Susan Brown Slizys (USA, Art signature name) - Blockchain Universe

Bitcoin: la verità dopo 10 anni

di *Vincenzo Rampolla*

(seguito)

Dalla creazione nel 2009, c’è voluto un decennio per scoprire chi c'era dietro il Bitcoin.

Lo pseudonimo Satoshi Nakamoto non mi aveva mai convinto.

L'idea che il nome fosse uno pseudonimo stava in piedi, ma dubitavo dell'origine Giapponese, leggendo sul forum i numerosi post in inglese. C'è chi ha proposto la derivazione da un acronimo di nomi di società tecnologiche composto da Samsung, Toshiba, Nakayama e Motorola.

Ci sta, ma è banale e modesto, non degno di una persona del suo livello. E poi la sua memoria di poche pagine, bibbia delle criptovalute, opera di una sola persona? Poco credibile… solo un team di cervelloni universitari può produrre un simile lavolo di sintesi, solido, profondo e complesso, non un neofita.

Dopo una rapida ricerca sul web, ho scoperto che *Satoshi* è un nome dato ai ragazzi e significa *dal pensiero chiaro, maturo, intelligente*, mentre Nakamoto sta per *origine centrale* o *uno che vive nel centro* e la combinazione può essere liberamente interpretata come Intelligenza Centrale e la cosa finisce lì.

Per anni si sono avvicendati molti nomi e personaggi, possibili identità del padre della criptovaluta.

C'è stato C.S.Wright, imprenditore australiano che ha fornito prove di essere il creatore di bitcoin. Ma subito dopo, qualcuno ha fatto irruzione nei suoi uffici *per una questione poco chiara*… L'Ufficio delle tasse australiano dichiarò che il raid era stato collegato a una vecchia indagine sui pagamenti delle tasse piuttosto che sul bitcoin.

Interrogato al riguardo Wright dichiarò di collaborare pienamente. *Ci sono avvocati che negoziano con loro su quanto devo pagare*, disse.

È spuntato anche un certo Nick Szabo e molti altri sono stati suggeriti come potenziali autori, ma nessuno è stato seriamente preso in considerazione.

Mi è capitato tra le mani uno scritto di una trentina di pagine di Sol Adoni, un giovane genio che dichiarava che a 15 anni aveva fatto uno studio su un sistema crittografico quantistico nello spazio a sei dimensioni e di avere continuato con studi di matematica superiore, ma alla fine non ha convinto neanche me.

Pure il New Yorker pubblicò un articolo indicando due possibili candidati, uno dei quali sembrava particolarmente affidabile: studente laureato in crittografia al Trinity College di Dublino, che aveva continuato a lavorare su un software di trading valutario per una banca e aveva sfornato un articolo su peer-to-peer tecnology.

L'altro era un ricercatore presso l'Internet Institute di Oxford, Vili Lehdonvirta.

Entrambi smentiti.

Fast Company ha evidenziato una domanda di brevetto di crittografia depositata da tre ricercatori - Charles Bry, Neal King e Vladimir Oksman - e una nota ben documentata che includeva un'analisi del testo di Satoshi con il commento: *... dal punto di vista dei calcoli è una pratica da tenere in considerazione*. Anche questa è stata categoricamente respinta.

Il 20 gennaio 2018 a San Pietroburgo si chiude la ricerca del misterioso Satoshi Nakamoto, se si crede a Natalya Kaspersky, ex CEO di Kaspersky Labs e attuale CEO di InfoWatch.

Durante il suo discorso agli studenti, tenuto all'Università ITMP, la donna dichiara che Satoshi Nakamoto è né più, né meno che un soprannome affibbiato da un gruppo di crittografi americani. Per anni si era speculato sulla sua identità… Dopo avere fotografato le diapositive della sua presentazione e averle discusse con i media, la notizia bomba ha fatto il giro del pianeta.

È poi apparsa un'altra diapositiva dal contenuto sorprendente: *Il Governo degli Stati Uniti è responsabile della creazione del bitcoin, progetto sviluppato in collaborazione con Agenzie di Intelligence americane. Scopo è stato fornire finanziamenti per attività di intelligence statunitensi, britanniche e canadesi in diversi Paesi. La tecnologia è privata, come Internet, GPS e TOR. È di tipo Dollar 2.0 e il suo livello è controllato dai titolari. Il routing (noto come TOR) è nato con il finanziamento del Governo federale Usa attraverso il programma DARPA. Mancano tuttora prove concrete che il bitcoin sia nato con finanziamenti Usa*.

Durante la presentazione Kaspersky ha anche condiviso la sua teoria secondo cui lo *smartphone* non è un sistema personale: è usato per controllare il suo proprietario.

Le notizie si sommano alle rivelazioni di E.Snowden, ex agente della CIA e consulente NSA, che da aprile a dicembre 2013 ha trasmesso a due giornalisti, Glenn Greenwald e Laura Poitras, un'enorme massa di documenti, inizialmente stimati tra 15-20.000 e costantemente alimentata fino a 1,7 milioni e progressivamente diffusi alle principali testate giornalistiche mondiali.

