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

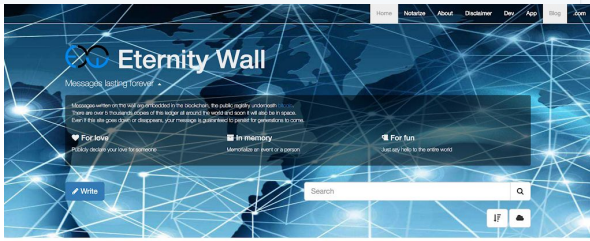
Chi siamo?

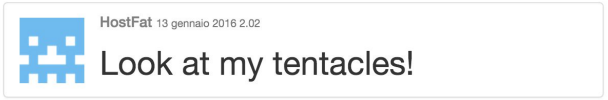
EW nasce nel 2015 per:

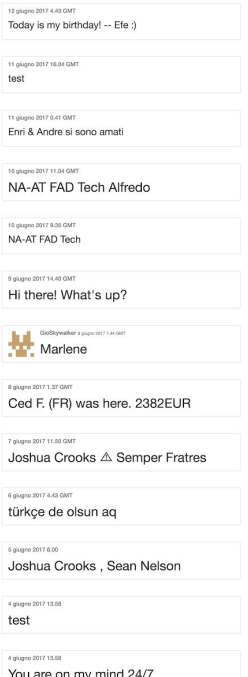
- scrittura di informazioni sulla blockchain
- voglia di sperimentare
- applicazioni non finanziarie su blockchain

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

www.eternitywall.it







GET IT ON Google play

Eternity Wall - https://eternitywall.com

Chi siamo?

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

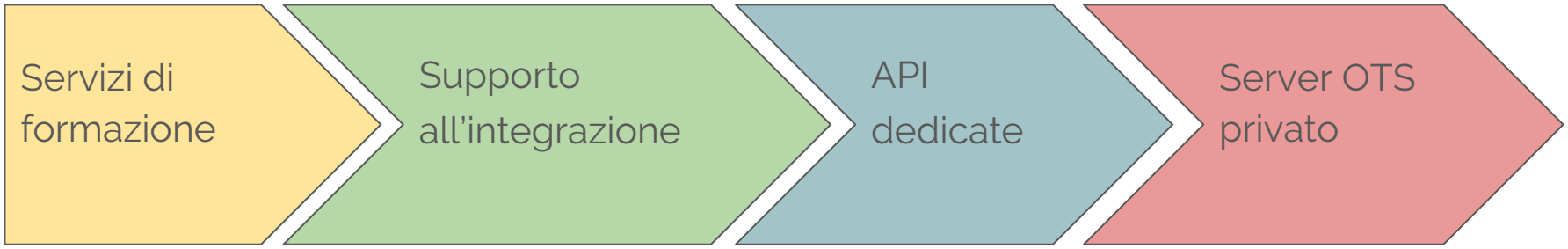
↓

Necessità di attribuire una data certa ad un documento.

↓

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

Business model



Lezioni	Sviluppo	API HTTP	Installazione
Corsi specifici	Integrazione	Autenticazione	Aggiornamento
	Personalizzazione	Assistenza	Manutenzione
		Servizi aggiuntivi	

Timestamping o marcatura temporale

- Il primo e più comune esempio è il **timbro postale**
  - Alice scrive a Bob, la data della comunicazione è apposto 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 uffciale, il notaio
  - Ad esempio per il rogito della casa

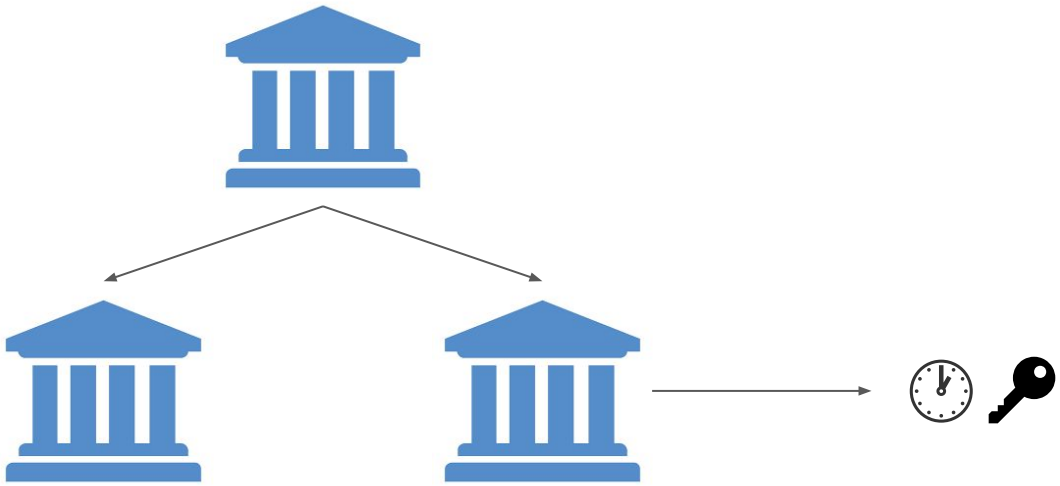
E per i documenti digitali?

Agenda

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

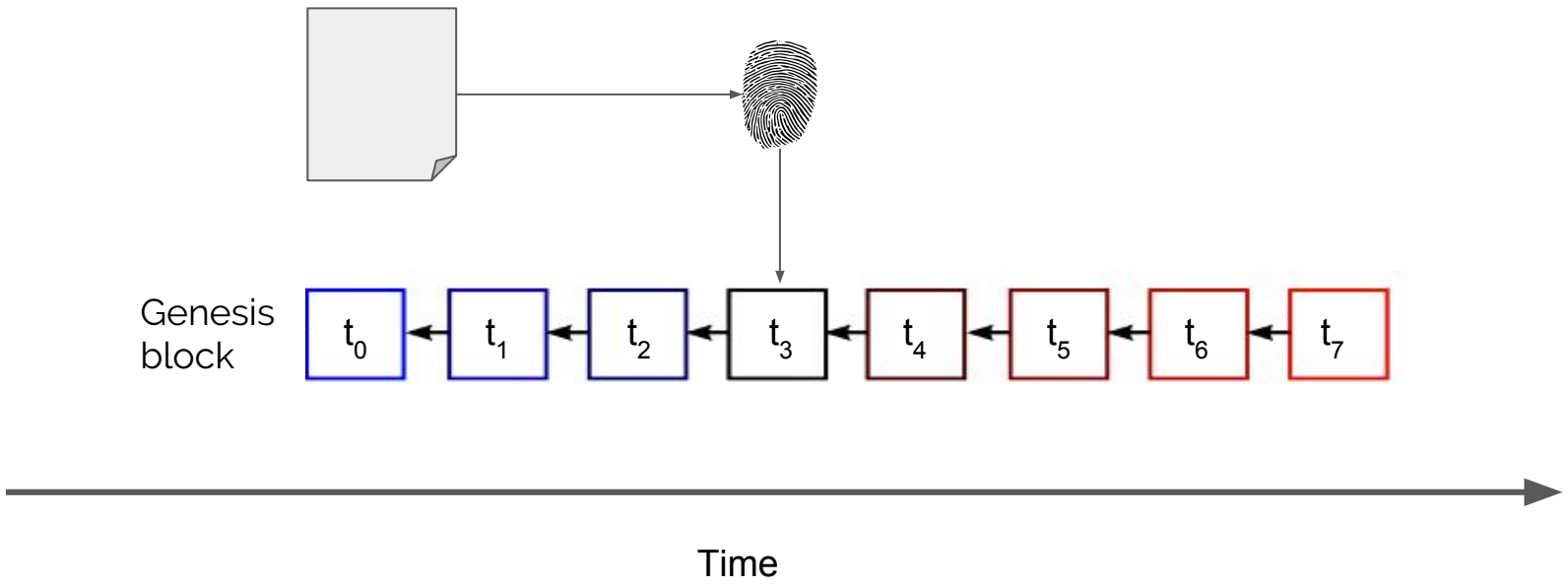
Marcatura temporale certificata

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



Marcatura temporale decentalizzata

Utilizza la blockchain in luogo della terza parte



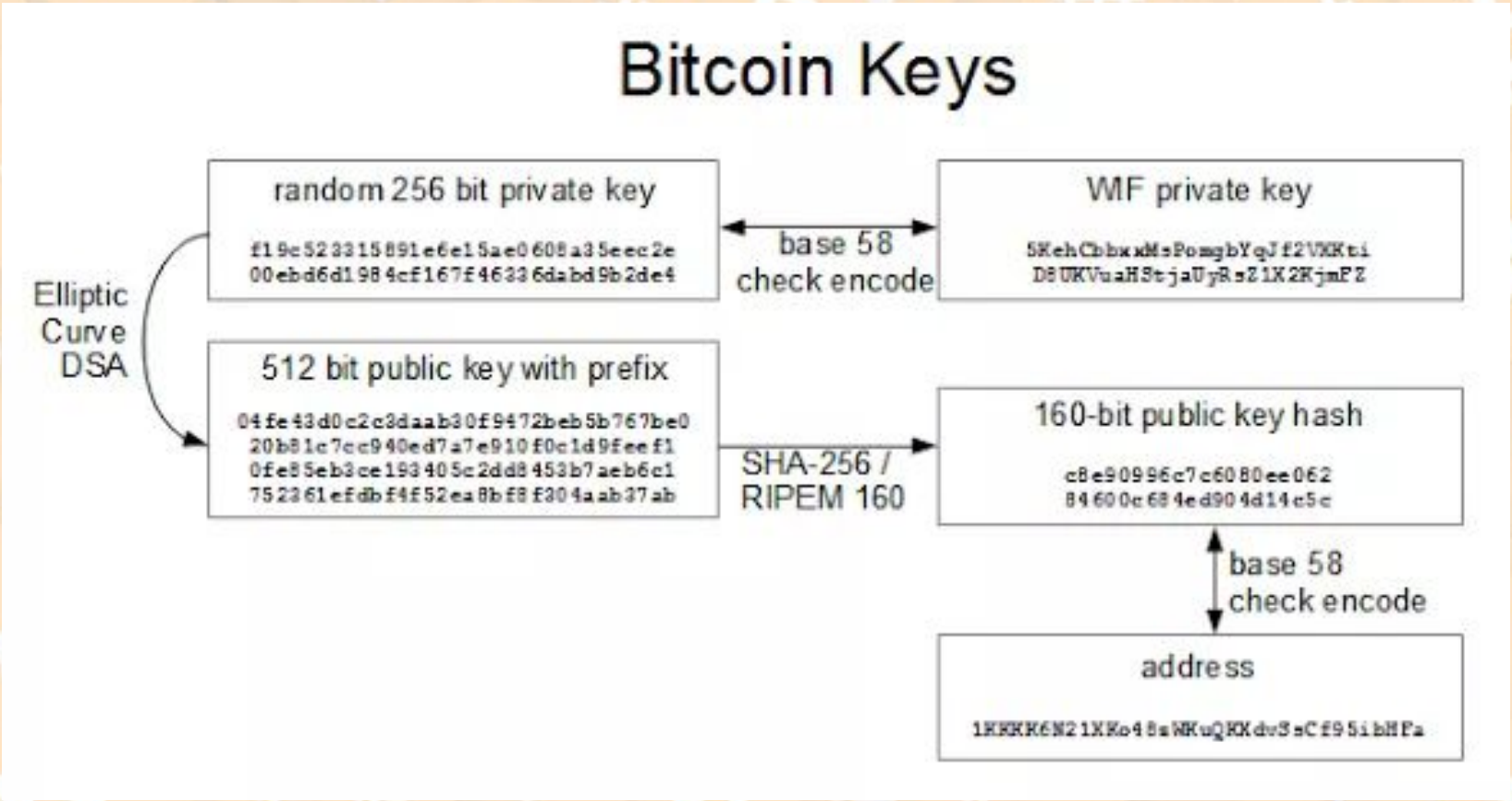
Introduzione a Bitcoin

Bitcoin: A Peer-to-Peer Electronic Cash System

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

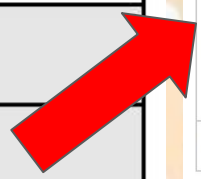
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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



