Marco Pizzuti

CRIPTOCRAZIA NON AUTORIZZATA

Dark web, bitcoin, fake news, profiling illegale e le nuove frontiere della schiavitù digitale

EDIZIONI IL PUNTO D'INCONTRO

Marco Pizzuti

CRIPTOCRAZIA
NON AUTORIZZATA

Dark Web, bitcoin, fake news, profiling illegale
e le nuove frontiere della schiavitù digitale

EDIZIONI
IL PUNTO
D'INCONTRO

Indice

Introduzione

Negli ultimi anni abbiamo assistito all'avvento delle criptovalute come i bitcoin, che in brevissimo tempo hanno fatto accumulare un patrimonio a tutti i loro fortunati possessori. L'enorme incremento di valore della nuova moneta digitale ha determinato un boom di acquisti di massa e adesso molti risparmiatori stanno investendo in bitcoin nella speranza di vedere moltiplicare le proprie disponibilità economiche in brevissimo tempo.

I mass media e i social network di tutto il mondo hanno accolto la novità con titoli sensazionalistici che stanno alimentando il fenomeno di una nuova corsa all'oro digitale. Alcuni esempi: "Bitcoin: da informatici a milionari, la storia di due italiani",[1] "Storia di Erik, che ha mollato la scuola ed è diventato milionario. Grazie a Bitcoin",[2] "La storia di un 19enne diventato milionario con 1.000 dollari di Bitcoin".[3]

Ciononostante, solo pochi esperti informatici hanno capito realmente di cosa si tratta per poterne valutare correttamente rischi e benefici. Spiegarne il funzionamento, infatti, è piuttosto complicato, perché appena si fanno ricerche approfondite sul sistema "blockchain", che è alla base della creazione delle criptovalute, ci si imbatte in termini e meccanismi informatici astrusi che possono essere descritti ai "non addetti ai lavori" solo ricorrendo a generiche analogie che non ne consentono l'esatta comprensione.

Questa nuova forma d'investimento, inoltre, viene presentata come una rivoluzione dal basso contro i monopoli dell'alta finan-

za, poiché la blockchain, oltre a essere congeniata su un sistema ritenuto sicuro, è decentralizzata e, almeno in teoria, non sarebbe controllabile da un ristretto gruppo di oligarchi. Tuttavia alcuni indizi, come gli imponenti investimenti delle più grandi banche d'affari del mondo nello sviluppo delle criptovalute, fanno nascere il sospetto che dietro i "fuochi d'artificio" della moneta decentralizzata del popolo in realtà ci siano gli interessi dei soliti big della finanza.

Nel frattempo si moltiplicano come funghi i truffatori che approfittano dell'ignoranza informatica degli investitori per improvvisarsi venditori di criptovalute, intascare i soldi e sparire nel nulla.

I bitcoin rappresentano solo la punta dell'iceberg di una trasformazione epocale in cui nessuno potrà più uscire dalla rete di internet e che culminerà con la totale abolizione del denaro contante in favore delle valute elettroniche. In tale contesto, multinazionali come Google e Facebook hanno già posto le basi per la creazione di una società interamente digitalizzata formata dai profili (una vera e propria schedatura di massa) di tutti gli utenti che utilizzano la Rete e i social network. In pochi anni, i loro database hanno raccolto più informazioni riservate (foto, dati anagrafici, luogo di residenza, professione, opinioni, fede religiosa, acquisti e segreti privati come amanti e gusti sessuali) sui cittadini di quanto siano riuscite a fare la CIA e l'NSA in tutti i decenni precedenti.

Ogni volta che usufruiamo di un servizio informatico o di un'app che ci chiede di poter accedere ai nostri contatti, alle nostre foto, alla nostra telecamera e al nostro microfono, accettiamo di perdere qualsiasi forma di privacy e può facilmente accadere che quando andiamo a prenotare dei posti in aereo su un sito web online, il programma di prenotazione della compagnia aerea con cui non abbiamo mai avuto nessun precedente contatto già conosca in anticipo tutti i nostri dati anagrafici.

Senza che ce ne rendiamo conto e in modo perfettamente legale, chi controlla i nostri dati controlla anche noi e può sfruttare le informazioni acquisite per fini commerciali, politici o criminali.

Le autostrade informatiche inoltre possiedono dei passaggi "segreti", ossia una sorta di "tombini digitali" che conducono alla fogna sotterranea del dark web (una zona della Rete invisibile ai motori di ricerca e ai browser ordinari), dove i servizi d'intelligence, le organizzazioni criminali e ogni genere di malintenzionato possono acquistare o vendere droga e armi, commissionare omicidi, corrompere politici o pagare mercenari per rovesciare governi utilizzando le criptovalute che garantiscono l'anonimato assoluto.

