



Eternity Wall

Riccardo Casatta e Valerio Vaccaro

Casi d'uso a confronto: blockchain pubblica o privata?

27 Febbraio 2018

In collaborazione con:



Media Partner



Agenda

- Chi siamo e cosa facciamo
- Blockchain pubblica o privata?
- OpenTimestamps
- 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.etsnitywall.it

Ma come sfruttare queste competenze in ambito business?

Nascita protocollo **OpenTimestamps**

<https://opentimestamps.org>



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



10 giugno 2017 4:43 GMT
Today is my birthday! -- Efe :)

11 giugno 2017 16:04 GMT
test

11 giugno 2017 8:04 GMT
Enri & Andre si sono amati

10 giugno 2017 11:04 GMT
NA-AT FAD Tech Alfredo

10 giugno 2017 8:36 GMT
NA-AT FAD Tech

8 giugno 2017 14:46 GMT
Li! theal What's in?



Eternity Wall 12 gennaio 2016 14:28

Signed messages are now public!



HostFat 13 gennaio 2016 2:02

Look at my tentacles!

6 giugno 2017 8:00



Giacomo Zucco 14 gennaio 2016 18:59

A lot of anon love messages, here's the FIRST signed one! LOVE YOU MIR!





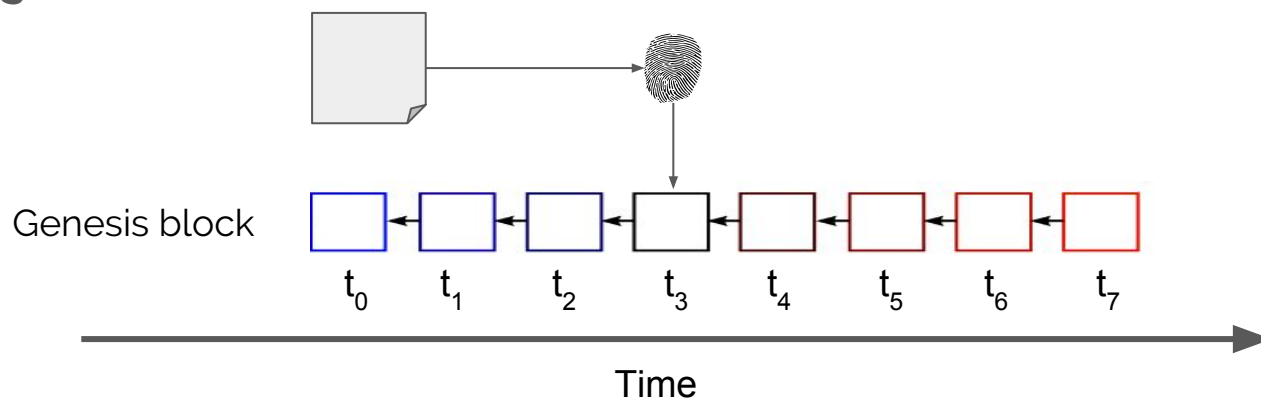
Timestamping

Il timestamping, o marcatura temporale, attribuisce una data certa ad un documento, il codice civile richiede sia presente su alcuni documenti pena la nullità:

es. il timbro dell'ufficio postale, la data apposta dal notaio su un rogito, ...

Per i documenti digitali:

- soluzioni basate su terze parti fidate, firma digitale + chain of authorities
es. PEC
- **soluzioni trustless**
es. OpenTimestamps



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

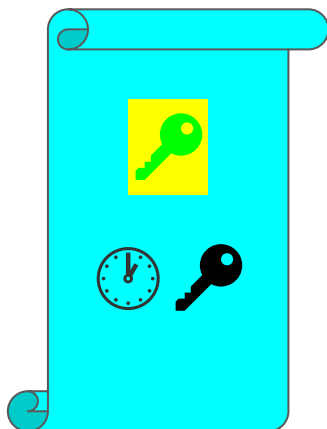
Nel modello basato su terze parti, cosa succede se una chiave viene compromessa?

