Mateusz **Riva**

AVANTI *Bitcoin*, DOPO *Bitcoin*

Un’analisi multidisciplinare
a partire dai princìpi primi di una tecnologia
che rappresenta un punto di singolarità dell’umanità.

Autore: Mateusz Riva

www.villaggiobitcoin.it
info@villaggiobitcoin.it

Codice ISBN: 9798336118124

Dedicato a Elio e Maria Helena, che con il loro esempio mi hanno ispirato a pensare sempre a lungo termine.

INDICE

PREFAZIONE

Avete mai paragonato un fenomeno sociale alla stregua di un buco nero, avente una densità talmente grande da inghiottire tutto quel che si trova sotto la sua influenza? Oppure avete mai preso in considerazione la possibilità di un nuovo elemento chimico che possa completare la tavola periodica degli elementi? Vi è mai balenata per la mente l'eventualità di dover interagire tutti i giorni con un nuovo organismo vivente nativo del mondo digitale? Avete mai provato a considerare il fenomeno economico e sociale dell'inflazione come un vettore ingegneristico che descrive una grandezza fisica? Avete per caso già considerato che, tra le unità di misura standard internazionali attualmente in uso come il metro, il chilogrammo o il grado centigrado, ora abbiamo a disposizione un nuovo sistema di riferimento assoluto per misurare il valore di qualsiasi bene o servizio?

La verità è che Bitcoin riguarda un fenomeno molto più complesso e molto più profondo rispetto a quanto possa apparire a prima vista. La creatura estratta dal cilindro da Satoshi Nakamoto è stata progettata in fin dei conti per risolvere un problema specifico – quello della rimozione della fiducia in soggetti terzi in merito alla gestione del denaro – e riferito ad un preciso periodo storico, quello che passerà tristemente agli annali come il "periodo incidentale del sistema fiat". Bitcoin è stato in sostanza ricercato con l'intento di "aggiustare" la moneta nei giorni nostri. E già questo sarebbe di per sé una grandissima rivoluzione.

Ma c'è di più. Lo strumento monetario risulta strettamente connesso con tutti gli ambiti della nostra società. Il denaro è da sempre uno degli elementi alla base di tutte le civiltà umane, utilizzato fin dall'alba dei tempi. Stiamo parlando di una tecnologia tanto importante quanto ancora inspiegabilmente sconosciuta alla stragrande maggioranza degli individui di tutto il mondo.

Il punto è che, trovando con Bitcoin finalmente una soluzione brillante al problema monetario che ci trascinavamo ormai da millenni, si stanno ora innescando a cascata tantissime altre implicazioni sociali, politiche e filosofiche. Si tratta di implicazioni dirompenti, con forti impatti sulle nostre vite e sulle nostre prospettive future come esseri umani. In campo energetico, questo nuovo protocollo rovescia gli schemi, creando un ponte di collegamento inedito e indissolubile tra il mondo fisico e il mondo digitale. In campo sociale, Bitcoin rovescia le preferenze temporali e il comportamento degli individui, incentivandoli a pensare a lungo termine e al risparmio piuttosto che al consumismo sfrenato e all'indebitamento. In fatto di economia, Bitcoin ribalta completamente le teorie dominanti applicate senza eccezioni in tutto il mondo, riportando finalmente al centro il buon senso, la tutela delle proprietà private e una società basata sul libero mercato. Il mondo della finanza viene letteralmente stravolto: non è mai esistito nella storia un asset con le caratteristiche di bitcoin. Dal punto di vista tecnologico, questo fenomeno rende obsoleto un intero sistema di gestione e trasferimento del denaro – quello bancario – nato ed evolutosi ormai da secoli. In campo imprenditoriale, questa innovazione è *game changer* per le aziende. Per quanto riguarda la politica, Bitcoin consente agli individui di sottrarsi in modo pacifico alle decisioni invadenti e autoritarie di governi e istituzioni pubbliche, difendendo i diritti fondamentali dell'uomo. In campo giuridico, Bitcoin opera secondo le Leggi immutabili della natura, rendendo irrilevanti i provvedimenti arbitrari dei regolatori che non sono allineati con esse.

Curiosamente, il testo che avete tra le mani sembra proprio ripartire in modo naturale dalle conclusioni del libro *Villaggio Bitcoin*, dove questa scoperta veniva identificata come un "Grande Filtro", una sorta di evento spartiacque per la storia evolutiva dell'Homo Sapiens. Il titolo *Avanti Bitcoin, Dopo Bitcoin* si riferisce infatti proprio al fatto che dovremmo iniziare a parlare di "epoca pre-Bitcoin" e di "epoca post-Bitcoin". Tutto diventerà chiaro e scontato ai posteri, ma non lo è ancora a chi si trova oggi immerso nel cambiamento. Il detto ricorrente nella

Bitcoin community: «*fix the money, fix the world*» non sarà considerato solo un motto, ma una verità empirica dimostrata sperimentalmente.

In queste righe, da leggere tutte d'un fiato, Mateusz ci accompagna in esplorazioni a partire dai princìpi primi verso l'ignoto del post-Bitcoin, spingendosi talvolta anche ai limiti dell'immaginazione nel tentativo di riuscire a vedere oltre lo *status quo*. Gli scenari dipinti potrebbero apparire a prima vista quasi surreali, percepiti ancora molto lontani nelle sue applicazioni pratiche, ma non per una mente curiosa e razionale, offrendo un'ottima guida per orientarsi in questi nuovi orizzonti.