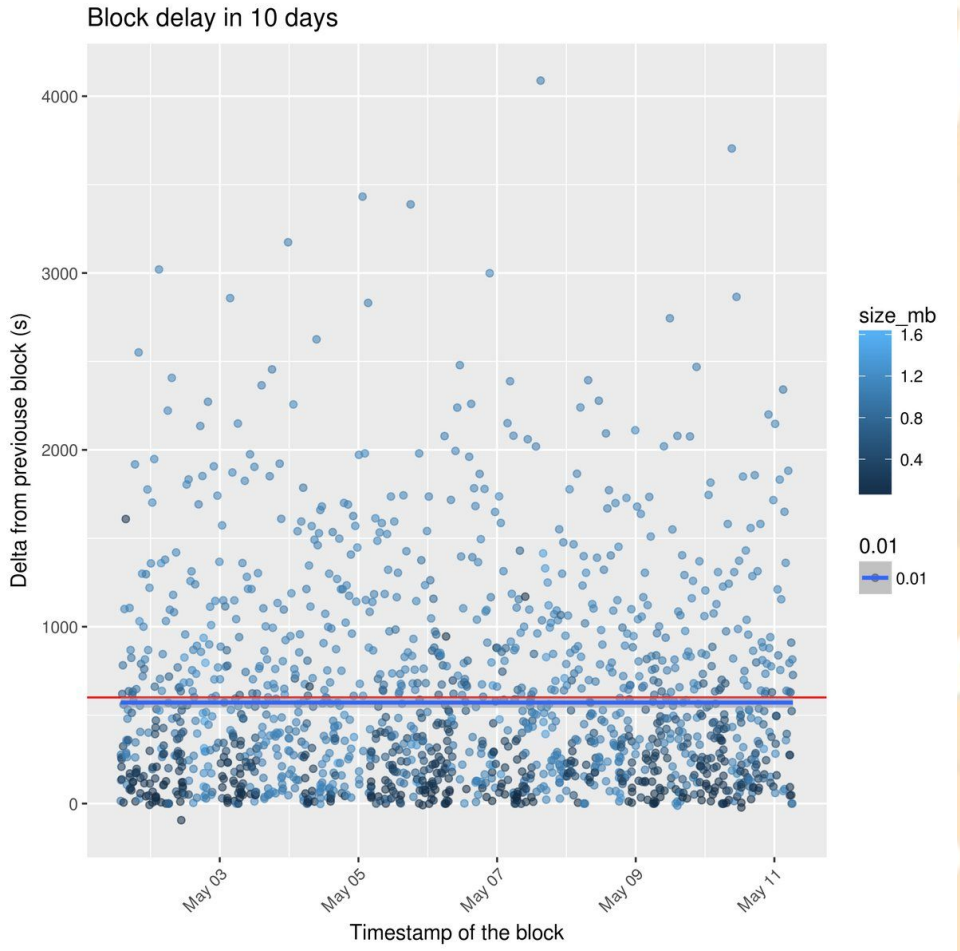
Introduzione a Bitcoin: blocchi e transazioni

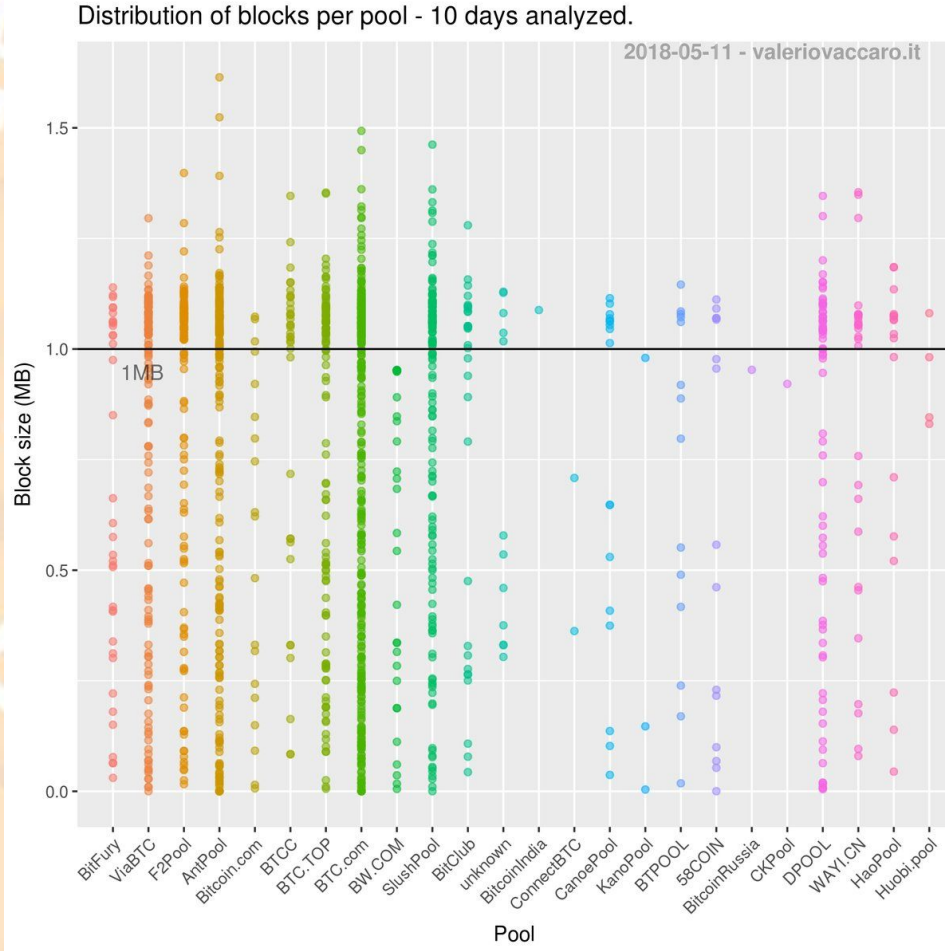
version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c8170100000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	



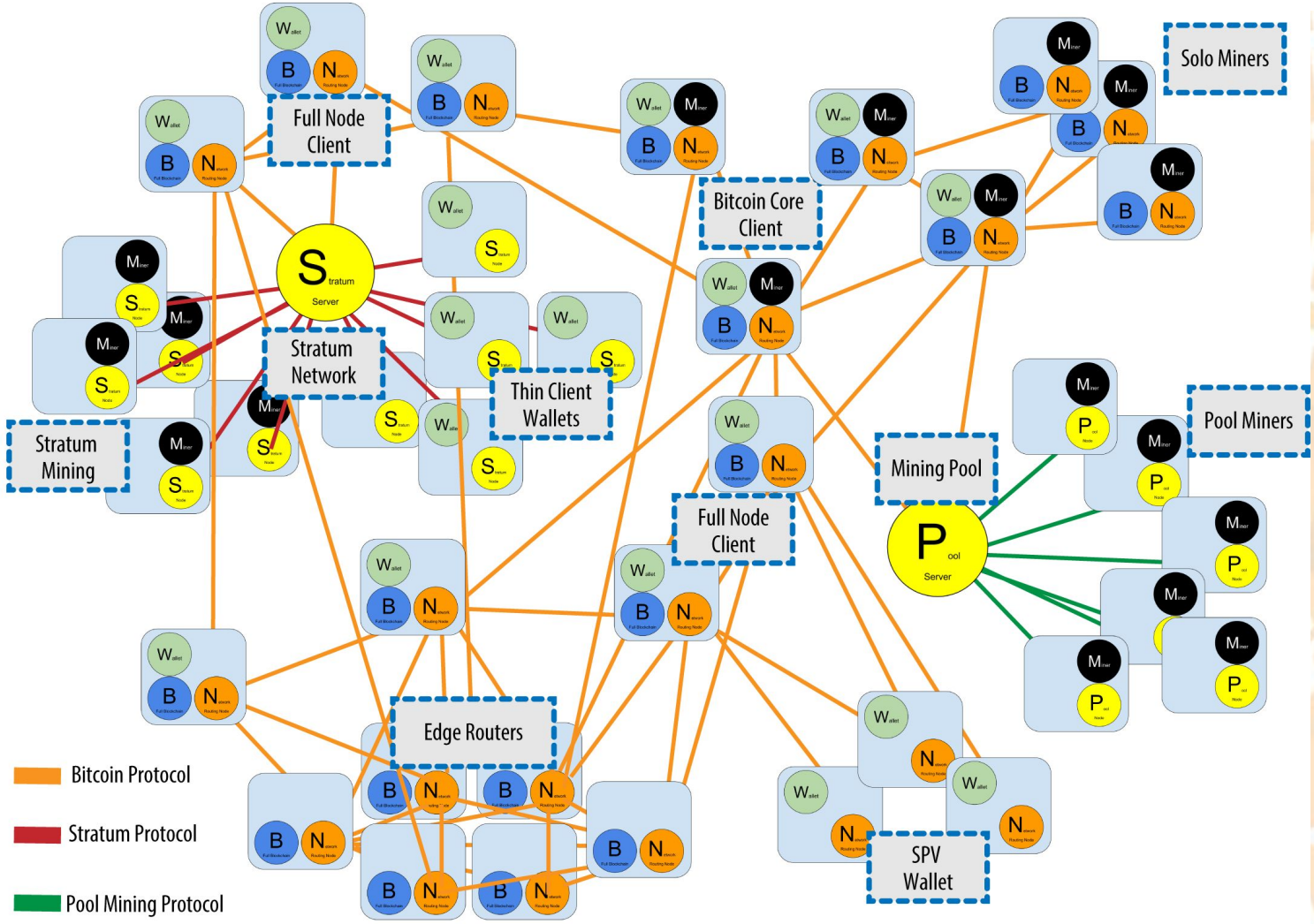
version		01 00 00 00
input count		01
input	previous output hash (reversed)	48 4d 40 d4 5b 9e a0 d6 52 fc a8 25 8a b7 ca a4 25 41 6f b5 0c d7 32 c8 b4 81
	previous output index	00 00 00 00
	script length	
	scriptSig	script containing signature
	sequence	ff ff ff ff
output count		01
output	value	62 64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