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

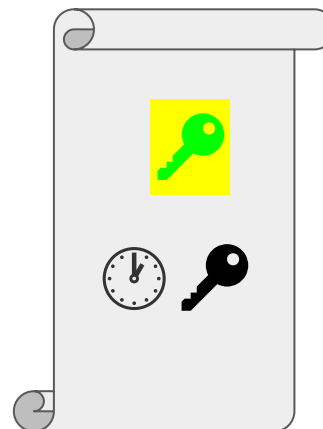
Errato

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

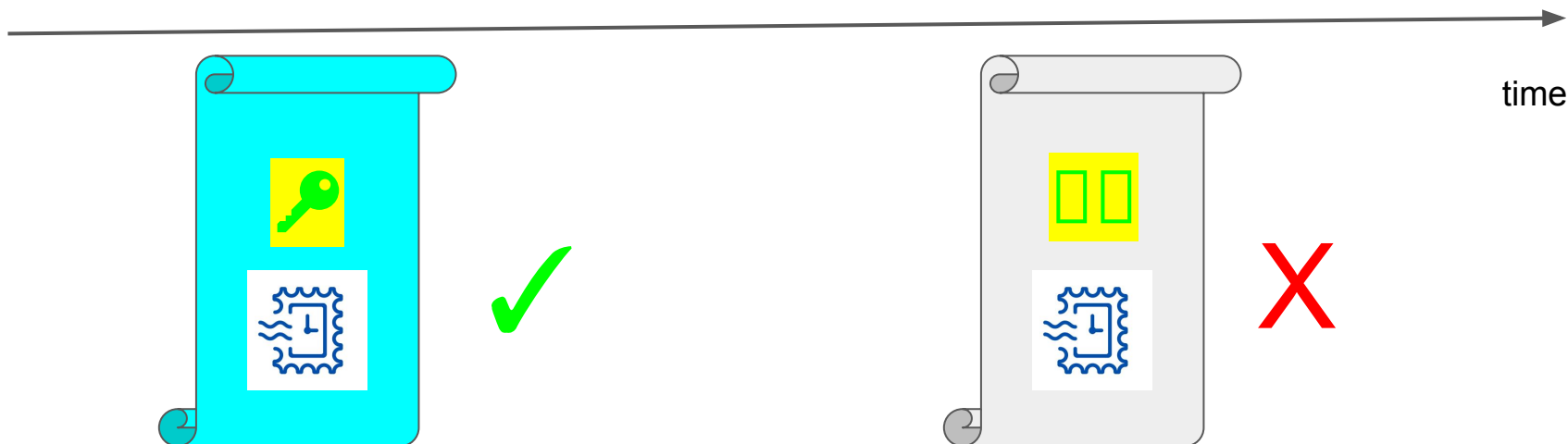


X



X

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.

OpenTimestamps

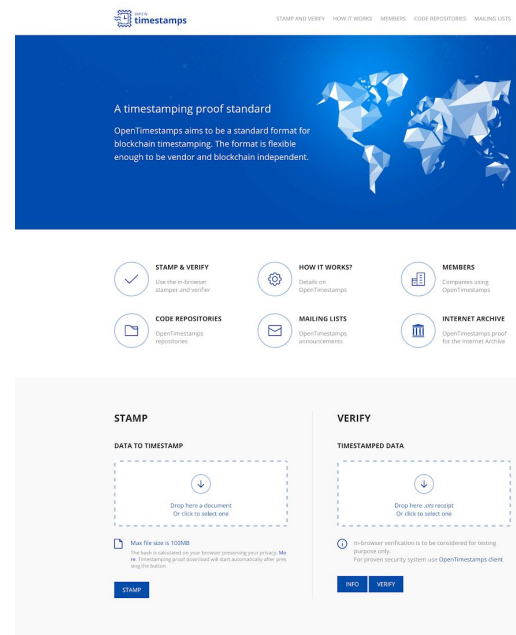
OpenTimestamps è un protocollo standard per la notarizzazione di qualsiasi informazione digitale con le seguenti caratteristiche:

- **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.

