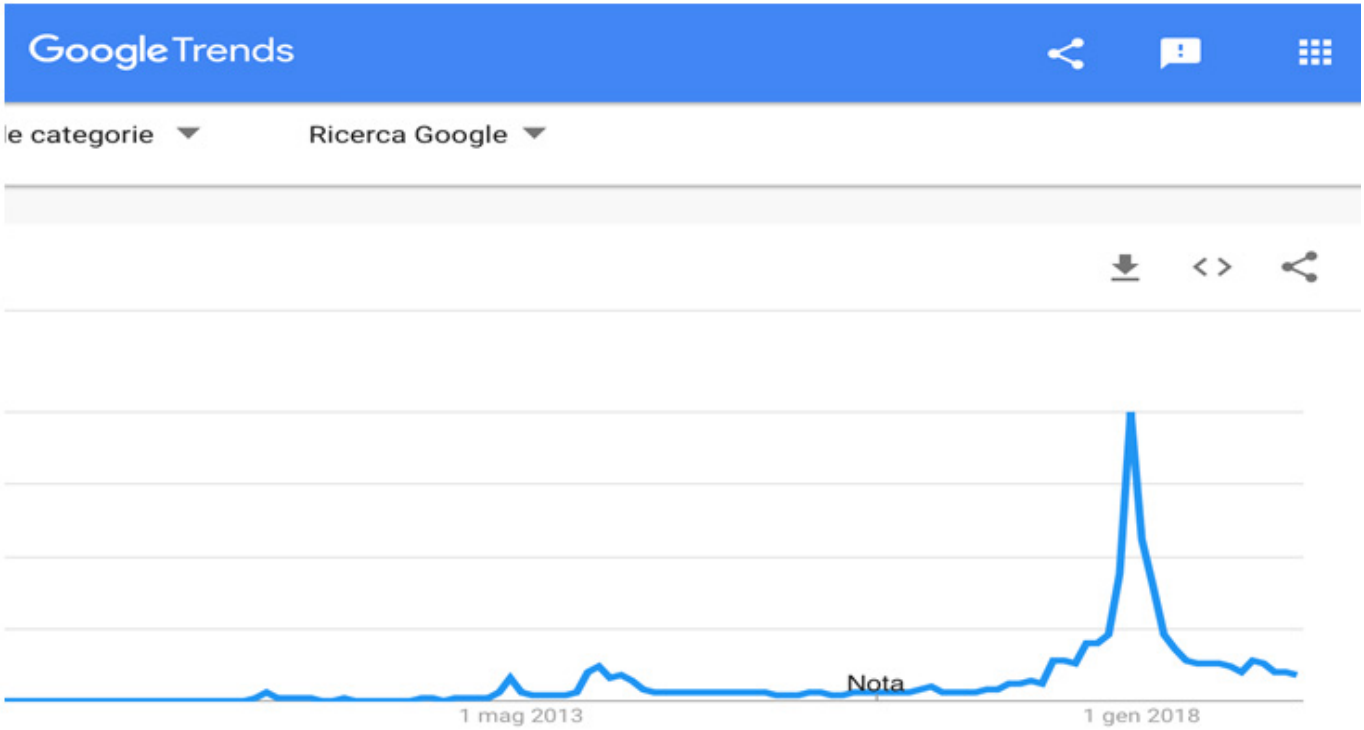
Cryptocurrency, Blockchain and Cyber Crime

Author : Redazione

Date : 6 Giugno 2019

Estratto dalla relazione di Stefano Bistarelli tenutasi al 10° Cyber Crime Conference 2019

Oggi non parlerò di Blockchain in termini di numeri: d’altronde, tutte le informazioni relative ai numeri si trovano facilmente in internet.
Parlerò essenzialmente di cyber security collegata alla Bitcoin Blockchain, un fenomeno disruptive di cui ormai tutti parlano - nel 2018 questo era il trend delle ricerche su internet dei termini Bitcoin blockchain - e che sicuramente dovremmo tutti affrontare nel corso del 2019. In realtà, avrei sperato che questo trend di ricerca fosse dovuto alla blockchain, la nuova tecnologia che dovremmo utilizzare; invece, come potete immaginare, il termine di ricerca usato più spesso era Bitcoin.