Ciò che ci aspetta nel prossimo futuro, insomma, è la criptocrazia di un potere nascosto che già ora viene esercitato a esclusivo vantaggio di chi detiene il controllo delle informazioni su ciascuno di noi. Possiamo far finta di non saperlo o sperare che questo potere venga usato sempre a fin di bene, ma se così non fosse, non potremmo far niente per impedirlo e di fatto, ogni volta che usiamo i servizi offerti dalla Rete in cambio di nostre informazioni (in modo sia cosciente che inconsapevole), stiamo aiutando la criptocrazia a costruire la nostra identità digitale su cui ha il totale controllo.

Capitolo I

Blockchain e bitcoin tra illusioni e realtà

Nel biennio 2017-2018 i grandi canali d'informazione mainstream hanno fornito un ulteriore contributo nel rendere i bitcoin molto popolari in tutto il mondo come nuova fonte di guadagni da capogiro. Ai mass media è bastato spiegare che nel 2010 un bitcoin valeva appena 0,39 dollari e che oggi viene quotato a circa 9000 euro (dopo picchi che hanno superato i 15.000 euro) per scatenare la prevedibile corsa agli acquisti degli investitori. Davvero "non male" come pubblicità mediatica per una valuta elettronica che, secondo i suoi promotori, sarebbe stata addirittura avversata dai potenti magnati della grande finanza.

Notoriamente infatti la stampa e le principali emittenti televisive sono controllate direttamente (per quote societarie) o indirettamente (attraverso l'acquisto degli spazi pubblicitari o pressioni sui partiti e i governi) dai poteri forti e difficilmente possono promuovere qualcosa che sia realmente contro i loro interessi.[4]

Ciononostante, nessuno sembra essersi accorto dei paradossi che hanno accompagnato lo straordinario successo delle criptovalute sin dal loro nascere. Gli eccezionali guadagni promessi dai guru delle monete virtuali in quasi totale assenza di critiche da parte degli esperti economici più blasonati sono bastati a rendere le nuove valute elettroniche "decentralizzate" il fenomeno del momento.

Ma di cosa si tratta realmente? E cosa c'è dietro lo specchietto delle allodole dei soldi facili? A queste domande purtroppo, non ha ancora risposto nessuno ed è giunto il momento di iniziare a farlo.

Cos'è e come funziona il sistema delle blockchain

Il rivoluzionario sistema informatico denominato "blockchain" (dall'inglese "catena di blocchi") è il meccanismo alla base delle transazioni dei celebri bitcoin e di tutte le altre criptovalute (valute coperte da un codice segreto) emergenti come Ethereum, Monero, Ripple, Litecoin ecc. (in tutto ne esistono circa mille). Attualmente tale tecnologia è stata dichiarata sicura e affidabile anche dall'Associazione bancaria europea (Abe) e gode di ampio consenso in ambito sia informatico che finanziario. Le grandi novità da essa introdotta riguardano essenzialmente l'alto livello di sicurezza e la decentralizzazione del sistema, che non richiede più alcuna autorità centrale di gestione e vigilanza. Così, mentre le transazioni di denaro effettuate sul nostro conto corrente bancario (entrate e uscite) vengono riportate nel registro elettronico del server di un istituto di credito che potrebbe anche essere modificato illegalmente, le transazioni di valuta digitale effettuate con la blockchain vengono registrate sugli archivi informatici di tutti i singoli computer collegati a un sistema di controllo distribuito. Pertanto, per poter modificare fraudolentemente i dati contenuti nel database informatico condiviso di una blockchain è necessario avere accesso a tutti i computer connessi al sistema e manipolare ogni copia dei file contenuti all'interno dei loro registri, poiché in caso contrario la truffa contabile verrebbe immediatamente scoperta.

Il bitcoin è una valuta virtuale (un semplice elaborato informatico), generalmente indicata con il simbolo "฿" (o con l'abbre-

viazione BTC o XBT), che ha la caratteristica di essere protetta da un codice segreto. Di conseguenza, affinché una transazione in bitcoin possa essere ritenuta valida, la valuta digitale deve essere riconosciuta come autentica attraverso un complicato lavoro di decriptazione del codice segreto, che viene svolto dai computer degli utenti connessi al programma della blockchain.