Tuttavia, a differenza delle speculazioni passate sul futuro dove non vi erano troppi elementi solidi su cui basare le intuizioni, con Bitcoin è diverso: possiamo contare su alcuni punti saldi e incontrovertibili. Bitcoin è un faro stabile e certo in un mondo di continue instabilità e incertezze. A partire finalmente da un punto fermo e affidabile, e sulla base di ragionamenti logici e concetti di buon senso condivisibili, si possono così delineare scenari e risultati davvero sorprendenti. Magari inizialmente controintuitivi, ma al tempo stesso estremamente affascinanti e plausibili.

Ogni capitolo di questo libro è un invito alla riflessione. Tanti, tantissimi interrogativi e domande aperte che, unite a ragionamenti logici, potrebbero (volutamente) spingere il lettore a rimettere in discussione alcune convinzioni date per scontate. In un secondo momento, inevitabilmente, dopo aver digerito e assimilato lo shock cognitivo, conducono a qualcosa di chiaro, limpido e, per certi versi, anche "ovvio".

Siamo davvero fortunati a vivere in questa particolare fase storica, quella dei primissimi anni Dopo Bitcoin. Ci troviamo immersi in uno dei più grandi cambiamenti della storia e possiamo agire in anticipo e da protagonisti. Ancora in pochi se ne sono resi conto, ma si tratta solo di una questione di tempo. L'insegnamento finale di questo libro che traspare in maniera velata in tutte le pagine – e che trova il sottoscritto certamente d'accordo – è che, per tutti noi, esiste un solo modo per sopravvivere indenni a questa brusca e repentina transizione epocale: abbandonare al più presto l'attuale sistema fiat e abbracciare con entusiasmo la rivoluzione Bitcoin.

Valerio Dalla Costa
Agosto, 15 Dopo Bitcoin

INTRODUZIONE

Se non mi credi o non capisci,
non ho tempo per cercare di convincerti, mi dispiace.

Satoshi Nakamoto, 29 luglio 2010

Trattandosi di un completo cambio di paradigma, comprendere Bitcoin richiede la capacità, la volontà e l'umiltà necessaria per rivedere l'insieme delle assunzioni, dei presupposti e degli schemi mentali che coscientemente o per assimilazione inconscia dello *status quo* del mondo in cui viviamo abbiamo fatto nostri e che oggi guidano la nostra vita. Se pensi che sia un'iperbole, probabilmente non hai ancora approfondito a sufficienza per rendertene conto.

Nelle seguenti pagine troverai tanti spunti di riflessione multidisciplinari che potrebbero a primo impatto risvegliare il tuo ego, magari non predisposto a mettere in discussione il filtro con cui fino ad oggi hai interpretato quanto ti circonda. Rimettere in gioco le conoscenze che hanno governato la nostra intera vita, la nostra esperienza fino a quel momento e la percezione del mondo che magari ci ha portato ad ottenere il successo di cui godiamo può richiedere molte ore di studio.

Se hai una mente curiosa che ti spingerà a guardare oltre, non escludo che anche tu rimarrai colpito da questa tecnologia.

In un mondo dove negli ultimi millenni il progresso della nostra specie è legato più alla tecnologia che all'impercettibile evoluzione naturale, se

possiamo individuare una costante, questa è il cambiamento esponenziale.

Come spesso accade con le rivoluzioni tecnologiche nel corso della storia, il tempo di adozione è direttamente legato e limitato dalla capacità umana di comprenderle, accettarle e farle proprie. In particolare, le conseguenze che da essa scaturiscono non sono né prevedibili né preventivabili cercando di immaginarle con la logica finora utilizzata, ma appaiono scontate per la generazione successiva che cresce con quella tecnologia già nel proprio orizzonte.

Come esempio, pensa all'adozione di Internet. Con l'utilizzo che ne fai oggi, con la sua diffusione capillare che arriva in ogni tasca di ogni persona, se fossi catapultato all'inizio degli anni '90 e potessi ascoltare i commenti che se ne facevano all'epoca, non ti sembrerebbe incredibilmente irrazionale sentire qualcuno criticarne l'utilità e dubitare del suo valore? Se sei nato con Internet in mano, pensandoci un attimo probabilmente ti domanderai: «*come è stato possibile che non tutti abbiano capito e adottato immediatamente Internet vista la sua utilità?*». D'altra parte, se hai vissuto in quel periodo di transizione, come avresti mai potuto immaginare che la tecnologia ed Internet avrebbero smaterializzato così tanti oggetti della tua vita quotidiana facendoli collassare in uno smartphone? Ecco, in 30 anni, il tempo di un cambio generazionale, è avvenuto un cambio di paradigma che ha portato una tecnologia dall'essere utilizzata da una piccola nicchia di persone all'essere utilizzata come presupposto indispensabile per partecipare alla vita lavorativa, sociale, finanziaria da parte di quasi tutta l'umanità.

