Non solo Bitcoin: la blockchain è utile anche per la cybersecurity

Utilizzata prevalentemente in ambito finanziario, la tecnologia di certificazione distribuita può trasformarsi in uno strumento che consente di blindare le comunicazioni e fare un salto di qualità verso il rispetto dei regolamenti europei (Fonte: https://www.wired.it/ 01.11.2025)

Viene immediatamente associata alle **criptovalute**, ma la tecnologia alla base di Bitcoin offre molto di più. I sistemi basati su **blockchain**, infatti, permettono di **certificare l'autenticità** di un dato con un'efficacia senza pari e si prestano ad applicazioni in molti campi "sensibili", come il voto elettronico e il controllo della filiera nel settore alimentare. Non stupisce, quindi, che qualcuno abbia deciso di usarla nel campo della cyber security.

Perché la blockchain è affidabile

Per comprendere il ruolo della blockchain in questo ambito, è necessario considerare il processo di verifica che utilizza. Ogni documento o comunicazione certificato tramite una blockchain viene infatti associato a un hash, cioè una sorta di "impronta digitale" del contenuto.

Quando quest'ultimo viene registrato nella blockchain, **una copia viene memorizzata da ogni nodo della "catena"**. Per verificare l'autenticità del contenuto che si è ricevuto, a questo punto, è sufficiente ricalcolare l'hash e confrontarlo con quello registrato.

La sicurezza del sistema è garantita dal fatto che, se qualcuno volesse alterare il dato, dovrebbe violare ogni singolo nodo della blockchain stessa e modificare l'hash registrato. Qualcosa che, se non impossibile, è per lo meno **molto improbabile**.

Per fare una metafora nel mondo scolastico, è come se la blockchain fosse un registro in cui vengono registrati i voti dei compiti in classe. Al posto di essere nelle mani del solo professore, però, il registro **viene dato in copia a tutti gli studenti**. Per alterare un voto, quindi, bisognerebbe intervenire su tutti i registri contemporaneamente.

L'applicazione nella cyber security

"Chi lavora con la sicurezza informatica ha bisogno di poter contare su informazioni certe e affidabili" spiega Riccardo Scalzi, Head of Offer Engineering di S3K in un'intervista a margine di Cybertech Europe 2025. "Per questo motivo abbiamo pensato di adottare blockchain per garantire la certificazione dell'autenticità delle comunicazioni, sia a livello di contenuto che di verifica della provenienza".

S3K opera nel settore della sicurezza informatica come fornitore di servizi gestiti, cioè mette a disposizione delle aziende strumenti come il Soc (Security Operation Center) che rappresentano il "cuore" dell'infrastruttura di security. Si tratta, in sostanza, di team formati da specialisti del settore che operano per **garantire la sicurezza di aziende ed enti pubblici** per individuare gli

attacchi informatici e contrastarli tempestivamente. Un ruolo particolarmente delicato, che richiede di mantenere alto il livello di attenzione.
Chi fornisce questo tipo di servizio, infatti, ha in mano "le chiavi" per gestire la sicurezza delle aziende e degli enti pubblici che protegge. Un'eventuale intrusione da parte di cyber criminali nel sistema, potrebbe avere conseguenze devastanti.
"Abbiamo deciso di sfruttare la blockchain per **garantire la massima affidabilità nelle comunicazioni** a questo livello" conferma Scalzi. "In questo modo abbiamo la certezza che tutte le informazioni che transitano all'interno della nostra piattaforma possano essere considerate sempre attendibili e verificabili".

La blockchain e le normative europee
Se l'implementazione della **blockchain** nelle comunicazioni tra i Soc e le organizzazioni che sfruttano il servizio è stato il primo passo, S3K ha deciso di espandere l'applicazione delle comunicazioni tramite blockchain ad altri ambiti.
Un primo progetto è stato quello di fornire questo sistema a Enac, l'Ente Nazionale per l'Aviazione Civile. Quello successivo, però, ha un respiro più ampio e guarda agli obblighi in ambito cyber security che derivano dai **regolamenti europei**.
Sia l'ormai ben noto **Gdpr** (Regolamento Generale per la Protezione dei Dati) che la **Nis2** (Network and Information Security) prevedono una serie di comunicazioni obbligatorie, per esempio nel caso di incidenti di sicurezza informatica, alle autorità competenti. In Italia sono il Garante per la privacy e l'Agenzia per la Cybersicurezza Nazionale.
"La legge non prevede una forma specifica per queste comunicazioni" sottolinea Scalzi. "Tuttavia, per la loro delicatezza sarebbe meglio utilizzare un sistema sicuro e affidabile, che garantisca a tutte le parti che **i contenuti sono autentici e il mittente verificato**". Insomma, nell'ottica di una comunicazione "ufficiale", la blockchain si trasforma in uno strumento di certificazione che permette di creare un canale estremamente sicuro e, dalle parti di S3C, sperano che un sistema del genere possa trasformarsi in uno standard.