BITCOIN & CO.
CHI SONO E CHI SI CREDONO DI ESSERE

NEL BENE O NEL MALE, SONO LE STAR DEL MOMENTO, SE NE PARLA E STRAPARLA. EPPURE IN POCHI HANNO DAVVERO LE IDEE CHIARE SUI RISCHI E LE OPPORTUNITÀ CHE PORTANO CON SÉ. IN QUESTE PAGINE, TUTTO QUELLO CHE DOVRESTE SAPERE SULLE CRIPTOVALUTE

testo di **Alberto Tundo**

In principio fu il Bitcoin, poi arrivarono tutte le altre criptovalute, oltre 1.500. Tante ne censisce il sito Coinmarketcap, per un valore che a metà febbraio era di poco inferiore ai 400 miliardi di dollari, 140 dei quali riconducibili al solo Bitcoin. Di questa moneta, fino a qualche mese fa, in pochi avevano sentito parlare. Poi è scoppiato un fenomeno mediatico alimentato dalla portentosa crescita della sua quotazione. Per dare un'idea, il 20 dicembre 2010 un Bitcoin valeva 20 centesimi di dollaro. Il 20 dicembre del 2017, ne valeva 16.454, ed era in discesa rispetto al picco toccato quattro giorni prima (19.343 dollari). Il 6 febbraio, il suo valore era sceso a 6.200 dollari. Una volatilità sulla quale si sono concentrati molto i media, che però non sorprende gli economisti. «La teoria economica», spiega Angelo Baglioni, ordinario alla facoltà di Scienze bancarie dell'Università Cattolica, «ci dice che, per essere tale, una moneta deve possedere tre caratteristiche: deve essere mezzo di scambio, cioè essere comunemente accettata, deve essere riserva di valore, cioè conservare il suo valore nel tempo e, infine, deve essere quello che in gergo si chiama "numerario", ovvero l'unità con la quale si misura il valore di attività finanziarie reali, beni e servizi. Se mi si chiede, quindi, se il Bitcoin sia una moneta, la mia risposta è negativa». Le monete virtuali, insomma, non sono monete: non sono comunemente accettate e il loro valore oscilla troppo. Questo perché non c'è uno Stato né una banca centrale a difenderlo, ma sono i flussi di domanda e offerta a determinarlo: maggiore è la richiesta di Bitcoin, più il loro prezzo aumenta, e viceversa. Ma era proprio questa mancanza di un'autorità centrale l'elemento cardine nella filosofia che sta dietro alla creazione del misterioso Satoshi Nakamoto, il cui obiettivo era dare vita all'equivalente digitale del contante, uno strumento per garantire transazioni che fossero istan- →

tanee, anonime, gratuite e non mediate, cioè che non avvenissero attraverso banche e altri intermediari che fungono da garanti. Nell'ecosistema Bitcoin, invece, gli utenti si scambiano denaro come si manderebbero una mail, solo che anziché avere un indirizzo di posta hanno un codice alfanumerico che ne identifica il conto. Le banche non servono più. Il sistema finanziario non ha più strumenti per prendere in ostaggio l'economia reale.

A rendere questa immediatezza e trasparenza possibile è la tecnologia sulla quale poggia tale moneta, la Blockchain, un impianto che mescola matematica, teoria dei giochi, informatica e crittografia di livello militare per proteggere i dati contenuti nelle reti (da qui la definizione criptovaluta). In breve, il sistema funziona così: chi vuole "estrarre" Bitcoin, deve scaricare un programma che trasforma il suo computer (o tablet o smartphone) in un nodo della rete, una sorta di torre di controllo che ha accesso a tutto lo storico dei movimenti in questa valuta dalla creazione di quest'ultimo. In questo modo, sono i computer degli utenti a verificare che il conto X abbia davvero il denaro che sta inviando a Y, ad autorizzare la transazione a maggioranza e quindi, in un secondo momento, a sigillare quell'operazione, insieme ad altre, in una teca trasparente (detta "blocco"), consultabile da tutti ma non più modificabile, affinché un'operazione non possa essere più cancellata e una certa somma utilizzata due volte. Il creatore di un blocco che viene validato dal sistema viene ricompensato con un tot di Bitcoin, che così vengono creati (è il cosiddetto *mining*). Uno o più computer potrebbero provare a "barare", ma per poter alterare le transazioni è necessario riuscire ad assumere il controllo di più della metà degli apparecchi della rete Bitcoin.