E se Bitcoin stesse ripercorrendo esattamente lo stesso processo di diffusione ed adozione? Chi lo utilizza oggi mediamente è visto come un pioniere-nerd di una tecnologia non conosciuta o uno speculatore-scommettitore finanziario. E se invece lasciando passare sufficiente tempo, vista l'immensa utilità di questa tecnologia, Bitcoin sarà adottato dalla maggior parte della popolazione con la stessa facilità di utilizzo con cui oggi mandiamo un messaggio?

Bitcoin richiede una certa conoscenza tecnica se si vuole verificare con mano il codice che ne costituisce l'anima, ma è estremamente semplice per l'utilizzatore finale. Quanti conoscono la chimica di un idrocarburo, la tecnologia del motore a scoppio o le leggi di Newton su cui poggia la dinamica? Eppure, senza farsi troppe domande, tutte le mattine utilizzano l'auto come mezzo di spostamento. Possedere Bitcoin in sostanza vuol dire conoscere 12 parole in un ordine specifico, e lo

scambio avviene condividendo una breve stringa di testo, anche scansionando banalmente un QR code. Spaventoso vero?

Certo, se non hai mai guidato, come puoi pensare di sapere utilizzare un'auto? Solo perché non ne hai una e non la sai ancora guidare diresti mai che è una tecnologia inutile, che consuma troppa energia o che vi sarà un'auto migliore tra 10 anni?

Ecco, posso affermare con serenità che la quasi totalità di chi ancora non apprezza o critica Bitcoin non lo ha mai utilizzato direttamente e le sue argomentazioni tipicamente sono solo quelle derivanti dall'aver letto il titolo di un articolo di giornale, forse nemmeno leggendo l'articolo stesso. Quanto è attendibile l'opinione di qualcuno che nemmeno conosce a fondo l'argomento di cui parla?

In tutti questi anni, ho incontrato varie persone scettiche nei confronti di questa tecnologia, ma nessuna di loro ne conosceva a fondo le proprietà. Viceversa, tutte le persone che avevano approfondito l'argomento appena sotto la superficie ne riconoscevano la genialità. Sarà un caso?

Come tutti, prima di studiarlo a fondo, anche io ne avevo già sentito parlare in precedenza. Anche io pensavo di essere arrivato tardi. Anche io l'ho notato per la sua rapida capacità di apprezzamento in termini di valuta fiat. Anche io pensavo che vi fosse la possibilità di bandirlo ed eliminarlo con un decreto, anche io…

Poi, ho fatto il mio bagno di umiltà. Un letterale battesimo che, pur non garantendomi la capacità di vedere quali saranno le effettive implicazioni sull'umanità derivanti dalla scoperta di Bitcoin, mi permette almeno di percepire l'incredibile potenzialità di questa tecnologia. In particolare, analizzandone le varie sfaccettature, sono arrivato a cogliere i benefici del suo sempre più inestricabile rapporto simbiotico con l'umanità e con la prossima sempre più autonoma Intelligenza Artificiale.

Dopo aver mantenuto per tutti questi anni l'assoluto riservo, mi sono reso conto che le migliaia di ore di studio che ho dedicato a Bitcoin non potevano più rimanere solo mie. Sento quindi una vera e propria necessità di condividere la mia incredibile passione per questa tecnologia.

CONSIDERAZIONI PRELIMINARI

La prima cosa a cui pensano tutti quando qualcuno parla di Bitcoin è il suo prezzo espresso in dollari o in euro. Pur essendovi un'infinità di altri aspetti che presenterò nelle seguenti pagine, quello finanziario ha

sicuramente caratteristiche interessanti, che per essere apprezzate a pieno richiedono come prerequisito la conoscenza di cosa sia il denaro, di come venga gestito e di come le sue proprietà influenzino la società. Risulta quindi intuitivo chiedersi: quando il denaro perde valore da un giorno all'altro siamo incentivati a pianificare risorse per il futuro? Assolutamente no: siamo incentivati a consumare e spendere, in quanto il potere d'acquisto è più alto oggi e sarà più basso nel futuro spingendoci inconsciamente a dare più valore alla gratificazione immediata.

Nel mondo Bitcoin avviene esattamente l'opposto: il potere d'acquisto cresce nel tempo e il costo della vita cala costantemente.

Cambiando anche solo questa condizione, siamo incentivati ad accumulare risorse e a pensare sempre di più a lungo termine. Una constatazione semplice, ma con implicazioni considerevoli su molti aspetti sia della nostra vita quotidiana, sia delle prospettive future come civiltà umana nel suo complesso.

Sempre più stretti nella morsa dei prezzi che aumentano a seguito dell'inflazione, alcuni si sentono sperduti e sopraffatti dalle circostanze che cambiano e che non riescono a comprendere. Altri si ingegnano sotto la spinta della necessità nella ricerca di forme di guadagno aggiuntive che vadano a compensare la perdita di potere d'acquisto, e consentano magari un miglioramento delle proprie condizioni di vita. Investire per esempio, è una professione che richiede competenze specifiche, e pertanto dovrebbe essere solo un'opzione per chi vuole intraprendere quella carriera, non una necessità per difendersi da una forma di denaro che perde valore nel tempo.

Studiando le varie classi di investimento, che vanno dal semplice acquistare oro come bene rifugio, al mercato immobiliare o agli investimenti nei mercati con azioni ed obbligazioni, si impara a conoscerne i dettagli, familiarizzando con le loro peculiarità fino ad arrivare a padroneggiarle con sufficiente sicurezza.