Gli elaboratori impegnati in questo lavoro di estrazione dei codici alfanumerici vengono chiamati "minatori" (*miner*), proprio in quanto devono riuscire a "estrarli" dalla matassa di tutte le combinazioni errate possibili con numerosi calcoli matematici. Il lavoro computazionale necessario a trovare il codice nascosto di convalida dei bitcoin non è sempre lo stesso poiché diviene più complesso con l'aumentare del numero delle transazioni effettuate.

Una volta che il bitcoin è stato convalidato, viene formato un nuovo blocco dati crittografati (versione digitale di un libro mastro contabile) con la registrazione di tutte le transazioni effettuate in precedenza. Il nuovo blocco dati così creato (ogni dieci minuti circa ne viene aggiunto un altro) si va ad agganciare agli altri blocchi preesistenti, mantenendo il corretto ordine cronologico affinché non si perda mai traccia di ogni operazione eseguita. Il software utilizzato per i bitcoin e la blockchain è ispirato alla trasparenza e per questo motivo la sorgente del programma è liberamente accessibile (open source) agli esperti informatici.

Tutte le transazioni convalidate, annullate o che hanno subito modifiche vengono trascritte sul database informatico condiviso tra i computer degli utenti (chiamati "nodi") e tale tipo di memorizzazione collettiva dei dati rende il procedimento particolarmente affidabile contro le truffe, perché ciascun elaboratore collegato al sistema possiede una copia di tutti i file all'interno della sua memoria digitale. In questo modo, ogni "nodo" può verificare la conformità delle trascrizioni sulle transazioni dei bitcoin e approvare o disapprovare la validità dell'operazione. Questo pro-

cedimento è chiamato "consenso" (deve ricevere l'approvazione di 50% +1 dei nodi) e serve a garantire maggiore sicurezza contro le falsificazioni e gli attacchi informatici.

Il principale difetto del registro distribuito creato dalle blockchain è l'utilizzo di un processo macchinoso molto più lento di quello usato per la valuta elettronica ordinaria. I bitcoin, inoltre, sono stati concepiti dai propri programmatori informatici per non poter superare mai la soglia dei 21 milioni di pezzi e tra pochi anni si arriverà al loro limite massimo di produzione.

Nel momento in cui viene creato un nuovo blocco, un marcatore temporale ne registra data e ora di emissione, mentre un "hash" di verifica (funzione matematica progettata per impedire la modifica dei dati in modo retroattivo e garantire la sicurezza contro le manipolazioni digitali dei file) va ad agganciarsi al codice hash del blocco precedente. Di conseguenza, se qualche hacker (esperto informatico in grado di violare i sistemi di sicurezza) volesse aggirare i codici "hash" per cambiare i dati dei file a suo piacimento, dovrebbe creare dei blocchi paralleli con la riproposizione degli stessi a tutta la rete, ma ciò è possibile solo ottenendo il controllo del 50% +1 dei blocchi.[5]

La ricompensa dei "minatori" e l'emissione decentralizzata di nuova valuta

Se il tentativo di decriptazione del codice segreto di un bitcoin va a buon fine, viene creato un nuovo blocco dati valido, la transazione in valuta digitale viene confermata dai nodi (l'insieme dei pc degli utenti) e il software genera ulteriore moneta elettronica come forma di ricompensa per l'oneroso lavoro svolto dai "miners".

Pertanto, a differenza delle monete elettroniche ordinarie a corso legale (utilizzate per esempio nei pagamenti con bonifici e carte di credito), l'emissione di nuova valuta virtuale in criptova-

luta non viene gestita da alcuna autorità centrale, poiché è lo stesso software della blockchain a generare automaticamente nuova valuta digitale dopo che i "minatori" hanno estratto i codici di un bitcoin e il nuovo blocco dati è stato convalidato.