La Blockchain è l'esempio più famoso di Dlt, acronimo che sta per *Distributed Ledger Technology* (ledger significa libro mastro, *ndr*). È questo tipo di tecnologia che è alla base delle altre critptovalute, nate a volte per imitazione, altre ancora per creare ecosistemi simili ma tarati su esigenze di un'altra utenza. Ripple, per esempio, è una moneta il cui protocollo non contempla il *mining*, ha un limite al circolante molto più alto (100 miliardi di monete, contro i 21 milioni di Bitcoin), ospita transazioni in altre criptovalute e, soprattutto, è costruita su una rete plasmata sulle necessità delle banche, che se ne servono per scambiarsi informazioni e valuta in maniera più veloce e con costi decisamen-

ALCUNE CRIPTOVALUTE

B

BITCOIN

È LA CRIPTOVALUTA PIÙ CELEBRE E AL SUO ANONIMO FONDATORE, CONOSCIUTO COME SATOSHI NAKAMOTO, SI DEVE ANCHE L'IDEAZIONE DELLA BLOCKCHAIN

RIPPLE

A DIFFERENZA DEL BITCOIN, NON CONTEMPLA IL MINING. VIENE UTILIZZATA ANCHE DA ISTITUTI FINANZIARI PER SCAMBIARSI VALUTA IN MANIERA PIÙ VELOCE E CON COSTI INFERIORI

R

L

LITECOIN

PUNTA A MIGLIORARE IL MODELLO BITCOIN: LA SUA GENERAZIONE È QUATTRO VOLTE PIÙ VELOCE E POSSONO ESSERE GENERATE FINO A 84 MILIONI DI MONETE (CONTRO I 21 MILIONI DI BITCOIN)

IOTA

ABBANDONA LA BLOCKCHAIN PER IL TANGLE, PROTOCOLLO SOFTWARE BASATO SU GRAFI ACICLICI DIRETTI, IL CHE LO RENDE INFINITAMENTE SCALABILE E RIMUOVE I COSTI DI TRANSAZIONE

I

M

MONERO

SE I PAGAMENTI IN BITCOIN NON ASSICURANO IL COMPLETO ANONIMATO, QUESTA CRIPTOVALUTA PUNTA SULLA NON TRACCIABILITÀ DELLE TRANSAZIONI

NEM

ACRONIMO DI NEW ECONOMY MOVEMENT, NON È SOLO UNA MONETA (DETTA ANCHE XEM) MA UN ECOSISTEMA BASATO SU UNA NUOVA INTERPRETAZIONE DELLA BLOCKCHAIN

