

Valerio Dalla Costa

Villaggio  
***Bitcoin***

L'ALBA DI UNA **NUOVA SOCIETÀ**

basata su una **moneta sana e onesta**

Copyright © 2022 Valerio Dalla Costa

Tutti i diritti riservati.

Questo libro o parte di esso non può essere prodotto o utilizzato in alcun modo senza l'espressa autorizzazione scritta dell'editore tranne per l'uso di brevi citazioni in recensioni.

Autore: Valerio Dalla Costa  
[www.villaggiobitcoin.it](http://www.villaggiobitcoin.it)  
[info@villaggiobitcoin.it](mailto:info@villaggiobitcoin.it)

Revisione: Giacomo Zucco

Copertina: Matteo Ducoli

Codice ISBN: 9798792600638

## **A Roberto**

Papà, anche se non sei mai stato in realtà un grande lettore, da lassù  
però gliela darai una sfogliata al libro... vero?



# INDICE

PREFAZIONE – Come nasce la magia	1
INTRODUZIONE	5
PARTE 1 – UNO SGUARDO AL PASSATO	15
<b>CAPITOLO 1 - LA MONETA NELLA STORIA</b>	<b>17</b>
Prime forme di denaro	20
I metalli preziosi	25
La moneta rappresentativa	29
La moneta fiat	35
Un possibile piano ß	41
<b>CAPITOLO 2 - L'AVVENTO DI BITCOIN</b>	<b>45</b>
Le origini: perché?	47
Le origini: come?	60
Le origini: chi?	65
Le origini: cosa?	68
Le origini: quando?	72
La nascita di Bitcoin	78
Storie di ordinaria rivoluzione	85

<b>PARTE 2 – NEL CUORE DELL’ORO DIGITALE</b>	<b>99</b>
<b>CAPITOLO 3 - IL PROTOCOLLO BITCOIN</b>	<b>101</b>
Come funziona l’oro digitale	107
Le transazioni passo dopo passo	111
Caratteristiche della blockchain	137
Tutta una questione di incentivi	144
La struttura di una transazione	148
<b>CAPITOLO 4 - IL WALLET</b>	<b>155</b>
Il concetto di portachiavi	157
Tipologie di wallet	172
Buone prassi di sicurezza e privacy	183
<b>CAPITOLO 5 - LIGHTNING NETWORK</b>	<b>193</b>
Il problema della scalabilità	194
Principi di funzionamento	203
Bitcoin e Lightning Network	212
<b>PARTE 3 – PENSIERI DAL VILLAGGIO</b>	<b>219</b>
<b>CAPITOLO 6 - LA MIGLIOR MONETA DI SEMPRE</b>	<b>221</b>
Le proprietà di una buona moneta	223
La forza degli effetti network	239
Rivoluzione senza leader	244
<b>CAPITOLO 7 - COME AVVENGONO I CAMBIAMENTI</b>	<b>249</b>
Modelli rovesciati	250
Bitcoin revolution	258
Il rapporto con imprese e istituzioni	263
Tempistiche di adozione	269
<b>CAPITOLO 8 – QUANTO VALE BITCOIN?</b>	<b>285</b>
Domanda e offerta	287
Alla ricerca della scarsità	292
Il valore dell’oro digitale	294

<b>CAPITOLO 9 - PRINCIPIO DI NON AGGRESSIONE</b>	<b>305</b>
Tecnologia opt-in	306
Una moneta etica e inclusiva	308
Il miglior voto contro le guerre	312
Denaro e preferenza temporale	322
Privacy e libertà	331
<b>CAPITOLO 10 - DOMANDE E RISPOSTE</b>	<b>343</b>
1. Bitcoin viene usato dai criminali?	344
2. È davvero energivoro e un pericolo per l'ambiente?	348
3. Chi c'è dietro Bitcoin?	360
4. Come si inquadra nel sistema fiscale?	365
5. Perché mai dovrei informarmi su Bitcoin?	375
CONCLUSIONI – Un Grande Filtro	379
RINGRAZIAMENTI	383
BIBLIOGRAFIA	385
INFORMAZIONI SULL'AUTORE	391





# **PREFAZIONE**

## **COME NASCE LA MAGIA**

29 marzo 2014.

