Diploma Bitcoin

L'educazione finanziaria nell'era Bitcoin

Versione - 1.01 - Giugno 2025 - Leo

Libro di lavoro per studenti

Versione italiana | 2025

Diploma Bitcoin

L'educazione finanziaria nell'era di Bitcoin

Libro di lavoro per studenti

Versione italiana | 2025

Il Mio Primo Bitcoin

Per Donare

bc1q5es60qpa7gpkp0k32xl4zefkj43kd9zjkzd54sgmv3yzr34dw8dqm9pzsd

La storia del diploma Bitcoin

«Nulla al mondo è più potente quanto un'idea della quale sia giunto il tempo» - Victor Hugo

La storia di Bitcoin Diploma è iniziata in El Salvador, con il primo gruppo di 38 studenti della scuola pubblica che si è diplomato nel giugno 2022; questo il primo gruppo di 38 studenti delle scuole pubbliche, diventando i primi possessori di un diploma Bitcoin in un sistema scolastico pubblico a livello globale.

Un evento che è difficile credere sia successo meno di tre anni fa.

Da allora, la crescita è stata fenomenale, con migliaia di diplomati delle nostre classi in tutto il Paese.
corsi in tutto il Paese. Tuttavia, la crescita più entusiasmante e stimolante è arrivata da altri. Il libro di lavoro è open source e una collezione incredibilmente varia di educatori Bitcoin ha adottato il materiale, sia nel corso The Bitcoin Diploma. Il materiale è stato adottato sia in El Salvador che altrove.

Il Ministero dell'Istruzione di El Salvador lo ha utilizzato come fonte primaria per il proprio diploma.
Nel 2024, in collaborazione con Bitcoin Beach, abbiamo formato oltre 400 insegnanti delle scuole pubbliche per insegnarlo nelle loro scuole.

Uno dei nostri obiettivi originari era quello di insegnare a una nazione intera e dimostrare che l'educazione ai Bitcoin è una forza per il bene su larga scala. Questo sogno è ben avviato.

El Salvador è il primo obiettivo; il mondo intero è la missione.

Nel marzo 2023 abbiamo fondato la rete internazionale di nodi educatori Bitcoin, che richiede l'accettazione di alcuni principi fondamentali da parte di tutti i nodi.
I nodi devono accettare i seguenti principi: l'educazione deve essere indipendente, imparziale, orientata alla comunità e basata esclusivamente su Bitcoin. L'educazione deve essere indipendente, imparziale, orientata alla comunità, di alta qualità e incentrata sull'empowerment. Questa rete, che ora ha tradotto l'opera in più di otto lingue e ha consegnato il Bitcoin Diploma in Canada, Stati Uniti, Messico, Guatemala, Honduras, Costa Rica, Cuba, Repubblica Dominicana, Haiti, Colombia, Suriname, Perù, Brasile, Argentina, Irlanda, **Italia,** Regno Unito, Portogallo, Georgia, Ghana, Nigeria, Uganda, Kenya, Zambia, Zimbabwe, Sudafrica, Afghanistan, Bangladesh, India, Hong Kong, Indonesia e Australia. La rete aggiunge nuovi nodi ogni mese e, poiché il lavoro è **open source, nessuno necessita di autorizzazioni**. È probabile che molti altri abbiano realizzato tutto da soli.

Si tratta di un movimento globale e decentralizzato.

Un'educazione indipendente, imparziale e guidata dalle comunità Bitcoin cambierà il mondo. È già successo.

Per un mondo migliore,

Il team di My First Bitcoin - 2025

Indice dei contenuti

Capitolo #5: Come i problemi portano alle soluzioni

Capitolo #6: Introduzione a Bitcoin

Capitolo #7: Come utilizzare Bitcoin

Capitolo #8: Rete Lightning: Utilizzare il bitcoin nella vita quotidiana

Capitolo #9: Introduzione al lato tecnico di Bitcoin

Capitolo #10: Perché Bitcoin?

Diploma Bitcoin

Un viaggio di trasformazione di dieci settimane attraverso l'istruzione indipendente, imparziale, di qualità e ***gratuita***

Prima di studiare il Bitcoin, è essenziale avere una conoscenza approfondita delle basi del denaro, della sua storia e dell'attuale sistema finanziario. La comprensione di questi concetti costituisce una solida base per comprendere la natura unica e dirompente del Bitcoin. Imparando a conoscere l'evoluzione del denaro, sarete in grado di comprendere meglio il potenziale e i limiti dell'attuale sistema finanziario e il modo in cui Bitcoin intende affrontarli. Senza queste basi, potrebbe essere difficile apprezzare appieno l'importanza e il potenziale impatto del Bitcoin. Abbiate fiducia nel processo di apprendimento e rimanete concentrati, perché la ricompensa di una comprensione più profonda di questo campo all'avanguardia sarà ampiamente ripagata.

Capitolo #1

Perché abbiamo bisogno del denaro?

Libro di lavoro per studenti

Versione italiana | 2025

Perché abbiamo bisogno del denaro?

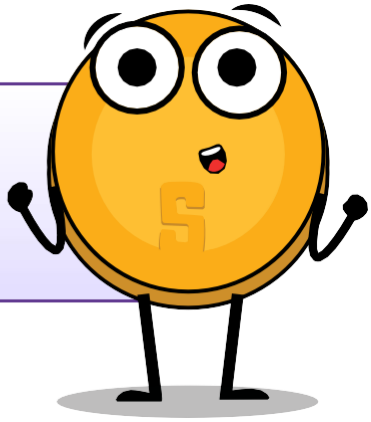
1.0 Introduzione

> Il denaro è uno dei più grandi strumenti di libertà mai inventati dall'uomo.
>
> **Friedrich Hayek**

Benvenuti al Diploma Bitcoin. In questo capitolo esploreremo la questione fondamentale del perché il denaro sia essenziale nella nostra vita. Analizzeremo la natura del denaro e le sue varie forme, con l'obiettivo di comprendere più a fondo il suo significato. Il denaro è qualcosa che usiamo quasi ogni giorno, ma capiamo davvero perché ne abbiamo bisogno e che cosa sia ? Perché i nostri genitori e familiari scambiano il loro tempo con il denaro? Perché alcune persone ne hanno più di altre? Perché il denaro è diverso in altri Paesi? Perché non possiamo crearne di più quando ne abbiamo bisogno?

1.1 Incontro con Satoshi

> *Ciao! Sono Satoshi, un assistente interattivo che ti aiuterà durante il Diploma Bitcoin. Ti fornirò risorse e consigli utili, in modo che tu possa approfondire i concetti chiave.*



Attività: Iniziamo il capitolo rispondendo ad alcune domande riportate di seguito:

Considerate gli usi pratici, come l'acquisto di beni di prima necessità come cibo e oggetti desiderati.

Cercate di essere precisi nel vostri esempi, bilanciando creatività e realismo.

Perché abbiamo bisogno del denaro ?

Che cos'è il denaro?

Perché abbiamo bisogno del denaro?

Chi controlla il denaro?

Che cosa dà al denaro il suo "valore"?

Avete domande sul denaro? Scrivete qui la vostra domanda per condividerla con la classe.

Estendete la discussione a tutta la classe, condividendo e confrontando gli elenchi per determinare le cinque ragioni più essenziali per cui si ha bisogno di denaro. Identificate le idee comuni a tutta la classe. Riflettete sulle vostre idee personali che non sono state inserite nell'elenco ma che vale la pena considerare. Annotate queste idee aggiuntive.

1.2 Discussione in classe: Perché abbiamo bisogno del denaro?

La classe deve dividersi in gruppi poi :

- Condividete e discutete le risposte alle prime quattro domande. Scrivete le risposte preferite.
- Condividete le risposte all'ultima domanda e votate la domanda preferita degli studenti. Scrivere il risultato.
- La classe può rivedere le risposte e le domande alla fine del Diploma Bitcoin.

Ora che avete una comprensione più chiara del perché il denaro sia necessario, i prossimi capitoli esploreranno cos'è, come si è evoluto nel tempo, chi lo influenza e la sua forma più recente. Continuate a fare riferimento ai vostri elenchi di questo primo giorno di lezione per tracciare collegamenti tra le vostre intuizioni e l'evoluzione della creazione, della definizione e dell'uso del denaro nel tempo.

Capitolo #2

Che cos'è il denaro?

Libro di lavoro per studenti

Versione italiana | 2025

Che cos'è il denaro?

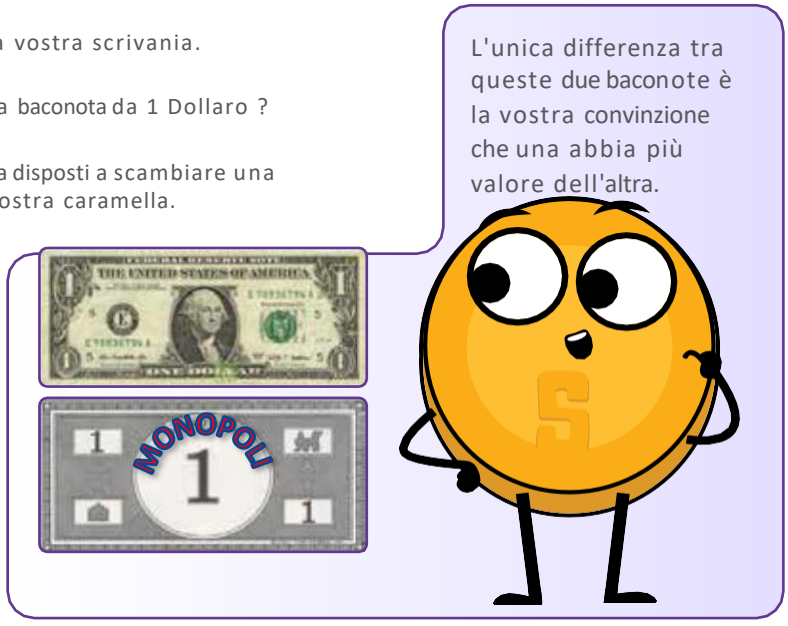
2.0 Introduzione

> Il denaro è la garanzia di poter avere ciò che desideriamo in futuro. Anche se non abbiamo bisogno di nulla al momento, ci garantisce la possibilità di soddisfare un nuovo desiderio quando si presenterà.
>
> **Aristotele**

Partendo dalla nostra esplorazione della necessità del denaro, questo capitolo esplora la domanda centrale: Che cos'è il denaro? Inizieremo con una discussione e un'attività di gruppo.

Attività: Discussione in classe - "Che cos'è il denaro?

- Non mangiate ancora la caramella posta sulla vostra scrivania.
- Chi scambierebbe la propria caramella con una baconota da 1 Dollaro ?
- Ora, tenete la mano alzata se sareste ancora disposti a scambiare una banconota del Monopoli da 1 dollaro per la vostra caramella.
- Perché si o perché no?
- Cosa rende una banconota così desiderabile e un altra come la spazzatura?
- Che cosa dà al denaro il suo "valore"?
- Da dove viene il denaro e chi decide quanto stamparne?
- Perché non stampare più altro denaro e distribuirlo equamente a tutti?



2.1 Definizione di denaro

Vi siete mai soffermati a pensare a cosa sia veramente il denaro? Vi siete mai chiesti cosa rende il denaro... beh, il denaro? La maggior parte di noi sa come usarlo, ma non molti capiscono da dove viene e come funziona. Il denaro è essenzialmente un modo per scambiare beni e servizi. Rappresenta il valore di questi oggetti in una forma che può essere facilmente scambiata. Può assumere diverse forme, come banconote di carta, monete di metallo e pagamenti elettronici.
I governi o altre autorità di solito emettono e controllano il denaro, ma il denaro è molto più di un mezzo di scambio fisico o digitale; è come un linguaggio universale che ci permette di commerciare con persone di tutto il mondo, anche se non parliamo la stessa lingua o non abbiamo la stessa cultura. Ad esempio, si può essere dall'altra parte del mondo e continuare a "parlare" di denaro mettendo un prodotto sul bancone e scambiandolo con la valuta locale o utilizzando una carta di credito.

Il denaro è come un contratto sociale che ci permette di effettuare scambi senza dover ricorrere al baratto o a trovare qualcuno che voglia specificamente ciò che abbiamo da offrire. Se un gruppo di persone iniziasse ad accettare il cioccolato come pagamento per la maggior parte dei beni e dei servizi, il cioccolato diventerebbe denaro (anche se, dato che in alcune parti del mondo si scioglierebbe, potremmo considerarlo denaro di scarsa qualità).

Come ha sottolineato l'economista francese Jean-Baptiste Say, "**il denaro non svolge che una funzione momentanea in uno scambio; e quando la transazione è conclusa, si scoprirà sempre che un tipo di merce è stato scambiato con un altro**".

In altre parole, il denaro in sé non ha il potere di soddisfare i desideri umani; è solo uno strumento che ci permette di scambiare un bene con un altro.

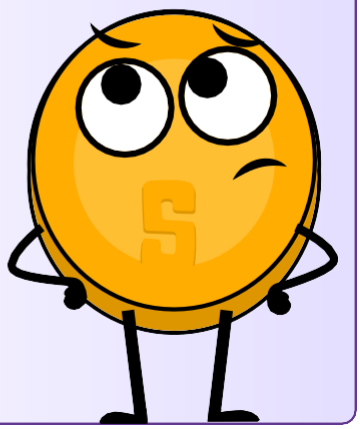
La transazione è uno scambio o un trasferimento di beni e servizi. È un modo di scambiare valore tra due o più parti.

Esistono diversi tipi di transazioni, che vanno da semplici scambi (come l'acquisto di un panino in un bar) a transazioni finanziarie più complesse (come l'acquisto di una casa o l'investimento in azioni o obbligazioni). Le transazioni possono essere condotte di persona, al telefono, online o con altri mezzi e possono coinvolgere un'ampia gamma di soggetti, tra cui individui, aziende e istituzioni finanziarie.

Senza denaro, quanto sarebbe facile o fattibile questo scambio?

Scambiereste una mucca con 1.000.000 di fragole?

O 600.000 fragole? Che ne dite di 50.000?



Guardate questo breve video!

Il denaro **è** il valore con cui si scambiano i beni.
Il denaro **NON è** il valore per il quale i beni vengono scambiati.

In sintesi, il denaro:

Facilita il commercio perché tutti lo accettano come pagamento finale. Inoltre, ci permette di misurare il valore e di fare confronti tra beni e servizi diversi. In seguito, analizzeremo la funzione del denaro.

Che cos'è il denaro?

2.2 Funzione del denaro

Quando si tratta di acquistare e vendere beni e servizi, il denaro è l'elemento chiave. Il denaro svolge diverse funzioni importanti nel mondo, come ad esempio:

1 Un deposito di valore

Il denaro dovrebbe mantenere il suo valore nel tempo, rendendolo utile come metodo per risparmiare e investire il valore del lavoro umano. In questo modo si può usare il denaro per pianificare azioni future, prendere in prestito e prestare denaro. Quindi, la prossima volta che risparmierete per qualcosa di speciale, ricordate che il denaro è più di un modo per pagare le cose: è uno strumento che vi aiuta a pianificare e investire nel vostro futuro.

Qual è il vostro deposito di valore?		BTC (USD)	Oro (USD)	USD (EUR)
	14 marzo 2019	$3,846	$1,293	€0.8817
	14 marzo 2020	$5,258	$1,529	€0.90056
	Guadagno/perdita	+36.71%	+18.25%	+2.14%

2 Mezzo di scambio

Con il denaro, non è necessario trovare qualcuno che voglia esattamente quello che avete da scambiare. Si può perciò usarlo per comprare e vendere tutto ciò che si vuole. Questo rende gli scambi e il commercio molto più convenienti ed efficienti.

3 Unità di conto

La moneta fornisce uno standard universale di valore che consente alle persone di esprimere e confrontare il prezzo di beni e servizi diversi. Questo consente un mercato più efficiente e trasparente in cui le persone possono prendere decisioni informate su cosa acquistare e vendere.

Unità di conto

I consumatori conoscono il valore di qualcosa quando gli si assegna un prezzo (valore monetario).

Pensate a questo: se voleste comprare un'auto nuova, potreste confrontare i prezzi di diversi concessionari e decidere con cognizione di causa quale comprare in base al prezzo in dollari. Senza un'unità di conto, dovreste cercare di confrontare il valore di un'auto con quello di un'altra utilizzando qualcos'altro, come il numero di vacche che vale o il tempo impiegato per produrre l'auto.

Queste tre funzioni permettono alle economie di diventare complesse e dinamiche. Senza denaro, sarebbe molto più difficile acquistare e vendere beni e servizi e la nostra economia sarebbe molto meno sviluppata.

Esercizio in classe: Quale funzione del denaro è un valido esempio ?

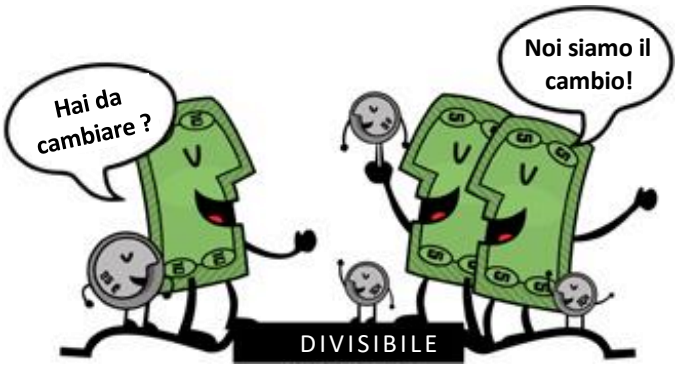
- Evan ha deciso di risparmiare una parte della sua paga settimanale per comprare un cucciolo.
- Adam compra due tranci di pizza per 8,30 dollari da Ray's Pizza.
- Marc non riesce a decidere se comprare i biglietti per un concerto a 75 dollari o uno skipass a 95 dollari.

2.3 Proprietà del denaro

Nel corso del tempo, le persone hanno capito che il denaro deve possedere determinate qualità per essere un efficace mezzo di scambio.
Queste caratteristiche includono la durabilità, la divisibilità, la portabilità, l'accettabilità, la scarsità e la fungibilità.

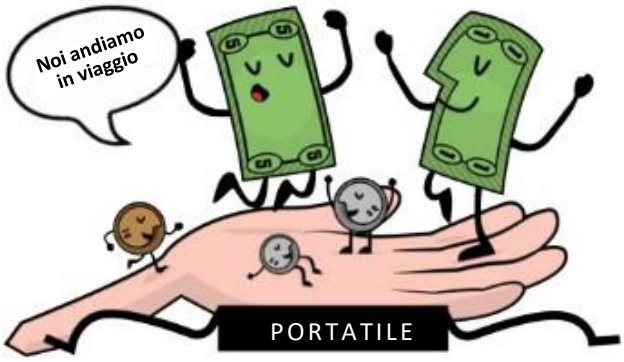
- **La durabilità** si riferisce alla capacità della moneta di resistere al deterioramento fisico e di durare nel tempo. Ciò garantisce che il denaro possa circolare nell'economia in uno stato accettabile e riconoscibile. L'oro è un materiale durevole, in grado di resistere all'usura, che lo rende una buona rappresentazione della caratteristica di durevolezza del denaro.

- **La divisibilità** si riferisce alla capacità del denaro di essere diviso in unità più piccole, in modo da poterlo utilizzare per effettuare acquisti di importo variabile. Le banconote di carta possono essere facilmente divise in tagli più piccoli, il che le rende una buona rappresentazione della caratteristica di divisibilità del denaro.



Che cos'è il denaro?

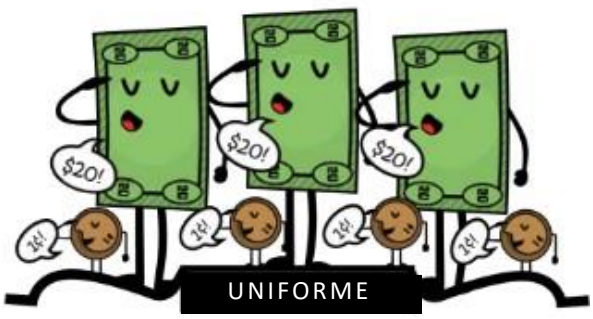
La portabilità si riferisce alla facilità con cui il denaro può essere trasportato e portato in giro. Ciò consente alle persone di utilizzare il denaro per acquistare e vendere beni e servizi senza difficoltà. Le carte di credito sono portatili, in quanto possono essere facilmente trasportate in un portafoglio o in una borsa, il che le rende una buona rappresentazione della caratteristica di portabilità del denaro.



L'accettabilità si riferisce all'accettazione diffusa del denaro come forma di pagamento, in modo che le persone possano usarlo per acquistare e vendere beni e servizi con sicurezza. Il dollaro USA è ampiamente accettato come forma di pagamento, il che lo rende una buona rappresentazione della caratteristica di accettabilità del denaro.

La scarsità si riferisce all'offerta limitata di denaro, che contribuisce a mantenerne il valore e a evitare di dover spendere di più per acquistare la stessa quantità di beni. I francobolli da collezione, soprattutto quelli rari e di valore, possono essere una buona forma di denaro perché sono scarsi e possono aumentare di valore nel tempo. I collezionisti di francobolli spesso usano i loro francobolli come un modo per investire la loro ricchezza e diversificare il loro portafoglio.

La fungibilità si riferisce all'intercambiabilità del denaro, in modo che un'unità di denaro sia equivalente a un'altra unità dello stesso valore. Il denaro deve essere uniforme. Le monete di rame hanno dimensioni e peso uniformi, il che le rende una buona rappresentazione della caratteristica di uniformità del denaro. Un centesimo è sempre un centesimo.



Nel complesso, queste caratteristiche rendono il denaro uno strumento utile ed efficace per facilitare gli scambi e il commercio, e sono essenziali per lo sviluppo e la stabilità delle economie.

Esercizio di classe

I diversi beni hanno proprietà diverse ed espletano le funzioni del denaro in misura variabile. È la società a stabilire quale bene viene utilizzato come denaro in base a fattori quali la stabilità, la scarsità, la divisibilità, la trasferibilità e l'accettazione come mezzo di scambio.

Per determinare quanto i diversi oggetti soddisfino le caratteristiche specifiche del denaro, si può assegnare un punteggio a ciascun oggetto su una scala da **1 a 5** per ogni caratteristica. Sommando i punteggi di ciascun oggetto, si può determinare quale sia il più adatto a diventare una forma di denaro.

[0 = pessimo; 3 = buono; 5 = ottimo].

*** Non compilare la colonna relativa al bitcoin; ci torneremo più avanti nel corso.**

Utilizzate le seguenti domande per determinare quanto le diverse voci della tabella soddisfino le caratteristiche del denaro.

- **Durabilità:** Il denaro è in grado di resistere all'usura nel tempo?
- **Portabilità:** Il denaro può essere facilmente trasportato e utilizzato in luoghi diversi?
- **Fungibilità:** Il denaro è intercambiabile con altre forme di denaro?
- **Accettabilità:** Il denaro è ampiamente accettato come forma di pagamento?
- **Scarsità:** Il denaro è scarso e non troppo abbondante?
- **Divisibilità:** Il denaro può essere diviso in unità più piccole per le transazioni?

Caratteristiche del buon denaro	Mucche	Sigarette	Diamanti	Euro	Bitcoin
Durevole					
Portatile					
Uniforme					
Accettabile					
Scarso					
Divisibile					
Totale					

Che cos'è il denaro?

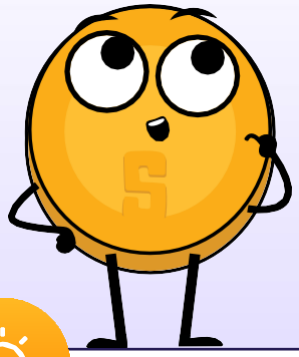
2.4 Tipi di denaro

Il denaro può essere suddiviso in due categorie principali: fisico e digitale.

Il denaro fisico comprende:

- **Denaro Fiat**, ovvero le banconote di carta e le monete emesse dai governi e accettate come mezzo di scambio.
- **Denaro rappresentativo**, che rappresenta un credito su un bene fisico.
- **Denaro merce**, ovvero un oggetto fisico che ha un valore intrinseco ed è ampiamente accettato come mezzo di scambio. Come ad esempio oro e argento.

Non tutto il denaro è uguale!



Denaro merce

Oggetti come questa polvere da sparo servivano un tempo come moneta di scambio.

Denaro rappresentativo

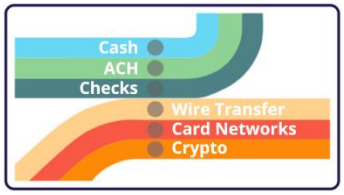
La moneta rappresentativa, come questo certificato d'argento, poteva essere scambiata con argento.

Denaro Fiat

Oggi le banconote della Federal Reserve sono denaro liquido, decretato dal governo federale come un modo accettabile per pagare i debiti.

Le valute digitali, invece, possono essere utilizzate per le transazioni online e comprendono valute elettroniche, monete stabili e criptovalute.

Le valute elettroniche sono versioni digitali del denaro normale, come il dollaro o l'euro, e possono essere utilizzate per acquistare e vendere prodotti online tramite **circuiti di pagamento** digitali.



I circuiti di pagamento sono l'infrastruttura che consente il movimento di valute elettroniche e altri beni digitali da un luogo all'altro. Tuttavia, nel sistema finanziario tradizionale c'è sempre un intermediario, come una banca o un istituto finanziario, che applica una commissione e ha l'autorità ed il potere di accettare, rifiutare, cancellare o ritardare le transazioni.

Nel sistema finanziario intermediato i principali tipi di circuiti di pagamento digitali includono le reti di carte - che facilitano il trasferimento di fondi tra le istituzioni finanziarie e gli esercenti quando un cliente effettua un acquisto utilizzando una carta di debito o di credito - e i portafogli digitali, che sono conti online che consentono agli utenti di memorizzare e gestire le proprie valute elettroniche e di effettuare pagamenti trasferendo fondi dal proprio conto a quello del destinatario.

Valute digitali delle banche centrali (CBDC – Central Bank Digital Currency)

Versioni digitali della valuta di un Paese emesse e sostenute dalla banca centrale e intermediate dal governo.

Monete stabili

Le valute digitali sono progettate per mantenere un valore stabile rispetto a un asset come la moneta nazionale, per esempio il Dollaro Americano.

Criptovalute

Un tipo di valuta digitale; alcune criptovalute sono decentralizzate e governate da regole, mentre altre sono centralizzate e controllate da un piccolo gruppo di persone.

In definitiva una moneta che opera senza intermediari è più efficiente e benefica per la società, in quanto impedisce a pochi individui di controllare l'offerta di moneta e di concentrare il proprio potere. Tuttavia, la creazione di una moneta che faciliti le transazioni sicure senza fare affidamento sulla fiducia tra le parti è stata una sfida nel corso della storia. Per raggiungere questo obiettivo, è necessario creare una moneta che funzioni come Internet, dove il controllo è distribuito tra tutti e nessuno allo stesso tempo. Ciò richiede il consenso di tutte le parti (compresi coloro che detengono il potere) a rinunciare al controllo per il bene comune.

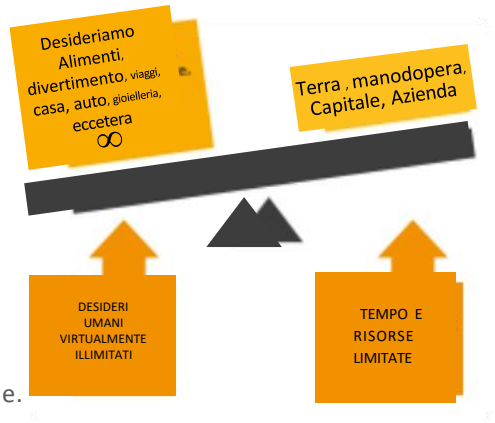
2.5 La psicologia del denaro: Scarsità, preferenza temporale e scambi commerciali

Immaginate di essere bloccati in un deserto e di avere solo una bottiglia d'acqua: avete sete e desiderate disperatamente bere, ma sapete anche che l'acqua vi servirà per sopravvivere fino a quando non riuscirete a trovarne altra. Questo è un classico esempio di scarsità: avete solo una quantità limitata di una risorsa (in questo esempio l'acqua) e dovete fare una scelta su come utilizzarla. In questa situazione potreste decidere di razionarla e di bere piccoli sorsi in un periodo di tempo più lungo per farla durare il più possibile.

Che cos'è il denaro?

La scarsità ci costringe a soppesare i pro e i contro dell'uso delle nostre risorse e a fare degli scambi.

In alternativa potreste decidere di bere il più possibile in una volta sola, sperando che l'esplosione di idratazione vi dia l'energia necessaria per cercare altra acqua. Indipendentemente dalla scelta fatta ci si trova di fronte a una decisione difficile. In questo caso la scelta è tra soddisfare la sete immediata e conservare l'acqua per il futuro. Il concetto di scarsità si applica a tutti i tipi di risorse non solo all'acqua. Che si tratti di denaro, tempo o persino di amore e attenzione, ci troviamo costantemente di fronte a scelte su come allocare le nostre risorse limitate.



Esistono due tipi di scarsità: quella causata dall'uomo e quella naturale.

- La scarsità prodotta dall'uomo, nota anche come scarsità centralizzata, comprende oggetti come borse firmate in edizione limitata, carte sportive rare e opere d'arte numerate. Queste possono essere facilmente replicate o contraffatte.
- La scarsità naturale, nota anche come scarsità decentralizzata, comprende oggetti come il sale, le conchiglie e i metalli preziosi come l'oro. Questi sono più difficili da replicare o contraffare. La principale differenza tra le due è il controllo.

La scarsità centralizzata è controllata da un'unica entità, come un'azienda o un governo, mentre la scarsità decentralizzata non è controllata da nessuno. Un esempio di scarsità centralizzata che colpisce in modo sproporzionato i poveri è il controllo di risorse essenziali come l'acqua potabile. In alcune regioni, l'accesso all'acqua potabile è gestito da aziende private o enti governativi che possono limitarne la distribuzione, determinando una scarsità di questa risorsa vitale. Questo controllo centralizzato può comportare aumenti dei prezzi o disuguaglianze nell'accesso all'acqua potabile, con le comunità più povere che spesso ne subiscono l'impatto maggiore. L'accesso limitato all'acqua potabile non solo influisce sulla loro salute e sul loro benessere, ma perpetua anche la povertà, in quanto le persone possono essere costrette a pagare prezzi più alti per l'acqua o a percorrere lunghe distanze per ottenerla.

La scarsità influenza le nostre scelte e comprenderla può migliorare il nostro processo decisionale. Spesso dobbiamo scegliere tra guadagni immediati e benefici a lungo termine e questi compromessi modellano il nostro percorso verso il raggiungimento dei nostri obiettivi.

La preferenza temporale si riferisce all'idea che le persone in genere preferiscono avere qualcosa ORA piuttosto che più tardi.

Un esempio di preferenza temporale:

Supponiamo che abbiate la possibilità di ricevere 100 dollari oggi o 110 dollari tra un anno. Se avete un'alta preferenza temporale, potreste scegliere di ricevere i 100 dollari oggi perché apprezzate di più i 100 dollari di adesso che i benefici di aspettare un anno per avere 10 dollari in più. D'altra parte, se avete una bassa preferenza temporale, preferirete aspettare la ricompensa maggiore perché siete più concentrati sulla pianificazione a lungo termine e meno interessati alla gratificazione immediata.

Attività: Preferenza temporale

Preferenza per il tempo alto vs. preferenza per il tempo basso

1. Ascoltate la spiegazione dell'insegnante sulla scelta della caramella.
2. Decidete se volete ricevere subito una piccola caramella o un marshmallow o se volete aspettare la fine della lezione per ricevere due caramelle o una caramella più grande e più buona.
3. Impegnatevi a prendere una decisione e comunicatela all'insegnante. Ricevete la caramella immediatamente o alla fine della lezione in base alla decisione che avete preso.
4. Partecipate alla discussione in classe sull'attività, riflettendo sul vostro processo decisionale e sul concetto di preferenza temporale.