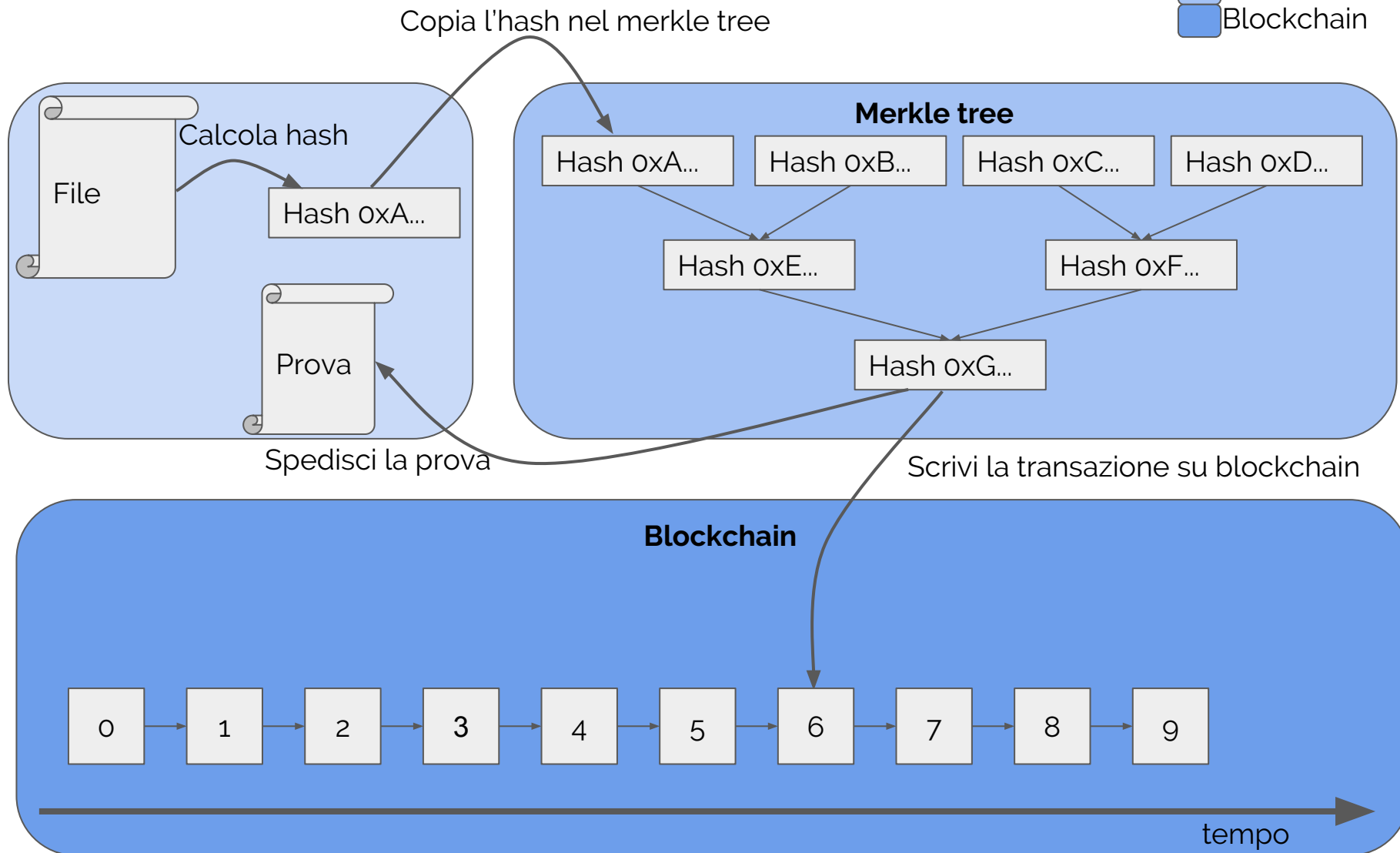
<https://opentimestamps.org>



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



OpenTimestamps



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**

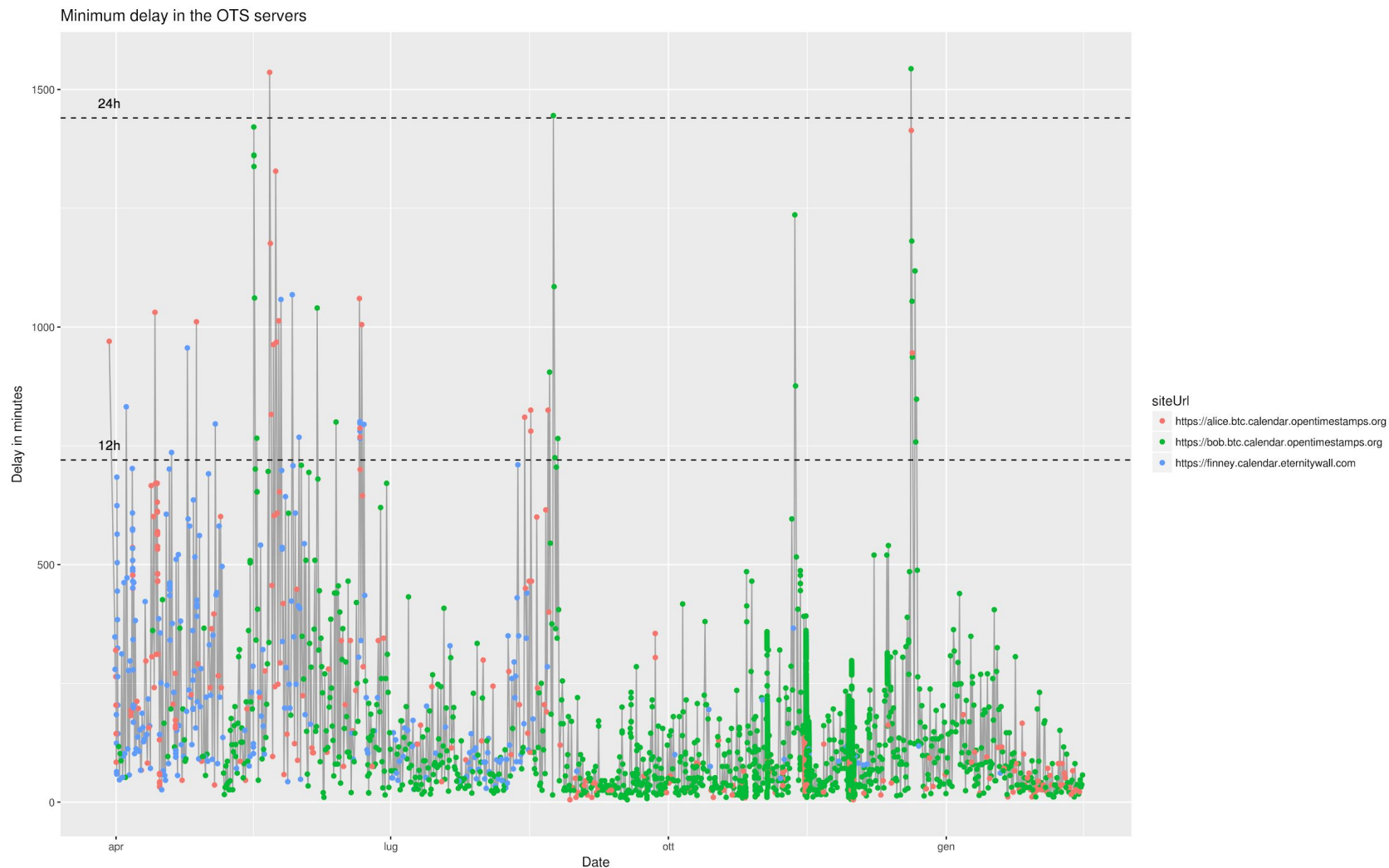
Un timestamp sicuro consente di distinguere i documenti firmati oltre un certo evento (es. furto della