Ricordo perfettamente la prima volta che sentii parlare di Bitcoin nella mia vita. Mi trovavo in una cascina in mezzo al bosco in Vallecamonica, in provincia di Brescia, che avevo affittato per un weekend. Con me c'erano tanti amici, invitati per festeggiare la mia fresca laurea, conseguita pochi giorni prima. Tra grigliate, aperitivi, musica e chiacchiere, ecco che sentii citare da un mio amico per la prima volta il termine *Bitcoin*. Che subito mi incuriosì tantissimo. Bitcoin... *Bitcoin?* Bitcoin.

Una moneta nativa di Internet? Slegata dall'attuale sistema economico e finanziario? In grado di funzionare da sola?

Suona bene! *Bitcoin...*

Ero da tempo molto critico sulla modalità con cui viene gestito oggi il sistema dell'euro e in generale della moneta fiat, gestita in monopolio e a corso legale dalle banche centrali. Tema sul quale mi ero informato – per mera curiosità - negli anni precedenti.

Una nuova moneta elettronica a livello globale, quindi? Con il potenziale di proteggere i risparmiatori dall'inflazione e di tutelare la privacy? Decentralizzata e basata su un network che non richiede alcuna fiducia in un intermediario?

L'idea era senz'altro stimolante, ma al momento non approfondii più di tanto anche perché, al tempo, non vi era praticamente nulla in termini di contenuti informativi, specialmente in Italia.

Passarono solo pochi mesi quando mi imbattei in un video in rete di un imprenditore che, in circa un quarto d'ora, presentò a grandi linee il fenomeno Bitcoin.

Apriti cielo.

Fu amore a prima vista.

«*Ma potrà davvero funzionare sta roba?*». Le incredulità del caso, condite da una buona dose di scetticismo iniziale, furono ben presto soppiantate da tanta, tantissima meraviglia, dando inizio ad un periodo di studio matto e disperatissimo (si fa per dire) per ricercare fonti, testi, blog, siti di ogni tipo. Tutto quel che poteva fornirmi ulteriori dettagli e informazioni sul tema era preziosissimo per soddisfare la mia curiosità.

Non c'erano molti siti italiani, al tempo. Pochi, alcuni ben fatti (e che ringrazierò per sempre), altri meno utili o incompleti, se non fuorvianti. Le mie ricerche mi portarono ad informarmi pertanto anche e soprattutto tramite blogger e siti stranieri, da tutto il mondo.

Imparai velocemente a scaricarmi il mio primo *wallet* (portafoglio elettronico) e ad iscrivermi ad un *exchange* (piattaforma di compravendita), provando così a comprare qualche spicchio. Nel giro di poco tempo capii come fare per acquistare e gestire al meglio i miei primi bitcoin. Un processo che dura tuttora, in un mondo in continua evoluzione, tanto complesso quanto affascinante.

Ma soprattutto ricordo tuttora – come fosse ieri - lo stupore e l'emozione che provai nel vederli accreditati sul mio primo wallet personale. In realtà, queste sensazioni subentrano ancora oggi, ogni volta che ricevo o invio fondi in bitcoin.

Sì, perché allora come oggi ritengo il fenomeno molto più grande di un semplice protocollo informatico, di un network o di una moneta elettronica (sappiate che Bitcoin è tutte e tre le cose contemporaneamente).

Bitcoin è un formidabile quanto inaspettato strumento di libertà.

Un nuovo paradigma, completamente indipendente e slegato dall'attuale sistema economico, finanziario, sociale e politico. Una sorta di universo parallelo, a sé stante, dove viene mostrato possibile un nuovo stile di vita. Sono dei nuovi occhiali con cui osservare, da un punto di vista inedito, la realtà che viviamo, la società, le dinamiche lavorative, i rapporti tra le persone. Tutto.

Bitcoin abbraccia ogni aspetto della nostra vita. Ci costringe a rimettere in discussione tutto quel che oggi ci sembra scontato e "ovvio". A partire dal concetto di moneta, di privacy, di libertà degli individui, di importanza e gestione del proprio tempo, dei propri risparmi, del proprio lavoro. Della propria vita.

Bitcoin ha aperto il vaso di pandora. Ha spalancato infinite opportunità ed incentivato creatività, progetti e idee a non finire. Con la scoperta di Bitcoin, tutto il resto è diventato, tutt'a un tratto, poco o per nulla interessante.

Dopo anni di studio ed approfondimenti – ed altrettanti che mi aspettano a venire - ho trovato una sola parola in grado di sintetizzare e descrivere quello che Bitcoin rappresenta, almeno per me.

Bitcoin è *felicità*.

Buona lettura.