Tuttavia, non è ancora sufficiente. C'è ancora qualcosa che non quadra, e i ritorni in termini reali dell'investimento sono in qualche modo distorti nel tempo. Anche gli addetti del settore, quelli che conoscono ogni aspetto, ogni modalità per ottimizzare ciascun investimento, perdono di vista quella che sono arrivato a credere sia la cosa più importante in qualsiasi valutazione economica: il *sistema di riferimento*.

Da ingegnere energetico, sono sempre stato ossessionato dalle unità di misura: la precisione è fondamentale in questa professione. Come è

possibile costruire, misurare e valutare qualsiasi cosa se non si dispone di uno strumento di misura affidabile?

Proprio dicendo «*qualcosa non quadra*» indico un difetto del sistema di riferimento che quotidianamente utilizziamo sia per quantificare il costo di un oggetto, sia per misurare i ritorni di un investimento: se l'unità di riferimento è artificialmente manipolata, variabile nel tempo, imprevedibile se in dilatazione o in contrazione, come possiamo fare delle misurazioni economiche affidabili?

Quasi tutti oggi sanno che il sistema di riferimento in uso per misurare il valore (le valute fiat, ovvero dollari, euro ed altre) si espande costantemente tramite l'operato del sistema bancario, con la conseguente perdita di potere d'acquisto di ciascuna unità da cui è composto. Tuttavia, mi rendo conto che non è altrettanto nota a tutti l'incoerenza tra il valore nominale dell'inflazione (quello ufficiale) ed il reale effetto dell'inflazione, come se un unico numero (ad esempio il 2%) sia in grado di rappresentare le variazioni in atto.

In particolare, ritornando all'esempio degli investitori, se il sistema di riferimento non è affidabile, con quale grado di confidenza sono in grado di determinare progressi e ritorni del loro operato? Non sono forse le loro misurazioni soggette all'errore dell'unità di misura e quindi le loro decisioni offuscate da questa approssimazione?

Se abbiamo un'unità di misura fissa ed immutabile per la lunghezza, lo spazio, il tempo, l'energia ecc., perché non dovrebbe essere altrettanto ragionevole e razionale avere un sistema di riferimento fisso ed immutabile per la misurazione del valore?

Dal 3 gennaio 2009, momento della singolarità che segna l'inizio di un nuovo paradigma, esiste una nuova unità di misura: il *Bitcoin Standard*. Questi è costituito da 21.000.000 di unità denominate bitcoin, ciascuna suddivisibile in 100.000.000 di unità denominate satoshi.

1 bitcoin = 100.000.000 satoshi

Quindi 2,1 quadrilioni di satoshi in totale.

In questa analisi presenterò fatti e spunti di riflessione che potranno darti un solido punto di vista generale ed informazioni di dettaglio che ti consentiranno di valutare, verificando con mano propria, se Bitcoin possa essere o meno l'unità di misura per il valore che mancava.

METODO UTILIZZATO

Questo libro ti darà una visione d'insieme sul denaro e sulle conseguenze a cui andremo incontro mantenendo in vita il sistema in uso evidenziando quali sono le criticità e dunque le opportunità per l'utilizzo di un sistema differente che può coesistere o sostituirsi del tutto a quello esistente, in un rapporto sempre più stretto con l'umanità.

Oltre ai temi economici, troverai riflessioni multisettoriali che ti aiuteranno a comprendere Bitcoin in modo olistico, esplicitando il potenziale impatto che avrà sulla nostra civiltà dal punto di vista etico, filosofico, politico, tecnologico, energetico, sociale.

L'analisi parte dai princìpi primi, facilmente riscontrabili dall'esperienza quotidiana di ciascuno. In particolare, con *Avanti Bitcoin, Dopo Bitcoin*, troverai 286 domande senza preclusioni di sorta sullo *status quo* del paradigma in cui viviamo, utili a stimolare la riflessione individuale sulle molteplici tematiche multisettoriali che sono e saranno sempre più impattati dall'esistenza di Bitcoin.

Il metodo utilizzato, il dialogo socratico, ovvero un metodo di indagine filosofica sviluppato dal celebre filosofo greco Socrate, è un'arte antica ma ancora rilevante nell'odierno panorama intellettuale. Questo approccio alla ricerca della verità non si limita a fornire risposte definitive, ma si concentra piuttosto sulla stimolazione del pensiero critico e sull'incoraggiamento delle persone a esplorare le loro convinzioni più profonde. L'obiettivo del dialogo socratico è far emergere la verità interiore, spingendo l'individuo a esaminare e mettere in discussione le proprie idee preconcette.

Il dialogo socratico si basa su una serie di domande aperte e mirate, poste con l'intento di far emergere le contraddizioni, le incertezze e le limitazioni delle opinioni e delle convinzioni di una persona, o in questo caso del paradigma di un'intera civiltà.

Questo libro esprime esclusivamente la mia personale interpretazione di questa nuova tecnologia attraverso una lente ingegneristica, e non può essere considerata né consulenza finanziaria, né sollecitazione all'investimento.