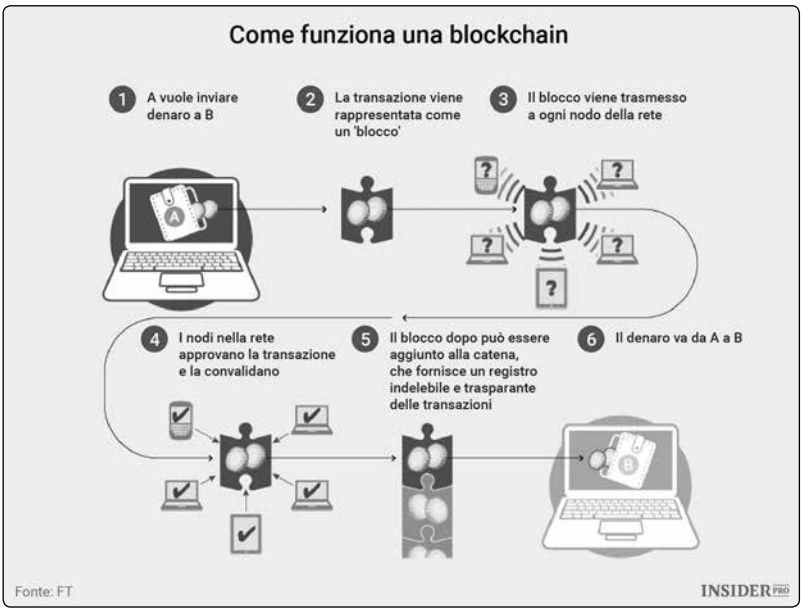
I computer impiegati nell'onerosa attività di estrazione dei codici ("*mining*") utilizzano un software e un hardware specifici che devono essere in grado di svolgere milioni di calcoli al secondo. Il valore economico del bitcoin invece, viene stabilito direttamente dal rapporto tra domanda e offerta (senza nessun intermediatore) e la sua accettazione come forma di pagamento si basa esclusivamente sulla fiducia (*trust*) che i suoi utilizzatori vi ripongono (a differenza delle monete a corso legale, la loro accettazione non è garantita dallo Stato).

I "miners" insomma svolgono un ruolo chiave del sistema blockchain, poiché oltre a estrarre i codici di verifica indispensabili a convalidare le transazioni, con il loro operato determinano anche l'emissione di nuova valuta virtuale. Le transazioni convalidate che hanno superato la cosiddetta "*proof of work*" (prova di lavoro da cui l'acronimo inglese "POW") sono costituite da dati crittografati registrati su tutti i nodi del database pubblico.

La complessità dei codici da decriptare inoltre è progressiva, in quanto diviene maggiore con il moltiplicarsi del numero dei blocchi della catena e per questo motivo l'attività di "mining" richiede elaboratori sempre più potenti e costosi caratterizzati da un consumo energetico in costante aumento.

In estrema sintesi, all'origine della creazione dei bitcoin ci sono le "hash", ossia delle formule matematiche che non sono modificabili retroattivamente. Ogni volta che un minatore riesce a estrarre la soluzione delle "hash" crea bitcoin, ma affinché l'operazione si concluda con successo è necessaria anche l'approvazione della maggioranza dei nodi degli altri utenti. La soluzione all'hash di ogni bitcoin è legata a quella precedente e alla successiva, in una catena temporale che è iniziata a gennaio

del 2009 e finirà quando tutti i bitcoin nascosti in Rete saranno stati letteralmente "estratti" dal Web.



Blockchain chiusa e sistema decentralizzato apparente

Le blockchain possono essere di tipo aperto (chiunque può contribuire al processo computazionale di validazione dei blocchi mediante lo scaricamento di uno specifico software) o chiuso ("*permissioned blockchain*"). Quest'ultimo ha la particolarità di limitare i soggetti abilitati alla convalidazione dei blocchi, in quanto tale attività viene riservata ai soli membri autorizzati. Le differenze tra i due sistemi sono notevoli, poiché nel tipo aperto (utilizzato da tutte le principali criptovalute come bitcoin, Ethereum, Monero, Litecoin ecc.) gli utenti non hanno bisogno di dimostrare la propria identità, mentre nel sistema chiuso ciascun "nodo" della blockchain deve essere previamente identificato e

autorizzato da un organo direttivo centralizzato a cui viene affidata la vigilanza sulla corretta gestione del sistema.[6]

La blockchain chiusa non ha un registro pubblico accessibile a tutti e per questo motivo garantisce la massima riservatezza sulle transazioni dei suoi utenti, che possono essere lette solo dai membri autorizzati. Il processo di validazione dei blocchi, inoltre, può essere reso molto più rapido della blockchain aperta mediante la semplice adozione di un regolamento semplificato che viene deciso dalla governance interna.[7]

In teoria quindi le criptovalute della blockchain aperta si basano su un sistema democratico, decentralizzato e trasparente, perché chiunque può diventare "minatore" semplicemente scaricando l'apposito software e utilizzando la potenza computazionale del proprio computer per estrarre i codici dei blocchi. Secondo gli esperti insomma nessun oligarca potrebbe mai assumere il controllo delle criptovalute, perché non esiste alcuna autorità centrale e tutti i soggetti coinvolti si troverebbero al medesimo livello decisionale.