# INTRODUZIONE

Capire Bitcoin è estremamente difficile.

Tutte le novità, in realtà, non sono mai inizialmente semplici da comprendere e da assimilare. Con questa tecnologia, per certi versi, questo aspetto risulta ancora più accentuato.

Anzitutto, per la prima volta va ad intersecare ambiti che, fino ad oggi, erano rimasti sostanzialmente scorrelati ed indipendenti tra di loro. Fino all'invenzione di Bitcoin, queste tematiche erano alla stregua di compartimenti stagni, isolati, a sé stanti, di competenza degli addetti ai lavori specializzati, ma questo nuovo sistema li ha intersecati ed uniti, dando vita ad un protocollo informatico decentralizzato che implementa una moneta elettronica.

Sono sostanzialmente quattro gli ambiti principali che Bitcoin fonde tra loro: la crittografia, lo studio dei sistemi informatici distribuiti (reti di computer), la teoria dei giochi e le teorie monetarie ed economiche. Descriviamole brevemente, per inquadrare meglio ciò di cui stiamo parlando.

- **Crittografia**

Come indica il nome (dal greco *kryptós* “nascosto” e *graphía* “scrittura”), la crittografia è una disciplina che si pone lo scopo di

nascondere il contenuto di un messaggio. Si tratta di un insieme di tecniche che consentono cioè di trasmettere un messaggio mantenendolo segreto a tutti, tranne alle persone che possiedono le chiavi per decifrarlo.

La crittografia fa riferimento ad una disciplina antica in uso già presso i greci e i romani, come ci testimonia, ad esempio, intorno al 120 d.C., Svetonio nella sua opera *De Vita Caesarum*. Lo storico racconta che Giulio Cesare era solito utilizzare dei codici di cifratura per trasmettere le sue comunicazioni mantenendone la riservatezza nei confronti dei suoi messengeri. Si trattava di combinare le lettere dell'alfabeto, sostituendole con altre lettere secondo una precisa logica: così facendo il testo del messaggio risultava completamente insensato agli occhi di chi lo voleva interpretare, ma non per il destinatario, il quale era a conoscenza della chiave per decifrare quel contenuto. In questo modo era possibile mantenere la riservatezza delle informazioni.

Questo esempio banale riguarda naturalmente una tecnica crittografica primordiale e facilmente scardinabile, ma conteneva già i due elementi fondamentali di un codice di cifratura:

- l'*algoritmo*, ovvero la regola con cui viene modificato il messaggio originale, rendendolo criptato (o cifrato);
- la *chiave*, vale a dire il parametro che permette di decodificare (o decifrare) il messaggio.

Con lo sviluppo dell'informatica e dei processori di calcolo la crittografia ha conosciuto grandi sviluppi, in particolare applicata all'ambito della sicurezza informatica e in tutti i casi in cui è richiesta confidenzialità dei dati. Ad esempio, la troviamo oggi nei messaggi e nei file presenti su supporti di memorizzazione, nelle procedure di login per l'accesso ad un sito o ad una piattaforma (per crittografare la password dell'utente), nelle transazioni finanziarie-bancarie (home-banking) oppure nelle comunicazioni wireless (Wi-Fi e reti cellulari).

Bitcoin utilizza una crittografia di tipo asimmetrico, chiamata anche crittografia *a chiave pubblica*, che utilizza chiavi diverse per cifrare e per decifrare un messaggio. C'è una chiave per cifrare (la chiave pubblica, che chiunque può vedere) e una per decifrare (la chiave privata, che conosce solo il destinatario) senza quindi necessità di scambiare questa frase tra mittente e ricevente.

Bitcoin, in realtà, vedremo che non usa questa tecnologia per cifrare, ma per firmare e per verificare le firme, usandola al contrario: la chiave privata in possesso del mittente viene impiegata per firmare il messaggio, mentre la chiave pubblica per verificare le firme.

La crittografia riguarda una disciplina davvero affascinante e tuttora in continua evoluzione. Il termine “criptovaluta” dovrebbe fare riferimento proprio al fatto che la valuta bitcoin sia basata su alcune primitive crittografiche.

- **Studio dei sistemi informatici distribuiti**

In informatica, quando si parla di *computer networking* (“reti di computer”) si intende l’insieme delle reti di telecomunicazione caratterizzata da un insieme di dispositivi hardware: in poche parole, di sistemi informatici distribuiti.