Mateusz Riva
Gennaio, 15 Dopo Bitcoin

PARTE 1

FILOSOFIA E SOCIETÀ

Capitolo 1

IO SONO BITCOIN

Tralasciando per un momento gli aspetti tecnici ed economici e facendo un'analisi ad un livello più profondo delle caratteristiche e delle implicazioni che derivano dalla scoperta di Bitcoin, emerge un mondo che ha dell'inverosimile: preparati, questo mondo è tanto intangibile quanto reale.

«Ma io non voglio andare tra i matti» ribadì Alice.
«Qui siamo tutti matti: io sono matto, tu sei matta!» disse il gatto.
«Come lo sai che sono matta?»
«Altrimenti non saresti venuta qui!»

Lewis Carroll - Alice nel paese delle meraviglie

Anche dopo migliaia di ore di studio, non ho ancora trovato il fondo della tana del Bianconiglio. Esaminando Bitcoin da differenti angolazioni mi rendo conto che presenta un'infinità di sfaccettature, una concatenata all'altra, e valutarne una sola alla volta non consente di comprenderlo a pieno.

Indipendentemente dal livello di approfondimento raggiunto, posso affermare con serenità che Bitcoin ha la tendenza di prendere le tue convinzioni e rimetterle nuovamente in discussione ogni volta che lo esamini da un'angolazione differente. Capirlo vuol dire esaminarlo dal

punto di vista delle teorie economiche, della teoria dei giochi, della probabilità e degli incentivi, avere un buon grado di comprensione di temi energetici, crittografia, filosofia, ma anche temi legati al diritto, alla fiscalità, alla geo-politica, solo per citarne alcuni.

Quelle che seguono quindi sono solamente considerazioni che riflettono il mio attuale grado di comprensione di questa tecnologia e che non vogliono essere né definitive, né esaustive.

In questa prima parte, vorrei accompagnarti in una breve analisi filosofica, mettendo in luce alcuni aspetti che mi portano a considerare Bitcoin un essere vivente del mondo digitale che mantiene però una diretta ed indissolubile connessione con il mondo reale.

Ogni tecnologia sufficientemente avanzata
non è distinguibile dalla magia.

Arthur C. Clarke

Quando viene introdotta una nuova tecnologia sufficientemente avanzata, per chi non ne ha studiato i princìpi, questa sarà indistinguibile dalla magia in quanto quest'ultima potrebbe sembrare la spiegazione più logica. Ti mostrerò alcuni aspetti magici di Bitcoin che ti incuriosiranno talmente tanto da costringerti ad entrare nel *mondo dei matti* e scoprire quanto è profonda la tana del Bianconiglio!

UNA SIMBIOSI NATURALE

Uno degli aspetti che più mi affascina di Bitcoin è che può essere cose differenti per persone differenti, pur restando sempre fedele a sé stesso. Che tu lo veda come un oggetto da collezione, una riserva di valore, un asset, un mezzo di scambio, una valuta, un essere vivente del mondo digitale, una minaccia o altro, la tua opinione su di esso è irrilevante in quanto lui semplicemente esiste, e non puoi fare nulla per modificarlo o farlo sparire.

Se lo studierai con un po' di attenzione, e ti spingerai appena sotto la superficie, noterai che è Bitcoin, in virtù della sua immutabilità, a cambiarti. Cambierà il modo in cui vedi il mondo, inizierai a pensare ancora più a lungo termine, ti interesserai di privacy e autodeterminazione, capirai il gioco delle valute fiat e probabilmente darai meno peso agli infiniti dibattiti politici.

Credo sia corretto paragonare Bitcoin al fuoco, all'elettricità, ad una marea o ad un qualsiasi altro fenomeno naturale: semplicemente esiste e dobbiamo prenderne atto. Ciascuno di noi poi è libero di interagirvi come più ritiene opportuno, ma la nostra opinione su di esso non lo cambierà. Ci sono quindi solamente due scelte possibili per interagire con esso: adottarlo o non adottarlo. Ciascuna scelta porta con sé le proprie conseguenze: puoi anche non essere d'accordo con uno tsunami, ma quando arriva o sei al riparo o verrai travolto. Il tuo essere in disaccordo non ti salverà.

L'umanità adotta e porta con sé nel suo processo evolutivo le scoperte e le tecnologie che ne hanno migliorato le condizioni di vita: dalla scoperta del fuoco, alle prime innovazioni legate alla lavorazione dei metalli, passando poi per la scoperta dell'elettricità e di tutti gli applicativi che ne sono poi derivati, fino all'utilizzo di Internet e alla nascita del mondo digitale.

Credo che Bitcoin sia qui per rimanere in un rapporto simbiotico e indissolubile con l'umanità, facendo da ponte tra il mondo reale ed il mondo digitale.

Infatti, fino alla scoperta di Bitcoin, il mondo digitale era completamente slegato dal mondo fisico in cui viviamo. Nel cyberspazio non esistono conseguenze per attori malevoli (es. mail di spam e bot-spam nei social network che possono propagare a costo zero) e non esiste l'unicità in quanto tutto può essere copiato senza costo un numero infinito di volte. Con la scoperta di Bitcoin, ora abbiamo trasferito alcune proprietà del mondo fisico nel mondo digitale. In particolare ora anche nel mondo digitale esiste il concetto di unicità.