Introduzione a Bitcoin: velocità e spazio

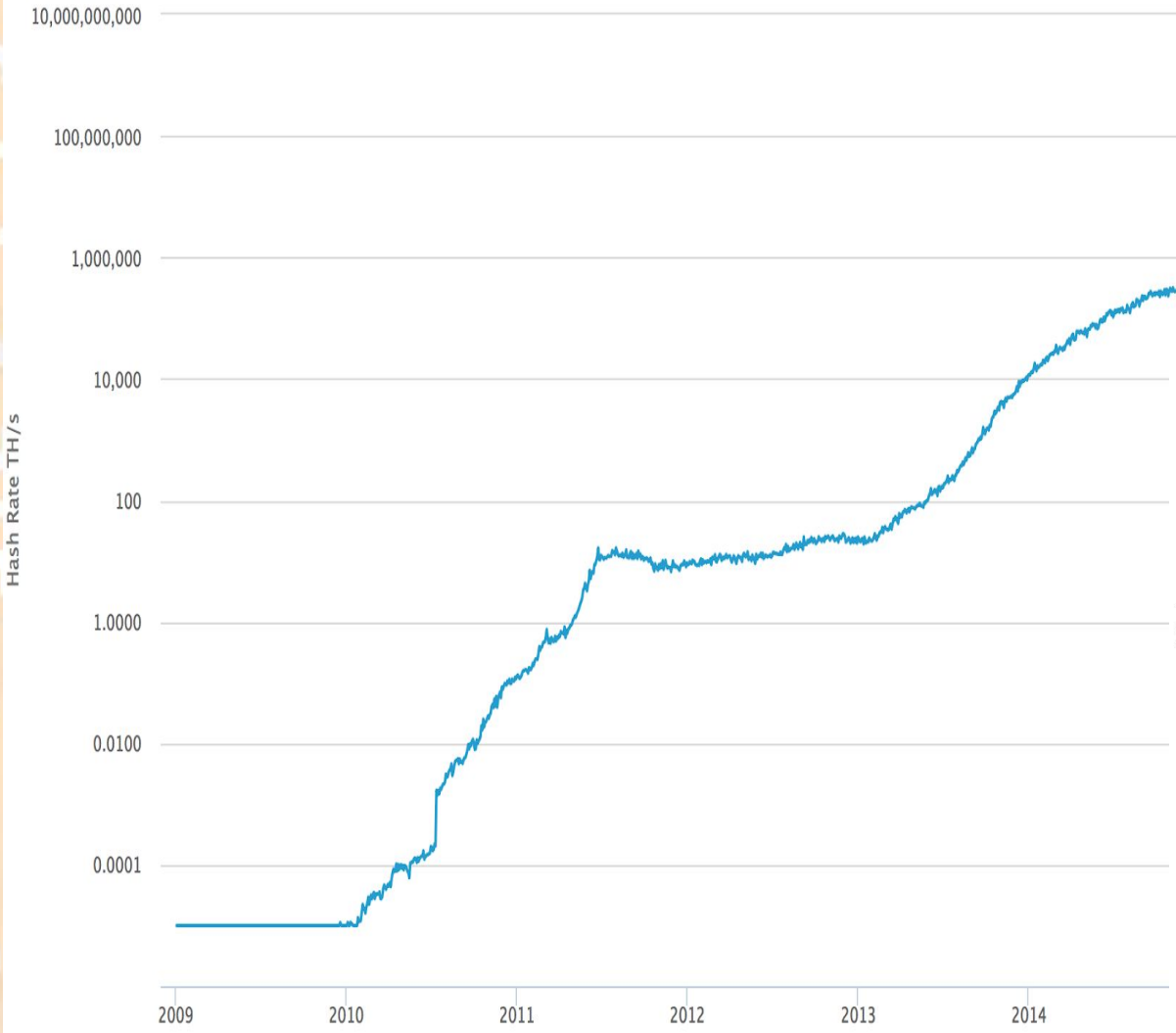


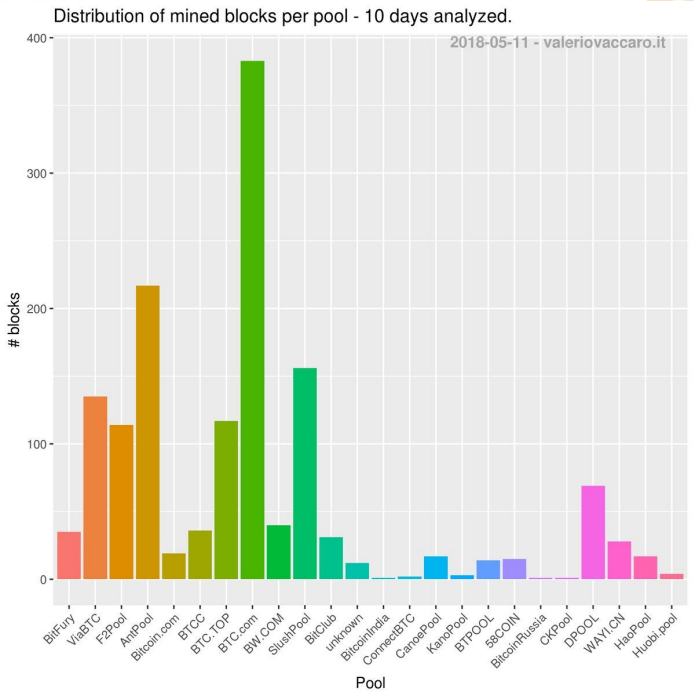


Introduzione a Bitcoin: architettura della rete



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

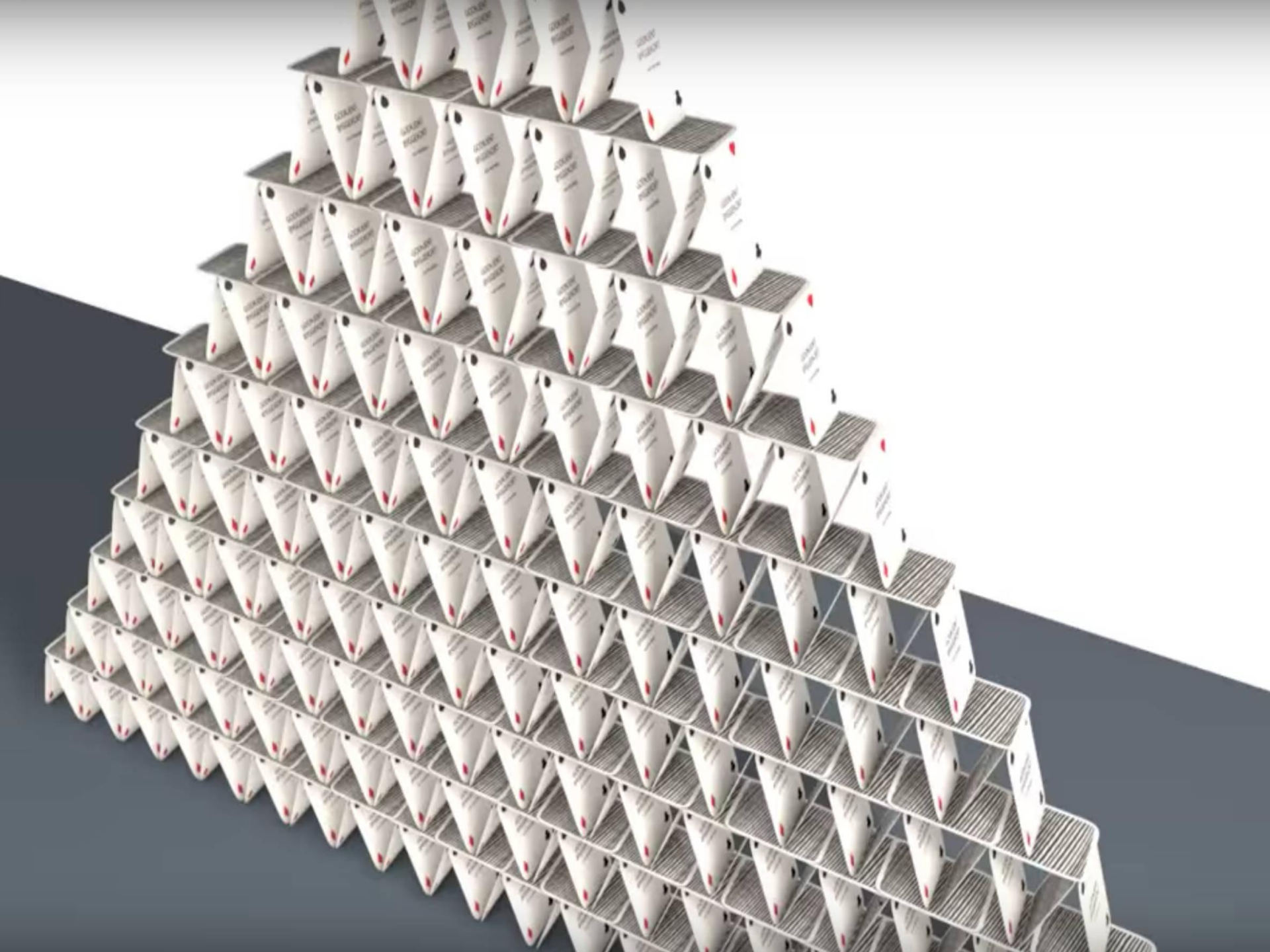
Differenza fra trusted e trustless timestamping

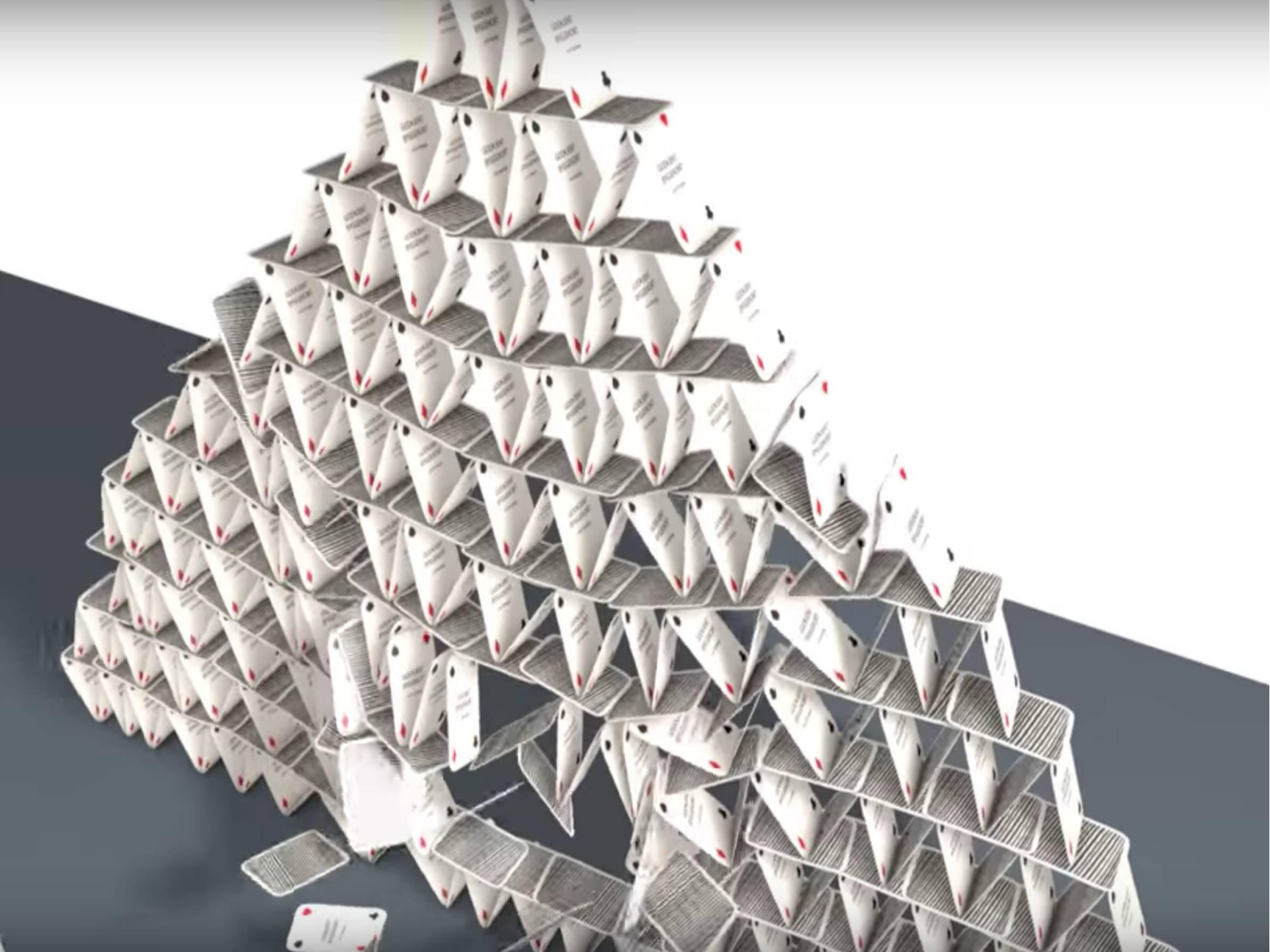
Nel modello basato su terze parti, cosa succede se una chiave viene compromessa?