Con l’avvento di Internet globale, il World Wide Web è diventato rapidamente il tipo dominante di rete di computer, consentendo alle persone di tutto il mondo di utilizzare la rete per l’e-commerce, le applicazioni interattive, le piattaforme informatiche, la telefonia, la posta elettronica ed altro ancora. Di conseguenza, lo studio delle reti di computer è ora praticamente sinonimo dello studio di Internet e delle sue applicazioni, avendo soppiantato – di fatto - protocolli e architetture informatiche non più rilevanti.

In quanto moneta digitale nativa di Internet, al fine di apprezzarne alcune dinamiche Bitcoin richiede pertanto qualche conoscenza di base anche in questo campo.

- **Teoria dei giochi**

Le origini della teoria dei giochi sono riconducibili al lontano 1654 e a Blaise Pascal e Pierre de Fermat con la loro analisi sul calcolo delle probabilità al gioco d’azzardo. La teoria nella sua veste attuale è attribuita a John von Neumann e Oskar Morgenstern con la pubblicazione di *Theory of games and economic behavior* nel 1944, oltre che ai contributi di studiosi di spicco come John Nash, premio Nobel per l’economia per le sue ricerche in questo campo, a cui è stato anche dedicato il film di successo *A Beautiful Mind*.

La teoria dei giochi fa riferimento ad un metodo matematico che permette di studiare i comportamenti umani in situazioni di interazione strategica, mirati al guadagno di ciascun individuo. Si tratta di una disciplina che analizza l’interazione tra gli individui e il loro processo decisionale in un contesto specifico, mediante una rappresentazione matematica dei comportamenti umani in speciali circostanze, in cui determinati incentivi e condizioni possono portare a risultati prevedibili da parte dei giocatori.

Tipicamente, all'interno di un gioco possiamo trovare tre elementi fondamentali:

- *Giocatori*: sono coloro che prendono le decisioni. In sostanza, si intendono i partecipanti.
- *Strategie*: sono le azioni che i giocatori sono autorizzati ad eseguire, tenendo in considerazione tutte le possibili scelte possibili da parte degli altri partecipanti.
- *Risultati*: sono il frutto delle strategie scelte dai vari giocatori. I risultati possono essere previsti su basi matematiche secondo una logica di meccanismi di incentivi.

Una delle applicazioni più famose della teoria dei giochi è il cosiddetto *dilemma del prigioniero*, dove i risultati matematici e razionali che emergono negli esiti possono essere talvolta controintuitivi.

Questa disciplina non si applica tuttavia solo a concetti astratti. La teoria dei giochi permette infatti alle grandi imprese, ad esempio, di prendere delle decisioni strategiche ed economiche sulla base di eventuali e possibili azioni di concorrenti di mercato.

Oppure può descrivere altrettanto bene la cosiddetta “corsa agli armamenti” negli anni ‘50 da parte degli Stati Uniti e URSS durante la guerra fredda. In questo caso, i giocatori sarebbero le potenze economiche mondiali e le strategie sarebbero le opzioni “armare” oppure “disarmare”. La teoria dei giochi infatti spiega facilmente come, per entrambe le nazioni, ricorrere agli armamenti fosse la strategia dominante, benché il risultato finale non fosse ottimale per nessuno dei due partecipanti.

Per le dinamiche di Bitcoin, la teoria dei giochi ricopre un ruolo vitale. Costituisce una delle ragioni per cui il sistema può reggersi e svilupparsi in modo decentralizzato, senza la presenza di un coordinatore centrale. Questo avviene tramite un meccanismo di incentivi in grado di mantenere il network sicuro e sostenibile, dove da una parte vengono premiati gli attori onesti e dall'altra parte i comportamenti disonesti, mirati a danneggiare il sistema stesso, sono resi sempre più difficili e sconvenienti dal punto di vista economico.

- **Teorie monetarie e economiche**

Bitcoin è una moneta elettronica. Diventa pertanto imprescindibile avere un minimo di infarinatura anche sui principi di funzionamento dell'economia e della finanza. Al fine di capire la portata di questa



tecnologia, conoscere almeno le principali teorie passate e presenti, ed avere un'idea di massima sul funzionamento dell'attuale sistema bancario e creditizio, risulta indispensabile. Si tratta in ogni caso di temi molto complessi, dove la letteratura è sterminata e dove le teorie economiche dominanti sono molto ampie e spesso discordanti tra loro.