chiave, compromissione dei server, ...), i miei documenti sono stati firmati prima che mi venisse rubata la chiave?

- **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>



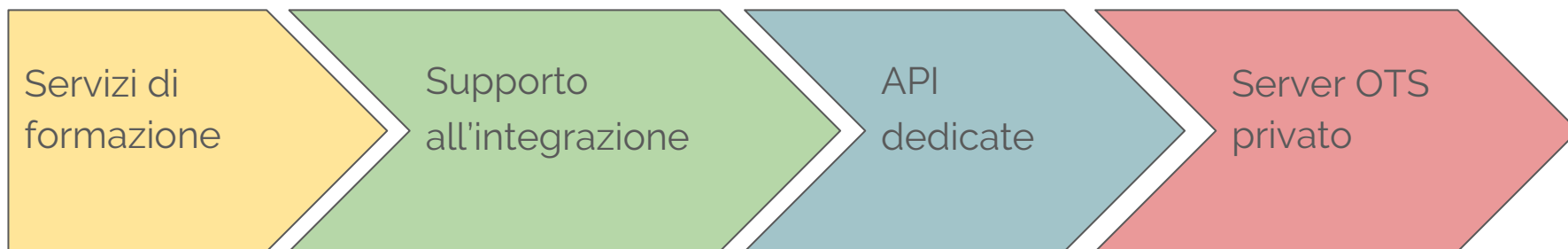
Timestamp of **58061bedef2a**

Document digest (sha256):
58061bedef2a684c72cd0f074c4a0903d27c077e00513a48838ce7c9c7686f

[DOWNLOAD THIS TIMESTAMP](#)

