ACCETTARE BITCOIN Vers. 1.1

Una guida semplice e completa per principianti

di Alessio Cardella

Indice

Prefazione

Ho voluto scrivere questo libro perché sento di dover essere evangelista di questa magnifica scoperta, per aprire gli occhi a quante più persone possibili sul mezzo di scambio di valore più efficiente e sicuro che l'umanità abbia mai scoperto.

E sì perché come dice Federico Rivi Bitcoin è una scoperta non un'invenzione, l'assoluta scarsità digitale regolata dalla matematica è una scoperta!

Probabilmente ti stai chiedendo perché dovresti perder tempo a leggere questo libro, Bitcoin è un mezzo di scambio nel dark web e non ti va di investire il tuo tempo nello studio di una cosa che non avrà futuro anche perché è un sistema che inquina e non ti permette di "toccare" i soldi.

Se ti rivedi nel pensiero espresso nel paragrafo precedente o in altri luoghi comuni sei proprio la persona giusta a cui è rivolta questa guida.

*Se sei un commerciante devi sapere che **accettare Bitcoin nel tuo negozio è oggi perfettamente realizzabile gratuitamente, istantaneamente e soprattutto a commissioni zero!** Quindi semplicemente perché non offrire questa possibilità in più nel tuo negozio? Sappi che attireresti nuova potenziale clientela disponibile a spendere Bitcoin, questi poi, felici di aver utilizzato la forma più libera e incensurabile di moneta, potrebbero spargere la voce e farti pubblicità a costo zero. Insomma, hai solo da guadagnarci!*

Questa breve guida è destinata a coloro che vogliono affacciarsi a Bitcoin in modo semplificato, poiché ritengo sia possibile studiarlo in modo approfondito, ma la maggior parte della gente non è tecnica e mai lo sarà. Io stesso non mi ritengo un esperto, anzi conosco molte persone più qualificate e più autorevoli a scrivere un libro su questo tema, ma è proprio questo il punto, scrivere un libro senza troppi tecnicismi, da chi ha imparato a muoversi evitando gli errori più comuni, in modo da padroneggiare la tecnologia senza dover conoscere a fondo tutti i processi che ne permettono il funzionamento. Ragion per cui troverete spesso delle semplificazioni che però non inficiano la possibilità di avere un'infarinatura sull'argomento.

Per aiutare il lettore, ho corredato ogni capitolo con un breve riassunto e delle domande e risposte per sciogliere i dubbi più comuni e un indicatore di difficoltà posto ad inizio capitolo che va da 1(semplice) a

3(difficile). Inoltre sono disponibili fonti esterne come link evidenziati in blu per approfondimenti o verifiche, poiché "don't trust verify", ossia non fidarti, ma verifica!

Come dicevo all'inizio faccio questo per passione e voglia di divulgare uno strumento disponibile all'umanità ma che ancora non ha realizzato tutto il suo potenziale, non lo faccio per soldi ma solo perché credo nell'ideale di cui si fa carico. In questo libro, infatti, non troverai nessun consiglio finanziario o di investimento, non si parlerà di predizione di prezzo futuro, né tantomeno di altre criptovalute poiché reputo le stesse una distrazione e una dispersione di energie che potrebbero essere impiegate nello studio di Bitcoin.

Non l'ho sempre pensata così, ma sulla base della mia esperienza, è da un po' che mi rendo conto di aver sprecato tempo e risorse in altro che potrei aver impiegato meglio in Bitcoin, quindi vorrei evitarti se posso tutto ciò.

Bitcoin non è una criptovaluta ma l'unica vera!

1. Brevi Cenni Storici

Difficoltà: 1

Satoshi Nakamoto è lo pseudonimo dell'inventore (o gruppo di inventori) che ha ideato nel 2008 il software di Bitcoin, donandolo definitivamente al mondo nel 2009.

Il periodo storico è quello in cui tra il 2007 e il 2009 si ha lo scoppio della bolla finanziaria trainata dalla concessione senza freni dei cosiddetti mutui subprime negli Stati Uniti, ossia mutui immobiliari definiti ad alto rischio (concessi a clienti con scarse garanzie) che in un altro periodo storico non avrebbero visto la luce, elargiti però con dei tassi d'interesse maggiorati. Tutto ciò alimentò di conseguenza una grande domanda nel mercato immobiliare scatenando un crescente e continuo innalzamento dei prezzi delle case, in crescita, già dai primi anni 2000.

Data l'apparente salute dell'economia americana la FED (Federal Reserve) decise di alzare i tassi di interesse che causarono di conseguenza effetti amplificati sui mutui subprime. Si generarono così insolvenze proprio di quest'ultimi, e a catena anche il fallimento di uno dei pilastri delle società finanziarie americane la Lehman Brothers attiva dal lontano 1850. Questa bancarotta è stata la più importante nella storia degli Stati Uniti causando un buco economico di ben oltre 600 miliardi di dollari.

È proprio questo il contesto economico nel quale venne creato Bitcoin, per offrire un mezzo alternativo al sistema finanziario marcio e pericolante. Il 3 Gennaio 2009, infatti, il blocco Genesi di Bitcoin riporta il testo "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" riferendosi all'articolo del Times che quella mattina trattava le azioni intraprese dal primo ministro inglese per salvare le banche del regno anglosassone.

Ma esiste almeno un altro fattore enzimatico ben più importante e storico che ha scatenato in Satoshi la volontà di donare al mondo la sua invenzione, e questa è la svolta epocale intrapresa dagli USA che tramite il Presidente Nixon annuncia nel 1971 la sospensione "temporanea" del cosiddetto Gold Exchange Standard, revocando di fatto lo standard istituito durante gli accordi di Bretton Woods.

Fino a quel momento infatti era possibile convertire moneta FIAT (monete nazionali a corso legale) in dollari e questi in oro. Dal 1971 quel "temporaneamente" è cementificato ormai come definitivo e la riserva mondiale economica (il dollaro) non è più sostenuta dall'oro.

Ciò significa che il dollaro e di riflesso tutte le monete nazionali (FIAT) non hanno nessun valore!

Da quanto detto si evince come il mondo necessitava già nel 1971 e a maggior ragione nel 2009 un sistema alternativo democratico, incensurabile e immutabile. Oggi, infatti, la stampa di denaro segue regole esattamente opposte, è incontrollata e fa comodo soltanto a pochi, ma ne parleremo meglio in seguito.

Riassunto:

1-Bitcoin viene creato nel 2008 quando la situazione economica mondiale è in crisi;

2-Bitcoin viene creato poiché dal 1971 il dollaro non è più sostenuto dall'oro, quindi non ha più valore intrinseco (anche perché questo viene stampato senza freni dallo Stato americano)

3-Bitcoin è una moneta forte perché non è duplicabile, non se ne possono creare a piacimento, è democratica, incensurabile e immutabile.

Domande e Risposte:

- ***Chi controlla Bitcoin?***
  Bitcoin è stata inventata da un anonimo che lo ha donato al mondo. Bitcoin è un software che è distribuito su tutta la terra (nei capitoli successivi vedremo come) e per questo non è centralizzato come una moneta emessa da uno Stato.
- ***È plausibile un ritorno al Gold Standard?***
  No, almeno finché il dollaro rimane la riserva di valore mondiale, poiché la quantità emessa e il debito pubblico sono impossibili da coprire con le riserve auree degli Stati Uniti.
- ***Perché Satoshi è rimasto anonimo?***
  Satoshi è rimasto anonimo per non essere un punto di attacco. Bitcoin è una spina nel fianco degli Stati che ne vogliono la distruzione poiché antagonista delle monete statali. Avere un fondatore pubblico sarebbe stata una debolezza per Bitcoin a quel punto facile da demolire, inoltre, il parere dell'inventore avrebbe potuto influire sulle decisioni e il corso democratico della moneta.
- ***È possibile che Bitcoin sia una truffa?***
  Bitcoin non è una truffa per diversi motivi che vedremo in questo libro, ma diciamo che le regole matematiche che lo governano sono pubbliche, poiché il codice è libero e verificabile da

chiunque, inoltre non esiste nessuna entità con un vantaggio economico che ne può modificare le sorti.

2. La Blockchain Di Bitcoin E Il Mining

Difficoltà: 3

Il concetto di Blockchain rappresenta il fulcro principale che sta alla base di Bitcoin, proverò a spiegarlo inizialmente con un esempio per rendere meglio l'idea.

Esempio:

Immaginiamo di trovarci insieme ad altre persone dove lo scopo dell'incontro è riempire un raccoglitore ad anelli con delle ricette. Inizialmente viene distribuito a tutti i partecipanti un raccoglitore vuoto, il primo che riesce a scrivere gli ingredienti per una ricetta vince il premio e ne distribuisce una copia a tutti gli altri. Adesso si ritorna a giocare ma stavolta la seconda ricetta da aggiungere deve abbinarsi alla prima in termini di un fattore che per comodità possiamo dire essere il gusto. Chi trova la soluzione ha il diritto di aggiungere la pagina al raccoglitore e distribuisce una copia anche agli altri, e così via. Ad ogni passaggio l'obiettivo è aggiungere una nuova ricetta che si abbini a tutte le altre. Nel caso uno dei partecipanti decidesse di utilizzare un ingrediente che stona al palato rispetto non solo all'ultima ricetta inserita, ma a tutte quelle già presenti nel raccoglitore, allora questa ricetta non verrà presa in considerazione. Al sistema di controllo troviamo anche dei giudici che possiedono una copia del raccoglitore contenente le ricette fino a quel momento aggiunte. Essi però non spendono energie per ricercare nuove ricette, questi verificano semplicemente che vengano rispettate le regole e possono in modo democratico accettare o rifiutare i fogli aggiunti se non conformi alle regole del gioco.

Il gioco diventa più interessante perché se i partecipanti trovano la soluzione troppo presto (rispetto a un tempo di circa 10 minuti) allora viene aggiunto un fattore di difficoltà maggiore, per esempio oltre l'affinità di gusto bisognerà trovare una ricetta con tutti gli ingredienti che iniziano con la lettera A. Questo induce i partecipanti a utilizzare ogni mezzo tecnologico per trovare la soluzione prima degli altri, per esempio utilizzando Internet dal cellulare o magari dei computer più potenti in grado di trovare la soluzione al problema più velocemente. Questo definito "coefficiente di difficoltà" viene ulteriormente alzato se la soluzione viene trovata in fretta, perché i partecipanti utilizzano tecnologie migliori di ricerca o semplicemente perché aumentano i partecipanti al gioco, che involontariamente innalzano la probabilità e la velocità che almeno uno di loro trovi la soluzione. Allo stesso modo se qualche partecipante decidesse di abbandonare il gioco, perché magari divenuto troppo dispendioso rispetto al valore del premio in palio, allora la probabilità di trovare in fretta la soluzione diminuirà e con questo anche il coefficiente di difficoltà che si riaggiusterebbe.

Adesso proviamo a descrivere la blockchain con i termini e concetti fondamentali ricollegandoli all'esempio precedentemente riportato.

I partecipanti al gioco vengono chiamati *Miners* e hanno il ruolo di aggiungere *blocchi* validi (le pagine di ricette) nella *blockchain* (il raccoglitore) che è effettivamente uno storico di tutte le informazioni fino a quel momento e distribuito a tutti gli attori, ossia Miners e *Nodi validatori* (i nostri giudici).

L'aggiunta di un blocco richiede un certo grado di difficoltà chiamato appunto *coefficiente di difficoltà,* questo viene rivisto dal software in automatico in base ai tempi che sono stati necessari ad aggiungere i precedenti 2016 blocchi. Ogni blocco dovrebbe essere minato ogni 10 minuti, quindi i 2016 blocchi rappresentano circa 14 giorni (6 blocchi l'ora per 24 ore sono 144, 2016 diviso 144 fa 14 giorni)

L'unità di misura della potenza di calcolo della tecnologia a disposizione di tutti i miners è detta *Hash rate*. Semplificando molto, l'*hash* rappresenta una sequenza esadecimale (quindi numeri da 0 a 9 e lettere dalla A alla F in totale 16 caratteri diversi), che mette in relazione univoca da un lato delle informazioni leggibili (tipo la nostra ricetta o l'insieme di tutte le ricette presenti nel raccoglitore) e dall'altro una stringa di lettere e numeri che è l'unica a rappresentare l'informazione leggibile delle ricette, queste informazioni in entrata possono essere le più svariate, mentre in uscita l'hash avrà sempre stessa dimensione in bit.

In Bitcoin il linguaggio di conversione è detto SHA 256 (256 sarebbero i bit) e permette in modo inequivocabile di tradurre del testo (o in generale delle informazioni) leggibile all'umano in un linguaggio comprensibile dalle macchine.

Facciamo un esempio reale:

L'hash della parola "ricetta" con linguaggio SHA256 è sempre:

39761d17241dd9c94dc1166bc9ad609d8ca596c0c048cc9025d49ffca5040a37

Aggiungendo anche un solo carattere, ad esempio "ricetta1" il risultato è completamente diverso:

1bf9ccca7eb20b8e9b9089799b534024c4a9ce8f350bd1d9040ada4cb6047805

Potete voi stessi verificare e testare queste proprietà andando su internet e ricercando "hash generator" si trovano dei siti che permettono queste conversioni e digitando del testo di lunghezza variabile si ha in restituzione l'hash univoco con linguaggio SHA256 con lunghezza fissa.

Questa relazione è alla base della *crittografia*, e in modo analogo vengono protetti anche i dati sensibili quando accediamo al sito della nostra banca, oppure se inseriamo i dati di pagamento su un sito internet per effettuare un acquisto. Semplificando anche in questo caso, noi immettiamo del testo noto (i dati della nostra carta di credito) il provider del servizio non li vede direttamente, ma riceve una conversione univoca, e quindi affidabile e può permettere l'autorizzazione del pagamento. Possiamo definire adesso l'hash rate come la velocità o potenza di calcolo di un miner o di tutta la rete di miner.

Le informazioni scritte nella blockchain blocco dopo blocco sono concatenate e immutabili, poiché chiunque volesse cambiare anche solo un carattere in qualsiasi punto della catena farebbe cambiare tutti gli hash successivi al cambiamento malevolo effettuato. Qui entrano in gioco i validatori della rete e i miner poiché possiedono una copia della blockchain e quindi individuano l'atto malevolo escludendolo dalla rete.

A questo punto possiamo introdurre qual è l'incentivo dei miner a spendere risorse e energie per fare il loro lavoro. La risposta è che lo fanno per soldi, competono infatti nel trovare la soluzione ad un problema matematico prima degli altri in modo da ricevere la ricompensa in bitcoin letteralmente nuovi di zecca. Quando Bitcoin è stato creato (avrete notato che scrivo Bitcoin in maiuscolo quando faccio riferimento al protocollo, in minuscolo invece quando intendo le monete) non esistevano bitcoin circolanti, ma questi lo sono diventati grazie al lavoro di chi ha aggiunto i blocchi alla rete.

Nel 2009 la ricompensa per trovare la soluzione matematica per l'aggiunta di un blocco valido era di 50 bitcoin. Secondo quanto detto prima, in base al coefficiente di difficoltà la soluzione veniva trovata ogni 10 minuti circa e così per i successivi 210.000 blocchi (ossia circa 4 anni) al passare dei quali la ricompensa si è dimezzata diventando quindi 25 nel 2012. Questo continuo dimezzamento delle ricompense ogni 210.000 blocchi è scritto nell'algoritmo di Bitcoin e nella primavera del 2024 porterà le ricompense ad abbassarsi a 3,125 ogni 10 minuti circa e via via così. Questo fenomeno di dimezzamento è definito come *halving* e accompagnerà il cammino di Bitcoin fino a quando l'ultimo bitcoin non sarà minato al raggiungimento dei famigerati 21 milioni totali di bitcoin ossia nel 2140 circa.

Nella Figura 1 è visibile il programma inflattivo di Bitcoin in arancione, in base al numero di blocchi (asse x) e al tasso di inflazione (asse y a sinistra)

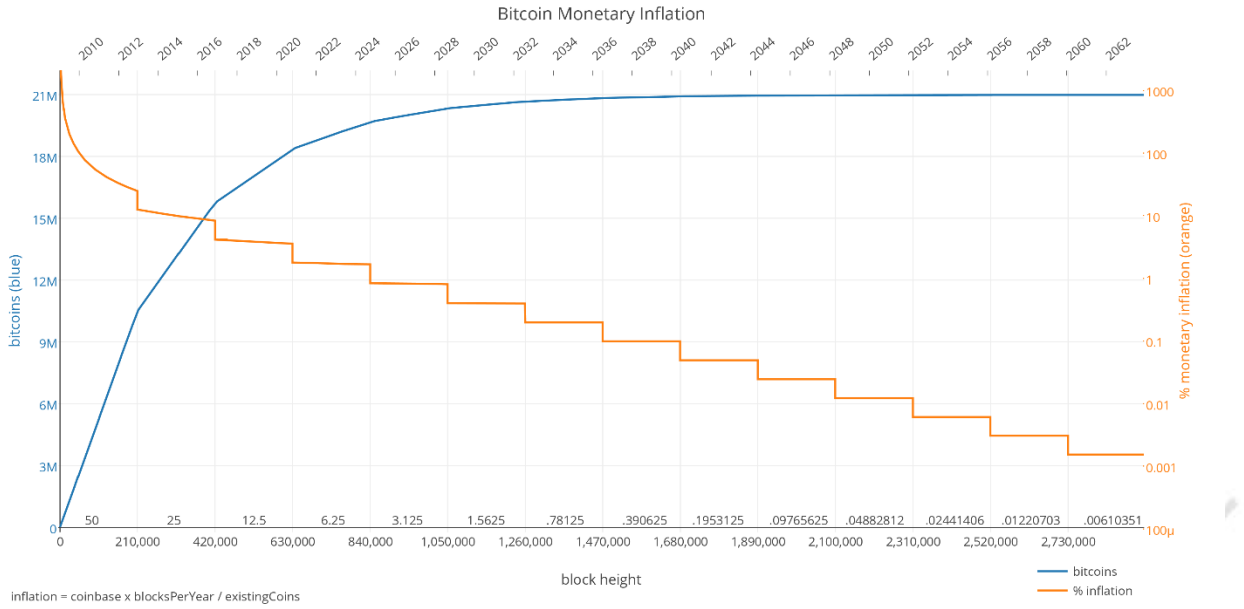

Figura 1

Dalla Figura 1 si può inoltre notare che i bitcoin circolanti oggi (2023) sono più di 19 milioni (linea Blu), e che la scarsità assoluta e programmata dall'halving lascia al domani soltanto 2 milioni scarsi di monete nuove da coniare.

Storicamente il coefficiente di difficoltà tende nel tempo ad aumentare, poiché correlato all'hash rate della rete che tende ad alzarsi, ciò significa che per ogni miner è sempre più complicato trovare la soluzione perché aumentano le macchine destinate al mining diventando, con la tecnologia che avanza, anche più performanti.

In cosa consiste il problema matematico da risolvere dal miner per potersi aggiudicare il blocco per primo?

