La sicurezza delle Blockchain e gli impatti sulla professione dell'IT Auditor

Author : Cristiano Paris

Date : 20 Marzo 2019

Dopo l'introduzione di Bitcoin nel 2006, le tecnologie legate alla **Blockchain** sono oggi impiegate in molti settori industriali diversi dagli strumenti di pagamento o di moneta elettronica. Peraltro, le implementazioni di applicazioni basate su Blockchain possono essere molto diversificate, sia rispetto ai suoi elementi costitutivi - come l'impiego di uno specifico algoritmo di consenso - sia per quanto concerne gli aspetti di contesto, come la struttura organizzativa in cui l'applicazione dovrà essere collocata. In un simile panorama, caratterizzato da un'estrema eterogeneità (oltre che da un'inerente immaturità delle soluzioni disponibili), si inseriscono tematiche orizzontali come la *governance*, gli aspetti normativi e regolamentari, la gestione dei rischi e la sicurezza delle informazioni.

Quest'ultimo aspetto appare senz'altro uno dei più critici per via della natura delle applicazioni sviluppate, che spesso presentano connessioni dirette con gli aspetti finanziari di un'organizzazione. Immaginiamo infatti il caso classico di un *token* gestito attraverso uno *smart contract*, sviluppato nell'ambito di una *Initial Coin Offer* (ICO) e rilasciato su una Blockchain pubblica come Ethereum. Qualora lo *smart contract* dovesse presentare delle **vulnerabilità**, l'effetto di un eventuale attacco potrebbe determinare impatti finanziari diretti, ad esempio tramite lo spostamento non autorizzato di *token* verso i conti dell'attaccante.

Un'eventualità tutt'altro che peregrina. In tal senso, il caso del cosiddetto **"DAO incident"** è in qualche modo paradigmatico degli effetti spesso drammatici che un problema di sicurezza può determinare in un simile contesto. In questo specifico incidente, una vulnerabilità nello *smart contract* su cui era basato il progetto *Distributed Autonomous Organization* (DAO) ha consentito a un attaccante esterno di sottrarre illecitamente ingenti somme dai fondi costituiti per il progetto, riuscendo a inserire, direttamente all'interno della Blockchain di Ethereum, transazioni fraudolente per centinaia di milioni di dollari.

In un simile scenario, i tempi a disposizione per una reazione efficace all'incidente sono compressi quasi fino ad annullarsi. Inoltre, le tipiche garanzie di forte integrità che caratterizzano la Blockchain possono rivelarsi controproducenti quando si tratta di correggere il

comportamento di uno *smart contract*, il quale, una volta rilasciato e inizializzato, è sostanzialmente immutabile, precludendo qualsiasi possibilità di *fixing* ex-post della vulnerabilità sfruttata dall'attaccante. Nel caso del DAO incident, tale dilemma è stato risolto in un modo unico e, ormai, irripetibile: attraverso un *hard-fork* del codice dei nodi Ethereum, lo stato dei conti dello *smart contract* del DAO è stato alterato per sterilizzare gli effetti dell'attacco. In un certo senso, **le attività di *patching* tipiche in una procedura di *incident management* in questo caso sono state applicate all'infrastruttura sottostante (la Blockchain)** anziché all'oggetto dell'attacco (lo *smart contract*).
Tale *modus operandi* viola in modo palese il principio di segregazione tra le componenti di un sistema informatico, intervenendo su un componente corretto per ripararne uno vulnerabile. Oltre ad essere del tutto insoddisfacente, come dicevamo, tale approccio risulterebbe oggi irripetibile. Infatti, applicare un *hard-fork* in una Blockchain pubblica come Ethereum equivale a convincere l'intera comunità dei *miner* ad applicare la relativa *patch* ai propri nodi. Il termine "convincere" è particolarmente appropriato, non esistendo alcuna leva, tecnologica od organizzativa, che possa imporre tale correzione a un *miner*. Nei fatti, l'applicazione di una procedura così estrema ed eterodossa ha determinato una spaccatura della comunità di Ethereum, conducendo alla creazione di una blockchain parallela nota come "Ethereum Classic". Le due fazioni, infatti, si sono polarizzate intorno a due diverse opinioni rispetto al principio noto come ***"code is law"***. In particolare la fazione più rigida sosteneva che, poiché il codice era pubblicamente disponibile agli utilizzatori dello *smart contract*, questi erano consapevoli dei possibili percorsi di esecuzione, inclusi quelli potenzialmente malevoli, e ne accettavano tutte le conseguenze. Gli *smart contract* infatti non sono ambigui, in quanto le modalità di esecuzione del codice sono note a priori e del tutto deterministiche.

Dal *DAO incident* scaturiscono **considerazioni** molto importanti:

- i processi tipici di gestione della sicurezza, come l'*incident management*, devono essere adattati e, a causa delle caratteristiche strutturali della Blockchain, il sistema dei controlli deve essere focalizzato nelle fasi di prevenzione e di rilevamento.
- La governance della Blockchain presenta problematiche specifiche a causa della totale decentralizzazione dell'algoritmo di consenso. Nelle blockchain pubbliche e non *permissioned*, in particolare, non esiste alcun controllo a livello accentrato che consenta di prevenire possibili situazioni di rischio per un'applicazione dovute a cambiamenti delle regole di funzionamento introdotti tramite *hard fork*. La comunità, in particolare, potrebbe spaccarsi ovvero la blockchain essere indotta al collasso.
- La dualità tra un accordo legale e il relativo *smart contract* che lo implementa (almeno in parte) potrebbe presentare rischi non facilmente identificabili in fase di progettazione dell'applicazione. Uno *smart contract* potrebbe infatti essere indotto in uno stato non previsto - o contrario - rispetto alle previsioni contrattuali dell'accordo legale.