In particolar modo, diventa imprescindibile capire cosa sia effettivamente la moneta, oltre che il ruolo centrale che questo strumento ha - e che ha sempre avuto - all'interno delle civiltà di ogni epoca. Tema oggi ancora profondamente sconosciuto e sottovalutato, ma che Bitcoin ha finalmente costretto a rimettere in discussione, dimostrando come la forma di denaro adottata costituisca, nei fatti, le fondamenta sulle quali poggia qualsiasi società.

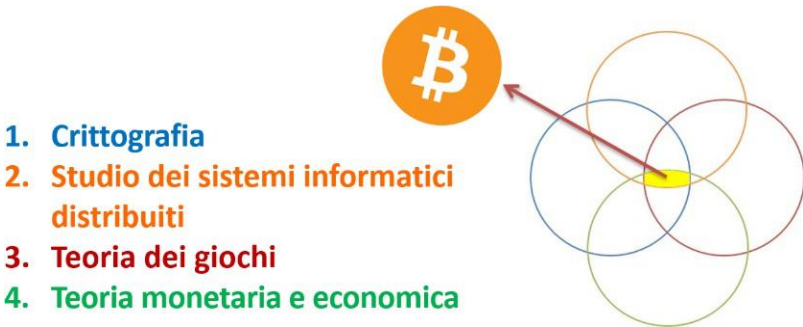


Figura 1. Bitcoin si trova all'incrocio di quattro principali ambiti tematici.

Questi quattro ambiti rappresentano - potremmo dire - l'ossatura della tecnologia. Bitcoin è probabilmente difficile da capire e da interpretare anche per questo: pochissime persone al mondo possono vantare di avere conoscenze e competenze approfondite su ognuno di questi quattro ambiti. La maggior parte delle persone può essere esperta e specializzata su uno di questi temi. Al limite forse due. Ma dal momento che non conoscono quasi nulla degli altri ambiti, gli esperti settoriali spesso non riescono a cogliere appieno la portata del fenomeno che stanno osservando, poiché la loro prospettiva è limitata solamente ad un ristretto punto di vista.

Per fare qualche esempio, esistono grandi esperti e luminari di economia e politica al mondo, che tuttavia sanno poco o nulla di crittografia e di reti distribuite informatiche: molti di loro faticano pertanto a cogliere l'essenza di Bitcoin e a capire il suo funzionamento decentralizzato e delle regole ferree del suo protocollo informatico.

Oppure, la maggior parte dei programmatori, seppur esperti nella scrittura di software, mostrano in genere di avere scarsa o nulla consapevolezza in merito alle teorie economiche e monetarie. Pur interpretando correttamente la parte tecnologica di Bitcoin, non riescono spesso ad apprezzarne l'enorme potenziale dal punto di vista sociale, politico e filosofico.

Insomma, per poter capire almeno l'essenza di quel che sta accadendo in questi anni risulta necessario avere una visione d'insieme, sforzandosi di considerare contemporaneamente tutti i diversi ambiti in gioco. Solo così appare realmente possibile cogliere le novità, apprezzare il valore di questa tecnologia rivoluzionaria ed intuirne le enormi potenzialità.

Data l'infinità delle informazioni necessarie e la complessità di tutti i temi che Bitcoin va a toccare (praticamente tutti quelli inerenti alla nostra sfera privata e sociale), risulta tuttavia molto difficile riuscire a sintetizzare il tutto in poche righe di testo divulgativo. Anzi, a dir la verità, appare proprio come impresa impossibile. Il tema è completamente nuovo, molto complesso, troppo vasto, infinitamente ampio. Un pozzo senza fondo, una sorta di vortice da cui, una volta entrati, non è più possibile uscirne. Dove più ci si informa e più ci si rende conto di quanto poco sappiamo e di quanto ancora dovremmo conoscere.

### **FINALITÀ**

La scoperta di Bitcoin rappresenta l'inizio di un vero e proprio percorso di formazione individuale. Per molti Bitcoin viene scoperto a piccoli passi: all'inizio magari lo si inquadra sotto una cattiva luce, oppure lo si prende poco sul serio vedendolo come uno svago, un passatempo, un giocattolino per speculatori. Poi lentamente si intuisce che vi è qualcosa di molto più profondo che si cela, silente, dietro questa innovazione.

Questo percorso di formazione deve in ogni caso iniziare da qualche parte. L'idea di questo libro nasce proprio in quest'ottica: provare ad offrire ai lettori un'introduzione generale all'universo Bitcoin, cercando di aiutare le persone a capire questa tecnologia destinata a rivoluzionare la nostra società.

