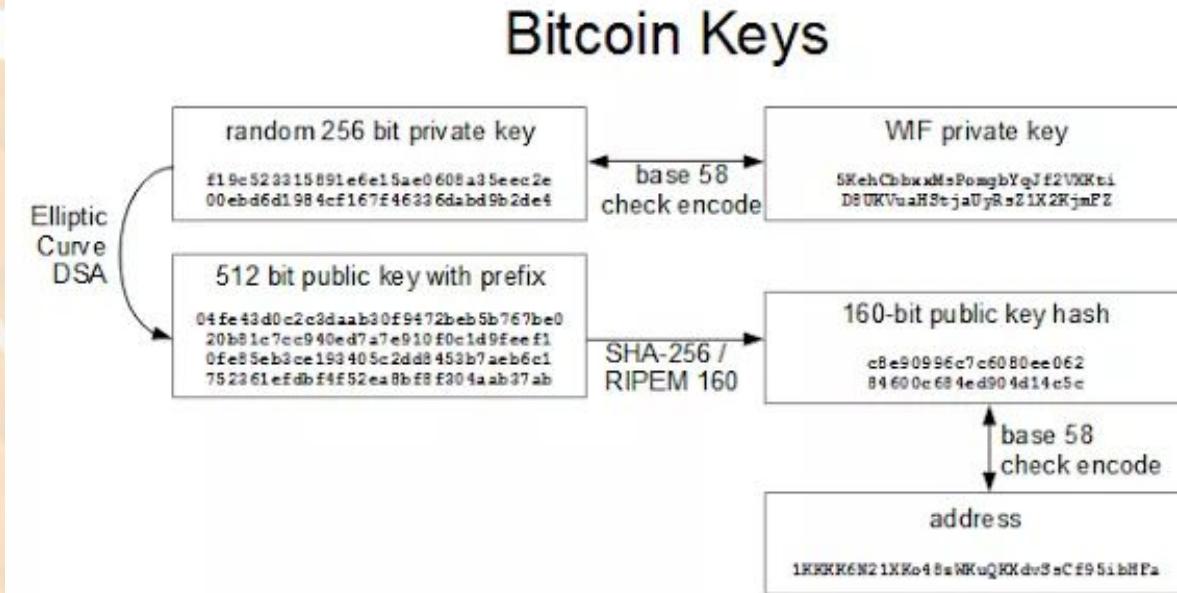
Bitcoin: A Peer-to-Peer Electronic Cash System

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



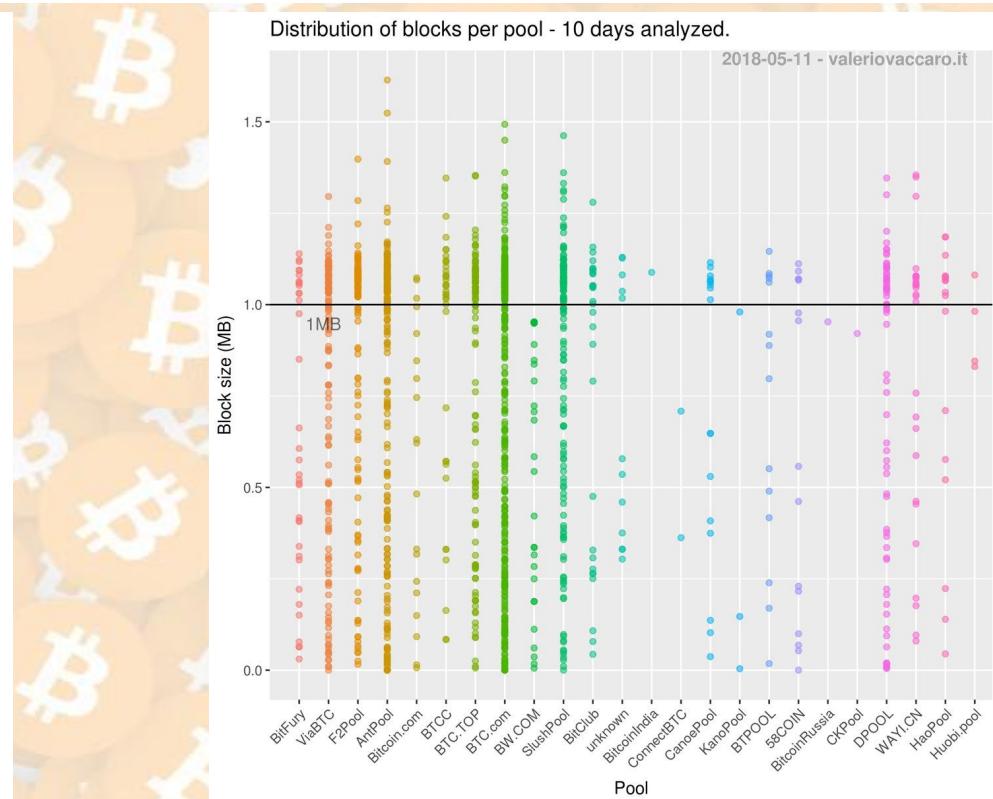
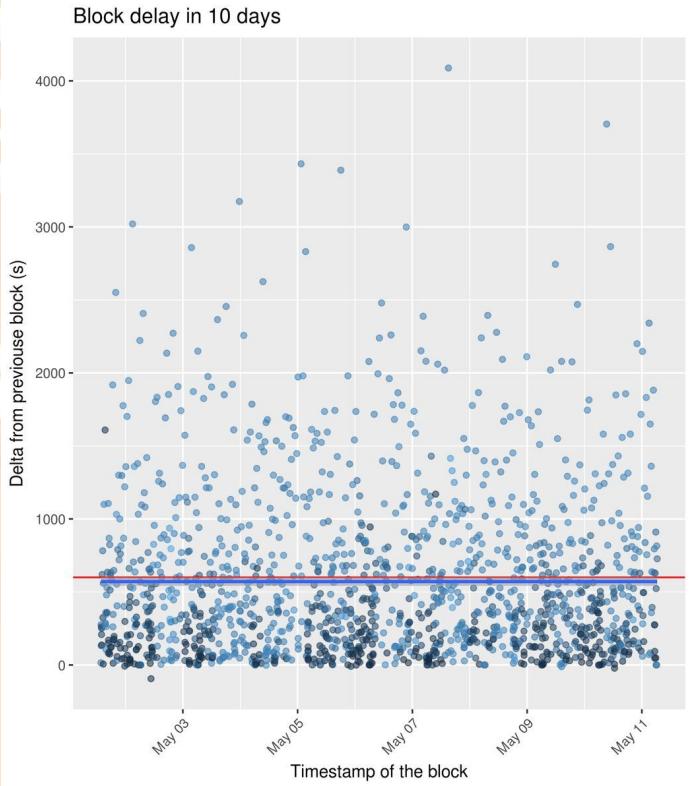
Introduzione a Bitcoin: blocchi e transazioni

version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c817010000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	

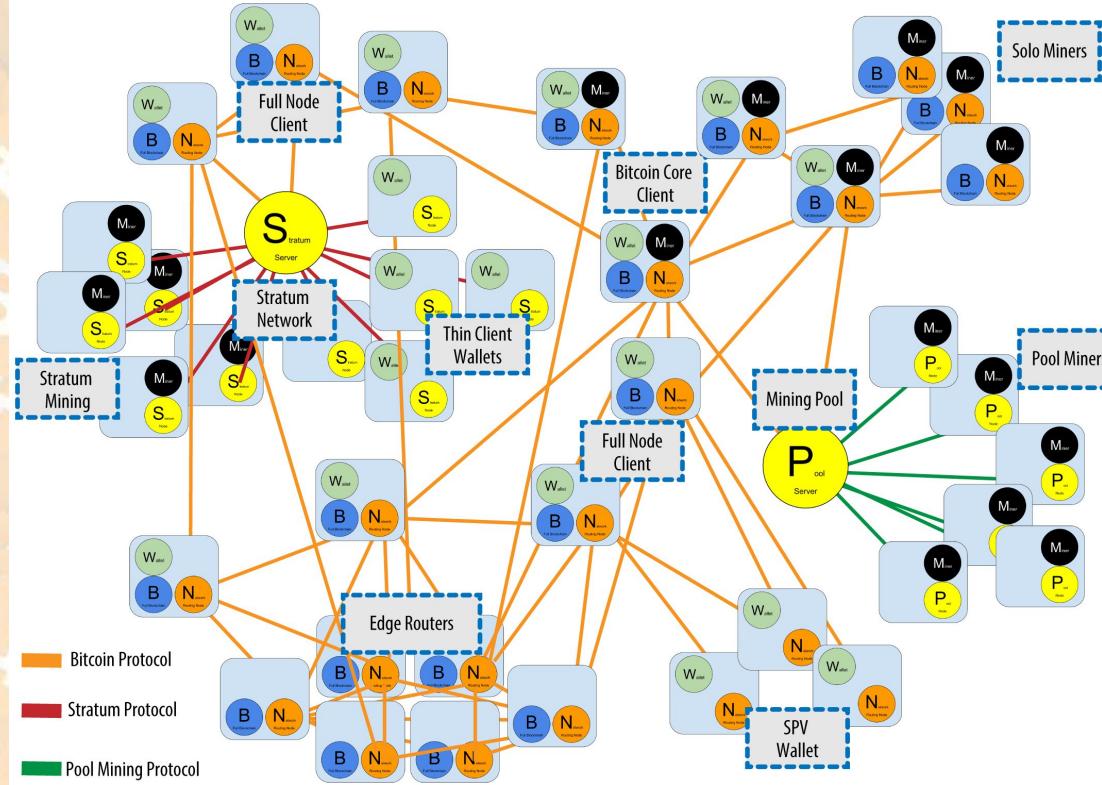
version	01 00 00 00
input count	01
input	previous output hash (reversed) 48 4d 40 d4 5b 9e a0 d6 52 fc a8 25 8a b7 ca a4 25 41 eb 52 97 58 57 f9 6f b5 0c d7 32 c8 b4 81
	previous output index 00 00 00 00
script length	
scriptSig	script containing signature
sequence	ff ff ff ff
output count	01
output	value 62 64 01 00 00 00 00 00
	script length
	scriptPubKey script containing destination address
block lock time	00 00 00 00



