

Cosa?

Bcademy ha perfezionato un **software di notarizzazione che permette l'inserimento di un codice univoco e deterministico** (hash generato elaborando un documento) **in una transazione sulla blockchain Bitcoin**, ergo consente di notarizzare sulla blockchain di Bitcoin un qualsiasi documento o archivio digitale (testo, audio, video, etc). In questo modo è possibile provare la data di inserimento (*timestamp*) e la corrispondenza di un documento con la versione depositata (in caso di modifica, il codice generato sarebbe diverso da quello depositato). **Questo prova l'esistenza (e il possesso in un dato momento) e l'immutabilità di un documento digitale, garantendone la non modificabilità a posteriori.**

In riferimento ad altre tecnologie che offrono servizi simili (Proof-of-Existence) Bnotary si distingue perché, basato su OpenTimestamps (OTS) sviluppato da Peter Todd, gode degli specifici vantaggi di questo approccio:

- **Fiducia:** Bnotary tramite OTS utilizza la blockchain di Bitcoin, decentralizzata e pubblica, eliminando il bisogno di parti terze fiduciarie;
- **Costi:** Bnotary tramite OTS è indefinitivamente scalabile, permettendo di creare timestamp liberamente e combinando un illimitato numero di timestamp all'interno di una transazione bitcoin;
- **Convenienza:** Bnotary tramite OTS può creare un timestamp come terza parte fiduciaria in meno di un secondo, non occorre attendere conferme sulla rete Bitcoin.

Perché?

La notarizzazione è l'atto o il processo di autenticazione notarile, la testimonianza dell'autenticità di un documento e delle sue firme accompagnatorie da parte di un notaio, ergo un ufficiale che può amministrare giuramenti e dichiarazioni statutarie, testimoniare e autenticare documenti. Con

l'avvento di sistemi come Bitcoin, è possibile creare e verificare prove dell'esistenza di documenti (timestamp o marca temporale, che potremmo tradurre con la perifrasi "timbrare con data e ora") **senza affidarsi ad una terza parte fidata, ergo riducendo i tempi e i costi dell'operazione.**

Dal punto di vista eminentemente legale, il valore delle registrazioni su blockchain è disciplinato dall'art. 8-ter del D.L. 135/2018, convertito con L. 12/2019, che si riferisce in generale a tutte le tecnologie basate su registri distribuiti. Secondo il dettato normativo la memorizzazione di un documento informatico attraverso l'uso di tali tecnologie produce gli effetti della validazione temporale elettronica di cui all'art. 41 Eidas, se fatta in conformità alle previsioni delle linee guida AgID (allo stato ancora da emanare).

Secondo l'interpretazione prevalente, il riferimento è alla validazione temporale semplice e non a quella (disciplinata nell'art. 42 Eidas) qualificata: si verificherebbe, in sintesi, un'inversione dell'onere della prova di cui all'art. 2697 c.c., ma resterebbe sempre ammessa, per i controinteressati, la possibilità di dimostrare la falsità della data. Sarà quindi la giurisprudenza a stabilire il grado di affidabilità probatoria delle diverse blockchain, **verosimilmente basandosi sul livello di hash rate.**

Le potenzialità giuridiche di questo servizio, tuttavia, sono ancora inesplorate: le caratteristiche della blockchain si prestano (oltre che alla memorizzazione di un certo documento) anche alla prova della sua trasmissione ad altri soggetti.

Dove?

Sulla blockchain, e posto che il grado di affidabilità probatoria delle diverse blockchain si giocherà sul livello di *hash rate*, **occorre ribadire che l'unica blockchain sicura è quella originale, la blockchain di Bitcoin.** Blockchain private non sono sicure per la loro stessa natura (i possessori possono sempre accordarsi per alterare i dati), mentre il livello di sicurezza di una blockchain pubblica e *permissionless* (ad assenza di permesso) è correlato al loro

hash power associata. L'hash rate, o hash power, è l'unità di misura di quanta potenza di calcolo ha bisogno una crittovaluta per mantenersi *funzionale*:

Hash rate denominations:

1 kH/s is 1.000 (one thousand) hashes per second;
1 MH/s is 1.000.000 (one million) hashes per second;
1 GH/s is 1.000.000.000 (one billion) hashes per second;
1 TH/s is 1.000.000.000.000 (one trillion) hashes per second;
1 PH/s is 1.000.000.000.000.000 (one quadrillion) hashes per second;
1 EH/s is 1.000.000.000.000.000.000 (one quintillion) hashes per second.