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

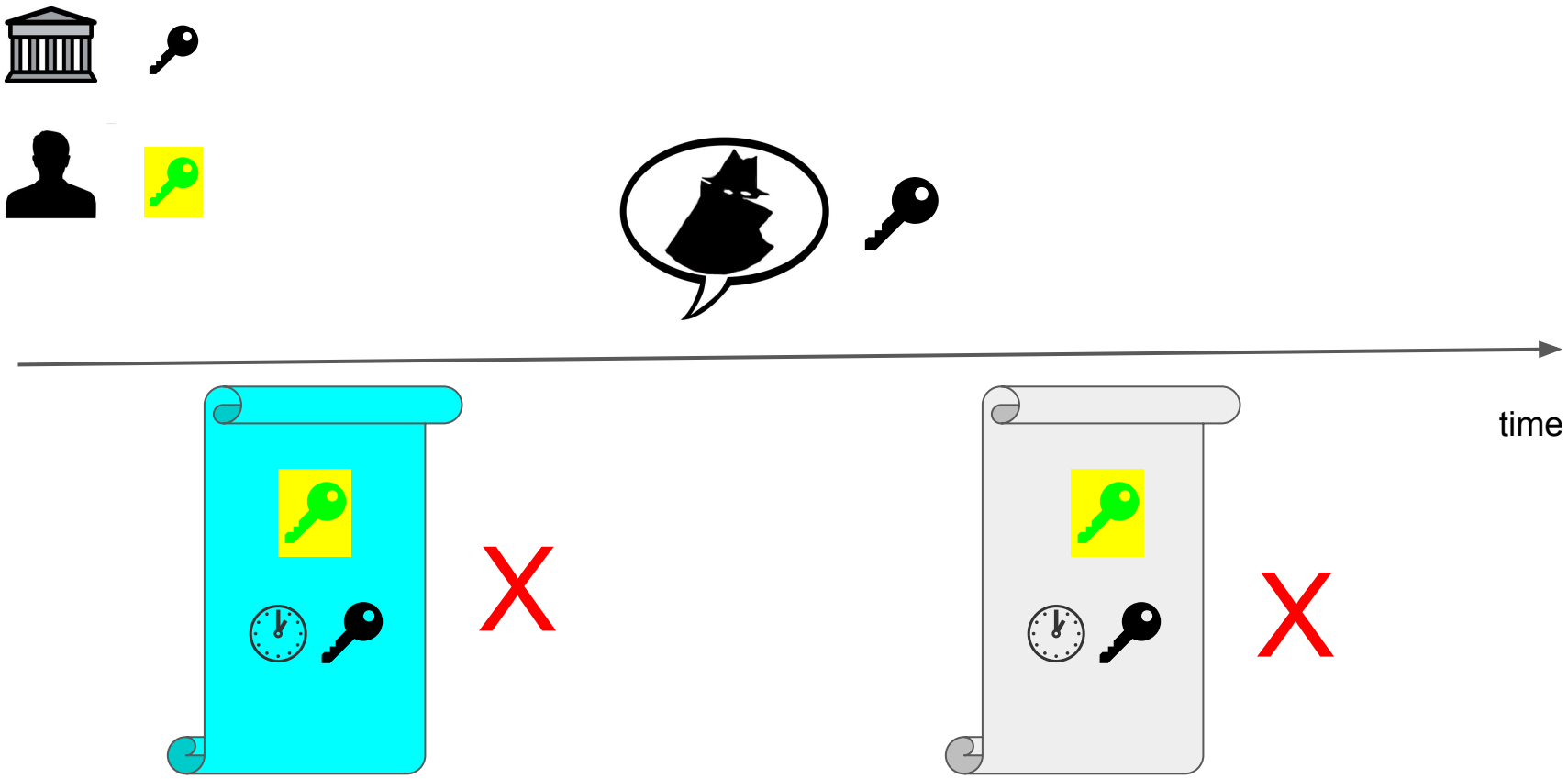
Errato

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

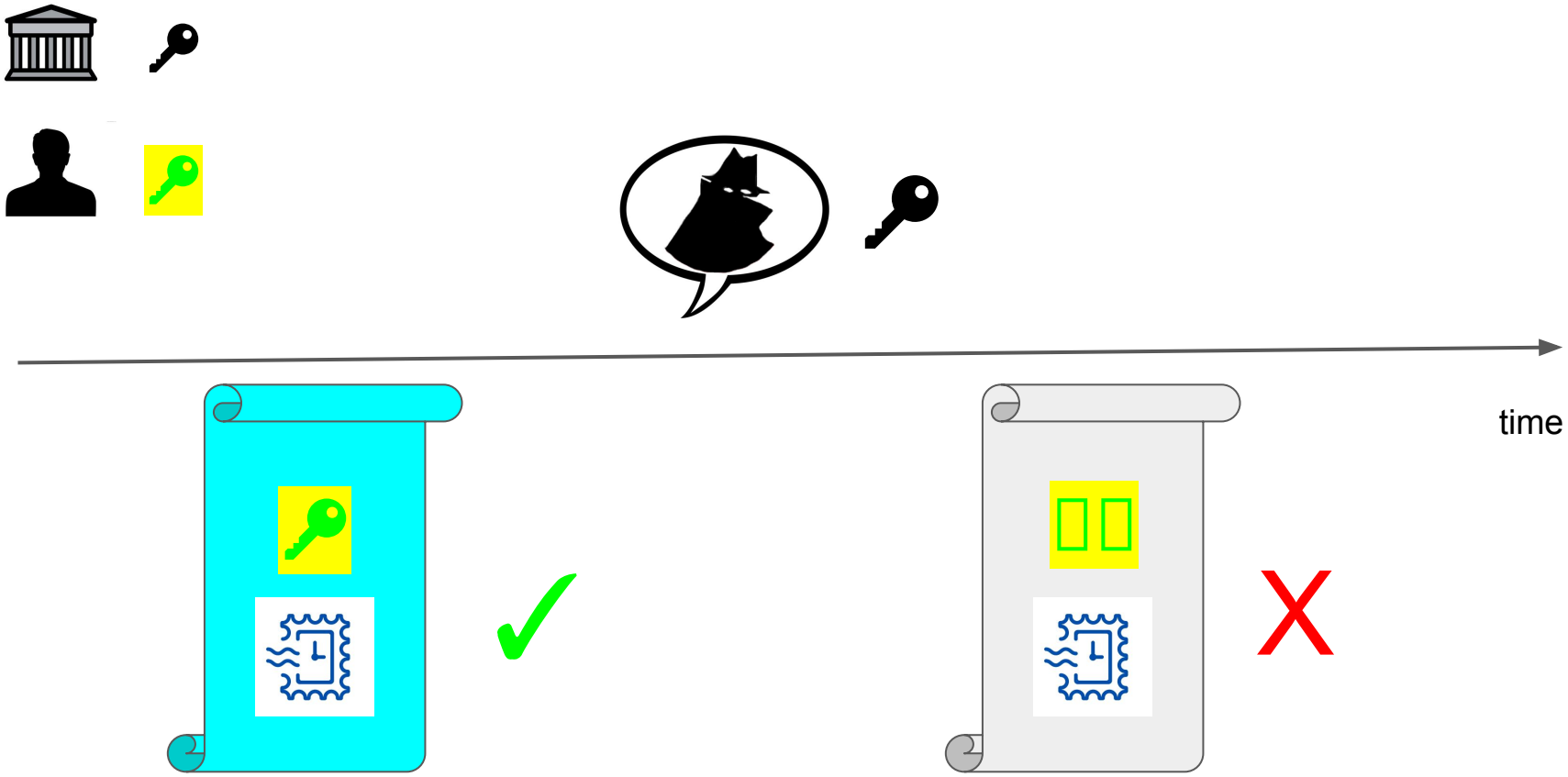




Marcatura temporale basata su firma digitale



Firma digitale con marcatura temporale trustless



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

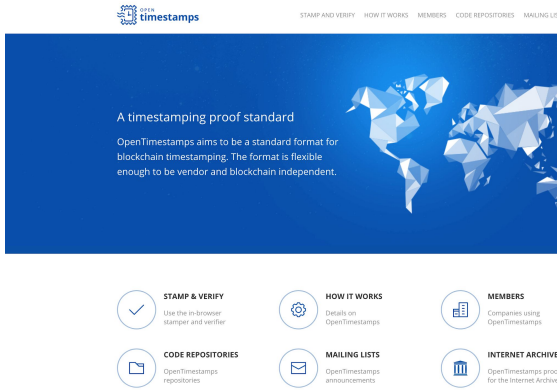
- Timestamping
  - An external viewer **could not** see all the element of the set
    - If someone timestamp two different version of a document, the rest of the world cannot see it
- Proof of publication
  - An external viewer **could** see all the the element of the set
    - Prevent double spend!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