Conclusione e discussione:

- Quali fattori hanno influenzato la vostra decisione di prendere la caramella ora o di aspettare una ricompensa più appagante più tardi?
- Come vi sentite in merito alla vostra decisione ora che l'attività è terminata?
- Vi vengono in mente esempi di vita reale in cui un'alta preferenza temporale potrebbe essere dannosa e una bassa preferenza temporale potrebbe essere benefica?
- Quali sono le potenziali conseguenze della scelta di un'alta preferenza temporale rispetto a una bassa preferenza temporale?

Nel contesto dell'esempio del deserto, ciò significa che si potrebbe essere più inclini a bere tutta l'acqua subito, anche se ciò significa che non ne rimarrà per dopo. Questo perché la sete che provate ora è più pressante della sete potenziale che potreste provare in futuro.

D'altra parte, se si sceglie di razionare l'acqua e di berla lentamente nel tempo, si dimostra una minore preferenza temporale. Ciò significa che siete disposti ad aspettare per soddisfare la vostra sete e migliorare le vostre possibilità di sopravvivenza. Il concetto di costo opportunità è strettamente legato a quello di scarsità e di preferenza temporale.

Che cos'è il denaro?

Il costo opportunità si riferisce al valore della prossima migliore alternativa a cui si rinuncia quando si prende una decisione. **Ogni decisione comporta degli scambi.**

La scelta di oggi	ADESSO	DOPO
	  	  
Acquistare un frullato di fragole da 7 dollari	Spendere 7 dollari in un altro modo	Approfittare di un risparmio regolare di 7 dollari

Nell'esempio del deserto, il costo opportunità di bere tutta l'acqua subito è il beneficio di sopravvivenza che si sarebbe ottenuto razionando l'acqua e usandola in un periodo di tempo più lungo.

Supponiamo quindi che si decida di razionare l'acqua e di bere piccoli sorsi per un periodo di tempo più lungo. In questo modo avete l'energia e l'idratazione necessarie per cercare altra acqua. Durante la ricerca, però, vi imbattete in un cactus che contiene una piccola quantità d'acqua. Non è molta, ma è sufficiente a placare la sete per il momento. Se aveste deciso di bere tutta l'acqua in una volta sola, forse non avreste avuto l'energia necessaria per cercare altra acqua e incontrare il cactus.

In questo caso, il costo opportunità di bere tutta l'acqua in una volta sarebbe stata la possibilità di trovare il cactus e idratarsi di più.

Questo esempio illustra come il costo opportunità non riguardi solo lo scambio immediato tra due opzioni, ma anche le potenziali opportunità future che possono essere guadagnate o perse come risultato delle nostre scelte.

La nostra disponibilità a rinunciare a una ricompensa maggiore in futuro in cambio di una ricompensa minore ora è influenzata dalla nostra preferenza temporale, ovvero da quanto apprezziamo la gratificazione immediata rispetto alla pianificazione a lungo termine.

In questo capitolo abbiamo esplorato il concetto fondamentale di denaro, affrontando la sua definizione, le sue funzioni, le sue proprietà e i suoi vari tipi. Un aspetto essenziale della nostra discussione è stata la comprensione della psicologia del denaro, concentrandoci su concetti come la scarsità, la preferenza temporale e gli scambi. Questa esplorazione ha posto le basi per comprendere la complessa natura del denaro e il suo ruolo nella nostra vita. Nel prossimo capitolo parleremo della storia del denaro e della sua evoluzione nel tempo.

Capitolo #3

La storia del denaro

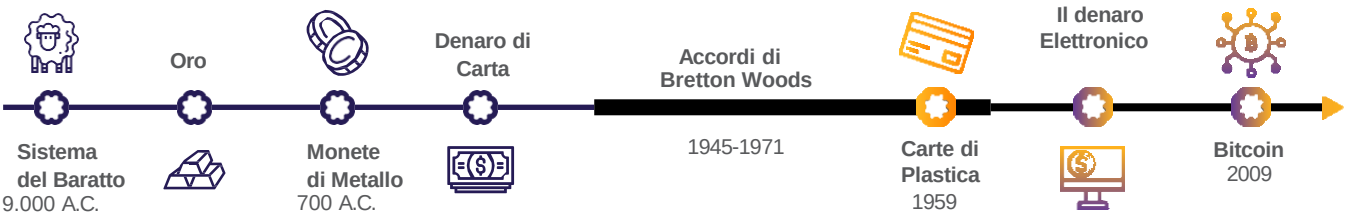
Libro di lavoro per studenti

Versione italiana | 2025

La storia del denaro

3.0 Introduzione

> Il denaro non si è evoluto per disegno, ma è nato dal processo di mercato. Non è stato creato dai governi. È emerso nel tempo come un ordine spontaneo.
>
> **Murray Rothbard**



Immaginate un tempo lontano in cui le persone non avevano le monete o le banconote di carta che usiamo oggi. A quel tempo, avevano un modo unico di scambiare le cose, usando oggetti come conchiglie o metalli preziosi come l'oro come una sorta di moneta speciale. Può sembrare strano, ma era la loro versione del denaro, qualcosa che tutti concordavano avesse valore. In questo capitolo intraprenderemo un viaggio nel tempo, vivendo l'evoluzione del denaro in prima persona. Ripercorreremo le sue origini e osserveremo come è cambiato e si è adattato nel corso della storia.

Attività: Esercizio in classe - Gioco del baratto

Il vostro insegnante vi ha dato un piccolo foglio di carta. Il vostro obiettivo è scambiare ciò che "avete" con ciò che "volete" in un gioco di commercio nel corso della storia. Scrivete il vostro nome all'inizio del foglio in caratteri piccoli e leggibili.

Passo #1: Baratto

È l'anno 6000 a.C. Inutile dire che il denaro come lo conosciamo non sia stato inventato. Siete in Mesopotamia e vi scambiate direttamente beni e servizi attraverso il **baratto**.

> Come nota a margine molte aziende ancora accettano pagamenti non monetari per i loro servizi, e le amministrazioni pubbliche trattano queste transazioni barattate alla stessa stregua delle transazioni in valuta ai fini della dichiarazione dei redditi.

Tagliate il foglio di carta in corrispondenza della linea tratteggiata. Il vostro obiettivo è scambiare il vostro "avere" per un numero di volte necessario ad ottenere finalmente il vostro "volere" originale. Non potete cambiare il vostro "desiderio" originale.
Avete a disposizione cinque minuti per raggiungere l'obiettivo di questo esercizio.

Quando il nuovo "avere" corrisponde al "volere" iniziale, tornate al vostro posto. Al termine del tempo a disposizione, se non avete trovato un partner commerciale, tornate comunque al vostro posto.

Alzi la mano chi è riuscito a ottenere ciò che voleva dopo un solo scambio. Due? Tre?

Rispondete alle seguenti domande in modo sintetico ma sostanziale.

1. Perchè solo alcuni di voi sono stati in grado di trovare qualcuno con cui commerciare e altri no ?

2. Quali sono i benefici del baratto?

3. In base alla vostra esperienza di questo esercizio, quali sono gli svantaggi del baratto?

Passo #2: Denaro in materie prime

Facciamo un salto in avanti e andiamo sulla costa occidentale dell'Africa intorno al XIV secolo a.C..
Il baratto è diventato noioso e inefficace. Ci siamo evoluti come civiltà e ora utilizziamo il **denaro delle materie prime.**

Gusci di conchiglia come monete _____

1.300 A.C.

1.000 A.C.

687 A.C.

FATTO DIVERSO
Le conchiglie di cowry sono state accettate come moneta legale in alcune parti dell'Africa fino al XX secolo.

Queste proto-monete avevano una forma ovale, erano fatte di "electrum" (una lega di oro e argento) e presentavano un disegno solo su un lato.

1.300 A.C.
Le conchiglie sono la forma di pagamento predominante nella maggior parte dell'Asia, dell'Africa, dell'Oceania e in alcune parti d'Europa.

1.000 A.C.
La dinastia Zhou occidentale della Cina Inizia ad utilizzare monete di metallo.

687 A.C.
Il re di Lidia (l'odierna Turchia), Alyattes, ordina la prima coniazione di monete metalliche nel mondo occidentale.

La storia del denaro

Il vostro insegnante vi ha dato un maccherone (per semplicità). Supponiamo per convenzione che il prezzo di ogni bene valga un maccherone.

Il vostro obiettivo è di nuovo quello di ottenere ciò che "volete", ma ora la nostra specie si è un po' svegliata e ha trovato un modo per risolvere certi problemi.

- Perché consideriamo i maccheroni merce di scambio?
- Come possiamo ottenere le cose che vogliamo adesso?
- Lo scambio con I maccheroni è stato più facile?
- Perché il denaro ha sostituito le materie prime, secondo te?
- In che modo l'uso del denaro di base è più efficiente del baratto?
- Quali sono gli svantaggi dell'uso dei maccheroni come denaro?
- Cosa pensate sia successo quando la Spagna ha iniziato a riportare barche di maccheroni nel vostro Paese ? (oro e argento dalle Americhe alla Spagna)?

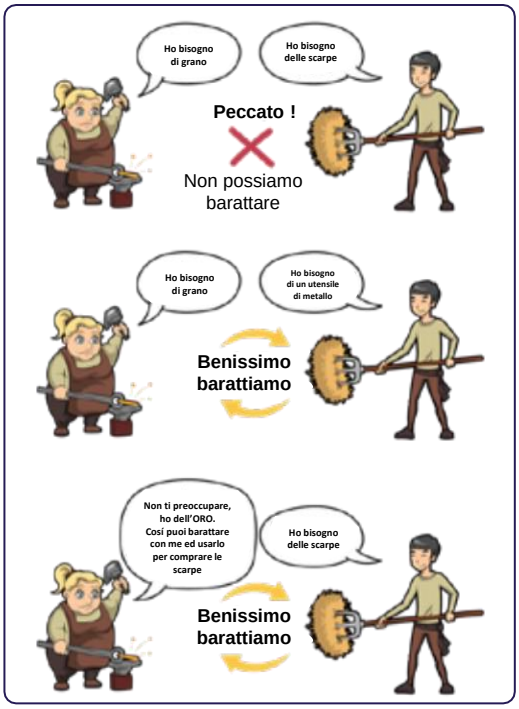
3.1 L'evoluzione dal baratto alla moneta moderna

3.1.1 Problemi con le prime forme di denaro

Guardate questo breve video per conoscere le origini del cambio, nella serie "La storia della cartamoneta".

Nelle economie di baratto, le persone scambiano tra loro in base al valore relativo dei beni e dei servizi che hanno da offrire. Le economie di baratto sono poco efficienti e possono essere difficili da gestire, soprattutto in società complesse.

Una situazione come la **doppia coincidenza** di desideri è necessaria in qualsiasi sistema di baratto, poiché le persone devono sempre trovare qualcuno che abbia ciò che desiderano, ma che desideri anche ciò che hanno da offrire in cambio.



Supponiamo che:

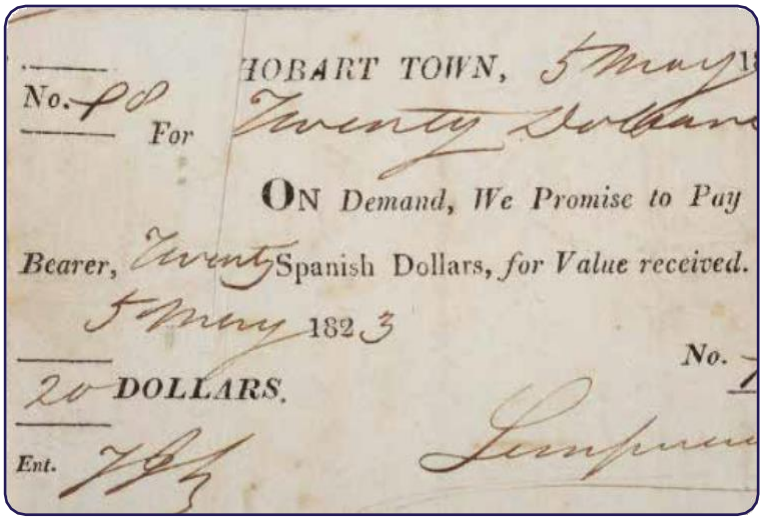
- Joseph vuole scambiare la sua banana con la noce di cocco di Yael.
- Ma Yael vuole scambiare la sua noce di cocco solo con il mango di Tammy.
- E Tammy vuole scambiare il suo mango solo per La banana di Joseph.
- Sono bloccati in un ciclo infinito di scambi di frutta senza una doppia coincidenza di desideri.
- Joseph suggerisce di scambiare la frutta con una bella bibita fresca, ma i due si rendono conto di essere su un'isola remota e di non avere bibite.
- Decidono di sedersi sulla spiaggia e di godersi i frutti in silenzio.

3.1.2 Sviluppo della moneta e della cartamoneta

Man mano che voi e la vostra comunità diventate più coinvolti negli scambi e nel commercio, vi renderete conto dei limiti dell'uso del baratto e di altre forme di scambio non monetario. Deciderete quindi di adottare l'uso di monete metalliche come forma di denaro.

La moneta-merce è una moneta costituita da materiali metallici di valore come l'oro e l'argento. Questi sono stati storicamente utilizzati come riserva di valore, mezzo di scambio e, in un lontano passato, come unità di conto.

La storia del denaro



Tuttavia, quando si iniziano a usare le monete di metallo con maggiore frequenza, si incontrano alcuni inconvenienti. Possono essere pesanti e scomode da trasportare nelle grandi transazioni, e si nota che alcune persone approfittano del sistema fondendo le monete creandone di nuove e mescolandole con metalli più economici, il che fa salire i prezzi e mina la fiducia nel sistema.

Per cercare di risolvere questi problemi, voi e la vostra comunità iniziate a usare le ricevute cartacee come forma di denaro. Queste ricevute cartacee, che hanno le loro origini nell'Antica Cina, sono una forma di moneta conveniente e facilmente scambiabile. Sono sostenute dall'oro e da altri metalli preziosi e possono essere convertite in questi metalli, come avveniva dal **XVII** al **XIX** secolo. Ciò consente di avere una forma di denaro più portatile e facilmente trasferibile, pur mantenendo il valore e la sicurezza dei metalli preziosi.

3.1.3 Transizione da denaro sano a denaro non sano

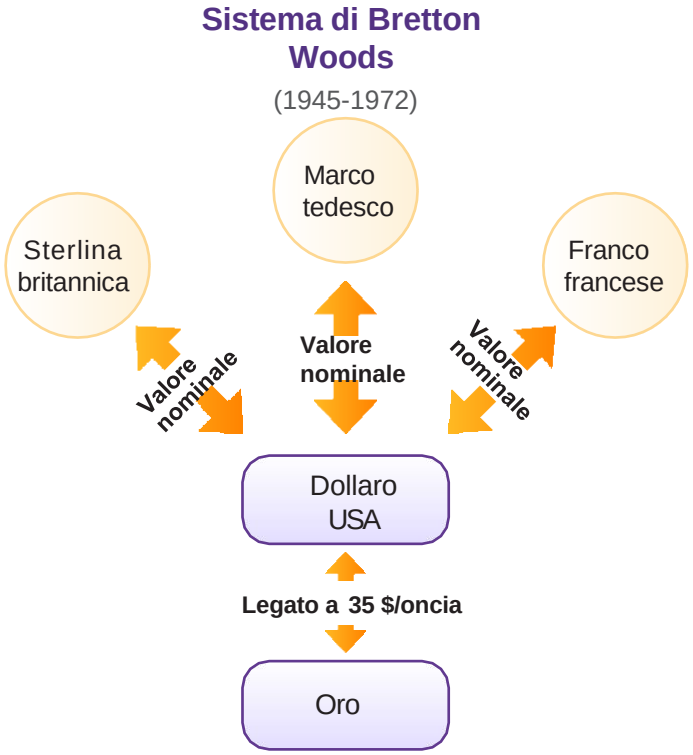
Arriviamo al 17° secolo in Svezia. Ora si dipende completamente dalle banche per custodire i propri beni di valore.
Tuttavia, si inizia a notare qualcosa di strano in questi banchieri: sembra che stiano emettendo più ricevute cartacee di quanto oro abbiano in deposito, consentendo loro di creare più denaro di quanto non abbiano beni a sostegno. Questa pratica subdola permette ai banchieri di trarre vantaggio dalla differenza tra il valore delle ricevute cartacee e il valore dell'oro che detengono per i loro clienti.

Cosa succede quando si cerca di mettere in pratica la dottrina della cartamoneta? Scopritelo nel quarto episodio di "Storia della cartamoneta".

Vi rendete conto che questo segna un cambiamento importante nel modo in cui funziona il denaro: si sta passando da un sistema di moneta sana (cioè sostenuta da metalli preziosi) a un sistema di moneta non sana (cioè non sostenuta da un bene fisico). Questa transizione non è avvenuta da un giorno all'altro, ma è stata un processo graduale influenzato da diversi fattori. La rivoluzione industriale, con la sua produzione di massa e l'urbanizzazione ha avuto un ruolo importante così come la crescita di sistemi finanziari avanzati tra cui banche e mercati azionari. La nascita delle banche centrali e di altre autorità monetarie ha contribuito alla centralizzazione o al controllo della moneta portando all'emissione di valute per sostenere la crescita economica.

Tuttavia, si cominciano a vedere anche gli **aspetti negativi di questa centralizzazione**, tra cui il consumo irresponsabile, **aumento del debito** e manipolazione dei cittadini attraverso incentivi economici.

Fino alla prima guerra mondiale era possibile convertire la cartamoneta in una quantità prestabilita di oro. Ma le due guerre mondiali e la crisi economica del 1929 posero fine a questa situazione. Nel 1944 furono firmati gli accordi di **Bretton Woods**, che imponevano il dollaro americano come valuta di riserva mondiale e ne fissava il valore al prezzo dell'oro al tasso di 35 dollari l'oncia. Le valute degli altri Paesi sono ancorate al dollaro il che contribuisce a stabilizzare i mercati finanziari internazionali.



Sfortunatamente, il sistema iniziò a cedere alla fine degli anni Sessanta, portando al **Nixon Shock del 1971**, quando il governo statunitense sospese la convertibilità del dollaro in oro. Questo segna la fine del gold standard e l'inizio di un mondo guidato dalla **creazione e dall'accumulo di debito**.

Nel corso della vita quotidiana, si inizia a notare che il valore del denaro non è più stabile come un tempo; proprio come un righello flessibile rende difficile misurare con precisione la lunghezza di un tavolo, vivere in un mondo **fiat** in cui il valore del denaro è soggetto all'imprevedibilità di chi detiene il potere può rendere difficile misurare con precisione il valore di beni e servizi. Si prova confusione e disagio nell'adattarsi a un mondo in cui il valore del denaro non è più legato a un bene fisico come l'oro.

Si vedono gli impatti di questo cambiamento sull'economia globale e si inizia a mettere in dubbio la stabilità e l'affidabilità delle valute. Ci si rende conto che, in questo mondo moderno, il dollaro non è più fisso e coerente come quando era ancorato all'oro, ma è soggetto a fluttuazioni. Ciò rende più difficile utilizzare il dollaro come unità di conto, poiché il suo valore è influenzato da vari fattori, tra cui l'infllazione (aumento dei prezzi), i tassi di interesse, la forza dell'economia del Paese, gli eventi politici, la speculazione di mercato e la domanda nel commercio internazionale. Può essere un periodo confuso e imprevedibile in cui si cerca di orientarsi tra i continui cambiamenti del valore del dollaro e il suo impatto sulla vita quotidiana.

Nonostante gli sforzi per migliorare la qualità della vita attraverso i moderni sistemi monetari, una maggiore efficienza, un maggiore accesso alle informazioni e una migliore comunicazione, il tenore di vita della maggior parte delle persone inizia a diminuire a causa di:

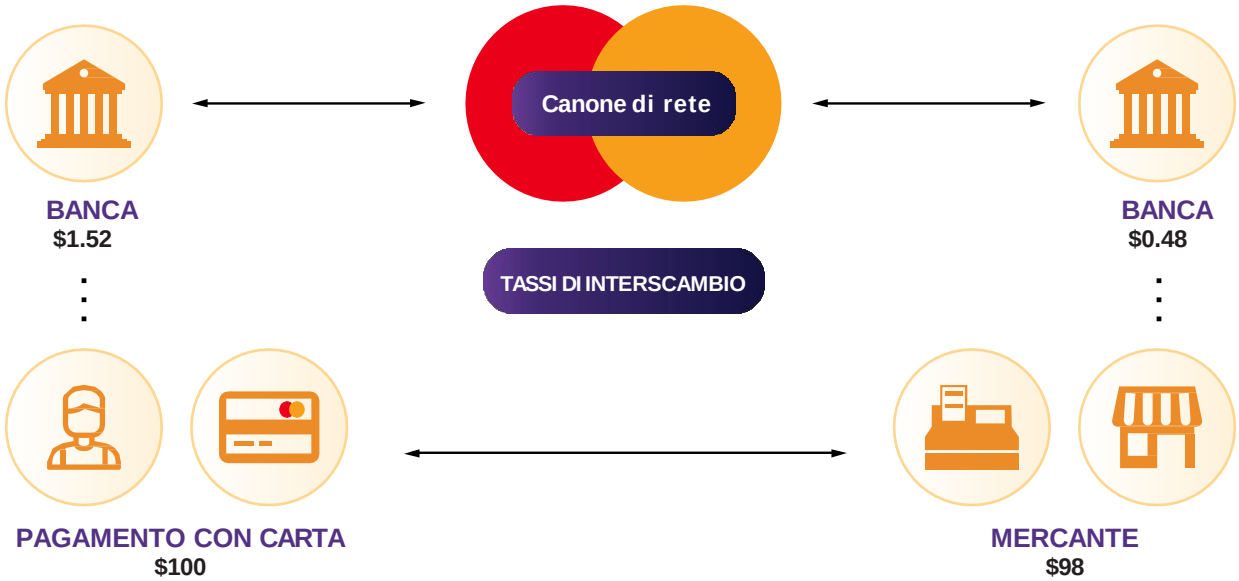
- Abuso di centralizzazione
- Aumento dei prezzi
- Stagnazione dei salari
- Reale indebolimento delle valute
- Necessità di spendere di più per meno cose

Questo comporta delle sfide per coloro che dispongono di risorse economiche inferiori e che possono avere un accesso limitato all'istruzione, al credito, alle risorse, alle reti sociali e alla rappresentanza politica, con conseguenti potenziali svantaggi nella loro capacità di avere successo.

Di conseguenza, i ricchi sembrano diventare sempre più ricchi e i poveri sempre più poveri.

3.1.4 Dalla carta alla plastica

Oggi abbiamo fatto molta strada dall'introduzione della prima carta di credito negli anni Cinquanta. Con una semplice strisciata di plastica possiamo comprare quello che vogliamo, quando vogliamo, senza problemi. È come se si aprisse un mondo di infinite possibilità e l'eccitazione di scoprire cosa ci riserva è palpabile... o almeno così pensavamo. Non sapevamo che la nostra dipendenza dal credito avrebbe avuto conseguenze dolorose come l'aumento del costo complessivo dei beni e l'incentivazione di una certa economia destinata a fallire.



Con il progredire della tecnologia cresce anche il modo in cui gestiamo il denaro. Internet diventa un attore importante nel mondo finanziario con siti di online banking e di e-commerce che permettono di gestire e spendere il denaro interamente online.

L'ascesa del denaro digitale segna il prossimo salto significativo in questa evoluzione, offrendo nuove possibilità e ridisegnando il modo in cui effettuiamo le transazioni finanziarie.

3.2 Moneta digitale

A differenza di quelle tradizionali, le valute digitali esistono esclusivamente in forma elettronica. Vengono memorizzate e scambiate utilizzando computer e software speciali.

Le valute digitali consentono di inviare il proprio denaro attraverso Internet: così come la posta elettronica ci permette di inviare messaggi istantaneamente e senza costi di spedizione, le valute digitali ci permettono di inviare e ricevere valore istantaneamente e con costi molto ridotti.

Le valute che utilizziamo oggi stanno diventando sempre più digitali: solo una piccola parte della massa monetaria esiste sotto forma di monete e banconote di carta. Le banche e i servizi bancari mettono a disposizione dei loro utenti applicazioni per lo scambio di denaro su Internet. Ma da dove proviene il denaro?

In questo capitolo abbiamo assistito alla trasformazione del denaro sano, rappresentato dall'oro, in denaro non sano sotto forma di carta e ora in moneta digitale. Nel prossimo capitolo esploreremo come funziona l'attuale sistema monetario fiat e come è nato.

Capitolo #4

Che cos'è il denaro Fiat e chi lo controlla?

Libro di lavoro per studenti

Versione italiana | 2025

Che cos'è il denaro Fiat e chi lo controlla?

4.0 Introduzione

> **La storia dell'umanità è la storia della perdita di valore del denaro.**
>
> **Milton Friedman**

Nel capitolo precedente abbiamo visto come il denaro si sia evoluto nel tempo e come il nostro sistema monetario sia passato da una moneta sana a una non sana, dando forma al mondo in cui viviamo oggi. Questo capitolo approfondisce il modo in cui questi sviluppi hanno portato al sistema monetario odierno e al suo funzionamento.

Come si presenta questo sistema fiat e come è nato?

Per rispondere a questa domanda, dobbiamo iniziare a concentrare la nostra attenzione sul dollaro americano, l'attuale valuta di riserva mondiale, che svolge un ruolo dominante nel mondo di oggi. Ogni Paese, direttamente o indirettamente, risente delle decisioni prese in merito al dollaro. Per capire veramente come funziona il sistema del denaro fiat nel vostro Paese, è essenziale dipanare i fili storici che lo collegano al luogo di nascita del sistema fiat: gli Stati Uniti d'America.

4.1 Breve storia della moneta Fiat

1815-1933	1913	1933	1934	1944	1971	1980
Oro usato come riferimento di valore (Gold stantard)	Creazione della banca centrale americana denominata “The Federal Reserve”	Ordine esecutivo 6102. Ogni cittadino viene obbligato a consegnare tutto il proprio oro in cambio di 20,67 Dollari per Oncia.	Atto per la riserva in oro, rubare ricchezza alle persone svalutando il dollaro del 40%, Imponendo un cambio di 35 dollari per oncia d’oro	Accordo di **Bretton Woods**: il dollaro americano diventa la riserva di valore a livello mondiale	**Nixon Shock** che ha dato vita alla moneta **FIAT** ponendo fine al legame fra il valore del dollaro ed il valore dell’oro	Il valore dell’oro aumenta da 35 dollari per oncia nel 1970 a 870 dollari per oncia nel 1980, che causa una perdita di valore del denaro del 96% in appena 10 anni

Linea del tempo

Nel XIX secolo, le civiltà di tutto il mondo prosperavano grazie a un solido standard monetario, utilizzando metalli preziosi come l'oro e l'argento per la loro scarsità, durata e riconoscibilità. Con la crescita del commercio globale, il trasporto di grandi quantità di metallo divenne un'impresa ardua, che portò alla nascita dei depositi d'oro e d'argento. Questi magazzini custodivano in modo sicuro i metalli preziosi delle persone e fornivano certificati cartacei riscattabili con quantità specifiche di oro o argento. In cambio del deposito del proprio denaro, gli individui ricevevano certificati direttamente

legati all'esatta quantità d'oro o d'argento che conservavano. Questo legame diretto tra i certificati cartacei e la moneta tangibile ha segnato i primi passi di quelle che oggi chiamiamo banche.

Inizialmente, le banche miravano a salvaguardare il denaro dei clienti, ma in seguito si impegnarono in pratiche di prestito rischiose, emettendo certificati per l'oro che non possedevano. Questa pratica comportava la minaccia di corse agli sportelli se troppi clienti avessero reclamato il loro denaro contemporaneamente. Per far fronte a questo rischio, le banche collaborarono con i governi per istituire un sistema di legalizzazione

dei prestiti. Nel 1913 crearono la **Federal Reserve**, una banca centrale responsabile della creazione di nuovi certificati cartacei e del salvataggio delle banche in difficoltà. A livello mondiale, i governi riconobbero il valore dell'oro e dell'argento, dando vita a conflitti e guerre per il controllo. Negli anni che precedettero la Seconda guerra mondiale, leader come Lenin, Stalin, Churchill, Roosevelt, Mussolini e Hitler si appropriarono dell'oro per scopi strategici.

All'inizio degli anni Trenta negli Stati Uniti si verificò un cambiamento significativo nel modo in cui la moneta era sostenuta da beni. All'epoca, gran parte della ricchezza delle persone era conservata sotto forma di oro. Tuttavia, nel 1933, il Presidente Roosevelt emanò l'Ordine Esecutivo 6102, che imponeva a tutti i cittadini di rinunciare al proprio oro. Non si trattava di uno scambio volontario: le persone erano obbligate a consegnare il loro oro e, se si rifiutavano, andavano incontro a gravi sanzioni.

Il governo fissò il tasso di cambio a 20,67 dollari per oncia d'oro. Ciò significava che per ogni oncia d'oro che una persona possedeva, riceveva certificati cartacei equivalenti a 20,67 dollari. Le persone dovettero accettare questi dollari di carta, sperando che un giorno sarebbero state in grado di scambiarli nuovamente con l'oro.


POSTMASTER: PLEASE POST IN A CONSPICUOUS PLACE — JAMES A. FARLEY, Postmaster General

UNDER EXECUTIVE ORDER OF THE PRESIDENT

Issued April 5, 1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

all GOLD COIN, GOLD BULLION, AND GOLD CERTIFICATES now owned by them to a Federal Reserve Bank, branch or agency, or to any member bank of the Federal Reserve System.

Executive Order

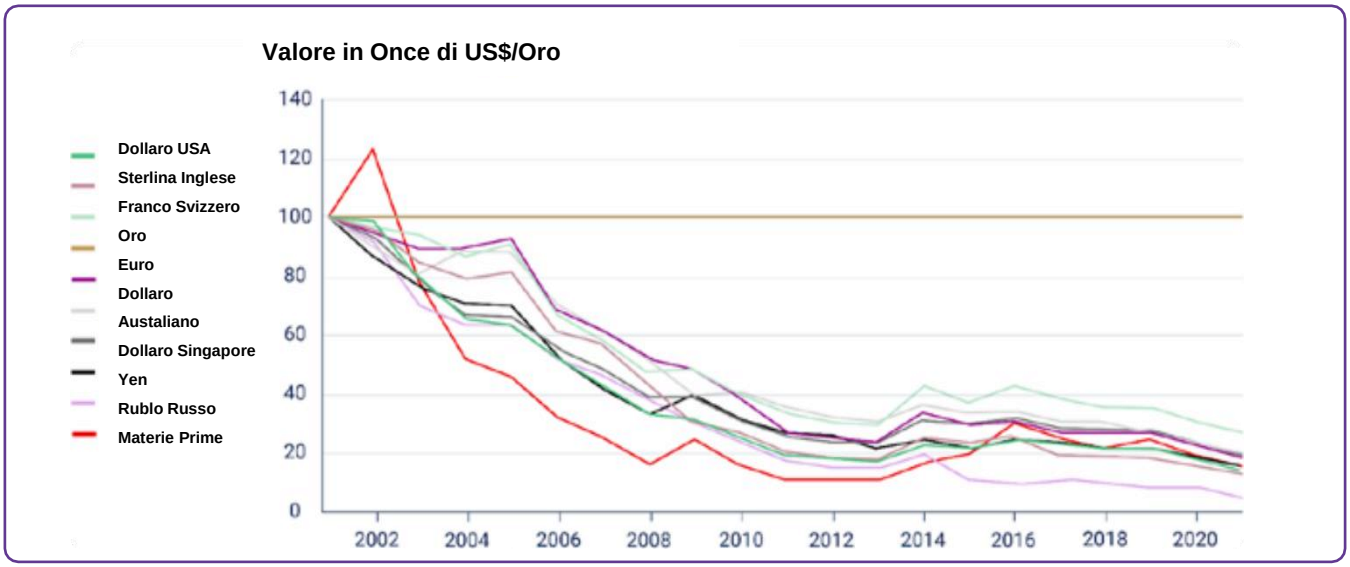
Traduzione: **IN BASE ALL'ORDINE ESECUTIVO DEL PRESIDENTE** emesso il 5 aprile 1933, tutte le persone sono tenute a consegnare, **ENTRO IL 1° MAGGIO 1933**, tutte **MONETE D'ORO, I LINGOTTI D'ORO E I CERTIFICATI D'ORO** di loro proprietà alla **Federal Reserve Bank,** ad una filiale o agenzia o a una qualsiasi banca che sia membro del **Federal Reserve System**.