Abbiamo detto che i miner hanno il compito di aggiungere un nuovo blocco nel minor tempo possibile, alla catena già esistente e immutabile. A tentativi i computer cercano di trovare la prima funzione di hash che colleghi il blocco precedente al nuovo considerando le informazioni in essi contenute, soddisfando però il coefficiente di difficoltà rappresentato dal numero di zeri iniziali presenti nel risultato hash da trovare. I miner aggiungono nel nuovo blocco una stringa per poter ottenere l'hash come da requisito, maggiore è il numero di zero iniziali e consecutivi maggiore è la difficoltà poiché le combinazioni possibili si abbassano esponenzialmente. Dover trovare la soluzione con l'adeguato numero di zeri iniziali richiede numerosi tentativi al miner e rappresenta la prova tangibile della suo

lavoro computazionale, *Proof of Work (letteralmente Prova di Lavoro).* Essendo una testimonianza di un lavoro dispendioso e non da tutti, rappresenta qualcosa di molto raro, e allo stesso modo i bitcoin coniati acquisiscono valore poiché sono il risultato della stessa prova. Questa poi, tende a diventare sempre più dispendiosa nel tempo e insieme all'halving ogni circa 4 anni, fanno sì che i bitcoin estratti nell'arco di quel tempo, diventino sempre più rari e di valore.

Riassunto:

1-La blockchain è una catena di blocchi dove sono contenute tutte le transazioni mai effettuate.

2-Gli attori che regolano il funzionamento di Bitcoin sono i miners, che aggiungono i blocchi contenti le transazioni e i nodi validatori che mantengono sicura la rete controllando che non vengano inserite informazioni non coerenti nella blockchain.

3-Ogni circa 10 minuti un miner vince la possibilità di aggiungere un blocco nuovo alla blockchain e con esso la ricompensa ossia dei nuovi bitcoin così coniati (ogni 4 anni questa quantità si dimezza con l'halving).

4-La prova di lavoro o proof of work rappresenta la testimonianza del lavoro computazionale del miner che ha trovato la soluzione al blocco da aggiungere.

Domande e Risposte:

- ***Perché si dice che la blockchain è immutabile?***
  Perché il cambiamento malevolo anche di una virgola o una cifra in una transazione contenuta in un blocco passato fa cambiare l'hash e quindi viene immediatamente scartata dai nodi generando una catena parallela che non è più di fatto la catena di Bitcoin.
- ***Che differenza c'è fra miner e nodo validatore?***
  Un miner compete con gli altri per trovare la soluzione al blocco da aggiungere nel più breve tempo possibile in modo da ricevere la ricompensa economica in bitcoin. Un nodo invece non ha nessun interesse economico a partecipare alla rete, ma è un controllore della stessa, lo fa inoltre per poter esprimere il proprio diritto di voto o per avere privacy personale.
- ***Cos'è l'hash?***

Una funzione di hash è una correlazione univoca fra delle informazioni in ingresso, come un testo e una stringa di un linguaggio alfanumerica esadecimale (SHA256 in Bitcoin)

3. 21 Milioni

Difficoltà: 2

Nel capitolo precedente abbiamo spiegato come la quantità di bitcoin (BTC) coniati ogni blocco (circa 10 minuti) si dimezza ogni 4 anni per la precisione ogni 210.000 blocchi. Proviamo a fare i calcoli:

50 BTC ogni blocco per 210.000 fa 10.500.000

1°Halving 2012 la quantità immessa ogni 10 minuti si è dimezzata (25 BTC) di conseguenza anche l'inflazione della moneta portando nei successivi 4 anni a 10.500.000:2 = 5.250.000 di nuovi BTC, che sommati ai precedenti diventano 15.750.000

2°Halving 2016 si passa, sempre per lo stesso meccanismo, a 5.250.000:2 = 2.625.000 che sommati ai precedenti diventano 18.375.000

3°Halving 2020 i nuovi BTC sono 2.625.000:2 = 1.312.500 che con i circolanti diventano 19.687.500

Ci aspetteranno altri dimezzamenti delle ricompense ogni 210.000 blocchi, fino ad arrivare all'anno 2140 circa quando l'ultima unità divisibile il satoshi (0,00000001 BTC) metterà fine al processo inflattivo della moneta.

Anno Halving	Ricompensa in BTC	Blocco	Nuova immissione	Tot Circolante	Anno Halving	Ricompensa in BTC	Blocco	Nuova immissione	Tot Circolante
2009	50,00000000	0	10500000,00000000	10500000,00000000	2076	0,00038147	3570000	80,10864258	20999919,89135740
2012	25,00000000	210000	5250000,00000000	15750000,00000000	2080	0,00019073	3780000	40,05432129	20999959,94567870
2016	12,50000000	420000	2625000,00000000	18375000,00000000	2084	0,00009537	3990000	20,02716064	20999979,97283940
2020	6,25000000	630000	1312500,00000000	19687500,00000000	2088	0,00004768	4200000	10,01358032	20999989,98641970
2024	3,12500000	840000	656250,00000000	20343750,00000000	2092	0,00002384	4410000	5,006790161	20999994,99320980
2028	1,56250000	1050000	328125,00000000	20671875,00000000	2096	0,00001192	4620000	2,503395081	20999997,49660490
2032	0,78125000	1260000	164062,50000000	20835937,50000000	2100	0,00000596	4830000	1,25169754	20999998,74830250
2036	0,39062500	1470000	82031,25000000	20917968,75000000	2104	0,00000298	5040000	0,62584877	20999999,37415120
2040	0,19531250	1680000	41015,62500000	20958984,37500000	2108	0,00000149	5250000	0,312924385	20999999,68707560
2044	0,09765625	1890000	20507,81250000	20979492,18750000	2112	0,00000075	5460000	0,156462193	20999999,84353780
2048	0,04882813	2100000	10253,90625000	20989746,09375000	2116	0,00000037	5670000	0,078231096	20999999,92176890
2052	0,02441406	2310000	5126,95312500	20994873,04687500	2120	0,00000019	5880000	0,039115548	20999999,96088450
2056	0,01220703	2520000	2563,47656250	20997436,52343750	2124	0,00000009	6090000	0,019557774	20999999,98044220
2060	0,00610352	2730000	1281,73828125	20998718,26171870	2128	0,00000005	6300000	0,009778887	20999999,99022110
2064	0,00305176	2940000	640,86914063	20999359,13085940	2132	0,00000002	6510000	0,004889444	20999999,99511060
2068	0,00152588	3150000	320,43457031	20999679,56542970	2136	0,00000001	6720000	0,002444722	20999999,99755530
2072	0,00076294	3360000	160,21728516	20999839,78271480	2140	0,00000000	6930000	0,001222361	20999999,99877760

Figura 2

Oggi, (per me il 2023) si trovano circolanti più di 19 milioni di bitcoin, ampiamente oltre il 90% della quantità massima che verrà mai coniata. Molti potrebbero pensare di aver perso un treno negli anni passati, ma in realtà non è così e provo a dimostrarlo.

Si stima che circa il 10% della popolazione mondiale detiene criptovalute e di questi circa la metà possiede BTC. Considerato che il 5% della popolazione mondiale oggi è circa 400 milioni, dividendo in

parti uguali il circolante per i possessori di bitcoin avremo che ognuno ha la possibilità di accumulare al massimo 0,05 BTC.

L'adozione sta aumentando di giorno in giorno e i portafogli contenenti almeno 1 BTC hanno superato il milione, esaminando questo trend crescente che è un indice di aumento di domanda, e il fatto che la fornitura di nuova moneta è regolata dalla matematica che ne impone un'inflazione che si dimezza in modo programmato, ecco che la scarsità delle monete circolanti aumenta.

In parole povere più passa il tempo più aumenta l'interesse delle persone, ma allo stesso tempo le nuove monete coniate sono sempre meno, quindi quelle circolanti sono sempre più scarse e di valore.

Possiamo dunque dire di non aver ancora raggiunto il punto critico di scarsità di approvvigionamento ma potremmo non essere così lontani. La Figura 3 ci mostra la scarsità delle monete di bitcoin (pallini in arancione) in proporzione alla popolazione mondiale, entrambe sono in scala per un fattore di 1milione.

Figura 3

Osservando il fenomeno dal punto di vista governativo, si stima che le riserve economiche di 160 paesi ammontano a circa 13 trilioni di dollari. Molti di questi paesi detengono anche oro, che rappresenta una buona riserva di valore contro l'inflazione monetaria ma che è anche di ardua divisibilità, difficile da conservare e da trasportare. Se questi paesi decidessero di sostituire circa il 3% dell'oro in cassa in bitcoin (750 milioni di dollari in media) ci sarebbe una richiesta di 22.5 milioni di BTC che supererebbe la fornitura massima di 21 milioni.

Riassunto:

1-Esistono massimo 21 milioni di bitcoin, di questi più di 19 milioni sono stati già emessi.

2-Rimangono da essere coniati meno di 2 milioni di bitcoin da oggi fino al 2140 circa.

3-Bitcoin è una risorsa assolutamente scarsa, più dell'oro e se i paesi più industrializzati decidessero di convertire una piccolissima parte delle loro riserve auree in bitcoin, non ce ne sarebbero abbastanza ai prezzi di oggi.

Domande e Risposte:

- ***Come mai non si possono creare più di 21 milioni di bitcoin?***
  L'emissione di bitcoin è regolata dalla matematica e dagli halving che si susseguiranno fino al 2140 decretandone la fine di nuova emissione.
- ***Quanti bitcoin potranno mai essere equamente distribuiti alla popolazione mondiale?***
  0.0025 BTC (21 milioni diviso 8.5miliardi di persone)
- ***Perché gli Stati dovrebbero convertire parte delle loro riserve auree in bitcoin?***
  Per diversificare, ma soprattutto perché bitcoin rispetto all'oro è più facile da conservare e da spendere.

4. Seed, Chiave Privata E Indirizzo Pubblico

Difficoltà: 2

Abbiamo visto che la blockchain racchiude le transazioni degli utenti scritte per sempre nei blocchi, ma cosa permette tutto ciò, come faccio io a trasferire delle informazioni (in questo caso del valore economico) e a dimostrare di avere dei fondi dai quali attingere? Per farla semplice si potrebbe dire che i fondi escono da un portafoglio (wallet) e che ognuno di questi possiede un codice di accesso privato chiamato Chiave Privata. Da quest'ultima poi è possibile generare una chiave pubblica simile all'IBAN di una banca che può essere divulgata al fine di poter ricevere o inviare pagamenti conoscendo l'indirizzo del destinatario.

Andando un pochino nello specifico (ma non troppo) il rapporto fra chiave pubblica e private è dettato dalla crittografia asimmetrica, che permette di determinare la chiave pubblica tramite la chiave privata, ma non viceversa. Il mittente crea un messaggio contenente per esempio il trasferimento economico fra 2 indirizzi, l'autenticità è attestata dalla firma tramite chiave privata e la transazione verso un altro indirizzo viene comunicata ai nodi che ne verificano la conformità e così approda nella Memory Pool, in attesa di essere presa in carico dal miner e inserita definitivamente in un blocco.

Tutto ciò avviene senza intermediari, senza banche ma "semplicemente" diffondendo l'informazione a tutti gli attori della rete, che a loro volta ne verificano l'autenticità, poiché solo chi è in possesso di quella chiave privata avrebbe potuto codificare il messaggio in quel modo, e solo il possessore di una data chiave pubblica poteva decodificare facendo propri i satoshi contenuti nella transazione, tramite l'impiego di decodifica della propria chiave privata.

In parole semplici le transazioni sono messaggi privati e utilizzabili solo da mittente e destinatario, ma che sono però registrate in modo pubblico in blocchi immutabili della blockchain distribuita a tutti i nodi.

La chiave privata essendo una stringa numerica di 256 bit, questa la si può convertire ad esempio in una stringa di numeri romani di 77 cifre, oppure utilizzare una semplificazione molto più agevole.

Grazie a delle proposte avanzate da sviluppatori (esempio nel BIP39) è stato possibile convertirla in una Seed Phrase formata da 12 o 24 parole estratte da un database di 2048 termini inglesi. In questo modo le 12 parole posizionate nell'ordine corretto permettono di ricomporre le chiavi private e di utilizzare il wallet in modo agevole. Una Seed Phrase codifica per un numero grande di chiavi private dalle quali è possibile, uno a uno ricavare un indirizzo pubblico. È come avere le chiavi di accesso al portale della nostra banca (seed phrase) e una volta dentro possiamo vedere tutti i nostri conti correnti con tutti i

saldi (chiavi private) e i loro relativi IBAN (indirizzi pubblici). Le uniche informazioni da condividere dunque sono gli indirizzi pubblici.

E' estremamente importante quindi **non divulgare mai per nessun motivo le parole che compongono la Seed Phrase o le chiavi private** poiché chiunque si trovi in possesso di quell'informazione è in grado di accedere al wallet e spendere i saldi degli indirizzi pubblici da essi derivati.

Ricordarsi prima di effettuare delle transazioni verso un wallet appena generato di aver fatto un backup del seed, e di custodirlo in modo da evitare che possa finire nelle mani di qualcun altro, nel mondo fisico, esempio copia cartacea non idoneamente nascosta o nel mondo digitale, poiché i sistemi cloud ma anche in locale nel proprio PC, rappresentano vulnerabilità in caso di attacco hacker. Una spiegazione più approfondita ma semplice è stata data sul palco 21 durante il Lugano Plan B Forum da Guybrush del Bitcoin Italia Podcast al seguente link trovate il video dove a circa 2h16min dall'inizio ne parla.

Riassunto:

1-Da una chiave privata si genera univocamente un indirizzo pubblico (equivalente all'IBAN di un conto corrente) che è l'unica informazione da condividere con altre entità.

2-Un wallet può essere codificato da una Seed Phrase (12 o 24 parole) dalla quale derivano un numero molto grande di chiavi private.

3-La Seed Phrase e le chiavi private non devono mai essere condivise con nessuno, chiunque le possiede può attingere dai fondi in essi contenuti.

Domande e Risposte:

- ***È possibile che qualcuno abbia la stessa mia Seed Phrase?***
  È praticamente impossibile, se questa è generata casualmente si avrebbe una probabilità più bassa a quella di catturare 2 volte lo stesso atomo nell'intero universo!
- ***È possibile inviare dei fondi da un indirizzo Bitcoin a uno Ethereum per esempio?***
  No, essendo due diverse blockchain, inviare dei fondi da un indirizzo Bitcoin a uno Ethereum significherebbe bruciarli. Gli indirizzi più comuni in Bitcoin iniziano per bc1...mentre quelli Ethereum con 0x.

- ***Posso scambiare le parole della Seed Phrase per ottenere lo stesso wallet?***

  No, scambiando l'ordine delle parole si ottengono wallet diversi.

5. Falsi Miti

Difficolta 1

Quasi tutti oggi possono affermare di aver sentito parlare di Bitcoin almeno una volta nella vita, ma spesso l'associazione che viene fatta è negativa.

Io stesso non ricordo esattamente quando ho sentito dire quella parola la prima volta, ma ricordo di averla accostata a un qualcosa di losco, di illegale ragion per cui non mi sono interessato, ma mi "fidavo" di quella sensazione.

1.Bitcoin è cattivo

La sensazione non era innata in me, ma era stata probabilmente instillata da media ascoltati distrattamente. Andando ad approfondire ci si accorge che Bitcoin è tutt'altro che cattivo, anzi si pone come strumento di libertà finanziaria, spesso soluzione all'iperinflazione nei paesi del terzo mondo. Satoshi Nakamoto, infatti, dona all'umanità un protocollo libero, open source (ossia il codice è leggibile e revisionabile da chiunque) senza trucco e senza inganno.

È vero anche che durante la storia di Bitcoin persone malintenzionate sono riuscite a commettere illeciti nascondendo la propria identità dietro degli indirizzi non associabili a persone per scambiarsi materiale illegale ad esempio. Questo problema è però lo stesso che si ha con il denaro contante, poiché non tracciabile e la stragrande maggioranza di queste azioni di dubbia moralità avviene con questo mezzo.

La verità è che Bitcoin a differenza del contante non è anonimo, ma pseudonimo, poiché le transazioni sono inscritte pubblicamente nel registro distribuito, la blockchain per l'appunto, e quindi sempre rintracciabili. Inoltre, essendo gli indirizzi anch'essi pubblici, è possibile ricostruire la storia dei movimenti effettuati da e verso ognuno di questi dietro al quale si cela un determinato soggetto. Esistono dei metodi per eludere questa tracciabilità come ad esempio i Coin Join, ma questi, non sono argomento di questa guida per principianti.

2.Bitcoin non ha valore intrinseco

Questa presunta criticità viene sollevata da chi non ha studiato come funziona Bitcoin, o da chi pur informandosi non ci ha capito molto. Per risolvere questo dilemma dobbiamo snocciolare alcuni concetti fondamentali. Il valore è da attribuirsi alla scambiabilità che ha un dato asset dettato dalla domanda e dall'offerta. L'oro, per esempio, è un metallo di valore grazie alle sue proprietà fisiche che lo rendono idoneo per la realizzazione di oggetti preziosi, inoltre estrarlo richiede un gran lavoro che diventa

proficuo solo se debitamente ricompensato. La sua più grande virtù è data dalla sua scarsità sulla terra. Se non ci fosse l'oro gli oggetti di valore si produrrebbero con altri materiali e nessuno ne sentirebbe la mancanza. L'oro però non è una pratica merce di scambio perché difficile da frazionare e trasportare. Inoltre, non è essenziale alla vita, ma esso, per esempio, vale più dell'ossigeno che invece lo è. Questo perché l'ossigeno è ampiamente distribuito ovunque nella troposfera terrestre, quindi, il suo valore è abbattuto dalla sua abbondanza, ma cosa succederebbe se questo venisse a mancare? Quanto sareste disposti a pagarlo? Abbiamo toccato quattro temi che sono l'utilità, la scarsità praticità, e il lavoro.

Dando ad ognuno di queste materie un punteggio da 1 a 5 dove 5 è il fattore maggiormente positivo, ho applicato l'esercizio in modo del tutto soggettivo ad alcuni materiali di diverso valore che ritroviamo sulla terra.

	Utilità	Scarsità	Praticità	Lavoro	Risultato
Oro	4	4	2	2	12
Ossigeno	5	1	3	5	14
Acqua	5	3	3	4	15
Dollari	4	1	4	2	11

Vediamo che la matrice da me costruita e soggettivamente compilata dà valori simili ai 4 asset.

Se applico lo stesso esercizio a Bitcoin otterremo: utilità 5, scarsità 5, praticità 4, lavoro 3 con un risultato di 17, superiore a tutto il resto. Per quanto riguarda l'utilità a mio avviso l'uomo ha bisogno in questo periodo storico di una moneta capace di apprezzarsi e non perdere valore nel lungo termine. In termini di scarsità lo abbiamo già affrontato, esistono ed esisteranno solo 21 milioni di bitcoin, battendo anche l'oro a mio avviso poiché non si conoscono le reali quantità sulla terra, nel sistema solare o nell'intero universo. Per la praticità possiamo dire che è la moneta perfetta nel senso che è molto divisibile, è digitale quindi facile da trasportare e permette dunque pagamenti ovunque nel mondo in modo veloce, lo sviluppo si sta concentrando per rendere le transazioni su livelli successivi a Bitcoin istantanee, sicure e a bassissime fee. Tutto ciò è già possibile con Lightning Network che ha ancora margini di miglioramento e che analizzeremo in seguito. In termini di lavoro possiamo dire che il mining è l'esempio perfetto di lavoro che rende possibile una sana competizione e la sua ampia distribuzione garantisce una buona sicurezza del network.