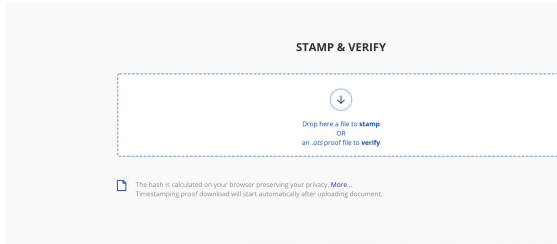
OpenTimestamps

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

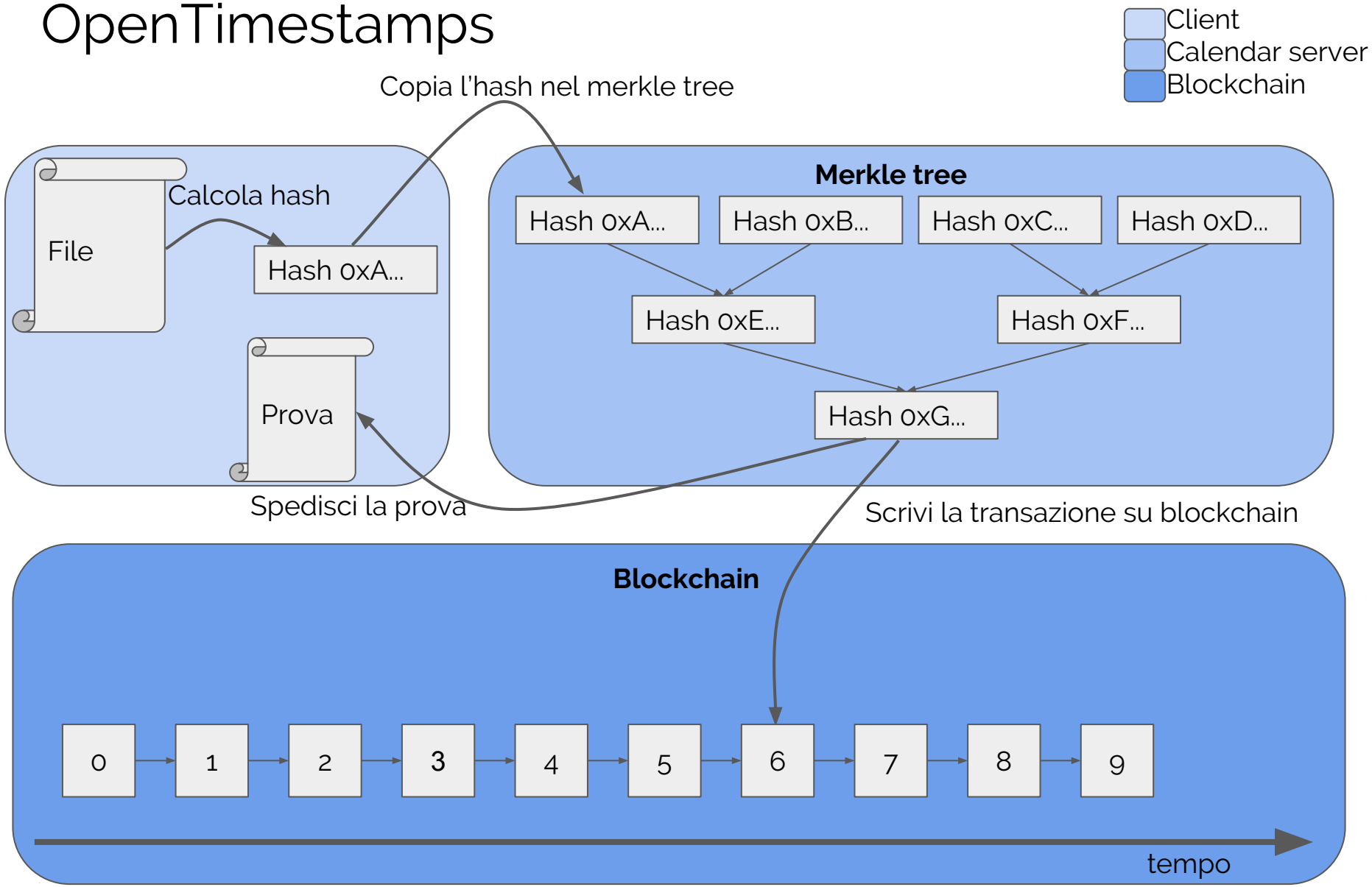
- **Trust** - OTS usa la blockchain bitcoin risultando decentralizzato, pubblicamente verificabile e rimuovendo la necessità di una certification authority,
- **Cost** - OTS può condensare un numero illimitato di timestamps in una singola transazione,
- **Convenience** - OTS genera un timestamp verificabile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

https://opentimestamps.org

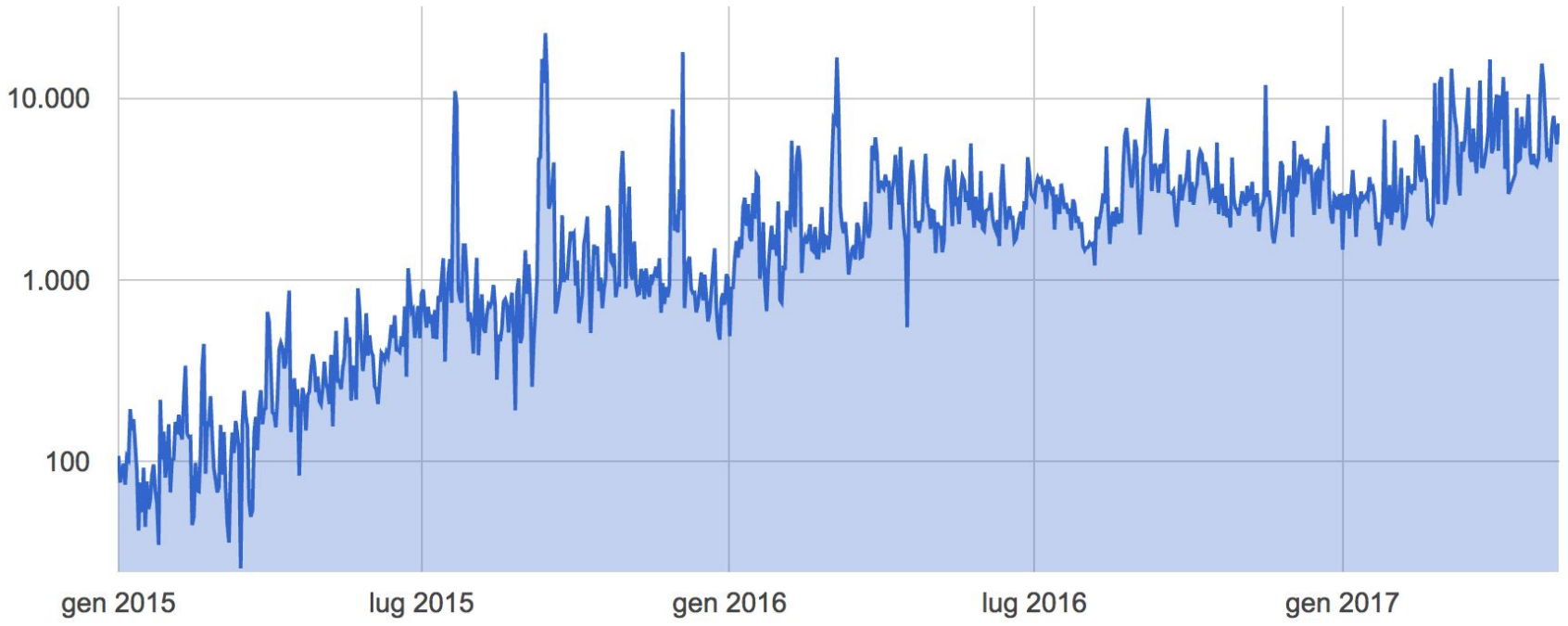




OpenTimestamps

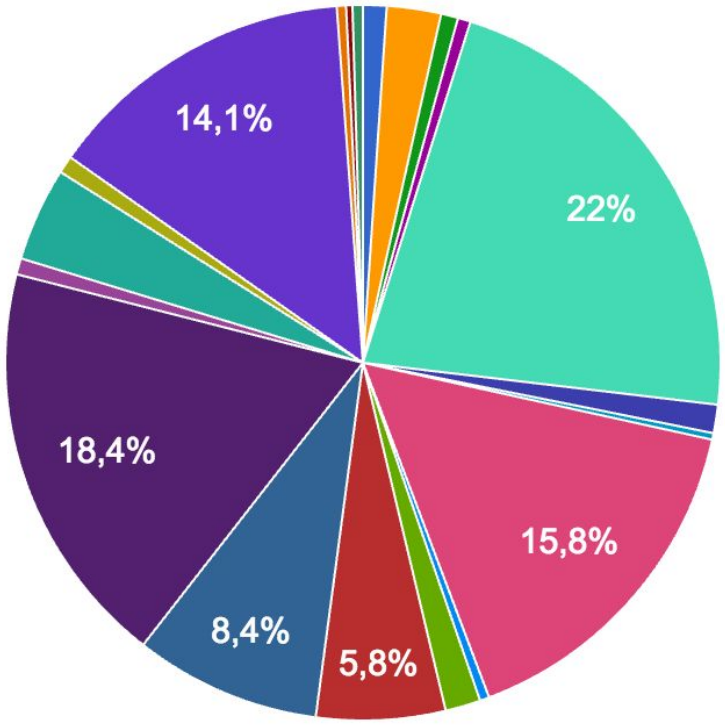


OP_RETURN tx per giorno



~5000 txs/day

Utilizzo di OP_RETURN



- Flu
- Coinspark
- SB.
- 0x4b4301
- Colu
- 503
- 0xe3b0c4
- Omni Layer
- Eternity Wall
- CP1
- Monegraph
- Factom
- Blockstack
- OKT
- Ascribe pool
- Stampery Old
- Open Assets
- 0xaa21a9
- Stampery 5
- 0x000000