Ordine Esecutivo

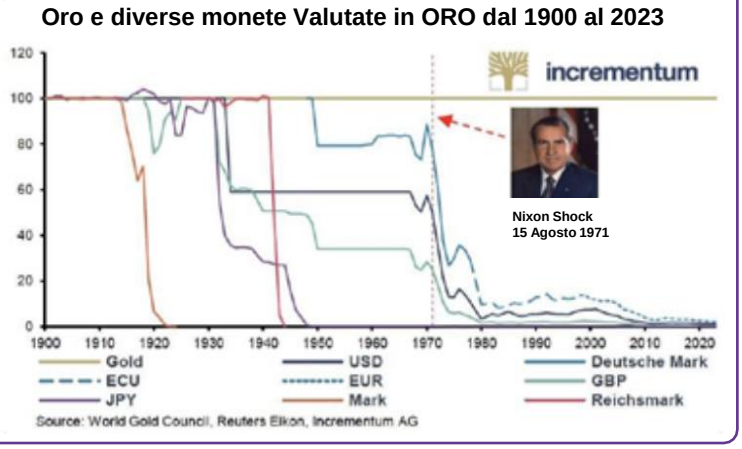
Che cos'è il denaro Fiat e chi lo controlla?

Nel 1934, il Gold Reserve Act permise ai cittadini di cambiare nuovamente i loro dollari di carta in oro. Tuttavia, c'era una fregatura: il governo svalutò deliberatamente i dollari di carta aumentando il tasso di cambio a 35 dollari per oncia d'oro. Questa svalutazione colpì i lavoratori delle classi medie e basse, in quanto i loro risparmi, che prima valevano di più, ora valevano di meno a causa della diminuzione del valore dei dollari cartacei.

Dopo la Seconda Guerra Mondiale, l'accordo di Bretton Woods del 1944 stabilì che il dollaro statunitense fosse la valuta di riserva mondiale e potesse essere scambiato con l'oro. Purtroppo però, questo legame tra il dollaro e l'oro fu interrotto nel 1971 quando il presidente **Nixon** pose fine alla possibilità di riscattare il dollaro in oro. Ciò segnò un cambiamento significativo portando all'adozione di un sistema monetario in cui il valore della moneta non è sostenuto da un bene fisico come l'oro, ma piuttosto dalla fiducia e dalla sicurezza delle persone che la utilizzano. Poiché i governi e le banche centrali hanno trattenuto la maggior parte dell'oro dei cittadini, il valore dell'oro ha subito un'impennata, raggiungendo il livello di 870 dollari l'oncia nel 1980.



In conclusione, la storia di come la società umana sia passata da uno standard monetario solido a uno standard non solido (fiat) ci racconta come i governi e le banche abbiano sottratto metalli preziosi ai loro cittadini. Mentre il denaro reale è finito nelle tasche dei governi e delle banche, ai cittadini sono rimasti pezzi di carta il cui unico valore deriva dai governi che ne hanno imposto l'uso.



4.2 Il sistema Fiat

> Il problema principale della moneta convenzionale è la fiducia necessaria per farla funzionare. Si deve confidare che la banca centrale non svilisca la moneta, ma la storia delle valute convenzionali è piena di violazioni di questa fiducia.
>
> **Satoshi Nakamoto**

L'umanità è passata da una moneta sana controllata da molti a una moneta non sana controllata da pochi. Ma come funziona esattamente questo sistema?

4.2.1 Un sistema monetario per decreto

Il Sistema Fiat si contraddistingue per la sua natura obbligatoria, imposta ai cittadini attraverso leggi sul corso legale. Il termine "fiat", di origine latina, significa "per decreto", ovvero una direttiva emessa dalle autorità.

A differenza della moneta sostenuta da beni tangibili, come l'oro, la moneta virtuale è priva di tale supporto. Ciò nonostante Il suo utilizzo sia imposto dalla legge: le valute di tutti i giorni, come dollari, euro, sterline, yuan, pesos e altre, rientrano nel sistema del denaro fiat.

Legge sul corso legale: Una legge che obbliga tutti i cittadini ad accettare un determinato tipo di moneta o valuta.

Il valore della moneta Fiat si basa sulla convinzione che possa essere scambiata con beni e servizi e sull'illusione che conservi il suo valore nel tempo. Il denaro fiat è paragonabile al biglietto di un concerto: il suo valore non risiede nel biglietto cartaceo in sé, ma nella certezza che la band (il governo e la sua banca centrale) offrirà un grande spettacolo (garantire la stabilità economica).

I vantaggi della moneta fiat

- **Facilità d'uso:** La moneta fiat è comoda per le transazioni quotidiane.
- **Costi e rischi inferiori:** La moneta fiat non richiede una forte sicurezza come l'oro, il che la rende più economica e sicura.

I contro della moneta Fiat

- **Rischi di infllazione:** I prezzi possono aumentare continuamente causando inflazione e casi storici di iperinflazione.
- **Controllo e manipolazione centralizzati:** Piccoli gruppi possono influenzare e manipolare il sistema portando alla censura e alla confisca.
- **Rischio di controparte:** Se il governo deve affrontare delle difficoltà, la valuta può perdere valore.
- **Potenziale di abuso:** Il sistema può essere utilizzato in modo improprio, con conseguente corruzione e perdita di fiducia.

Che cos'è il denaro Fiat e chi lo controlla?

Materie Prime vs. Fiat: Immaginate la differenza

Ricordate: prima dell'avvento della moneta elettronica i governi coniavano monete a partire da un bene fisico di valore, scarso e difficile da ottenere, come l'oro o l'argento oppure stampavano cartamoneta che poteva essere riscattata in cambio di una determinata quantità di un bene fisico: questo era il sistema basato sulle materie prime.

Nel sistema fiat, invece, è come avere i soldi del Monopoli. Il denaro nel sistema fiat consiste in pezzi di carta stampati dalla banca centrale e le politiche del governo ne influenzano direttamente il valore. Il governo e le banche centrali sono fondamentalmente "i banchieri del Monopoli" che controllano il funzionamento del gioco, chi ottiene cosa e quanto vale. In altre parole, il governo promette di fare un buon lavoro nella gestione del sistema monetario.

In conclusione, le valute fiat hanno valore solo perché il governo ne impone l'uso; non c'è alcuna utilità nella moneta fiat in sé.

Riassumendo, il sistema finanziario è un gioco di fiducia in cui il valore del nostro denaro si basa sulle promesse di chi è al comando e i cittadini possono solo sperare che il loro governo agisca per il bene di tutti. Vedremo poi come le banche creano nuovo denaro, chi è coinvolto e come questo influisce sull'economia.

4.2.2 *Il sistema bancario a riserva frazionaria: un sistema alimentato dal debito*

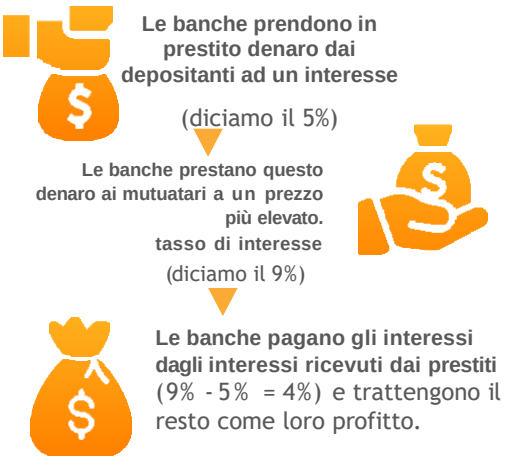
> È abbastanza giusto che la gente della nazione non capisca il nostro sistema bancario e monetario, perché se lo capisse, credo che ci sarebbe una rivoluzione prima di domani mattina.
>
> **Henry Ford**

Il sistema bancario a riserva frazionaria è una delle parti principali dell'intero sistema bancario mondiale che consente alle banche di prestare una parte significativa dei depositi dei loro clienti. Vi siete mai chiesti perché le banche offrono così tanti servizi ai loro clienti? Anche se può sembrare che siano generose, è importante ricordare che le banche sono imprese e il loro obiettivo primario è quello di ottenere un profitto. Ma come fanno a guadagnare se permettono alle persone di prendere in prestito denaro ?

Oltre a percepire interessi sui depositi, le banche generano entrate in altri modi, tra cui:

- Addebito degli interessi sui prestiti concessi
- Addebito di commissioni per servizi come l'utilizzo di bancomat e la gestione del conto.
- Guadagno di denaro attraverso gli investimenti, come l'acquisto e la vendita di titoli o l'investimento in immobili.
- Mantenimento di una percentuale di prestiti in riserva e investire o prestare il resto
- Pagamento di interessi sui depositi e addebito di commissioni su conti correnti e libretti di risparmio

Quando una banca riceve un deposito, è tenuta a trattenerne solo una frazione (obbligo di riserva) e può prestare la parte restante.



Ad esempio, se si depositano 100 dollari con un obbligo di riserva del 10%, la banca può prestare 90 dollari, trattenendo solo 10 dollari come riserva. Il mutuatario deposita 90 dollari in un'altra banca, permettendo al ciclo di continuare nonostante il valore iniziale sia invariato.
Con un deposito di 100 dollari il denaro totale nell'economia cresce fino a 271 dollari, apparendo dal nulla - un fenomeno noto come effetto moltiplicatore.

Questo processo porta a un sistema monetario basato sul debito, in quanto le banche creano nuova moneta con ogni prestito, aumentando la massa monetaria complessiva. Se il sistema bancario a riserva frazionaria continua, il debito totale dell'economia aumenta contribuendo all'infllazione.

Il sistema si basa su un ciclo continuo di creazione di moneta attraverso i prestiti, come una fornitura costante di droga per un tossicodipendente. Tuttavia, se le banche prestano più denaro di quanto ne abbiano in riserve e i depositanti si precipitano a ritirarlo simultaneamente, le banche potrebbero andare incontro al fallimento.

In questo caso, la banca centrale interviene come prestatore di ultima istanza, fornendo nuova valuta per evitare i fallimenti delle banche. A tal fine, la banca centrale riacquista attività o inietta valuta direttamente nei conti delle banche. In sostanza, le banche vengono salvate dal fallimento grazie alla costante iniezione di nuova moneta da parte delle banche centrali: questo sistema alimentato dal debito e sistematicamente salvato dalla banca centrale dà luogo a cicli di boom e bust (salita e discesa).

Immaginate di avere un amico che è anche un banchiere; chiamiamolo Dax.

Dax ama le biciclette e vuole prendere in prestito la vostra bici perché deve andare in molti posti. Gliela date e, con un colpo di scena, Dax inizia a promettere la stessa bici a tanti altri amici nello stesso momento. Con l'unica bici vera che gli avete prestato, Dax riesce a creare altre bici immaginarie e inizia a prestarle agli amici. Ognuno dei suoi amici pensa di poter fare un bel giro quando vuole. Ma, ecco il colpo di scena: c'è solo una bici vera! Tutte le altre sono immaginarie e solo promesse.

Quindi, cosa succede? Quando circolano più biciclette immaginarie, tutti sono molto contenti, almeno all'inizio, perché all'inizio nessuno usa la bicicletta nello stesso momento: sembra che non ci siano problemi e che ci sia abbondanza di biciclette per tutti. Così, tutti gli amici iniziano a fare altri progetti, pensando a tutti i posti in cui andranno con le loro biciclette.

Purtroppo è qui che la magia inizia a perdere il suo fascino. Un giorno di sole, tutti decidono che è una giornata perfetta per un giro in bicicletta: si presentano tutti alla porta di Dax, entusiasti di fare un giro con le loro biciclette immaginarie, ma la realtà li tradisce: c'è solo una bici vera. La delusione è tanta e improvvisamente il valore dei giri promessi diminuisce.

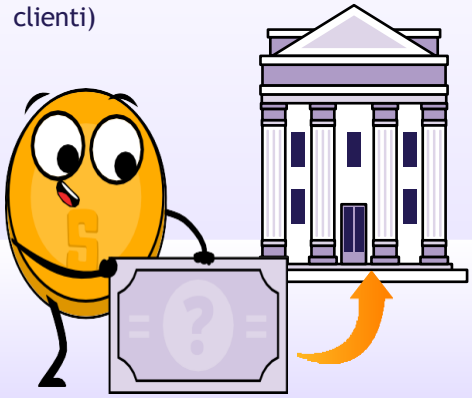
Nel mondo dei prestiti a riserva frazionaria, la storia è simile. Le banche prestano più denaro di quanto ne abbiano in realtà e per un po' tutti ne godono i benefici: circola più denaro e sembra che ce ne sia in abbondanza. Ma se troppe persone cercano di ritirare il loro denaro nello stesso momento, il vero valore diventa evidente: non c'è abbastanza per soddisfare tutte le promesse.

Questo scenario intacca il bene comune e il valore di tutte le persone coinvolte; la promessa di abbondanza si trasforma in una truffa. Proprio come le biciclette immaginarie perdono il loro valore percepito quando tutti vogliono un giro reale, il valore del denaro nell'economia può diminuire quando tutti si affrettano a reclamare la loro parte reale. Quando ciò accade, le persone scoprono che i soldi che hanno in banca non sono realmente lì, il che provoca panico, corse agli sportelli e persino il collasso di intere economie. A pagare per questi crolli, finora, è sempre stato lo stesso gruppo: la classe media e bassa del mondo.

Che cos'è il denaro Fiat e chi lo controlla?

Espansione

Espansione del credito attraverso l'attività bancaria a riserva frazionaria (le banche commerciali creano moneta fiat e la prestano ai clienti)



Espansione dell'offerta di moneta (la moneta appena creata entra nel sistema e gonfia l'offerta di moneta)

Sovrainvestimento (i clienti utilizzano i prestiti per investire nei mercati, creando un aumento della domanda).

Inflazione dei prezzi (i prezzi aumentano a causa della nuova domanda)

Mancanza di nuova domanda

Recessione

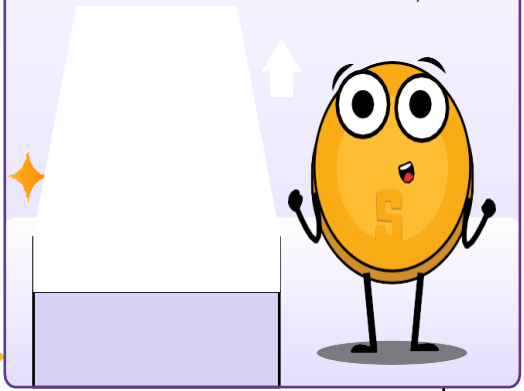
I prezzi scendono (gli investitori si lasciano prendere dal panico e iniziano a vendere i loro investimenti a prezzi più bassi perché nessuna domanda reale)

Gli individui e le aziende non riescono a onorare i loro prestiti (poiché il valore delle loro garanzie reali non è più in grado di garantire la loro sicurezza).

Le banche vanno in default (poiché ora detengono attività che valgono meno del valore dei prestiti che hanno emesso).

Intervento della banca centrale, per il salvataggio delle banche private.

Le banche vengono salvate con nuova moneta (la banca centrale riacquista le attività che le banche detengono a un prezzo superiore alla valutazione corrente di mercato per salvarle, oppure crea direttamente nuova moneta e la dà loro).



Ripetizione (ulteriore espansione del credito, preparazione per la prossima fase di Espansione economica [Boom])

Attività: Banca a riserva frazionaria

Nel seguente esercizio esploreremo come il sistema bancario a riserva frazionaria possa portare allo svilimento della moneta, all'infllazione e alla diminuzione del potere d'acquisto. Utilizzeremo un esempio semplificato che prevede sei partecipanti, uno dei quali agirà come banca, e un coefficiente di riserva molto utilizzato ancora oggi: 10%.

- La persona **A** ha appena vinto 100.000 dollari alla lotteria e li deposita in un conto corrente nella banca (**B**). Con un coefficiente di riserva del 10%, **B** deve mantenere 10.000 dollari nel suo caveau e può prestare i restanti 90.000 dollari.
- La persona **C** prende in prestito da **B** l'importo massimo (90.000 dollari) e lo usa per comprare una casa da **D**.
- La persona **D** deposita i 90.000 dollari ricevuti da **C** nella banca (**B**). Il totale dei depositi nella banca è ora di 190.000 dollari.
- La persona **E** chiede un prestito a **B** e la banca concede il 90% del nuovo deposito, pari a 81.000 dollari.
- La persona **E** utilizza il prestito di 81.000 dollari per acquistare un'opera d'arte da **F**, che poi deposita il denaro in banca (**B**). Il totale dei depositi registrati è ora di 271.000 dollari.

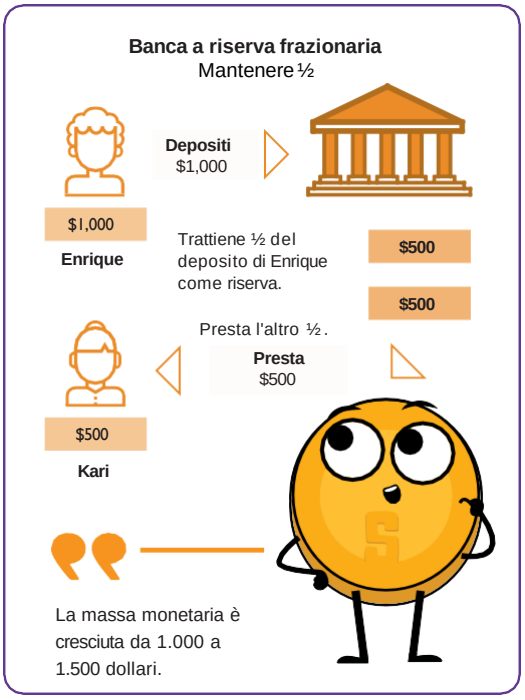
In questo scenario, il deposito iniziale di 100.000 dollari ha generato un totale di 271.000 dollari di depositi dopo essere circolato nell'economia.

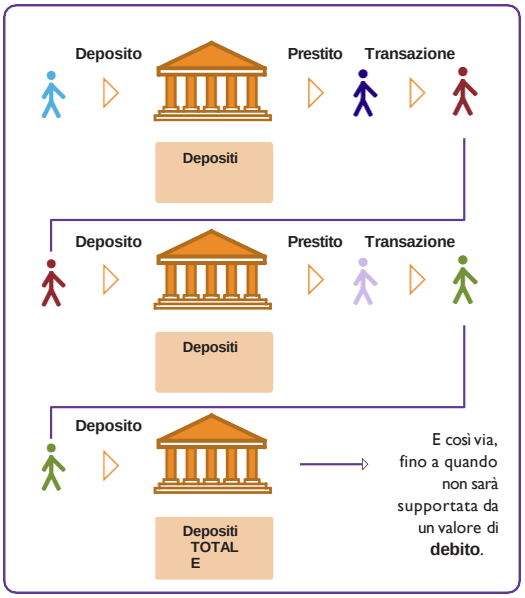
Se l'aliquota di riserva venisse abbassata all'1%, la quantità di moneta creata sarebbe significativamente più alta ($100.000 / 0,01 = $10,000,000). In questo caso, quanto denaro verrebbe effettivamente creato con quei 100.000 dollari se il denaro continua a circolare nell'economia?

È importante notare che a partire dal 2020 la Federal Reserve (la banca centrale degli Stati Uniti) ha ridotto i coefficienti di riserva obbligatoria allo **zero per cento** per stimolare l'economia.

Abbiamo bisogno dei seguenti volontari:

A = Depositante (vincitore della lotteria) (azzurro)
B = Cassiere di banca (banca)
C = Debitore n. 1 (blu scuro)
D = Proprietario/Depositante (rosso)
E = Debitore n. 2 (viola chiaro)
F = Proprietario/depositario della galleria d'arte (verde)



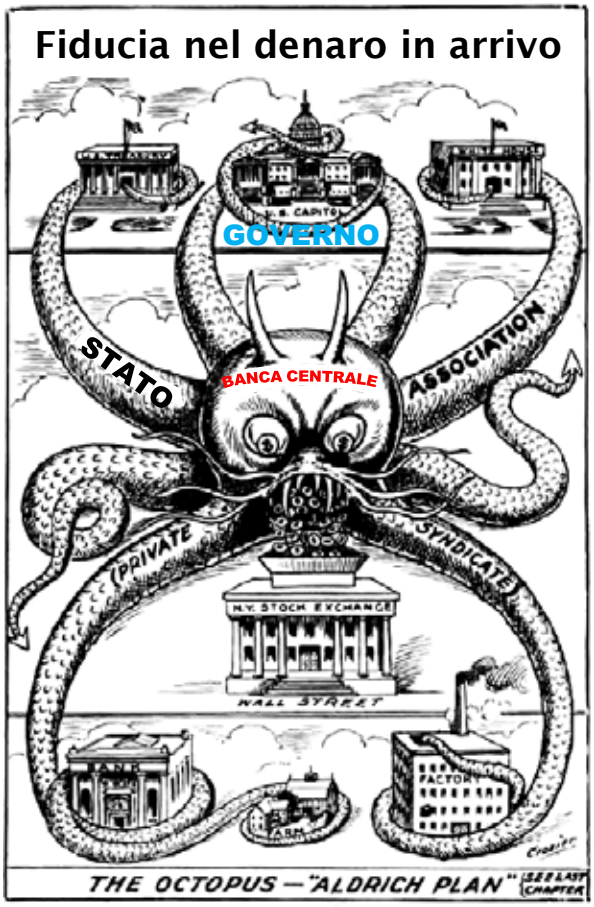


Che cos'è il denaro Fiat e chi lo controlla?

4.2.3 Chi controlla il Sistema Fiat e come ne beneficia?

Gli attori principali sono quattro: il governo, gli individui ricchi, il settore finanziario e la banca centrale. Insieme, controllano il sistema finanziario.

- **Il governo:** è il regista dello spettacolo. Insieme alla riscossione delle imposte, si finanzia attraverso il nuovo debito (obbligazioni) emesso dal Tesoro. Quando la domanda di questi titoli è insufficiente, il debito residuo viene acquistato dalla banca centrale. Ciò significa che possono continuare a svolgere le loro attività e a perseguire i loro interessi senza bisogno dell'approvazione del popolo. È come avere una carta di credito senza preoccuparsi di ripagarla immediatamente. Questo potrebbe sembrare un bene per il governo, ma ha un costo per tutti gli altri.



- **Persone ricche:** traggono molti vantaggi dal sistema del credito. Con la possibilità di accumulare più debiti, possono investire in attività come materie prime, immobili e azioni, creando nuova ricchezza quasi senza sforzo.

- **Settore finanziario (banche):** Le banche e le altre istituzioni finanziarie non controllano direttamente il sistema monetario, ma ne traggono grandi vantaggi. Libere da responsabilità, possono perseguire e accelerare la creazione di nuova moneta attraverso il prestito a riserva frazionaria, beneficiando di maggiori entrate. Le banche sono virtualmente libere da conseguenze, in quanto vengono salvate con nuova moneta per evitare il collasso dell'intero sistema.

- **La Banca Centrale:** è colei che tira le fila, controllando presumibilmente la crescita della massa monetaria. Ma ecco il trucco: la banca centrale è anche soggetta alle leggi del governo e serve gli interessi del governo; è come se un burattinaio fosse controllato da un altro burattinaio. La banca centrale può sembrare quella che comanda, ma è indirettamente al servizio del governo che vuole stampare denaro dal nulla quando ne ha bisogno.

Come traggono vantaggio: Questi gruppi traggono vantaggio in vari modi, creando una complessa rete di controllo. Il governo ottiene fondi senza conseguenze immediate, gli individui ricchi e le banche fanno soldi senza sforzo e la banca centrale mantiene lo spettacolo. Nel frattempo, il resto della popolazione potrebbe risentire degli effetti, affrontando le sfide che il sistema comporta.

Alla fine i burattinai del sistema creano uno spettacolo in cui pochi traggono grandi benefici, ma molti si interrogano sull'equità del palcoscenico finanziario in cui si trovano.

Il ruolo delle banche centrali

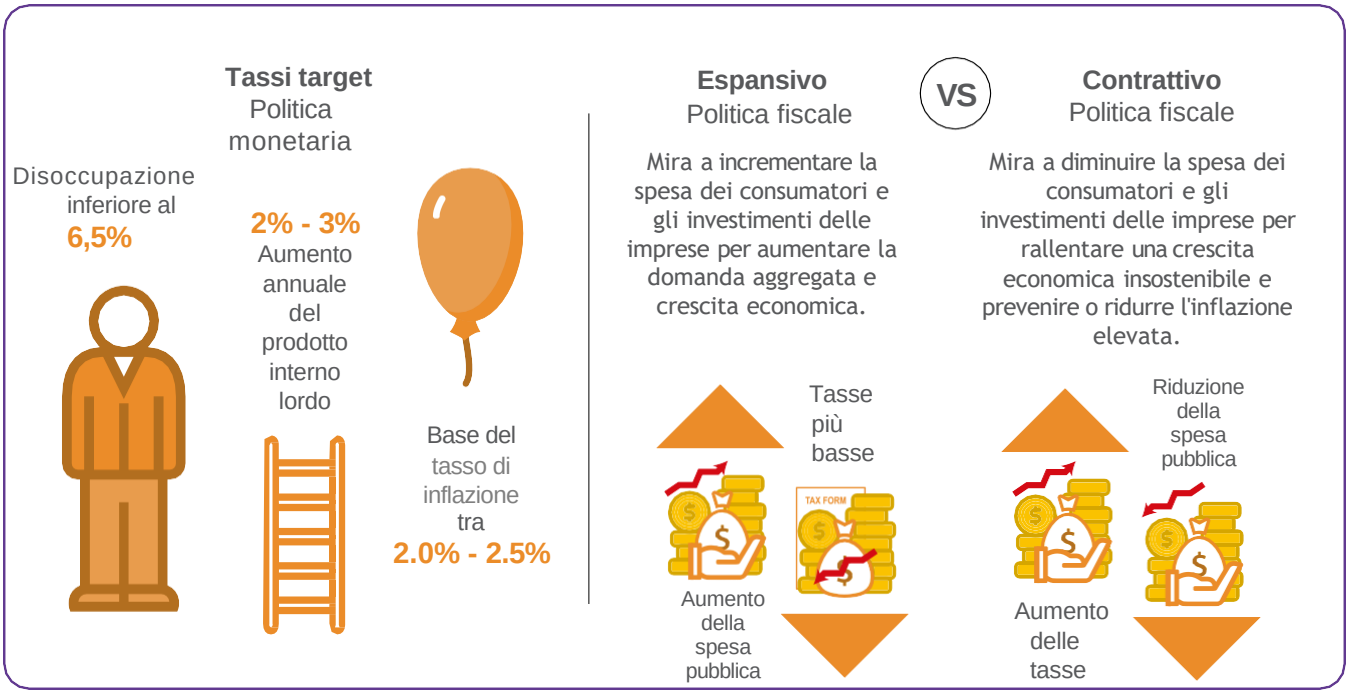
Le banche centrali plasmano silenziosamente il funzionamento di un'economia. Il loro compito principale è quello di garantire la stabilità e l'integrità e "mantenere le cose stabili", ma i loro metodi rivelano un lato più misterioso.

Le banche centrali lavorano a stretto contatto con i governi e tirano le fila della politica monetaria, controllando l'offerta di moneta con strumenti come i tassi di interesse. In tempi di crisi, stampano denaro dal nulla e lo iniettano nell'economia attraverso le banche commerciali, facendo sembrare che tutto vada bene.

Le banche centrali non si limitano a vigilare, ma regolano le banche commerciali, stabiliscono le regole del gioco e intervengono per aiutare le banche in difficoltà (agendo come prestatori di ultima istanza). Questa rete di controllo, pur sembrando protettiva, rende l'economia e le banche ancora più dipendenti da loro.

Capire da dove provengono i trilioni di dollari di fondi di stimolo e chi ne decide l'allocazione è fondamentale per comprendere il più ampio sistema finanziario. I governi utilizzano diversi strumenti per gestire l'offerta di moneta in momenti specifici.

Le banche centrali e i governi possono utilizzare strumenti di politica monetaria e fiscale per influenzare la moneta e l'economia. Ad esempio la Federal Reserve degli Stati Uniti (Fed) utilizza la politica monetaria per regolare i tassi di interesse, influenzando la quantità di denaro in circolazione. La politica fiscale, invece, prevede l'utilizzo di politiche di spesa e fiscali per influenzare l'attività economica.



Che cos'è il denaro Fiat e chi lo controlla?

Le politiche del tasso di cambio, gli shock dell'offerta e il controllo dei prezzi sono strumenti aggiuntivi per regolare l'offerta di moneta e avere un impatto sul commercio e sull'economia. Sebbene queste politiche mirino a stabilizzare i prezzi e a controllare l'inflazione, l'intervento porta spesso a cicli di boom e bust, creando problemi per tutti coloro che utilizzano la valuta controllata.

Esempio: "Troppo grandi per fallire" si riferisce ad istituzioni finanziarie così grandi e interconnesse che il loro fallimento avrebbe ripercussioni catastrofiche sull'intero sistema finanziario. Durante la crisi finanziaria del 2008, diverse grandi banche sono state considerate "troppo grandi per fallire", portando il governo degli Stati Uniti a intervenire e a fornire salvataggi per evitare il loro collasso.

Uno degli esempi più evidenti di istituzione "troppo grande per fallire" durante la crisi finanziaria è stata la banca d'investimento Lehman Brothers. Quando Lehman Brothers ha dichiarato bancarotta nel settembre 2008, si è innescato un effetto domino di eventi, tra cui il quasi crollo del gigante assicurativo AIG e un massiccio calo del mercato azionario. Il governo degli Stati Uniti è dovuto intervenire e fornire salvataggi ad altre importanti istituzioni finanziarie per evitare un ulteriore caos e salvaguardare l'economia in generale.

Conoscere il funzionamento di queste politiche è fondamentale per comprendere i limiti dei sistemi monetari centralizzati. Finché non si comprende il problema, non si riconosce la soluzione. Dopo aver illustrato come il sistema monetario ha funzionato nel passato e nel presente, discuteremo del futuro del sistema monetario: Le valute digitali delle banche centrali, meglio note come **CBDC**.

4.3 Valute digitali delle banche centrali: Il futuro del denaro Fiat

Le valute digitali delle banche centrali (Central Bank Digital Currencies, **CBDC**) sono il passo successivo alle valute nazionali. A differenza della combinazione di banconote fisiche, monete e pagamenti digitali, le CBDC sono forme completamente digitali di valute a corso emesse dai governi e controllate dalle banche centrali.

Immaginate la valuta che utilizzate ogni giorno, ma senza alcuna presenza fisica: niente monete che tintinnano in tasca o banconote da piegare. Ciò che distingue le CBDC è il maggior livello di controllo e monitoraggio che offrono a governi e banche centrali. Con le CBDC le autorità ottengono una visibilità senza precedenti sulle transazioni finanziarie, rendendo più facile tracciare e regolare il flusso di denaro.

I governi e le banche centrali possono facilmente regolare la forma e l'offerta di CBDC, manipolare i tassi di interesse e utilizzare con maggiore precisione gli strumenti di politica monetaria e fiscale. In sostanza le CBDC forniscono alle autorità un mezzo più efficiente per influire e gestire la propria valuta.

Sebbene le CBDC sembrino il futuro della moneta fiat, l'attuale sistema monetario mondiale opera già su uno standard fiat puro. Le valute fiat non sono più legate all'oro, il che ha portato a una significativa espansione dell'offerta monetaria senza alcuna restrizione reale.

Ora che avete una comprensione più chiara del funzionamento del sistema fiat, è il momento di esplorare il suo funzionamento e le conseguenze nel Capitolo 5.

Capitolo #5

Come i problemi portano alle soluzioni

Libro di lavoro per studenti

Versione italiana| 2025

Come i problemi portano alle soluzioni

5.0 Introduzione al problema

> Chiunque controlli il volume di denaro nel nostro Paese è padrone assoluto di tutta l'industria e il commercio... Quando vi renderete conto che l'intero sistema è molto facilmente controllato, in un modo o nell'altro, da pochi uomini potenti ai vertici, non avrete bisogno di sentirvi dire come nascono i periodi di inflazione e depressione.
>
> **James A. Garfield, Presidente degli Stati Uniti.**

Nel Capitolo 4 avete imparato che il mondo finanziario si basa su un sistema che potrebbe non essere così solido come sembra. Il sistema finanziario, sostenuto da continue aggiunte di cartamoneta, sembra giovare più a pochi che a molti.
Questo capitolo spiega cosa significa il sistema fiat per le persone normali e per la società. Infine, esploriamo la storia di un gruppo di individui che ha notato i problemi e ha lavorato silenziosamente per trovare una soluzione che potrebbe cambiare il futuro della società umana.