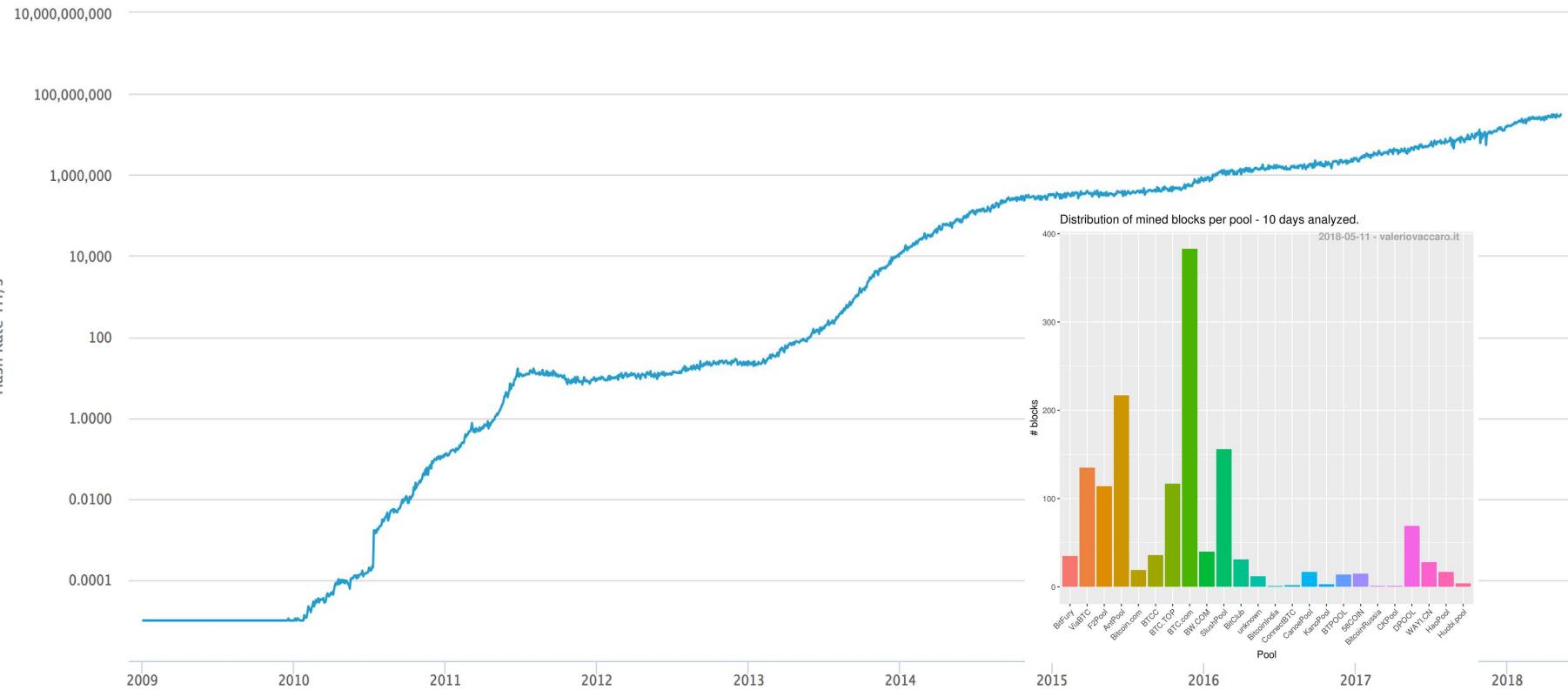
Introduzione a Bitcoin: velocità e spazio



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

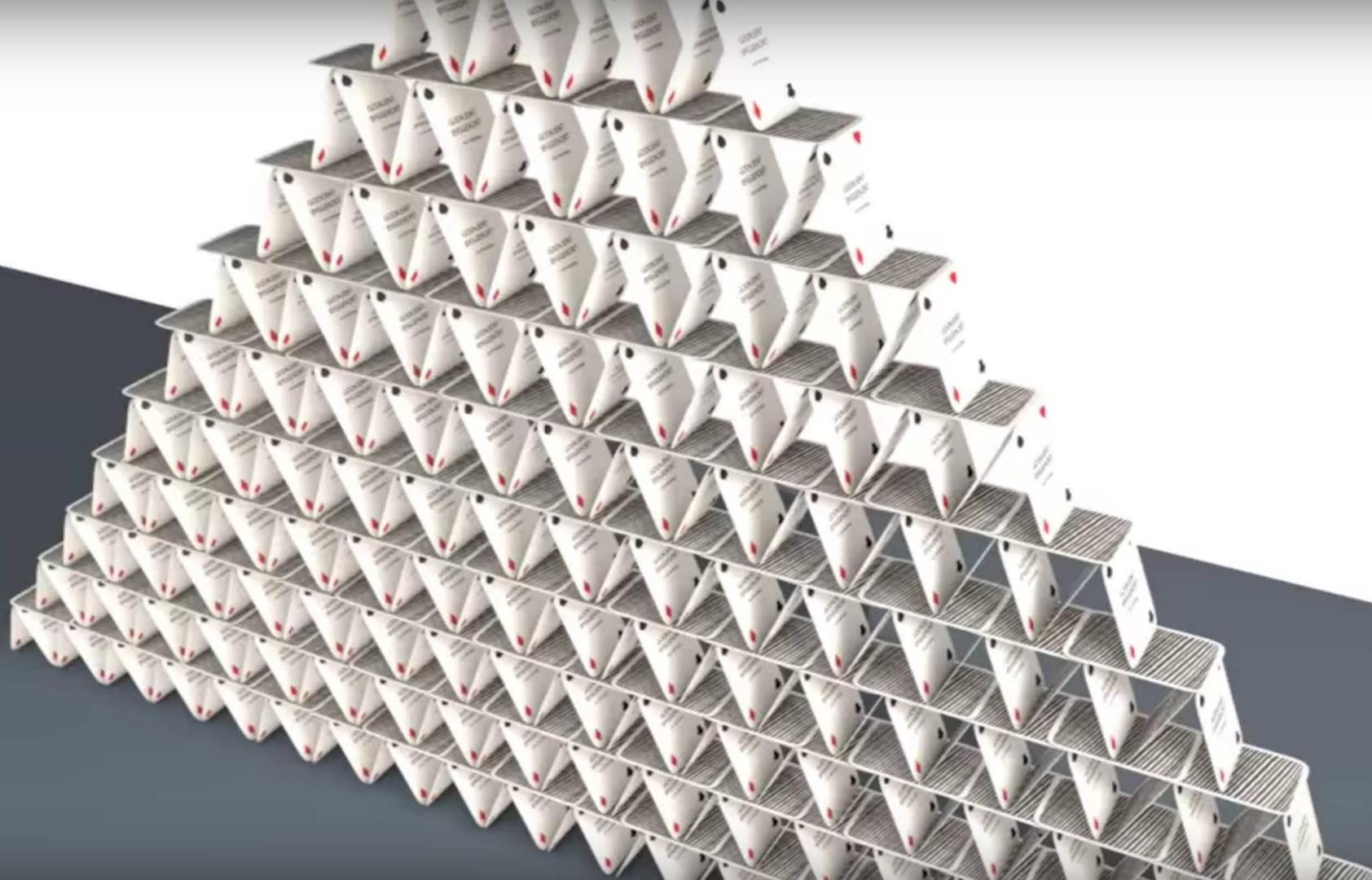
Nel modello basato su terze parti, cosa succede se una chiave viene compromessa?

