Blockchain Security, un paradigma multilayer

Author : Maria Letizia Perugini

Date : 11 Marzo 2019

> *Security technologies and products may be improving, but they're not improving quickly enough. We're forced to run the Red Queen's race, where it takes all the running you can do just to stay in one place. As a result, today computer security is at a crossroads. It's failing, regularly, and with increasingly serious results*[1].
> Bruce Schneier

È opinione comune che in ambito di *Computer Security* i problemi si dividano in due grandi categorie: quelli relativi a dispositivi e programmi e quelli che sono situati sopra la tastiera. I sistemi basati su blockchain non fanno eccezione alla regola: il modello prescelto deve essere sicuro sia sotto l'aspetto tecnico sia nell'uso che ne viene fatto dall'utente.

Generazione delle credenziali

L'educazione degli utenti è la prima tessera del puzzle. Per quanto possa apparire improbabile, a volte anche gli utenti esperti dimenticano le regole di base. È il caso, ad esempio, delle indagini condotte nel 2016 su alcuni venditori del *black-market AlphaBay*, un sito (chiuso dalle autorità nel 2017) dove merci illecite venivano scambiate per un controvalore in *bitcoin*. Uno dei *dealer* si era presentato con due diverse identità, AREA51 e DARKAPOLLO, attivate con protezione *PGP*. Per individuarlo, gli investigatori non sono dovuti ricorrere a tecniche di analisi della *blockchain* ma hanno potuto utilizzare la chiave pubblica *PGP*, che include l'indirizzo *mail* fornito dall'utente. Entrambi i profili facevano, infatti, riferimento a un indirizzo unico che era stato attivato con dati anagrafici reali [2].

Dove ho messo le chiavi?

Un tipico problema lato utente è, da sempre, quello della conservazione di *username*, *password* e *P.I.N.* I sistemi di *blockchain* sono messi in sicurezza crittografica ma la conservazione delle chiavi spetta agli utenti. Hal Finney conservava i *bitcoin* di cui aveva fatto *mining* in un *DVD* [3], riprodotto in copia di *back up* (e chiuso in cassaforte quando il loro valore è divenuto ingente).

Nel tempo si sono susseguiti diversi scandali relativi al furto di *bitcoin*. Già nel 2016, in occasione di un'intervista rilasciata a *Cointelegraph* su *chat Twitter*, Andreas Antonopulos ha cercato di sensibilizzare gli utenti alla gestione personale delle chiavi crittografiche, lanciando lo slogan "*your keys your bitcoins*" [4]. È un dato di fatto che questa soluzione non è praticabile da chi sia privo di conoscenze informatiche approfondite. In questo caso, la *second best option* applicabile è quella di scegliere un gestore di capacità e serietà riconosciute. Resta comunque ferma la necessità di gestire il portafoglio in sicurezza lato utente, attuando le misure necessarie a mantenere riservate credenziali e chiavi crittografiche. È fondamentale adottare un atteggiamento cauto, prestando attenzione alle trappole informatiche come *phishing*, *farming* e *free download* che contengono spesso anche del *malware*; ma bisogna anche tenere le macchine in condizione di sicurezza, adottando gli strumenti informatici idonei come *firewall* e *antivirus.*

Supporto tecnico e strumenti di sicurezza

La sicurezza di *hardware* e *software* sconta, anch'essa, un problema situato sopra la tastiera: la brutta abitudine di considerare l'informatica roba da smanettoni, con largo affidamento su fai da te e soluzioni *on the shelves.* È opportuno tenere sempre presente che l'informatica è un ramo applicato della matematica e che prodotti con costi sensibilmente differenti hanno, normalmente, una resa diversa. Quindi: **no** ai lavori affidati al figlio del cugino del vicino del lattaio ("cosa vuole signora, non ha mica mai studiato, ma con quelle robe lì è tanto bravo..."), **no** ai dispositivi usati in maniera impropria e **no** a soluzioni apparentemente vantaggiose ma mal progettate e messe in opera ancora peggio (quante volte abbiamo sentito frasi come "guardi, mi hanno detto che se uso un *NAS* al posto del *server* risparmio un bel po' di soldini...")