5.1 Diminuzione del potere d'acquisto

5.1.1 L'inflazione monetaria e il suo effetto sul potere d'acquisto

L'inflazione monetaria è l'aumento dell'offerta di moneta all'interno di un'economia che ha un impatto diretto sulla persona media riducendo il suo potere d'acquisto. Il ciclo di inflazione dei prezzi inizia quando c'è più denaro in circolazione. Questo, a sua volta, aumenta la domanda di beni e servizi causando in ultima analisi un aumento dei prezzi.

Immaginiamo un piccolo gruppo di amici - Alex, Bob e Charlie - ognuno con un dollaro in mano e una bottiglia d'acqua disponibile per la vendita. La situazione iniziale è semplice: tre persone con un totale di tre dollari e una bottiglia d'acqua. Ora supponiamo che qualcuno - diciamo l'amministrazione locale - decida di dare a ciascun amico un dollaro in più. Ora hanno complessivamente sei dollari: con questo nuovo denaro tutti hanno voglia di comprare quella singola bottiglia d'acqua. Poiché tutti e tre gli amici vogliono la stessa bottiglia, iniziano a fare offerte l'uno contro l'altro.

L'aumento della domanda alimentato dai soldi in più, li spinge ad offrire più del prezzo iniziale della bottiglia d'acqua. Alla fine la guerra delle offerte fa aumentare il prezzo della bottiglia d'acqua. Questa situazione riflette una diminuzione del loro potere d'acquisto. Anche se hanno più soldi, non possono comprare tante bottiglie d'acqua come prima, mostrando l'impatto dell'inflazione sul valore del loro denaro.

In questo esempio gli amici hanno subito una diminuzione del loro potere d'acquisto perché stavano utilizzando una forma di denaro influenzata da fattori esterni come i dollari aggiuntivi introdotti dal governo. La mancanza di controllo sull'offerta di moneta, unita all'aumento della domanda, ha portato a un aumento dei prezzi, rendendo più difficile per gli amici acquistare la stessa quantità di beni con i loro dollari aggiuntivi.

Questo illustra come il potere d'acquisto degli amici sia stato influenzato da fattori al di fuori del loro controllo, sottolineando l'importanza di comprendere e mettere in discussione i sistemi che influiscono sul valore del nostro denaro.

Analizziamo ora come si svolge nella vita reale.

Attività: Gli effetti dell'inflazione - Un'attività d'asta

Obiettivo: Comprendere il concetto di inflazione e il modo in cui influisce sui prezzi di beni e servizi in un paese.

Definizioni:

- L'offerta di moneta: la quantità totale di moneta in circolazione in un'economia in un determinato momento. Questo include:
  - Valuta fisica, come monete e banconote
  - Conti correnti
  - Conti di risparmio
  - Conti di trading
  - Piccoli depositi a tempo (come i CD) inferiori a 100.000 dollari
- Asta: vendita pubblica in cui beni o proprietà vengono venduti al miglior offerente.

Esercizio in classe - Seguite le istruzioni riportate di seguito:

1. Riceverete dall'insegnante una quantità casuale di denaro del Monopoli: questo rappresenta l'offerta di denaro in una società.

2. Scrivete la massa monetaria totale nel grafico fornito.

3. L'insegnante metterà all'asta una barretta di cioccolato per gli studenti. Per aggiudicarsi la barretta, è necessario fare l'offerta più alta usando i soldi del Monopoli. Registrate l'offerta vincente accanto alla scorta di denaro.

4. L'insegnante aggiungerà quindi una quantità significativa di denaro del Monopoli alla massa monetaria totale. Questo rappresenta un aumento dell'offerta di moneta in un'economia. In seguito, imparerete come si aggiunge o si riduce la massa monetaria in un'economia.

Le società possono spesso essere imprevedibili e ingiuste, come dimostra la simulazione di un insegnante che dà a caso una quantità significativa di denaro solo ad alcuni studenti selezionati. Questa simulazione riproduce le situazioni reali in cui può verificarsi una distribuzione ineguale delle risorse e delle opportunità, evidenziando la casualità e l'iniquità intrinseche di molte situazioni.

5. L'insegnante metterà all'asta una seconda barretta di cioccolato tra gli studenti, seguendo lo stesso procedimento. Riportate l'offerta vincente accanto alla dotazione di denaro sul grafico.

6. L'insegnante ripeterà l'asta una terza volta.

Giro	Offerta di moneta	Offerta vincente
1		
2		
3		

Conclusioni:

1. In che modo l'aumento dell'offerta di moneta ha influito sulle offerte vincenti per le barrette di cioccolato?
2. Qual'è la relazione tra aumento dell'offerta di denaro e l'inflazione?
3. In che modo l'offerta di moneta è rilevante nel mondo reale?
4. Quando viene immesso nuovo denaro nell'economia, cosa pensate che succeda ai prezzi di beni e servizi? Ritenete che la variazione dei prezzi sia temporanea o permanente, Perché?

Come pensate che le variazioni dei prezzi influenzino i cittadini nel lungo periodo?

5.2 L'onere del debito globale e la disuguaglianza sociale

5.2.1 Impatto sui singoli - Perdita del potere d'acquisto

Jaime è uno studente universitario che vive in un piccolo appartamento. Lavora part-time in un bar per pagare le spese di vita e le tasse universitarie. Non appena ha iniziato a vivere in modo indipendente, Jaime è diventato bravo a gestire il proprio libro mastro.

Un **libro mastro** è un registro dettagliato di tutte le transazioni monetarie, sia che si tratti di denaro che di guadagni o spese, un libro mastro vi aiuta a tenere traccia di tutto.

All'inizio del 2023, ha preventivato 10.000 dollari per le sue spese di vita per l'intero anno, compresi affitto, cibo e altri beni di prima necessità. Queste sono le sue transazioni per il mese di gennaio 2023:

Data	Descrizione	Importo	Tipo	Equilibrio
01/01/2023	Saldo iniziale			$1,600
01/01/2023	Affitto di gennaio	$800	Debito	$800
05/01/2023	Generi alimentari	$100	Debito	$700
15/01/2023	Busta paga part-time	$500	Credito	$1,200
20/01/2023	Gas per auto	$350	Debito	$850
30/01/2023	Libri di testo	$150	Debito	$700

Il libro mastro mostra che il saldo iniziale di Jaime era di 1.600 dollari, di cui ha speso (a debito) 800 dollari per pagare l'affitto del mese. Ha poi speso 100 dollari per la spesa e ha ricevuto 500 dollari (un credito) per il suo lavoro part-time, portando il saldo a 1200 dollari. Ha poi speso soldi per la benzina e i libri di testo portando il saldo da 1200 dollari a 700 dollari alla fine del mese.

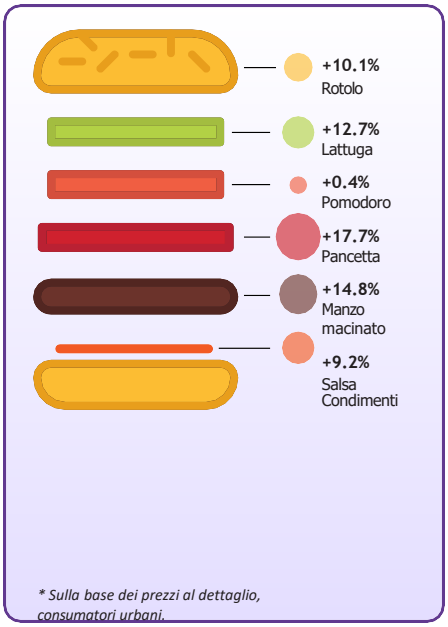
Dodici mesi dopo, Jaime è a pranzo con il nonno con cui condivide i dettagli del suo bilancio per il 2024 e parlandone con il nonno nota che il suo budget non si estende più come prima e che il costo della vita è aumentato in modo significativo nell'ultimo anno. Mentre Jaime si chiede come sia possibile, il nonno gli mostra l'immagine successiva.

Jaime non può credere ai suoi occhi: è il momento in cui scopre che il costo dei beni e dei servizi aumenta drasticamente nel tempo, portando a una diminuzione del suo potere d'acquisto.

Racconta il nonno: "Nel 1956, ero solo un giovane che si affacciava al mondo. Ricordo che guadagnavo 380 dollari al mese come operaio. Può sembrare poco, ma all'epoca era uno stipendio decente. In effetti, sono riuscito a risparmiare abbastanza per comprarmi una casa in periferia".

Il nonno prosegue: "I costi delle cose erano molto differenti nel secolo scorso. Ad esempio, nel 2020, l'acquisto di 30 barrette di cioccolato Hershey's costerà 26,14 dollari. Tuttavia, se torniamo indietro nel tempo fino al 1913, il costo per la stessa quantità di tavolette di cioccolato Hershey's sarebbe di solo un dollaro".

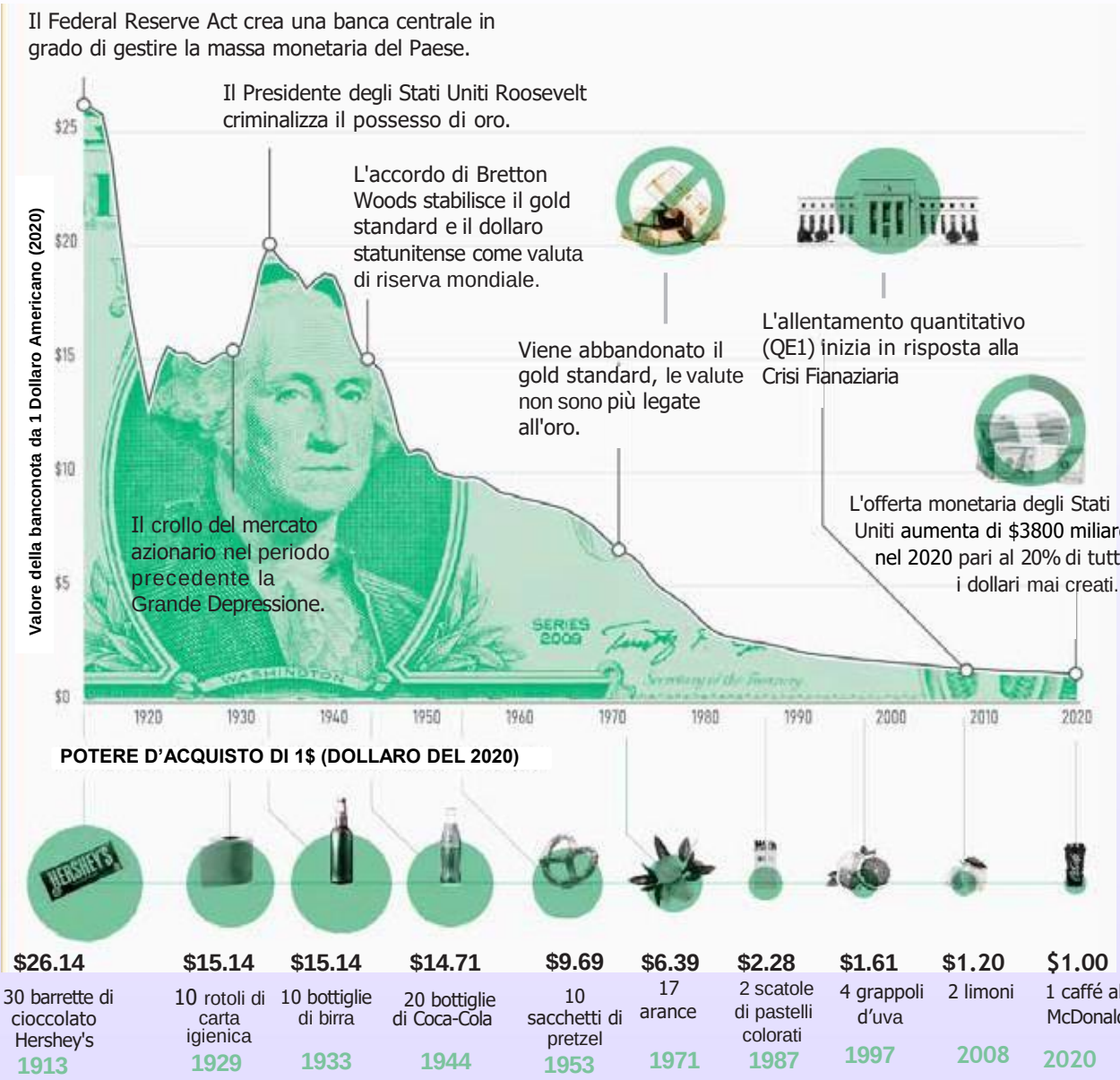
Questa significativa differenza di prezzo mette in evidenza la variazione del potere d'acquisto della valuta nel tempo e come essa si sia spostata nel corso degli anni a causa dell'inflazione.



Come i problemi portano alle soluzioni

Il valore di un dollaro
Potere d'acquisto del dollaro USA

Il potere d'acquisto del dollaro statunitense è diminuito drasticamente nel corso dell'ultimo secolo a causa dell'aumento dell'infllazione e dell'offerta di moneta.



Jaime: *"Cosa? È pazzesco! Non riesco a immaginare quanto sarebbe stato basso il mio affitto allora rispetto ad oggi".*

Nonno: *"Beh sì, il tuo affitto sarebbe stato molto più economico a quei tempi. Ho un altro esempio per illustrarlo: all'epoca con un dollaro si compravano circa 10 sacchetti di pretzel. Nel 2020 ho pagato 9,69 dollari per la stessa quantità. Immaginate quanto costerebbero oggi 10 sacchetti di pretzel".*

Jaime: *"Wow, è davvero interessante, nonno. Come hai vissuto tu stesso questa esperienza quando eri più giovane?".*

Nonno: *"Oh, Jaime, tutte le cose erano molto più economiche quando ero giovane. Una pagnotta costava solo 0,18 dollari e si poteva comprare un gallone di benzina a soli 0,29 dollari. È incredibile quanto sia aumentato il costo della vita".*

Dopo la conversazione con il nonno Jaime torna a casa per dare un'altra occhiata al suo libro mastro. Scopre subito che per il 2024 deve mettere a bilancio altri 1.000 dollari per poter acquistare lo stesso paniere di beni e servizi dell'anno precedente. Ciò significa che il suo potere d'acquisto è diminuito di 1.000 dollari, poiché ora deve spendere di più per acquistare gli stessi beni e servizi. Mentre lo stipendio di Jaime aumenta solo di poco, i suoi costi di vita salgono alle stelle ogni anno.

La tabella seguente mostra i costi sostenuti da Jaime nel primo e nel secondo anno, nonché l'aumento percentuale di tali costi.

Affinché Jaime possa vivere con lo stesso tenore di vita, dovrà lavorare più ore alla settimana per ricevere 1.000 dollari in più.

In base ai dati dell'Ufficio Statistico del Lavoro degli Stati Uniti, i prezzi di oggi sono circa 30 volte superiori a quelli del 1913. Ciò significa che un dollaro oggi può comprare solo il 3% circa di quanto poteva comprare allora.

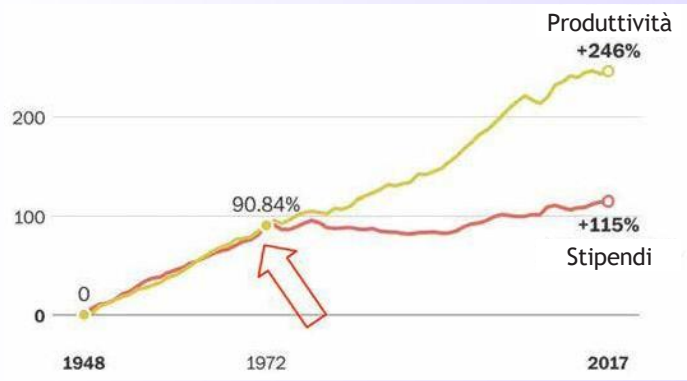
Articolo	Costo Anno #1	Costo Anno #2	% Aumento
Affitto	$4,000	$4,500	12.5%
Generi alimentari	$2,000	$2,300	15%
Necessità	$4,000	$4,200	5%
Totale	**$10,000**	**$11,000**	**10%**

Per esempio qualcuno offre a Jaime una scelta di viaggio nel tempo: prendere 100 dollari nel 1913 o aspettare fino al 2023 e ricevere solo 3 dollari - è come scegliere tra una spesa fatta in passato o qualche piccolo sfizio oggi. La significativa differenza di valore mostra quanto sia diminuito il potere d'acquisto del denaro nel corso degli anni.

Come i problemi portano alle soluzioni

Se pensiamo ai numeri, Jaime guadagna molti più dollari in un anno di quanti ne abbia mai guadagnati suo nonno, ma i dollari che il nonno di Jaime possedeva erano molto più preziosi e potevano comprare molto di più all'epoca.

Crescita della produttività e della retribuzione oraria (1948-2017)



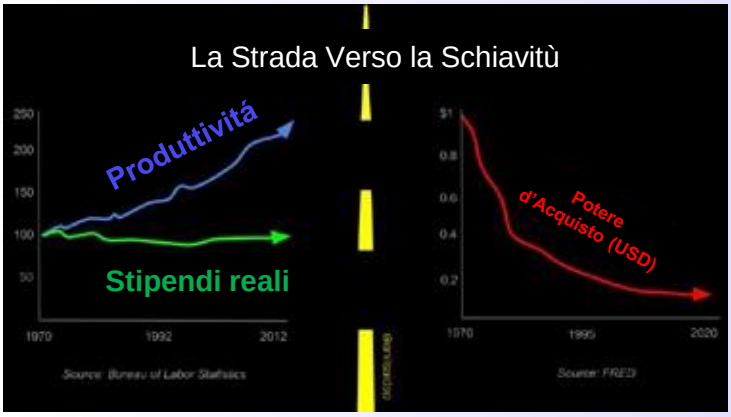
NOTA: La retribuzione comprende stipendi e benefit per i lavoratori di produzione e non addetti alla supervisione.

Nel mondo di oggi l'impatto significativo dell'inflazione scoraggia le persone dal risparmiare.

Al contrario, la maggior parte sceglie di spendere subito il proprio denaro perché il suo valore diminuisce rapidamente. Questa visione pessimistica ostacola la capacità di pianificare il futuro.

Come si vede nel grafico, la crescita salariale di un individuo medio rimane stagnante se aggiustata per l'inflazione, il che significa che non riceve aumenti allo stesso ritmo della diminuzione del valore del suo denaro, nonostante lavori di più.

L'esempio di Jaime è solo uno dei tanti. Nel mondo attuale è abbastanza comune che i governi creino denaro dal nulla per promuovere la propria agenda lasciando che siano i singoli cittadini di tutto il mondo a subirne le conseguenze. I prezzi dei beni di uso quotidiano, dal pane alla casa, dai generi alimentari alle vacanze, aumentano ogni anno. Mentre i ricchi beneficiano dell'inflazione grazie al possesso di beni, la gente comune vede il proprio denaro guadagnato con fatica perdere valore. Il risultato? Le persone e le famiglie di tutto il mondo sono in difficoltà a causa della diminuzione del loro potere d'acquisto.



Le persone di tutto il mondo si ritrovano a fare più lavori e più ore di lavoro solo per mantenere lo stesso tenore di vita. È come essere su un tapis roulant: si corre sempre più veloce, ma non si riesce mai ad andare avanti. Il sistema del fiat fa sentire gli individui come se fossero in una corsa perpetua contro l'aumento dei prezzi.

Nella lotta per tenere il passo con l'aumento dei costi, molti ricorrono al credito, che è come usare un piccolo cerotto su una ferita molto profonda. Le persone contraggono prestiti o prendono decisioni impulsive solo per tirare avanti. Il denaro veloce diventa una necessità e le persone si ritrovano in un circolo vizioso in cui la sopravvivenza di oggi ha la precedenza sulla pianificazione del domani.

Il sistema monetario con la sua costante stampa di denaro, ha un impatto sulla psicologia dell'umanità. Infonde un'alta preferenza per il tempo, nonchè un'attenzione ai guadagni a breve termine rispetto alla pianificazione a lungo termine. Proprio come un fix veloce per un sollievo immediato gli individui nel mondo del fiat tendono a dare priorità ai benefici a breve termine. È un istinto di sopravvivenza che crea un ciclo di dipendenza in cui gli individui cercano qualsiasi mezzo per ottenere denaro veloce, anche se non è sostenibile o praticabile nel lungo periodo.

In sostanza, l'impatto del sistema fiat dipinge un quadro difficile per gli individui a livello globale. Nel sistema del fiat i prezzi aumentano, i redditi ristagnano e la lotta per la sopravvivenza diventa una battaglia quotidiana. Mentre alcuni gruppi si arricchiscono, la maggior parte degli individui in tutto il mondo rimane dipendente da un sistema che li rende sempre più poveri.

5.2.2 Impatto sulla società - Aumento della disuguaglianza di ricchezza

In una società basata sulla moneta sonante, il processo decisionale finanziario di un governo è legato all'approvazione del popolo. Nel sistema monetario, invece, i governi possono indebitarsi illimitatamente sulle spalle dei cittadini.

Il potere di stampare moneta a piacimento porta spesso a una centralizzazione politica. Il sistema del fiat permette ai governi di accumulare debiti enormi, prendendo decisioni che vanno a vantaggio di se stessi piuttosto che della maggioranza.
Le superpotenze come gli Stati Uniti ottengono un vantaggio competitivo grazie a questo fenomeno: possono stampare denaro all'infinito per finanziare i loro piani, guerre comprese. Questa capacità permette a queste nazioni dominanti di controllare, influire e impegnarsi in conflitti geopolitici, creando uno squilibrio di potere globale. Le guerre e le azioni più importanti per controllare gli altri diventano finanziariamente fattibili per le superpotenze, mentre gli altri che non hanno la stessa flessibilità finanziaria devono affrontare delle limitazioni.

Con il sistema fiat la ricchezza non si distribuisce in modo uniforme. Al contrario, tende a concentrarsi nelle mani di pochi eletti. Questo fenomeno è come una partita a Monopoli, dove una manciata di giocatori possiede quasi tutti gli alberghi e le proprietà, mentre la maggioranza lotta per rimanere a bocca asciutta. Il sistema monetario è diventato uno strumento per alcuni gruppi per concentrare la ricchezza. La stampa di moneta permette ai governi e alla loro stretta collaborazione con le banche centrali di iniettare più moneta nell'economia, e i destinatari di questo denaro appena creato sono coloro che hanno già ricchezza e status - entità e individui potenti. Questi gruppi beneficiano del denaro appena stampato prima che i suoi effetti negativi, come la diminuzione del potere d'acquisto, inizino a manifestarsi nell'economia.

Come i problemi portano alle soluzioni

La disuguaglianza di ricchezza non riguarda solo chi ha e chi non ha, ma anche la soppressione della mobilità economica. Chi proviene da ambienti meno privilegiati trova sempre più difficile salire la scala economica, come se dovesse iniziare una corsa con uno zaino pesante. Il crescente divario tra ricchi e poveri causa problemi a tutti, con i ricchi che modellano le politiche a loro favore. Questo rende le cose più difficili per le persone normali, portando a disordini sociali, mancanza di fiducia nelle istituzioni e comunità che cadono a pezzi come un castello di carte. L'instabilità del sistema del fiat si manifesta nell'incertezza economica, nei disordini politici e nelle ripercussioni globali quando il mondo occidentale affronta una recessione economica.

Si tratta di un fenomeno globale, che colpisce le società dei Paesi sviluppati e di quelli in via di sviluppo. I ricchi che spesso operano su scala transnazionale, utilizzano il sistema finanziario globale a loro vantaggio, ampliando ulteriormente il divario tra le classi superiori e quelle inferiori.

Con il sistema del fiat, indebitarsi è diventata la norma per l'umanità. Governi, istituzioni, imprese e individui di tutto il mondo si trovano immersi in un mare di debiti.

Il cambiamento psicologico che porta a considerare il debito come accettabile ha le sue radici nella struttura del sistema finanziario. Negli ultimi decenni è diventato sempre più facile per le entità contrarre debiti consistenti, che spesso diventano una necessità per la gente comune a causa dell'aumento dei prezzi e del costo della vita.

Il consumismo, ovvero il costante bisogno di comprare e consumare in breve tempo, porta le persone ad acquistare più del necessario con conseguente consumo eccessivo e spreco. Sebbene possa sembrare una corsa agli acquisti senza fine, il costo reale va oltre il cartellino del prezzo, incidendo sulla salute e sul benessere psicologico delle persone.

Diventa chiaro che il sistema fiat non è solo un meccanismo economico: è soprattutto un sistema che modella la società umana nel suo complesso. Dalla concentrazione del potere alle dinamiche globali, alle disparità di ricchezza e alle norme sociali, il sistema fiscale influenza direttamente il funzionamento delle nazioni e la vita dei cittadini.

Attività: Conseguenze del sistema Fiat

1. Ci sono altre conseguenze che gli individui e la società nel suo complesso subiscono come risultato del sistema fiat?

2. Quali sono le conseguenze nel tuo paese a causa del sistema FIAT ? Cos'è accaduto nel corso della storia e come ha influenzato la popolazione del tuo paese?

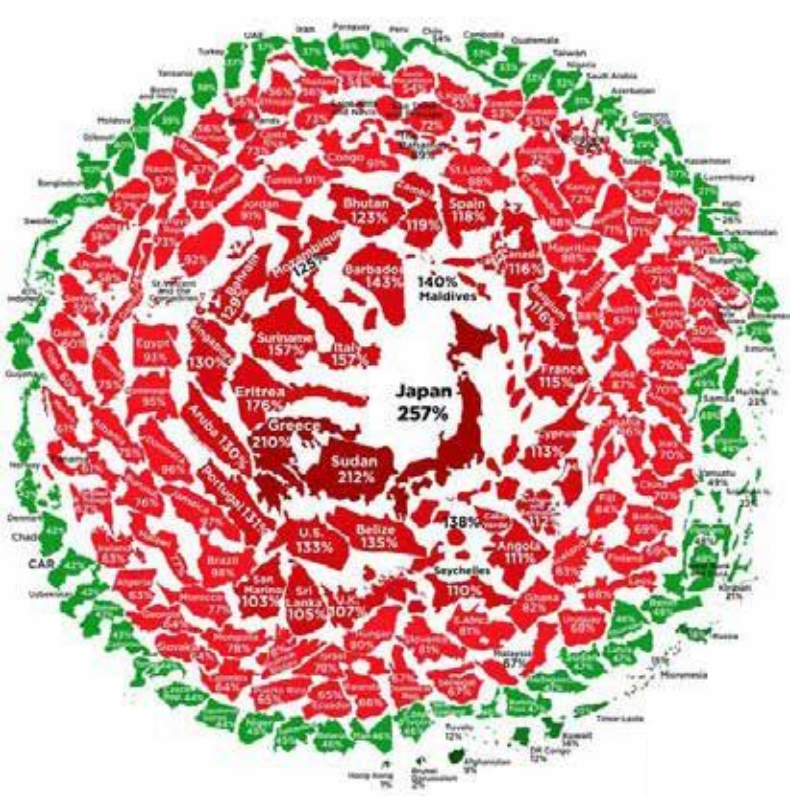
a. Esempi personali : sessione interattiva

5.2.3 L'onere del debito globale

Come risultato del sistema del fiat, i governi di tutto il mondo si trovano bloccati in un'enorme rete di debiti, intrappolati in quella che viene chiamata "la spirale del debito globale". Immaginate uno scenario in cui si prende in prestito più denaro di quanto si possa sperare di ripagare: questo sta accadendo su vasta scala in tutto il mondo. I governi, affogati nel debito, sono rimasti intrappolati in un pericoloso gioco di accumulare più debito di quanto possano mai restituire. È una storia di spese sconsiderate, prestiti e mancanza di lungimiranza che ora spinge le nazioni di tutto il mondo sull'orlo del disastro finanziario.

Ad oggi il governo federale degli Stati Uniti ha aggiunto uno sconcertante debito di 10.000 miliardi di dollari dal 2019. Il debito totale è schizzato da circa 23.000 miliardi di dollari nel quarto trimestre del 2019 all'astronomica cifra di 34.000 miliardi di dollari di oggi. Il ritmo con cui i governi a livello globale sfornano nuovo debito non sta rallentando, anzi, sta accelerando. Secondo le proiezioni, il 2023 sarà l'anno con il maggior incremento del debito dai tempi turbolenti del 2021, segnati dalla pandemia di Covid.

Lo stato del debito pubblico mondiale



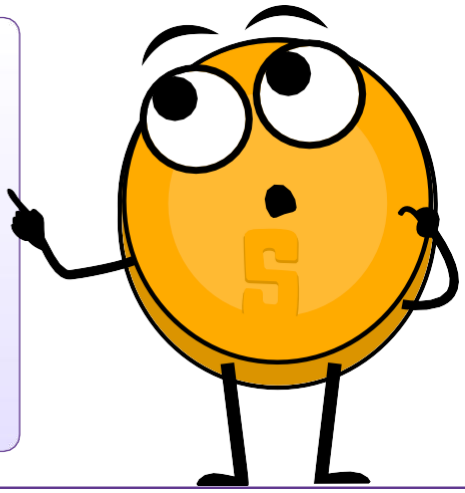
Che cosa significa tutto ciò per gli individui e le società che devono già affrontare le conseguenze del sistema finanziario? La spirale del debito in cui sono invischiati è come una palla di neve che rotola giù da una collina: continua a crescere e non sappiamo come fermarla.

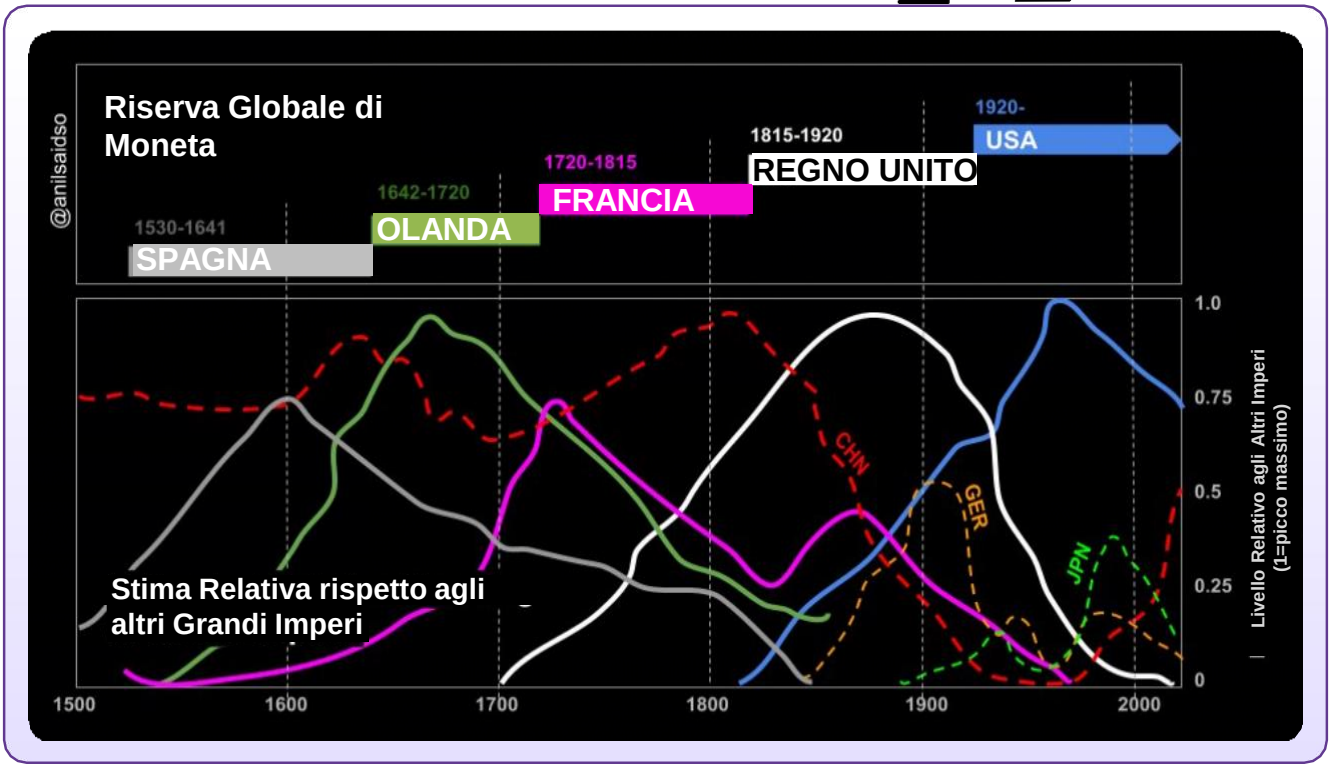
Le conseguenze menzionate in precedenza, dalla disuguaglianza di ricchezza ai disordini sociali, non svaniranno. Al contrario, l'onere del debito globale ha raggiunto un punto di non ritorno, garantendo che le cose siano destinate a peggiorare.