In aggiunta è vero anche l'inverso: il mondo fisico in cui viviamo si è arricchito con un nuovo elemento che ha proprietà mai viste prima, un elemento nativo del mondo digitale, assolutamente scarso, senza massa, che si muove istantaneamente attraverso Internet mediante messaggi di testo. Pur essendo intangibile, può essere "distrutto" solo utilizzando un enorme consumo di energia. Vive e muore in simbiosi con gli esseri umani e non umani, dove anche una macchina, governata da un'Intelligenza Artificiale è in grado di poter interagire e vivere in simbiosi con questo nuovo elemento. Tecnologia molto avanzata o magia?

I BITCOIN NON ESISTONO

Ti sei mai chiesto dove sono i "Bitcoin"? Potrà sembrarti strano, ma rispondere a questa domanda non è banale. Puoi cercarli quanto vuoi ma non li troverai né su qualche server, né su un cloud, né nei nodi facenti parte del network e nemmeno presso i miner: semplicemente perché non esistono.

Rispondere a questa domanda richiede una spiegazione dettagliata sul funzionamento combinato delle varie parti di Bitcoin. Per facilità di lettura, riporto qui solo una versione sintetica dando però un solido spunto di riflessione che ti aiuterà a mettere in luce le innumerevoli sfaccettature di questa tecnologia.

In modo estremamente semplificato, Bitcoin non è altro che un database decentralizzato che tiene traccia "*di chi deve cosa a chi*". Grazie all'utilizzo di energia elettrica (che per essere prodotta richiede dispendio di lavoro che non può essere falsificato), il protocollo Bitcoin riesce a garantire che nessuno possa alterare tale archivio storico se non ne ha titolo e che nessuno possa impedire a chi ne ha titolo di effettuare un'inscrizione su di esso.

Se quindi possedere Bitcoin equivale ad avere uno spazio con il proprio pseudonimo all'interno del database, ed il database non è altro che un elenco di transazioni avvenute fin dall'origine, allora il possesso di Bitcoin coincide con il titolo ad effettuare un'inscrizione (transazione) nel database stesso.

APPROFONDIMENTO: *la dicitura "pseudonimo" ha fortissime implicazioni. Non è richiesto un passaporto, un'identità o perfino l'essere "umani" è superfluo in quanto anche un'Intelligenza Artificiale può avere titolo.*

Da un certo punto di vista è facile immaginare questi bitcoin come gettoni d'oro all'interno di un forziere: tutti possono vederli e verificare che vi siano solo 21 milioni di monete all'interno, non una di più. Solo chi ha titolo verso di essi può cederne a sua volta la proprietà ad un terzo, senza doverli mai spostare dal forziere.

Tuttavia, bisogna ricordarsi che si tratta di un'immagine parziale e limitante. Il forziere non esiste, i gettoni non esistono. Vi sono solo dei messaggi di testo all'interno di un database decentralizzato di cui ciascun nodo custodisce una copia e verifica in modo autonomo e perentorio la veridicità di tutti i passaggi di proprietà.

Figura 1. L'immagine rappresenta ciò che tipicamente si pensa cercando di associare Bitcoin a cose che conosciamo.

Per questo motivo, visto che tutti possono copiare e incollare questi messaggi di testo, i bitcoin veri e propri non esistono in un luogo specifico. Quello che conta è il titolo a poter operare in questo database.

LA MAPPA È IL TERRITORIO

In tutta la storia umana vi è sempre stata una netta separazione tra "l'oggetto fisico" del mondo reale e "l'informazione" che lo rappresenta.

Se pensiamo per esempio a cosa è il Denaro, ci rendiamo subito conto che una delle sue più importanti caratteristiche è quella di dover tenere traccia di "chi deve cosa a chi" in modo onesto ed inalterabile.

Nella storia umana fino ad oggi si sono utilizzati due strumenti: le monete di materiale prezioso e i database.

Le monete, per via della loro fisicità tengono in modo automatico conto della propria distribuzione (possesso) e veridicità (diamo per scontato per un attimo che sia facile verificare il contenuto di metallo prezioso in una moneta). In particolare non bisogna affidarsi a nessun ente terzo per tenere traccia di tutti gli scambi di quella moneta: averla in mano ti dà pieno titolo a scambiarla, sotterrarla o farne quello che più ti pare.

Il problema del database (che si tratti di una tavoletta di argilla in Mesopotamia, o di un registro elettronico di una banca centrale) è che bisogna avere fiducia nell'entità che custodisce il database, e che questi non lo alteri aggiungendosi senza fatica delle unità in più. Che si tratti di disegnare una "X" a suo conto sulla tavoletta di argilla o mediante un

click sui moderni database che gestiscono le valute, l'effetto è il medesimo.

Per esempio, immagina una tavoletta che riporta tante "X" quante pecore possiedi. Se conti le tue pecore arrivando a possederne 10 e le rappresenti su una tavoletta mediante 10 "X" è subito evidente che le croci non coincidono e non sono le pecore stesse, ma ne sono meramente una loro rappresentazione.

Se tu custodissi il database di tutta la tua comunità, a parte la tua onestà, cosa ti frenerebbe nell'attribuirti una "X" in più?