3.Bitcoin inquina

Il lavoro è alla base del prossimo punto riguardante i luoghi comuni. Una delle accuse più persistenti e che si ripresenta ciclicamente è: Bitcoin inquina. Una spiegazione, che ritengo molto efficace e puntuale,

è quella che dà Riccardo Giorgio Frega (Rikki) co-autore del Bitcoin Italia Podcast, un podcast tra i più seguiti in Italia che tratta argomenti inerenti il tema Bitcoin. Lui dice infatti: "*Bitcoin consuma energia, punto. E ne consumerà sempre di più*", poi precisa: "*e noi vogliamo che sia così perché più corrente elettrica consuma più la rete è sicura*". Tutto ciò è assolutamente vero poiché vediamo un continuo aumento dell'hashrate del mining dovuto a una parallela crescita della rete dei miner, permettendo ogni giorno che passa di diventare un network sempre più difficile da attaccare e quindi più sicuro. Spesso si sente dire che Bitcoin inquina come l'Austria, o il Portogallo o qualsiasi altro paese, (ogni tanto cambiano per non essere troppo ripetitivi). Questi complicatissimi studi, essendo delle stime sono solo assunzioni e non certezze. Ognuno di questi, infatti, tiene conto della CO2 emessa in base all'energia elettrica richiesta, ma non prendono assolutamente in considerazione quanta di questa energia è servita da fonti rinnovabili, per esempio, o quanto di queste deriva da energia che sarebbe comunque dissipata nell'ambiente con o senza Bitcoin. Come spiega anche Rikki, l'industria del mining è alla ricerca dell'energia più a basso costo, poiché il loro guadagno è controbilanciato dai soli costi dei computer per il mining e dal costo dell'energia elettrica. Oggi l'industria del mining utilizza energie rinnovabili per un 52% come si legge da batcoinz.com e questa percentuale è in continuo aumento, proprio perché l'energia a basso costo permette loro profitti maggiori. Nella Figura 4 si vede come il mining di Bitcoin ha registrato un incremento percentuale decisamente maggiore nella sostenibilità ambientale con un +38%.

Figura 4

Un'altra fonte di energia a basso costo è rappresentata da quelle aziende che la producono in surplus rispetto al fabbisogno della comunità circostante. Ad esempio, le aziende che producono energia bruciando il gas naturale estratto, non hanno la possibilità di "chiuderlo". Nelle ore notturne quando la richiesta della comunità è più bassa, sono costretti a bruciarlo (Gas Flaring), poiché l'immissione di gas metano nell'atmosfera risulterebbe molto più inquinante della CO2 trasformata dalla combustione, ed è a questo punto che Bitcoin diventa cruciale. I miner sono disposti a comprare quell'energia in surplus a basso costo che altrimenti andrebbe sprecata. In questo caso è vero che Bitcoin sta usando combustibili fossili, ma si tratta di energia proveniente dal gas flaring che sarebbe comunque sprecata.

La corrente elettrica in esubero non può essere conservata, né tantomeno trasportata via cavi, poiché per effetto Joule viene dissipata sotto forma di calore. Teoricamente si potrebbe costruire una distesa di pannelli solari nel deserto del Sahara di 254 km quadrati per soddisfare il fabbisogno energetico dell'intero pianeta dice Nadine May, ma sarebbe inefficiente trasportarla. Quindi ad oggi in qualunque parte del mondo si produca energia elettrica nella qualsivoglia modalità, questa non può essere trasportata per lunghe distanze. In questo senso Bitcoin potrebbe rappresentare una soluzione poiché l'energia prodotta in luoghi remoti può essere convertita come dice Rikki in "*assoluta scarsità digitale*",

ossia dei bitcoin che possono essere trasferiti ovunque nel mondo in modo praticamente istantaneo e a commissioni quasi zero. In questo senso Bitcoin rappresenta una “batteria digitale”.

La necessità dei miner di ricercare energia a basso costo si tramuta in ricerca continua di fonti rinnovabili o di energia in esubero, questo fa sì che Bitcoin rappresenta un grosso incentivo verso lo studio di nuove soluzioni di produzione di energia sempre più sostenibili per l’ambiente. **Bitcoin non rappresenta una sorgente di inquinamento, ma al contrario un incentivo nell’investimento della ricerca e sviluppo di soluzioni ambientali più sostenibili.**

Per concludere il tema, è vero che Bitcoin utilizza tanta energia, ma questa rappresenta oggi lo 0,67% del fabbisogno mondiale (dati dell’Università di Cambridge in tempo reale), che ha un impatto minuscolo rispetto a tutte le altre attività umane. Di questo 0,67%, più del 50% deriva da fonti rinnovabili, e una parte dell’energia proveniente da combustibili fossili è energia in esubero.

Detto ciò, voi rinuncereste a uno strumento di emancipazione finanziaria, di libertà, al metodo più sicuro che abbiamo per scambiare valore ovunque nel mondo in modo praticamente istantaneo senza intermediari e senza censura per uno 0,15% di CO2 immessa all’anno nel mondo?

0,15% rappresentano 76 mila tonnellate di CO2, ma prima di rinunciare a Bitcoin sono disposto a rinunciare alle luci di Natale (20 mila tonnellate di CO2), al video gaming (24 mila tonnellate), Youtube (10 mila tonnellate) o all’industria del tabacco (84 mila tonnellate di CO2). Quindi siamo realisti e non diamo la colpa a Bitcoin per il riscaldamento globale!

4.Bitcoin è volatile

Un altro falso mito è che Bitcoin è un investimento troppo rischioso perché volatile. Questo è quello che mi fa sorridere di più se devo essere sincero, perché proveniente da due possibili cause. Dice così chi è detrattore di Bitcoin, ed è schiavo della propaganda politica degli Stati o dei sistemi finanziari tradizionali, oppure è un giudizio espresso da chi si è bruciato acquistandolo in un periodo di euforia del mercato senza aver studiato, e poi lo ha venduto magari in perdita nel panico quando lo ha visto scendere troppo. Bitcoin andrebbe acquistato solo dopo aver compreso perché esiste e dopo aver recepito un minimo il suo funzionamento.

Proprio per tale motivo esiste questo libro.

Cercherò di affrontare il tema senza parlare del prezzo attuale o di previsioni future, poiché non in scopo e perché non sono abilitato a dare consigli finanziari.

Il prezzo di Bitcoin è il frutto di domanda e offerta come qualsiasi asset di mercato. Essendo relativamente giovane il suo prezzo non si è stabilito, anzi ha avuto delle fluttuazioni abbastanza ampie generalmente cicliche, ma che hanno portato nel tempo a vedere il suo valore crescere. Il rumore di fondo dato da prezzi altalenanti all'interno dei cicli passati è espressione di pura speculazione. Al contrario la media del prezzo tra un ciclo e un altro è frutto di dinamiche basate sui fondamentali dell'ecosistema. In Figura 5 si vede il grafico del prezzo di Bitcoin preso da Coinmarketcap.com in scala logaritmica.

Figura 5

Chiunque, ad esclusione di chi ha comprato nella fase euforica dell'ultimo ciclo rialzista, adesso si trova in guadagno, la pazienza è la virtù dei forti. Anche chi ha comprato in una fase euforica dei cicli passati e ha avuto la capacità di saper attendere, adesso si trova in profitto.

Perché il valore di Bitcoin, che tende nel lungo tempo ad apprezzarsi, è dato dalla sua scarsità come abbiamo già visto nei capitoli passati, ma la sua volatilità nel breve è dovuta anche alla sua piccola capitalizzazione totale. Stiamo parlando del controvalore di tutti i bitcoin circolanti che al momento è di poco superiore a 500 miliardi di dollari, quindi facilmente manipolabile da grosse entità per scopi speculativi.

Bisognerebbe però oltrepassare il pregiudizio mentale che ad un certo punto bisogna tornare alla "realtà" ossia riconvertire i bitcoin in Euro, Dollaro o altra moneta FIAT. Chi acquista Bitcoin lo dovrebbe fare perché cosciente dei valori che rappresenta, e quindi inerte alle fluttuazioni di breve.

1 bitcoin = 1 bitcoin sempre.

Riassunto:

1-Bitcoin non è anonimo come si crede, quindi non è il sistema preferito dai criminali per commettere reati che rimane il contante.

2-Il valore intrinseco di un asset è dato dalla sua fungibilità e da domanda e offerta. Bitcoin ha valore perché rispetta tutte le caratteristiche base che un asset di valore dovrebbe avere: utilità, scarsità praticità, e il lavoro per ottenerlo.

3-Bitcoin non inquina! Bitcoin utilizza tanta energia (circa lo 0,67% di quella mondiale). Di cui, più del 50% deriva da fonti rinnovabili, e una parte dell'energia proveniente da combustibili fossili è energia in esubero. La continua ricerca verso fonti alternative a basso costo da parte dei miner incentiva loro a investire verso il rinnovabile più di qualsiasi altra industria.

4-Bitcoin ha una grande volatilità di prezzo sia verso l'alto che verso il basso poiché è una tecnologia giovane e poco capitalizzata, quindi guidata nel breve da speculatori. Storicamente l'investimento in bitcoin diviene profittevole anche nel peggiore dei casi dopo 4 anni. Rimane il fatto che prima di investire in bitcoin bisogna studiarlo, a quel punto ogni paura svanisce.

1 BTC è sempre 1 BTC!

Domande e Risposte:

- ***Se è vero quanto specificato sopra, come mai esistono ancora delle notizie di testate giornalistiche importanti che affermano il contrario?***
  Bitcoin è una tecnologia scomoda, riporta la sovranità monetaria al popolo. Ma dato che è impossibile da arrestare, l'unico modo possibile per arginarlo è infangarlo utilizzando dati parziali, vecchi, ma anche completamente errati o scopiazzati. Nel penultimo capitolo vedremo anche degli esempi pratici di articoli scritti da pseudo-giornalisti, o direttamente dalla BCE.

- ***Dove è stata presa la matrice che tabella i valori degli asset?***
  È una classificazione di mia invenzione, non è possibile trovarla da altre parti, e i punteggi assegnati corrispondono soltanto al mio parere personale e soggettivo.
- ***Qual è la previsione del prezzo nei prossimi 4 anni?***
  Nessuno è in grado di prevedere il prezzo futuro di bitcoin, né tantomeno io che non sono un consulente finanziario. In ogni caso diffidate da chi vi promette ritorni sicuri, poiché il futuro è incognito, possiamo però esaminare lo storico del prezzo, i fondamentali dietro la tecnologia e l'inflazione programmata sono dati certi, e valgono più di qualsiasi previsione.

6. Differenze Con Il Sistema Tradizionale

Difficoltà: 1

Nel nostro sistema economico troviamo le banche centrali che guidano le politiche monetarie e le banche commerciali che offrono servizi alla popolazione e alle imprese. In mezzo esistono anche dei fornitori di servizi economici come le assicurazioni e i fondi di investimento ad esempio.

Il denaro viene quindi regolato dalle banche centrali (in Europa la BCE e negli USA la FED) tramite immissione di nuova moneta o innalzamento dei tassi di interesse. Loro hanno il potere di diluire il valore del denaro in caso di crisi stampandone altro ed aumentando così la massa monetaria. Questo movimento però abbassa il valore del danaro perché diventa meno scarso causando inflazione. Finché l'inflazione della moneta rimane intorno al 2%, gli economisti la reputano salutare per l'economia. Quindi paradossalmente coniando denaro per la spesa pubblica, migliorando le infrastrutture, si ottiene come conseguenza l'effetto Cantillon. Questo ha come risultato il continuo arricchimento dei ceti sociali vicini alla "stampante" di denaro, ma che alla fine, nella piramide sociale, si tramuta in crescente povertà dei gradini più bassi della società, causando quindi la diminuzione della scarsità del denaro.

Il caso opposto è quando l'inflazione inizia a diventare troppo alta e le banche centrali procedono alzando i tassi di interesse, in questo modo si diminuisce la massa monetaria circolante.

Negli ultimi anni (a partire dalla crisi del 2008) abbiamo visto gli interessi arrivare a zero intorno al 2016, ma nell'ultimo periodo, dopo grandi immissioni di liquidità a seguito della pandemia e della guerra in Ucraina, i tassi hanno subito un'impennata mai vista arrivando a superare il 4%. Questo brusco innalzamento è stato effettuato per bilanciare la crescente inflazione che stava galoppando in modo preoccupante sopra il 10%.

In entrambe le situazioni, sia quando viene stampato denaro, che quando viene imbrigliato alzando i tassi, gli unici a perderci sono i piccoli risparmiatori, che per difendersi in genere si affidano a fondi di investimento. Chi, infatti, non fa qualcosa a protezione dei risparmi, ma li detiene semplicemente in banca, vede deprezzare il gruzzoletto accumulato ogni anno a seguito dell'inflazione positiva. Nel caso opposto, quando vengono alzati i tassi di interesse, il colpo viene maggiormente incassato da chi soldi non ne ha, che si trova in banca a richiede un prestito, o magari si trova a pagare delle rate più alte a causa dei tassi variabili.

In merito ai prestiti, entrano in gioco le banche commerciali che non possono stampare denaro direttamente come quelle centrali, ma possono concedere prestiti generando di fatto nuova liquidità grazie al potente strumento della riserva frazionaria.

Questa consiste nel detenere come riserva soltanto una frazione del denaro depositato dai clienti. In pratica quando si deposita della liquidità in banca, quest'ultima può utilizzarla per concedere un prestito a chi lo richiede, ma la cosa sorprendente è che la riserva da detenere per le banche in Italia è soltanto dell'1%. Questo significa che se ad esempio depositate 1000 Euro, la banca è obbligata a conservare 10 Euro ma il resto lo può prestare. In genere i 990 Euro prestati finiscono nuovamente in una banca che ne presta altri 980. È facile notare come le banche commerciali stiano di fatto creando soldi dal nulla. I piccoli risparmiatori questo non lo sanno, e immaginano di aver depositato i propri risparmi all'interno del sistema più sicuro e solido a loro noto, ossia le banche, ma in realtà quei fondi nella quasi totalità non esistono più. Se tutti i risparmiatori decidessero di ritirare i propri depositi, tutte le banche sarebbero a rischio fallimento. Questo meccanismo è molto simile ad uno Schema Ponzi destinato a crollare! Il premio Nobel per l'economia Maurice Allais disse già nel lontano 1988:

"*L'attuale creazione di denaro dal nulla operata dal sistema bancario, è come la creazione di moneta da parte dei falsari, l'unica differenza che sono diversi gli attori che ne traggono profitto.*"

Che soluzioni porta Bitcoin?

Bitcoin si propone di essere un sistema economico immutabile decentralizzato e trasparente (ma non solo) snocciolIamo i concetti.

L'**immutabilità** è una caratteristica chiave della blockchain di Bitcoin, questa infatti come già descritta in precedenza, è conferita dal fatto che tutte le transazioni storiche, quindi ogni movimento e saldo di ogni indirizzo, sono salvate come informazioni all'interno di qualche blocco inserito nella blockchain. Se un attore malevolo decidesse di modificare qualsiasi informazione già presente nella blockchain, gli altri nodi lo saprebbero e lo escluderebbero. Quindi è praticamente impossibile modificarla, anche grazie alla sua **decentralizzazione**, data appunto da un elevato numero di nodi validatori 16700 circa al momento (quelli raggiungibili) che rendono la rete quanto più democratica possibile e sicura. Chiunque con un computer modesto e un hardisk di almeno un terabyte (conviene stare sui 2 Tb per non doverlo cambiare fra qualche anno), può far andare un nodo sul pc di casa propria. Il concetto di **trasparenza** è strettamente legato agli altri due, poiché è intrinseco nell'immutabilità e nella decentralizzazione. Trasparente significa che ogni transazione è raggiungibile tramite un blockchain explorer. Inserendo infatti in uno di questi l'indirizzo pubblico di un wallet si possono vedere tutte le transazioni storiche e il

saldo. Da qui poi per esempio continuando ad esplorare, si può analizzare una transazione specifica andando a vedere l'importo, l'indirizzo di partenza e quello di arrivo e i rispettivi saldi, e così volendo si possono analizzare tutti i movimenti e i saldi di ogni indirizzo che ha mai movimentato dei bitcoin dal 2009 ad oggi. Per quello si dice che Bitcoin è **pseudonimo** e non anonimo.

Bitcoin è uno strumento di **libertà economica**, immaginate di vivere in Canada durante il periodo del Covid, un paese super civile e democratico a meno che tu sia un camionista che protesta per le restrizioni statali in seguito alla pandemia. Questi, infatti, si sono visti bloccare i conti correnti per aver esercitato il diritto di manifestazione, non solo loro, ma anche tutti coloro che hanno partecipato alla raccolta fondi. Si può discutere sulla moralità della loro protesta, ma non sul esercizio del diritto di manifestazione pacifica. Come scrive il Wall Street Journal "è stato un inutile abuso di potere", aggiungo che è stato probabilmente una prova per testare un metodo di soppressione delle libertà in caso di dissidenza della popolazione. In questo caso Bitcoin, essendo **incensurabile**, ha potuto aiutare quelle persone che in quella situazione si trovavano senza soldi, poiché con una raccolta fondi in bitcoin sono riusciti ad andare avanti.

Lo Stato tramite le banche è in grado di esercitare il potere di congelare i risparmi di chi non la pensa come lui, il fatto è che chi dirige uno Stato non è detto che abbia sempre ragione.

Un'altra caratteristica di Bitcoin è che **non ha confini**, poiché effettuare una transazione dall'Italia all'Italia oppure dall'Italia alla Cina, per esempio, impiega stesso tempo e stessi costi, essendo una tecnologia **peer to peer** (fra pari). La tecnologia peer to peer implica un sistema decentralizzato e diffuso come internet, ma che è anche incensurabile, poiché nessuno è in grado di vietarne l'utilizzo.

A differenza di un sistema centralizzato un sistema fra pari è ingovernabile, in merito a ciò, l'esempio che rende meglio l'idea è quello di Napster. Quest'ultimo è stato a cavallo dell'inizio del 21° secolo un sistema di condivisione di file tramite internet, ma è stato immediatamente censurato e chiuso a causa del fatto che la condivisione dei file non era regolata e venivano condivisi senza concessione dei diritti d'autore, portando sotto i riflettori il termine di pirateria. Il sistema peer to peer si è successivamente evoluto portando alla nascita dei torrent, Emule ecc. Questi a differenza del primo rispondono al concetto di peer to peer puro, senza server centralizzati di facile censura. È praticamente impossibile per gli organi regolatori censurare ogni utilizzatore della rete di un torrent, allo stesso modo bloccare i nodi della rete Bitcoin dislocati in tutto il mondo.