Rapporto debito/PIL 2021 (%)

- 200% e oltre
- 100% - 199.9%
- 50% - 99.9%
- 20% - 49.9%
- 10 - 19.9%
- Meno del 10%

> Non credo che avremo mai più denaro buono finché non toglieremo la questione dalle mani del governo... Tutto ciò che possiamo fare è introdurre e fare circolare, in qualche modo astuto, qualcosa che non possano fermare.
>
> ***Friedrich Hayek***
> Premio Nobel per l'economia





5.3 I Cypherpunk e la ricerca di un Valuta decentralizzata

Nel corso della storia abbiamo osservato una progressiva appropriazione del denaro da parte di banche e governi, che ha portato al sistema monetario odierno e alle sue disastrose conseguenze per la società. Ma l'avvento di nuove tecnologie come la crittografia e Internet ha permesso l'emergere di nuove idee, come il denaro digitale indipendente, libero dall'intervento dei governi, aperto e accessibile a tutti. Immergiamoci nel viaggio di coloro che guidano questo movimento rivoluzionario: i cypherpunk.

5.3.1 I Cypherpunk

> Il computer può essere usato come strumento per liberare e proteggere le persone, piuttosto che per controllarle.
>
> **Hal Finney**

La seconda metà del XX secolo ha visto l'affermarsi di molteplici scoperte tecnologiche, come il computer e Internet, aprendo la strada a una nuova era digitale.

Un gruppo di persone scoprì che queste enormi innovazioni avrebbero presto trasformato il funzionamento della società. Prevedevano sia il potenziale che il pericolo del personal computer, tanto come strumento di libertà per potenziare l'individuo quanto come mezzo di controllo e sorveglianza totale.

Queste persone erano chiamate Cypherpunks. Sono emersi come un gruppo di attivisti, crittografi, programmatori e attivisti per la privacy che condividevano una visione comune: la ricerca della privacy, della sicurezza e di un futuro digitale decentralizzato. Il termine "Cypherpunk" è una fusione di "cypher", che si riferisce al codice crittografico e "punk", che rappresenta l'etica controculturale della ribellione.

I Cypherpunk credevano nel potere della crittografia per proteggere le libertà individuali. Tra i loro obiettivi c'era lo sviluppo di strumenti per proteggere le comunicazioni online, anonimizzare le attività su Internet e creare valute digitali per operare al di fuori del controllo delle autorità centralizzate.

I Cypherpunk compresero le conseguenze del sistema fiat e videro la minaccia di un "futuro orwelliano". Credevano di dover fare in modo che il personal computer e Internet diventassero un bene per l'umanità, anziché strumenti in grado di esacerbare il controllo dello Stato sulla popolazione.

LA DEFINIZIONE DI "FUTURO ORWELLIANO":

Un futuro orwelliano si riferisce a una visione distopica ispirata alle opere di George Orwell. Il termine è associato a una società da incubo e totalitaria, caratterizzata da un controllo governativo oppressivo, da un'ampia sorveglianza, dalla propaganda e dalla manipolazione delle informazioni. Il termine "orwelliano" descrive spesso uno scenario in cui le libertà dei cittadini e l'autonomia individuale sono fortemente limitate, il dissenso è soppresso e la realtà è distorta per servire gli interessi di un regime potente e autoritario. Il concetto prende il nome da George Orwell, che nei suoi scritti ha messo in guardia dai potenziali pericoli di un potere governativo incontrollato e dall'erosione dei diritti umani fondamentali.

Come i problemi portano alle soluzioni

Tra le figure chiave del movimento Cypherpunk figurano luminari come Eric Hughes, Timothy C. May e John Gilmore. Nel 1992 Eric Hughes scrisse "A Cypherpunk Manifesto" delineando i principi del gruppo. Il manifesto enfatizzava l'importanza della privacy, della crittografia e della necessità per gli individui di assumere il controllo della propria identità digitale.

Guardate questo video e scoprite la storia dei Cypherpunk!

Una delle invenzioni più notevoli dei Cypherpunk è stata la creazione di strumenti e protocolli crittografici. Nel 1991 Phil Zimmermann introdusse PGP (Pretty Good Privacy), un software per la crittografia delle e-mail che divenne un progetto di punta. PGP permetteva agli utenti di inviare messaggi crittografati su Internet senza che nessuno potesse decifrarli, tranne il destinatario. Prima di allora qualsiasi messaggio inviato su Internet poteva essere intercettato e letto da altri, governi compresi.

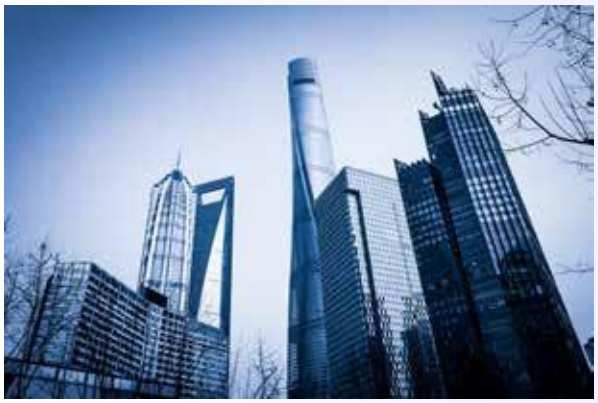
I Cypherpunk pensavano che la scoperta della crittografia, insieme ad Internet e al computer, fornisse una solida base per la creazione di reti decentralizzate nello spazio digitale, consentendo agli individui di comunicare e di effettuare transazioni su Internet privatamente e senza l'interferenza di un'autorità centrale.

I Cypherpunk erano sulla strada giusta per promuovere un futuro più luminoso per l'umanità, dove la tecnologia sarebbe stata uno strumento per massimizzare la libertà invece del controllo. Gli unici pezzi mancanti erano una rete decentralizzata e una moneta digitale.

5.3.2 Sistemi centralizzati e sistemi decentralizzati

Sistemi centralizzati: un solo sovrano, molti problemi
In un sistema centralizzato tutto ruota attorno a un'autorità principale, come un alto edificio in una città. Queste autorità controllano il funzionamento dell'intero sistema. Si pensi ad esempio alle banche tradizionali, dove un piccolo gruppo prende tutte le decisioni.

Esempio del mondo reale: Nel 2022 durante le proteste pacifiche in Canada, le banche hanno bloccato i conti dei manifestanti, dimostrando come un'autorità centrale possa intervenire e controllare l'accesso finanziario.



Problemi con i sistemi centralizzati:

- Punto di guasto centrale: se qualcosa va storto con l'autorità centrale, l'intero sistema può crollare.
- Controllo: un piccolo gruppo al vertice ha tutto il controllo e il potere e spesso prende decisioni che vanno a vantaggio principalmente di chi è al vertice.
- Inefficienza e intermediari: come gli ingorghi in città, i sistemi centralizzati possono diventare lenti e costosi a causa di intermediari non necessari.
- Mancanza di autonomia: le persone potrebbero non essere in grado di fare le proprie scelte finanziarie; tutto viene deciso dalle autorità.
- Censura e restrizione: proprio come alcune zone di una città possono essere bloccate, i sistemi centralizzati possono bloccare o limitare l'accesso a determinate risorse finanziarie.
- Sfide di scala: quando più persone hanno bisogno di servizi finanziari, i sistemi centralizzati possono faticare a tenere il passo.
- Rischi per la sicurezza: problemi con l'autorità centrale possono mettere l'intero sistema a rischio di attacchi informatici.
- Mancanza di trasparenza e fiducia: Il funzionamento interno dei sistemi centralizzati può essere difficile da comprendere, rendendo difficile la fiducia delle persone.

Sistemi decentralizzati: Potere al popolo

- Ora pensate a un sistema decentralizzato come a una grande foresta: ogni albero rappresenta una parte separata e l'intera foresta rappresenta l'intero sistema. A differenza di una città con un unico punto centrale, un sistema decentralizzato è più simile a una foresta resiliente che può andare avanti anche se una parte ha dei problemi.

Esempio del mondo reale: La rete Tor e il suo browser creano un sistema decentralizzato in cui le persone possono rimanere anonime su Internet e la rete è difficile da fermare o censurare.

Vantaggi dei sistemi decentralizzati:

- Maggiore resilienza e affidabilità: non esiste un singolo punto di guasto, il che rende il sistema solido anche se ci sono dei problemi.
- Maggiore sicurezza: con la giusta crittografia/protezione un sistema decentralizzato resiste meglio al controllo di un'unica autorità.

- Maggiore sovranità: le persone hanno un maggiore controllo sul proprio denaro, sui propri dati e sulle proprie decisioni.
- Maggiore trasparenza: tutti vedono le stesse informazioni, rendendo il sistema più affidabile.
- Natura libera e illimitata: chiunque può aderire o partecipare, rendendolo un sistema finanziario inclusivo.
- Pari opportunità: tutti hanno la possibilità di contribuire e dire la loro.
- Maggiore privacy: i dati sono distribuiti tra più partecipanti e per lo più pseudonimi, il che rende i sistemi decentralizzati più privati.

Sebbene i sistemi decentralizzati presentino molti vantaggi, prendere decisioni può rivelarsi complicato perchè richiede che tutti lavorino insieme.

Cambiare il modo in cui il potere viene esercitato

Nel mondo dei sistemi centralizzati e decentralizzati, tutto dipende da chi detiene il potere. I sistemi centralizzati danno il potere a un piccolo gruppo, mentre i sistemi decentralizzati lo distribuiscono, permettendo a tutti di avere voce in capitolo. Questo spostamento di potere significherebbe un futuro più equo e democratico, in cui molte persone influenzano il sistema che plasma le loro vite.

5.3.3 Breve storia delle valute digitali

Uno dei concetti più importanti discussi dai Cypherpunk è stato il denaro digitale. I Cypherpunk si resero conto che Stato e denaro dovevano essere separati per garantire che il futuro andasse a beneficio del bene comune. Il lavoro pionieristico di David Chaum sui protocolli crittografici per transazioni sicure e private ha gettato le basi. L'aspetto negativo era che questo protocollo richiedeva un'autorità centrale per funzionare in modo efficiente, sollevando preoccupazioni circa un singolo punto di fallimento e una potenziale censura.

Negli anni successivi, diversi Cypherpunk hanno cercato di iterare le idee degli altri per creare una soluzione praticabile per una valuta digitale libera dal controllo governativo. La tabella seguente descrive alcune innovazioni chiave sviluppate dai Cypherpunk nel loro tentativo di creare denaro digitale:

Nome e data	Descrizione	Limitazioni
E-Cash (1982)	L'E-Cash di David Chaum è stato un primo concetto di denaro elettronico, incentrato sulla privacy attraverso tecniche crittografiche.	È stata richiesta un'autorità centrale, sollevando preoccupazioni riguardo a un singolo punto di fallimento e a una potenziale censura.
DigiCash (1990)	DigiCash, fondata da David Chaum, mirava a creare una forma di moneta digitale con un'attenzione particolare alla privacy.	Il modello centralizzato ha contribuito al suo fallimento nel 1998.

B-Money (1996)	B-Money, proposto da Wei Dai, era una proposta teorica per un sistema di denaro elettronico anonimo e distribuito.	Non è mai stato implementato, rimanendo un'idea concettuale. Mancava un'implementazione pratica.
HashCash (1998)	HashCash, sviluppato da Adam Back, era un sistema proof-of-work progettato per limitare lo spam via e-mail e gli attacchi denial-of-service.	Non ha affrontato direttamente il problema della doppia spesa associata alle valute digitali.
Bit Gold (1998)	Bit Gold, proposto da Nick Szabo, descrive un sistema di valuta digitale decentralizzato con elementi di proof-of-work.	Mai implementato, è rimasto un concetto teorico.
e-Gold (2004)	e-Gold era una valuta digitale centralizzata sostenuta da oro fisico, che permetteva agli utenti di acquistare e trasferire unità di e-Gold.	Problemi legali hanno portato alla sua chiusura nel 2009, evidenziando le sfide associate alle valute digitali centralizzate.

Nonostante i numerosi tentativi fatti dai Cypherpunk nel corso di decenni per creare una moneta digitale libera dal controllo di un gruppo o di un governo, i loro progetti hanno dovuto affrontare sfide pratiche e non sono riusciti a concretizzarsi completamente nel mondo reale. I Cypherpunk hanno concluso che non era così facile costruire una forma digitale di denaro contante che fosse sicura, scalabile e che avesse il potenziale per essere adottata su larga scala.

Tuttavia, la storia subisce una svolta quando un individuo, imparando dalle lezioni dei Cypherpunk, eleva il concetto di moneta digitale decentralizzata a nuove vette. Nei capitoli che seguono esploreremo come il contributo di questa persona, basato su 40 anni di lavoro precedente, abbia portato alla creazione di un sistema funzionale.

Capitolo #6

Introduzione a Bitcoin

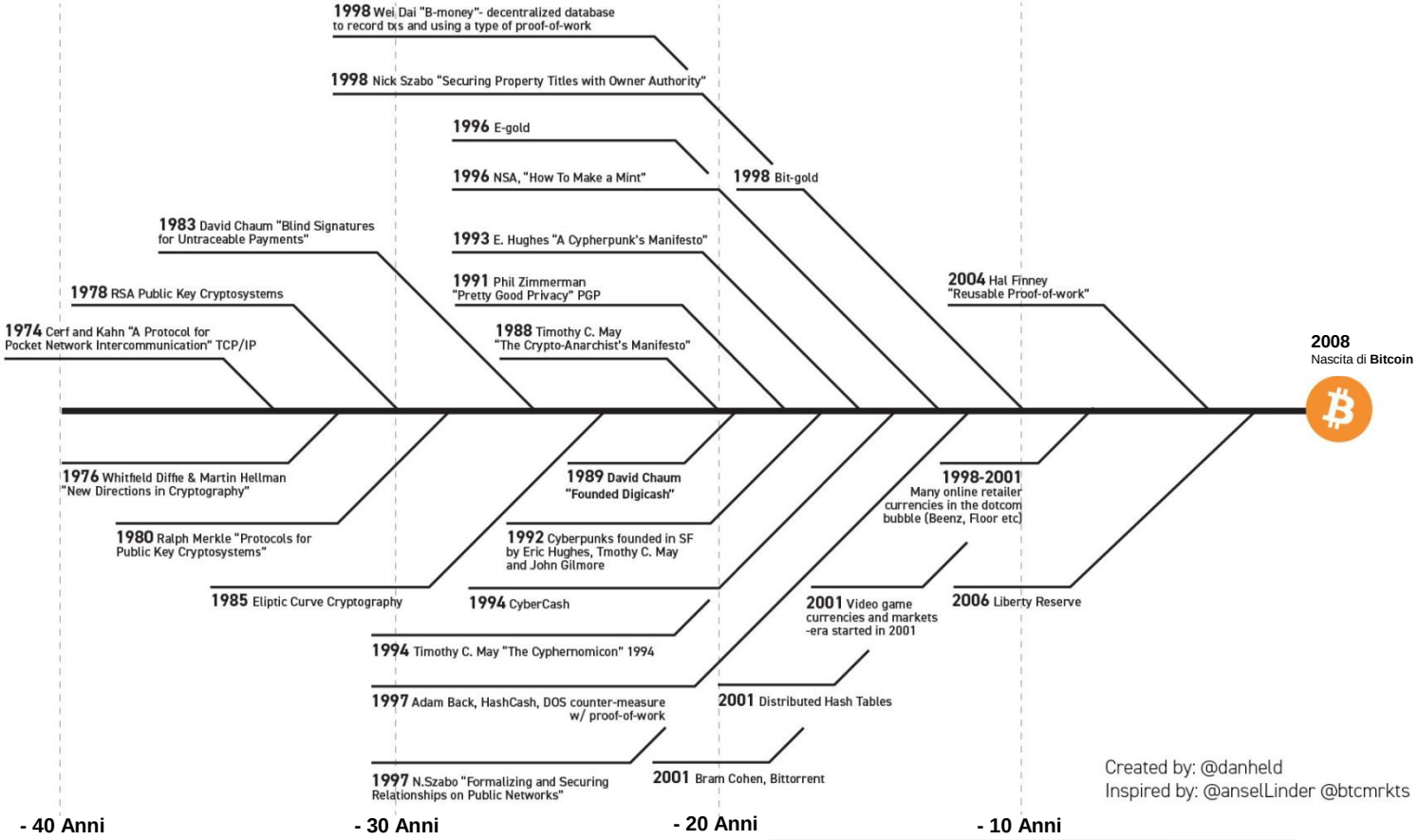
Libro di lavoro per studenti

Versione italiana| 2025

6.0 Satoshi Nakamoto e la creazione di Bitcoin

> Molte persone liquidano automaticamente le valute elettroniche come una causa persa, a causa di tutte le società che sono fallite a partire dagli anni Novanta. Spero sia evidente che è stata solo la natura centralizzata di quei sistemi a condannarli. Credo che questa sia la prima volta che proviamo un sistema decentralizzato non basato sulla fiducia.
>
> **Satoshi Nakamoto**

Preistoria di Bitcoin – **È il risultato di 40 anni di ricerca, sviluppo e necessità**



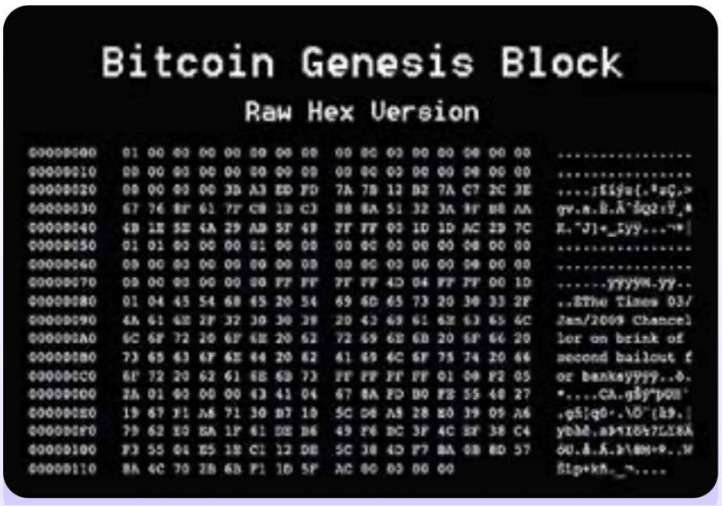
Come avete letto nel capitolo precedente, diversi cypherpunk hanno tentato di creare un sistema monetario alternativo. Questo capitolo continua la storia di uno di loro: una mente visionaria di nome "**Satoshi Nakamoto**". Questa persona anonima (uomo, donna o gruppo), molto prima di Bitcoin, faceva parte degli appassionati di crittografia, come gli scienziati informatici e gli hacker, impegnati in discussioni per trovare soluzioni pratiche per sostituire il sistema del denaro fiat.

Nell'ottobre 2008 Nakamoto ha presentato un innovativo whitepaper intitolato "**Bitcoin: A Peer-to-Peer Electronic Cash System**" su una mailing list di crittografia. Questo documento gettava le basi per un protocollo decentralizzato peer-to-peer, progettato per facilitare le transazioni online sicure senza la necessità di intermediari.

https://bitcoin.org/files/bitcoin-paper/bitcoin_it.pdf

La visione di Nakamoto era chiara: creare un sistema puramente peer-to-peer del contante elettronico, senza intermediari e libera dal controllo di governi e istituzioni finanziarie potenti.

Il 3 gennaio 2009 Nakamoto ha estratto il primo blocco di Bitcoin, noto come "blocco genesi". Questo segna il lancio ufficiale della rete Bitcoin, un nuovo sistema monetario costruito sulla fiducia e sulla sicurezza attraverso un libro mastro decentralizzato. Nei mesi e negli anni successivi, sempre più appassionati hanno iniziato ad aderire e a contribuire all'idea.



Nel 2011 dopo che la rete Bitcoin ha dimostrato di poter operare con successo senza la presenza del suo influente creatore, Nakamoto ha inviato un'e-mail a un collega sviluppatore di Bitcoin, annunciando di volersi ritirare dalla scena di Bitcoin e di affidare il suo futuro ad altre "buone mani" che condividessero la sua visione.

Sebbene l'identità di Nakamoto rimanga ancora oggi un mistero, l'obiettivo della creazione di Bitcoin non è mai stato tale. In sostanza, Nakamoto l'ha creato per togliere il potere a pochi e restituirlo a molti, creando un'alternativa sotto forma di un sistema monetario decentralizzato, aperto e trasparente, che separa il denaro dallo Stato. La creazione di Bitcoin è stata la risposta di Nakamoto alla crisi finanziaria del 2008, che ha danneggiato le persone normali in tutto il mondo e arricchito la classe elitaria, ancora una volta. Bitcoin è stata la risposta di Nakamoto alla corruzione e alla fragilità del sistema finanziario. Nakamoto ha gettato le basi per una nuova rivoluzione e se ne è allontanato invece di rivendicarne il merito.

Introduzione a Bitcoin

Negli anni successivi, il Bitcoin ha iniziato a crescere rapidamente ed è emerso come simbolo di speranza, potere e resilienza, sfidando il sistema del fiat e fornendo un mezzo sicuro e resistente alla censura per le transazioni finanziarie. Bitcoin è un protocollo open-source, il che significa che nessuno ha il potere di possederlo o controllarlo. Il suo design è pubblico e aperto alla partecipazione di chiunque.

Oggi, il sogno di Nakamoto di un sistema finanziario senza confini, trasparente e sicuro continua a vivere, dando vita alla rivoluzione globale della libertà a cui stiamo assistendo. Ogni giorno, le persone comuni scelgono di uscire dal sistema monetario per entrare nel mondo del Bitcoin. I cosiddetti "hub" del Bitcoin - le cosiddette economie circolari del Bitcoin - sono stati lanciati da appassionati della libertà in regioni di tutto il mondo. Anche interi Paesi alla ricerca di un percorso alternativo, come El Salvador, stanno iniziando ad adottare il Bitcoin a modo loro.

6.1 Come funziona Bitcoin?

6.1.1 Il meccanismo di consenso di Nakamoto

Bitcoin ha molte caratteristiche e la tana del coniglio è profonda, molto profonda. Fortunatamente, se si entra nel mondo Bitcoin per la prima volta, non è necessario capire perfettamente come funziona per iniziare a usarlo.

Lo stesso vale per l'uso di Internet: la maggior parte delle persone non sa come funziona il protocollo TCP/IP, eppure ogni giorno invia e-mail, messaggi e pubblica contenuti sui propri account di social media. Lo stesso vale per la guida di un'automobile: la maggior parte delle persone non sa esattamente come funziona un'automobile, eppure sa come si guida.

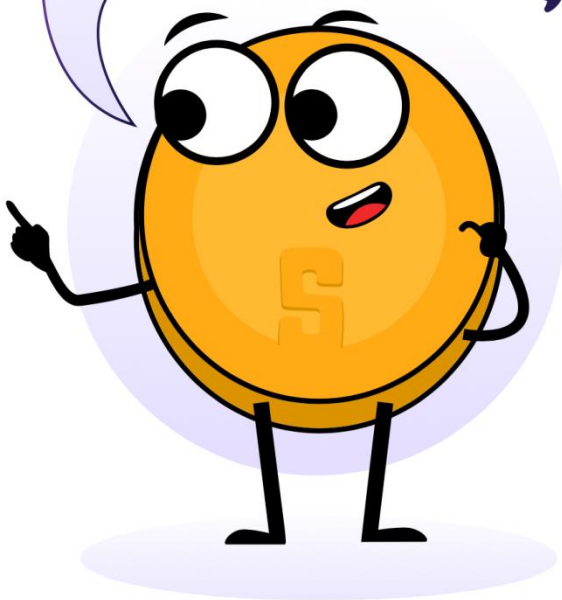
Tuttavia, il Bitcoin non è ancora ampiamente adottato. È ancora una tecnologia piuttosto nuova, come lo era Internet negli anni '90. Per questo motivo, può essere utile capire le basi di Bitcoin in modo semplice e meno tecnico.

L'idea chiave del funzionamento del Bitcoin può essere condensata in una frase: Bitcoin è un accordo tra persone online. Si può pensare che sia come giocare a un gioco da tavolo con gli amici. In un gioco come il Monopoli ci si accorda con gli altri giocatori su regole specifiche. Una delle regole del Monopoli prevede che vengano accettate solo speciali "banconote del Monopoli". Se James (uno dei giocatori) va contro le regole usando la carta igienica per comprare una casa invece delle banconote del Monopoli, gli altri giocatori direbbero a James che è un imbroglione e semplicemente smetterebbero di giocare con lui. In breve, per giocare, bisogna concordare una serie di regole con gli altri giocatori e non allontanarsi da queste regole, altrimenti si viene respinti.

Questo è essenzialmente il modo in cui funziona Bitcoin. Si tratta di una rete di persone che si accordano sullo stesso insieme di regole. Queste regole sono matematicamente vincolate, scritte in codice informatico e accettate direttamente da tutti coloro che eseguono il software Bitcoin. Le regole di Bitcoin si applicano a tutti i partecipanti allo stesso modo, il che significa che tutti o seguono le regole del gioco o non possono giocare perché la rete li rifiuta.

Ad esempio una delle regole di Bitcoin è: "**Non ci saranno mai più di 21 milioni di bitcoin**". Se qualcuno volesse creare un milione di bitcoin in più per sé, non gli servirebbe a nulla perché verrebbe automaticamente identificato e rifiutato da tutti gli altri. Questo è ciò che rende Bitcoin così robusto.

> Sapevate che dal 2009 ad oggi, Bitcoin ha resistito a decine di migliaia di tentativi di hacking, manomissione o alterazione?
> Bitcoin ha dimostrato che nessuno può fermarlo, controllarlo o manipolarlo.



Non importa chi siete o da dove venite: se entrate nel mondo Bitcoin, dovete giocare con le stesse regole di tutti gli altri.

Questo vale anche per tutte le persone e le entità che hanno un'enorme quantità di controllo e di influenza, nel mondo Bitcoin dove non c'è spazio per imbrogli o sabotaggi: tutti vengono trattati allo stesso modo e nessuno lo può cambiare.

6.1.2 I partecipanti al gioco

Per comprendere meglio la decentralizzazione di Bitcoin, dobbiamo approfondire i diversi ruoli all'interno della rete. In questo mondo diversi partecipanti svolgono ruoli distinti ma armoniosi, contribuendo al perfetto funzionamento della rete.

1. Minatori: Gli architetti della sicurezza

I minatori sono la spina dorsale di Bitcoin: si tratta di persone o gruppi di persone che lavorano dietro le quinte per mantenere e rendere sicura la rete attraverso un meccanismo chiamato **Proof-of-Work (PoW).**
Questi giocatori sono dotati di computer speciali che contengono una grande potenza di calcolo.
Mettono il loro hardware a disposizione della rete Bitcoin e competono tra loro per trovare numeri crittografici complessi, verificare le transazioni e aggiungere nuovi blocchi di informazioni sulle transazioni al registro decentralizzato di Bitcoin (la cosiddetta blockchain).
Il loro impegno garantisce l'immutabilità del libro mastro e protegge da attacchi malevoli.

La natura decentralizzata del mining consente a chiunque disponga di risorse informatiche sufficienti di partecipare. Grazie al loro duro lavoro, i minatori che risolvono il puzzle più velocemente vengono ricompensati sotto forma di bitcoin.

I minatori di Bitcoin sono distribuiti in tutto il mondo, salvaguardando la rete dalla centralizzazione e garantendo che la sicurezza di Bitcoin rimanga solida e distribuita.

2. Nodi: I guardiani della convalida

I nodi Bitcoin sono persone comuni che vivono in tutto il pianeta. Questi partecipanti costituiscono i guardiani della rete Bitcoin, eseguendo il software Bitcoin sui loro piccoli computer in cui mantengono una copia dell'intero libro mastro. I nodi convalidano le transazioni e assicurano che tutti i partecipanti aderiscano alle regole del consenso.

Distribuendo la responsabilità della convalida su una rete di nodi, Bitcoin rimane resistente agli attacchi e mantiene la sua natura priva di fiducia. I nodi svolgono un ruolo cruciale nel sostenere l'integrità del libro mastro, contribuendo all'etica di decentralizzazione di Bitcoin.

3. Utenti: Partecipanti responsabilizzati

Gli utenti - la linfa vitale della rete Bitcoin - sono individui che effettuano transazioni. Si può pensare agli utenti come a persone normali che vivono semplicemente la loro vita, ma che si sono anche potenziate integrando il Bitcoin. Ad esempio, alcuni utenti risparmiano i loro soldi in bitcoin, mentre altri, come i cittadini di El Salvador, li usano come denaro per comprare generi alimentari e ricevono bitcoin sotto forma di stipendio.

Il Bitcoin dà potere agli utenti eliminando la necessità di intermediari come banche e governi, consentendo transazioni dirette peer-to-peer. Questo significa anche che gli utenti hanno il pieno controllo sul proprio denaro, garantendo il controllo dei propri fondi e delle proprie transazioni.

4. Sviluppatori e progetti: Architetti dell'innovazione

Il sistema monetario del futuro non si costruisce da solo, né viene adottato a livello globale in modo eticamente corretto senza un sostegno. È qui che entrano in gioco gli sviluppatori e i progetti Bitcoin.

Gli sviluppatori mettono a disposizione le loro competenze tecniche per migliorare e innovare il protocollo Bitcoin. Questi individui contribuiscono al codice, propongono miglioramenti e risolvono le vulnerabilità, assicurando che la rete si evolva in risposta a tutti i tipi di sfide. La natura open-source di Bitcoin invita alla collaborazione, consentendo agli sviluppatori di tutto il mondo di contribuire alla sua crescita.

La bellezza di questo sviluppo decentralizzato impedisce a una singola entità di monopolizzare il controllo del protocollo. Ciò avviene attraverso un processo guidato dal consenso: gli sviluppatori propongono idee e cambiamenti e solo quelli con le idee migliori e allineate con la visione più ampia di un mondo migliore ricevono il sostegno della comunità, consentendo un'evoluzione trasparente e democratica del Bitcoin fino a quando non sarà pronto per 8 miliardi di persone.

I progetti Bitcoin coinvolgono gruppi diversi, dalle organizzazioni no profit e dalle società che perseguono una missione ai gruppi e agli individui che creano contenuti di valore. Queste persone lavorano insieme su un obiettivo specifico o su un focus all'interno della più grande missione Bitcoin verso la libertà collettiva.

I progetti Bitcoin svolgono un ruolo cruciale nel plasmare e promuovere l'adozione di Bitcoin, lavorando verso un futuro che dia priorità all'emancipazione e alla libertà della razza umana.

La Sinfonia

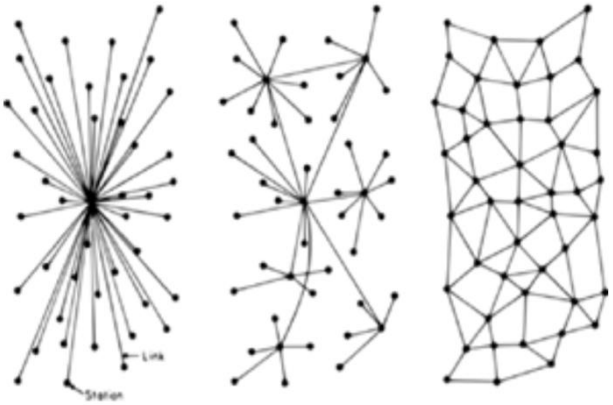
La decentralizzazione di Bitcoin può essere vista come un'orchestra musicale sinergica, un gioco di equilibri in cui tutti i musicisti differenti fanno insieme la musica più bella. Nella rete Bitcoin non c'è un capo, ma minatori, nodi, utenti, sviluppatori e progetti svolgono i loro ruoli in autonomia e collaborazione.

