Alle origini del mito

Come spesso accade, anche la nascita di Bitcoin affonda le radici in una serie di progetti incompiuti e falliti, ma anche nella... teoria economica, la cosiddetta 'scuola austriaca'.

Thomas Zara, Managing Partner di Arkadia Digital Advisory.

Bitcoin è concettualmente un nuovo sistema monetario completamente slegato e alternativo all'attuale basato sulla valuta fiat. La sua resilienza e il suo continuo diffondersi, con annesse implicazioni economiche sociali sta attirando sempre più l'attenzione. Ma come nasce questo strumento che sta 'minacciando' l'ordine costituito?

Risale formalmente al 2009 e al misterioso Sathoshi Nakamaoto, ma è in realtà il frutto di alcuni decenni di sperimentazioni, tentativi, errori, confronti e dibattiti. È sicuramente figlio di un innovativo fenomeno sociale che si è diffuso a partire dagli anni '90: l'*open source*.

Vi sono stati in passato numerosi casi simili di progetti, incompiuti o falliti, propedeutici a tale invenzione. Non è nient'altro che un assemblaggio perfezionato di tali sperimentazioni. Bit Gold di Nick Szabo, DigiCash di David Chaum ed Hash Cash di Adam Back sono solo gli esempi più rilevanti. Concetti come le firme digitali e funzioni crittografiche di hash su cui si basa la tecnologia del protocollo Bitcoin sono prese, pari pari, da questi progetti.

Ma quante e quali sono invece, le motivazioni o ragioni ideologiche all'origine di questa rivoluzionaria invenzione? Due.

La prima, di natura economica, fa riferimento alla cosiddetta scuola monetaria austriaca, che si contrappone in maniera decisa al pensiero dominante keynesiano, a oggi considerato quale unica dottrina.

In estrema sintesi, secondo tale corrente di pensiero, persone e imprese dovrebbero essere lasciate libere di decidere con quale moneta essere pagate. Senza imposizioni dall'alto, il mercato convergerebbe automaticamente verso la 'moneta migliore', intesa sia come mezzo di scambio, di unità di conto, che riserva di valore. Sarebbe quindi il mercato a scegliere il mezzo di pagamento migliore!

Risulta chiaro ed evidente lo stravolgimento epocale a cui verrebbe sottoposto lo status quo politico-finanziario. Le analogie con la nascita di Bitcoin, almeno ideologiche, appaiono quantomai evidenti.

Infatti, una moneta digitale libera e non inflazionabile, decentralizzata e slegata da qualsiasi pianificatore centrale appare proprio la forma di denaro che questi economisti hanno, da sempre, teorizzato. A tal riguardo suonano profetiche le parole pronunciate nel 1974 da uno dei suoi maggiori esponenti, Friedrich Von Hayek: "*Non credo potremmo disporre ancora di una moneta sana e onesta, senza prima averla tolta dalle mani dei governi. Se non riusciamo con la violenza dovremmo inventarci uno stratagemma, introducendo qualcosa che loro non possono fermare*".

> «Prima della nascita di Bitcoin ci sono stati numerosi progetti simili, incompiuti o falliti, propedeutici alla sua invenzione, che ne è un assemblaggio perfezionato. Bit Gold, DigiCash e Hash Cash sono solo alcuni degli esempi più rilevanti»

La seconda, ha implicazioni più sociologiche, ed è focalizzata sui concetti di libertà e privacy. Trae origine dal movimento socio-culturale, emerso e sviluppatosi tra gli anni '70 e '90 e noto con il nome di cyberpunk: una corrente di attivisti globali che condivideva i medesimi ideali e che sosteneva l'uso della crittografia come strumento di difesa nei confronti dell'invasività dei governi e delle grandi *corporations* nella vita dei cittadini.

Rifiutavano l'idea di dover fornire i propri dati a enti in grado di poterli tracciare, monitorare o controllare. Erano inoltre ossessionati dal fatto che tali enti potessero in qualche modo negare loro l'autorizzazione a transazioni finanziarie. Tale movimento incentrò quindi le proprie risorse nella collaborazione per la creazione di una moneta digitale 'privata', distribuita e decentralizzata, che permettesse transazioni anonime e che potesse contrapporsi al sistema monetario 'fiat'.

Gli esperimenti e i tentativi in questo senso non mancarono. Alcune fallirono, sia per limiti tecnico-informatici, sia per l'essere troppo in anticipo sui tempi. Altre come ad esempio e-gold, furono chiuse d'ufficio dalle autorità. Tutti questi progetti erano accumunati dall'essere centralizzati, quindi vulnerabili quando la loro popolarità raggiungeva una soglia considerata rischiosa dalle autorità. Tale criticità è stata l'origine del concetto di decentralizzazione, il 'peer to peer'. Programmi di condivisione di file come eMule e BitTorrent possono quindi essere considerati parenti prossimi di Bitcoin.

L'intuizione di Sathosi è stata quella di combinare il 'peer to peer' con una tecnologia (datata!), che faceva riferimento alla firma digitale di tipo asimmetrica (o a chiave pubblica). Tale ingegnosità gli ha già conferito di diritto l'onore dell'incisione del suo 'anonimo' nome nel travertino digitale della storia delle invenzioni.