Ci sono volute 24 ore per accorgersi che il 5 gennaio 2019 la rete di Ethereum Classic (il genitore di Ethereum) ha subito un *attacco al 51%* (il che significa che un gruppo di persone ha aggregato una potenza di calcolo pari a più della metà di quella della rete ETC, alterando transazioni e sottraendo valore). La rete Ethereum (ETH) aggrega una potenza di calcolo 20 volte superiore alla rete di Ethereum Classic (ETC). Così, se un attacco al 51% su ETH non è impossibile, è sicuramente meno probabile. Da questo punto di vista, la rete Bitcoin aggrega una potenza di calcolo 4.500 volte superiore a quella di tutta la potenza aggregata per l'attacco del 5 gennaio. Questo, così come la governance realmente distribuita, è il motivo per cui attualmente **solo il network Bitcoin sembra idoneo a garantire l'immutabilità dei dati memorizzati**.

Nel dicembre 2017, durante l'ATH (All Time High, il picco del prezzo) l'hash rate di Bitcoin era di 15 *exahashes per second*, tre volte inferiore a quello odierno (marzo 2019), nonostante il prezzo sia calato di oltre l'80%, a garantire che l'investimento dietro Bitcoin, in termini di mantenimento in sicurezza della rete, è cresciuto indipendentemente dal calo momentaneo del prezzo.

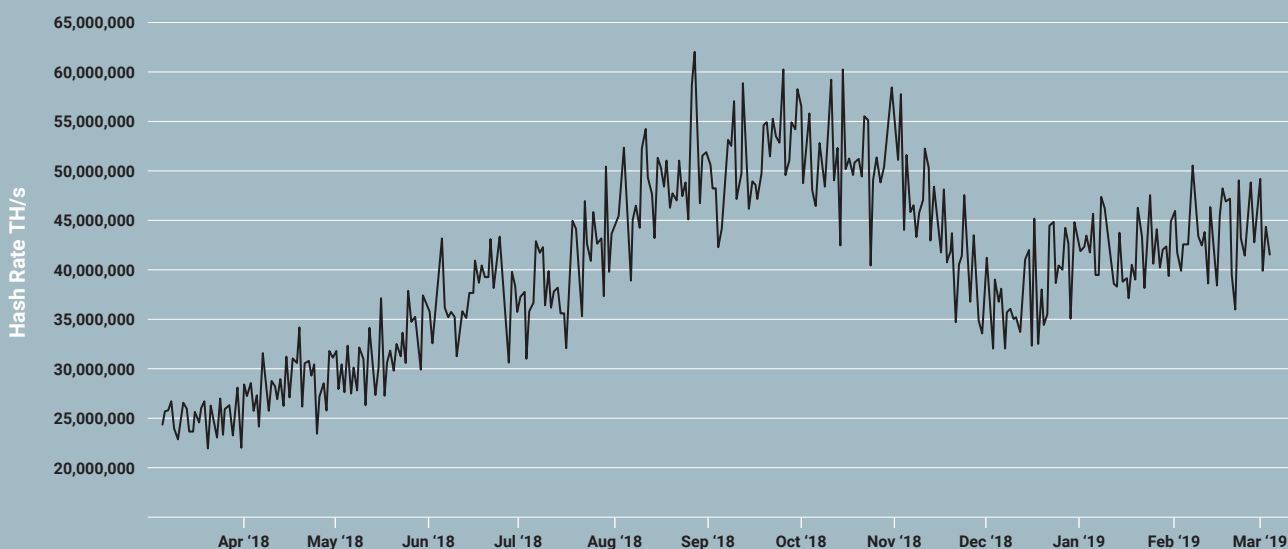
Chi?