Il libro mastro decentralizzato, gestito dai nodi, garantisce la trasparenza, mentre il meccanismo proof-of-work fornisce sicurezza e scoraggia la centralizzazione del mining. Gli utenti sperimentano la sovranità finanziaria e l'empowerment, liberi dal controllo del sistema. Gli sviluppatori, guidati dal consenso, assicurano che il protocollo si adatti alle esigenze in evoluzione dell'umanità. I progetti Bitcoin, nei loro modi unici, contribuiscono alla più ampia missione di libertà collettiva.

Introduzione a Bitcoin

Come si può vedere, ogni partecipante svolge un ruolo vitale nel plasmare l'adozione di Bitcoin e nel potenziare l'umanità. Ogni partecipante a questa orchestra decentralizzata contribuisce alla resilienza e alla longevità del Bitcoin, creando un ecosistema privo di fiducia, senza confini e con potere alle singole persone.

In sintesi, la sinfonia della decentralizzazione in Bitcoin risuona come testimonianza della visione di **Satoshi Nakamoto** e dell'immensa passione di una comunità globale alla ricerca di libertà e alla riacquisizione del potere.



RETE-CENTRALIZZATA (A) | RETE-DECENTRALIZZATA (B) | RETE-DISTRIBUITA (C)

Esercitazione in classe - Creazione del consenso in una rete Peer-to-Peer

Obiettivo

Capire come si raggiunge il consenso in un gruppo e conoscere la crittografia. e il livello di consenso di Bitcoin.

I materiali

Messaggio con istruzioni criptate e non criptate per azioni ("attacca" o "non attaccare").

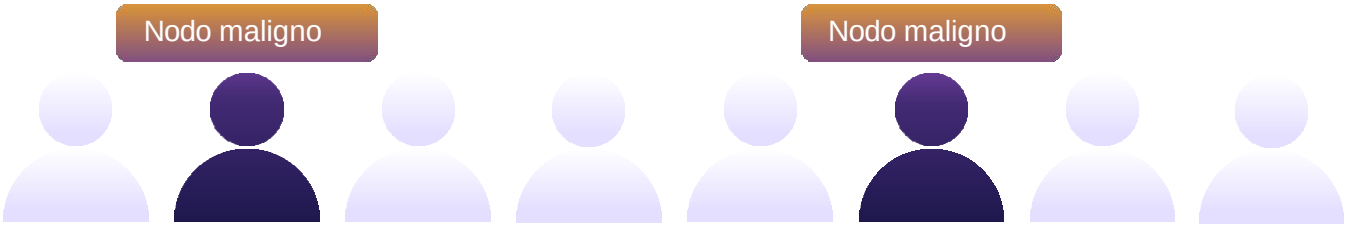
Preparazione dell'attività

L'insegnante selezionerà prima della lezione un gruppo di 3 o 4 studenti che saranno i nodi maligni dell'attività seguente, poi assegnerà a questi nodi maligni un rompicapo crittografico come compito a casa nella lezione precedente.

Esercizio a tappe :

1. L'insegnante selezionerà un "originatore" che riceverà un messaggio su un foglio di carta con scritto "ATTACCO" e una serie di numeri che dice "4-16-14-21-1-21-21-1-3-11-" a uno studente del gruppo.

2. Gli studenti formeranno un cerchio nello spazio designato, assicurandosi che gli studenti selezionati che saranno nodi maligni siano separati per migliorare l'effcacia della lezione.



3. Una volta che il gruppo ha formato un cerchio, l'ideatore passerà il biglietto all'individuo alla destra del cerchio.

4. Dopo che tutti hanno letto il messaggio, l'ideatore darà il segnale al gruppo dicendo "ora" e il gruppo reagirà al messaggio simultaneamente. Se il messaggio recita "ATTACCO" tutti i partecipanti faranno un passo avanti.

5. Dopo la reazione iniziale alcuni studenti (quelli che hanno ricevuto il messaggio criptato e lo hanno interpretato correttamente) rimarranno fermi, mentre gli altri seguiranno l'istruzione originale, rivelando una mancanza di consenso.

Conclusione:

Discutere il motivo per cui non è stato raggiunto il consenso, introducendo il concetto di problema dei generali bizantini, il modo in cui si collega alla necessità di un obiettivo comune e, successivamente, discutendo di come Bitcoin fornisca una soluzione a questo problema.

6.2 Bitcoin come moneta digitale solida

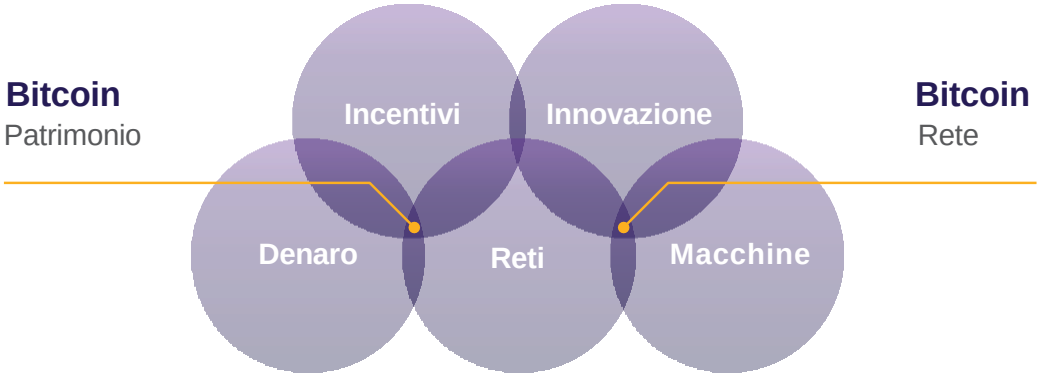
62.1 Introduzione

Attività:

Guarda il video di 1,5 min, **"Cosa è Bitcoin?"**.

In parole povere, il Bitcoin è denaro. Il Bitcoin non è un investimento, ma piuttosto un modo sicuro e vantaggioso di risparmiare il proprio denaro duramente guadagnato.

Avere bitcoin non vi renderà ricchi perché non vi darà un ritorno di altri bitcoin. Il suo valore, misurato rispetto a una valuta nazionale, sale, ma solo a causa della sua crescente adozione e della svalutazione delle valute nazionali.



Bitcoin è una nuova forma di denaro; è "l'Internet del denaro", il che significa che chiunque può aderire e iniziare a scambiare valore con altri utenti. Anche le comunità più isolate e povere del mondo hanno finalmente accesso a un sistema monetario. Proprio come tutti coloro che hanno un telefono e una connessione a Internet possono usare un motore di ricerca, Bitcoin rende possibile a tutti coloro che hanno un telefono e una connessione a Internet di accedere a un nuovo sistema monetario globale.

Pagamenti più rapidi ed economici

Inviate denaro in tutto il mondo in pochi minuti con commissioni estremamente basse.

Inclusione finanziaria

2,5 miliardi di persone che non possono avere un conto bancario, possono accedere al denaro tramite telefono o computer.

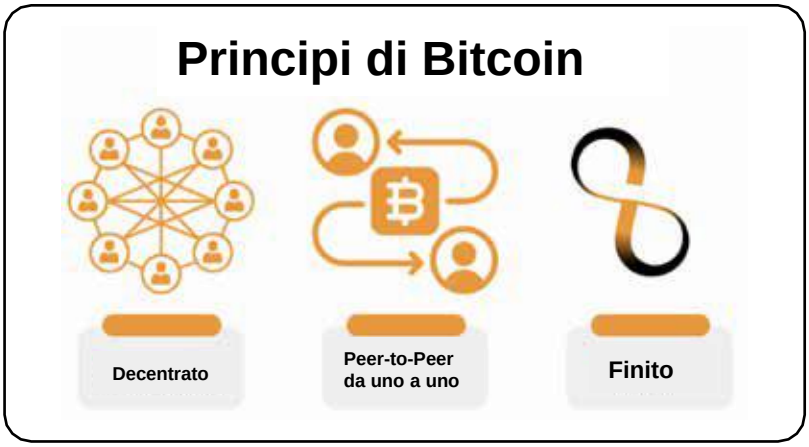
Maggiore privacy

Le transazioni in Bitcoin sono pubbliche ma la vostra identità non lo è.

Il Bitcoin è completamente digitale e privo di confini. Non importa dove ci si trovi, perché vive su computer e smartphone di tutto il mondo. Molti utenti in tutto il mondo utilizzano il software Bitcoin e una copia del suo libro mastro.

Questo software e la registrazione di tutte le transazioni hanno una probabilità molto bassa di scomparire, poiché ne esistono innumerevoli copie. Per spegnerlo, bisognerebbe spegnere l'intera rete Internet, per sempre, il che è estremamente improbabile che accada.

Infine, il Bitcoin è scarso, il che significa che la quantità di token bitcoin che possono esistere è assolutamente limitata. Nessuno può contraffare il Bitcoin, nemmeno i governi e le istituzioni finanziarie più potenti.



6.2.2 Le caratteristiche di Bitcoin

L'evoluzione del denaro sano

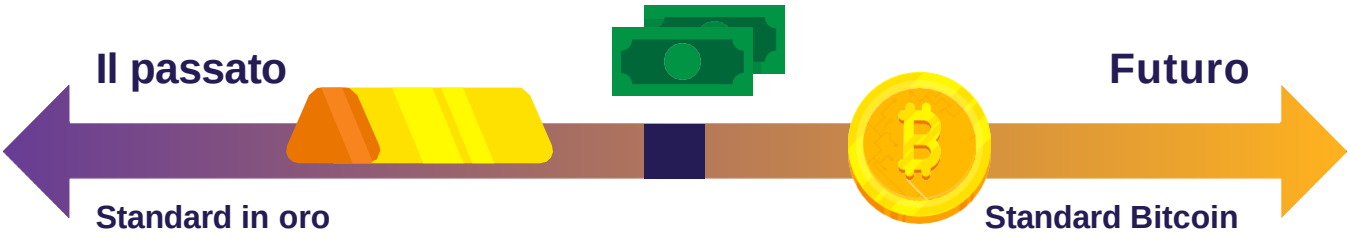
Come si è appreso nel Capitolo 2, il ciclo di vita del denaro sano passa attraverso tre fasi per ricevere l'accettazione generale da parte della società: da riserva di valore a mezzo di scambio e, infine, unità di conto.

Il primo stadio del denaro, una riserva di valore, si ha quando una valuta inizia a guadagnare fiducia come bene stabile (o che si apprezza) nel tempo. Le persone che lo riconoscono presto cercano di proteggere la loro ricchezza immagazzinandola in questa forma di denaro, soprattutto in un periodo di incertezze geopolitiche e macroeconomiche.

Alcuni gruppi come i media, definiscono il Bitcoin una forma di "oro digitale". Questo perché il Bitcoin si è affermato con forza come riserva di valore nell'ultimo decennio. Ogni giorno sempre più persone iniziano a considerare Bitcoin come una copertura contro l'inflazione, come l'oro ha fatto storicamente.

La fase successiva è quella in cui si consolida la fiducia nella stabilità di una valuta. A questo punto la moneta si trasforma in un mezzo di scambio che facilita le transazioni nella vita quotidiana delle persone. In questa fase la moneta inizia a essere ampiamente accettata per lo scambio di beni e servizi.

Bitcoin sta progressivamente diventando un mezzo di scambio, con la crescente accettazione da parte dei commercianti e lo sviluppo del protocollo, le transazioni in Bitcoin stanno diventando sempre più efficienti e comuni nel commercio quotidiano. Ne è un esempio El Salvador, dove Bitcoin è officialmente riconosciuto come moneta legale. Ogni giorno sempre più cittadini e imprese utilizzano Bitcoin come mezzo di scambio.



Nella fase finale una valuta raggiunge lo status di unità di conto, fungendo da misura comune per la determinazione del prezzo di beni e servizi. È questa la fase in cui diventa il metro standard rispetto al quale vengono misurati tutti gli altri valori.

Il percorso per diventare un'unità di conto è un processo più esteso (a lungo termine). Attualmente il mondo misura i beni e i servizi solo in valute nazionali e per questo motivo Bitcoin deve essere adottato e integrato in vari sistemi finanziari. Tuttavia, le fondamenta sono già state gettate, poiché le aziende e gli individui iniziano a considerare e a denominare i valori in Bitcoin.

Come si vede, Bitcoin è a buon punto in questo ciclo evolutivo del denaro sano. Quando Bitcoin sarà pienamente integrato nel sistema finanziario globale, potrebbe diventare un'unità di conto standard, rimodellando l'intero sistema monetario mondiale.

Proprietà del denaro

Come si è appreso nel Capitolo 2, nel corso del tempo l'umanità ha capito che il vero denaro sano deve possedere alcune proprietà per essere efficace. Queste proprietà sono la durabilità, la divisibilità, la portabilità, l'accettabilità, la scarsità e la fungibilità.

Vediamo se Bitcoin supera il test.

Durabilità: Bitcoin è puramente digitale e quindi completamente durevole.

Divisibilità: Per fare un paragone, il dollaro USA può essere diviso al centesimo (.01). Bitcoin può essere diviso nel cosiddetto **satoshi** o **sat** (.00000001). E dato il carattere digitale di Bitcoin, in futuro potrà essere ancora più diviso se l'umanità ne avrà bisogno. Attualmente Bitcoin è il bene monetario più divisibile al mondo.

Portabilità: Nell'aprile 2020 sono stati trasferiti 1,1 miliardi di dollari in pochi minuti, al costo di soli 68 centesimi. Nessun altro modo di pagare può spostare così tanto denaro a un costo così basso, così rapidamente e da solo. È questo che rende Bitcoin la forma di denaro più facilmente trasferibile al mondo.

Accettabilità: Bitcoin è ancora nelle prime fasi del suo sviluppo come mezzo di scambio e rispetto alle altre valute l'accettabilità è attualmente bassa.

Scarsità: Esisteranno solo 21 milioni di bitcoin. E per codice è impossibile che questa quantità aumenti, il che significa che il Bitcoin non solo è scarso, ma è anche il bene monetario più scarso al mondo.

Fungibilità: Ogni unità di bitcoin è uguale a qualsiasi altra unità e può essere scambiata e transata attraverso il protocollo Bitcoin su una base di similitudine, il che la rende una valuta fungibile.

Bitcoin vs oro vs dollaro USA

Proprietà del denaro	Oro	Fiat	Bitcoin
Durabilità	Alto	Moderato	Alto
Portabilità	Moderato	Alto	Alto
Divisibilità	Moderato	Moderato	Alto
Fungibilità	Alto	Alto	Alto
Scarsità	Moderato	Basso	Alto
Verificabile	Moderato	Moderato	Alto
Storia consolidata	Alto	Moderato	Basso
Resistente alla censura	Moderato	Moderato	Alto
Intelligente/programmabile	Basso	Moderato	Alto

"Bitcoin vs Oro vs Dollaro USA" Bitcoin Magazine, https://bitcoinmagazine.com

Bitcoin è un tipo di denaro intelligente che è programmabile, non può essere sottratto e ha tutte le qualità che lo rendono ottimo per il risparmio e facile per gli esercenti che desiderano transazioni rapide.

Essendo un libro mastro digitale trasparente, Bitcoin può essere super efficiente nel catturare le frodi e nell'individuare i rischi nei suoi servizi. Ha gli aspetti positivi dell'oro, come il fatto che ne esiste solo una quantità limitata, ma ha anche i vantaggi delle valute, perché si può dividere e portare in giro facilmente. Inoltre, introduce nuove funzionalità che funzionano bene nel nostro mondo digitale.

Cosa ne pensate? Bitcoin non è ancora ampiamente riconosciuto e adottato, ma è una moneta sana?

Attività: Discussione in classe - Bitcoin è una moneta solida?

Ora che abbiamo discusso Bitcoin in modo più approfondito, esaminiamo di nuovo la nostra tabella di confronto del denaro del Capitolo 2 e vediamo come Bitcoin si confronta con altre forme di denaro:

Caratteristiche del buon denaro	Mucche	Sigarette	Diamanti	Euro	Bitcoin
Durevole					
Portatile					
Uniforme					
Accettabile					
Scarso					
Divisibile					
Totale					

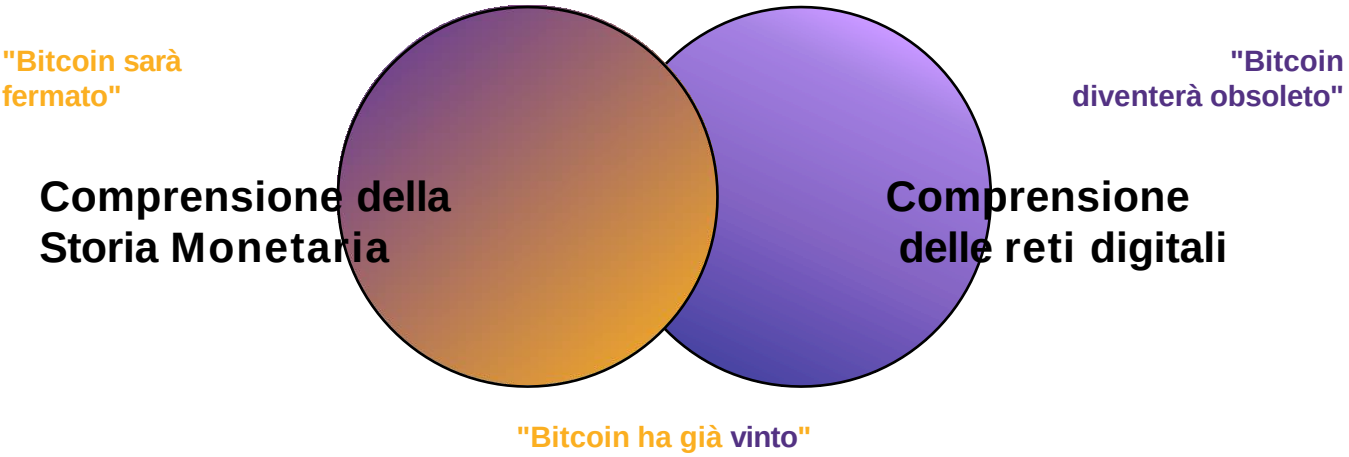
6.2.3 Abbracciare la responsabilità personale

> Il risultato è un sistema distribuito senza un singolo punto di fallimento. Gli utenti detengono le chiavi crittografiche del proprio denaro e effettuano transazioni direttamente tra di loro con l'aiuto della rete P2P, per controllare che non ci siano doppi pagamenti.
>
> **Satoshi Nakamoto**

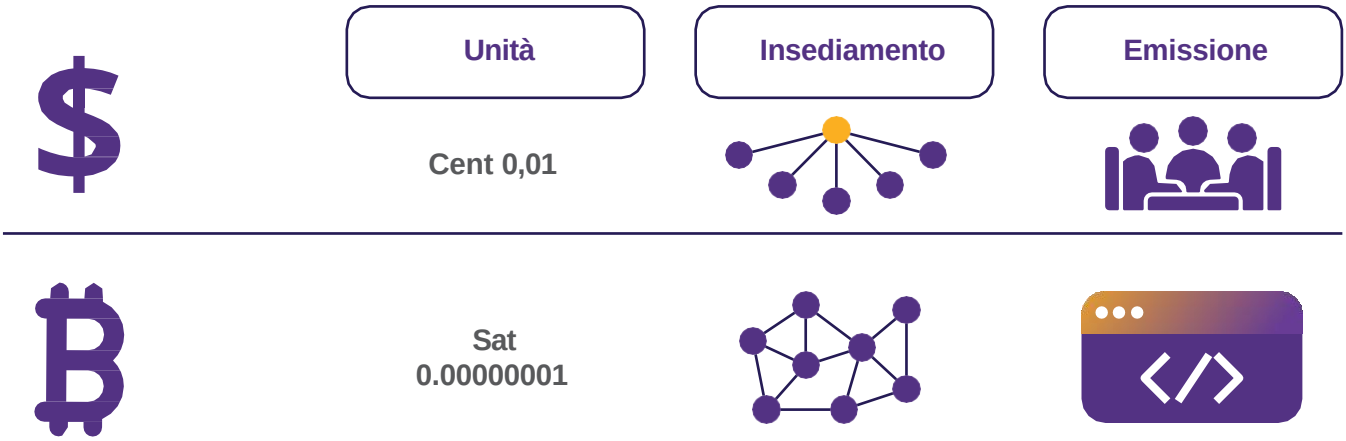
Introduzione a Bitcoin

Nel mondo virtuale le persone si affidano ai governi, alle banche e ai fornitori di servizi di pagamento. I responsabili di queste istituzioni (finanziarie) stabiliscono le regole della rete e i partecipanti, per lo più i comuni cittadini, devono rispettarle. Non importa dove si vive: ci sono sempre una serie di procedure standard che indicano cosa fare e come farlo. Nel tempo, questo ha portato a un ciclo di difficoltà, in particolare per le famiglie che lottano con le crescenti sfide della vita quotidiana.

Grazie a questo sistema, le persone sono abituate ad affidare ad altri la responsabilità delle proprie finanze. Per esempio, la maggior parte delle persone si affida a qualcun altro per essere aiutata, soprattutto quando qualcosa va storto (come perdere l'accesso al proprio conto corrente).



Come sapete, il sistema monetario di Bitcoin è molto diverso. Bitcoin opera in modo particolare e i governanti sono stati sostituiti da un sistema autonomo di regole. Non c'è un dittatore o un leader, il che significa anche che nessuno vi imporrà cosa dovete fare. Se volete ottenere la libertà e l'autonomia di Bitcoin, dovrete imparare come funziona e integrare la tecnologia in modo personale.



Con Bitcoin avete il pieno controllo dei vostri fondi, ma questo controllo aggiuntivo comporta una maggiore responsabilità. Ad esempio, se perdete l'accesso ai vostri bitcoin perdendo le chiavi del vostro portafoglio digitale, avete perso i vostri risparmi - in modo permanente. Non c'è una linea telefonica di assistenza clienti da chiamare o qualcuno a cui rivolgersi: quando c'è un problema, dovete occuparvene voi stessi.

Fortunatamente, questo non accadrà a chi decide di assumersi la piena responsabilità della propria vita. Utilizzare Bitcoin non è intrinsecamente complicato, è solo un concetto nuovo. Il disagio nasce dal fatto che non è familiare, ma se si è disposti ad imparare a usare Bitcoin e ad assumersi la piena responsabilità di salvaguardare il proprio patrimonio, Bitcoin diventa uno strumento di potere, poichè se ne ha personalmente il controllo e nessuno può limitare o impadronirsi della nostra ricchezza.

In sintesi la chiave sta nell'azione, nella comprensione del funzionamento di Bitcoin e nella sua implementazione in base alle proprie esigenze e alla propria filosofia di vita. In seguito, inizieremo a usare i bitcoin impostando un portafoglio Bitcoin, inviando e ricevendo le nostre prime transazioni e rivedendo le migliori pratiche di sicurezza.

Capitolo #7

Come utilizzare Bitcoin

Libro di lavoro per studenti

Versione italiana| 2025

Come utilizzare Bitcoin

7.0 Introduzione

> Perché qualcuno dovrebbe fidarsi del denaro dei nerd rispetto a quello delle banche centrali? I nerd hanno portato internet. Le banche hanno portato la grande depressione.
>
> **Andreas M. Antonopoulos**

Ora che abbiamo capito meglio cos'è Bitcoin e il suo scopo, è il momento di imparare a usarlo praticamente. In questo capitolo vi guideremo passo dopo passo nel processo di acquisizione di bitcoin, esploreremo i vari tipi di portafogli disponibili, vi aiuteremo a configurare il vostro portafoglio Bitcoin e ci eserciteremo ad inviare e seguire una transazione bitcoin sulla rete. È ora di passare all'azione!

7.1 Acquisizione e scambio di Bitcoin

Ci sono molti modi per acquisire bitcoin.
Ad esempio, è possibile:

- Essere pagati in bitcoin in cambio del proprio lavoro e pagare i prodotti e i servizi di altre persone con bitcoin (per saperne di più, vedere il capitolo 8).
- Estrarre bitcoin (maggiori informazioni nel Capitolo 9)
- Cambiare la vostra valuta fiat in bitcoin o cambiate i vostri bitcoin in valuta fiat di persona.
- Cambiare la vostra valuta fiat in bitcoin o cambiate i vostri bitcoin in valuta fiat online.

Di seguito analizzeremo il cambio di valuta in bitcoin e viceversa, sia con transazioni di persona che con metodi online, in quanto sono le opzioni più comuni.

7.1.1 Peer-to-Peer: Di persona

Le transazioni peer-to-peer (P2P) per l'acquisto e la vendita di bitcoin comportano lo scambio diretto della propria valuta (o di qualsiasi altro bene o servizio) in bitcoin con un'altra persona, eliminando la necessità di coinvolgere una banca o altri soggetti nella transazione.

Entrambe le parti stabiliscono di comune accordo l'importo e il tasso di cambio. L'acquirente fornisce il contante, il venditore trasferisce i bitcoin e la transazione si conclude. Sebbene sia più facile effettuare scambi P2P fisicamente, incontrando direttamente l'altra persona nel mondo reale, grazie ad Internet è possibile farlo praticamente ovunque. Inoltre, lo scambio di bitcoin in valuta locale segue un processo simile ma inverso.

7.1.2 Peer-to-Peer: Online

Le piattaforme P2P, sono il sistema dove acquirenti e venditori di Bitcoin si incontrano nel cyber-spazio per effettuare transazioni senza intermediari, direttamente su Internet.

Grazie a queste piattaforme, non dovete affidare a nessuno le vostre informazioni o il vostro denaro; potete incontrare altri colleghi e commerciare direttamente con loro.

Sulla maggior parte delle piattaforme P2P i peer devono depositare una parte dei fondi per garantire che rispettino la loro parte dell'accordo. Il deposito a garanzia significa mettere il denaro in un luogo sicuro che la piattaforma controlla finché entrambe le parti non rispettano le promesse. È come un amico fidato che custodisce i vostri fondi fino a quando tutti non mantengono la parola data.

7.1.3 Scambi centralizzati

L'utilizzo di exchange centralizzati può essere il modo più semplice per acquistare e vendere bitcoin, ma comporta anche significativi scambi commerciali. Gli exchange centralizzati sono società che consentono ai clienti di acquistare e vendere bitcoin direttamente tramite loro. Tuttavia, questa comodità ha un costo.

CENTRALIZZATO

Le borse centralizzate e i loro scambi commerciali

È importante notare che quando si acquistano bitcoin tramite un exchange centralizzato, spesso viene richiesto di fornire informazioni personali e di verificare la propria identità. Questo crea un rischio di furto di identità ed espone le informazioni personali a potenziali minacce. Inoltre, gli exchange centralizzati detengono i bitcoin per voi, il che significa che non avete il controllo del vostro denaro finché non lo ritirate.

A queste preoccupazioni si aggiunge il fatto che le borse centralizzate possono appropriarsi indebitamente dei fondi degli utenti o prestare più bitcoin di quanti ne abbiano in riserva fino al collasso. Sì, proprio come le banche !
Tuttavia, nel mondo dei Bitcoin, non c'è una banca centrale che possa salvare le banche fraudolente stampando più moneta, perché non si possono stampare più bitcoin !

7.2 Introduzione ai portafogli Bitcoin

A differenza del denaro fisico, i bitcoin non sono presenti in un portafoglio Bitcoin. Vivono invece nel libro mastro distribuito che la rete Bitcoin verifica e protegge costantemente. Come si possono possedere i bitcoin ?

Si è proprietari dei propri bitcoin solo quando si possiedono le chiavi private che consentono di firmare le transazioni e di trasferire la proprietà dei bitcoin a qualcun altro. Questo è l'atto di inviare bitcoin.

Tenendo presente questo aspetto, diamo un'occhiata a due concetti che descriviamo quando utilizzando il termine **"portafoglio":**

- Una chiave privata principale (come una password) da cui è possibile generare chiavi pubbliche da condividere con altri per ricevere e inviare bitcoin.
- L'interfaccia mobile o desktop da cui è possibile interagire con la rete Bitcoin per recuperare il proprio saldo di bitcoin, inviare e ricevere transazioni e trasmetterle alla rete. Nella prossima sezione verranno descritti i diversi tipi di portafogli e i loro vantaggi.

7.2.1 Portafogli autocustoditi (non custodial) e portafogli custoditi (custodial)

Prima di descrivere nel dettaglio i diversi tipi di portafogli Bitcoin e le loro caratteristiche, facciamo un'importante distinzione tra portafogli autocustoditi e portafogli custoditi, illustrati nella tabella seguente. Si possono vedere i vantaggi e i rischi dell'utilizzo di ciascun tipo di portafoglio e chi controlla i bitcoin in ciascun caso. Autocustodia significa che l'utente detiene le chiavi private e quindi è il vero possessore dei suoi bitcoin, mentre il secondo tipo, un terzo, detiene i suoi bitcoin.

Tipo di porta foglio	Chi controlla il mio bitcoin?	Benefici	I rischi
Portafogli auto custoditi (non custodial)	**L'utente**	Controllo completo su fondi e transazioni, nessun processo di approvazione o congelamento del conto, nessun controllo aziendale o governativo, protezione contro le truffe arbitrarie, come tenere il denaro a casa.	Nessuna possibilità di recupero se la frase di recupero viene persa, meno supporto al cliente, la responsabilità ricade interamente sull'utente.
Portafogli di custodia (custodial)	**Il fornitore di terze parti**	Facile recupero in caso di perdita dell'accesso, più facile assistenza ai clienti	I fondi sono sempre connessi a Internet e sono quindi più vulnerabili a hacking e violazioni. I depositari controllano e possono anche bloccare i conti.

In un portafoglio auto-custodito (chiamato anche portafoglio non-custodial), siete gli unici a possedere le chiavi del portafoglio e avete il pieno controllo su ciò che entra ed esce. In un portafoglio di custodito (custodial), invece, qualcun altro detiene le chiavi private e può accedere e gestire il contenuto del portafoglio per conto dell'utente.
Il portafoglio non custodito (non custodial) ha i seguenti vantaggi:

- La possibilità di essere la propria banca. Le transazioni non sono soggette al controllo o all'autorità di alcun governo o società, ma significa anche che vi assumete la piena responsabilità di mantenere al sicuro i vostri bitcoin.
- Garantisce che terze parti non possano trasferire i vostri bitcoin senza il vostro consenso.
- Garantisce la tranquillità nei momenti di incertezza, sapendo che i vostri bitcoin sono sempre al sicuro, e nessuno puó limitarvi nell'utilizzo.

È importante scegliere il tipo di portafoglio giusto per le esigenze di ciascuno. A volte è difficile distinguere se si sta installando un portafoglio auto-custodia o un portafoglio custodia.
Questa tabella mostra le differenze nel processo di installazione.

Tipo di porta foglio	Passo 1: scegliere un porta foglio	Passo 2: installare il porta foglio	Passo 3: creare un nuovo porta foglio	Fase 4: Assicurare la frase seme	Fase 5: iniziare a utilizzare il portafoglio
Portafogli auto custoditi	Scegliere un fornitore di portafogli per l'autotutela	Seguire le istruzioni del fornitore del portafoglio	Generare la **frase di recupero** e almeno una **chiave privata.**	Conservare la **frase di recupero** in un luogo sicuro	Iniziare a usare il portafoglio per ricevere e inviare **bitcoin**
Portafogli custoditi	Scegliere un fornitore di portafogli di custodia	Seguire le istruzioni del fornitore del portafoglio	Creare un account con il fornitore del portafoglio	Non possible (il fornitore del portafoglio detiene le **chiavi private**)	Iniziare a usare il portafoglio per ricevere e inviare **bitcoin**

"**Not your keys, not your coins**" è un detto popolare tra i possessori di bitcoin. Si riferisce all'idea che se non si ha il controllo diretto delle chiavi private associate al proprio portafoglio Bitcoin, non si ha la vera proprietà delle monete.