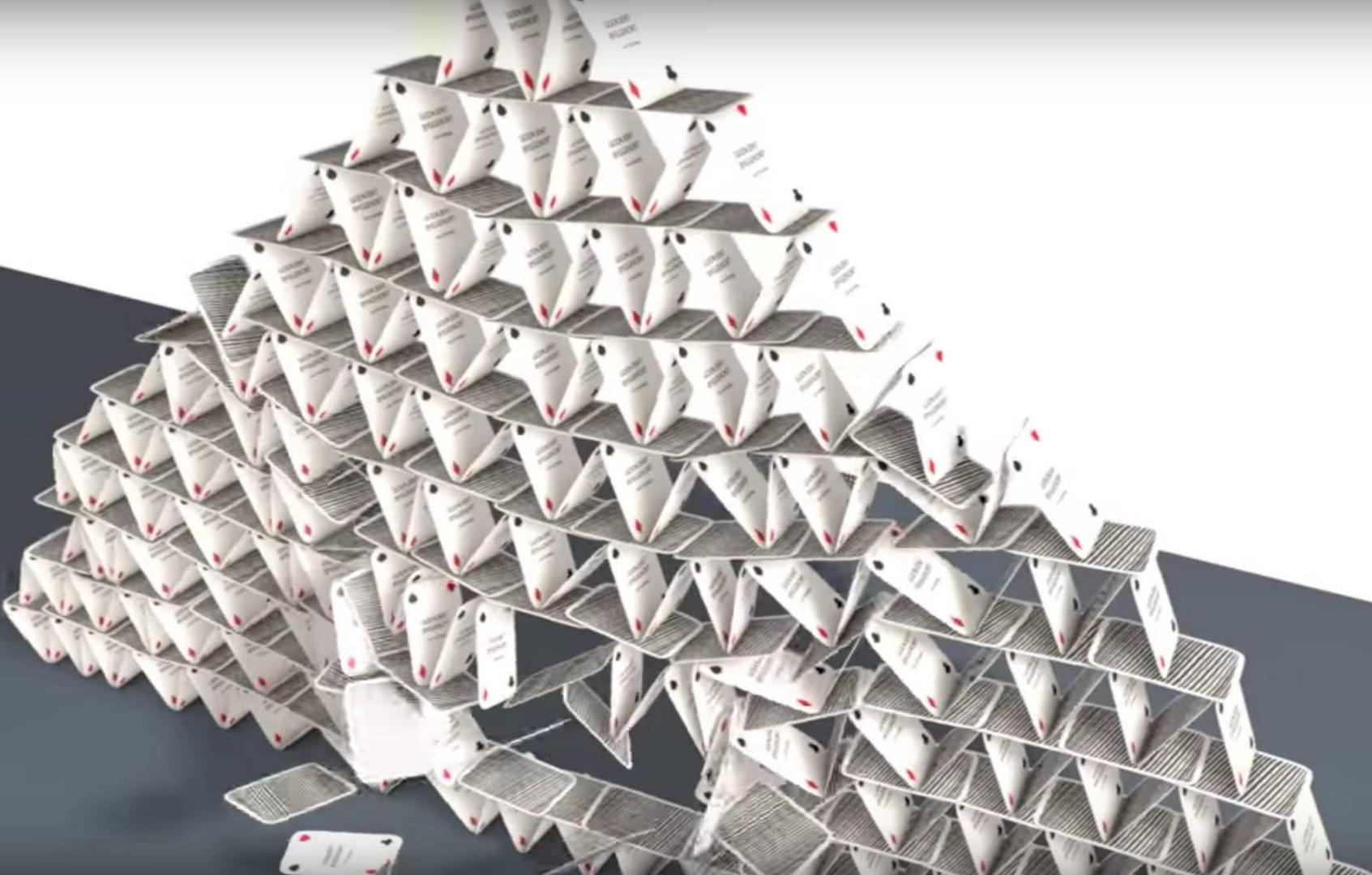
Basta revocare il relativo certificato, da quel momento in poi tutte le marcature temporali sono considerate invalide