In pratica, invece, la situazione è molto diversa da come viene fatta apparire: soltanto i computer dei primi "miner" che riescono a estrarre i codici di sblocco dei bitcoin ricevono il premio in valuta e per avere successo nell'operazione è necessario poter disporre di costosi elaboratori dalla notevole capacità di calcolo. Tale situazione pone i "miner" in concorrenza tra loro e chi possiede un semplice pc da casa o da ufficio dalla potenza di calcolo modesta non ha nessuna concreta possibilità di arrivare primo. I "miner" professionisti invece dispongono di capitali da investire e di super computer dall'enorme potenza di calcolo che consente loro di estrarre i codici per primi e di prendersi il "bottino" dei bitcoin premio. A tutti gli altri "miners" non resta che unire la capacità computazionale dei loro computer per creare dei gruppi di "minatori" chiamati "*mining pool*", che una volta estratti i codici si spartiscono i bitcoin premio ottenuti in

base alla rispettiva capacità di calcolo di ciascun utente.[8] Ciò significa che nonostante la blockchain sia stata concepita come sistema totalmente decentralizzato, l'emissione e la proprietà dei bitcoin finisce per concentrarsi nelle mani dei "miners" più facoltosi (ossia nella rete informatica di una multinazionale o di una banca d'investimenti dell'alta finanza) e dei grandi gruppi di mining pool, che possono permettersi di disporre di enormi potenze di calcolo e di consumare ingenti quantità di energia elettrica.

I "mining pool" utilizzano una rete di computer peer-to-peer ("da pari a pari") in cui ogni elaboratore è un nodo che tratta alla pari con gli altri nodi. Il "premio" in bitcoin viene spartito tra i minatori dell'intero gruppo, ma più sono i miners partecipanti e più modesta sarà la percentuale di bitcoin a cui avranno diritto come ricompensa. Il più grande problema tecnico e commerciale emerso finora riguarda solo l'estrema lentezza del sistema di pagamento in bitcoin, che ancora non è in grado di reggere il confronto con l'immediatezza garantita dalle transazioni in moneta digitale ordinaria.

I rischi e le denunce del Codacons

I bitcoin, possono essere creati dagli utenti mediante l'attività di "mining" (estrazione dei codici) oppure possono anche essere acquistati su una piattaforma di scambio online, pagandoli con moneta ordinaria a corso legale. Nel caso di acquisto, i tassi di cambio e i costi di commissione variano di molto a seconda del tipo di rivenditore ma le truffe in questo campo sono molto comuni (alcuni hacker si prendono i soldi degli acquirenti e poi spariscono senza inviare i bitcoin promessi) ed è buona regola rivolgersi solo a venditori affidabili (anche se più cari) di livello internazionale.

Questo sistema di valuta virtuale consente la detenzione e la cessione anonima di moneta elettronica all'interno della Rete da parte di utenti che hanno indirizzi bitcoin e il possessore della criptovaluta potrà rivenderla in qualsiasi momento in cambio di moneta legale. Per poter acquistare, conservare e svolgere operazioni in bitcoin (o in qualsiasi altra valuta digitale), gli utenti devono creare il proprio "portafoglio elettronico" (*e-wallet*) scaricando uno dei tanti software deputati a questa funzione. Tale conto elettronico può essere salvato e gestito sulla memoria di un dispositivo informatico (computer, tablet, smartphone, microchip sottocutaneo ecc.) oppure può essere scaricato su un database accessibile online tramite autenticazione dell'utente sul sito del proprio wallet provider (in questo caso si tratta di un portafoglio digitale che in lingua inglese viene indicato come "virtual wallet") di fiducia. Ovviamente, ciascun metodo di conservazione dei bitcoin comporta dei rischi, in quanto il virtual wallet online può essere hackerato, mentre la memoria fisica del dispositivo con l'e-wallet può essere smarrita, rubata o danneggiata. In tutti questi casi infatti, non si avrà più alcuna possibilità di recuperare i propri bitcoin.

Il valore delle criptovalute inoltre si basa sulla fiducia e, come accade normalmente in borsa, è sufficiente che qualche speculatore riesca a diffondere menzogne sul loro imminente crollo o aumento esponenziale per determinare la corsa alle vendite o agli acquisti.

Negli ultimi anni, il valore delle criptovalute è stato sempre in forte ascesa nonostante le prevedibili oscillazioni tra picchi massimi e livelli minimi. Investire in bitcoin o in altre criptovalute emergenti è l'affare del momento, ma se è vero che possono farci diventare milionari in pochissimo tempo (semplicemente acquistandoli oggi e aspettando che il loro prezzo continui a levitare in modo esponenziale come hanno fatto in precedenza) è altrettanto vero che il loro valore può crollare ancora più rapidamente.