In particolare, teniamo presente che quell'aggiunta non equivale alla creazione di una pecora extra. Semplicemente, se dopo aver alterato il database tu la reclamassi prima di tutti gli altri legittimi proprietari, la staresti sottraendo a qualcun altro. Di fatto è una sorta di gioco delle sedie, dove l'ultimo arrivato si trova con in mano una "X", ma senza la pecora.

L'informazione sul database non è l'oggetto, ne è solamente una rappresentazione.

Un altro paragone interessante è quello della mappa e del territorio rappresentato. Il possesso del territorio è differente dal possesso della mappa. Quest'ultima infatti ne è solo una rappresentazione, e in particolare nel mondo digitale può essere copiata infinite volte senza costi. Oggi tutti abbiamo mappe digitali disponibili sullo smartphone ma questo non vuol dire che possediamo il territorio.

Una storia affascinante è quella di come si è sviluppata la gestione e la rappresentazione del denaro alle isole Yap, troverai una breve descrizione nei capitoli seguenti.

Il network Bitcoin funziona in modo analogo: tutti possono vedere quanto possiede ciascun indirizzo (che ricordo essere pseudonimo, ovvero può non essere collegabile ad una persona fisica), ma solo chi possiede le chiavi private di quell'indirizzo ha titolo per spendere/cedere a terzi quei determinati bitcoin.

Se quindi la possibilità di utilizzo è riservata a chi possiede le chiavi private, possiamo identificare il possesso di bitcoin nel controllo delle chiavi private e, siccome le chiavi private non sono altro che una combinazione di 12 parole, la conoscenza di quelle parole equivale all'oggetto.

In Bitcoin l'informazione coincide con l'oggetto (i nostri bitcoin), la mappa è il territorio, conoscere (sottointeso, la chiave privata) equivale a possedere.

Le 12 parole tra le 2.048 parole del vocabolario inglese utilizzabili nelle combinazioni sono tutto ciò che è sufficiente ricordare. Mediante un algoritmo tale combinazione consente di custodire in modo univoco le chiavi private: se ti sembra facile, sei libero di provare ad utilizzarle.

Suggerisco di fermarti un attimo a riflettere sull'ultima frase per darle il peso che merita. Si tratta della prima volta nella storia dell'umanità che possiamo affermare:

conoscere = possedere

E questo possesso è assoluto, inviolabile e per tutti.

Se ci pensi, ad oggi tutti i titoli di proprietà richiedono fiducia verso un ente terzo (pur affidabile che sia) che garantisca per noi il diritto a possedere un oggetto, come fa per esempio il certificato di proprietà di un immobile dove lo Stato si fa garante del rispetto dei nostri diritti. Se hai pensato egoisticamente solo a te stesso, e alla tua condizione di vita privilegiata dove la proprietà dei tuoi beni è tutelata, suggerisco di estendere il pensiero a quei milioni di persone che non possono dare per scontato questo diritto.

Riesci ad immaginare le conseguenze di questa rivoluzione?

Spero che la risposta sia stata "no" in quanto credo nessuno di noi oggi sia in grado di prevedere le incredibili applicazioni che potranno essere sviluppate a partire da questa rivoluzione.

CHIAVI PRIVATE, CASUALITÀ E LIBERTÀ DI PAROLA

Visto che l'informazione (ovvero conoscere le chiavi private) equivale al possesso di Bitcoin, è fondamentale conoscere come vengono originate le chiavi private.

Evito di entrare eccessivamente nei dettagli tecnici, suggerendo però a tutti di approfondire e constatare con mano quanto scrivo. Nonostante la semplificazione, lascerò un importante spunto di riflessione.

Dopo che avrai letto quanto segue, sono sicuro che anche tu risponderai con un sorriso a chi ancora oggi parla di *rischio* che questa tecnologia venga bandita e resa illegale.

L'essenza di Bitcoin poggia su matematica, casualità e teoria dei giochi. Se qualcuno volesse bandirne l'uso, dovrebbe prima bandire e rendere illegale la stessa matematica, così come lo scambio di messaggi di testo e l'utilizzo di energia elettrica per risolvere problemi matematici. Sarebbe veramente possibile?

Se quanto sopra è vero quindi, l'unica cosa possibile da fare è escludere sé stessi dall'utilizzo di Bitcoin. Una scelta potenzialmente paragonabile a quella della Corea del Nord che ha deciso di autoescludersi da Internet.

Le chiavi private, che garantiscono la sicurezza nella custodia di Bitcoin, fanno leva sulla casualità e sulla forza che hanno i grandi numeri.

Infatti, una chiave privata non è altro che un numero molto, molto, molto, molto grande generato casualmente. Potresti generarlo lanciando in aria 256 volte una moneta e segnando quale faccia esce ogni volta. In alternativa è possibile utilizzare un piccolo ed economico calcolatore che genera in modo random una serie molto grande di numeri. È veramente possibile rendere illegale il lancio ripetuto di una moneta?

Se 256 cifre non ti sembra un numero sufficientemente grande per garantire la tua sicurezza, pensa che per generare per tentativi lo stesso numero dovresti provare 10^77 (un numero con 77 zeri) volte in media per riprodurre la medesima combinazione.

Giusto per rendere l'idea di quanto sia grande quel numero, paragonalo alla stima del numero di atomi dell'universo a noi conosciuto, da 10^78 a 10^82 atomi. Un tentativo per ogni atomo dell'universo.