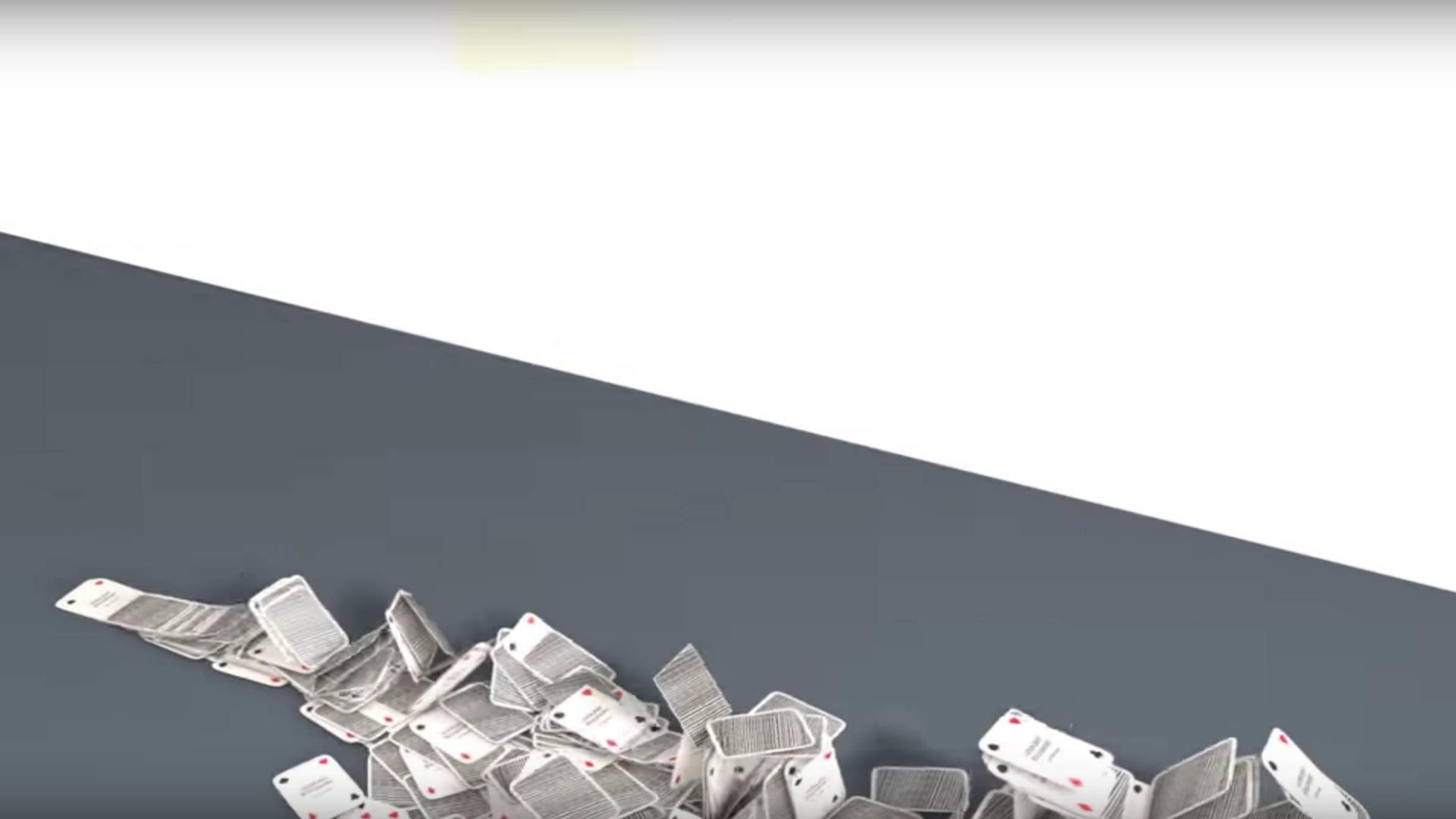
Errato

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

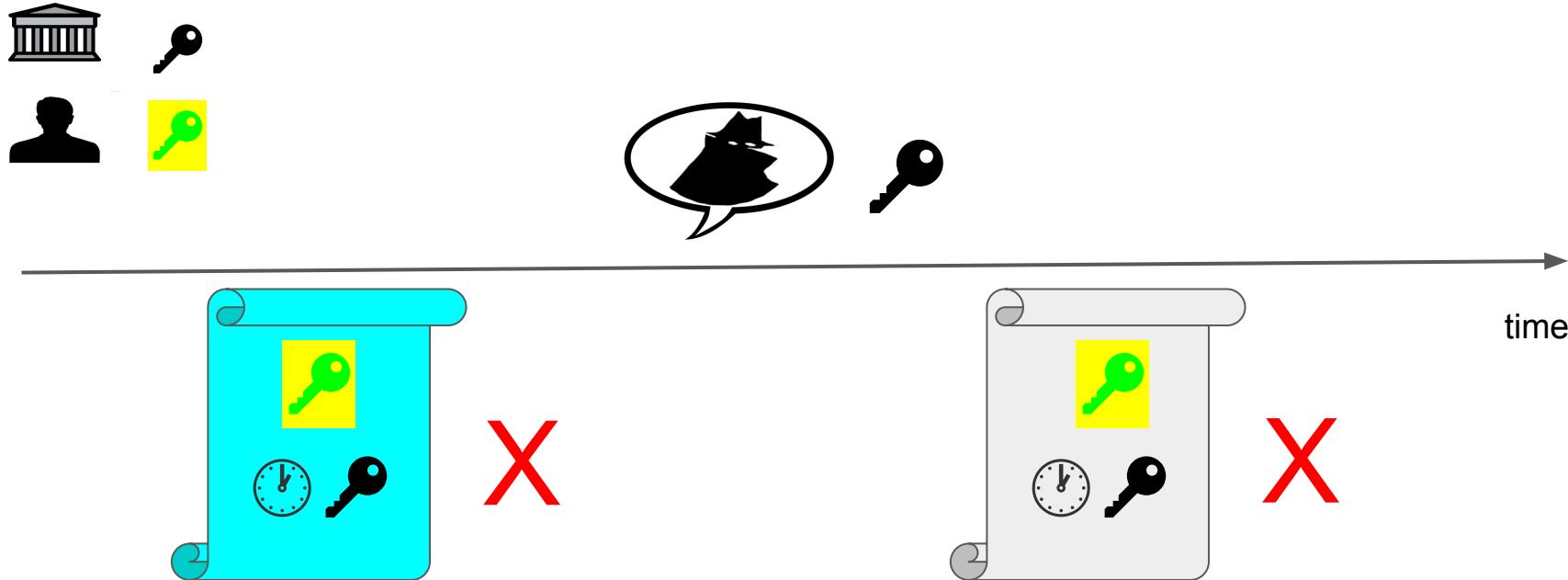




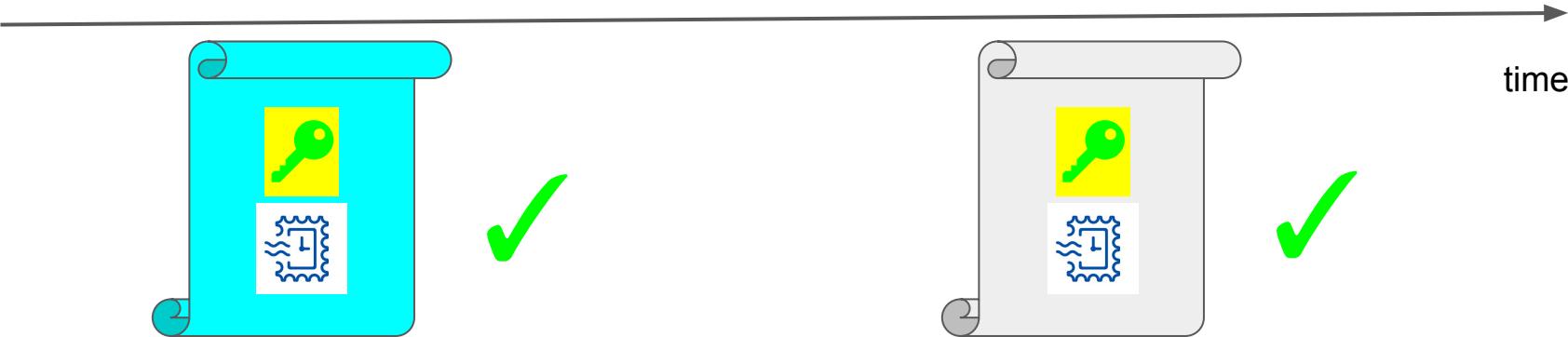




Marcatura temporale basata su firma digitale

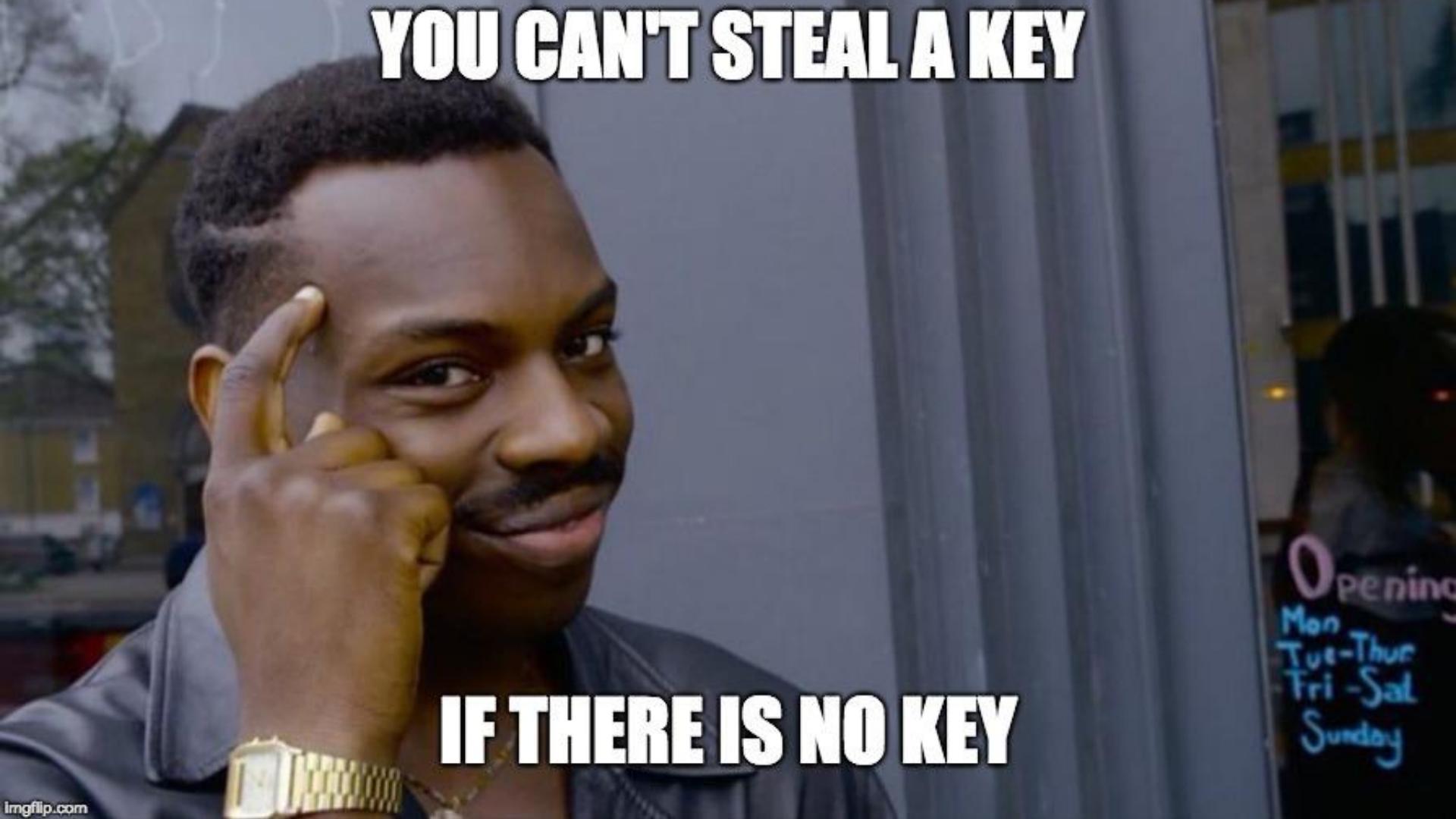


Firma digitale con marcatura temporale trustless

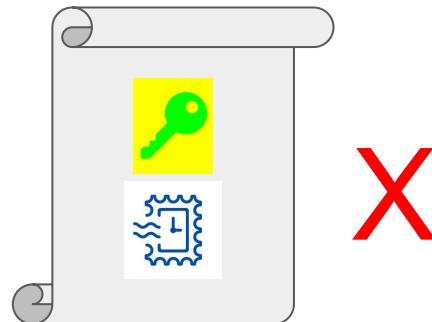
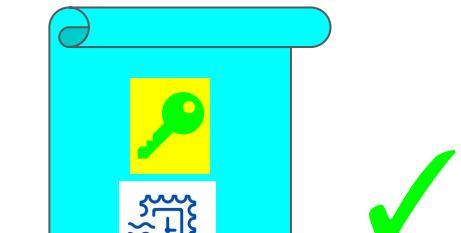
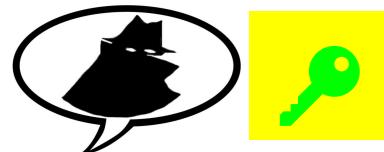


YOU CAN'T STEAL A KEY

IF THERE IS NO KEY



Firma digitale con marcatura temporale trustless



time



Could not back-forge documents

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

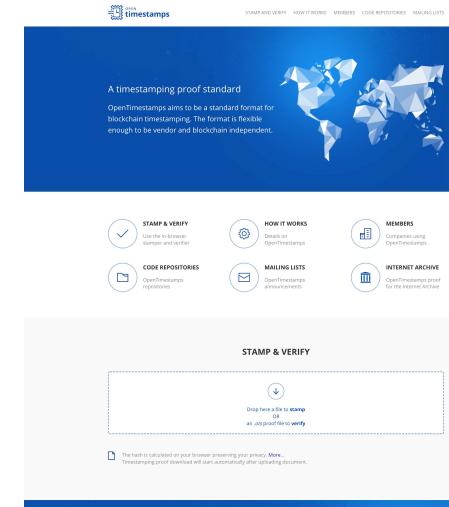
- Timestamping
 - An external viewer **could not** see all the element of the set
 - If someone timestamp two different version of a document, he cannot see it
- Proof of publication
 - An external viewer **could** see all the element of the set
 - Prevent double spend!
 - Bitcoin UTXO (Unspent Transaction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



