

Argomento: Università degli Studi di Perugia: Si parla di Noi

Un algoritmo svela lo schema Ponzi in Bitcoin

Un insieme di tecniche per andare a caccia di chi usa i bitcoin per compiere transazioni illegali. Sono quelle sviluppate all' **Università di Perugia** dal team di Stefano Bistarelli, Direttore del Nodo **UniPG** CINI Cyber Security National Lab. Qui i ricercatori hanno realizzato "Blockchainvis suite": un tool che ha lo scopo di superare i metodi di anonimizzazione usati per i bitcoin. L'idea è quella di studiare con i Big Data gli oltre 130 Gigabyte rinchiusi nella blockchain. «Una mole di informazioni che in realtà si traduce in Terabyte», spiega Bistarelli, perché possano essere davvero analizzati. La suite comprende uno strumento per controbattere i mixing services, ossia quei siti che mescolano gli indirizzi dei bitcoin rendendo difficile ricostruire il percorso delle transazioni. «Con tecniche di reverse engineering riusciamo invece in alcuni casi a ricostruire questi percorsi». Blockchainvis consente anche il clustering, ossia la possibilità di attribuire più indirizzi ad un unico utente che si è servito di diversi alias per nascondere la sua attività. Partendo da un database composto da oltre 115 milioni di indirizzi i ricercatori sono riusciti a clusterizzarne, ossia a connetterli in wallet, più del 76%. Attraverso tecniche di scraping, ossia analisi automatica del contenuto delle pagine web, i ricercatori riescono anche in alcuni casi a individuare autori unici di pagine sul deep web, associando i loro alias. Gli studiosi hanno anche creato un' applicazione internet, ancora in versione alpha, per visualizzare le transazioni sulla base ad esempio del valore o del periodo. Il progetto ha avuto finanziamenti sotto forma di Amazon AWS e da Microsoft Azure for research awards. All' **Università** di Cagliari, invece, il team di Massimo Bartoletti sta lavorando ad un tool per "l' analisi automatica degli schemi Ponzi su Bitcoin, basata su tecniche di machine learning", come spiega lui stesso. Lo schema Ponzi è una truffa nella quale gli investimenti sono ripagati soltanto con i fondi versati da nuovi utenti, con il risultato che gli ultimi arrivati perdono il proprio capitale perché il sistema non regge più. Continua Bartoletti: «Individuare automaticamente gli schemi Ponzi su Bitcoin è abbastanza



arduo», in quanto si ha a disposizione solamente «una sequenza di transazioni tra indirizzi Bitcoin. Inoltre, uno schema Ponzi può usare tanti indirizzi diversi per ricevere e inviare pagamenti, rendendo più difficile l'analisi». Tuttavia, i primi risultati si vedono già: «Al momento siamo in una fase avanzata di sperimentazione del tool, e dovremmo a breve inviare il lavoro in peer review». La possibilità di deanonimizzare le transazioni registrate sulla blockchain attraverso tecniche di machine learning è studiata anche da Adam Turner e Angela Maitland Irwin, del Dipartimento di Criminologia dell' **Università** Macquarie di Sydney. La loro conclusione, pubblicata sul "Journal of Financial Crime" è chiara: «attraverso tecniche euristiche e di analisi dei grafi» è possibile seguire il comportamento «degli indirizzi bitcoin e delle transazioni», attivando anche una serie di indicatori di allarme che rivelano le attività illecite. Anche secondo loro con il machine learning è possibile risalire lungo la blockchain per individuare le transazioni sospette. Un obiettivo importante per combattere il crimine e per rendere l' economia dei bitcoin uno strumento affidabile. © RIPRODUZIONE RISERVATA.