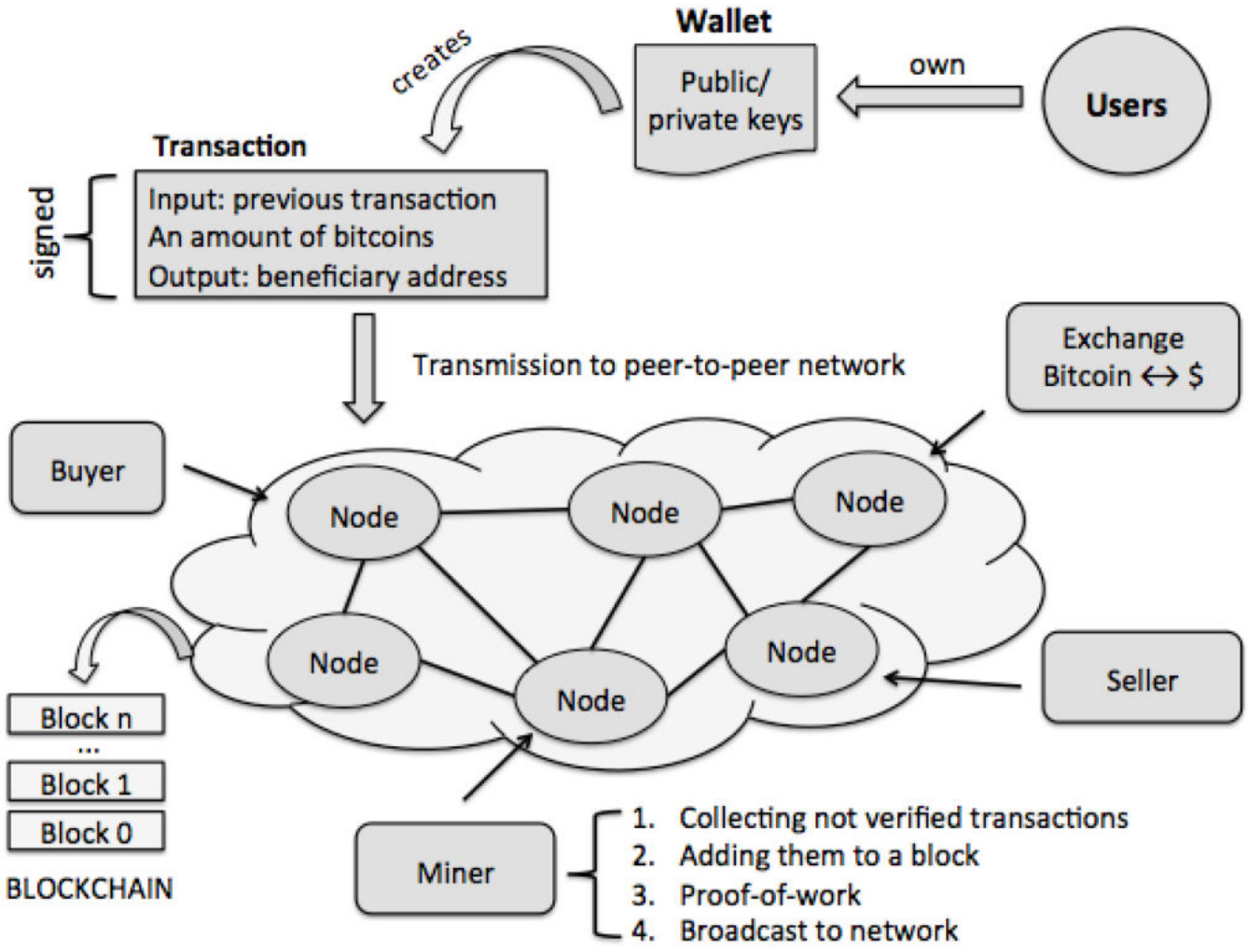
Sono due cose strettamente collegate; qualcuno dice che Bitcoin sia il motore della blockchain, altri che ne sia solo un'applicazione. Esistono vari punti di vista, ma quel che è certo è che l'interesse scaturito dal Bitcoin sia stato anche un punto di avvio per attività tecnologiche intorno alla blockchain. In realtà, si tratta di due realtà che dovremo affrontare in stretta correlazione: da una parte vediamo la blockchain come una tecnologia che può offrire innumerevoli benefici, un amico da proteggere, un friend; dall'altra parte, spesso si storce la bocca perché sono stati molti gli attacchi di tipo ransomware che hanno avuto pagamenti in Bitcoin e, così, qualcuno vede nel Bitcoin "un foe". Proveremo a considerare entrambe le sfaccettature: sia la parte di blockchain come "amico da proteggere" - esaminandone il funzionamento e le problematiche da affrontare - sia gli aspetti di sicurezza collegati ai ransomware e perché vedano il frequente utilizzo di Bitcoin come strumento di pagamento.