OpenTimestamps

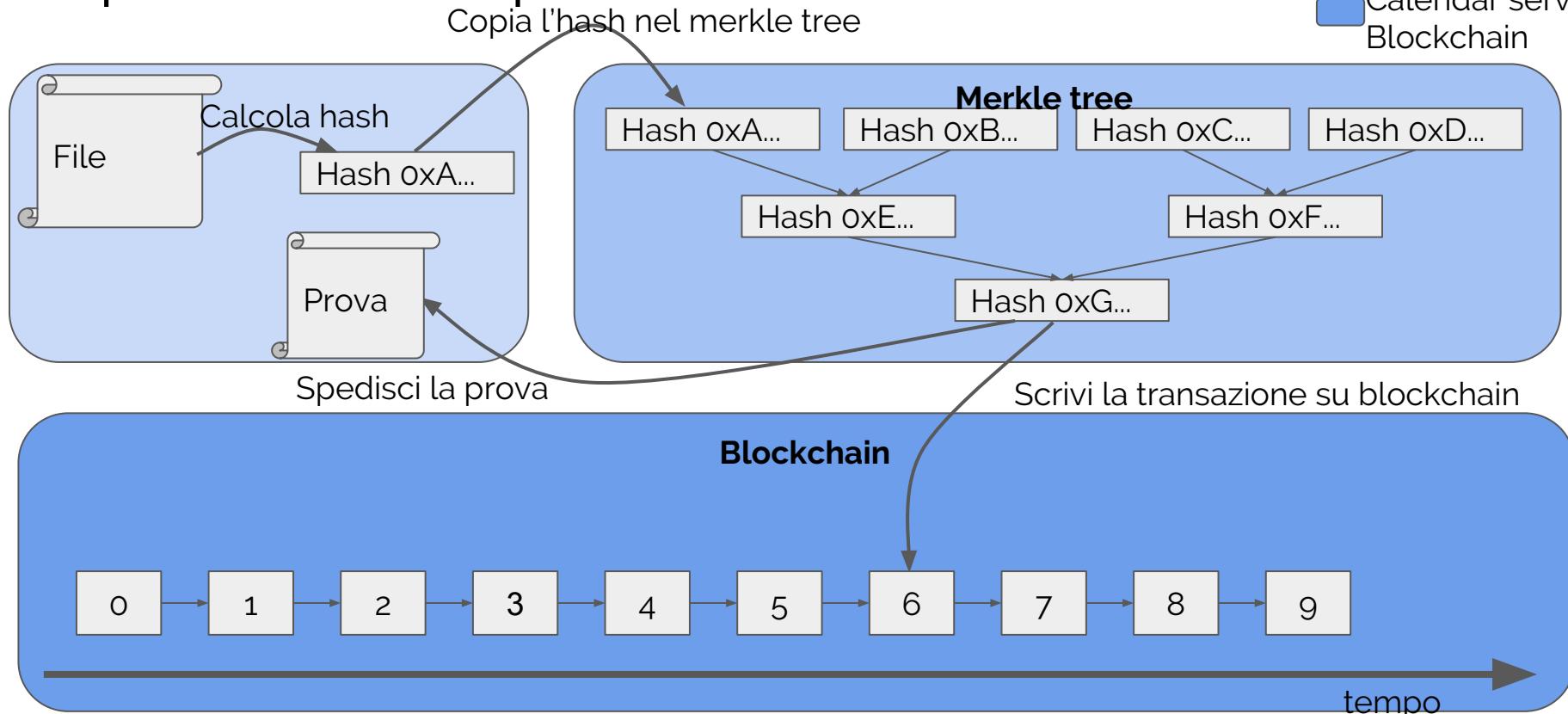
OpenTimestamps è un protocollo standard per la notarizzazione di qualsiasi informazione digitale con le seguenti caratteristiche:

- **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.