In questi anni di studio, sicuramente lo strumento più importante che ha contribuito alla formazione dell'autore è arrivato dalla lettura di libri. Leggere obbliga infatti le persone a fermarsi e a prendersi il tempo necessario per riflettere. Costringe ad essere parte attiva rispetto alle righe

che si trovano davanti ai nostri occhi. Costringe il lettore a mettere in moto ragionamenti, a sollevare nuovi dubbi, a immaginare nuove soluzioni e a sviluppare un sano pensiero critico. Che è esattamente quello che occorre per riuscire ad afferrare appieno questa nuova tecnologia.

Questo testo divulgativo nasce pertanto con l'idea di fornire un quadro complessivo e per quanto possibile completo su questa affascinante innovazione. L'intento è quello di cercare di abbracciare un po' tutti i principali aspetti che Bitcoin va a toccare per provare a fornire un quadro generale - il più possibile logico e coerente - da cui iniziare il proprio percorso formativo individuale. Con la speranza di innescare l'interesse e il dibattito intorno al cambiamento epocale a cui stiamo assistendo da anni.

Specialmente nel momento in cui è nata l'idea di un *Villaggio Bitcoin*, un ufficio/negozio fisico situato nelle valli bresciane e bergamasche dove le persone possano avvicinarsi e "toccare con mano" una rivoluzione ancora ampiamente sottovalutata. Lo scopo di un punto fisico incentrato su una moneta digitale come bitcoin è quello di incontrarsi e di condividere, con tutte le persone interessate, lo stupore e la meraviglia continua che questa tecnologia, destinata a cambiare profondamente la nostra vita, ogni giorno irradia.

## **STRUTTURA, DESTINATARI E REQUISITI**

Il libro risulta strutturato in tre parti distinte – parte narrativa, parte tecnica e parte di analisi/riflessiva - pensate per risultare abbastanza indipendenti l'una dalle altre. Ciò significa che potrebbero anche essere considerate separatamente, senza inficiare troppo la comprensione generale del testo.

### **PARTE 1. UNO SGUARDO AL PASSATO**

In questa parte, prevalentemente narrativa, si ripercorre il ruolo che la moneta ha ricoperto nella storia dell'uomo, fino all'attuale sistema della moneta fiat. Per poi raccontare e descrivere come ha avuto origine la tecnologia Bitcoin: dalle motivazioni, ai primi esperimenti, alle problematiche tecnologiche che si sono dovute affrontare, al lancio del network e ai primi anni del suo sviluppo. Una sorta di cronaca storica con fatti, personaggi e vicende che hanno portato alla nascita del fenomeno che oggi conosciamo.

## **PARTE 2. NEL CUORE DELL'ORO DIGITALE**

Nella seconda parte, più propriamente tecnica, si passa ad esplorare il funzionamento generale dell'ecosistema Bitcoin, illustrando le tecnologie sottostanti. Si affrontano le dinamiche della blockchain, dell'algoritmo della proof-of-work, dell'importanza dell'attività di mining, illustrando come possano avvenire le transazioni all'interno di un sistema decentralizzato e disintermediato, senza che i partecipanti del network debbano fornire dati sensibili o riporre fiducia in un ente centrale.

Viene poi affrontato il concetto di wallet bitcoin, fondamentale per gli utenti per conservare e gestire, in piena autonomia, i propri fondi. Per concludere infine con alcune dinamiche future e possibili sviluppi tecnologici sui quali si sta focalizzando lo sviluppo in questi anni. Tra tutti, il protocollo Lightning Network, pensato per risolvere l'annoso problema della scalabilità e per ottimizzare gli scambi nel quotidiano.

## **PARTE 3. PENSIERI DAL VILLAGGIO**

Nell'ultima parte, più di analisi e riflessiva, si vanno a considerare alcuni aspetti di questa tecnologia che si ritiene possano avere degli impatti decisivi nell'evoluzione della nostra società. A partire dall'analisi delle caratteristiche di una buona moneta, passando dal considerare come vengono percepiti i grandi cambiamenti agli occhi delle persone, soffermandosi sul concetto di valore e sulle dinamiche legate al prezzo di bitcoin nel tempo.

Si avanzano poi riflessioni sulle conseguenze dell'adozione della tecnologia nell'ambito delle relazioni sociali e dei comportamenti degli individui, ma anche su temi sempre più attuali come la privacy, la tutela dell'ambiente, le guerre o il tema fiscale. Infine, si prova a rispondere ad alcune domande tipiche che una persona, di fronte a situazioni nuove e mai sperimentate prima, può ritrovarsi a sollevare.