1/2

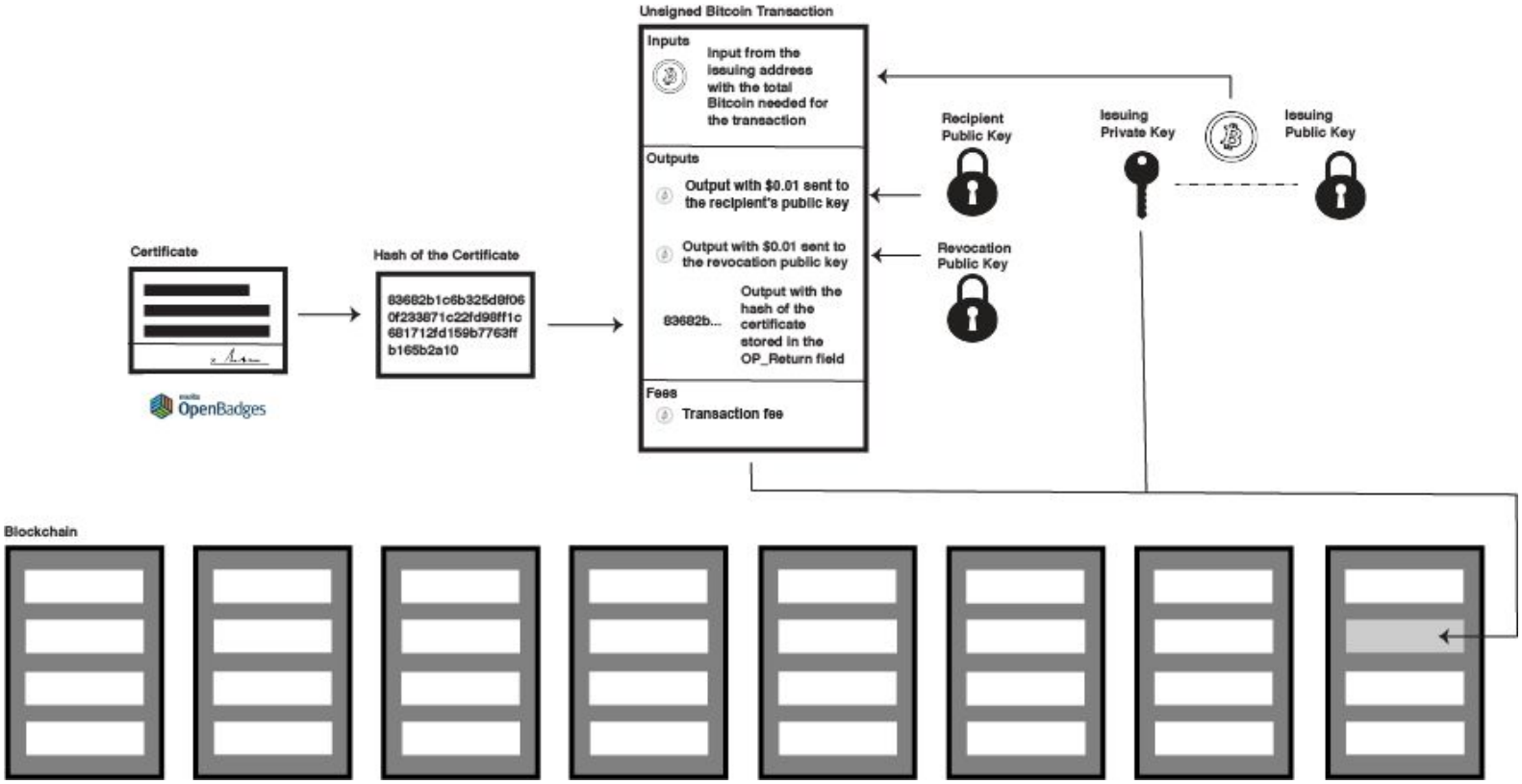
Source:
http://opreturn.org/

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 ≈ …

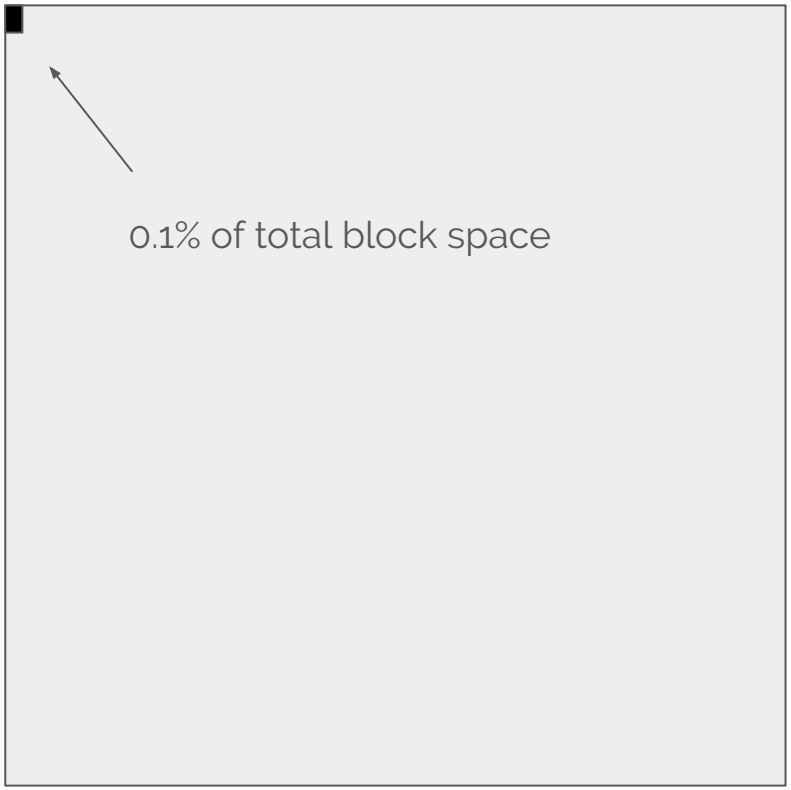
One-certificate-one-transaction

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

80MB blocks!