Esistono persone provenienti da paesi del terzo mondo che dopo aver attraversato mari e confini, giungono verso terre più fertili per poter guadagnare qualche spicciolo da mandare alla famiglia

residente nel loro paese d'origine, questo è il fenomeno delle rimesse. I metodi per far arrivare loro il denaro sono i sistemi bancari internazionali, ma spesso in un paese povero la gente non ha accesso ad un conto in banca, oppure si utilizzano dei servizi di money transfer come Western Union o MoneyGram. L'utilizzo di questi però implica un'alta commissione, (tra il 10 e il 20%) e il fatto che bisogna versare e prelevare la somma in presenza. Capite bene che per una persona che abita in un villaggio sperduto in Africa diventa difficoltoso camminare a piedi fino alla città più vicina dove è situato l'ufficio per il prelievo, luogo di ritrovo ideale per malviventi che non attendono altro. Bitcoin rappresenta dunque una soluzione alternativa anche a questo problema.

Riassunto:

1-Il sistema finanziario globale è governato da banche centrali (con potere di emettere moneta e regolare i tassi di interesse), banche commerciali in grado di elargire prestiti con riserva frazionaria del capitale depositato dai correntisti.

2-La stampa di denaro per effetto Cantillon arricchisce solo chi è vicino alla stampante.

3-Bitcoin è uno strumento di libertà perché è immutabile, decentralizzato, trasparente e libero da ogni forma di limite territoriale.

4-Bitcoin è una tecnologia peer to peer, caratteristica che ne consente la non censurabilità.

5-Le rimesse sono i soldi inviati dai lavoratori verso i parenti residenti nei loro luoghi d'origine. Questi trasferimenti avvengono prevalentemente tramite contanti utilizzando money transfer con commissioni altissime, Bitcoin è un'alternativa.

Domande e Risposte:

- ***Se è vero che il sistema bancario è alimentato da prestiti non garantiti, come mai non si ha un crollo del sistema?***
  Per mettere in ginocchio tutto il sistema è necessario che buona parte della popolazione vada a ritirare i propri soldi in banca. Quando questo avviene in piccola scala si ha una Bankrun localizzata ad un singolo istituto che ne può provocare il fallimento.
- ***Cos'è l'effetto Cantillon?***

È l'effetto per il quale alla stampa di nuovo denaro, la ricchezza che questo porta viene beneficiata solo da chi è vicino alla stampante. Successivamente, quando passa nelle mani della comune popolazione subisce l'effetto inflattivo dovuto alla diluizione della massa monetaria, impoverendo i ceti più bassi.

- ***Perché è impossibile bloccare il peer to peer?***
  Il peer to peer è una condivisione di informazioni fra pari di una rete, in questo caso internet. La decentralizzazione di un'informazione, cioè condivisa e detenuta da tutti o da molti partecipanti alla rete, è praticamente impossibile da censurare. Bisognerebbe infatti bloccare l'intera rete dislocata in tutto il mondo (con giurisdizioni differenti). La censura di un solo attore non implica il blocco di quell'informazione che è libera di essere condivisa fra gli altri partecipanti alla rete.

7. Attuale Situazione Economica

Difficoltà: 1

Ricollegandoci al tema affrontato nel capitolo precedente, ossia l'immissione di nuova moneta che determina inflazione di quella esistente, per comprendere meglio il problema, possiamo chiamare in causa alcune canzoni del secolo scorso come testimoni del fenomeno nella sola Italia.

Dalla seconda metà dell'800 un canto popolare faceva cosi: "mamma mia dammi 100 Lire che in America voglio andar", poi nel 1939 Gilberto Mazzi pubblicava una canzona il quale ritornello era: "se potessi avere 1000 Lire al mese". 100 Lire oggi sono l'equivalente di 0,05 Euro, ma nel 1861 rappresentavano un potere di acquisto di circa 480 Euro (come si vede nel sito inflationhistory.com), abbastanza da permettere un viaggio in America. Nel 1939 le stesse 100 Lire avevano un potere di acquisto che si era abbassato a 87 Euro e di conseguenza le famose 1000 Lire al mese rappresentavano 870 Euro ma evidentemente erano uno stipendio sufficiente, ma stiamo comunque parlando di 50 centesimi di Euro al valore di oggi. A fine anni 90 ricordo che con 1000 Lire non potevi comprarci nemmeno un gelato perché ne servivano 1500 almeno! Con l'avvento dell'Euro poi i prezzi di tutti i beni si sono quasi raddoppiati, ricordo che ci si lamentava che ciò che costava 10 mila Lire poco prima (circa 5 Euro) è passato a 10 Euro nel giro di pochissimo tempo. Questa inflazione della moneta continua inesorabile ancora oggi, ma ci sono paesi che stanno peggio dell'Italia. In Turchia per esempio si ha un'inflazione annua che si attesta intorno al 60% con dei tassi di interesse già al 15%, ciò significa che nonostante i tassi mostruosamente alti l'inflazione rimane fuori controllo. Sta messo peggio il Venezuela, infatti il paese è colpito da un iperinflazione tra il 400 e il 700% all'anno, la più alta mai verificatasi nel 21° secolo. Immaginate di lavorare e di percepire uno stipendio in Venezuela. Questo ben presto non permetterà più il vostro tenore di vita, ma sarete costretti a lavorare di più per permettervi di acquistare i beni di cui avete bisogno.

Accade ciò perché gli Stati hanno acquisito tacitamente il potere monetario, ossia di emettere e regolare la moneta. Il continuo impoverimento dei risparmi si può dire essere esclusivamente frutto di sole due cause a mio avviso: azioni volte proprio allo scopo di impoverire la popolazione per far sì di tenerla sotto controllo distraendola con la continua necessita di lavorare di più, oppure incapacità nella gestione del denaro, poiché si pensa che elargirlo alla popolazione sotto forma di bonus, sostegni o redditi di cittadinanza, sia il modo più veloce e più semplice per ricevere consensi, senza la minima preoccupazione che tutto ciò può avere nel medio termine. "*Bitcoin fixes this*" Bitcoin risolve questo problema con una produzione di nuova moneta con un inflazione programmata matematicamente e

praticamente immodificabile, che si dimezza ogni 4 anni circa, ottenendo il risultato opposto ossia che le monete circolanti al posto di deprezzarsi si apprezzano perché sempre più scarse anche data la crescente adozione.

Oltre il potere monetario gli Stati hanno quello militare e politico, ma togliendo la leva monetaria allo Stato, come evolverebbero gli altri due? Nessuno può sapere cosa succederebbe su scala mondiale, ma verrebbero sicuramente a mancare degli incentivi per chi sfrutta il sistema a suo favore, forse ci si potrebbe auspicare la fine di tutte le guerre, poiché non economicamente vantaggiose se non sono sostenute da una stampa di denaro incontrollata come adesso. Potremmo sperare in una nuova classe politica meno corrotta e che a sua volta non faccia promesse di corromperci con dei sussidi o premi di vario genere in cambio di voti. Di sicuro oggi la nostra società ha l'assoluto bisogno di un sistema economico alternativo alle monete FIAT, perché malato e fallimentare.

Riassunto:

1-L'inflazione è causata dalla stampa di denaro, che può essere considerata salutare se mantenuta intorno al 2%, ma come si è visto nel lungo periodo, questa soglia è spesso scavalcata.

2-Il potere di stampa di denaro è forzatamente assegnato agli Stati.

3-L'inflazione di Bitcoin che è programmata e praticamente immodificabile, ogni 4 anni con l'halving si dimezza, fino a scomparire completamente intorno al 2140. Questo fa sì che il circolante acquista la caratteristica scarsità.

Domande e Risposte:

- **Perché se è noto che l'immissione di nuova moneta crea inflazione si continua a stampare denaro?**
  Nella migliore delle ipotesi viene stampata moneta per migliorare le infrastrutture, e questo porta un certo beneficio a tutta la popolazione. Ma possono accadere delle condizioni di emergenza come una pandemia, una guerra o una crisi di altro tipo, che "giustifica" la stampa di nuova moneta. Il problema è che grazie all'effetto Cantillon, di questa stampa, ne beneficia (come abbiamo visto nel capitolo precedente) solo chi è vicino alla stampante, mentre ha

effetto di diluire il valore nei confronti della gente comune. Chi ha questo potere è ovviamente chi ne gode per primo non curante della prosperità del resto della popolazione.

- **Come si genera il debito pubblico?**

  La nostra società economica è ancora in piedi poiché è alimentata dal debito. Gli Stati emettono in genere degli strumenti finanziari come titoli di Stato per avere la liquidità momentanea per ripagare il proprio debito, solo che questo viene poi gravato dagli interessi, sempre più difficili da colmare. È un conto senza reale sottostante che viene rimandato a creditori diversi, e se le uscite di un paese superano le entrate, questo deficit va a sommarsi al debito già in essere, alimentando la spirale del debito.

8. Lightning Network

Difficoltà: 2

Abbiamo visto nei capitoli precedenti come Bitcoin è lo strumento perfetto in termini di decentralizzazione, immutabilità, trasparenza, incensurabilità e riserva di valore, ma andrebbe approfondito anche il tema dell'impiego di Bitcoin come moneta di scambio. In tal senso tutte le caratteristiche sopra elencate sono punti a favore di una moneta, ma per essere facile e comoda da usare deve essere efficiente secondo altri parametri come la scalabilità, divisibilità e la diffusione. Quest'ultimo aspetto dipende dall'adozione, ossia da quanto questo metodo è accettato su larga scala fra chi vuole comprare e chi vuole vendere. Nessuno accetterebbe mai una moneta che presenta le caratteristiche ideali, se questa poi per qualche motivo non si potrà mai scambiare in cambio di qualche altro bene. L'adozione di Bitcoin è in crescita esponenziale e sempre più esercenti nel mondo anche in Italia sono disposti ad accettarlo come metodo di pagamento, esamineremo il tema nei prossimi capitoli.

La divisibilità invece è la caratteristica che rende possibile anche dei micro pagamenti, come un caffè al bar. In Bitcoin questo è possibile poiché è stato pensato per avere fino a otto cifre decimali dopo la virgola. Per cui un satoshi è uguale a 0,00000001 bitcoin e 100000000 satoshi (cento milioni di satoshi) sono equivalenti a un bitcoin, cambia solo l'unità di misura.

Per scalabilità invece si intende la capacità di una rete di assorbire quante più transazioni possibili ed elaborarle nel minor tempo possibile, senza perdite di prestazioni. Considerando che un blocco di Bitcoin viene minato ogni 10 minuti circa, significa che effettuare un pagamento richiede un tempo minimo tra 10 minuti e 20 minuti circa per essere confermato, quindi diventa scomodo per piccoli pagamenti, anche perché le commissioni potrebbero superare il valore dell'acquisto effettuato. A causa di ciò, lo sviluppo di Bitcoin si sta spostando verso gli strati successivi al protocollo chiamati layer 2, che hanno come obiettivo rendere la rete scalabile. Il più famoso al momento è il Lightning Network, su questo livello infatti, si stanno concentrando le più grandi risorse di sviluppo.

Lightning Network è costituito da nodi, i quali mettono a disposizione una certa liquidità aprendo canali di pagamento diretti verso altri nodi, provo a spiegarlo con un esempio.

Immaginiamo di uscire la sera con un paio di amici Alice e Bob. Alice decide di pagare il conto in pizzeria per tutti. Successivamente andiamo al bar per un drink e questa volta è l'amico Bob a pagare. A fine serata decidiamo di prendere un gelato e di pagare noi. A questo punto si giunge al momento in cui

bisogna tirare le somme e regolare tutti i crediti e i debiti prima di ritornare ognuno nelle proprie case. Non serve tracciare i saldi parziali di ogni singolo movimento, ma basta sapere a quanto ammonta il credito o il debito totale di ognuno, l'importante è mettere a disposizione la liquidità per saldare l'eventuale debito. Chi ha del credito invece lo riceverà dagli altri.

Lightning Network funziona in modo simile, vengono aperti dei canali di pagamento diretti fra nodi, dove entrambi mettono a disposizione una certa liquidità. Questa apertura di canale viene tracciata come una transazione sulla blockchain di Bitcoin (quindi permanentemente registrata) tramite l'apertura di un wallet multi-signature, ossia un portafoglio particolare che necessita la firma di almeno 2 proprietari (o più in caso di portafogli più complessi) per effettuare delle transazioni. A questo punto i due nodi hanno un canale preferenziale per trasferirsi valore in modo praticamente istantaneo e senza commissioni. Ogni nodo può aprire più canali in modo da essere connesso direttamente a più attori della rete Lightning, e gli utenti della rete possono connettersi al nodo che preferiscono (o crearne uno proprio) destinando parte della liquidità in modo da poterla spendere all'interno della rete Lightning.

Ma cosa succede se vogliamo effettuare un pagamento verso qualcuno connesso ad un nodo che non ha un canale aperto a quello nel quale siamo connessi noi? Avviene un pagamento indiretto tramite routing del percorso migliore, ossia l'informazione viene trasmessa utilizzando il percorso più efficiente tra nodi connessi fra loro, anche se l'origine e il ricevente non sono direttamente connessi.

Esempio: A deve pagare C ma non hanno un canale diretto aperto, però entrambi lo hanno con B e quindi è lui che funge da ponte. Ovviamente questi passaggi indiretti sono possibili solo se sia i nodi in questione, ma anche quelli coinvolti in mezzo presentano la liquidità necessaria.

Lightning Network quindi rappresenta un sistema di pagamento istantaneo, poiché non bisogna aspettare conferme on chain, e con commissioni bassissime. A queste condizioni la rete diventa estremamente competitiva anche con Visa e Mastercard, inoltre qui **le commissioni da pagare oltre essere bassissime, sono a carico di chi paga, mai nei confronti di chi riceve il pagamento!**

Per fare un esempio pagare una singola penna a sfera in cartolibreria con Bitcoin è possibile. Grazie alla rete Lightning Network, per un costo di 30 centesimi di Euro (circa 1000 satoshi) si può pagare istantaneamente e con commissioni di 2 sats (satoshi) ossia 0,0005 Euro! Inoltre il quantitativo viene immediatamente ricevuto dal negoziante che non deve attendere le tempistiche di trasferimento dei fondi tramite i sistemi bancari. Sfido qualsiasi altro sistema a fare meglio, soprattutto se teniamo conto che lo si può fare senza intermediari (se avete un nodo Lightning), o quanto meno mediante delle entità che offrono un miglior routing per la transazione, nell'istante che questa viene trasmessa.

Quando quindi i nodi decidono di chiudere un canale, tutte le transazioni avvenute fra loro non importeranno, ma avrà rilevanza solo il loro saldo finale, e a questo punto si potrà chiudere la transazione come un'unica spesa. Detto ciò va precisato che Lightning Network rappresenta il più grande bacino di sviluppo in Bitcoin e che, nonostante sia una tecnologia ancora acerba, è perfettamente funzionante.

Il sistema ha una capacità che sfiora i 6000 bitcoin (poco meno di 180 milioni di dollari) come si può vedere in Figura 6, Immagine proveniente dal sito The Block che monitora i dati on chain e lightning.

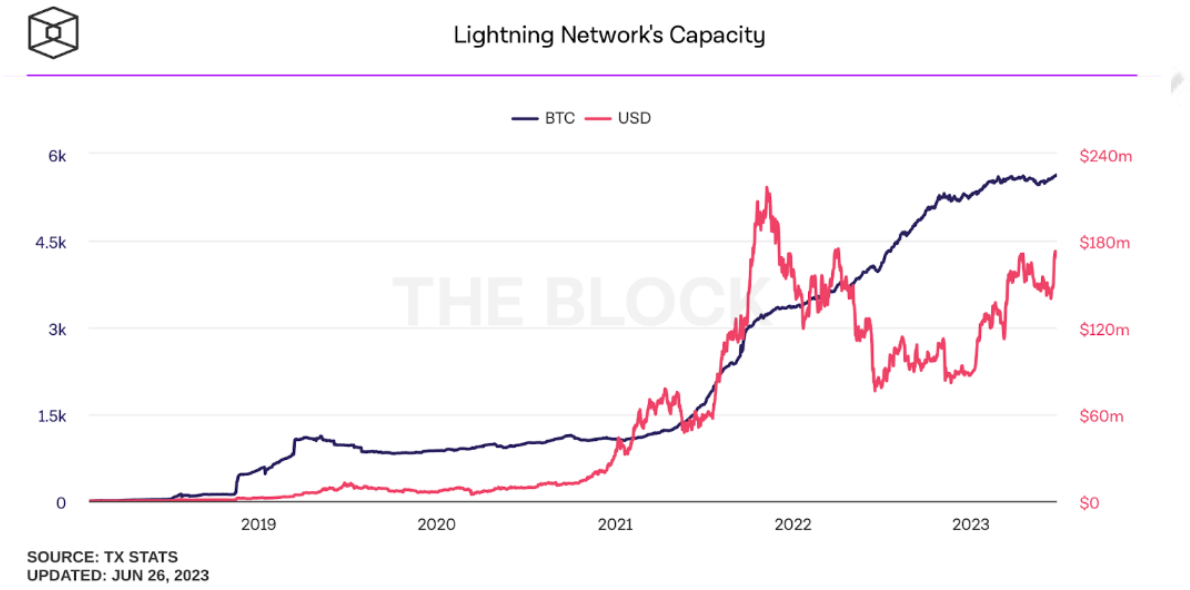

Figura 6

Se siete dei commercianti, a questo punto immagino vi stiate domandando, come mai nessuno ne parla? Quanti soldi potrei risparmiare se Bitcoin e Lightning Network diventassero utilizzati su larga scala come Visa e MasterCard? Ma non solo, immagino che per chi offre servizi online come un'e-commerce, (o vorrebbe farlo) avere la possibilità di poter vendere il proprio prodotto in tutto il mondo, e ricevere compensi in un'unica moneta senza dover pensare a cambi valuta, commissioni internazionali, e ricezione pagamenti in ritardo. Un insegnante di qualsivoglia materia potrebbe offrire lezioni online in tutto il mondo ricevendo pagamenti in bitcoin, senza barriere e senza costrizioni alcuna. La conoscenza e la diffusione di Bitcoin è lenta a causa dei pregiudizi, ma anche perché non esiste un ufficio marketing in grado di promuoverlo, ma questo è demandato soltanto ai volontari che decidono in un modo o nell'altro di fare qualcosa nel loro piccolo come ad esempio il gruppo del Satoshi Spritz di Bologna di cui faccio orgogliosamente parte. Di questo, Leonardo (uno degli amministratori) titolare del Pastis, locale

nel cuore della città che già accetta Bitcoin, ha organizzato a Luglio una giornata ai Giardini Margherita intitolata PlanBolo, per far conoscere Bitcoin a chi non lo aveva mai provato. Sono stati raccolti oltre 750 Euro da distribuire gratuitamente a chiunque volesse provarlo come sistema di pagamento tramite LN (Lightning Network). Come questa tante altre iniziative spontanee partono dal basso come d'altronde anche questo libro!