Tramite un algoritmo denominato *funzione hash* questo grande numero viene processato in una funzione monodirezionale, ovvero una volta ottenuto il prodotto di questo algoritmo nessuno è in grado di ricostruire il numero di partenza (chiave privata) che l'ha generato. Tuttavia mediante una semplicissima verifica tutti sono in grado di dire che il risultato è stato derivato da quella specifica chiave privata, come se si trattasse di un'impronta digitale unica, una firma unica.

Il prodotto di questo algoritmo, partendo da una specifica chiave privata, consente quindi di ottenere infinite chiavi pubbliche (che tutti possono vedere).

A loro volta le chiavi pubbliche vengono elaborate da una funzione hash che può generare infiniti indirizzi. Anche in questo caso tutti possono verificare facilmente che uno specifico indirizzo appartiene ad una chiave pubblica, ma partendo dal solo indirizzo, non possono risalire ad essa.

Ecco spiegato perché tutti possono vedere i bitcoin appartenenti ai vari indirizzi verificando che complessivamente vi siano 21 milioni di gettoni nel forziere immaginario, ma solo i rispettivi proprietari possono spenderli. La transazione della chiave pubblica (che tutti possono vedere) è valida solo se firmata della rispettiva chiave privata.

La forza nei grandi numeri sta nel fatto che, se qualcuno volesse provare ad indovinare le chiavi private di un indirizzo, dovrebbe lanciare dei dadi virtuali un numero inimmaginabile di volte, cercando per tentativi di indovinare la combinazione delle chiavi private. Con i computer di oggi questa operazione richiede una spesa energetica incalcolabile visto l'elevatissimo numero di combinazioni da provare ed un tempo di computazione che sarebbe più lungo della storia dell'universo partendo dal Big Bang.[1]

Dato che gli indirizzi non sono altro che un derivato mediante una funzione hash delle chiavi pubbliche; dato che le chiavi pubbliche non sono altro che un derivato mediante una funzione hash delle chiavi private; dato che queste non sono altro che un numero grandissimo generato casualmente, appare evidente che l'intero costrutto su cui poggia Bitcoin non è altro che matematica.

Di conseguenza, se "i bitcoin non esistono" non trovandosi in un luogo specifico, ma di fatto coincidono con la conoscenza di un numero grandissimo, che grazie ad un'altra funzione può essere ridotto a conoscere/ricordare 12 parole, mi chiedo: non si tratta forse di libertà di parola?

Possedere bitcoin equivale a parlare, in quanto tutto il processo non è altro che trasmissione di numeri, matematica e messaggi di testo. Il fatto che noi attribuiamo un valore a delle stringhe di testo è un applicativo che abbiamo deciso di dare a Bitcoin per il fatto che ne esistono solo 21 milioni. Ma appena sotto la superficie ora hai visto che Bitcoin non è altro che matematica e trasmissione di messaggi di testo.

E anche se Bitcoin venisse per assurdo bandito, veramente vorresti vivere in un Paese che non consente la libertà di parola? O in un Paese in cui è illegale lanciare in aria una moneta molte volte per creare un numero molto grande, utilizzare delle funzioni matematiche e trasmettere messaggi di testo?

[1] Video di approfondimento: "Quanto è sicura la cifratura a 256 bit" https://youtu.be/S9JGmA5_unY

Bitcoin metterà alla prova le leggi relative alla libertà di parola di tutto il mondo, ponendo in luce quali sono i governi gestiti da tiranni e quali sono i Paesi democratici dove tale diritto è tutelato.

In particolare, proprio riguardo alla libertà di parola lascio un estratto della Costituzione Italiana:

Art 21: *Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione.*

Aggiungo anche il primo emendamento della costituzione degli Stati Uniti:

Emendamento 1: *Il Congresso non potrà porre in essere leggi per il riconoscimento ufficiale di una religione o per proibirne il libero culto, per limitare la libertà di parola o di stampa o che limitino il diritto della gente a riunirsi in forma pacifica e a presentare petizioni al governo per riparare alle ingiustizie.*

PROPRIETÀ FINO ALLA MORTE

Riassumendo i concetti appena visti è possibile, mediante una specifica funzione crittografica, convertire la propria chiave privata (generata in modo random) in una combinazione di 12 parole. Queste parole sono la chiave che consente di firmare le transazioni in modo tale che il network con una verifica immediata sia in grado di validare la legittimità dell'operazione e quindi l'inscrizione nel database. I partecipanti del network Bitcoin possono solo riconoscere che la firma è di una specifica chiave privata, e che quindi ha titolo ad effettuare un'inscrizione nel database per uno o più specifici indirizzi, ma non possono risalire a come sia composta tale chiave.

In Bitcoin la mappa è il territorio e conoscere equivale a possedere. Questo vuol dire che i bitcoin possono essere utilizzati solo da qualcuno che sta custodendo le chiavi private.

Estendendo ancora un po' il concetto: se quelle 12 parole sono custodite nella mia memoria, io e quei bitcoin diventiamo una cosa sola: "*Io sono Bitcoin*".

L'esistenza e la "vita" di quei bitcoin è legata indissolubilmente alla vita della persona che custodisce le chiavi private.