Blockchain, applicazioni open source più efficienti ma anche meno sicure

Si dovrebbe fare di più per migliorare la protezione dei codici dei progetti ***software open source*** per la ***blockchain***. È quanto si legge in un nuovo studio pubblicato dal software vendor Cast, "***Software intelligence Report. Open source software projects***", in cui sono stati esaminati 61 progetti open source e quasi 9 milioni di linee di codice, tra cui quelli di MongoDB, Ethereum, BitcoinJ, Apache Struts, Kubernetes Helm e Microsoft Orleans.

"*La prevalenza di software open source nelle applicazioni aziendali evidenzia la necessità di una maggiore capacità di software intelligence per la prevenzione e la gestione di* ***attacchi hacker***", si legge nel documento.

"*L'open source è il 10% più efficace, ma il 7% meno efficiente delle applicazioni di software non libero o proprietario (closed source)*".

Un dato quest'ultimo da riferire ad un ritardo legato alle prestazioni del software open source e spesso a causa del codice open source della blockchain ("***open source blockchain code***"), secondo i ricercatori Cast.

Esaminando attentamente i codici BitcoinJ, Ethereum e Solidity, si nota che **le *app open source* per la *blockchain* risultano come detto più robuste, ma meno efficienti e non abbastanza sicure** ("*they are not secure or efficient enough*").

Il Rapporto sostiene inoltre che i progetti *blockchain* tendono

a violare le regole della "*changeability*", cioè quelle disposizioni che abilitano la capacità di trasformarsi e adattarsi a nuovi contesti, che potrebbero rappresentare una preoccupazione sul lungo periodo, poiché la tecnologia si diffonderà rapidamente nei prossimi anni e si moltiplicheranno i suoi utilizzi.

A livello mondiale il mercato della tecnologia e delle applicazioni blockchain potrebbe raggiungere il valore approssimativo di 2,3 miliardi di dollari nel 2021 secondo stime Statista.

Per quanto riguarda la conformità a livello di sistema, il codice *blockchain* ha raggiunto uno score del 98,5%, il che significa che sono state registrate 15 violazioni a livello di sistema su 1000 attività.

Più bassi i punteggi di conformità a livello di sistema per i codici relativi a *web & framework software*, rispettivamente al 93,7% e al 93,6%.

La *blockchain*, nonostante le sue enormi potenzialità tecnologiche ed economiche, dimostra ancora di avere diversi punti deboli, vere e proprie vulnerabilità, per quel che riguarda ad esempio i wallets di Bitcoin, Ethereum e Solidity sulla piattaforma Github: "*È davvero importante per le organizzazioni conoscere il livello di qualità del software open source che supporta le applicazioni aziendali*", ha affermato **Lev Lesokhin**, EVP of strategy and analytics presso Cast.

"*Questo perché le vulnerabilità software più evidenti nelle componenti open source possono essere facilmente sfruttate dai cyber criminali (exploitable by hackers)".*

Sul livello di vulnerabilità generale della blockchain, **Lex Sokolin**, direttore della strategia FinTech presso Autonomous Research LLP, ha ricordato su Wall Street Italia che in meno di dieci anni gli hacker son riusciti a rubare Bitcoin ed

Ether per un valore complessivo pari a 1,2 miliardi di dollari: “*Le attività criminali informatiche nel mercato delle criptovalute sono diventate un settore da 200 milioni di dollari di ricavi*“.

Tra un’altra decina di anni la tecnologia alla base di Bitcoin e delle altre criptovalute diventerà vulnerabile anche agli attacchi informatici sferrati da computer quantistici.

In conclusione, le blockchain possono in alcuni casi rivelarsi anche più vulnerabili di altri software: “*Ce ne sono migliaia e ognuna ha i suoi bug*”.

Finché il campo non si restringe a quelli più efficienti e preferiti dagli utenti, come è accaduto in passato con i browser, “*garantirne la sicurezza assoluta sarà complicato, ogni implementazione presenterà i suoi problemi*”.

> *Blockchain, applicazioni open source più efficienti ma anche meno sicure*