I documenti riguardano la sorveglianza globale su Internet, ma anche sui telefoni fissi e cellulari e altri mezzi di comunicazione, svolta dalla NSA (National Security Agency) organismo che insieme alla CIA e all'FBI si occupa di sicurezza nazionale.

The Guardian per primo inizia a pubblicare alcune delle rivelazioni, seguito da molti altri media che diffondono i dettagli operativi del monitoraggio condotto dalla NSA e dai suoi partner internazionali.

Il web magazine *The Intercept* svela intanto un programma segreto destinato a spiare il trading di bitcoin sul mercato delle criptovalute con informazioni destinate a influenzare i mercati finanziari e a rintracciare possibili flussi di denaro diretti a organizzazioni terroristiche.

Tutti sono coinvolti nel mondo delle valute virtuali, Bitcoin o altre. Non a caso, la CIA e la NSA sono i genitori della criptovaluta.

Gli annunci a ripetizione e ben dosati scuotono l'intero web, essendo stato il bitcoin sempre associato a transazioni oscure, tra cui il traffico di armi, droghe, lavaggio di denaro, finanziamenti occulti … Cose che la CIA e la NSA hanno sempre combattuto.

Rivelazioni contraddittorie e al contempo sconvolgenti per il mondo delle criptovalute.

Il bitcoin è un progetto CIA o NSA o di entrambe le Agenzie? E se Satoshi Nakamoto era una persona reale e non un gruppo segreto, perché non farsi avanti e rivendicare il diritto sui quasi €7 miliardi pari al milione e più di bitcoin acquistati alla data della creazione del bitcoin?

Se si trattasse della NSA, una volta emersa l'identità, perché continuare a nasconderla?

Le affermazioni secondo cui la NSA ha creato Bitcoin sono circolate per anni.

Perché dubitare dell'impiego dell'algoritmo hash SHA-256, progettato dalla stessa NSA e pubblicato dal National Institute for Standards and Technology (NIST).

È evidente che l'algoritmo utilizzato per proteggere il bitcoin, non era disponibile al tempo di Satoshi perché realizzato dopo, nel 2001.

Tale fatto porta ad assumere che sia stata creato un artificio per la funzione hash che nessuno ha mai rilevato, il che le ha permesso di spiare gli utenti di bitcoin e di manipolare le transazioni, senza forzature né enormi risorse hardware necessarie e prendere alla fine il controllo della rete, questo secondo il parere di Matthew D. Green ricercatore di crittografia della Johns Hopkins University di Baltimora, sede della NSA.

È ragionevole pensare che NSA sia l'autore del progetto bitcoin?

L'NSA è stata una delle prime organizzazioni a descrivere un sistema simile a Bitcoin.

Circa 12 anni prima che Satoshi Nakamoto pubblicasse il suo leggendario white paper nella mailing list di crittografia di Metzdowd.com, un gruppo di ricercatori della sicurezza delle informazioni della NSA nel 1996 preparò un documento intitolato *How to make a mint: the Cryptography of Anonymous Electronic Cash* e lo pubblicò su una mailing list del MIT e nel *The American Law Review* (Vol. 46, Numero 4).

Il documento descrive in 30 pagine un sistema molto simile al bitcoin in cui sono possibili transazioni finanziarie sicure attraverso una rete decentralizzata che i ricercatori chiamano informalmente banca.

Quattro sono le funzionalità indispensabili per la rete: privacy, identificazione dell'utente, integrità del messaggio con protezione contro la manomissione, modifica delle informazioni della transazione con protezione contro duplicazioni di impiego, inserimento di serie di transazioni successive (blockchain).

Per completezza è in essere un'infrastruttura di autenticazione che consente l'accesso alle quattro funzionalità di sicurezza. Scritto da 3 studiosi, è il progetto della criptovaluta. 10 anni dopo si chiama bitcoin, è qualcosa di perfetto per le organizzazioni che hanno operazioni clandestine come NSA e CIA.

È un modo per il Deep State di dotarsi un'infrastruttura finanziaria inattaccabile e al di fuori dello sguardo e del controllo della finanza istituzionale, svincolabile da Wall Street o da qualsiasi altra banca del pianeta. Rende più facile mascherare operazioni in corso, rende possibile sorvegliare il crimine informatico, con la registrazione pubblica dei conti e delle transazioni sulla blockchain. È pubblico e totalmente trasparente. Le sue chiavi possono essere usate come un'impronta digitale per i dati originali.

Perché alla NSA interessa una criptovaluta che risponde al documento del 1996? Una semplice risposta, un unico scopo, una sola parola: controllare, ispezionare, verificare, catalogare.

Non è importante chi o perché abbia creato il bitcoin.

Quel che conta è com'è fatto e come funziona. La criptovaluta e il bitcoin in quanto primo esempio, è *open source*, quindi accessibile agli esperti che ne scavano il codice bit su bit e lo migliorano in continuazione.