Ritornando al tema lightning network esistono diverse tipologie di wallet con diverse caratteristiche. Ne esistono alcune completamente custodial come Wallet of Satoshi, una semplicissima app con i 3 pulsanti inviare, ricevere e scan per inquadrare un QR Code per effettuare un pagamento, niente di più semplice.

Andando nelle opzioni permette di cambiare la lingua e la valuta per visualizzare i sats nella moneta di riferimento. Un'altra caratteristica di quest'app è che le transazioni sono veramente velocissime, oserei istantanee. Come dicevo all'inizio però essendo un'implementazione custodial significa che non possediamo le chiavi private del wallet ma ci stiamo fidando del provider del servizio.

L'alternativa lightning non custodial può essere Breeze. Un'app wallet che funge essa stessa da nodo lightning. Anche qui troviamo i pulsanti essenziali ben in vista, ma esplorando il menu è possibile trovare delle opzioni anche per sviluppatori, oltre a podcast da poter ascoltare con il metodo value for value, ossia ascoltando si può decidere di donare una quantità di satoshi al minuto stabilita dall'utente, in base alle proprie preferenze. L'app ovviamente permette di fare il backup delle chiavi private tramite un server remoto o tramite Google drive (dove è possibile anche crittografarle). Inoltre l'applicazione integra delle altre funzioni che permettono l'acquisto di servizi, ma anche un POS dove è possibile inserire l'elenco dei prodotti in vendita anche con codice a barre, questo lo vedremo meglio nel capitolo relativo.

Di contro rispetto a Wallet of Satoshi, in Breeze le transazioni possono richiedere qualche secondo in più proprio perché avviene tutto peer to peer, senza un provider centralizzato.

Esistono molte altre soluzioni come Phoenix e Muun che come Breeze non sono custodial, ma suggerisco di approfondire e scegliere quello che più fa per voi.

Ricevere, o inviare on chain dei fondi su Lightning Network è semplicissimo. Una volta installata l'app, sul pulsante ricevi potrete scegliere di ricevere satoshi su lightning oppure tramite un indirizzo on chain (in genere iniziano per bc1) che vi fornisce l'app stessa. Copiatelo e incollatelo come indirizzo di ricezione nell'app da dove volete spostare i fondi da on chain a Lightning. Viceversa cliccando sul

pulsante invia potrete fare un pagamento sia tramite Lightning che far ritornare i fondi on chain inserendo l'indirizzo di destinazione.

Riassunto:

1-Una moneta per essere perfetta non basta che sia decentralizzata, immutabile, trasparente, incensurabile e fungere da riserva di valore, ma deve anche avere altre caratteristiche quali, la scalabilità, divisibilità e diffusione.

2-La scalabilità non è intrinseca in bitcoin, ma è acquisita grazie allo sviluppo del Lightning Network, che è un secondo strato (layer 2) in comunicazione con la rete principale di Bitcoin. Le transazioni trasmesse fra nodi lightning sono praticamente istantanee (senza dover attendere le conferme ogni 10 minuti on chain) e questo ne permette l'utilizzo per piccoli importi (anche pochi satoshi), aiutando la diffusione fra gli esercenti disposti a riceverli come metodo di pagamento.

3-Le commissioni su Lightning sono veramente bassissime e sono a carico di chi paga, non di chi riceve.

4-Esistono diverse soluzioni di wallet Lightning con diverso grado di compromesso, rimane il fatto che questo tipo di wallet è da utilizzare come contenitore di fondi da spendere, non come salvadanaio dei risparmi.

Domande e Risposte:

- **Perché utilizzare un layer 2 di Bitcoin, non si potrebbe abbassare la difficoltà del mining in modo da avere dei blocchi ogni minuto?**
  Tecnicamente è fattibile, ma questo significherebbe inflazionare molto di più la moneta (ricordiamoci che ad ogni blocco i miner ricevono dei bitcoin nuovi di zecca), e anche aggiustando la ricompensa dei miner in modo da evitare ciò, significherebbe avere uno spazio di blocco inutilizzato che creerebbe un aumento del peso della blockchain, anche se con blocchi praticamente vuoti.
- **È possibile avere un nodo Lightning anche senza un nodo bitcoin?**
  No, per avere un nodo Lightning bisogna per forza avere un nodo bitcoin, viceversa avere un nodo bitcoin non implica per forza gestire un nodo Lightning.

- **Perché le commissioni su Wallet of Satoshi sono molto più basse rispetto agli altri wallet? Perché Wallet of Satoshi è un wallet custodial, significa che una terza parte custodisce i vostri fondi, e per questo è anche più facile fare un pagamento. Effettuare una transazione fra due wallet non custodial, invece, implica la capacità economica dei canali di routing, che per il loro servizio si fanno pagare una piccola commissione.**

9. Perché esiste solo Bitcoin

Difficoltà: 2

Le soluzioni proposte come innovative dalle altre blockchain spesso sono idee passate già da Bitcoin e scartate, ad esempio quelle che riguardano il consenso.

Abbiamo già descritto che per produrre nuovi bitcoin i miner devono a tentativi trovare la soluzione al requisito minimo (un certo numero di zeri iniziali nell'hash del nuovo blocco) tenendo conto dell'hash del precedente, altre informazioni come il timestamp, e le transazioni nuove da aggiungere. Questo è possibile grazie al pezzo di codice chiamato Nonse che è variabile a questo scopo, e permette al miner, mutandolo, di trovare l'hash contenente un certo numero di zeri iniziali, requisito del coefficiente di difficoltà.

Questo lavoro è una corsa contro il tempo, chiunque riesca a dimostrare di aver trovato la soluzione sta mettendo al sicuro la rete con un sigillo di autenticità ed è giusto che venga ricompensato. Ha dimostrato di aver compiuto un lavoro, che in questo caso significa aver speso energia elettrica per alimentare le macchine che sono state le più veloci a trovare la soluzione. Questa prova di lavoro, chiamata appunto in inglese Proof of Work (PoW), è essenziale per una moneta come Bitcoin perché testimonia la buona fede dei miner, dei validatori e di tutti gli attori della rete. Agire in mala fede per un miner ad esempio sarebbe assolutamente controproducente, perché si verrebbe immediatamente scoperti, perdendo di fatto la ricompensa del blocco e vanificando il lavoro svolto e quindi anche i costi sostenuti, questo quindi è un tassello fondamentale per la sicurezza della rete.

Esistono delle alternative al consenso PoW, la più famosa è il Proof of Stake (PoS) adottata recentemente anche dalla seconda criptovaluta in termini di capitalizzazione che è Ethereum. Esistono movimenti alimentati da Greenpeace e da altri ambientalisti che vorrebbero cambiare il codice di Bitcoin per renderlo sostenibile per l'ambiente, ma sprecano il loro fiato e le loro risorse (anche energetiche fra le altre cose) e adesso proverò a spiegarvelo iniziando dal funzionamento del PoS e che differenze ha con il PoW.

Nel PoS non ci sono super computer che devono risolvere dei calcoli, ma il consenso si basa sullo stake ossia sul gruzzoletto accumulato dai validatori. Questo significa che le transazioni possono anche essere immediate, con commissioni quasi nulle e sono quindi un presunto ambiente perfetto anche per poter usare la rete per altre funzioni matematiche (smart contract). Questo ci mette però di fronte diversi problemi, per essere un validatore della rete bisogna possedere una quantità di moneta nativa e quindi

possedere una grande liquidità, a differenza di Bitcoin dove chiunque può fare da validatore (basta un vecchio pc o anche un cellulare). Possedere una grande liquidità significa appartenere ad un determinato ceto sociale (grandi aziende o società) con possibili conflitti di interessi, e di fatto ciò setaccia la popolazione e esclude i piccoli dal consenso, inoltre le entità in grado di possedere una quantità di moneta così grande non sono tantissime, e quindi il risultato è un sistema poco decentralizzato, e di conseguenza poco democratico. Inoltre la presenza di pochi nodi implica la possibilità che un attacco malevolo o che una censura abbia successo. Bitcoin invece è la rappresentazione migliore di democrazia in questo ambito, infatti troviamo un numero altissimo di nodi validatori, provenienti da tutte le parti del mondo, proprio perché mettere in piedi un nodo significa potenzialmente avere un PC (o un cellulare) anche vecchio con un hard disk di discrete dimensioni ed eseguire un programma e anche per questo censurarlo o bloccarlo è quasi impossibile.

C'è inoltre un'altra sostanziale differenza fra PoW e PoS. Nel primo essendo che il miner compie un lavoro, e tramite la risoluzione dell'hash corretto dimostra di averci investito tempo e denaro, è ovvio che la ricompensa da ottenere deve per forza di cose essere vantaggiosa per lui. È come un contadino che investe lavoro e soldi solo perché sa che può produrre un frutto che riuscirà a vendere con del margine di guadagno. Ed è questo uno dei motivi che rende Bitcoin di valore, perché il lavoro svolto per minarli deve essere inferiore alla potenziale rivendita. Nel PoS tutto questo viene a mancare, i validatori che ricevono la ricompensa non hanno compiuto nessun lavoro, non hanno affrontato spese e quindi il valore della moneta, tenendo conto solo di questo parametro, è praticamente zero.

Un'altra differenza è il costo delle commissioni, in genere nel PoS (ma non sempre) sono più basse. Questo che apparentemente è un vantaggio in realtà causa intasamenti della rete dovuti a transazioni spam a costi quasi nulli, che spesso in alcune reti hanno causato il blocco e un successivo riavvio, dimostrando come un attacco spam intenzionale a costo infinitesimale può essere efficace al fine di rendere inutilizzabile una rete che non sia Bitcoin.

Abbiamo già detto che Bitcoin è democratico ed è anche open source, ossia il codice è pubblico e chiunque può revisionarlo, ma anche copiarlo e modificarlo generando una biforcazione della rete (fork). Le due strade avranno in comune il passato, ma non il futuro. A quel punto i miner e i nodi possono volontariamente decidere quale è la vera rete da seguire e quindi quale delle due considerare ancora Bitcoin. Sulla base di ciò, il movimento "*change the code*" alimentato e sostenuto da Greenpeace, che invoglia i partecipanti della rete Bitcoin con terrorismo informatico a cambiare il consenso in PoS, potrebbe in qualsiasi momento, in modo democratico, avere luogo, ma nessuno la sceglierebbe perché

verrebbero a mancare le caratteristiche sopra descritte che rendono unico Bitcoin. Parliamoci chiaro, Bitcoin non è la causa dei cambiamenti climatici, che indubbiamente sono comunque da attribuirsi ad attività antropica. Il contributo di Bitcoin al problema è minuscolo e trascurabile, ma come già argomentato in precedenza semmai rappresenta un incentivo per gli investimenti volti ad efficientare il settore delle rinnovabili.

Qualsiasi altra blockchain è il prodotto commerciale di un'azienda che ha potere decisionale, questa può facilmente essere bloccata da poteri governativi, poiché qualcuno ha la responsabilità dell'azienda e quindi essere perseguito anche penalmente. Questo non può avvenire in Bitcoin, poiché non esiste un'azienda che è responsabile o ha potere decisionale. Il "fondatore" è rimasto volutamente celato dallo pseudonimo di Satoshi Nakamoto proprio per non essere se stesso un punto debole per Bitcoin, che altro non è che codice e basta. Non si possono censurare delle lettere e dei numeri, il codice informatico rappresenta libertà di espressione.

Quanto detto si collega al prossimo punto, ossia perché Bitcoin e non altre chain PoW come Litecoin, Bitcoin Cash ecc.? Oltre l'aspetto appena discusso, ossia che le altre hanno un fondatore e/o un'azienda di riferimento, senza tener conto delle differenze in termini di codice, rimane l'ambito della decentralizzazione. Tutte le altre blockchain con consenso PoW hanno ordini di grandezza inferiori in termini numero di nodi validatori, intaccando gravemente la decentralizzazione e la sicurezza della rete. Questa bassa diffusione è da attribuirsi invece alle modifiche e alle "innovazioni tecnologiche" apportate al loro codice, rispetto a Bitcoin. Molte di queste chain sono dei fork proprio di esso con poco successo, poiché la comunità ha scelto democraticamente di seguire la rete che ancora oggi si chiama Bitcoin. Spero che quanto detto in questo capitolo vi sia di spunto di approfondimento e che vi abbia trasmesso il mio pensiero, ossia che sprecare tempo e denaro in altre criptovalute non ha nessun senso. Questo è perché esiste solo Bitcoin.

Riassunto:

1-Il processo di Proof of Work in Bitcoin richiede che i miner risolvano problemi matematici per creare nuovi blocchi nella blockchain. Questo sistema è una corsa contro il tempo, dimostrando il lavoro svolto e garantendo la sicurezza della rete attraverso la distribuzione di nodi validatori in tutto il mondo.

2-Alcune blockchain, come Ethereum, adottano il Proof of Stake (PoS) invece del PoW. Nel PoS, il consenso si basa sulla quantità di moneta nativa posseduta dai validatori anziché sul lavoro computazionale. Questo implica che il PoS è maggiormente centralizzato escludendo partecipanti con liquidità limitata.

3-In Bitcoin, i miner investono tempo e denaro per aggiungere un blocco, confermando il valore della criptovaluta. Nel PoS, i validatori ricevono ricompense senza compiere lavoro computazionale, portando il valore potenziale della moneta a zero. Le commissioni nel PoS possono essere più basse, ma possono anche causare intasamenti della rete, ed essere un facile punto di attacco.

4-Avere un nodo Bitcoin è estremamente semplice, ed è per questo che è democratico e decentralizzato grazie a un gran numero di nodi validatori sparsi in tutto il mondo. Questa caratteristica rende difficile la censura e gli attacchi malevoli. Bitcoin è open source, il che significa che chiunque può contribuire e revisionare il codice.

5-Rispetto ad altre blockchain PoW, come Litecoin e Bitcoin Cash, Bitcoin è più decentralizzato e quindi sicuro. Queste blockchain sopra menzionate sono state create come fork di Bitcoin, per portare delle "innovazioni", ma la comunità ha continuato a sostenere la rete originale, evidenziando l'importanza della sua adozione. Anche il movimento "change the code" per far passare Bitcoin a PoS può immediatamente essere messo in pratica da chiunque essendo open source, ma nella realtà dei fatti nessun miner o nodo sarebbe disposto a sostenere il fork.

Domande e Risposte:

- **Perché un massimalista di Bitcoin detesta tutte le altre cripto?**
  In generale non è un obbligo di un massimalista odiare le altre cripto. Ma in generale dopo aver studiato, ci si rende conto che, i sistemi adottati dalle altre, esistono perché sono già state discusse e scartate in Bitcoin, ne è un esempio il Proof of Stake. Il motivo di questa esclusione risiede nei motivi sopra elencati, quindi un rischio di centralizzazione, o di censura hanno fatto sì che questa non era una strada percorribile. A questo punto se un'altra chain, nonostante ciò, decida comunque di utilizzare questo metodo di consenso pubblicizzandolo come più veloce e scalabile rispetto a Bitcoin, senza menzionare di aver intaccato pesantemente la decentralizzazione, allora siamo di fronte ad una frode. Per questo motivo molti bitcoiner hanno allergia alle cripto, anche perché alcune si

confermano come delle truffe evidenti che mettono in cattiva luce anche Bitcoin, e di conseguenza persone che avrebbero magari approfondito scappano via ancor prima di aver studiato.

- **Bitcoin potrà mai passare a PoS?**
  Secondo quanto detto fino ad adesso no, perché ne risentirebbe soprattutto la decentralizzazione, e quindi anche eventuali censure. Bitcoin nasce per essere uno strumento di tutti, non per un élite con un enorme potere decisionale. Ogni decisione presa in Bitcoin viene valutata e ogni nodo è libero di implementare una propria modifica, se questa rappresenta il volere della maggioranza è ciò che diventerà Bitcoin in futuro. Allo stato attuale non è una valida soluzione, a meno che non si trovi un modo per eliminarne i problemi.
- **Perché esistono le altre criptovalute, e perché hanno ancora una quotazione di mercato?**
  È relativamente semplice creare una nuova criptovaluta, basta prendere il codice pubblico di Bitcoin e modificarlo cambiandone nome, quantità, emissione e metodo di consenso, ed è ancora più semplice creare banalmente un token. Questo ha fatto sì che oggi esistono migliaia di coin inutili ma che magari sono spinte dall'azienda che li ha emesse e che magari ha coniato la metà di queste inviandole al proprio wallet. La maggior parte sono delle evidenti truffe, chi le crea infatti punta a far pompare il prezzo per poi liberarsene. Molte rimangono in piedi perché "gli investitori" continuano a comprarne e venderne sperando di poter beccare il momento perfetto e diventare ricchi in poco tempo. Alla base c'è questo, l'avidità che tiene viva la fiammella di progetti senza senso. Prima di buttare dei soldi bisognerebbe ragionare con spirito critico studiando quanto meno il progetto.

10. Diversi Modi Per Acquistare Custodire e Scambiare Bitcoin

Difficoltà: 2

Questo capitolo insieme al prossimo saranno più pratici e raccolgono le istruzioni per muoversi in questo ambito. Se avete ben compreso i capitoli precedenti ogni cosa detta qui avrà senso. È come se aveste sostenuto l'esame teorico della patente senza aver guidato mai una macchina, qui impariamo a farlo.

Sintetizzando in tre parole i passi per detenere bitcoin sono: l'**acquisto**, **custodia** e **scambio**.

Oggi esistono svariati modi per **acquistare** bitcoin, con diversi gradi di difficoltà e diversi gradi di trade-off (compromessi).

All'utente al quale è rivolta questa guida ne consiglio alcuni semplici senza compromettere la sicurezza o la privacy.

Prima di dedicarci all'acquisto affrontiamo insieme la seconda parola chiave ossia la **custodia**.

Facciamo subito una distinzione, possedere Bitcoin significa avere le chiavi private di un wallet che li contiene. Stiamo parlando delle 12 o 24 parole (seed phrase) di cui abbiamo già parlato nel capitolo 4 che non vanno mai divulgate per nessuna ragione, poiché chi ha accesso a quelle, ha accesso ai fondi. Infatti Bitcoin è trustless (senza fiducia) ossia non esiste un entità alla quale possiamo rivolgerci per recuperare eventualmente i soldi persi. Non esiste un ente terzo che ci possa aiutare a recuperarli, perché la **custodia** (la seconda parola chiave per possedere bitcoin) è responsabilità del solo possessore, questi portafogli sono detti **Non Custodial**.

Bitcoin, anche da quanto detto nei capitoli precedenti, è un sistema che abolisce la fiducia verso terzi, però esistono delle entità come gli exchange verso i quali ci si può rivolgere per la custodia. In questo caso si parla di **Wallet Custodial**, poiché loro possiedono un wallet contenente i saldi di tutti i clienti e questi ultimi non sono tenuti a possedere il seed.