Cos'è questo Bitcoin? Se ne sente parlare tanto e, quando si parla di Blockchain, si deve inevitabilmente parlare di Bitcoin perché è la criptovaluta che, a partire dal 2009, ha diffuso questa tecnologia. Potrei usare molte parole difficili, parlare di "problema bizantino", CAP theorem, crittografia... ma non è la sede giusta: la scelta della pillola rossa o blu - chi conosce il film Matrix capirà il significato - oggi cade sulla pillola blu. Prima di parlare di aspetti tecnici, qualche aneddoto divertente a tema Bitcoin: una storiella che circola su Internet parla di uno studente norvegese che è diventato milionario perché nel 2009 si era divertito ad acquistare dei Bitcoin (che non valevano nulla) per poi ritrovarsi, nel 2013, con un portafoglio veramente consistente. Sarà vero? Penso di sì, perché una cosa del genere è successa anche a me: nel 2010 un mio studente, a cui avevo assegnato uno studio sui Bitcoin, in realtà ne aveva anche acquistati per conto suo. Qualche anno fa scrisse un'email per ringraziarmi: pensavo fosse perché gli avevo insegnato qualcosa, invece mi ringraziava perché a quel tempo aveva comprato dei Bitcoin ed era diventato milionario.

Chiunque abbia sentito parlare di Bitcoin conosce anche questo fantastico nome - Satoshi Nakamoto - collegato alla criptovaluta e sa che, nel 2008, è stato sviluppato (e diffuso in una mailing list crittografica) un documento che ne descrive il funzionamento.

Ma chi è questo Satoshi Nakamoto? Si tratta di un mistero che in tanti provano a risolvere. Qualcuno dice che sia Dorian Satoshi Nakamoto ma cosi' non è. Lui era così stanco di queste richieste da pubblicare un post in cui diceva "Non sono Satoshi Nakamoto, non chiedetemelo più". Qualcun altro ha pensato fosse un dipendente della NSA che lavora in ambiente crittografico; potrebbe essere, ma in realtà non è neanche lui. In ogni caso, chi sia in realtà è ancora un mistero e penso rimarrà tale per molto tempo.

Dopo questi aneddoti, passiamo agli aspetti più complessi dell'universo Bitcoin:



Tale universo è composto da nodi distribuiti che mantengono traccia delle transazioni digitali effettuate per trasferire cryptocurrencies, ovvero denaro virtuale. La transazione, quindi, è l'attore principale che dobbiamo considerare per capire quali siano le problematiche di questo ambiente distribuito.

Tutti noi compiamo transazioni nel mondo reale: ma in quel caso il trasferimento del bene – per

esempio del caffè - avviene contestualmente al pagamento del bene stesso. Questo garantisce sia il compratore che il venditore, garantendo un alto livello di fiducia; è difficile che il barista mi dia il caffè se io non gli do la moneta e io non gli do la moneta se non mi dà il caffè. Nel mondo digitale non è così: il trasferimento di denaro avviene in un momento separato rispetto al trasferimento del bene, specie se si tratta di un acquisto online.

Questa non è una problematica esclusiva del Bitcoin, ma riguarda ogni tipo di acquisto digitale. Se avvengono transazioni in momenti diversi del trasferimento del bene, sorge il primo dubbio: come posso fidarmi di un acquisto di questo tipo? Chi mi vieta di copiare, con un “magico” control C+control V, la mia moneta elettronica e spenderla un’altra volta? Questo è il principale problema che Satoshi Nakamoto ha dovuto risolvere nel documento citato. Sembrerebbe, infatti, possibile effettuare doppi acquisti: compro un caffè in un bar, poi spendo la stessa moneta (crittografica) in un altro bar. In realtà il protocollo prova a risolvere questo problema: quando Alice vuole fare una transazione verso il coniglio, invia questa transazione in broadcast a tutti i nodi di questa rete che appartengono al protocollo Bitcoin. E cosa fanno i nodi? Non si comportano come una banca che, quando avviene una transazione, la memorizza sul proprio database centralizzato: in questo la banca sarebbe stata la famosa “terza parte fidata” (Alice ha pagato Bob e ve lo dimostro con la transazione “scritta” nel database). Con Bitcoin le transazioni non sono mantenute da una terza parte fidata ma, in maniera distribuita, da tutti gli appartenenti alla rete. Questa è una grande garanzia: primo, non dovete fidarvi dell’unico attore che mantiene l’informazione; secondo, le informazioni sono replicate ed è difficile, per un utente, modificare la propria copia della transazione senza che gli altri se ne accorgano, così com’è facilmente verificabile se qualcuno prova a “barare”. Quindi siamo abbastanza sicuri che, se la transazione verrà inserita all’interno di uno di questi database distribuiti, esisterà una copia con cui dimostrare che quella transazione sia avvenuta.

Continua a leggere…

Scarica gratuitamente gli atti del 10° Cyber Crime Conference 2019