Bitcoin, la cripto valuta complicata

di Roberto Vacca – Il 27/1/2021 Creso comprò un bitcoin a 25.592 $. Lo rivendette dopo 2 mesi e mezzo a 46.696 $: guadagnando l'82%. L'8/9/21 Giobbe compra un bitcoin a 57.060 e la rivende il 17/1/2022 a 36.571 $: in 4 mesi perde il 64% dell'investimento. Sembra che abbiano giocato d'azzardo: quelle variazioni non riflettono quelle del valore di un bene (il "sottostante") che sia cambiato in proporzione. Pochi anni prima un bitcoin valeva molto poco. Poi ha subìto variazioni selvagge. Ecco la storia:

Il bitcoin (btc) è una valuta (nascosta = cripto valuta) inventata con un dotto e oscuro articolo nel 2008 da Satoshi Nakamoto, un individuo (forse un gruppo) le cui generalità sono incognite. Fu accettata negli ultimi anni da aziende, da privati, da El Salvador, da Malta – perché garantirebbe transazioni (bonifici) sicure, irreversibili, anonime, senza alcun intervento di banche o enti pubblici.

I bitcoin si possono comprare on line su numerose piattaforme e anche in molte banche. Un bitcoin valeva 32 $ nel 2013, 770 $ nel 2014, 998 $ nel 2017, da 4000 a 19000 $ nel 2018, da 13.500 a 4000 $ nel 2019, da 3850 a 19.860 $ nel 2020, 66.000$ nel febbraio 2021 e 37.070 $ il 20 gennaio 2022. Elon Musk ci investì un miliardo e mezzo di dollari nel 2021. Anche grossi finanzieri e assicuratori ci hanno investito capitali notevoli.

Una transazione in bitcoin ha bisogno di essere validata da investitori ("peer to peer" – da pari a pari) collegati – detti "miner" (minatori) che devono trovare all'uopo una soluzione crittografica a un problema numerico complesso. Un minatore (in consorzio con altri) per effettuare le operazioni di convalida deve acquistare adeguato software e, per il suo

grosso computer una moltitudine di schede grafiche che gli costano ben oltre 20.000 $. Per ogni bitcoin assorbe l'energia di 1700 kWh (che costano circa 1000 Euro). I minatori in Kazakistan e Kossovo, molto attivi, consumavano tanta elettricità da produrre una carestia: la loro attività è ora vietata, come nella Repubblica Popolare Cinese.

I minatori registrano le garanzie di affidabilità e copertura delle transazioni in bitcoin suddividendole in catene di blocchi, ove ciascun blocco ne contiene da 1000 a 2000) in un libro mastro (ledger) su Internet accessibile a tutti. Per ogni blocco certificato, il minatore riceve una ricompensa che inizialmente era di 50 btc che si sono dimezzati 3 volte (lo fanno ogni volta che si aggiungono 210.000 blocchi al libro mastro); all'inizio del 2022 la ricompensa era scesa a 6,25 btc – per arrivare da 50 btc a 6,25 si è dimezzato tre volte.

Ogni investitore in bitcoin è incognito; ha un suo – convenzionale derivato da una chiave privata e da una pubblica secondo il sistema RSA.

A ogni transazione si applica l'operazione "hash" (taglio), che genera una registrazione di ora e data ("timestamp") e una stringa crittografata di 256 bit, qualunque sia la lunghezza del documento originale. La stringa viene generata dai minatori per tentativi mediante grossi computer che col loro software sono venduti dal "coregroup" = nucleo centrale degli investitori iniziali. Lo hash viene certificato e adottato quando genera un numero da usare una sola volta (OTP – One Time Pad, detto "nonce") che soddisfa certe prescrizioni connesse con un parametro detto "difficoltà". Questi dati sono associati al blocco che viene "incatenato" a blocchi precedenti e, quindi, ai successivi. Le procedure di generazione e controllo dei "blockchain" (catene di blocchi) sono complesse e descritte in saggi e testi on line. Le definizioni di operatori e parametri sono peculiari: chi esegue operazioni con bitcoin può ignorarle e affidarne la gestione al sistema informatico. In caso di incongruenze, i

minatori votano sottoponendo il contenuto dei blocchi ad analisi informatica. In tale processo predominano i voti di chi possiede maggiore dotazione di bitcoin e processori che consentano maggiore velocità di hashing. Il funzionamento non è, quindi, affatto “peer to peer”.

Il fantomatico Nakamoto ha guadagnato molto vendendo bitcoin ai prezzi citati sopra: di questa ciptovalua esiste oggi l’equivalente di circa 800 miliardi di dollari. I minatori hanno incassato, per i loro servizi, poco più di 2 miliardi. Nakamoto ha definito ogni meccanismo dei bitcoin e delle relative catene. In particolare; il numero massimo di bitcoin che potranno essere creati è di 21 milioni; all’inizio del 2022 siamo quasi a 20 milioni.

Sebbene la nomenclatura (usata in inglese) e le procedure usate siano arduamente comprensibili [includono “soft fork”, “hard fork”, “segwit” – definiti in modi astrusi] il sistema funziona ed è sicuro. È usato da non troppo numerose aziende e privati – e anche da ricattatori (coi loro “ransomware”) che siano capaci di bloccare il funzionamento di un computer fin quando non ricevano anonimamente (in bitcoin) un riscatto.

Malgrado le procedure rigide e la crittografia, vari criminali hanno acceduto ai sistemi di criptovalute e hanno rubato varie centinaia di milioni di dollari a Bitcoin e varie decine di milioni a Ethereum (il secondo sistema di criptovaluta – ormai ne esistono migliaia).

In molti decenni di attività professionale ho interagito con banche italiane, francesi, inglesi, statunitensi, svizzere. Non ho avuto problemi, né ho subito furti. Solo un abile impiegato di una banca provinciale riuscì a falsificare un mio assegno di 17.000 Euro usando un modulo di assegno originale, ma lo bloccai in tempo.

Concludo che i vantaggi offerti dalle criptovalute siano soluzioni di non problemi, che si ottengono a prezzo di

svantaggi notevoli: vulnerabilità ad attacchi criminali, imprevedibili e forti variazioni di valore, incompleta accettazione dal mercato, scarsa protezione di chi compra beni o servizi, assenza di sottostante, complicazione delle procedure. Gli originatori avrebbero dovuto anche meditare sul principio KISS = Keep It Simple, Stupid!