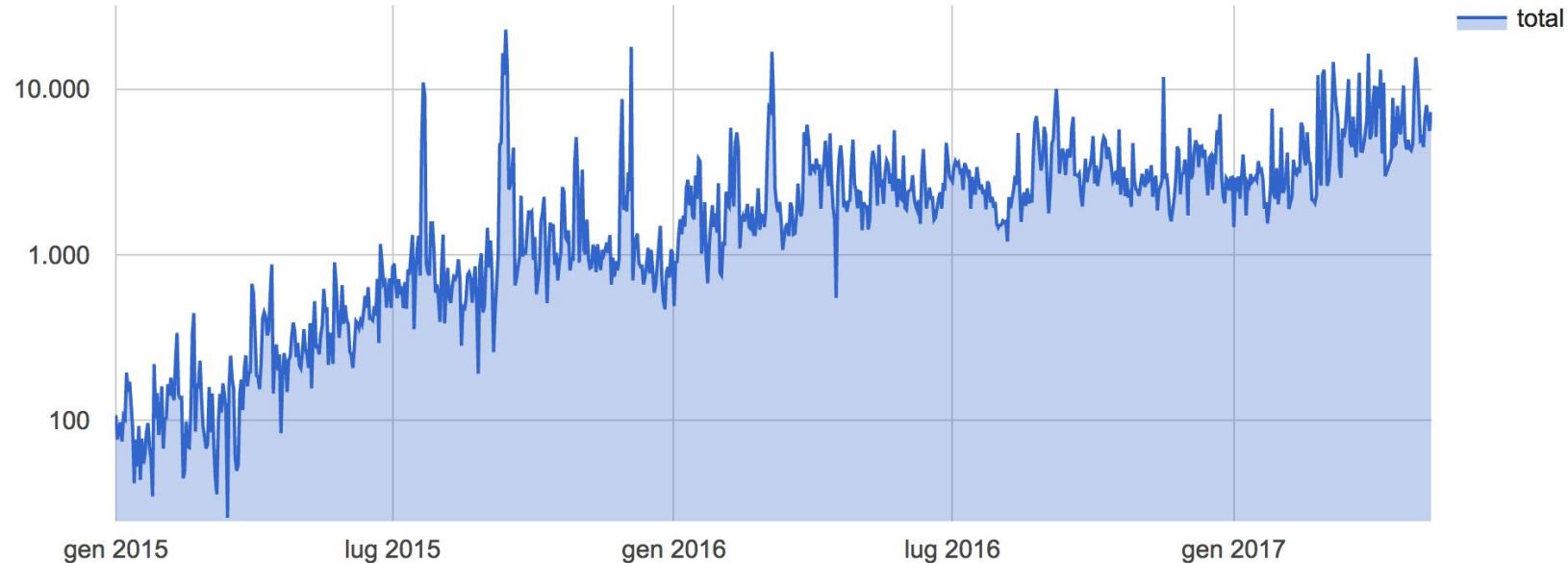


OpenTimestamps

Client
Calendar server
Blockchain

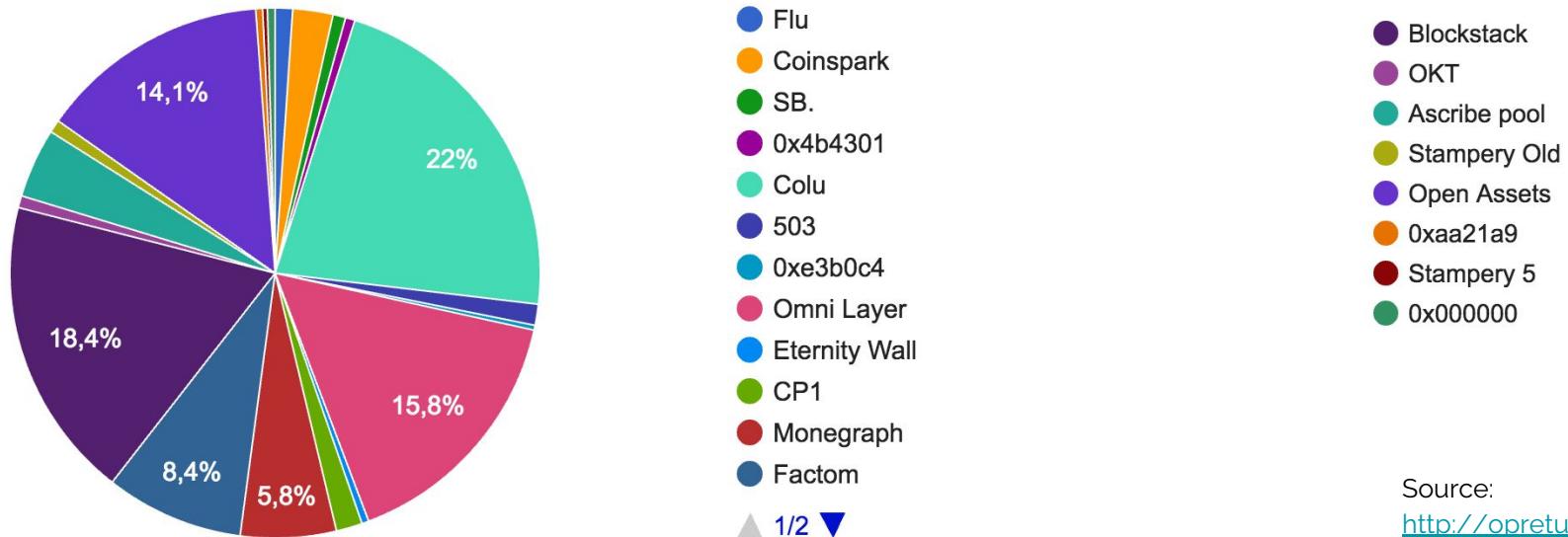


OP_RETURN tx per giorno



~5000
txs/day

Utilizzo di OP_RETURN



Source:
<http://opreturn.org/>

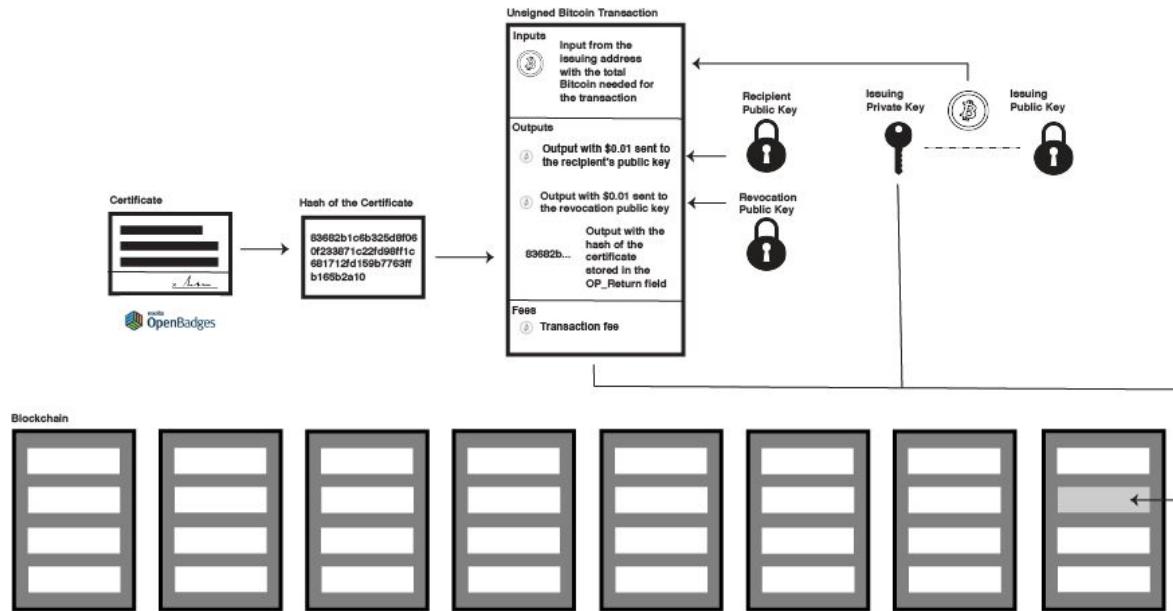
Utilizzo di OP_RETURN

~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

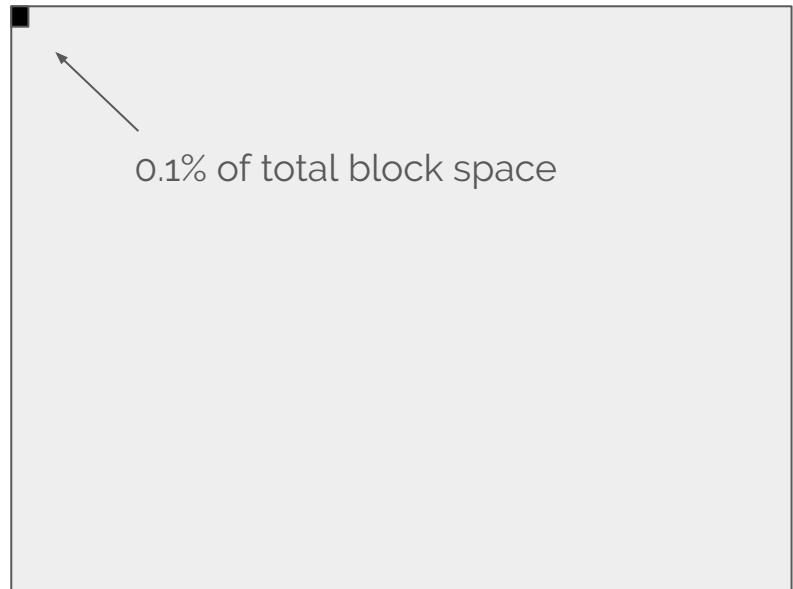
3000 degrees/year * 40 exam/year * 40000 universities ≈ ...

80MB blocks!