N

DESCRIVERE LE CRIPTOVALUTE COME MONETE CHE CONSENTONO AI CRIMINALI DI PROSPERARE, È UN ERRORE

te inferiori. Litecoin, invece, è nata per superare la lentezza delle transazioni in Bitcoin, che fino a poco fa non poteva processare più di sette operazioni al secondo (il circuito Visa, sotto Natale, arriva a processarne 4 mila al secondo). ZCash e Monero, dal canto loro, si propongono come monete garanti di un anonimato totale. Le Blockchain possono essere intese come reti autostradali sulle quali oggi viaggiano le monete virtuali ma potrebbero ospitare traffico di altro tipo. Everledger, per esempio, usa la Dlt per creare certificati digitali di diamanti e gioielli, proteggendoli dalla contraffazione, perché ne certifica l'intera filiera. Ma lo stesso si potrebbe fare con il cibo o, come spiega Luigi Laura, docente di Machine Learning alla Luiss di Roma, si potrebbe usare la Blockchain per organizzare elezioni online, anziché ricorrere a seggi, schede e scrutatori, procedura che ha tempi e costi non indifferenti. «Lo Stato potrebbe stampare una moneta virtuale per ogni elettore, il quale voterebbe inviandola al candidato prescelto. In questo modo sarebbe facile verificare chi ha vinto, cioè →

L'INTERVISTA

UN PORTAFOGLIO (VIRTUALE) IN TASCA

INTERVISTA A VINCENZO DI NICOLA, COFONDATORE DI CONIO, BITCOINWALLET PER SMARTPHONE

Nel mondo delle criptovalute, un posto particolare spetta ai Wallet, luoghi in cui conservare le monete virtuali, se non ci si fida a lasciarle negli Exchange dai quali le si è acquistate. Possono essere installati sul computer, su una pen drive o sul cellulare. Conio è una start up italiana, cofondata dallo sviluppatore Vincenzo Di Nicola. Con lui, Business People ha parlato di trading, procollo Bitcoin e sicurezza informatica.

Che cos'è Conio?

È una compagnia fondata nel 2015 da Christian Miccoli (creatore di Conto Arancio di Ing Direct, tra i padri dell'online banking in Italia, ndr) e da me con un investimento iniziale di Poste Italiane. Lo scopo è di rendere accessibili a tutti le monete virtuali, specialmente i Bitcoin, offrendo una soluzione perché il loro acquisto, conservazione e utilizzo siano semplici e sicuri.

Convinzione diffusa è che queste tecnologie non siano a prova di hacker: l'attacco all'Exchange giapponese Coincheck è costato agli utenti qualcosa come 580 milioni di dollari in Nem.

Bisogna distinguere tra il protocollo Bitcoin, un prodigio tecnologico non indifferente, e gli Exchange. Il primo in nove anni si è dimostrato ultrasicuro, avendo

resistito a moltissimi attacchi. Altra cosa sono queste compagnie, che detengono criptovalute per i clienti e che sono state attaccate. Specialmente all'inizio si trattava di piattaforme colabrodo, messe in piedi da persone con scarsa esperienza informatica. Oggi le società sono sempre più professionali e con team più qualificati. In più, sono emersi sistemi di protezione più evoluti, detti a chiave multipla.

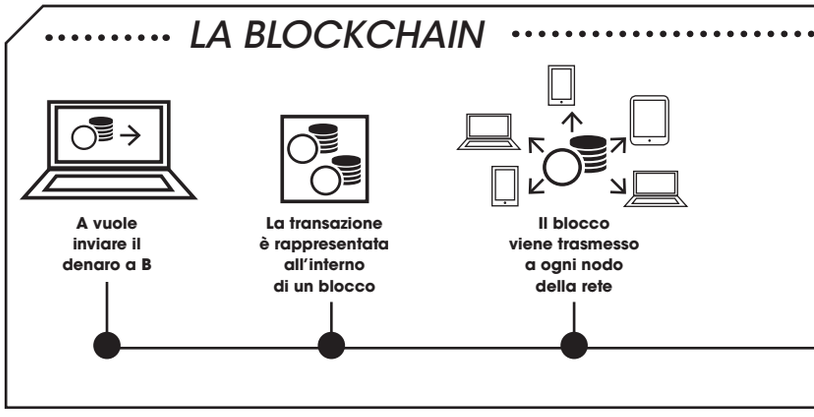
La sicurezza, quindi, è stata una sfida anche per voi.