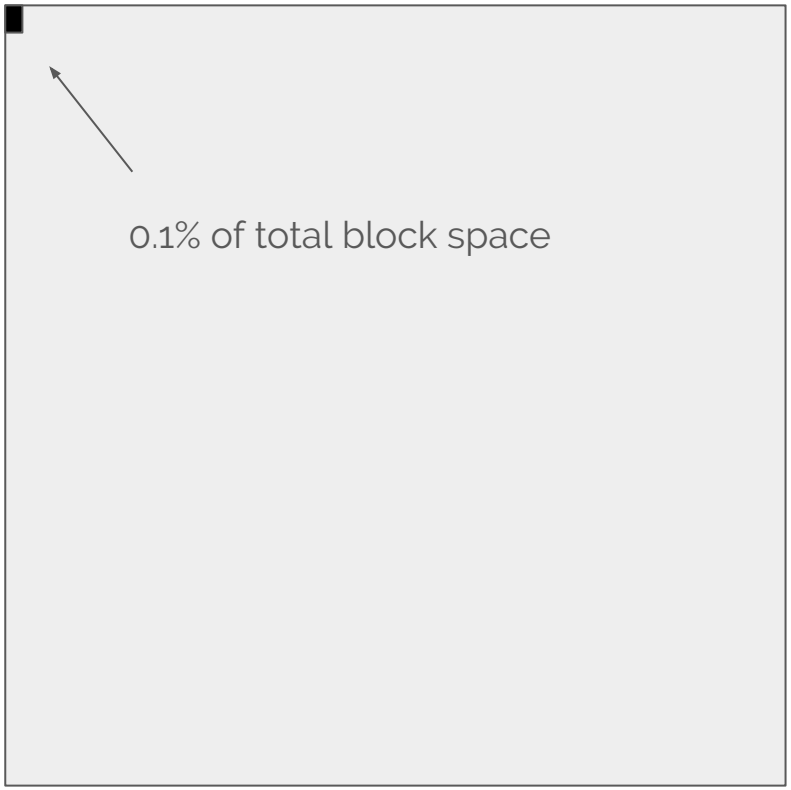
OpenTimestamps goal

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

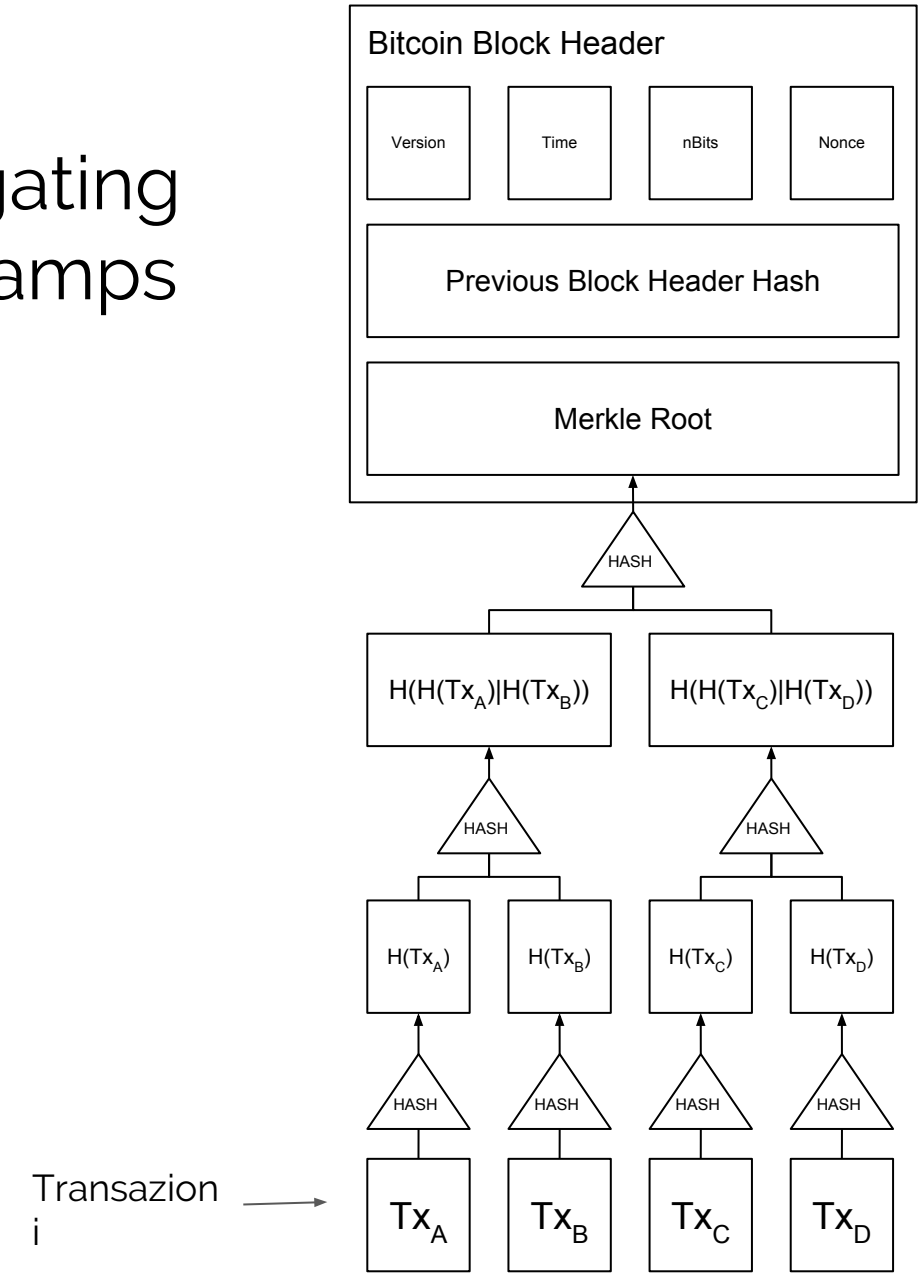


OpenTimestamps goal

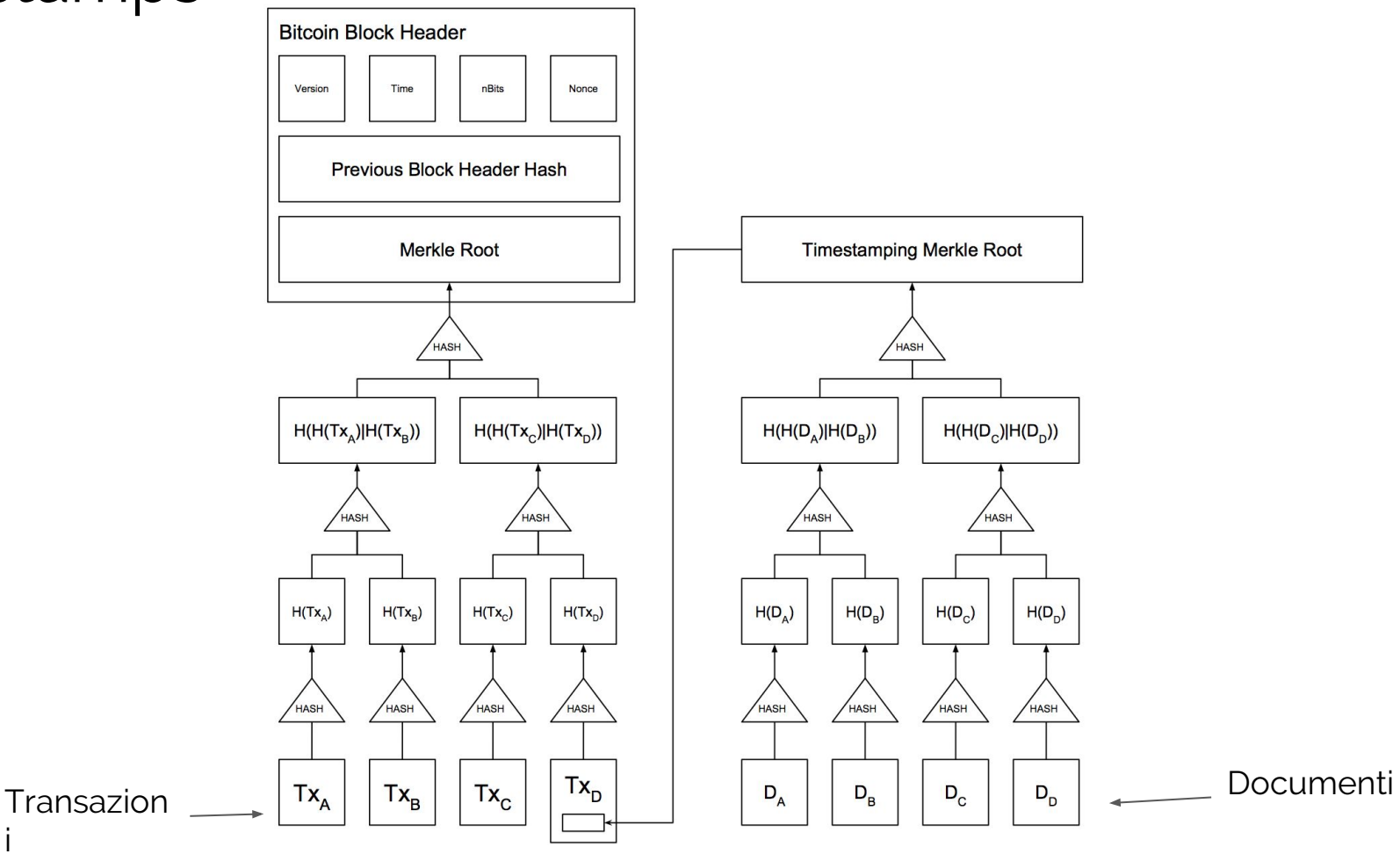
- ≈ 144 tx/day for global timestamping
- For maximum precision
- Less cost, 1/10 than now
- 0.1% of block
- 0% ? -> Sign to Contract R&D