La "sicurezza della blockchain"

Ciò premesso, va necessariamente detto che parlare di "sicurezza della *blockchain*" in quanto tale, come purtroppo spesso si sente dire, non ha senso perché la *blockchain* è una struttura dati, cioè uno strumento di rappresentazione delle informazioni. Sarebbe come disquisire della "sicurezza dei numeri interi" o della "sicurezza delle liste concatenate". La *blockchain* in sé non garantisce né aumenta la sicurezza di un sistema o di una applicazione. La sicurezza è un attributo dei sistemi nel loro complesso e, in informatica, viene rapportata al paradigma *C.I.A.*: *Confidenzialità*, *Integrità* e *Disponibilità* (*Availability* in inglese). La *blockchain* è una struttura dati che in presenza di determinate condizioni (come accade ad esempio in *Bitcoin*, il modello di riferimento di molti sistemi) garantisce la certificazione del dato in essa conservato: pertanto la sua funzione c.d. notarile (cioè di rendere notorio e certo un fatto) la esenta dal vincolo di *Confidenzialità*; saranno eventualmente i sistemi che la usano a dover prevedere delle funzioni di controllo degli accessi ai dati ivi conservati, implementando la *Confidenzialità* a livello esterno. Anche l'*Integrità* è una proprietà che deve essere garantita attraverso specifiche di implementazione: nel caso *Bitcoin*, di cui stiamo facendo esempio, questo avviene subordinando la validità degli *hash* dei blocchi all'avveramento di determinate condizioni. Infine, la *Disponibilità* è una proprietà che sancisce che il dato debba essere consultabile quando necessario, quindi è una proprietà dinamica che richiede di garantire la raggiungibilità

dello stesso tramite ridondanze e copie di riserva (nel caso di *Bitcoin* è ottenuta con la replica della catena in tutti i *full nodes*).

Turing completeness e velocità di sistema

Quindi, per i sistemi basati su *blockchain* le questioni di sicurezza da prendere in considerazione sono più di una. Bitcoin, ad esempio, è stato volutamente disegnato con un linguaggio di programmazione *non Turing complete*. Questo significa che molte funzioni, come lo *smart contracting*, non sono sviluppabili direttamente su questa piattaforma, ma significa anche che la sicurezza del sistema rispetto ad attacchi che si prefiggano di sfruttarne la programmazione interna è maggiore. Per dirla con Bruce Schneier, è la complessità che rende il sistema vulnerabile [5]. Nei sistemi di *blockchain* anche la velocità di esecuzione delle operazioni complica la questione della sicurezza in maniera direttamente proporzionale. Infatti, più aumenta questa velocità più diventa probabile che i nodi lavorino ognuno sulla propria copia del registro, aprendo la porta a una serie di *fork* che possono facilitare l'azione a eventuali *double spender*. Il problema viene risolto alla radice da molti sistemi introducendo l'irreversibilità delle transazioni, che impedisce di utilizzare nuovamente somme già trasferite in precedenza.

Attacco ai nodi

Nei sistemi pubblici, ogni *full node* gestisce in maniera autonoma una copia del registro delle transazioni che resterà dunque al sicuro anche in caso di attacco a singoli *end point*. Ai fini di una valutazione di affidabilità del sistema, risulta così molto importante il numero dei nodi operativi che è direttamente proporzionale alla stabilità del sistema medesimo. Infatti, non tutti i nodi lavorano all'unisono, come nel caso di progetti nati da fork in cui i *miners* si dedicano selettivamente all'attività che in quel momento risulta maggiormente redditizia.

Nel caso delle *mining pool,* diviene fondamentale il tipo di architettura adottato, che deve consentire la convergenza degli sforzi di calcolo di macchine autonome e indipendenti fra loro. L'*Integrità* dei dati dipende, qui, anche dalla sicurezza dei protocolli di calcolo distribuito implementati.

Nei sistemi privati, o a gestione ristretta, la sicurezza dipende anche dal grado di indipendenza dei nodi. Le credenziali di accesso vengono qui autorizzate a livello centrale. In questo caso ha rilevanza anche il sistema di autenticazione che non deve concedere privilegi amministrativi *passe-partout* né consentire l'accesso indiscriminato a *superuser* la cui attività sfuggirebbe, così, a ogni controllo.

Gli esempi che precedono sono riconducibili a minacce all'integrità delle informazioni rappresentate. Peraltro, negli attacchi a gruppi di nodi, l'alterazione della maggioranza di potenza computazionale potrebbe essere finalizzata non solo alla manipolazione della struttura dati, ma anche al blocco del sistema, facendone venire meno la *Disponibilità*.