Detenere fondi su un wallet custodial ha pochissimi vantaggi ma tantissimi svantaggi. Per i traders, ossia coloro che si occupano si scambiare le valute per avere un profitto, può aver senso utilizzarlo, ma non si tratta della maggioranza di persone alla quale è rivolta questa guida. Acquistare Bitcoin su exchange è comunemente e erroneamente concepito come più semplice, in realtà non è così. Oggi tutti gli operatori economici che vogliono offrire questo servizio richiedono una procedura di KYC (know your customer), cioè viene richiesta al cliente un'approfondita prova di identità, tramite registrazioni video, scansione dei documenti comprovanti anche l'indirizzo di residenza. Questo oltre comportare una burocrazia

inutile fa sì che l'utente sia esposto a possibili attacchi, dovuti ad esempio a quelli subiti dall'exchange stesso, con conseguente fuoriuscita di informazioni sensibili dei clienti quali appunto nomi, patrimonio e indirizzi di residenza. A questo grave problema si aggiunge il fatto di fidarsi di un ente terzo per la custodia dei propri bitcoin. Come spesso succede non è detto che questi agiscano nell'interesse del cliente reinvestendo i capitali ottenuti in progetti nell'ambito digitale di dubbia necessità. Magari questi investimenti non rendono, anzi in periodi di bear market falliscono e con essi vengono bruciati i fondi. L'esempio più recente ed eclatante è stato quello del secondo exchange mondiale in termini di volumi FTX, fallito miseramente nel giro di pochi giorni poiché l'azienda "reinvestiva" i fondi dei clienti. Ma esistono anche altri esempi simili, come quello dell'italiano The Rock Trading, il più longevo exchange di criptovalute (fino a quel momento). Altre volte invece queste entità dichiarano di aver subito il furto delle chiavi private e di aver perso tutti i fondi in modo permanente. Con quanto detto non voglio dire che tutti gli exchange sono gestiti da criminali, ma allo stesso tempo l'esperienza ci dovrebbe insegnare che non possiamo escluderlo a priori, anche se si tratta di quelli che hanno volumi più elevati o che calpestano la scena da più tempo. In conclusione, se proprio una persona dovesse decidere di acquistare su exchange centralizzato, (operazione comunque da evitare per le possibili ripercussioni sulla privacy), la prima cosa da fare una volta ricevuti i propri satoshi è depositarli in un wallet non custodial di cui si hanno le chiavi private.

Parlando di wallet non custodial ne esistono diversi e con svariate interfacce grafiche io consiglio uno tra Sparrow ed Electrum. Il primo ha un interfaccia simile alle applicazioni moderne, il secondo molto minimalista con un'interfaccia in stile Windows con menu a tendina, entrambi sono open source (con codice verificabile) e per questo anche più sicuri, permettono di effettuare funzioni semplici, ma anche avanzate come creare wallet multi-signature, firma, cifratura e decifratura del messaggio ecc.

Rispondo ad un possibile dubbio di un nuovo utente: si è possibile creare un wallet con Sparrow e aprirlo anche con Electrum tramite le 12 o 24 parole generate, poiché lo standard BIP39 è universale. Possedere il seed significa possedere i fondi, e questi possono essere importati in tutti i wallet che supportano lo standard.

Entrambi i wallet sopracitati sono interfacciabili con i più noti **hardware wallet**, che altro non sono che dei device in grado di custodire le chiavi private offline senza esporle a potenziali attacchi provenienti dalla rete internet. Questi device infatti permettono di firmare una transazione sul dispositivo stesso non collegato ad internet, grazie a un pin o una password che cifra le chiavi private.

Detto ciò, che modo si possono **acquistare** bitcoin in modo semplice e in modo non custodial rispettando la nostra privacy?

A mio parere esistono un paio di possibilità semplici adatte al lettore di questa guida.

1-RELAI

Relai è un'azienda svizzera che ha sviluppato un'app intuitiva e comoda scaricabile sia da Google Play Store per i dispositivi Android, che da Apple Store per gli amanti della mela morsicata.

L'applicazione permette di acquistare Bitcoin tramite carta di credito, prepagata o bonifico bancario il tutto senza rilasciare dati personali. La legge svizzera infatti consente di acquistare **fino a 900 franchi (circa 900 Euro) al giorno** senza che il provider del servizio debba richiedere i dati personali dei clienti.

Acquisti di importi maggiori sono consentiti solo dopo aver effettuato la procedura di KYC di identificazione.

Dopo aver scaricato l'applicazione, questa prima di effettuare il vostro primo acquisto di satoshi vi chiede di associare un wallet. Potrete in modo semplice crearne uno tramite l'app stessa (il modo più semplice e che consiglio) generando 12 nuove parole che codificheranno il vostro wallet, oppure associandone uno vostro già esistente. In questo caso bisogna verificare l'indirizzo di destinazione utilizzando la firma tramite il software wallet usato per il portafogli personale. Qui trovate una guida di Relai che chiarisce gli step da fare, nello specifico spiega come collegare un indirizzo tramite Electrum associato ad un hardware wallet.

Adesso che siete pronti per acquistare i vostri primi satoshi vi troverete di fronte una schermata come la Figura 7, dove sono visibili le principali funzioni dell'applicazione. Si può vedere il saldo del wallet, si possono effettuare le azioni di acquisto e di vendita, si possono verificare le transazioni effettuate, verificare lo stato dell'investimento totale e cambiare o consultare le impostazioni del profilo.

Figura 7

Per prima cosa andiamo nell'icona in basso a destra del profilo segnalata nella Figura 8 con la freccina verde

Figura 8

In questa schermata come già detto abbiamo la possibilità di consultare:

- -le impostazioni dell'app e le nostre preferenze come la lingua, la valuta di riferimento, notifiche e altro.
- -il supporto via chat.
- -il livello del wallet (dipende dalla verifica dell'identità, opzionale solo per chi volesse acquistare oltre i 900 Euro al mese)
- -il codice invito che vi permette di ottenere uno sconto sulle commissioni
- -potete consultare la frase di recupero o seed phrase (siate sicuri di averla scritta e conservata correttamente)
- -Per i dispositivi che permettono la rilevazione dell'impronta o del face ID qui può essere attivato o disattivato
- -termini e condizioni e informativa sulla privacy.

Impostati tutti i parametri a piacimento, vi consiglio di inserire un codice invito come indicato dalla freccia verde in Figura 9

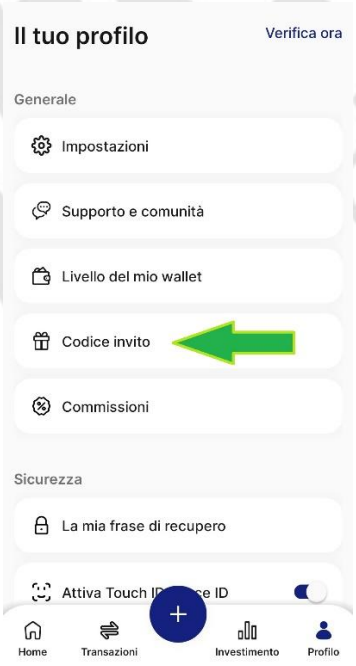

Figura 9

A questo punto vi si aprirà una schermata come in Figura 10 dove potrete aggiungere un codice invito. Potete utilizzare quello di un amico, oppure se vi va di supportarmi potreste inserire il mio che è:

REL93841

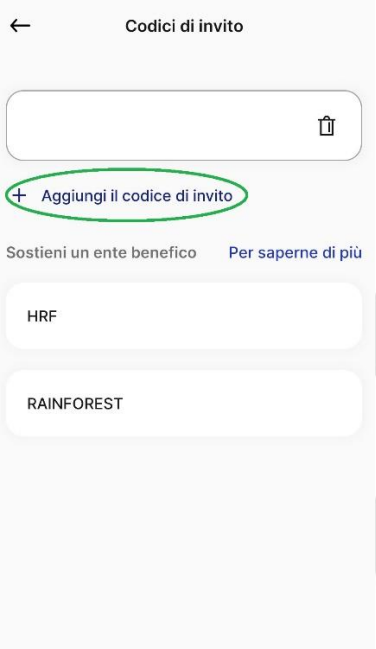

Figura 10

Il codice invito vi garantisce uno sconto sulle commissioni di acquisto pari allo 0,5%, allo stesso tempo Relai riconosce una piccola commissione a chi ha promosso il loro prodotto. Vi ringrazio dunque nel caso vogliate utilizzare il mio codice **REL93841.**

Le commissioni totali di acquisto partono da un 2,5%, ma utilizzando delle accortezze si possono abbattere fino all'1%:

- Utilizzando il codice invito otterrete uno 0,5% di sconto;
- Facendo acquisti superiori a 100 Euro si ha un ulteriore sconto dello 0,5%;
- Facendo acquisti ricorrenti si ottiene un altro 0,5% di sconto sulle commissioni (può essere sia settimanale che mensile e non è vincolante)

Massimizzando i tre fattori sopra si ha uno sconto totale dell'1,5% andando a pagare solo 1% di fee.

Lo sconto su importi superiori a 100 Euro e quello relativo agli acquisti ricorrenti si ottengono di volta in volta durante l'acquisto, che è una procedura guidata a step molto semplice. Al termine dell'acquisto viene richiesto il metodo di pagamento, che può essere tramite carta o a mezzo bonifico. In quest'ultimo caso nell'ultimo passaggio vi verrà chiesto di effettuare un bonifico tramite la vostra banca all'IBAN indicato da Relai. A questo punto potrete cliccare su "fatto" e una volta ricevuto il bonifico Relai procederà inviandovi i satoshi acquistati direttamente nel vostro wallet. Potrete facilmente consultare lo stato del vostro acquisto dalla schermata principale.

2-POCKET BITCOIN

Pocket Bitcoin è un sito di un'altra azienda svizzera, che permette di acquistare satoshi con gli stessi benefici e limitazioni di Relai. Differisce però dalla prima che ho descritto perché è raggiungibile sia tramite il sito internet, oppure tramite l'app scaricabile dagli store digitali di Apple e Android. Sia l'app che il sito sono abbastanza semplici, in quest'ultimo per esempio, dopo aver copiato un proprio indirizzo nell'apposito riquadro viene chiesta la conferma tramite firma vedi Figura 11

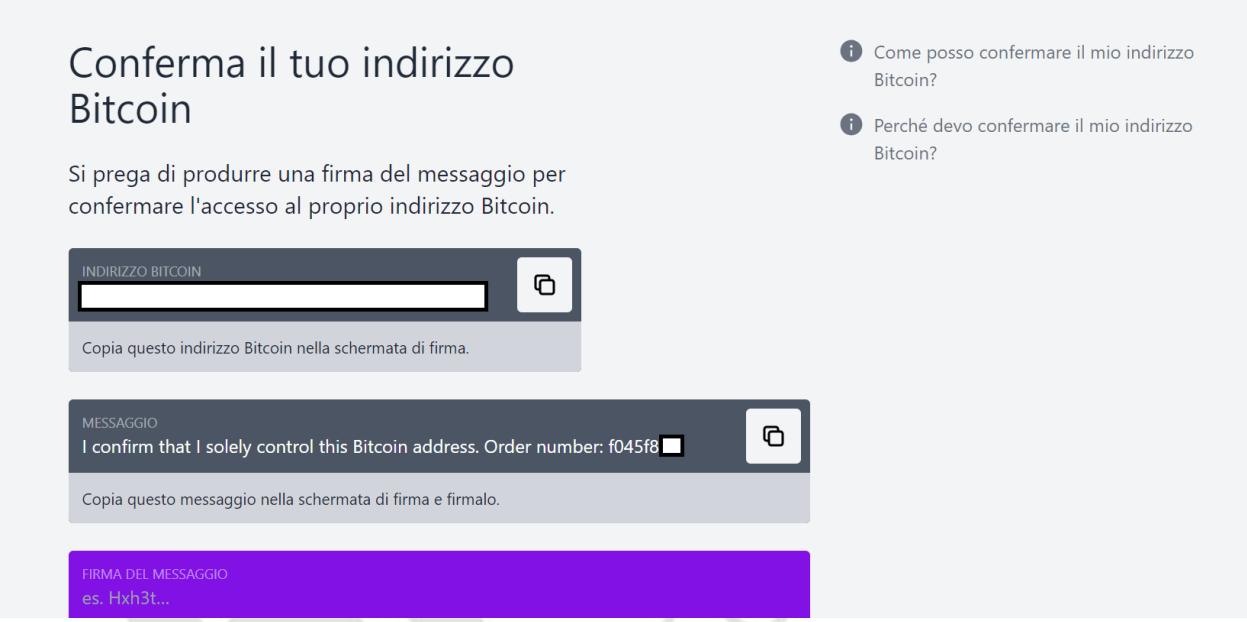

Figura 11

A questo punto poi tramite il proprio wallet inserendo il messaggio copiato lo si può firmare e la stringa che viene generata come risultato va inserita nel riquadro viola della Figura 11. Questa verifica viene fatta per assicurarsi che l'indirizzo sia corretto, che non ci siano errori o manomissioni esterne.

Una volta scelto l'importo da acquistare Pocket vi fornirà l'IBAN al quale fare il bonifico e una causale da inserire nel bonifico via email per associare univocamente il pagamento al vostro indirizzo.

Entrambe le opzioni per acquistare bitcoin sono valide, Pocket permette di non dover per forza importare un wallet, poiché utilizza un indirizzo pubblico fornito da voi, mentre Relai a mio avviso è più immediata e semplice per l'utilizzatore meno esperto poiché presenta meno passaggi.

In merito al terzo punto ossia lo **scambio**, utilizzando i wallet sopracitati quali Electrum e Sparrow ma anche tutti gli altri, è possibile tramite la funzione “invia” di spostare dei bitcoin da un indirizzo ad un altro.

Prendendo ad esempio Electrum, dopo aver cliccato su “invia”, bisogna copiare l’indirizzo del destinatario nel campo “paga a”. È importante ricontrollare l’indirizzo che sia corretto, poiché se è errato si potrebbero perdere i fondi per sempre. Il campo “descrizione” è facoltativo e non rimane inscritto nella blockchain, ma è solo un promemoria di chi invia. Inserendo poi la quantità in BTC o in valuta fiat (esempio Euro o Dollaro) e cliccando su “paga” si apre una finestra dove è possibile impostare la commissione. Il software in automatico dovrebbe fornirvi delle commissioni medie necessarie a far sì che la transazione vada a buon fine in poco tempo. Se si vuole però ottimizzare questa operazione, minimizzando i costi transazionali, sul sito di Mempool è possibile consultare i costi in sats per vB (virtual Byte) in tempo reale.

Ad esempio con una transazione che occupa 141 byte, e una commissione di 50 sats/vB, questa ha un costo di 141*50 = 7050 satoshi.

Di default l’applicazione utilizza l’indirizzo di resto, ossia ad ogni transazione il resto viene inviato ad un altro indirizzo dello stesso wallet frazionando il suo contenuto per migliorare la privacy. In pratica se avete 1 BTC su un indirizzo e inviate 0,2 per un pagamento ad un altro indirizzo esterno, il resto (ossia 0,8 meno le commissioni) non rimarranno nell’indirizzo di partenza, ma verranno inviati ad un altro indirizzo di resto del vostro wallet. Questa opzione è possibile rimuoverla da Strumenti/Preferenze/Transazioni, ma ripeto, intacca notevolmente la vostra privacy, anche se all’apparenza avere tutto il saldo in un unico indirizzo possa sembrare più comodo. Bisogna inoltre tenere presente che spendere satoshi che si trovano in diversi indirizzi, aggregandoli in un'unica grande spesa aumenta i costi transazionali.

Merita una menzione un altro metodo per acquistare bitcoin che rispetta la vostra privacy, questo è Bitcoin Voucher Bot. Un bot su Telegram che tramite dei semplici comandi vi guida nell’acquisto di bitcoin on chain tramite voucher, su indirizzo Lightning Network, ma vi permette anche di acquistare dei servizi come abbonamenti VPN ecc.

Riassunto:

1-Per possedere bitcoin bisogna padroneggiare tre aspetti: l'acquisto, la custodia e lo scambio.

2-Acquistare bitcoin è semplice esistono diverse vie, sia in modo custodial che non custodial. Il primo caso è quando ci muoviamo tramite un ente terzo che custodisce le chiavi private e noi deteniamo un credito di fatto. Nel secondo siamo noi a detenere fisicamente il seed e ad essere sicuri di possedere inconfutabilmente quei bitcoin.

3-L'utilizzo degli exchange custodial, per acquistare e detenere bitcoin è un rischio in termini di privacy. Poiché questi servizi sono costretti a richiedere procedure di KYC (Know Your Customer) con conseguente pericolo di esposizione dei dati che possono causare attacchi di terzi o malversazioni da parte degli exchange stessi.

4-Fra i wallet non custodial più utilizzati abbiamo Sparrow con un'interfaccia user-friendly, ma anche Electrum che si presenta con una schermata più vintage stile Windows 95, ma ugualmente efficace. Sono entrambi open source quindi il codice è stato verificato da diversi utenti e per questo li possiamo considerare tendenzialmente affidabili.

5-Acquistare bitcoin in modo sicuro è senza KYC è possibile grazie ad aziende svizzere come Relai e Pocket Bitcoin, che sfruttano la legge locale permettendo ai propri clienti di acquistare fino a 900 Euro al giorno di bitcoin senza la raccolta di dati personali.

6-Per spostare dei fondi, quindi scambiarli, bisogna controllare sempre di aver incollato l'indirizzo corretto del destinatario, di aver impostato l'importo e le commissioni in modo da ottimizzare i costi e le tempistiche di validazione della transazione.

Domande e Risposte:

- **Cosa sono peggio i rischi dovuti a terze parti (esempio gli exchange) o quelli relativi alla custodia personale?**
  Questo è un tema delicato, perché molte persone tendono a fidarsi per non avere la responsabilità di custodire un segreto. Personalmente penso che demandare ad un ente terzo i nostri fondi, senza la garanzia che questo li custodisca in modo appropriato, sia sempre peggio. I modi per fare il backup del seed sono tantissimi e questi possono anche essere ridondanti, in modo tale che se un sistema di backup viene compromesso i fondi non vengano persi.
- **Perché gli Stati obbligano gli exchange al KYC?**

Gli Stati pretendono il KYC ufficialmente per le norme antiriciclaggio. In questo modo, essendo gli exchange il ponte di contatto fra le criptovalute e le monete FIAT, sono in grado di monitorarne i flussi. Questo non è esattamente così poiché oggi è perfettamente possibile spendere i propri satoshi in cambio di servizi, e quindi si fa fatica a mapparli se spesi su Lightning Network per esempio.

- **Essendo il codice open source di libero accesso non dovrebbe essere più facile da attaccare?**

  Il codice open source essendo libero è visibile sia da chi ha intenzioni malevole che da chi lo revisiona, lo controlla e lo perfeziona. Essendo che, fortunatamente ancora oggi, viviamo in una società dove chi ha buone intenzioni è in numero maggiore di chi invece è un attore malevolo, eventuali bug vengono presto intercettati e sistemati. Inoltre, il codice reso pubblico da tempo in genere senza subire attacchi è la prova vivente della sua resistenza. Al contrario codice privato non è revisionabile il che significa che è vero che non dovrebbe subire attacchi, ma ci stiamo nuovamente fidando di chi lo ha generato.