Aggregating Timestamps



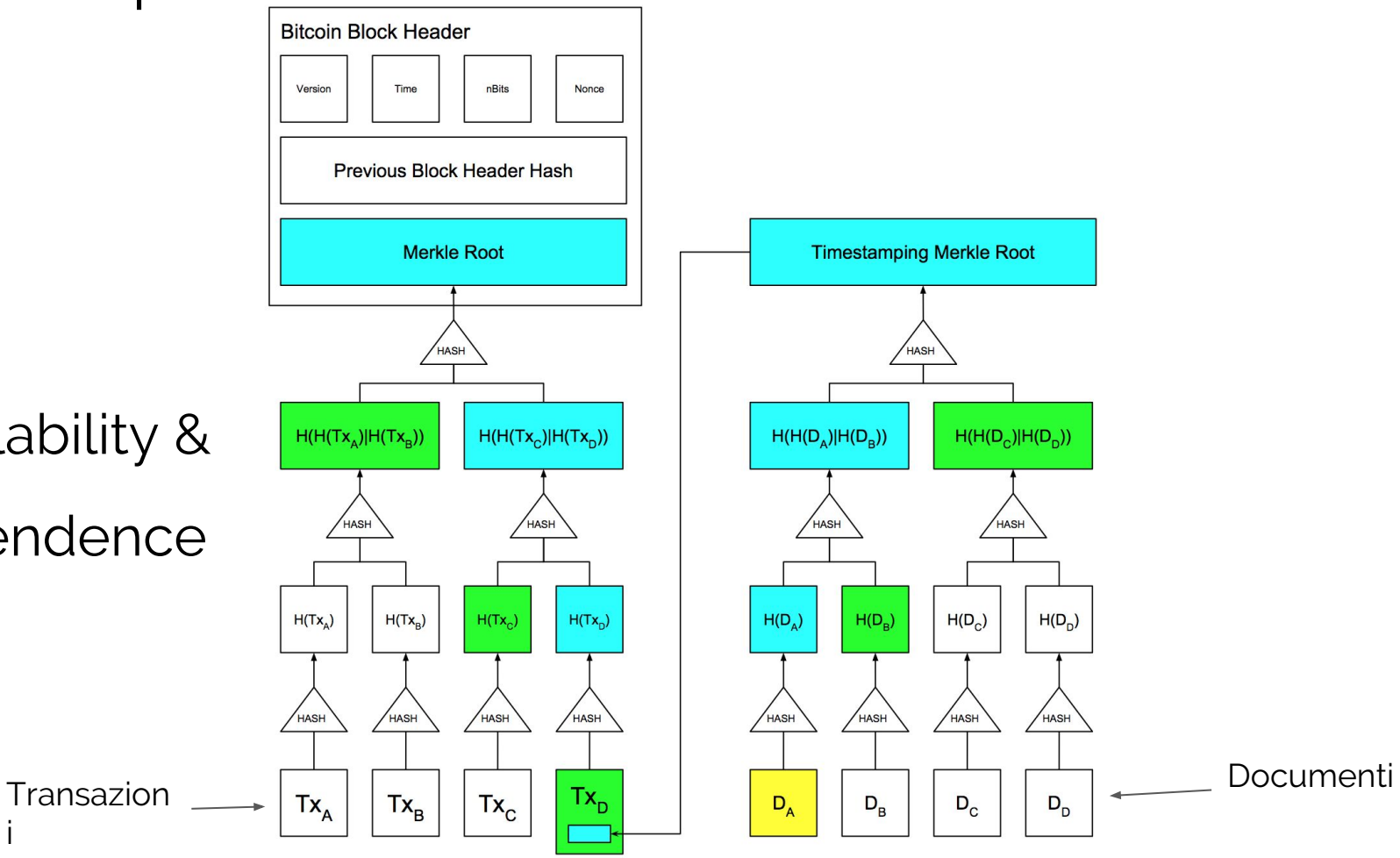
Aggregating Timestamps



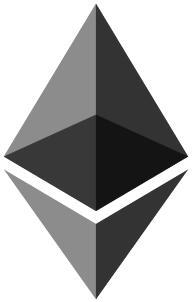
Aggregating Timestamps

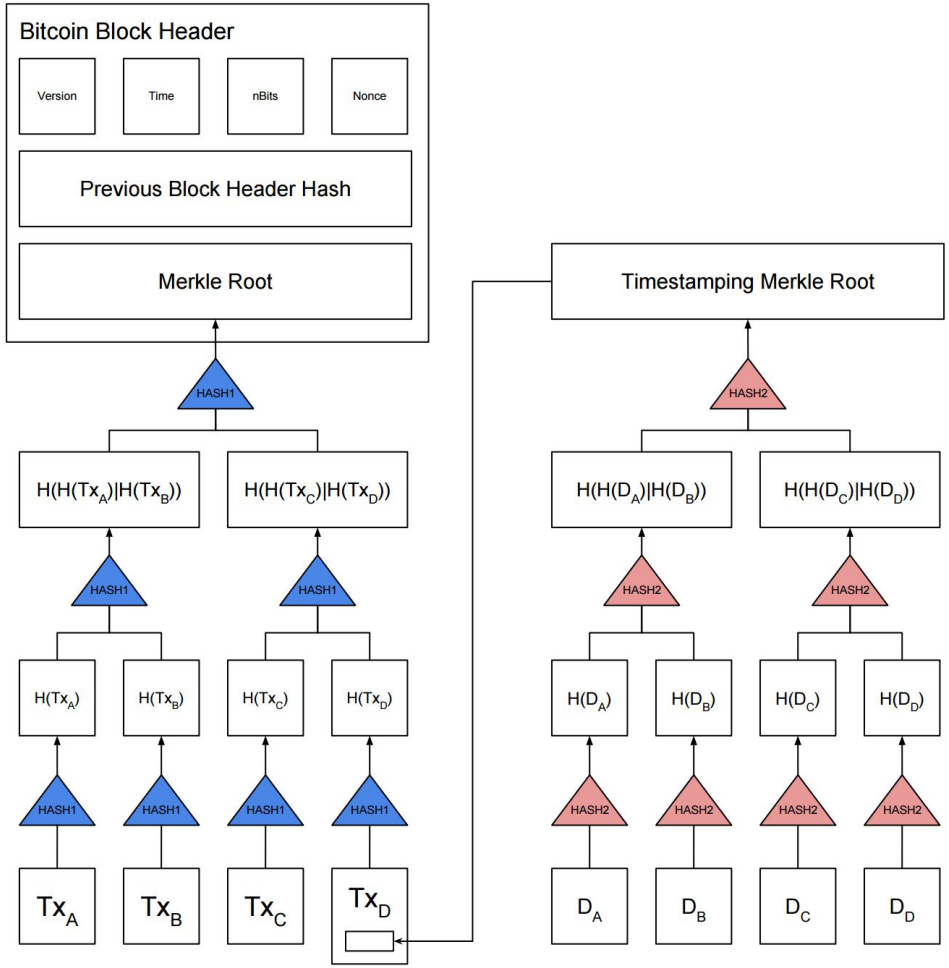
✓ scalability &

independence



OpenTimestamps is flexible





Scenari di utilizzo

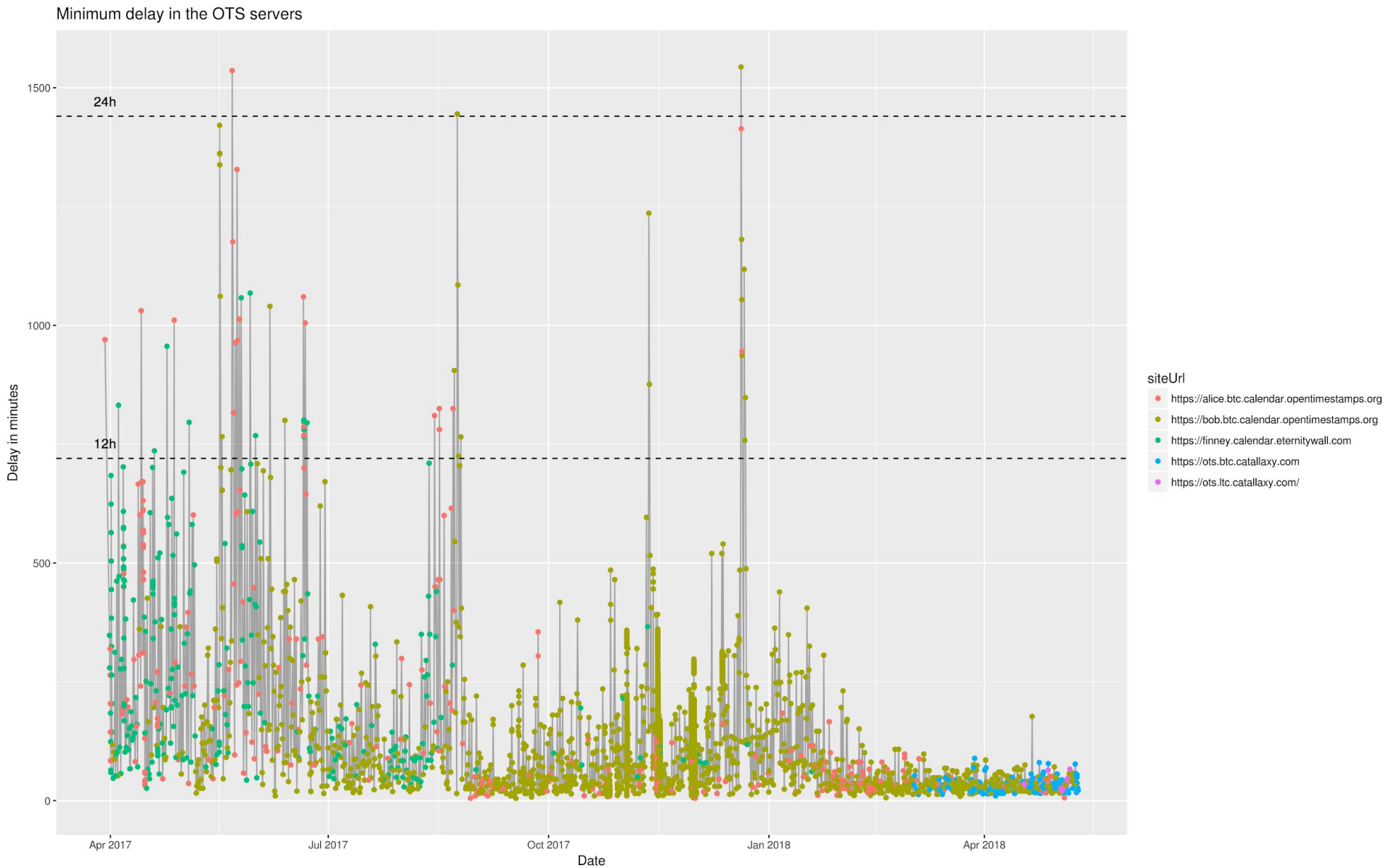
- **Scenario regolatorio**
  Creazione di prove di integrità dei dati e timestamping compatibili con le richieste regolatorie (es. Dodd-Frank), i dati sono integri secondo le direttive?

- **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



Software

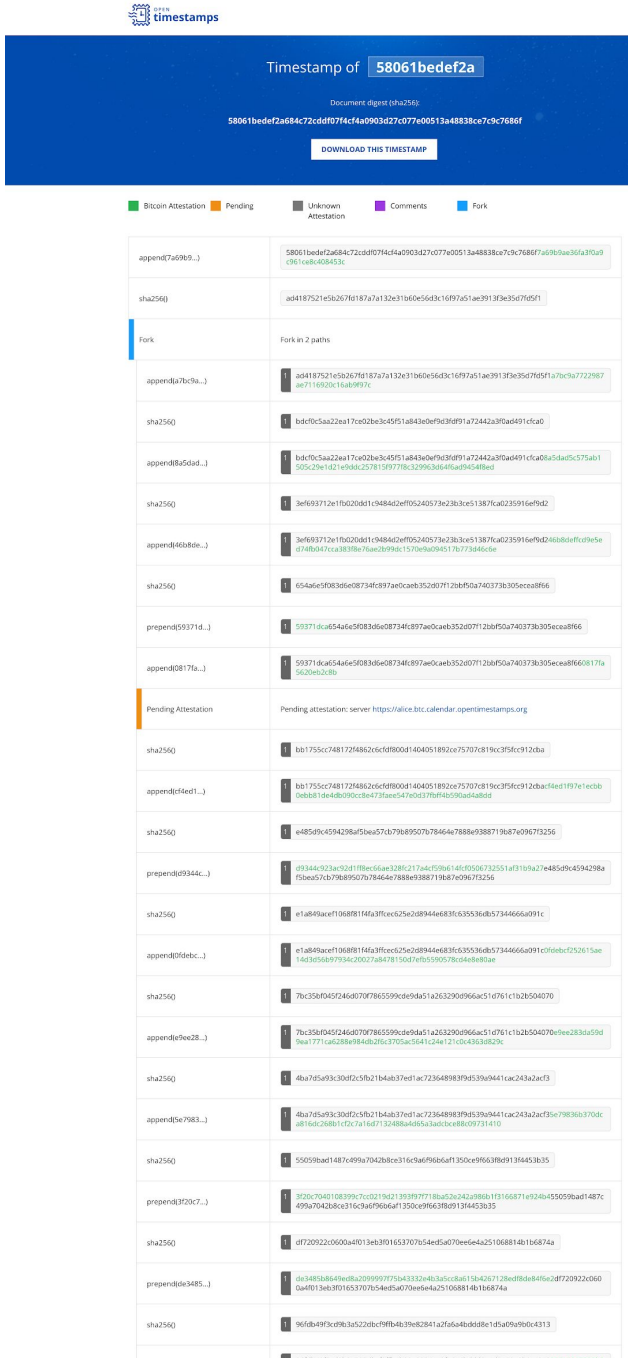
Tutto il software di OpenTimestamps è open source e già disponibile su github.

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!



Eternity Wall - https://eternitywall.com

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.

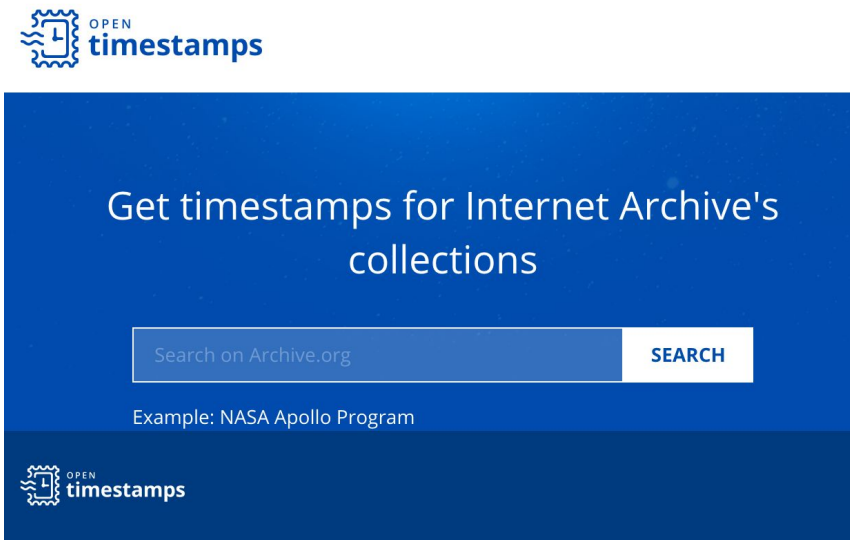
Svantaggi

- 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.



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

26-02-2018

Seccion	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

Seccion	PDF hash	Certificación	PDF	OTS
1	dd95bf584feb5a4ee269337de993621966b7e8e5a62440135c0d0cb073ce8e5c	23-02-2018 06:18:28		
2	49431926b8414921bef5851c731bafaafcd158d05cd277b1c92d174bdf3cb300	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

Eternity Wall - https://eternitywall.com

OTSProofBot

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

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

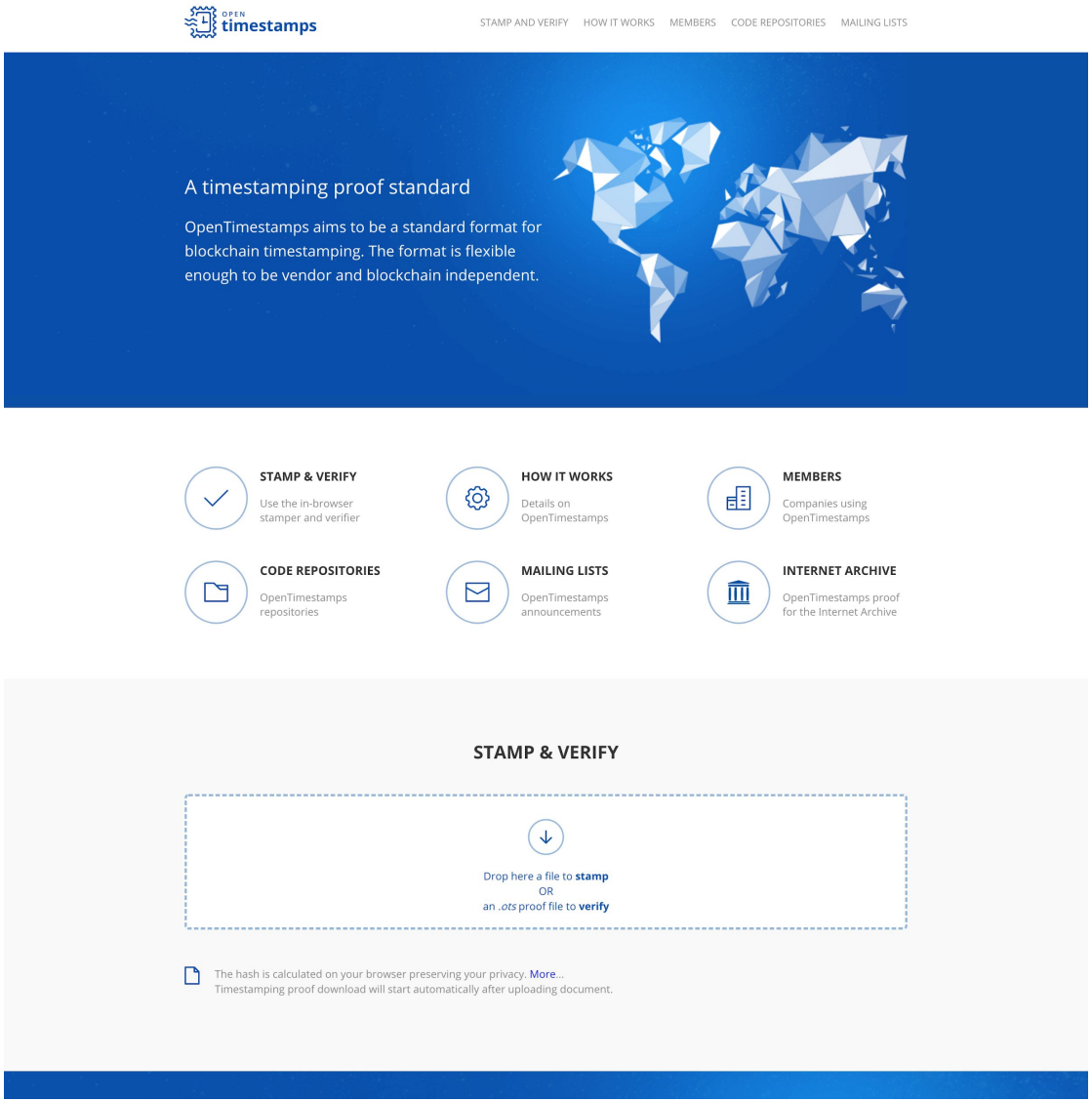
Agenda

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

Javascript lib stamp demo


```
$ 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
```

Verifica online



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/zt30

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 | valerio@eternitywall.com

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