Il tutto è orientato a descrivere e ad immaginare gli impatti sociali, politici e filosofici che Bitcoin sta portando in tutti gli ambiti della nostra società.

Il taglio è prevalentemente divulgativo, pensato sia per le persone che si avvicinano per la prima volta a questo nuovo mondo, cercando un punto di partenza da cui iniziare per informarsi, sia per tutti quelli interessati ad approfondire ed esplorare il tema Bitcoin nelle sue molteplici sfaccettature.

In bibliografia sono riportati alcuni tra i testi, le fonti ed il materiale informativo che si ritengono rilevanti e significativi per approfondire tutti gli ambiti trattati o citati solo marginalmente.

I requisiti necessari per approcciarsi a questo testo riguardano, anzitutto, l'interesse e la curiosità nel voler esplorare nuovi concetti e nuove dinamiche. Ma la sola curiosità, probabilmente, non basta. Appare necessario soprattutto dotarsi di pazienza e di un certo grado di apertura mentale: è soltanto rimettendo in discussione ciò che oggi diamo per "ovvio" e scontato, abbinato ad un sano spirito critico e ad un atteggiamento propositivo verso il cambiamento, che è possibile cogliere appieno l'essenza della rivoluzione Bitcoin.



## **PARTE 1**

### **UNO SGUARDO AL PASSATO**





## Capitolo 1

### LA MONETA NELLA STORIA

Tra i vari aspetti che Bitcoin costringe a rivedere e a rimettere in discussione vi è, anzitutto, la questione su *cosa sia* effettivamente la moneta.

Sì, proprio la moneta, il denaro, i soldi o come si voglia chiamarli. Quelli che utilizziamo tutti i giorni, quelli che scambiamo di continuo con altre persone, quelli che cerchiamo di guadagnare (e in quantità sempre maggiori) durante la nostra vita. Quelli che vengono spesso visti come qualcosa di negativo, legati a episodi di corruzione, a emozioni come l'avidità delle persone, agli egoismi, oppure semplicemente a comportamenti poco apprezzati (avete presente quando ci accusano di essere “troppo attaccati al denaro”?). Insomma, tutta la nostra vita, il nostro lavoro e il nostro tempo sono strettamente legati allo strumento denaro.

Perché dunque inventare una nuova moneta? In pochi sentono la necessità di dotarsi di un'alternativa completamente slegata dall'attuale sistema economico e finanziario.

Al fine di poter comprendere al meglio questo nuovo fenomeno dobbiamo partire inevitabilmente dal concetto di moneta, aprendo una parentesi - neanche troppo breve ma necessaria - sul ruolo che questa

ha avuto nella storia dell'uomo, a partire dalle origini e dalle civiltà primitive. Stiamo infatti parlando di uno strumento che vanta una millenaria evoluzione nella storia dell'uomo: ci sono addirittura alcune fonti che dimostrano come l'invenzione del denaro sia antecedente o concomitante all'invenzione della scrittura<sup>1</sup>.

Per prima cosa, va precisato che la moneta non è altro che una *tecnologia*. Uno strumento ricercato ed inventato dall'uomo per un obiettivo preciso: facilitare la cooperazione all'interno di un qualsiasi contesto socio-economico. Così come la scoperta del linguaggio – permettendo agli individui di comunicare facilmente tra loro per aggregarsi e organizzarsi in villaggi - ha determinato il punto di svolta nell'evoluzione delle civiltà; così anche la moneta - consentendo agli individui di comunicare *valore* – ha da sempre avuto impatti cruciali nella cooperazione e negli scambi commerciali necessari per creare società prospere e durature.

Il denaro è quindi uno strumento inventato dall'uomo e solamente dall'uomo. In particolare, fondamentale non è altro che una sorta di *convenzione sociale*. Ciò che lo caratterizza in modo particolare è l'accettabilità, cioè il fatto che gli individui all'interno di un certo villaggio si mostrano disposti a lavorare o vendere beni e servizi in cambio di un certo oggetto accettato per convenzione.

La cosa curiosa è che questo oggetto usato come mezzo di scambio non prevede un particolare valore intrinseco, di utilizzo diretto. Assume valore solamente come risultato di un implicito accordo che emerge nella società, che si autoalimenta e che si rafforza nel tempo. Il valore della moneta dipende pertanto sostanzialmente dall'*aspettativa* circa le scelte degli altri membri della comunità: tanto più un individuo si aspetta che un oggetto sia accettato come mezzo di scambio, tanto più è probabile che egli stesso lo accetti in cambio di beni o servizi.