Chiunque acceda alle vostre chiavi private diventerà proprietario dei vostri bitcoin. Per questo motivo è estremamente importante proteggerle e tenerle lontane da occhi indiscreti! Nel corso del libro vedremo alcuni modi per farlo.

Di seguito parleremo solo di portafogli autocustoditi, in cui l'utente possiede le proprie chiavi e ha il controllo completo dei propri bitcoin.

Non preoccupatevi se vi sembra complicato o se non capite tutto: si tratta di un viaggio e capirete di più man mano che inizierete a usare Bitcoin!

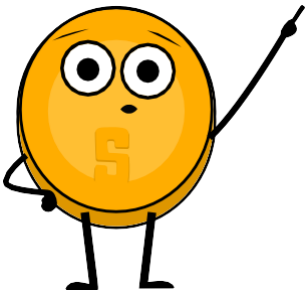
7.2.2 Diversi tipi di portafogli Bitcoin

A seconda del luogo in cui viene creata e conservata la chiave privata, comunemente si usano nomi diversi per descrivere i portafogli Bitcoin. Se le chiavi sono memorizzate sul vostro smartphone, lo chiamiamo "portafoglio mobile". Se sono memorizzate in modo sicuro su un dispositivo dedicato, lo chiamiamo "portafoglio hardware". Se le chiavi sono memorizzate solo su carta, si parla di "portafoglio cartaceo" (paper-wallet).

I diversi nomi che attribuiamo ai portafogli Bitcoin a seconda della loro struttura:

Tipo di portafoglio	Descrizione	Vantaggi	Svantaggi	Tipologia di utente
online	Un portafoglio a cui si accede tramite un browser web.	Accessibile da qualsiasi dispositivo con connessione a Internet. Facile da usare.	Meno sicuro. Può essere violato o compromesso.	Chi ha bisogno di accedere frequentemente al proprio portafoglio e non ha molti fondi da conservare.
mobile	Un portafoglio installato su un dispositivo mobile.	Conveniente. È possibile accedervi da qualsiasi luogo.	Può essere perso se il dispositivo viene smarrito, rubato o violato.	Chi ha bisogno di effettuare transazioni in movimento e non ha molti fondi da conservare.
Per PC	Un portafoglio installato su un computer desktop.	Più sicuro dei portafogli online. Può essere utilizzato offline.	Può essere violato se il computer è infettato da malware.	Chi vuole conservare una grande quantità di **bitcoin** e si trova a suo agio nell'usare un computer desktop.
Hardware	Un dispositivo fisico che memorizza i **bitcoin** offline.	Molto sicuro. Può essere utilizzato anche in linea.	I fondi potrebbero essere irrecuperabili in caso di smarrimento o furto del dispositivo.	Chi vuole conservare una grande quantità di **bitcoin** ed è disposto a pagare per la maggiore sicurezza di un portafoglio hardware.
di carta Paper-wallet	Una registrazione fisica delle chiavi private e pubbliche di un portafoglio Bitcoin.	Molto sicuro. Può essere utilizzato anche in linea.	Può essere smarrito o rubato se viene smarrito o rubato il documento fisico.	Chi vuole conservare una grande quantità di **bitcoin** ed è disposto a prendere ulteriori precauzioni per garantirne la sicurezza.

Poiché le chiavi possono essere spostate da un dispositivo all'altro, lo "stato" del portafoglio Bitcoin non è definitivo. Ad esempio, se genero le chiavi del mio portafoglio Bitcoin su un computer e successivamente le carico sul mio telefono, il "portafoglio desktop" diventa un "portafoglio mobile".



Quando si tratta di conservare i bitcoin, non si tratta solo di sapere chi ne ha il controllo: ci sono molti altri rischi da considerare. Ecco perché è importante trovare una soluzione di archiviazione che sia sicura e conveniente.

Analizzando le caratteristiche commerciali dei vari tipi di portafogli, si apprenderà che non esiste un portafoglio ideale in grado di soddisfare tutte le esigenze.

Quando si sceglie un portafoglio Bitcoin, ci sono diversi aspetti da considerare:

- **Sicurezza:** assicuratevi che il portafoglio disponga di solide misure di sicurezza, come l'autenticazione a due fattori e politiche di password sicure.
- **Privacy:** considerate se il portafoglio vi permette di rimanere anonimi o se richiede informazioni personali per la creazione di un account.
- **Facilità d'uso:** scegliete un portafoglio facile da usare e da navigare, soprattutto se siete alle prime armi con i Bitcoin.
- **Compatibilità:** assicuratevi che il portafoglio sia compatibile con il proprio dispositivo e sistema operativo.
- **Commissioni:** confrontate le commissioni applicate dai diversi portafogli per assicurarvi di ottenere la migliore offerta.
- **Reputazione:** ricercate la reputazione del portafoglio e del suo team per assicurarvi che sia affidabile.
- **Controllo:** alcuni portafogli consentono un maggiore controllo sulle chiavi private, il che può rappresentare un vantaggio per la sicurezza.

Bisogna considerare se si vuole un portafoglio che vi dia il pieno controllo ma piú complicato da utilizzare oppure uno che sia più facile da usare ma che permetta di avere meno controllo.

7.2.3 Sorgenti aperti (open-source) vs. sorgenti chiusi (closed-source)

Un altro fattore importante da tenere presente quando si sceglie un portafoglio Bitcoin è sapere se l'applicazione o il software sono open-source.

Il codice open-source è molto importante perché permette alla comunità di rivedere il codice e di continuare a sviluppare il progetto se il team di lavoro dovesse smettere di lavorarci.

Proprio come il codice di Bitcoin è completamente aperto a tutti per essere rivisto, utilizzato e modificato, così dovrebbe essere il codice del portafoglio che utilizzate per memorizzare i vostri bitcoin.

Attività: Discussione in classe e valutazione di Portafogli Bitcoin su bitcoin.org

Andate al seguente sito web: **https://bitcoin.org/it/scegli-il-tuo-portafoglio** e utilizzate le vostre nuove conoscenze sui portafogli Bitcoin per scegliere il migliore in base ai criteri che abbiamo discusso oggi.

7.3 Creazione di un portafoglio Bitcoin mobile

Ora che abbiamo una migliore comprensione dei portafogli Bitcoin e delle loro differenze, vediamo come utilizzarne uno nella pratica. Per questo esempio, creeremo un portafoglio mobile direttamente sul nostro smartphone.

Attività: Creazione/recupero di un portafoglio Bitcoin

Se gli studenti non hanno un cellulare, l'insegnante ne fornirà uno in prestito a ogni studente. Ci sono due opzioni per questa attività.

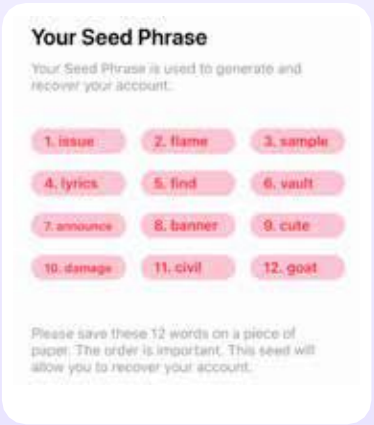
Esercizio in classe: Opzione 1 - Scaricare un nuovo portafoglio.

Come creare e utilizzare un portafoglio Bitcoin:

1. Cercare l'applicazione nell'App Store (iOS) o nel Google Play Store (Android).
2. Aprite la app e inserite le 12 o 24 parole della frase di recupero (anche chiamata frase seme). **Assicuratevi di annotarla e di conservarla in un luogo sicuro!** Questa frase di recupero vi permette di recuperare l'accesso completo ai vostri fondi, se necessario.

Ricordate che se perdete o dimenticate questa sequenza di parole, non potrete accedere ai vostri bitcoin e perderete per sempre l'accesso al vostro portafoglio.

3. È quindi necessario accertarsi di aver effettivamente salvato la frase di recupero o seme. A tal fine, bisogna inserire nello stesso ordine le parole della frase iniziale.



4. Come ulteriore misura di sicurezza alcuni portafogli consentono di scegliere una password sicura. La chiave privata e il primo indirizzo Bitcoin vengono creati automaticamente dal portafoglio.

Considerate il vostro indirizzo pubblico come il vostro indirizzo e-mail: volete condividerlo con altri in modo che possano inviarvi bitcoin o, nel caso di un indirizzo e-mail, per farvi inviare un messaggio e-mail.

Considerate il vostro indirizzo privato come la password della vostra e-mail: non vorreste condividerlo con nessuno perché darebbe accesso alla vostra e-mail.

5. Utilizzate il vostro indirizzo "receive" per ricevere bitcoin. Con un portafoglio autocustodito non è sempre possibile acquistare bitcoin direttamente con fiat, quindi potrebbe essere necessario acquistarli e trasferirli da un exchange.

Esercitazione in classe: Opzione 2 - Ripristino del portafoglio (a tempo limitato).

Scaricate un portafoglio Bitcoin e aggiungete alcuni satoshis per ogni studente.

Date a ogni studente un foglio con una frase-seme per recuperare un portafoglio.

Guidare gli studenti passo dopo passo:

1. Quando si avvia il portafoglio, vengono visualizzati tre metodi di creazione del portafoglio, toccate **[Importa un portafoglio esistente].** Verrà visualizzata una schermata introduttiva, toccate **[Ripristino con frase di recupero].**
2. Inserite la vostra frase di recupero di 12/18/24 parole, una per una, nei campi previsti ed in ordine corretto.
3. Al termine toccate **[Ripristina]**.
4. Quando il portafoglio è stato importato con successo, viene visualizzato il messaggio "Importazione riuscita".

7.4 Ricezione e invio di transazioni

Una transazione bitcoin è un trasferimento di proprietà di bitcoin esistenti a un nuovo proprietario. Tuttavia, invece di trasferire le monete vere e proprie, tutti i nodi della rete aggiornano la loro copia locale del libro contabile pubblico per evidenziare il cambio di proprietà.

Quando si invia una transazione in bitcoin, il mittente firma un messaggio che solo lui può firmare con la sua chiave privata, segnalando alla rete che la proprietà dei bitcoin passa all'indirizzo del destinatario.

I bitcoin saranno ora legati a un indirizzo da cui solo il nuovo proprietario potrà trasferirli, dandogli la proprietà dei bitcoin ricevuti.

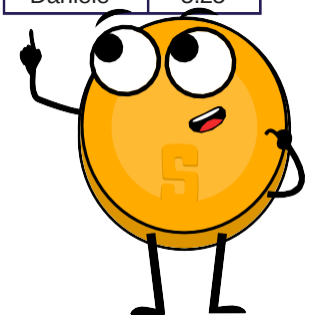
Libro Contabile

Proprietario del conto	Valore
Sam	2.50
Adamo	3.00
Michele	6.00
Jim	1.50
Robert	2.00
Eliana	1.75
Daniele	5.25

Messaggio di richiesta di transazione Bitcoin che Jim invia 0,50 BTC a Eilana
Jim ▸ Eilana 0,50 BTC

Libro Contabile

Proprietario del conto	Valore
Sam	2.50
Adam	3.00
Michele	6.00
Jim	1.00
Robert	2.00
Eliana	2.25
Daniele	5.25



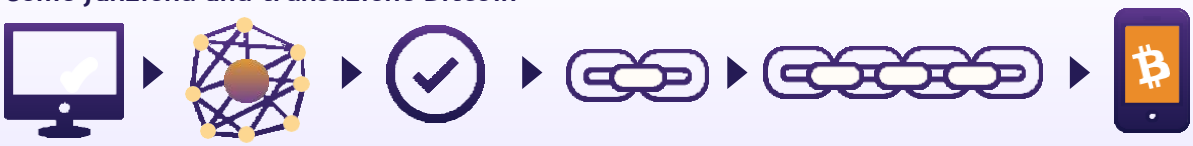
Le nuove transazioni in bitcoin vengono avviate dai portafogli di tutto il mondo, ma non esiste un processore o gestore di pagamento centrale. Al contrario, i minatori di tutto il mondo fanno a gara per registrare le transazioni nel libro mastro.

Supponiamo che Jim debba a Eliana 0,5 BTC e sia pronto a ripagarla. Entrambi hanno un portafoglio digitale.

1. Eliana condivide il suo indirizzo con Jim.
2. Jim utilizza il suo software di portafoglio (wallet) per creare la transazione, che include l'indirizzo di Eliana, l'importo da trasferire (0,5 BTC) e una commissione per il miner.
3. Dopo aver firmato la transazione, questa viene trasmessa alla rete, dove viene verificata dai nodi. I nodi verificano la validità della transazione e si assicurano che Jim abbia fondi sufficienti. In caso contrario, rifiutano immediatamente la transazione.
4. Una volta verificata, la transazione viene aggiunta alla blockchain dai minatori e i fondi vengono trasferiti all'indirizzo di Eliana.
5. Eliana può quindi utilizzare la sua chiave privata per accedere ai fondi trasferiti nel suo portafoglio.

È importante notare che una volta completata, la transazione non può, essere annullata.

Come funziona una transazione Bitcoin



Qualcuno richiede una transazione | Transazione trasmessa ai computer P2P (nodi) | I minatori verificano la transazione | Transazioni combinate per formare un blocco di dati | Nuovo blocco aggiunto alla blockchain esistente | La transazione è completa

Ricezione di transazioni Bitcoin:

Per ricevere bitcoin, è necessario fornire al mittente l'indirizzo del proprio portafoglio Bitcoin. Si tratta di una stringa unica di lettere e numeri che rappresenta il vostro portafoglio e viene utilizzata per identificarlo sulla rete Bitcoin. È possibile trovare l'indirizzo del portafoglio accedendo al proprio portafoglio Bitcoin e cercando l'opzione "Ricevi" o "Deposita" bitcoin.

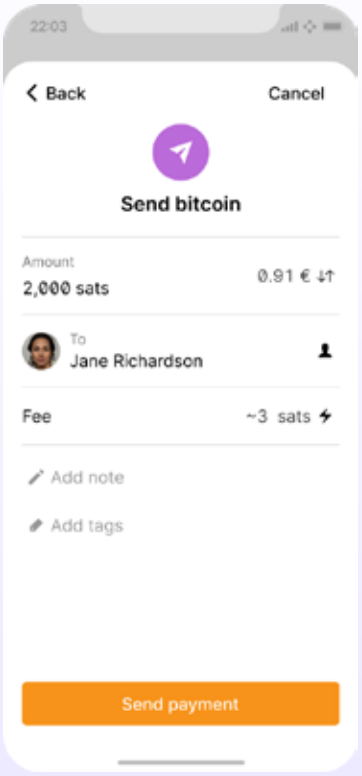
È quindi possibile condividere il proprio indirizzo Bitcoin con il mittente in diversi modi:

1. Copiare e incollare l'indirizzo: È possibile copiare l'indirizzo evidenziandolo e premendo "Copia" sulla tastiera, quindi incollarlo in un'e-mail o in un messaggio al mittente.
2. Condividere un link al proprio portafoglio Bitcoin: alcuni portafogli Bitcoin consentono di creare un link al proprio portafoglio da condividere con il mittente. Il mittente può quindi cliccare sul link per accedere al suo portafoglio e inviare i bitcoin.
3. Condividere il QR code: se il mittente ha uno smartphone con l'app del portafoglio Bitcoin, può scansionare il codice QR per ottenere il vostro indirizzo Bitcoin.

Come utilizzare Bitcoin

Una volta che il mittente ha il vostro indirizzo Bitcoin, può inviarvi bitcoin inserendo il vostro indirizzo e l'importo che vuole inviarvi e avviare la transazione. I bitcoin saranno inviati al vostro portafoglio e saranno visibili una volta che la transazione sarà confermata dalla rete Bitcoin. Questa operazione richiede di solito pochi minuti.

Successivamente, daremo un'occhiata all'invio di transazioni in bitcoin.



Invio di transazioni Bitcoin:

Per inviare bitcoin sono necessari alcuni elementi: un portafoglio Bitcoin, l'indirizzo Bitcoin del destinatario e la quantità di bitcoin che si desidera inviare.

1. Aprite il vostro portafoglio Bitcoin. Un codice SMS verrà inviato al vostro numero di telefono e dovrete inserirlo nella finestra di dialogo. In alternativa, se avete attivato Google 2FA, dovrete inserire il codice di sei cifre dall'app Google Authenticator.
2. Selezionate la voce "Inviare" o "Ricevere" e copiate l'indirizzo del destinatario.
3. Inserite l'indirizzo Bitcoin del destinatario incollandolo nel campo "Destinatario".
4. Inserire l'importo dei bitcoin che si desidera inviare nel campo "Importo".
5. Ricontrollate l'indirizzo del destinatario e l'importo da inviare.
6. Prima di fare clic su "Conerma e invia", vi consigliamo di ricontrollare i dettagli della transazione un'altra volta per assicurarsi di inviare l'importo corretto di bitcoin all'indirizzo corretto del portafoglio del destinatario.
7. Confermare la transazione e attendere che la rete conermi la transazione.

Ora sapete come valutare, selezionare e impostare un portafoglio Bitcoin autocustodito. L'invio di bitcoin da un portafoglio a un altro sulla rete Bitcoin si chiama transazione "on-chain", questo perché la transazione avviene sulla blockchain principale della rete Bitcoin. Le transazioni "on-chain" sono il modo più sicuro per effettuare transazioni con i bitcoin; tuttavia, queste transazioni sono più costose e più lente rispetto ad altre opzioni, come verrà illustrato nel Capitolo 8.

Attività: Transazioni Bitcoin in azione

Obiettivo: Comprendere i concetti e i meccanismi di base di una transazione bitcoin peer-to-peer.

Prima di iniziare, ecco un breve promemoria sugli attori principali di una transazione in bitcoin:

- I mittenti e i destinatari sono le parti che desiderano effettuare transazioni tra loro.
- I nodi convalidano le transazioni e memorizzano una copia completa della blockchain. Esistono anche nodi “leggeri” che hanno solo una parte recente della blockchain, questi consentono di convalidare le transazioni utilizzando meno memoria e meno risorse computazionali.
- I minatori sono responsabili dell'aggiunta di nuove transazioni alla blockchain.

Comprendere il proprio ruolo. Vi è stato assegnato uno dei seguenti ruoli: mittente, destinatario, nodo o minatore.

- I mittenti saranno responsabili della creazione e della trasmissione delle transazioni.
- I ricevitori saranno responsabili della ricezione e della verifica delle transazioni.
- I nodi saranno responsabili della convalida delle transazioni.
- I minatori saranno responsabili dell'aggiunta delle transazioni alla blockchain.

Sia i nodi che i ricevitori devono verificare le transazioni

Come mittente: Creare una transazione.

Procedere come segue: prendere una nota di transazione e scrivere il numero di monete che si desidera inviare e il nome o le iniziali del destinatario. Firmare la nota con il proprio nome o le proprie iniziali, simulando una chiave privata. Passare la nota di transazione e il numero corrispondente di monete al destinatario.

2 **In qualità di destinatario:** siete responsabili della verifica delle transazioni. Seguire i seguenti passaggi:

- Controllare la nota di transazione per assicurarsi che il numero di monete e il nome del destinatario siano corretti o siano almeno scritte le iniziali.
- Contate le monete ricevute e confrontatele con il numero di monete scritte sulla nota.
- Se le monete corrispondono, selezionare la casella di approvazione. Se le monete non corrispondono o se avete dei dubbi, rifiutate la transazione.

Monete inviate	**Mittente**	**Firma mittente**	**Ricevente**	**Data e ora**	**Approvazione destinatario**

3 **Come nodo:** Verifica e convalida le transazioni. Sei responsabile della verifica delle transazioni.

- Verificate che l'indirizzo del mittente e del destinatario siano validi.
- Verificate che il mittente disponga di fondi sufficienti per completare la transazione e che questa non comporti una doppia spesa di monete.

Monete inviate	**Mittente**	**Firma mittente**	**Ricevente**	**Data e ora**	**Approvazione del Nodo**

Come utilizzare Bitcoin

4 **Come minatore:** siete responsabili dell'aggiunta delle transazioni alla blockchain. Seguite questi passaggi:

- Controllate le transazioni approvate dai ricevitori e convalidate dai nodi.
- Tirate i dadi e confrontate i numeri con quelli dell'altro minatore. Il minatore con il numero più basso aggiungerà la transazione alla blockchain.
- Per il tempo, l'energia e l'effort guadagnerete un punto. Alla fine dell'attività, vince il minatore con il maggior numero di punti.

Una volta aggiunta alla blockchain, una transazione non può essere modificata o annullata.

5 **Tenete traccia del saldo delle monete:** per tutta la durata dell'attività, tenere traccia del saldo delle monete contando le monete nel vostro portafoglio digitale.

Monete inviate	Mittente	Firma mittente	Ricevente	Data e ora	Approvazione

6 **Discutete i concetti appresi con il resto della classe.**

7.5 Risparmio in Bitcoin

Il Bitcoin è un modo per salvaguardare il proprio denaro dall'inflazione e proteggerlo dal controllo di chiunque altro, se lo si fa correttamente. Il risparmio in bitcoin è un mezzo per conservare, accumulare e costruire ricchezza nel tempo. Come ormai sapete, il tipo di denaro che scegliete di risparmiare è una delle decisioni più importanti che possiate prendere. Scegliere con saggezza vi permette di costruire un futuro migliore per voi stessi e la vostra famiglia.

Tranquillità: se conservato correttamente, il Bitcoin è l'unica forma di proprietà che **nessuno può portarvi via**.

7.6 Non fidatevi, verificate ! (Don't Trust, Verify)

Qualunque cosa facciate in Bitcoin, ricordate questo: "Non fidatevi, verificate". Non ci sono leader in Bitcoin. Non dovreste mai seguire ciecamente le affermazioni di qualcuno, piuttosto, dovreste sempre mettere in discussione ciò che vi viene detto e verificarlo da soli. Seguendo questo mantra, vi proteggerete dalla perdita dei vostri bitcoin. Questo vale per affermazioni come "il prossimo Bitcoin", così come per le "opportunità di investimento" o le promesse di "profitti facili e veloci".

In sintesi, il Capitolo 7 vi ha fornito le competenze importanti per utilizzare i Bitcoin nella vostra vita quotidiana. Avete imparato come ottenere e scambiare bitcoin in modi diversi e come tenerli al sicuro utilizzando vari portafogli.

Impostando il vostro portafoglio Bitcoin mobile ed effettuando transazioni con altri, ora avete un'esperienza pratica per utilizzare confidentemente Bitcoin ogni giorno. Comprendendo il Bitcoin come un modo per risparmiare denaro e seguendo l'idea del DYOR (fate le vostre ricerche personali, non credete ad altri, verificate personalmente - Don't Trust, Verify), ora avete il controllo del vostro denaro.

Nel prossimo capitolo esploreremo la Rete Lightning. Vedremo come questa tecnologia innovativa sta cambiando il modo in cui le persone in tutto il mondo accedono al proprio denaro e lo utilizzano. Dalle transazioni di tutti i giorni alle applicazioni più avanzate, imparerete come la Rete Lightning dia potere a individui, comunità e aziende, fornendo loro l'accesso ai servizi finanziari.

Capitolo #8

Rete Lightning: Utilizzare Bitcoin nella vita quotidiana

Libro di lavoro per studenti

Versione italiana| 2025

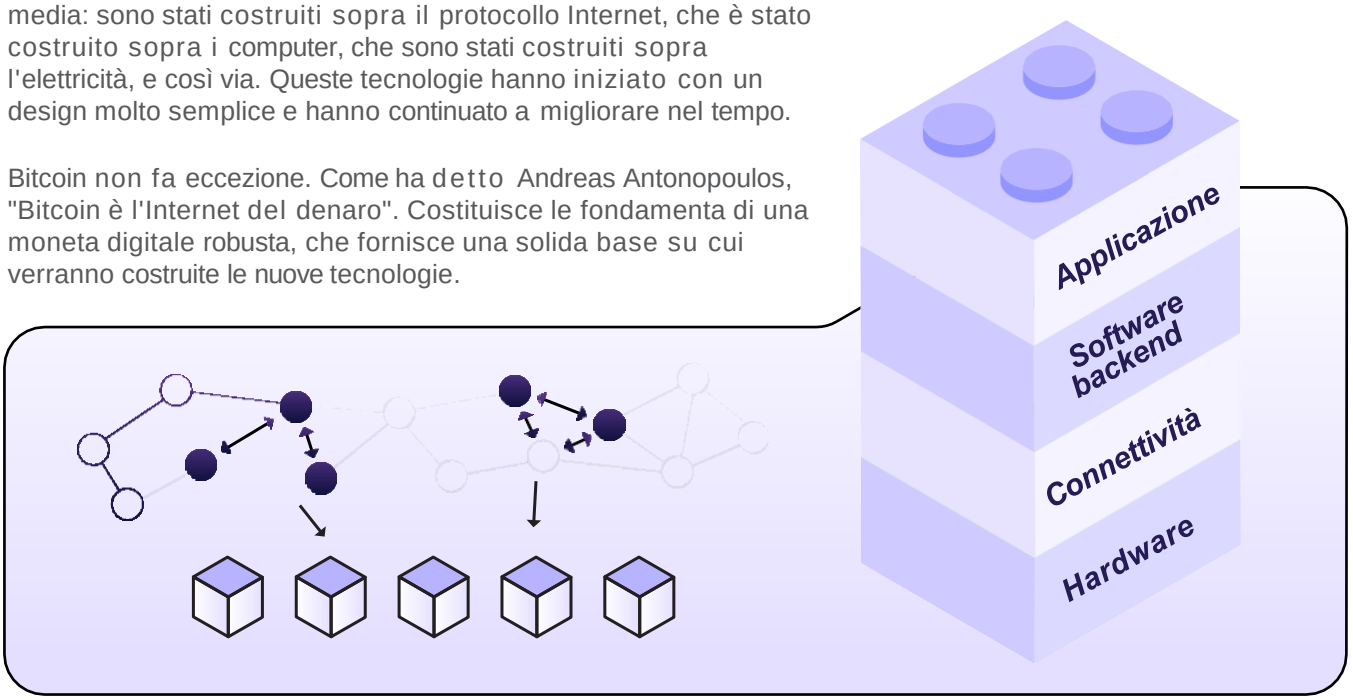
Rete Lightning: Utilizzare Bitcoin nella vita quotidiana

8.0 Introduzione

> Stiamo costruendo la rete Visa per bitcoin. Ma ciò che penso sia potente è che, a differenza di Visa, chiunque può costruirci sopra.
>
> **Elisabetta Stark**

Le tecnologie di solito crescono e si espandono a strati, come una pila. Pensate al vostro sito web preferito, alla posta elettronica o ai social media: sono stati costruiti sopra il protocollo Internet, che è stato costruito sopra i computer, che sono stati costruiti sopra l'elettricità, e così via. Queste tecnologie hanno iniziato con un design molto semplice e hanno continuato a migliorare nel tempo.

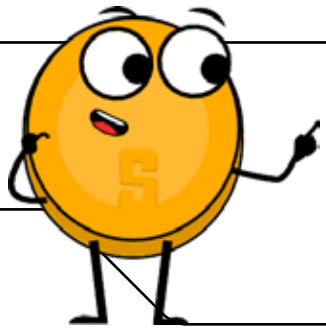
Bitcoin non fa eccezione. Come ha detto Andreas Antonopoulos, "Bitcoin è l'Internet del denaro". Costituisce le fondamenta di una moneta digitale robusta, che fornisce una solida base su cui verranno costruite le nuove tecnologie.



Uno di questi livelli è chiamato "**Lightning Network**". Si tratta di una sorta di autostrada superveloce per Bitcoin, che aiuta le persone a inviare e a ricevere bitcoin in modo rapido e con commissioni molto basse. Permette agli utenti di effettuare pagamenti istantanei, per piccole transazioni in aggiunta alla normale rete Bitcoin. Questo rende possibile acquistare un caffè o pagare un amico in modo semplice e veloce !
Ricordate: un **satoshi** è come la più piccola moneta di bitcoin. Proprio come un dollaro può essere suddiviso in centesimi, un bitcoin può essere suddiviso in unità più piccole chiamate **satoshi**. Un bitcoin equivale a 100 milioni di **satoshi**, e questo rende i **satoshi** i più piccoli valori nel sistema Bitcoin. In questo capitolo, quando parliamo di invio di bitcoin attraverso **Lightning Network**, lo chiameremo "invio di **sats**", che sono solo parti più piccole di un bitcoin.

Satoshi	Bitcoin
1	0.00000001
10	0.00000010
100	0.00000100
1,000	0.00001000
10,000	0.00010000
100,000	0.00100000
1,000,000	0.01000000
10,000,000	0.10000000
100,000,000	1.00000000

Attività: Guardare questo video sulla Rete Lightning



8.1 La Rete Lightning

Come abbiamo appena visto, la Lightning Network funge da sistema di pagamento, facilitando transazioni rapide ed economiche con i bitcoin. Funziona creando un portafoglio condiviso in cui entrambe le parti detengono alcuni bitcoin. Possono effettuare numerose transazioni tra loro senza la necessità di registrare ciascuna di esse sul libro mastro principale (block-chain). Il saldo finale viene registrato sul libro mastro una volta completate le transazioni.

La Lightning Network è un sistema di pagamento che consente agli utenti di inviare e ricevere pagamenti in modo rapido ed economico utilizzando i bitcoin. Funziona creando un portafoglio condiviso in cui entrambe le persone memorizzano i loro bitcoin e poi effettuano transazioni illimitate tra loro senza toccare la blockchain principale. Al termine il saldo finale viene registrato sulla blockchain principale.

Immaginate una giornata di lavoro in un bar. Prevedendo un'intera giornata di permanenza, aprite un conto e pagate in anticipo invece di pagare ogni volta che ordinate qualcosa. Alla fine della giornata, quando siete pronti per andarvene, voi e il proprietario rivedete il conto per saldare il conto finale. Se si è pagato più del consumo effettivo, si riceve un rimborso.

Ora, immaginate migliaia di persone che fanno la stessa cosa contemporaneamente e che permettono ad altri di usare le loro schede per connettersi con più persone. Questa è la rete Lightning!

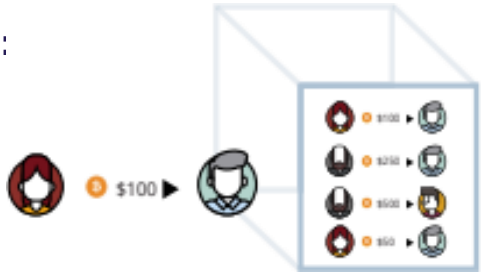
Con Lightning è possibile effettuare pagamenti a chiunque nella rete, non solo alla persona con cui si condivide una scheda diretta. Il pagamento può attraversare la rete fino a raggiungere la destinazione, anche se non si ha un canale aperto con il destinatario.

Vediamo la differenza tra le transazioni on-chain (il tipo di transazioni di cui abbiamo parlato nel Capitolo 7) e le transazioni off-chain (Lightning Network).

Transazioni on chain (registrate sulla blockchain):

Si tratta di transazioni che avvengono direttamente sulla blockchain di Bitcoin. Richiedono almeno 10 minuti per essere concluse e le commissioni dipendono dalla dimensione della transazione in byte.

Sono più sicure ma più lente e costose.

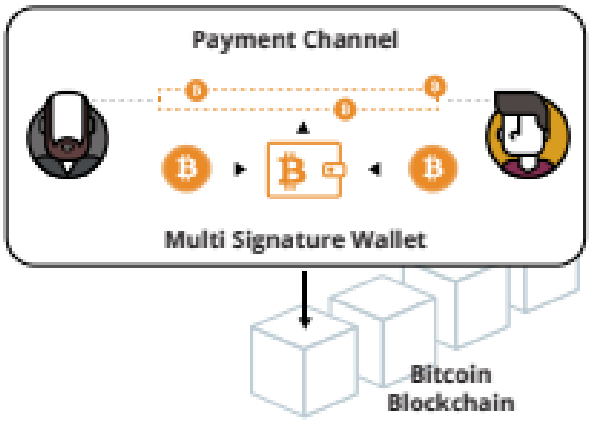


Rete Lightning: Utilizzare Bitcoin nella vita quotidiana

Transazioni off chain (Lightning Network)

Queste transazioni avvengono su una rete separata costruita sulla blockchain di Bitcoin. Vengono regolate più velocemente e con commissioni più basse.