Bnotary, a meno che non sia diversamente richiesto dall'acquirente, **si occupa di sostenere i costi bitcoin** delle transazioni necessarie a notarizzare gli archivi digitali, evitando al cliente/utente la necessità di utilizzare wallet e crittovalute. Allo stesso tempo **garantisce all'utente la massima privacy e autonomia nel caricamento e gestione dei dati e degli archivi digitali** (Bnotary non ha accesso al documento), nella certezza che una volta confermata la transazione, l'hash del documento è permanentemente depositato, la sua esistenza è provata e la sua integrità garantita (non modificabilità).

Occorre ribadire che **nel caso di integrazione con sistemi che implicino elementi reali**, come nella funzione di tracciamento e garanzia, **il sistema garantisce la non-mutabilità del dato inserito, non la sua verità**, ovvero il sistema notarizza il responso dell'oracolo (si immagini ad esempio il grado zuccherino in un dato momento all'interno di una determinata botte di vino in una cantina geolocalizzata).

All'interno della piattaforma online di Bnotary - bnotary. network - è prevista la possibilità non solo di notarizzare archivi digitali, ma anche di mantenere i propri file all'interno della piattaforma, di fatto archiviandoli. In maniera semplice, documento per documento, è possibile scegliere se notarizzare solamente, o se notarizzare ed archiviare nello spazio dedicato al proprio account. Mentre nel secondo caso una copia dell'archivio sarà presente all'interno dei nostri server, come ribadito in precedenza nel caso della semplice notarizzazione, Bnotary non ha in nessun caso accesso al documento.

The estimated number of tera hashes per second (trillions of hashes per second) the Bitcoin network is performing.



Quando?

Bnotary è stato rilasciato all'inizio del 2019, data di uscita della prima versione di questo documento (che fino a qui abbiamo voluto mantenere originale). Attualmente (ottobre 2021, immagini in calce), a 30 mesi dal rilascio, Bnotary è correttamente funzionante, il valore di un bitcoin ha superato i 65.000\$ e l'hash rate rispetto al 2019 è ancora una volta più che triplicato, segnale di una rete costantemente più solida e influenzata solo in minima parte dal valore di mercato dell'asset.

Bnotary è disponibile in quattro differenti *layer*.

- **Drag & Drop:** notarizzazione di un documento digitale dal portale Bnotary - bnotary.network - tramite semplice *drag & drop*, pagamento del singolo documento notarizzato (o acquisto di pacchetto di notarizzazioni), con certificato inerente le specifiche della notarizzazione (*hash* del documento e *.ots* per la marca temporale).
- **Software as a Service (SaaS):** fornitura delle rest-API del software, supporto nell'installazione e assistenza continuativa. Questo permette di: (I) notarizzare privatamente set di documenti digitali propri o di terzi; (II) offrire un servizio di notarizzazione (analogo al Layer 1, con pacchetti custom per i propri clienti); (III) agganciare il software ad altre soluzioni aziendali per notarizzare pacchetti di documenti o dati.

- **White Label:** cessione del sorgente del software, in licenza con *product key*. Il software è documentato, customizzabile, integrabile con altre soluzioni software aziendali. Questo comprende tutti i servizi dei Layer 1 e 2, così come di agire liberamente sul software per impiegarlo come parte di un sistema più ampio (ad esempio per notarizzare i documenti generati in itinere e rendere possibile l'ultimo miglio nel tracciamento all'interno di una filiera produttiva).
- **Supply Chain Tracker:** integrazione del software in un sistema-ambiente a diagramma di stati per il tracciamento di flussi. Questa soluzione può prevedere la *creazione di smart-contract in and/or off-chain* (come nel caso si volesse implementare un rimborso automatico in favore di un cliente a fronte di un particolare evento - quale il ritardo di un mezzo di trasporto), o in generale l'integrazione con *oracoli*, termine tecnico per indicare una determinata fonte di informazioni reale che viene digitalizzata e marcata temporalmente, come nel caso di tracciamento della filiera produttiva.

Il team di Bcademy rimane disponibile a proposte di collaborazione e/o eventuali customizzazioni del servizio.

Bcademy, 19.10.2021
bnotary.network

Total Hash Rate (TH/s)

The estimated number of terahashes per second the bitcoin network is performing in the last 24 hours.



Market Price (USD)

The average USD market price across major bitcoin exchanges.