È stata la prima questione e l'abbiamo risolta. Anche nel caso in cui il cliente dovesse perdere il cellulare, si dimenticasse la password o – anche tocchiamo ferro – passasse a miglior vita, riusciamo a ricostruire la posizione e ridare a lui o agli eredi i suoi soldi. Sembra una cosa semplice, ma posso assicurare che non lo è, perché nel mondo Bitcoin conoscere la password significa avere accesso al conto. Perciò è fondamentale da un lato non perderla, ma dall'altro essere salvaguardati in caso di emergenze.

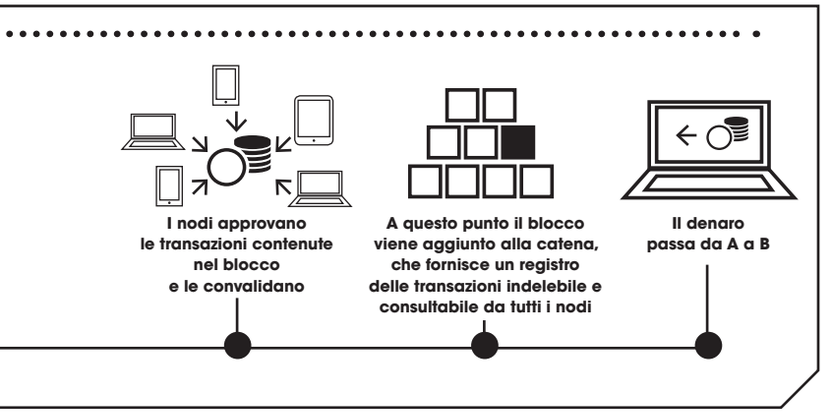
il candidato che ha preso più soldi». C'è un ma, secondo il professore: chi controlla e gestisce l'infrastruttura di voto? «Il problema della tecnologia sulla quale si regge il Bitcoin è che, una volta che si diffonde, con utenti indipendenti in grado di partecipare aggiungendo il proprio computer alla rete, chi l'ha creata ne perde il controllo che, per definizione stessa dell'infrastruttura, è affidato alla maggioranza». La prova la si è avuta quando si è trattato di risolvere uno dei principali problemi, la non scalabilità, cioè l'incapacità di aumentare le prestazioni in caso di grande domanda, andando oltre le sette transazioni al secondo. La soluzione è arrivata con Lighting Network, una sorta di autostrada sovrapposta a quella sulla quale scorrono i pagamenti in Bitcoin, capace di ospitare un traffico molto più consistente, ma arrivarci non è stato facile.

L'uso della Blockchain riesce meglio quando i nodi sono pochi attori uniti da interessi convergenti, come le banche. Sì, proprio quelle che l'invenzione di Nakamoto doveva tagliare fuori stanno investendo enormi risorse nello sviluppo di reti condivise, progetti come Corda, sviluppata dal consorzio R3 o come l'Utility Settlement Coin, come Hyperledger o la già citata rete Ripple. Il perché lo spiega Emilio Barucci, docente di Matematica finanziaria al Politecnico di Milano: «Tramite una Dlt, le banche potrebbero, per esempio, scambiarsi titoli in maniera semplice, veloce ed economica. Oggi questi scambi devono passare attraverso un meccanismo molto complesso di verifica, con dei passaggi tecnici molto onerosi. La Blockchain li renderebbe superflui perché le banche potrebbero consultare lo stesso database e verificare l'affidabilità della controparte in tempo reale». Però, mentre fanno ricerca sulla Blockchain, conducono una guerra sotterranea alle criptovalute. Prima hanno cominciato diffondendo un senso di sfiducia verso le monete virtuali, adesso stanno passando alle maniere forti. Jp Morgan, Bank of America, Citigroup, Capital One e Discover Bank per esempio, hanno vietato l'acquisto di Bitcoin e