Rispetto a queste considerazioni, possiamo cercare di capire **se e come cambia il lavoro dell'IT auditor** sotto il punto di vista dell'approccio metodologico e della cassetta degli attrezzi di cui dispone. In effetti, come peraltro abbiamo già accennato, possiamo considerare un'applicazione basata su Blockchain come un qualsiasi altro componente informatico che fa parte dell'universo di audit su cui l'auditor è chiamato a dare assurance. Tale applicazione sarà infatti composta da componenti IT che fanno tradizionalmente parte del bagaglio

esperienziale di un auditor: certamente avremo un'interfaccia di front-end (ad es. un'app per smartphone o un sito web), uno o più componenti di *middleware* (come ad es. un *message broker*) e un sistema di memorizzazione (il tipico database relazionale). L'applicazione sarà poi inserita in un contesto IT in cui saranno presenti altre componenti infrastrutturali comuni come un sistema di autenticazione, un accentratore di log, proxy di frontiera ecc.

Ecco che quindi l'assessment portato a termine dall'auditor per tali componenti IT non prevede peculiarità specifiche rispetto alle attività *business as usual*. Rimane quindi da comprendere **come affrontare l'analisi della componente "blockchain"**. Sebbene l'approccio di analisi della blockchain stessa si differenzi in modo sostanziale qualora ci si trovi in presenza di una blockchain pubblica o privata, da un punto di vista applicativo, le primitive esposte da questa componente tecnologica non risultano molto diverse da quelle di un normale sistema di memorizzazione tradizionale: attraverso l'uso di transazioni, dalla blockchain è possibile leggere (in modo sincrono) o modificare (in modo asincrono) lo stato di un *smart contract*. Se rimaniamo a questo livello di astrazione, possiamo senz'altro applicare tutti gli strumenti metodologici utilizzati dall'auditor per condurre il proprio assessment sotto i profili tipici di efficacia, efficienza e sicurezza. Risultano quindi utilizzabili, seppure con qualche adattamento, framework come COBIT, ISO, COSO, NIST, ITIL ecc.

Attraverso questi strumenti, in sede di audit, è possibile analizzare taluni **aspetti tipici di un'applicazione IT**:

- Quali controlli sono stati previsti per assicurare che l'applicazione rispetti tutti i requisiti normativi e regolamentari cogenti? Per le blockchain pubbliche, il tema della privacy appare particolarmente significativo, per via delle previsioni del GDPR. Nel caso di strumenti di pagamento, i requisiti della PSD2 vanno soddisfatti.
- Contratti e accordi. Com'è possibile tutelare l'organizzazione proprietaria dell'applicazione rispetto a eventuali scenari di rischio legale? Ad esempio, se un'applicazione gestisce quantità di tipo finanziario, in caso di abuso da parte di soggetti interni o esterni, come vengono gestite eventuali richieste di risarcimento?
- Processi IT. Come vengono gestiti aspetti del ciclo di vita tipici di un servizio informatico, come ad es. il *change management* o l'*incident handling*? In particolare, l'evoluzione di uno *smart contract* è senz'altro rilevante per via dell'immutabilità della Blockchain. L'auditor quindi dovrà capire quali controlli, prevalentemente di tipo tecnologico, consentono a uno *smart contract* di subire cambiamenti in modo controllato. Dalla prospettiva del forensics invece la situazione appare più rosea, in quanto l'intera storia delle transazioni di una blockchain è dispoinibile pubblicamente.
- IT General Controls. Come qualsiasi componente informatica, anche la blockchain deve essere protetta da scenari di rischio tipico, come l'accesso non autorizzato a quantità di sicurezza come le chiavi crittografiche.
- Costi e ritorni. Anche per la blockchain andranno valutati aspetti finanziari ed economici tipici, come i costi di progetto, il ritorno sull'investimento, il raggiungimento del *break-even*.
- Infine, andrà capito l'allineamento dell'applicazione della blockchain rispetto agli obiettivi di business dell'organizzazione.

Oltre a questi ausilii metodologici, l’auditor può disporre infine di strumenti che consentono di analizzare, in modo più o meno automatico, le applicazioni basate sulla blockchain per quanto riguarda aspetti più squisitamente tecnologici. Seppure in fase ancora embrionale, nella comunità delle blockchain cominciano ad apparire tool che consentono di effettuare veri e propri *vulnerability scanning* di *smart contract*. Un esempio molto importante è rappresentato dal progetto Mythril di ConsenSys per *smart contract* su rete Ethereum. Altri strumenti utili riguardano senz’altro lo sviluppo di checklist e compendi di *best practices* che consentono di guidare l’auditor nell’assessment di un'implementazione di uno smart contract - o di un’intera blockchain privata. Per il futuro assumeranno sicuramente un peso preponderante gli **strumenti di analisi formale degli *smart contract***, che consentiranno di fornire assurance sull’aderenza del codice sviluppato rispetto alle clausole contrattuali dell’accordo legale a esso associato.

In conclusione, si può senza dubbio affermare che l’avvento della Blockchain determinerà un cambiamento significativo nelle attività di IT audit sebbene, da un punto di visto strettamente metodologico, gli strumenti e gli approcci correntemente utilizzati dall’auditor risultino senz’altro ancora validi e pertinenti. Da un punto di vista tecnologico, i tool a disposizione sono ancora primitivi ma la direzione verso cui questi si stanno muovendo è senz’altro quella corretta. Certamente, la sfida più rilevante che attende la comunità degli IT auditor sarà quella di sviluppare un bagaglio di esperienze che consentirà di individuare e comprendere gli scenari di rischio tipici di un’applicazione basata sulla Blockchain.

Articolo a cura di **Cristiano Paris**