- **Come mai se ho effettuato un trasferimento di bitcoin da un wallet ad un altro non lo visualizzo?**

  Dopo essersi accertati di aver copiato bene l'indirizzo di destinazione (poiché se errato i fondi potrebbero essere perduti per sempre), si può verificarne lo stato copiando l'identificativo della transazione all'interno di un blockchain explorer come Mempool che ci fornisce le informazioni quali, indirizzo di partenza, di arrivo, fee pagate ecc.
  Spesso se non si visualizza lo spostamento dei fondi, è possibile che le fee (commissioni) impostate siano troppo basse e questo fa sì che i miner non la inseriscano nel blocco.
  È possibile modificare la fee impostata in modo da dare priorità alla transazione facendo un "replace by fee" (RBF), letteralmente rimpiazzare la commissione. Una transazione si considera quasi indelebile nella rete dopo sei conferme, ossia sei blocchi, poiché la probabilità che questa venga invalidata oltre quel termine diventa irrisoria.

11. Cenni di Sicurezza e Privacy

Difficoltà: 1

Il senso di sicurezza e di privacy è un concetto personale. C'è chi la sottovaluta e chi la sovrastima, possiamo semplificare e dire che dipende principalmente da due fattori: le quantità da proteggere e l'esperienza dell'utente.

Nel primo caso infatti proteggere un portafoglio che contiene 0,1 BTC rispetto a quello che custodisce 10000 satoshi, è ben diverso, nel secondo infatti possiamo decidere di detenerli anche in un wallet custodial Lightning per pagare il caffè al bar praticamente senza commissioni. Conservare 0,1 BTC in un wallet lightning invece è un rischio, in quel caso parliamo magari di risparmi che siamo intenzionati a proteggere, e per questo vanno custoditi all'interno di un wallet non custodial di cui si hanno le chiavi private. Il seed va poi conservato in modo da durare nel tempo e non essere alla vista di tutti, non va salvato su cloud e preferibilmente generato offline con metodi randomici. Un ottimo metodo per fare ciò è come quello dei dadi o utilizzando ad esempio il rumore del microfono per generare un'entropia, ossia delle informazioni casuali e caotiche per essere quanto più difficili da duplicare. Lo spiega molto bene Massimo Musumeci in questo video con una guida passo passo.

Un seed va protetto prima di tutto da noi stessi, se non stiamo attenti a custodirlo e lo perdiamo non avremo più accesso a quei fondi. In linea di massima possiamo definire 3 tipi di rischio: noi stessi come abbiamo appena detto, attaccanti online e attaccanti fisici. Un metodo per contrastare un attacco fisico è quello di dividere il seed in 3 parti aventi ognuno delle parole in comune in modo da poter rigenerare il wallet con 2 parti qualsiasi di 3 totali. Questo fa sì che si possa dare a 2 persone di cui ci si fida parte del seed, scegliendole con criterio poiché insieme potrebbero ripristinarlo. Questa metodologia di custodia è descritta dettagliatamente da Riccardo Masutti in questo video. Nella tabella sotto proverò a dare un punteggio ad azioni diverse per tutti e tre i rischi sopra elencati:

Valutazione del rischio (Basso, Medio, Alto)					
Detenere BTC	**Noi stessi**	**Attaccanti Online**	**Attaccanti Fisici**	**Difficoltà Utente**	**Commenti**
Su Exchange	Medio	Alto	Medio	Basso	Come già specificato il rischio è alto e dipende dal provider del servizio, vale sempre la regola: "Not your keys not your coins" ossia se non hai le chiavi private non sono i tuoi fondi.

Detenere BTC	Noi stessi	Attaccanti Online	Attaccanti Fisici	Difficoltà Utente	Commenti
Con Seed salvato su PC connesso a Internet	Alto	Alto	Alto	Basso	Qui il pericolo arriva da tutti i fronti, non avere un backup offline ci espone a rischi di attacco hacker diretti a noi stessi, all'app che usiamo o peggio se salvato su cloud l'attaccante può appropriarsi delle nostre chiavi
Con Seed salvato su Cellulare	Alto	Alto	Alto	Basso	Vale il discorso sopra, con l'aggravante che l'attaccante potrebbe sfruttare le nostre vulnerabilità anche fuori casa. Dato che i device moderni si sboccano con impronta o riconoscimento facciale.
Seed su carta custodito nel portafoglio	Alto	Basso	Alto	Basso	Rischiamo che il seed sia sottoposto a deterioramento, oltre il fatto che venire derubati o perdere il portafoglio significa perdere tutto.
Seed su carta nascosto in casa	Medio	Basso	Medio	Medio	La carta potrebbe rovinarsi nel tempo e un attaccante fisico potrebbe trovarlo se non adeguatamente nascosto.
Seed inciso su acciaio nascosto in casa	Basso	Basso	Medio	Medio	Va nascosto in modo intelligente, esistono diversi metodi, ma potete usare la vostra fantasia.
Seed Memorizzato	Alto	Basso	Basso	Alto	Molto rischioso poiché la perdita di memoria, equivale a perdere i fondi, questo metodo inoltre è difficile da tramandare ai familiari
Su Hardware Wallet Open Source	Basso	Basso	Medio	Medio	Il rischio è basso ma solo se si utilizzano degli hardware wallet open source, ne esistono diversi, Bitbox02, Jade tra i più semplici da usare. Va nascosto per bene, considerato che è un oggetto più ingombrante di una lastra di alluminio.
Su Wallet Multi-signature	Alto	Basso	Basso	Alto	È attuabile da utenti esperti. Inoltre serve conoscere le XPub dei wallet. È una soluzione utile in un'azienda meno per un privato.
Dividere il Seed in 3 parti con Backup 2 di 3 parti	Medio	Basso	Basso	Medio	Bastano 2 porzioni del seed per ripristinare il wallet, ma attenzione che i nostri 2 amici non si mettano d'accordo…
Utilizzare un vecchio PC come signing device offline	Basso	Basso	Medio	Alto	È un metodo sicuro, ma più complicato. Il PC funge da Signing device, e le transazioni vanno comunicate ad un nodo.

Questi non sono gli unici metodi possibili, ma sono tra i più comuni. Ogni azione con almeno una valutazione alta andrebbe scartata, a meno che non si riesca a prendere delle contro misure per arginare il rischio. Bisogna sempre essere coscienti di quello che si fa, e soprattutto studiare accuratamente la migliore opzione in base al proprio grado di esperienza e all'importanza del capitale che si vuole proteggere.

Per chi volesse approfondire il tema della sicurezza e della privacy in Bitcoin e non solo, ma anche su internet in generale, vi consiglio il sito di Turtlecute e di ascoltare il suo podcast Il Priorato del Bitcoin

Riassunto:

1-Il concetto di sicurezza e privacy è soggettivo e dipende dal potenziale rischio in gioco, in questo caso l'ammontare, o meglio la destinazione (spesa o risparmio) del nostro capitale. Nel primo caso va bene anche un wallet Lightning custodial, nel secondo è importante possederne il seed e conservarlo con cura.

2-Esistono diversi modi per custodire i propri bitcoin, ma l'importante è farlo scegliendo il modello più idoneo alle nostre esigenze e attitudini, poiché anche noi stessi rappresentiamo una vulnerabilità oltre ovviamente ad attaccanti esterni (fisico o online).

3-Nella tabella sopra ogni valutazione a rischio alto andrebbe scartata. Inoltre vale sempre la regola che detenere bitcoin tramite un exchange è la soluzione più rischiosa poiché "not your keys, not your coins".

Domande e Risposte:

- **Se io non ho conoscenze informatiche, perché dovrei preferire di detenere bitcoin su un wallet non custodial?**
  Perché è vero che è più semplice gestire i fondi e in genere un servizio di custodia ci assiste in caso di difficoltà, ma affidarsi completamente a terzi è altamente rischioso. Salvare 12 parole su un foglio di carta non è poi così difficile, ed elimina completamente il rischio exchange.
- **Perché dovrei preoccuparmi della privacy se non ho nulla da nascondere?**

Per la propria sicurezza. Mantenere un certo grado di privacy migliora la vostra sicurezza, poiché avere informazioni significa magari conoscere i potenziali punti di attacco. Ogni volta che usiamo un social o navighiamo su internet stiamo concedendo delle nostre informazioni che vengono usate nella migliore delle ipotesi per proporci pubblicità mirata, nelle peggiori invece esporre il nostro indirizzo, patrimonio ecc.

12. Ricevere Pagamenti in Bitcoin

Difficoltà: 1

Se sei un commerciante che vorrebbe accettare bitcoin come forma di pagamento hai diverse strade, alcune sono semplici ma hanno delle limitazioni, altre più complesse che una volta comprese però hanno dei grandi vantaggi. A mio avviso un negoziante dovrebbe offrire pagamenti sia on-chain nel caso di spese importanti che Lightning. Tra i wallet on-chain mobile si può scegliere fra tantissimi come ad esempio Blue wallet, Green wallet oppure Sparrow ed Electrum di cui abbiamo parlato anche nel capitolo 10. Se invece volessimo ricevere pagamenti su Lightning Network, (da qualche centesimo a 100/200 Euro) come già accennato nel capitolo 8 inerente Lightning Network le opzioni in ordine di semplicità a mio parere sono:

-Wallet of Satoshi si definisce il wallet Lightning più semplice in assoluto ed è effettivamente cosi. Come già detto ha i pulsanti essenziali per poter inviare e ricevere pagamenti, che arrivano istantaneamente con il compromesso di essere custodial. Fra le opzioni esiste la possibilità tramite il pulsante "punto vendita" di generare un QR Code dopo aver impostato il totale di pagamento e una nota (dove si può scrivere per esempio un'ID dello scontrino in modo che sia riconducibile al pagamento, oppure semplicemente l'elenco degli articoli acquistati). È inoltre possibile fornire ai nostri clienti un indirizzo, che è visibile se si clicca sul pulsante "ricevi" in modo da poter ricevere delle donazioni libere da parte di chi ci paga (il mio ad esempio è **alessio@walletofsatoshi.com**) poiché per loro basta inserire importo e indirizzo. Potreste per esempio inviarmi qualche satoshi all'indirizzo sopra oppure semplicemente inquadrando il QR Code per fare pratica e mi raccomando di lasciarmi anche un messaggio.

-Breeze abbiamo anche di questo wallet mobile già parlato, ma affrontiamo meglio la questione relativa ai pagamenti qui. La sezione più interessante è il POS per un rivenditore, si può infatti creare una lista di prodotti con il prezzo in Euro inserendo un codice univoco come un codice a barre (SKU), è anche possibile importare una lista tramite file .csv o esportarla per fare un backup, o per trasferirla a più device. Immaginate di andare al supermercato e di scansionare gli articoli che volete acquistare e quasi per magia al termine di questa operazione vi compare a schermo un QR Code riassuntivo del pagamento da effettuare, con al suo interno la lista dei prodotti presi. Oppure in pizzeria al posto del menu potreste avere uno schermo dal quale scegliere le vostre pizze e una volta fatto l'app vi genera in automatico il QR Code del pagamento e allo stesso modo funzionerebbe per uno store online.

Esistono poi dei sistemi che vi permettono di avere di più, come BTCpay Server che è un software open source modellabile in base alle vostre esigenze. Esso infatti è integrabile all'interno del vostro store online, ma anche capace di creare un crowdfunding per scopi umanitari o artistici ad esempio. BTCpay Server è dunque uno strumento versatile e personalizzabile, ma richiede un minimo di studio personale e di impegno, al contrario del servizio chiavi in mano offerto da Bitcoin People. Essi infatti hanno sviluppato un gestionale chiamato BPay partendo proprio da BTCpay Server, ed essendo un'azienda italiana forniscono assistenza e personalizzazione del servizio anche tenendo conto degli obblighi legislativi, fornendo per esempio un report utilizzabile per i calcoli dichiarativi. Saranno loro a guidarvi e metteranno in piedi la struttura di pagamento a vostro piacimento.

Riassunto:

1-Accettare bitcoin come metodo di pagamento oggi è possibile sia via Lightning che on chain per importi più significativi.

2-Tra i wallet on chain spiccano Sparrow ed Electrum di cui abbiamo parlato anche in precedenza, invece fra i wallet Lightning troviamo soluzioni custodial come Wallet of Satoshi, e non custodial come Breeze. Per entrambi i casi esiste anche la finestra POS adatta ad un negozio.

3-Nel caso di un wallet Lightning è anche possibile ricevere pagamenti o donazioni semplicemente fornendo un identificativo facile da ricordare al posto del QR Code, il mio ad esempio è alessio@walletofsatoshi.com.

Domande e Risposte:

- **Quali attività sono più indicate per un wallet Lightning?**
  Un negozio a mio avviso dovrebbe offrire entrambe le possibilità, perché l'una non esclude l'altra. In genere dei pagamenti di piccoli importi e frequenti come possono essere quelli di un bar o un ristorante, avvengono immediatamente e senza commissioni su Lightning. Al contrario un rivenditore di auto usate ad esempio, non ha alcun motivo di ricevere pagamenti su Lightning, perché preferisce affidarsi al pagamento sicuro on chain anche se questo costa qualche Euro a chi paga, e se significa aspettare qualche conferma dalla rete.
- **Quanto variano le commissioni su lightning?**

Le commissioni possono variare in base allo strumento che si usa, se si paga tramite Wallet of Satoshi verso un altro dello stesso provider, in genere si può pagare anche 1 satoshi circa 3 centesimi di centesimo di Euro (0,0003 Euro). Altri servizi offrono una commissione in percentuale, o in base all'instradamento del pagamento(routing), anche in questo caso parliamo di quantità minime sempre a carico di chi paga.

13. Bitcoin nel Mondo, in Italia e Propaganda di Stato

Difficoltà: 1

Adesso che abbiamo approfondito e ci possiamo definire dei neo patentati in Bitcoin capaci di muoverci ma non di strafare, vediamo qual è il ruolo che ha già acquisito Bitcoin nel mondo e qual è suo livello di adozione.

Il 7 Settembre 2021 Bitcoin diventa moneta a corso legale nel paese di El Salvador (anche se non in modo restrittivo) questo traguardo segna un momento storico fondamentale per il percorso di Bitcoin. Seppur l'adozione nel paese risulta essere scarsa come ampiamente testimoniato dai Bitcoin Explorers Rikki e Laura, due ragazzi che viaggiando nel paese centroamericano, hanno deciso di soggiornarvi spendendo solo bitcoin. La loro avventura è stata difficile ma possibile, infatti sono riusciti nel loro intento di non utilizzare la moneta FIAT. Al di là di questo, nel paese stanno nascendo delle interessanti iniziative di istruzione in favore dei cittadini in merito al tema Bitcoin e il paese si sta muovendo per poter attivare una centrale elettrica che utilizza energia geotermica per minare Bitcoin. Il paese di El Salvador se pur piccolo ha fatto parlare di sé negli ultimi due anni, e il turismo ne ha risentito positivamente. Inoltre buona parte delle rimesse hanno iniziato a confluire nel paese in bitcoin. Le rimesse, come accennato nel capitolo 6 sono i soldi inviati verso i cittadini di un paese (in questo caso El Salvador) da parenti che invece lavorano nei paesi del primo mondo in genere.

Altri paesi stanno iniziando ad interessarsi al fenomeno come la Repubblica Centrafricana che nell'Aprile del 2022 dichiara Bitcoin a corso legale. In entrambi i casi si tratta di paesi del terzo mondo che si trovano ad essere schiavi del dollaro nel primo caso o del Franco coloniale nel secondo.

Esistono altre realtà dove non vi è un'autorizzazione governativa a permettere gli scambi in bitcoin, ma è la gente che si rende conto della straordinaria efficienza e della libertà che acquisiscono utilizzandolo. Sono esempio di questo modello la Nigeria, dove l'obbligo all'utilizzo della moneta digitale di Stato la eNaira ha praticamente eliminato il contante, e ha fatto sì che la gente trovasse l'alternativa in bitcoin. Il paese africano è infatti al terzo posto mondiale per numero di transazioni. Ritornando in centroamerica altri paesi si dimostrano Bitcoin friendly con un adozione che parte dal basso ossia dalla gente. Fra questi va menzionato il Guatemala con il suo Bitcoin Lake e la Bitcoin Jungle del Costa Rica. In entrambi i casi si tratta di formazioni spontanee da parte della comunità locale consistenti in un micro ambiente dove bitcoin è ben visto e accettato dagli esercenti locali.

A far nascere queste iniziative può essere una quasi assenza dello Stato, che non è in grado di tenere sotto controllo l'iperinflazione della moneta FIAT. Questo è ciò che sta accadendo in Libano dove l'inflazione viaggia intorno al 260%, dove alla popolazione è stato negato l'accesso al proprio conto in banca e quindi ai propri risparmi. Situazione simile ma meno grave è quella della Turchia con un iperinflazione del 60% all'anno. In questi paesi diventa fondamentale proteggersi con una moneta forte, magari incensurabile come bitcoin, infatti le testimonianze dirette di Rikki e Laura che hanno intrapreso anche un'avventura in questi luoghi ce lo ci confermano.

Eccezione in mezzo ai paesi in via di sviluppo è la Svizzera e in particolare la città di Lugano. Qui l'amministrazione comunale ha dichiarato bitcoin moneta a corso legale, i cittadini potranno spenderli nelle oltre 300 attività che il accettano, ma anche usarli per pagare le tasse. La città è fortemente impegnata nel promuovere l'istruzione sul protocollo Bitcoin, e ospita una delle conferenze in tema più importanti d'Europa, il PlanB Forum.

In molti paesi invece il traino è il vantaggio economico che hanno i miner, poiché questi decidono di piazzarsi dove riescono ad ottenere energia a basso costo. Stati come il Texas ad esempio negli USA sembrano aver compreso il contributo che può dare questa nuova forma di utilizzo dell'energia in esubero, e sembrano muoversi nella direzione di favorirne lo sviluppo. Questo potrebbe anche essere un mezzo al fine dell'adozione degli esercenti nelle zone limitrofe.

Esaminando la situazione in Italia invece vediamo che si iniziano a formare delle comunità di esercenti che accettano bitcoin magari grazie allo sforzo di persone entusiaste della tecnologia che l'hanno proposta generando intorno un effetto rete nei confronti di altri negozianti. Tramite il sito BTC Map, o tramite la stessa app mobile, è possibile consultare e aggiornare i negozianti che accettano bitcoin anche in Italia o bitcoin ATM dislocati nel paese. Esistono inoltre dei siti sostenuti dalla comunità locale dove si possono trovare dei prodotti o servizi a km0, ne è un esempio il sito Orange Economy messo in piedi dai ragazzi del Satoshi Spritz Bologna

In contrapposizione a quanto detto vi sono gli Stati mondiali che soffrirebbero una perdita enorme di potere. Ricordiamo infatti che uno Stato, anche democratico basa la sua influenza e la sua forza autoritaria grazie ai tre poteri che gli sono stati "concessi" dai cittadini tramite delle elezioni che nella migliore delle ipotesi sono rappresentative, ossia il potere politico, economico e militare. Questi sono strettamente correlati, poiché in assenza di uno gli altri vengono a mancare. Nel nostro caso specifico l'introduzione di una moneta decentralizzata, non governabile, non inflazionabile e inarrestabile come bitcoin, fa sì che venga a mancare uno dei tre pilastri di uno Stato autoritario, ossia la possibilità di

regolare l'emissione della moneta. A questo punto diventa difficile sostenere un potere militare senza la stampa di denaro a debito, e di conseguenza viene a mancare la fiducia verso un ente che non riesce più ad imporsi con la forza che perde anche il suo potere di dettare legge e di fare politica.