LA TECNOLOGIA ALLA BASE DELLE MONETE VIRTUALI POTREBBE ESSERE UTILE ANCHE PER LE ELEZIONI



Altcoin con le loro carte di credito, lo stesso hanno fatto in Gran Bretagna le banche del gruppo Lloyd. E si stanno muovendo anche gli Stati. Secondo l'*Mit Technology Review*, in Cina, Corea del Sud e Giappone, i governi hanno già adottato diversi provvedimenti per vietare il trading anonimo, le Ico (le *Initial Coin Offering*, ovvero offerte di valuta virtuale a opera di start up che si finanziano così anziché emettendo azioni) e per regolamentare in maniera più stringente le attività degli Exchange, le piattaforme attraverso le quali si possono comprare o sulle quali si possono depositare Bitcoin e Altcoin. Il vento sta cambiando: il mercato



delle criptovalute è scoppiato all'improvviso, attirando enormi capitali in un contesto caratterizzato dalla mancanza di regole, che verranno verosimilmente introdotte. Come spiegato da Paul Donovan, capo del team di economisti di Ubs, i governi hanno bisogno di soldi e non possono accettare che fiorisca un'attività economica rigogliosa che sfugga al loro potere di tassazione. Negli Usa, l'Internal Revenue Service, cioè il Fisco, stanga gli evasori in Bitcoin già dal 2015. È una questione economica, non di sicurezza. Descrivere il Bitcoin e le Altcoin come monete che garantiscono l'anonimato e che, quindi, consentono a terroristi e trafficanti di prosperare, è un errore. La Blockchain fa l'esatto contrario: registra e rende immodificabile ogni transazione. Certo, sono noti solo i numeri dei conti che comunicano e non le identità dei loro proprietari, ma a un governo sufficientemente motivato non ci vorrebbe molto per ricavare queste informazioni. Un primo passo sarebbe quello di costringere gli Exchange a condividere i dati dei loro clienti. D'altronde, sono molti ormai i documenti ufficiali di banche centrali e autorità di vigilanza che assegnano un basso rischio alle criptovalute per quanto riguarda il finanziamento di criminalità e terrorismo. L'ultimo documento a scagionarle è stato diffuso a ottobre dalla National Crime Agency britannica.

Ma il mondo delle criptovalute è decisamente più vasto e un dibattito focalizzato su quotazioni in perenne oscillazione e anonimato delle transazioni fatica a inquadrare il reale potenziale di certe innovazioni. Eppure, un luogo da cui partire per provare a capire che Blockchain e monete virtuali sono molto più di una bizzarria o di uno strumento speculativo c'è ed è in Italia. È Rovereto, cittadina che può essere considerata la principale Bitcoin Valley italiana, se non mondiale. Qui ha sede InBitcoin, start up multiforme attiva sul fronte a 360 gradi, dalla ricerca alla consulenza, dalla gestione di una piattaforma di acquisto di Bitcoin all'assistenza agli esercenti che decidessero di accettarli, passando per la comunicazione specialistica legata al mondo Blockchain. Marco Amadori, tra i primi in Italia a occuparsi seriamente di criptovaluta, ne è il Ceo. «Qui Bitcoin sta entrando nella quotidianità di molti cittadini, che lo usano, se ne interessano, ne parlano. Diversi imprenditori stanno dando vita a un'economia circolare, con clienti che pagano in criptovaluta ed esercenti che la girano ai fornitori e la usano per pagare gli stipendi e tutto questo senza rivolgersi ad alcuna banca», racconta l'imprenditore. «Le potenzialità offerte da questa tecnologia sono enormi, possono rendere davvero le banche non più indispensabili e cambiare i meccanismi di accesso al credito. È come se la rivoluzione di Internet, che finora aveva modificato la società ma senza toccare il mondo economico-finanziario, adesso fosse arrivata anche sotto quelle torri d'avorio. Negli anni '80 e '90 due ragazzini potevano lanciare una sfida alla Ibm da un garage. Adesso possono lanciarla a JP Morgan e qualsiasi altro colosso».