Bitcoin Attestation	Pending
Unknown Attestation	Comments
Fork	
append(7a69b...)	58061bedef2a684c72cd0f074c4a0903d27c077e00513a48838ce7c9c7686f2a69b395d9c961ced408453c
sha256()	ad4187521e5b2676187a7a132e31b6e56d3c16f97a51ae3913f3e35d7d5f1a7b3a7722987ae7116920c16ab997c
Fork	Fork in 2 paths
append(a7bc9a...)	ad4187521e5b2676187a7a132e31b6e56d3c16f97a51ae3913f3e35d7d5f1a7b3a7722987ae7116920c16ab997c
sha256()	bdcf0c5aa22ea17ce02be3c45f1a843e9f93f9f1a72442a3f0ad491cfca0
append(B845da...)	bdcf0c5aa22ea17ce02be3c45f1a843e9f93f9f1a72442a3f0ad491cfca05da5c575ab1905c29e1d21e9d4c257815f9778b3299c3a64f9a9448ed
sha256()	3ef93712e1f020d81c94842ef0540573c236c3e1387fca0235916ef9d2
append(d6bde...)	3ef93712e1f020d81c94842ef0540573c236c3e1387fca0235916ef9d26bdeff0f9e5e748b047cca3838e76a2b994c1570eb9a517b773446c6e
sha256()	654a6e5f083d6e08734c897a0c0eb352077128b95a740373b305ceea8f66
prepend(9371d...)	59371dca654a6e5f083d6e08734c897a0c0eb352077128b95a740373b305ceea8f66
append(d817fa...)	59371dca654a6e5f083d6e08734c897a0c0eb352077128b95a740373b305ceea8f6617fa5a20eb20b
Pending Attestation	Pending attestation: server https://alice.bit.calendar.opentimestamps.org
sha256()	bb7755c748172f4862c6cfd800d1404051892ce75707b318cc3f5fc912c0a
append(f4ed1...)	bb7755c748172f4862c6cfd800d1404051892ce75707b318cc3f5fc912c0a4ed1f97e1ecb6c0eb819e4b0805c0e170a5c1f001709a205a0a86d
sha256()	e485d9c494294296a51eaa57d79b9507b79464e7888e9388719a7e096773256
prepend(d9344c...)	d9344c923a02d1f8ec66a328c217a4c750614c49026732551a31b9a27e485d9c494296a750a57d2b79b9507b79464e7888e9388719a7e096773256
sha256()	e1a849acef100881f4fa3f0cc25a2d8944e683f535536db5734466a091c
append(d0feb...)	e1a849acef100881f4fa3f0cc25a2d8944e683f535536db5734466a091c0feb2c52b15ae1ad3f5969793420027ab78150d7e5590578a04eb8ae
sha256()	7bc3d8f045f246d0707865599cde9da51a263290a96ac51d761c1b28504070e283a5d9d7ea1771ca28b9894db2f6c3705a5641c24e121c04363a029c
append(bee28...)	7bc3d8f045f246d0707865599cde9da51a263290a96ac51d761c1b28504070e283a5d9d7ea1771ca28b9894db2f6c3705a5641c24e121c04363a029c
sha256()	4ba785a3c30df25b21b4b37ed1ac7236489839d539a441cac243acdf3
append(9c7983...)	4ba785a3c30df25b21b4b37ed1ac7236489839d539a441cac243acdf39c79830d370dcad16dc26b81cd7ca16d7132488a465a3ac3cc8b809731410
sha256()	55059baed1487c499a7042b0ce31c6f96baf1350c9963f80913f4453b35
prepend(d320c7...)	920c704d1083997c0d11a21393997718a0a3c42a288a1f3166871e934a55059baed1487c499a7042b0ce31c6f96baf1350c9963f80913f4453b35
sha256()	d7220922c060a4013e3b0165370754ed5a070ee64a251068814b1b6874a
prepend(d0a385...)	9c3d8f045f246d0707865599cde9da51a263290a96ac51d761c1b28504070e283a5d9d7ea1771ca28b9894db2f6c3705a5641c24e121c04363a029c
sha256()	966db49fc9863a522b0c79fb4b39e028a7a2fafa4b4b8b1d5a09a9e0d0313

Business model



Lezioni

Corsi specifici

Sviluppo

Integrazione

Personalizzazione

API HTTP

Autenticazione

Assistenza

Servizi aggiuntivi

Installazione

Aggiornamento

Manutenzione



Casi d'uso



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

SEARCH

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>



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

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 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	6967b0c6e30496e4e81551b5e7708920d625be495bf044cd08866897bea836c	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.