Quando i cambi BTC / $ e BTC / € saranno disponibili presso le principali banche e i broker, potremo dire che il bitcoin ce l'ha fatta.

Non c'è nulla di rivoluzionario nella criptovaluta (di seguito denominata bitcoin per semplificare), si tratta solo di un'applicazione logica della tecnologia alla finanza.

Bitcoin è un sistema chiuso in numero finito e questo già lo rende una valuta anti-inflazionistica e per lo meno capace di mantenere stabile il suo valore. Il valore del dollaro nel frattempo, continua a deteriorarsi lentamente nel tempo con l'introduzione nel sistema della nuova M3. Geniale strategia della FED …

Il bitcoin può diventare la moneta unica mondiale e consentire all'Agenzia per la sicurezza di registrare perfettamente e totalmente ogni transazione sulla rete. Tutte le transazioni sono memorizzate pubblicamente e senza interruzione, il che significa che chiunque può vedere il saldo e le transazioni di qualsiasi indirizzo bitcoin.

Tuttavia, l'identità dell'utente con il suo indirizzo rimane sconosciuta finché le informazioni non vengono rivelate durante un acquisto o in altre circostanze: entrano in gioco le chiavi, pubbliche e private. Il bitcoin gioca un ruolo insperato nel QE per la Fed e per la maggior parte delle banche centrali mondiali.

Il QE può risolvere la crisi del credito, ma il QE stesso non è e non ha la soluzione.

Oggi tutte le valute hanno una velocità che tende a zero e i banchieri centrali sanno che il sistema monetario è condannato dai tassi di interesse nulli o negativi: è un sistema basato sul debito, sul nulla. Due funzioni nuove sono disponibili ora quasi esclusivamente per le banche centrali e potrebbero presto essere aperte ad altri utenti come risultato di un nuovo progetto di moneta digitale.

La prima è il sistema di Regolamento Lordo in tempo reale (RTGS) utilizzato dalle banche centrali e tipicamente riservato a transazioni di alto valore da risolvere istantaneamente e l'altra è la gestione del denaro contante emesso dalla Banca Centrale.

Usando la Utility Settlement Coin (USC) disponibile ad oggi nelle banche svizzere, è nato un consorzio formato da cinque membri per aiutare le banche centrali a favorire a più clienti l'accesso a questi strumenti.

Sempre più chiara appare la connessione tra il sistema del dollaro Usa e il sistema militare, di difesa e di controllo. Vale un esempio, uno solo, significativo: il modo in cui l'Iraq è passato all'euro proprio prima dell'invasione dell'esercito. Nell'ottobre del 2000 l'Iraq ha insistito per sbarazzarsi del dollaro - la valuta del nemico – in favore dell'euro.

Il passaggio è stato annunciato esattamente lo stesso giorno in cui l'euro ha raggiunto il livello più basso, acquistato a soli $ 0,82, e i ministri delle finanze del G7 sono stati costretti a salvare la valuta.

Venerdì l'euro aveva raggiunto $ 1,08, in crescita del 30% ... Dal 2001 nell'ambito del programma Oil-for-Food delle Nazioni Unite, quasi tutte le esportazioni di petrolio iracheno sono state pagate in euro. Circa €26 B sono stati versati

per 3,3 miliardi di barili di petrolio in un conto di garanzia a New York. Il conto iracheno, detenuto a BNP Paribas, ha anche beneficiato di un tasso di interesse in euro maggiore rispetto a quello in dollari.

In definitiva l'NSA controlla e raccoglie letteralmente tutte le comunicazioni elettroniche, internet, telefonate, tutto. Ascolta anche le chiamate vocali criptate con microfoni ad alta potenza, dispositivi cellulari dotati di sistemi di registrazione ed è sempre più difficile comunicare in privato sul pianeta Terra, senza essere ascoltati dall'NSA. Dal controllo delle comunicazioni è breve il passo al totale controllo del sistema finanziario, inclusi i record di tutte le transazioni fornite dal bitcoin.

Tutto chiaro ora, anche senza Nakamoto?

Curiosa sorte quella del bitcoin.

Misterioso, desiderato, vituperato, fonte di grandi ricchezze e di colossali rapine, cercato da ladri, terroristi e truffatori, incomprensibile alla gente, intoccabile, senza peso e senza colore, distruttibile con un click, depredatore di energia elettrica, detestato da chi non lo conosce, anarchico e rifiutato dalle banche perché nemico del loro potere di controllo, corteggiato dalle banche perché salvagente dai mali della finanza, libro aperto per tutti quelli che lo sanno leggere.

La sua quotazione oggi è in crescita del 4% rispetto a ieri, pari a circa 7.933€. 16M di BTC sono in circolazione, nelle mani di circa 14M di clienti. La capitalizzazione del mercato è €120,6 B con volume di scambi pari a 17,7 M per un controvalore quotidiano riferito al 9 maggio di €14,3 B.

Gli scambi totali delle 100 Top criptovalute sono stati di €215,8 B (pari al 10.3% del PIL Italia).