Questa è la ragione per la quale la diffamazione nei confronti di Bitcoin è l'unica strada percorribile, da parte degli Stati, servendosi dei media, al fine di influenzare le coscienze dei cittadini.

A prova di ciò, sotto trovate alcuni articoli pubblicati da testate giornalistiche che screditano Bitcoin.

Leggendo questi articoli scorgo solo due possibilità: o chi ha scritto conosce bene Bitcoin e ne vede un pericolo per lo status quo e quindi ne parla volutamente omettendo o travisando informazioni in malafede, oppure questi giornalisti sono assolutamente degli ignoranti patentati, e fanno male il loro lavoro, senza fare le dovute ricerche, e scopiazzando articoli vecchi.

https://www.tgcom24.mediaset.it/e-planet/bitcoin-mining-criptovaluta-impatto-ambientale-inquinamento_71751272-202302k.shtml#:~:text=I%20Bitcoin%2C%20buco%20nero%20energetico,dell'elettricit%C3%A0%20consumata%20in%20Italia&text=I%20Bitcoin%2C%20la%20moneta%20virtuale,ha%20un%20devastante%20impatto%20ambientale.

Nell'articolo sopra di Tgcom24 oltre fare riferimento ad una ricerca vecchia sui consumi di Bitcoin, si associa il consumo energetico alla produzione di CO_2, senza considerare che il mining di Bitcoin è l'industria più green al mondo con oltre il 52% di energia prodotta da rinnovabili. Comico anche il video che esordisce dicendo che Bitcoin pur essendo intangibile è una delle attività più inquinanti al mondo e ripetono gli stessi luoghi comuni di sempre ma lasciando intendere come epilogo: Ethereum, la "prediletta dalla commissione europea", omettendo che questa tecnologia non porta nessuna innovazione ed è assolutamente centralizzata poiché i nodi risiedono per la maggior parte su server di Amazon.

https://www.lastampa.it/economia/2023/10/24/news/bitcoin_valore_produzione_oggi-13806336/#:~:text=Bitcoin%2C%20produrre%20le%20monete%20digitali,in%20un%20anno%20in%20Italia

Anche nell'articolo sopra si utilizzano gli stessi dati vecchi, la vera domanda è quale giornalista ha scritto per prima l'articolo e chi invece ha scopiazzato?

https://forbes.it/2022/10/06/bitcoin-industria-inquinamento-pianeta/

Anche Forbes usa gli stessi dati del 2020-2021, arrivando anche loro alla stessa conclusione che Ethereum ci salverà tutti!

Questi sono solo alcuni esempi di articoli fuorvianti in merito al tema Bitcoin. Se non siete ancora convinti della malafede di chi scrive i prossimi articoli vi faranno cambiare idea, poiché emerge chiaramente il loro intento malevolo, soprattutto se si tratta della Banca Centrale Europea (BCE) che avrebbe solo da perdere in un mondo basato su un bitcoin standard.

https://www.ecb.europa.eu/ecb/educational/explainers/tell-me/html/what-is-bitcoin.it.html

Questo articolo fa sbellicare dalle risate. Nello spiegare cos'è Bitcoin fanno leva sul fatto che ***non sono garantiti da nessuno***. Su questo punto abbiamo visto che in realtà è vero che tecnicamente non sono garantiti da nessuno perché sono garantiti da tutti i nodi della rete in modo immutabile. Se poi per garanzia intendono una moneta detenuta o emessa a piacimento dalle banche centrali o commerciali, le quali fanno riserva frazionaria dell'1% quando va bene, allora si, preferisco che non sia garantita da nessuno!

Si fa inoltre appello alla parola ***fiducia*** come se fosse un termine positivo nell'ecosfera economica, e poi i paladini aggiungono: "*Come custodi della moneta unica, lavoriamo per garantire il tuo diritto di pagare in Euro e per **preservare il suo valore**.*" A questo punto ho bisogno di un fazzoletto perché l'intensa risata mi sta facendo lacrimare gli occhi…Preservare il suo valore??? Stiamo scherzando? Con un inflazione a doppia cifra che valore stanno preservando?

Si continua poi rilanciando sul fatto che bitcoin non è una forma di pagamento comunemente accettata, (questa mappa dei negozi che accettano bitcoin nel mondo è in continuo aggiornamento vale la pena darci un occhio esiste anche la versione app per cellulare), infilano il dito nella piaga dicendo che le transazioni sono lente e costose, ovviamente senza menzionare Lightning Network dove le stesse sono istantanee e con commissioni praticamente trascurabili.

Concludono la carrellata delle stupidaggini enfatizzando il fatto che gli utenti sono a rischio hacker senza tutele legali (la seed phrase va custodita in un luogo sicuro e non online, noi siamo gli unici responsabili di eventuali smarrimenti e nessuno può aiutarci) e pressando sul fatto che il valore di bitcoin è estremamente volatile, ma noi sappiamo che può esserlo in un breve periodo. Nel lungo invece, 3-4 anni ha sempre dimostrato un apprezzamento notevole, poiché è un asset assolutamente scarso che si sta diffondendo.

Quanto scritto dalla BCE sembra il preambolo per l'articolo successivo che introduce la CDBC (Central Bank Digital Currency) dell'Europa ossia l'Euro digitale.

https://www.ecb.europa.eu/paym/digital_euro/html/index.it.html

Dall'articolo si intuisce che l'Euro digitale si baserà su tecnologia blockchain, gli utenti infatti potranno avere un proprio wallet, inizialmente affiancherà il contante, per non spaventarci troppo. Non ci saranno commissioni, e si potrà scambiare valore anche fra amici all'istante come ad esempio per dividere un conto alla romana in pizzeria. Tutto bellissimo, ma allora questo ebook è totalmente inutile! Che ce ne frega di Bitcoin quando possiamo utilizzare il fantasmagorico Euro digitale?

Se la pensate ancora cosi vi consiglio di rileggerlo, l'Euro digitale è una forma di schiavitù, di cessione completa di privacy all'ennesima potenza.

Ad ogni wallet corrisponde un cittadino con nome e cognome, questo è continuamente monitorato negli acquisti, negli spostamenti concedendo così l'ultima briciola di privacy che si aveva prima dell'avvento degli smartphones.

La BCE, e quindi di conseguenza gli Stati, possono erodere i conti dei cittadini con le tasse senza possibilità di appello, allo stesso modo con le multe, o magari porre una data di scadenza alla moneta digitale, in modo da favorirne la messa in circolo e disincentivare il risparmio.

L'Euro digitale, o le CDBC in generale, sono il modo più efficace per tenere sotto controllo la popolazione. Lubrificheranno la supposta con le commissioni a zero spese, o con del bel cashback (tanto è moneta stampata…anzi scusate a questo punto è semplicemente emessa dal nulla) in questo modo ci corromperanno e ci accompagneranno in questa transizione.

Chiudo il capitolo con un'ultima riflessione. Come mai si sta facendo tanta pubblicità contro Bitcoin e non lo si sta facendo per altre criptovalute, a partire da Ethereum? Spesso questa viene addirittura proposta come soluzione. Il motivo è subdolo ma basilare, non è perché la rete Ethereum consuma meno energia, ma bensì perché essendo centralizzata è facile da stroncare o da plasmare a piacimento. Dimostrando di fatto la concentrazione del lavoro di disinformazione verso l'unico ostacolo che è rappresentato da Bitcoin, poiché questo è inarrestabile, gestito da tantissimi nodi dislocati nel mondo alcuni anche oscurati impossibili da raggiungere. Bitcoin è la voce della maggioranza e del popolo, per questo Bitcoin è libertà.

Riassunto:

1-Bitcoin ha fatto parlare di se in molti paesi come in El Salvador e nella Repubblica Centroafricana diventandone moneta a corso legale, ma anche in paesi come la Nigeria, Guatemala e Costa Rica dove l'adozione è partita da iniziative popolari.

2-Esistono nel mondo paesi come il Libano e la Turchia dove l'iperinflazione è un serio problema e per il quale Bitcoin potrebbe rappresentare una valida via di fuga.

3-Bitcoin è nemico degli Stati, perché ha il potenziale di sottrarre uno dei tre poteri allo Stato ossia quello di emettere moneta e di regolarne i flussi. Senza questo gli altri due (potere militare e politico) fanno fatica a sostenersi.

4-Per questo motivo la stampa, che non è oggettiva, cerca in tutti i modi di infangare Bitcoin con articoli che riportano notizie vecchie, parziali o completamente false. Allo stesso modo gli articoli della BCE (Banca Centrale Europea) denigrano Bitcoin in favore di Ethereum o addirittura preparano il campo alla CDBC (Central Bank Digital Currency) ossia l'Euro digitale. Nel capitolo sopra alcuni articoli come esempio.

Domande e Risposte:

- **Perché l'adozione di Bitcoin è più efficace se proveniente dalla popolazione e quindi dal basso?**
  Un'adozione imposta da uno Stato è tirannia, soprattutto se questo non gode della fiducia dei propri cittadini. Agli occhi di quest'ultimi infatti, anche Bitcoin è una cosa di Stato e per questo non è il metodo più veloce per un'adozione di massa. Personalmente credo di più in una diffusione che parta dai commercianti, magari in piccole comunità che concretamente provino e permettano di utilizzare bitcoin come metodo di pagamento, come prova concreta della bontà del protocollo e dei vantaggi che porta. Questo è anche lo scopo di questo libro, ossia riuscire a far conoscere Bitcoin ai commercianti per un'adozione dal basso, come rivoluzione pacifica ad investimento zero.
- **Se Bitcoin elimina il potere monetario di uno Stato, e questo a cascata fa crollare quello militare e politico, cosa potrebbe succedere agli Stati?**
  Questa domanda me la pongo pure io, poiché sarebbe il primo esperimento in tal senso e nessuno ha la certezza di quello che un cambiamento cosi grande porterebbe alla società

umana. Esistono diverse teorie più o meno libertarie che spaziano dal completo fallimento degli Stati e la privatizzazione di tutti i servizi (con conseguente miglioramento degli stessi), a una coesistenza di uno Stato che migliora l'efficienza grazie alla concorrenza privata. Personalmente credo nella corruzione dei governanti, che ad un certo punto avranno capito il potenziale economico di Bitcoin e per puro egoismo e ingordigia, troveranno il modo per permetterne una maggiore diffusione. Questa, seppur poco nobile, è forse l'eventualità meno drastica, nei casi più estremi l'astio dello Stato potrebbe essere vigoroso.

- **Perché alcune banche commerciali iniziano ad offrire servizi di custodia di bitcoin andando contro quanto viene pubblicizzato dalle banche centrali?**
  Una banca centrale di uno Stato emette moneta, di fatto ne ha il potere, Bitcoin elimina questa concessione, quindi una banca centrale non ha alcun interesse nel sostenere Bitcoin al momento. Al contrario una banca commerciale non emette moneta, ma concede prestiti alla popolazione, in cambio di un interesse (che fluttua a causa delle politiche monetarie della banca centrale). Possiamo paragonarle quindi ad altri commercianti perché offrono un servizio in cambio di un pagamento (in questo caso gli interessi, ma anche i costi di gestione dei conti ecc.). Allo stesso modo di un bravo commerciante le banche commerciali andranno a cercare il miglior guadagno con il minor sforzo e quindi offrire custodia di bitcoin in cambio di un costo di gestione o di prelievo. Si aprirebbe così un mondo di entrate nuove e diversificate che fungerebbero anche da collaterale nel caso di prestiti e tante altre possibilità.

14. Bitcoin e Tassazione in Italia

Difficoltà: 1

L'Italia è stato uno dei primi Paesi in Europa a regolarizzare le cripto-attività con l'introduzione della Legge di Bilancio 2023 in accordo al Regolamento MiCA dell'Unione Europea.

Non essendo io un commercialista, né tantomeno un avvocato fiscalista, mi atterrò semplicemente ad accennare l'argomento. Ogni valutazione o decisione intrapresa andrebbe coordinata con un professionista, aggiungo anche che in questo capitolo, non esprimerò la mia opinione in merito al fatto se sia moralmente corretto o no, pagare le tasse sulla detenzione o sullo scambio di bitcoin.

La Legge di Bilancio 2023, definisce il concetto di cripto-attività inglobando tutto il comparto (monete, token, NFT ecc.). Prima di questa introduzione non vi era una legge specifica che disciplinasse le criptovalute, ma queste venivano considerate (forse impropriamente) alla stregua delle valute estere.

Questo significava, per i possedimenti prima del 2023, un monitoraggio fiscale utilizzando il quadro RW della Dichiarazione dei Redditi e imposizione fiscale del 26% alle plusvalenze se il patrimonio era superiore a 51645,69 Euro (100 milioni delle vecchie Lire) per almeno sette giorni consecutivi.

Con la nuova Legge di Bilancio 2023 rimane il monitoraggio delle cripto, ma con l'introduzione dell'imposta di bollo del 2%. Si tassano invece gli scambi da cripto a moneta FIAT o anche fra cripto-attività di natura diversa, nella misura del 26% su plusvalenze maggiori di 2000 Euro.

Questo in breve ciò che mi sembra di aver capito dalla legge, ma per avere conferme e maggiori dettagli consultare un professionista.

Questo capitolo non presenta il riassunto perché la mia descrizione sopra è già molto poco approfondita, inoltre non ho inserito nemmeno le domande e risposte poiché non sono competente a dare risposte in questo ambito.

15. Conclusioni e Contatti

Difficoltà: 1

Spero che questo libro vi sia piaciuto, mi scuso nel caso possano esserci imprecisioni o veri e propri errori, non sono né un informatico né uno scrittore. In questo ebook abbiamo trattato argomenti di storia, tecnologia, matematica, crittografia, politica, economia, ecologia, libertà, attualità, sicurezza, privacy e forse altri. Questo perché Bitcoin è un argomento (come dice Ale The Orange Way nel suo Arancione Podcast) multidisciplinare che tange e devia la nostra visione del mondo in diversi aspetti. Non sempre ciò che ci viene raccontato è verità, bisogna crearsi una propria idea attingendo da diverse fonti anche contrastanti, per poter elaborare un proprio pensiero. Bitcoin in me ha incrementato lo spirito critico costruttivo, rendendomi una persona migliore. Immaginiamo per un attimo di essere un cristiano qualsiasi vissuto a cavallo del 1600. Un giorno arriva un pazzo con un nome è un cognome praticamente identico e afferma che la terra ruota attorno al sole e non viceversa come sempre saputo. Tutto ciò è smentito dal fatto che il sole si sposta, come sempre, ogni giorno da est a ovest, quindi non può essere vero. Eppur (la Terra) si muove, e aveva ragione! Quindi raccogliete le informazioni ed elaboratele anche se queste possono sembrare assurde.

Il mio intento con queste poche pagine non è erudirvi o rendervi dei professionisti in Bitcoin, né tanto meno davi dei consigli finanziari, ma scatenare in ognuno di voi una scintilla per poter approfondire in modo autonomo. Mi rendo dunque conto che la “guida” non sarà esaustiva, ma abbastanza per iniziare a masticare l’argomento e a poter effettuare in autonomia i vostri primi movimenti, e le vostre ricerche perché Bitcoin non è una cosa assoluta, ma per ogni persona può avere diverse sfaccettature.

Vi condivido altre due fonti di approfondimento molto valide:

Mir Serena

In questa pagina di GitHub trovate una “lista di risorse” come le definisce Mir molto esaustiva di materiale inerente Bitcoin

PlanB Network

In questo sito si possono trovare diversi corsi gratuiti da livello facile ad avanzato in collaborazione con il nostro grande Giacomo Zucco.

Io non guadagno nulla nel promuovere questo libro, che è assolutamente gratuito, ma sono arrivato alla conclusione che le persone hanno bisogno di ascoltare un'altra campana diversa da quella che ci viene

inculcata di forza dai media statali, e che possano farsi un idea propria e soprattutto libera. Conoscere Bitcoin è un'opportunità data a coloro che sono pronti ad ascoltare, e se questo ti risulta difficile, o ti fa arrabbiare è perché quanto detto stravolge il tuo modo di pensare. Non è un problema, ma questo spero possa scatenare in te la curiosità almeno all'approfondimento della materia.

Se questo contenuto ti è piaciuto e pensi possa essere utile a qualcun altro sei obbligato a condividerlo assolutamente, non ci sono copyright proprio per i motivi sopra descritti. Il mio intento è quello di diffonderlo quanto più possibile fra i commercianti, iniziando da Bologna, e se questo funziona spingermi oltre. Il vostro aiuto del diffonderlo può essere quindi determinante, fatelo conoscere ad amici e parenti, ma anche ai vostri negozianti preferiti in modo che anche voi possiate provare l'ebrezza di spendere sotto casa una moneta libera.

Se poi questo ebook ti è stato utile e vuoi sostenermi economicamente affinché io possa continuare a diffonderlo e a produrre materiale informativo anche sotto diverse forme (scrivo anche canzoni e sto tentando di indirizzare la mia produzione musicale incentrandola sul tema Bitcoin), allora potresti aiutarmi facendo una donazione e mettendo in pratica le tue skills da bitcoiner usando:

Indirizzo Bitcoin on chain:

bc1qkw9uwtaexdxu5573xnzcccryv777l32frzl9l4

QR Code:

Indirizzo lightning:

alessio@walletofsatoshi.com

Potrete scrivermi tramite indirizzo email: alessiocardella@proton.me per qualsiasi dubbio, o per darmi consigli e migliorie riguardanti questa versione 1.0 della guida. Allo stesso modo se siete dei commercianti che magari (anche grazie a questo e-book) avete deciso di accettare bitcoin, fatemelo sapere in modo tale da verificare la vostra presenza all'interno della BTCMap e nel caso aggiungervi.

Potrete inoltre visualizzare i miei contenuti tramite i social sotto:

Facebook

Instagram

X

Youtube

Spotify

GitHub qui troverete l'ultima versione dell'E-book.

Per essere sicuri di avere quella ufficiale confrontare l'Hash SHA256 del PDF in vostro possesso con quello del sito riportato su GitHub.

Grazie e buono studio, acquisto, custodia e spesa dei vostri bitcoin!

Un ringraziamento speciale a Sylvia, fondatrice e amministratrice del Satoshi Spritz Bologna nonché consulente e divulgatrice Bitcoin, per aver revisionato l'E-book.

"If you don't believe me or don't get it, I don't have time to try to convince you, sorry."

-Satoshi Nakamoto