Tracciabilità delle transazioni

La tracciabilità delle transazioni, infine, costituisce una sensibilità assolutamente personale degli utenti. Bisogna comunque ricordare che nei sistemi pubblici il registro delle transazioni è liberamente consultabile. Ci sono casi in cui la *privacy* assume connotazioni particolari, come nel caso dei *trial* clinici, dove diventa fondamentale occultare l'identità dei pazienti che partecipano alla sperimentazione. Per questo genere di esigenze si rivelano particolarmente utili i sistemi basati su algoritmi che agiscono da *tumbler*, aggregando gli utenti in gruppi e impedendo di rintracciare l'effettiva provenienza della transazione. Nel caso si tratti di operazioni economiche, bisogna sempre tenere in conto che le transazioni in entrata saranno comunque dirette a un indirizzo specifico e che per mantenere questo indirizzo anonimo bisogna che esso sia stato creato allo scopo e utilizzato solo in maniera oscurata. Come evidenziato da Husam Basil Al Jawaheri [6], esiste infatti la possibilità di mettere in relazione alcuni degli indirizzi *Bitcoin* utilizzati in *TOR* con identità e indirizzi pubblicati su varie pagine in chiaro, correlandoli poi a transazioni e *wallet*.

Ancora una volta, un problema di sicurezza situato sopra la tastiera…

Note

[1] Bruce Schneier, *Secrets and Lies*: *Digital Security in a Networked World, 15th Anniversary Edition*, 2015, ed. John Wiley & Sons, Inc., ISBN: 9781119092438.

[2] Paolo Dal Checco, *Arresti nel dark web grazie (anche) alle chiavi PGP*, 2016: "Durante la generazione della chiave pubblica, per comodità dell'utilizzatore più che altro, viene richiesto l'indirizzo email al quale tale chiave sarà associata e tale indirizzo email verrà inserito all'interno della chiave pubblica PGP, quindi pubblicamente visibile da chiunque abbia la chiave. [...] La "leggerezza" dei due venditori di AlphaBay AREA51 e DARKAPOLLO e? stata quella di inserire nella loro chiave pubblica l'indirizzo di posta elettronica, Adashc31@g___l.com, che ha permesso agli investigatori di risalire ai loro profili Facebook, Twitter e Instagram anche tramite l'utilizzo del nick "Adashc31". Ci e? voluto poco, quindi, a richiedere a Facebook i dati di registrazione e accesso al profilo e scoprire che i due venditori erano in realtà la stessa persona residente a Brooklyn, New York", http://www.bitcoinforensics.it/2016/08/arresti-dark-web-chiave-pgp/.

[3] Hal Finney, *Bitcoin and me* (Hal Finney), 2013, https://bitcointalk.org/index.php?topic=155054.0.

[4] Olusegun Ogundeji, Antonopoulos: *Your Keys, Your Bitcoin. Not Your Keys, Not Your Bitcoin*, 2016: *"My primary goal is to ensure that none of the simple users who just need to exchange currencies are using custodial exchanges and leaving money there," Andreas Antonopoulos says in a Twitter chat with Cointelegraph. "It is risky, it is unnecessary and they are the least aware or capable of understanding and managing that risk. Hence the slogan: your keys, your Bitcoin. Not your keys, not your Bitcoin*", https://cointelegraph.com/news/antonopoulos-your-keys-your-bitcoin-not-your-keys-not-your-bitcoin.

[5] Bruce Schneier, *Secrets and Lies*: Digital Security in a Networked World, 15th Anniversary Edition, 2015, ed. John Wiley & Sons, Inc., ISBN: 9781119092438: "*Complex systems are inherently more vulnerable than simple ones, and the Internet is the most complex machine mankind has ever built. It's simply easier to attack our modern computer systems than it is to defend them, and this is likely to remain true for the foreseeable future. It's not that defense is futile, it's that attack has the upper hand*".

[6] Husam Basil Al Jawaheri, *Deanonimizing TOR hidden service users through bitcoin transaction analysis*, 2018, https://qspace.qu.edu.qa/handle/10576/5797.

Bibliografia

- Schneier Bruce, *Secrets and Lies: Digital Security in a Networked World, 15th Anniversary Edition*, 2015, ed. John Wiley & Sons, Inc., ISBN: 9781119092438.
- Dal Checco Paolo, Arresti nel dark web grazie (anche) alle chiavi PGP, 2016, http://www.bitcoinforensics.it/2016/08/arresti-dark-web-chiave-pgp/.
- Finney Harold, *Bitcoin and me* (Hal Finney), 2013, https://bitcointalk.org/index.php?topic=155054.0.
- Ogundeji Olusegun, Antonopoulos Andreas: *Your Keys, Your Bitcoin. Not Your Keys, Not Your Bitcoin*, 2016, https://cointelegraph.com/news/antonopoulos-your-keys-your-bitcoin-not-your-keys-not-your-bitcoin.
- Al Jawaheri Husam Basil, *Deanonimizing TOR hidden service users through bitcoin transaction analysis*, 2018, https://qspace.qu.edu.qa/handle/10576/5797.

Articolo a cura di **Maria Letizia Perugini** e **Marco Carlo Spada**