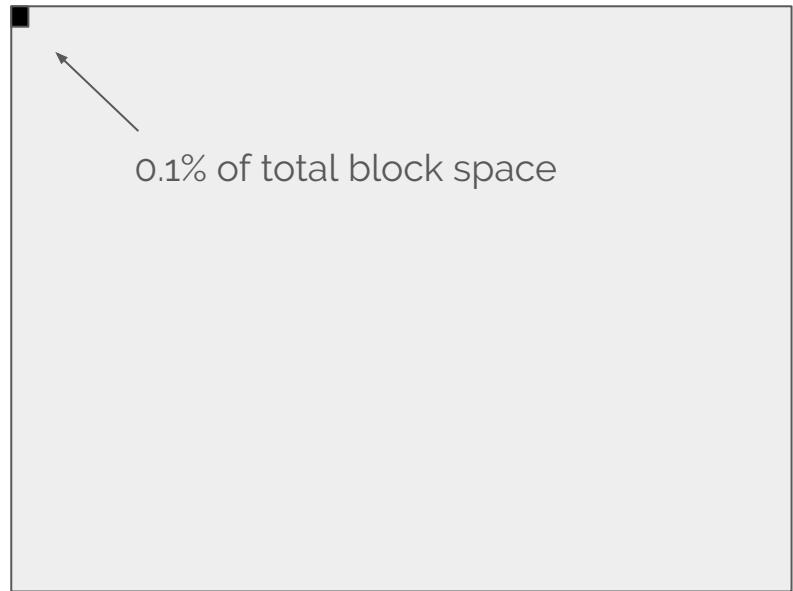
OpenTimestamps goal

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

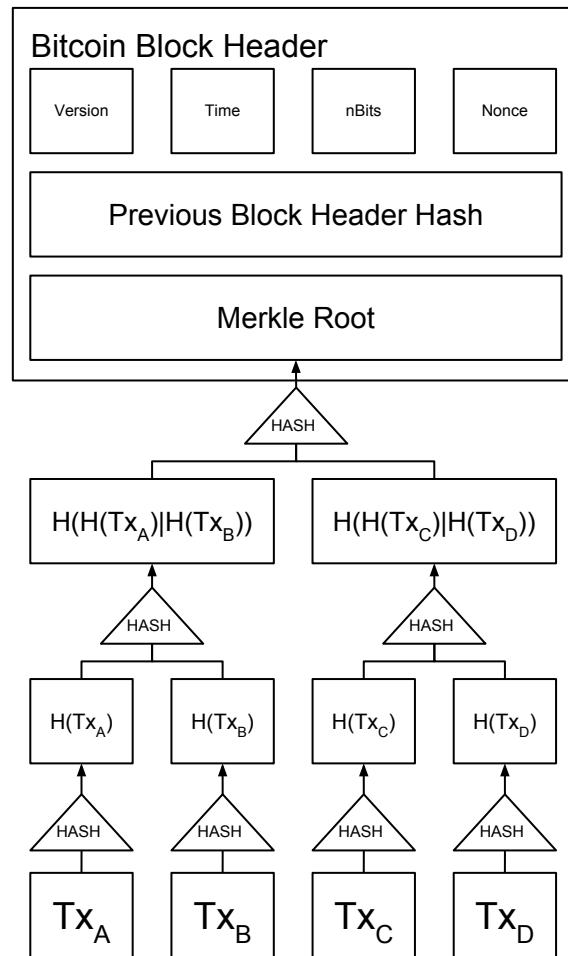


OpenTimestamps goal

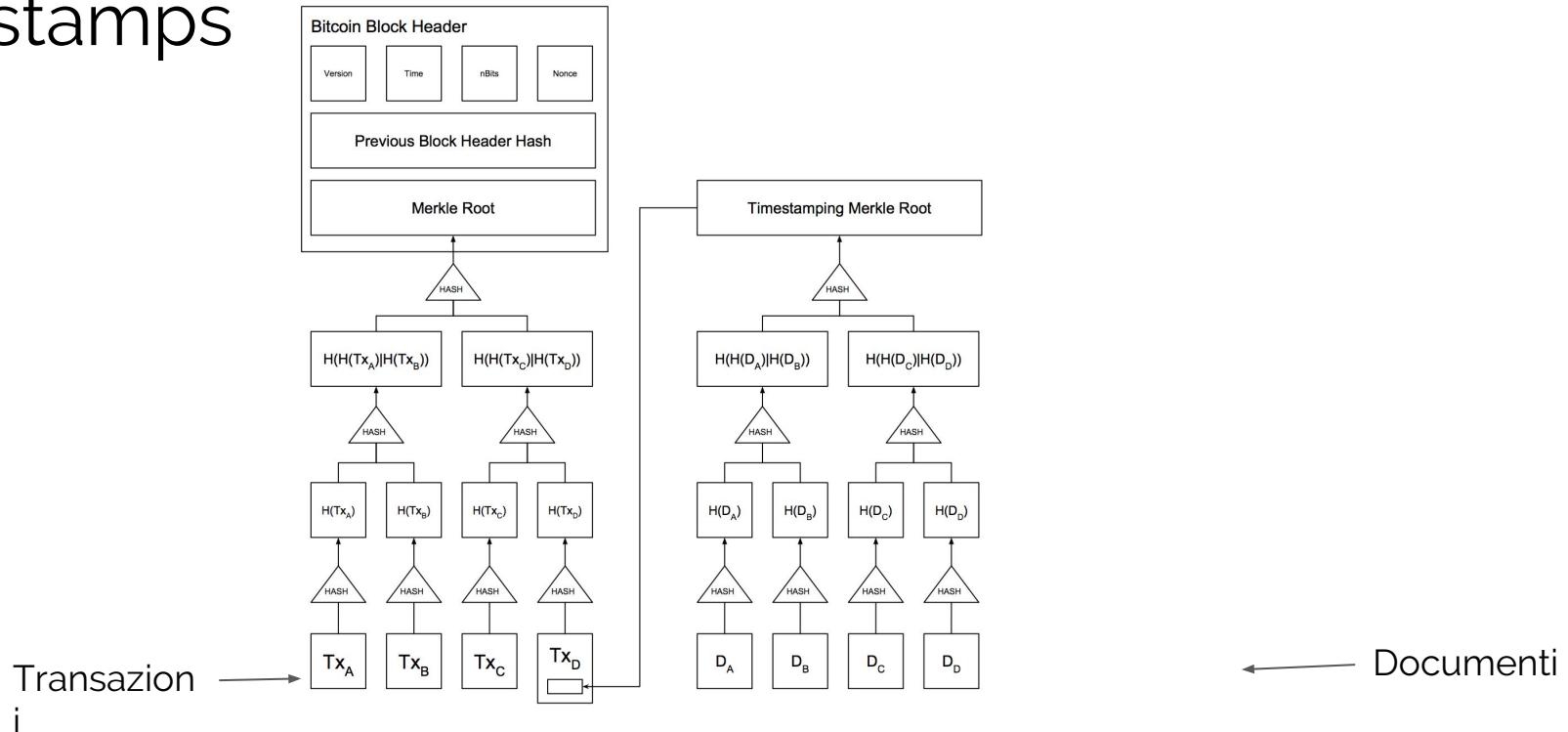
- ≈ 144 tx/day for global timestamping
- For maximum precision
- Less cost, 1/10 than now
- 0.1% of block
- 0% ? -> Sign to Contract R&D



Aggregating Timestamps



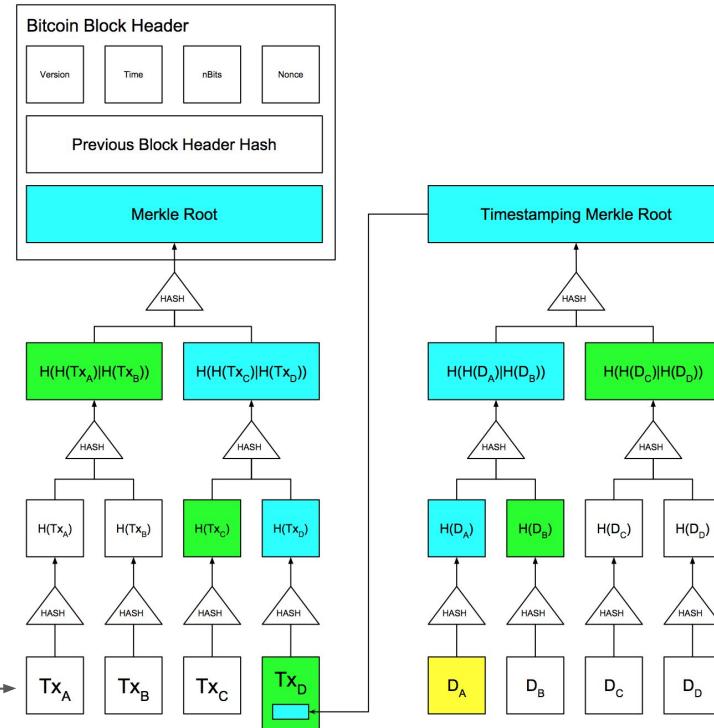
Aggregating Timestamps



Aggregating Timestamps

✓ scalability &
independence

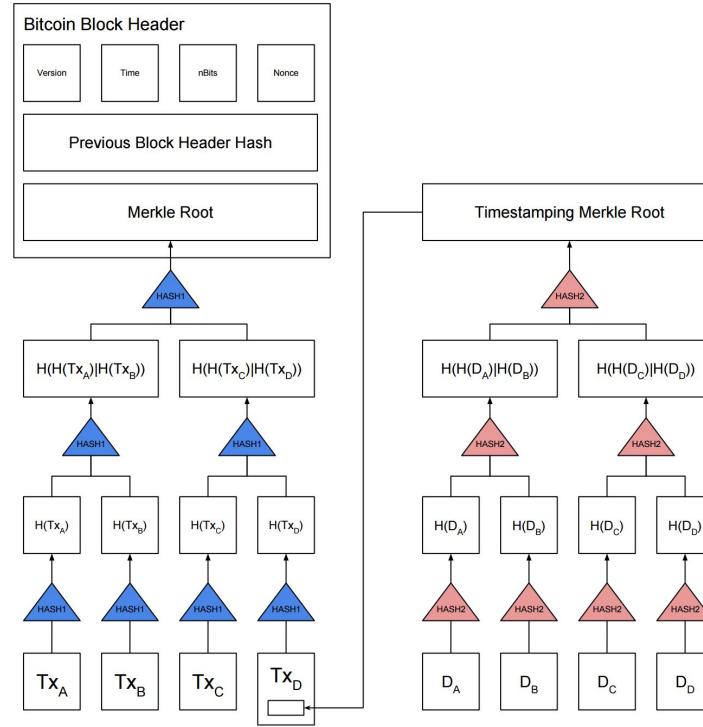
Transazion
i



stamps.org

← Documenti

OpenTimestamps is flexible

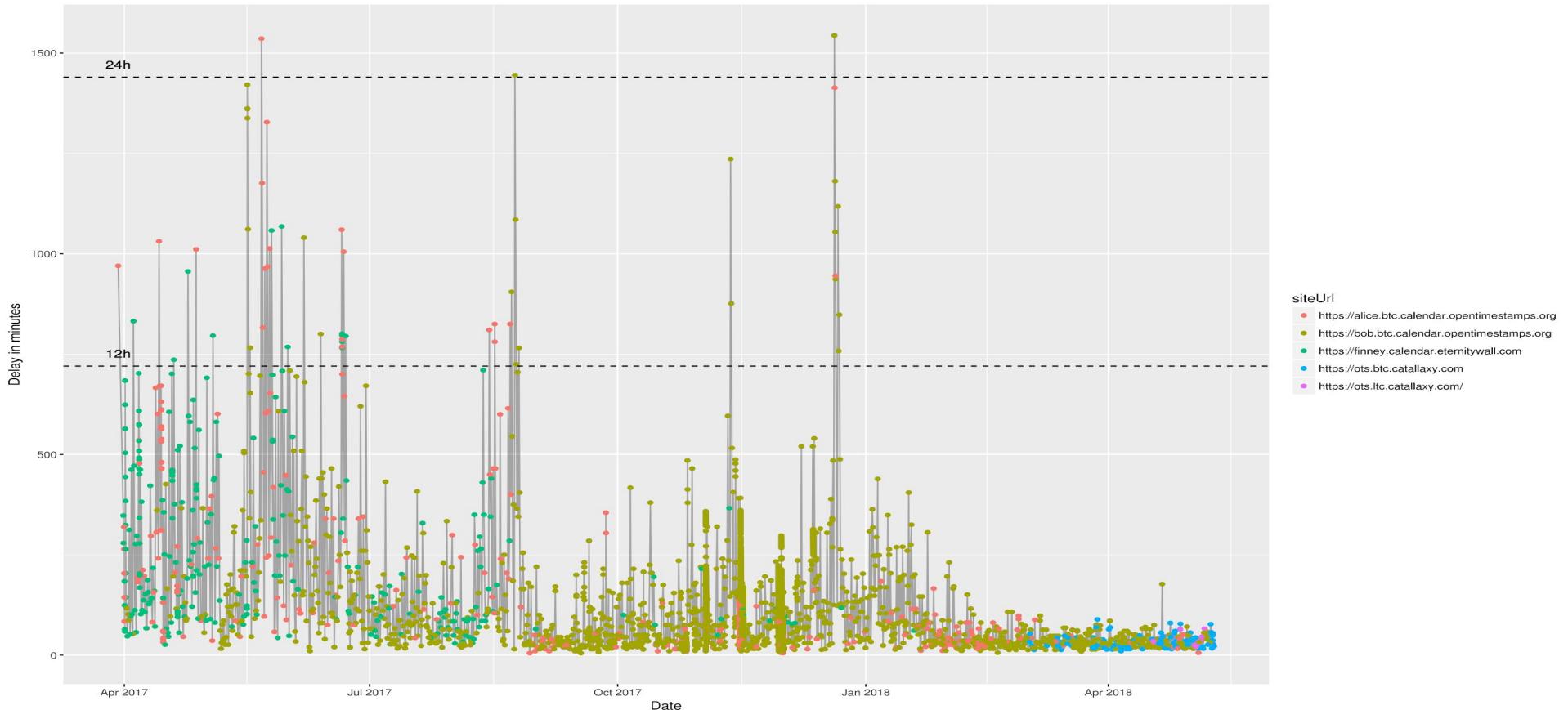


Scenari di utilizzo

- **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!