Proprio per il fatto di essere il prodotto di relazioni sociali, la moneta ha consentito nella storia di accedere facilmente ad acqua, cibo, cure, sostentamento, costruzione di ripari e utensili di caccia. Mediante questo strumento si sono potuti ottimizzare gli scambi di prodotti e servizi tra persone che non si conoscono e che si trovano al di fuori

---

<sup>1</sup> Escludendo le antecedenti forme di baratto, il primo denaro della storia è da attribuire ai Sumeri. Comparve nel 3000 a.C. nello stesso periodo, luogo e contesto in cui nacque la scrittura e faceva riferimento all'orzo: quantità fisse di grani d'orzo, misurate in *sila*, erano usate come strumento per valutare e scambiare ogni altro bene o servizio. Fonte: *Sapiens*, di Yuval Noah Harari.

della ristretta cerchia di conoscenti.

La moneta deve infatti consentire agli individui di potersi specializzare in determinate competenze, sempre più specifiche. Proviamo ad immaginare se dovessimo occuparci personalmente di procacciare il cibo tutti i giorni andando alla ricerca di qualche animale selvatico, ma anche di recuperare ogni giorno l'acqua da un pozzo al centro del villaggio, di recuperare i materiali necessari per costruire un riparo nella foresta, di acquisire conoscenze e tecniche per erigere una capanna, di studiare per capire come accendere il fuoco e cucinare.

Scambiarsi cibo, beni e servizi era fondamentale per sopravvivere già ai tempi degli uomini primitivi. Una necessità insita nell'ottica della cooperazione ai fini della nostra salvaguardia come specie. Senza lo strumento della moneta, in grado di facilitare gli scambi con i propri simili, le nostre possibilità di sopravvivenza si ridurrebbero drasticamente.

Il denaro si presenta quindi come uno strumento indispensabile per ottimizzare gli scambi commerciali e creare così benessere e prosperità, estendendo i benefici del progresso anche ad altri individui. Serve cioè a facilitare la diffusione di conoscenze, competenze e cultura in aree e confini sempre più estesi. Per un qualsiasi villaggio o società che voglia evolvere, ingrandirsi o prosperare nel tempo e nello spazio, il denaro si configura - in definitiva - come lo strumento basilare e fondante.

In quanto strumento tecnologico, la moneta deve in particolare coprire essenzialmente tre funzioni:

1. *Riserva di valore.* Con questa funzione si intende la capacità di conservare il valore nel tempo. Analogamente ad una batteria, che risulta tanto più idonea quanto riesca a conservare la carica elettrica accumulata senza scaricarsi nel tempo, così una buona moneta risulta tanto più idonea quanto riesca a garantire che il valore immagazzinato non venga diminuito nel tempo. Quando si parla di "bene rifugio" si intende proprio la sua caratteristica di saper conservare il valore negli anni, senza perdere il suo potere di spesa.

2. *Mezzo di scambio.* Lo strumento monetario dovrebbe risultare funzionale da scambiare, sia nel tempo che nello spazio. Per coprire al meglio questa funzione dovrebbe, ad esempio, dimostrarsi facile da trasportare, pratico da dividere in frazioni più piccole, dovrebbe essere fungibile, oltre che semplice da poter verificare per chiunque lo accetti come pagamento.

3. *Unità di conto*. Una moneta adottata da una società diventa unità di conto quando il valore di tutti i beni e i servizi vengono misurati a partire da questa forma di denaro.

Al giorno d'oggi, la funzione di unità di conto mondiale è ricoperta dal dollaro statunitense: tutte le materie prime, i beni di prima necessità oppure lo stesso prezzo di bitcoin vengono misurati a partire dal dollaro, proprio in virtù del fatto che è oggi riconosciuto come unità di conto.

Proviamo allora a schematizzare la storia millenaria della moneta, dalle origini fino ai giorni nostri. Impresa ardua, se non impossibile, da trattare in poche righe. In ogni caso, non vi è la pretesa di essere esaustivi: l'intento è piuttosto quello di offrire un'infarinatura generale sul tema al fine di poter cogliere le motivazioni di questa nuova, affascinante novità chiamata Bitcoin.

**- FINE ESTRATTO -**