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 ⚡ ㄣ(ツ)ㄣ
@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



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>



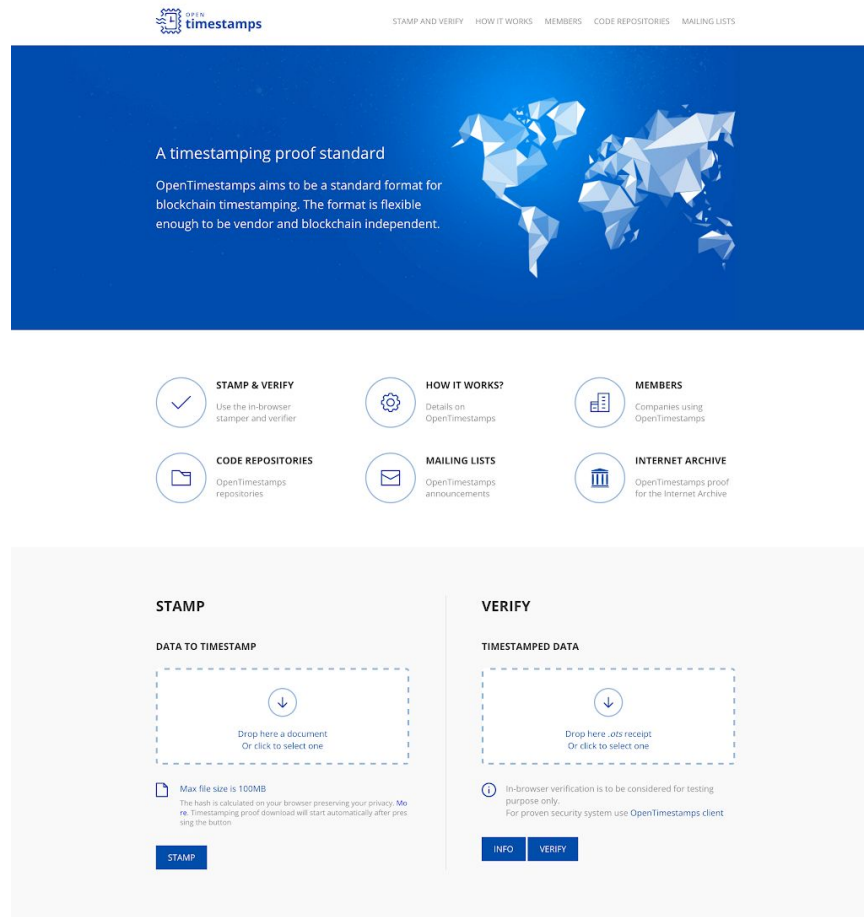
Eternity Wall - <https://eternitywall.com>



Demo



Verifica online



The screenshot shows the OpenTimestamps website. At the top, there is a navigation bar with the logo and links: STAMP AND VERIFY, HOW IT WORKS, MEMBERS, CODE REPOSITORIES, and MAILING LISTS. The main header area has a blue background with a world map and the text: "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." Below this is a grid of six icons with labels: STAMP & VERIFY (checkmark), HOW IT WORKS? (gear), MEMBERS (people), CODE REPOSITORIES (folder), MAILING LISTS (envelope), and INTERNET ARCHIVE (archive). The bottom section is divided into two columns: STAMP and VERIFY. The STAMP column has a "DATA TO TIMESTAMP" section with a dashed box for dropping a document, a "Max file size is 100MB" note, and a "STAMP" button. The VERIFY column has a "TIMESTAMPED DATA" section with a dashed box for dropping a .ots receipt, a note about in-browser verification, and "INFO" and "VERIFY" buttons.

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

DATA TO TIMESTAMP

Drop here a document
Or click to select one

Max file size is 100MB
The hash is calculated on your browser preserving your privacy. More: Timestamping proof download will start automatically after pressing the button.

STAMP

VERIFY

TIMESTAMPED DATA

Drop here .ots receipt
Or click to select one

In-browser verification is to be considered for testing purpose only.
For proven security system use OpenTimestamps client.

INFO **VERIFY**





Grazie

Riccardo Casatta & Valerio Vaccaro

riccardo@eternitywall.com | valerio@eternitywall.com

- Presentazione: <https://ew.link/g8b4>
- Marcatura temporale: <https://ew.link/ah62>