Block Alleviation	Pending	Unknown	Comments	Fork
append7fa90f..	1580513645468000000	1580513645468000000		
sha256d	ad4f17512f6a20761f87a7a132e1154d4561c16979c1aa3913a25d7e95f1			
Fork	Fork in 2 paths			
appenddfa7c8a..	1580513645468000000	1580513645468000000		
sha256d	b0fc95ca22ea17c02be89518843ebe8950f24423f3949f1c50			
appendff45d..	1580513645468000000	1580513645468000000		
sha256d	1a6933712a1e0200d1c15446075c0273a2d3e1387a2d35910a94			
appendfb0b1..	1580513645468000000	1580513645468000000		
sha256d	654a461985069734f091aee0e052d101f150473b305ecea896			
prependff537d..	1580513645468000000	1580513645468000000		
sha256d	933716c1a544c65f983a6e8774f0f91aee0352d071216f501a0373b305ecea896			
appendff917b..	1580513645468000000	1580513645468000000		
Forking Alleviation	Pending alleviation server: https://ice.etc.calendar.opentimestamps.org			
sha256d	861755c1481725462e6f8006146951892e757078f9e2f98c912be			
appendff4fe1..	1580513645468000000	1580513645468000000		
sha256d	e485f5c454296a56e557b798f89507b76464468849388719a8796791256			
prependff934c..	1580513645468000000	1580513645468000000		
sha256d	e14d4f4ec09880196a99e0c5a18946837630536a5754666a091			
appendff94e..	1580513645468000000	1580513645468000000		
sha256d	7b139405451460670975595696951420322095a51c7d71c1625040270			
appendff9e2f..	1580513645468000000	1580513645468000000		
sha256d	4b37f69a309516b716ab7aef17235481939539a441e2a2d30e73			
appendff98f3..	1580513645468000000	1580513645468000000		
sha256d	595595ba1487f991794280c16ce1f5f5e0af195036f96a909134453825			
prependff20d7..	1580513645468000000	1580513645468000000		
sha256d	407295206046013eb1913370154545479e6e4257129e098d1e005300			
prependff485..	1580513645468000000	1580513645468000000		
sha256d	95649493a49e02099917751a355246e5a501394027129e098d1e005300			



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>



Eternity Wall - <https://eternitywall.com> | OpenTimestamps - <https://opentimestamps.org>

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



Eternity Wall - <https://eternitywall.com> | OpenTimestamps - <https://opentimestamps.org>

<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.



A screenshot of the OpenTimestamps website. At the top, it says "Get timestamps for Internet Archive's collections". Below that is a search bar with the placeholder "Search on Archive.org" and a "SEARCH" button. Underneath the search bar, there is sample text: "Example: NASA Apollo Program". At the bottom left is the OpenTimestamps logo.



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 | Seleccionar la fecha | FILTRAR | 1 2 3 4 5 6 7 8 »

26-02-2018

Sección	PDF hash	Certificación	PDF	OTS
1	e87d91aa9d1574ae2c699a65ddff344941aab50a32a07948b887755dd702257	26-02-2018 06:10:18		
2	4a0b9a3111041d61035c9300194ac62597598a5ed8f6938672fb9973636e3d0	26-02-2018 07:00:09		
3	2c9955d95d12ba939ce86cf1efc416d239b3f07185446ada92b99d1a38eeaa1	26-02-2018 07:00:10		
4	7c3983fb3b55b2e1b8673bed04e882f9356065576b5815706495a374d7301723	26-02-2018 06:10:18		

23-02-2018

Sección	PDF hash	Certificación	PDF	OTS
1	dd95bf584fe85a4ee269337de993621966b7e8e5a62440135c0d0cb073ce8e5c	23-02-2018 06:18:28		
2	49431926bd8414921bef5851c731bafaafcd158d05cd277b1c92d174bd3c300	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

@otsproofbot2 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.



Malwario ✨_(`)_)_辜负
@tulipan81

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

1 1 1 1

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

1 1 1 1

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> | OpenTimestamps - <https://opentimestamps.org>

Agenda

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



Eternity Wall - <https://eternitywall.com> | OpenTimestamps - <https://opentimestamps.org>



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>

Verifica online

The screenshot shows the main landing page of OpenTimestamps. At the top, there's a navigation bar with links for "STAMP AND VERIFY", "HOW IT WORKS", "MEMBERS", "CODE REPOSITORIES", and "MAILING LISTS". Below the navigation is a large blue banner featuring a world map composed of geometric shapes. To the left of the map, the text "A timestamping proof standard" is displayed, followed by a paragraph about OpenTimestamps' aim to be a standard for blockchain timestamping. Below the banner, there are six circular icons with accompanying text: "STAMP & VERIFY" (in-browser stamper and verifier), "HOW IT WORKS" (details on OpenTimestamps), "MEMBERS" (companies using OpenTimestamps), "CODE REPOSITORIES" (OpenTimestamps repositories), "MAILING LISTS" (announcements), and "INTERNET ARCHIVE" (OpenTimestamps proof for the Internet Archive).

This screenshot shows the "STAMP & VERIFY" feature. It features a large dashed rectangular input field with a "Drop here a file to stamp OR an .ots proof file to verify" placeholder. Below the input field, a note states: "The hash is calculated on your browser preserving your privacy. More... timestamping proof download will start automatically after uploading document." At the bottom of the page, there's a footer with the Eternity Wall logo and the URL "Eternity Wall - <https://eternitywall.com> | OpenTimestamps - <https://opentimestamps.org>".

The screenshot shows a timestamp detail page. At the top, it displays the timestamp "efaa174f68e5" and its "Document digest (sha256)": "efaa174f68e59705757460f4f7d204bd2b535cf194d9d945418732129404ddb". Below this is a button labeled "DOWNLOAD THIS TIMESTAMP". A legend at the bottom identifies five types of attestations: Bitcoin Attestation (green square), Unknown Attestation (grey square), Pending/Other Attestation (orange square), Comments (purple square), and Fork (blue square). The main area lists various timestamp entries, each with a unique ID, a timestamp type (e.g., "append", "sha256", "Fork"), and a corresponding hex string value.

	Bitcoin Attestation	Unknown Attestation	Pending/Other Attestation	Comments	Fork
append(839037...)					efaa174f68e59705757460f4f7d204bd2b535cf194d9d945418732129404ddb839037eeff449de6da322ca27347c45
sha256()					679a59f6661f9d809d6f72d2cc080a20435c5c793ace1961ca78e38693f2f53d6b4023b6edd3a
Fork					Fork in 2 paths
append(6b4023...)		1	679a59f6661f9d809d6f72d2cc080a20435c5c793ace1961ca78e38693f2f53d6b4023b6edd3a 0ebe09e5d718723b9e		
sha256()		1			fdd8c2334c77bf1204338bb2178d73e523988d7dcda13259d3a099f31623755d
prepend(57d465...)		1			57d46515fd8c2334c77bf1204338bb2178d73e523988d7dcda13259d3a099f31623755d
append(eadd66...)		1	57d46515fd8c2334c77bf1204338bb2178d73e523988d7dcda13259d3a099f31623755d 66b168bd574		
Pending Attestation					Pending attestation: server https://alicebtc.calendar.opentimestamps.org
append(a3ad70...)	2				679a59f6661f9d809d6f72d2cc080a20435c5c793ace1961ca78e38693f2f53da3ad701ef9f105 35a8496805a9908580
sha256()	2				76e9ac3b57c1548428ea5162979c96483a03c87c69a1b8614d1cba387e0f5
prepend(57d465...)	2		57d4651576e9ac3b3b57c1548428ea5162979c96483a03c87c69a1b8614d1cba387e0f5		
append(647b90...)	2		57d4651576e9ac3b3b57c1548428ea5162979c96483a03c87c69a1b8614d1cba387e0f5 90ea1b27097		
Pending Attestation					Pending attestation: server https://bobbtc.calendar.opentimestamps.org



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 hash 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
```





Domande?



Eternity Wall - <https://eternitywall.com> | OpenTimestamps - <https://opentimestamps.org>





Grazie

Valerio Vaccaro

valerio@eternitywall.com

- Presentazione: <http://ew.link/8Uq2>
- Marcatura temporale: <http://ew.link/9xV3>