Sono comunemente utilizzate nei casi in cui le normative e le leggi ne sostengono l'adozione e dove caratteristiche come la velocità e il costo delle transazioni sono più importanti.
Rispetto alle transazioni on-chain, sono meno sicure.



Rete di pagamento	Rete Bitcoin	Rete Lightning
Definizione	Una rete digitale decentralizzata che utilizza la crittografia per proteggere le transazioni finanziarie.	Un protocollo di pagamento di secondo livello che opera sulla blockchain di Bitcoin, consentendo transazioni più rapide ed economiche.
Vantaggi	Decentrato e sicuro. Nessuna possibilitá di annullamento o frode. Può essere utilizzato in modo anonimo. Accettazione globale.	Transazioni più rapide ed economiche. Maggiore scalabilità. Le transazioni sono off-chain pertanto non intasano la blockchain.
Svantaggi	Tempi lenti per le transazioni. Commissioni elevate per alcuni tipi di transazioni. Complesso per i principianti.	Richiede fiducia negli operatori del canale. Ancora sperimentale e non ampiamente adottato. Richiede una transazione on-chain per aprire e chiudere i canali.

2. Diversi tipi di portafogli lightning

Un portafoglio Lightning è un po' diverso da un portafoglio Bitcoin, anche se svolge la stessa funzione: ricevere e inviare bitcoin. La differenza sta nel fatto che un portafoglio Lightning consente di inviare bitcoin sulla rete Lightning, che a sua volta è un secondo livello sopra la rete Bitcoin.

Proprio come abbiamo visto nel capitolo precedente con i portafogli Bitcoin, i portafogli Lightning hanno caratteristiche diverse che devono essere considerate prima di sceglierne uno.

1. Portafogli autocustoditi e portafogli custoditi

I portafogli Lightning possono essere suddivisi in categorie molto specifiche, ma per semplicità le divideremo in due: auto-custoditi (non custodial) e custoditi (custodial).

Proprio come i portafogli Bitcoin, un portafoglio Lightning auto-custodito è quello in cui si controllano le chiavi del portafoglio, mentre un portafoglio Lightning custodito è quello in cui qualcun altro controlla le chiavi.

Quando si utilizza un portafoglio di custodia, si ottiene solo l'accesso al portafoglio, ma si dipende da qualcun altro per il permesso di utilizzare il proprio denaro: si rinuncia quindi alla proprietà del proprio denaro per comodità.

Questa soluzione può essere accettabile per piccole somme, anche se si consiglia di utilizzare un portafoglio auto-custodia una volta acquisita una certa familiarità con la tecnologia.

Di seguito parleremo solo dei portafogli Lightning autocustoditi.

2. Open Source vs Closed Source

Proprio come i portafogli Bitcoin che abbiamo visto nel capitolo precedente, i portafogli Lightning possono essere open-source o closed-source. Utilizzate sempre portafogli open-source, perché sono completamente aperti alla revisione e controllati dalla comunità.

Un'applicazione open-source significa anche che chiunque può contribuire al miglioramento del software, rendendolo una scelta migliore per gli utenti.

3. Creazione di un portafoglio Bitcoin Lightning

La creazione di un portafoglio Bitcoin Lightning auto-custodito è identica a quella di un portafoglio Bitcoin on-chain auto-custodito.

Rete Lightining: Utilizzare Bitcoin nella vita quotidiana

Esercitazione in classe - Opzione 1**:** scaricare un nuovo portafoglio Lightning auto-custodito.

Come creare e utilizzare un portafoglio Bitcoin Lightning.

1. Cercate l'applicazione nell'App Store (iOS) o nel Google Play Store (Android).

2. Aprite l'applicazione e digitate la vostra frase di recupero di 12 o 24 parole (a volte chiamata frase seed o seme). **Assicuratevi di scriverla e di conservarla in un luogo sicuro!** Questa frase di recupero vi permette di recuperare l'accesso completo ai vostri fondi, se necessario.

Ricordate che se perdete o dimenticate questa sequenza di parole, non potrete accedere ai vostri bitcoin se perdete l'accesso al vostro portafoglio.

3. È quindi necessario accertarsi di aver effettivamente salvato la frase di recupero o seed. A tal fine, è necessario inserire, nello stesso ordine, le parole della frase iniziale.

4. Come ulteriore misura di sicurezza, alcuni portafogli consentono di scegliere una password sicura. La chiave privata e il primo indirizzo Bitcoin vengono creati automaticamente dal portafoglio.

5. Generate una fattura Lightning, un indirizzo o un codice QR per ricevere bitcoin. Trasferite i bitcoin al proprio portafoglio. Con un portafoglio autocustodito, non è sempre possibile acquistare bitcoin direttamente con fiat, quindi potrebbe essere necessario acquistarli e trasferirli da un exchange.

La vostra frase seed (o seme)

La frase iniziale viene utilizzata per generare e recuperare il protafoglio.

1 Emissione	2 Fiamma	3 Campione	4 Testi	5 Trovare
6 Volta	7 Forbici	8 Banner	9 Carino	10 Danno
11 Civile	12 Capra			

Conservate queste 12 parole su un foglio di carta. L'ordine è importante. Questa sequenza di parole (o seme) vi permetterà di recuperare il vostro portafogli, e fondi.

* Nota: se si utilizza un portafoglio di custodito, non sarà necessario seguire alcuni dei passaggi della sezione 8.3. L'utilizzo di un portafoglio custodito comporta dei rischi, in quanto non avrete il controllo della vostra chiave privata e ciò vuole dire che non avrete il controllo del denaro che conservate nel vostro portafoglio.

Ora che abbiamo configurato il nostro portafoglio Bitcoin Lightning, analizziamo la ricezione e l'invio delle transazioni Lightning e la loro differenza rispetto alle transazioni on-chain inviate nel Capitolo 7.

8.4 Invio e ricezione di transazioni Lightning

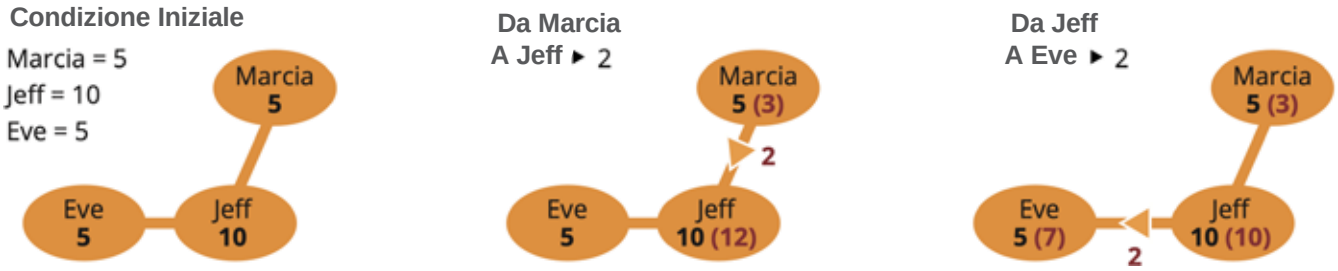
Con un portafoglio Lightning, l'utilizzo di Bitcoin è veloce, economico e privato, rendendo facili le transazioni tra due persone. È possibile inviare e ricevere rapidamente bitcoin per le attività di tutti i giorni, come l'acquisto di prodotti alimentari o lo shopping.

Vediamo alcuni esempi di Lightning Network in azione.

Esempio 1:

Di seguito, sia Marcia che Eve hanno 5 unità di valuta ciascuna. Marcia vuole inviare 2 delle sue unità a Eve, quindi invia 2 unità a Jeff. Jeff passa poi le 2 unità a Eve, che ora ha 7 unità. Marcia ha ora 3 unità.
E questo è quanto! La transazione è conclusa.

Il punto chiave è che Marcia ed Eve non devono passare attraverso una banca o un altro intermediario per effettuare la transazione.



Jeff agisce come un intermediario o una "terza parte fidata" in questo scenario, in cui Marcia ed Eve non si fidano direttamente l'una dell'altra. Jeff riceve le 2 unità da Marcia e le passa a Eve, completando così la transazione. Utilizzando Jeff come intermediario, Marcia ed Eve possono completare la transazione senza bisogno di una banca o di un'altra istituzione centralizzata, rendendo la transazione più veloce, economica e sicura. Jeff è un elemento chiave in questo processo di transazione peer-to-peer.

In qualità di operatore di nodo in una transazione della Lightning Network, Jeff beneficia di diversi vantaggi:

1

Commissioni di transazione

Jeff guadagna una piccola commissione per ogni transazione che passa attraverso il suo nodo, che lo ricompensa per il tempo e l'impegno che dedica alla manutenzione e alla gestione del suo nodo.

2

Partecipazione alla rete

Gestendo un nodo Lightning, Jeff partecipa alla rete e contribuisce ad aumentarne la decentralizzazione, la sicurezza e la stabilità. Questo può aumentare la reputazione e la credibilità di Jeff come operatore di nodi affidabile, rendendolo un intermediario più interessante per le transazioni future.

Rete Lightning: Utilizzare Bitcoin nella vita quotidiana

3 Crescita della rete

Con la crescita della Lightning Network e l'utilizzo da parte di un maggior numero di persone, è probabile che il numero di transazioni che passano attraverso il nodo di Jeff aumenti, il che può comportare un aumento delle entrate derivanti dalle commissioni sulle transazioni.

4 Maggiore sicurezza della rete

Il ruolo di Jeff come intermediario contribuisce ad aumentare la sicurezza della rete aggiungendo un ulteriore livello di protezione tra Marcia ed Eve. Questo può aumentare la fiducia degli utenti nella rete, rendendola più appetibile per i nuovi utenti e contribuendo alla crescita. Nel complesso, essere un operatore di nodi della rete Lightning può fornire a Jeff una fonte di reddito costante, oltre all'opportunità di contribuire alla crescita e allo sviluppo della rete.

In sintesi, le **transazioni on-chain sono più lente ma più sicure, mentre quelle off-chain (Lightning Network) sono più veloci ma meno sicure.** È necessario valutare il compromesso tra sicurezza e velocità in base alle proprie esigenze.

Esempio 2:

Lea ha un grande amore per il McDonald's: ci va ogni giorno per colazione, pranzo e cena!
Ma con le tante opzioni di pagamento disponibili, non è sicura di quale sia la scelta migliore. Per fortuna, ha imparato qualcosa su Bitcoin e sulla rete Lightning. Dopo aver confrontato le tabelle sottostanti, Lea non ha dubbi: utilizzare un metodo di pagamento Lightning è la soluzione migliore.

La rete Lightning a confronto con il sistema bancario tradizionale

Benefici	Lightning	Sistema bancario tradizionale
Velocità	Veloce	Lento
Trasparenza	Trasparente	Opaco
Sicurezza	Sicura	Vulnerabile
Commissioni	Bassa	Alto
Inclusione finanziaria	Alta	Limitato

Benefici	Lightning	Sistema bancario tradizionale
Scalabilità	Alta	Basso
La privacy	Alta	Moderato
Interoperabilità	Alta	Basso
Conformità legale	Moderata	Alto
Costo. Efficacia	Alta	Moderato

Visa, Inc.

1.700 transazioni di media al secondo

Capacitá di 65.000 transazioni per secondo

Bitcoin On-chain

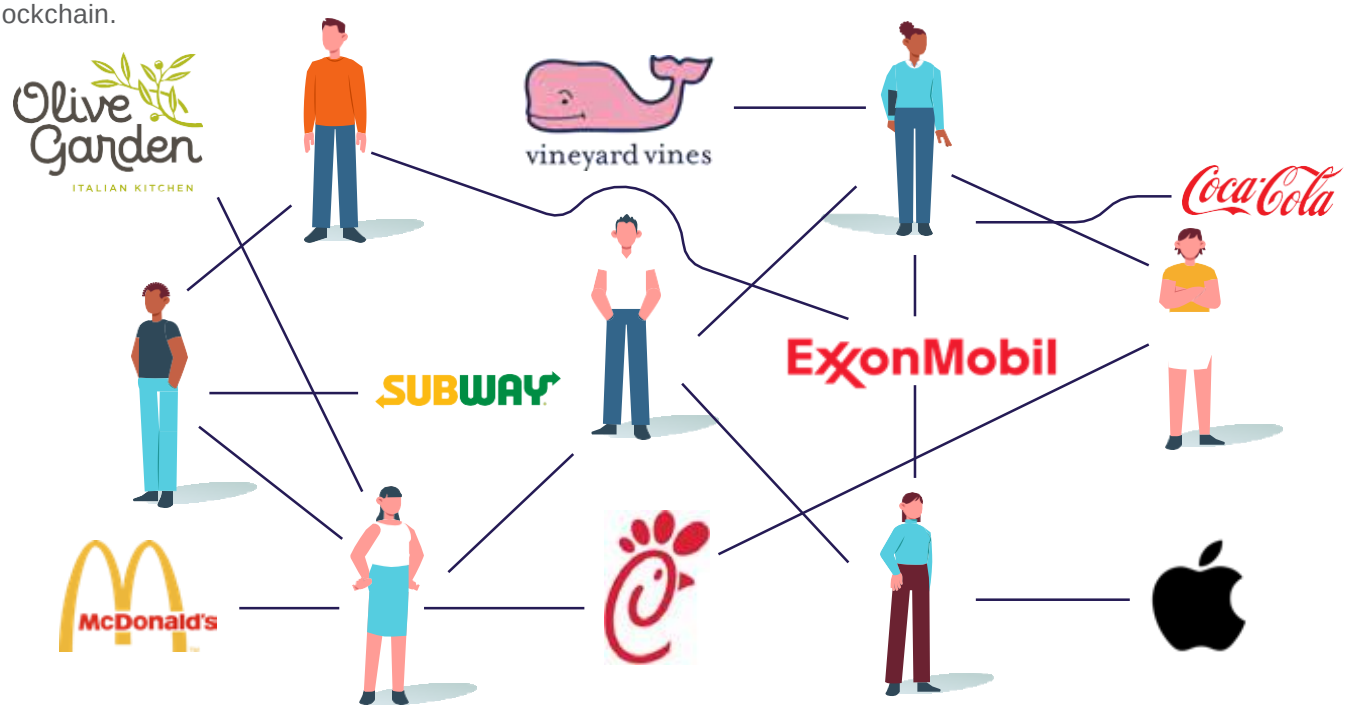
Capacitá di 7 transazioni di media al secondo

Bitcoin Lightning Network

Milioni di transazioni al secondo

Lea è anche un'appassionata di transazioni rapide, sicure e convenienti, quindi ha deciso di utilizzare Lightning per i suoi acquisti da McDonald's. Con Lightning, può godersi ancora di più i suoi pasti sapendo che i pagamenti vengono elaborati istantaneamente, in modo sicuro e con commissioni ridotte. Inoltre, poiché la rete Lightning garantisce l'inclusione finanziaria, Lea può ora pagare i suoi pasti anche se si trova in una zona remota di El Salvador.

Per iniziare a utilizzare questa rete, Lea scarica un portafoglio Lightning sul suo telefono. Poi finanzia il suo portafoglio inviando alcuni bitcoin dal suo normale portafoglio Bitcoin al suo nuovo portafoglio Lightning. Questo processo è chiamato "finanziamento del portafoglio" o "finanziamento di un canale di pagamento". Lea può finanziare il suo portafoglio con qualsiasi quantità di bitcoin, ma è importante notare che la quantità di bitcoin che blocca nel suo portafoglio Lightning non può essere utilizzata per le transazioni sulla blockchain.



Una volta che il suo portafoglio Lightning è stato finanziato, può utilizzarlo per effettuare pagamenti da McDonald's.

McDonald's ha un nodo Lightning, quindi Lea può aprire un canale di pagamento con loro inviando una parte dei suoi bitcoin dal suo portafoglio Lightning a un indirizzo specifico fornito da McDonald's.
Questo sposta i suoi bitcoin dalla blockchain Bitcoin a una transazione sulla rete Lightning.

Con il canale di pagamento aperto, Lea può ora fare acquisti da McDonald's senza dover aprire un nuovo canale o pagare ogni volta commissioni elevate. Il canale rimane aperto finché sia Lea che McDonald's vogliono utilizzarlo. Ad esempio, se Lea acquista un hamburger per 0,0005 bitcoin, il canale tiene traccia del fatto che ora Lea possiede 0,9995 bitcoin. E se il giorno dopo acquista un frullato per 0,0003 bitcoin, il canale rileva che Lea ha ora 0,9992 bitcoin.

Rete Lightning: Utilizzare Bitcoin nella vita quotidiana

Quando Lea decide di voler utilizzare il suo saldo in bitcoin per qualcos'altro, chiude il canale trasmettendo una transazione di chiusura alla blockchain Bitcoin. Questo avviene avviando una transazione di chiusura nel suo portafoglio Lightning, che contiene il saldo finale del canale concordato da entrambe le parti. La transazione viene quindi trasmessa alla blockchain Bitcoin e confermata da un miner. Una volta conclusa la transazione, il canale viene chiuso e i bitcoin rimanenti nel canale vengono restituiti sia a Lea e al McDonald's.

È importante notare che la chiusura di un canale può richiedere del tempo per essere configurata sulla blockchain. Durante questo periodo di attesa, i fondi sono ancora bloccati nel canale e non possono essere utilizzati per le transazioni sulla catena. Lea riceverà una notifica quando la transazione di chiusura sarà confermata.

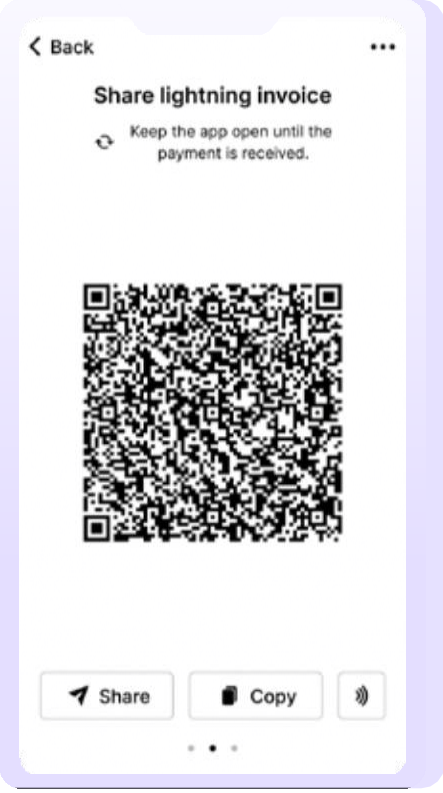
Dopo aver configurato il nostro portafoglio Lightning e aver letto come utilizzare la rete Lightning per inviare transazioni, faremo un gioco in cui invieremo satoshi (la più piccola unità del sistema bitcoin) ad altri studenti della classe attraverso la rete Lightning.

Questa è una mappa del mondo intero. Con la Lightning Network, è possibile inviare satoshi a qualsiasi utente con un portafoglio Bitcoin Lightning. Il pagamento arriverà in pochi secondi e costerà solo pochi centesimi.

Verificate voi stessi:

Attività: Esercizio in classe - Gara a staffetta di portafogli Lightning

1. Innanzitutto, è necessario scaricare un portafoglio Lightning sul telefono o sul computer.
2. Seguite le istruzioni per l'installazione del portafoglio sul dispositivo nella sezione 8.3 di questo capitolo.
3. Una volta installato il portafoglio, apritelo e seguite le istruzioni per configurarlo. Ciò può comportare la creazione di un nuovo portafoglio o il ripristino di uno esistente e la sua protezione con una password o un'altra forma di autenticazione.
4. Generate una fattura Lightning, un indirizzo o un codice QR per ricevere bitcoin.
5. Quando il vostro portafoglio è configurato e siete pronti a ricevere i satoshis, l'insegnante darà a voi e al vostro gruppo una quantità iniziale di satoshis inviandoli direttamente al vostro portafoglio.



A. L'obiettivo del gruppo è passare i satoshis dal portafoglio di una persona all'altra utilizzando la rete Lightning fino a raggiungere l'ultima persona del gruppo.

B. Per inviare satoshi a un'altra persona, aprite il portafoglio e seguite le istruzioni per effettuare un pagamento. È necessario fornire la fattura Lightning del destinatario o scansionare un codice QR e inserire l'importo di satoshis che si desidera inviare.

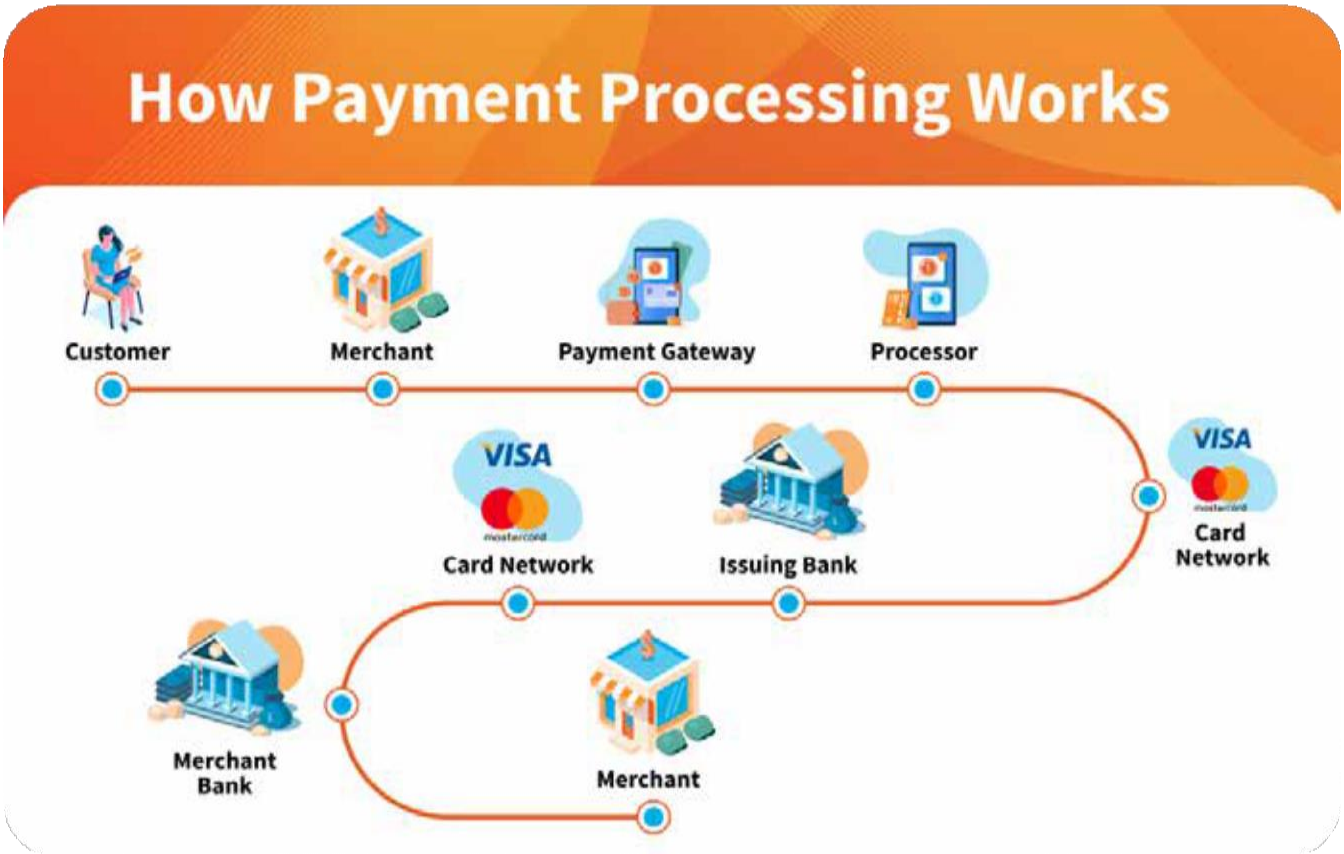
C. Se il vostro gruppo è il primo a inviare con successo i satoshi all'ultima persona, avrete vinto ! (E potrete tenere i satoshi).

Discutete le eventuali difficoltà incontrate dal vostro gruppo durante l'attività. L'invio di una transazione è stato facile, veloce e poco costoso? Ritenete che la rete Lightning sia facile da usare e da capire?

8.5 Acquisto di prodotti alimentari con Bitcoin

Vi siete mai chiesti se potete usare bitcoin per comprare la vostra tazza di caffè quotidiana o per fare la spesa? A quanto pare è possibile. Ci sono molte opzioni, sia online che di persona, che vi permettono di pagare con i bitcoin. Esploreremo alcune di queste opzioni e gli strumenti che vi aiuteranno a trovare i negozi locali in modo da poter spendere bitcoin.

Anche se pagare con una carta di credito o un'app può sembrare facile da capire per la persona che paga, l'elaborazione del pagamento è in realtà molto complessa e coinvolge molte parti differenti.



Quando si acquistano prodotti, ci sono molte parti coinvolte e ognuna di esse applica una commissione. Per i negozianti, queste commissioni possono essere molto elevate: più del 3% del prezzo, una cifra notevole per loro.

Senza contare le spese di cambio valuta!

Commissioni di elaborazione delle carte di credito

$100	-$1.75	-$0.14	-$0.30	-$97.81
Il cliente paga	Banca emittente	Rete di schede Processori	Processori di pagamento	Il Commerciante riceve.

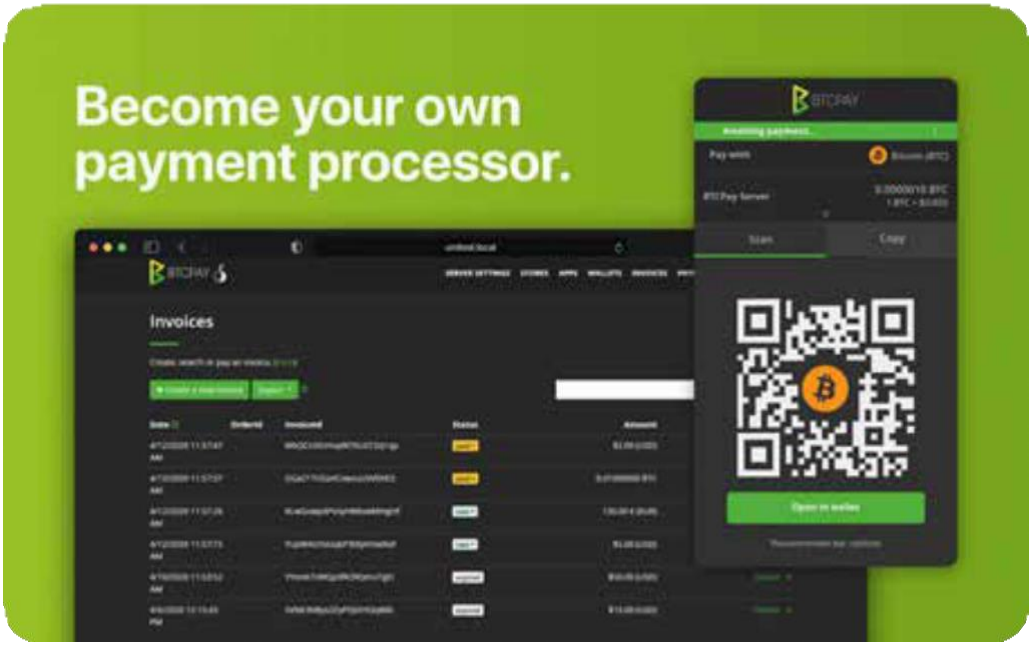
Con Bitcoin e la Lightning Network, le aziende possono ricevere pagamenti istantanei da tutto il mondo attraverso un sistema monetario aperto, sicuro, nativo di Internet, senza confini e resistente alla censura.

A seguire, analizzeremo alcuni modi in cui i commercianti possono facilmente accettare pagamenti in bitcoin.

8.5.1 Online: Plugin di pagamento - Ecommerce

BTCPay Server è un processore di pagamenti open-source che consente ai commercianti di accettare pagamenti in bitcoin con poche conoscenze tecniche. È completamente gratuito e non applica alcuna commissione.

Le aziende online possono integrare il server BTCPay senza problemi aggiungendo il plugin BTCPay al proprio sito web.



Poiché BTCPay Server è un progetto open-source e non un'azienda, è possibile contribuire al progetto una volta acquisite maggiori informazioni su di esso e sulla programmazione informatica.

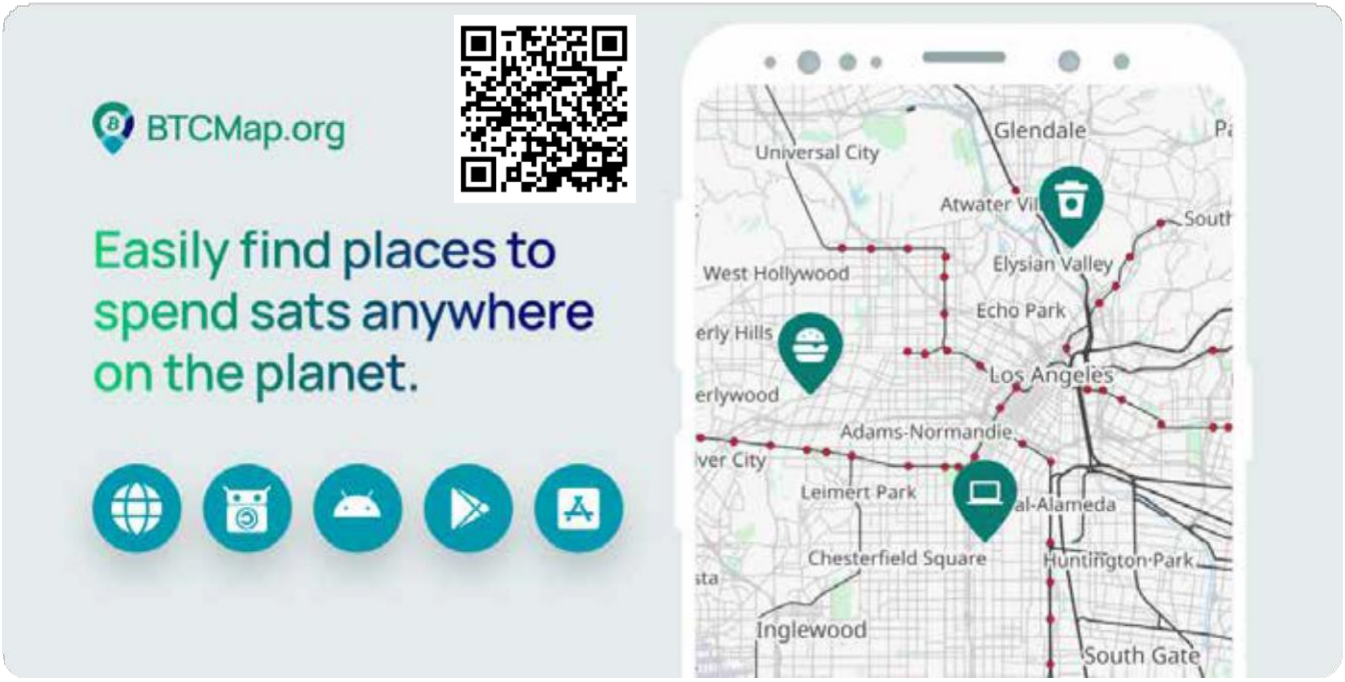
Consultate il server BTCPay https://btcpayserver.org/it_IT/ per maggiori informazioni su come utilizzare questo sistema di pagamento per la vostra attività commerciale online o di persona.

8.5.2 Di persona: Trovare un commerciante nella vostra zona

I negozi fisici possono anche utilizzare il server BTCPay per accettare i pagamenti, oppure possono semplicemente scaricare un portafoglio Bitcoin e accettare pagamenti in Bitcoin direttamente dal proprio telefono.

Per trovare un commerciante che accetta Bitcoin nella vostra zona, andate su BTCMap.org e cercate la vostra regione.

BTCMap.org è una mappa open-source dove i commercianti che accettano Bitcoin possono elencare le loro attività. È uno strumento potente per chi desidera spendere i propri bitcoin.



8.5.3 Strumenti di transizione: Buoni, carte regalo e carte di pagamento

Per acquistare prodotti o servizi da aziende che non accettano ancora Bitcoin, esiste uno strumento di intermediazione: **le carte regalo**.

Alcune aziende si concentrano sulla compravendita di carte regalo in cambio di bitcoin. Ciò significa che è possibile acquistare una carta regalo per il negozio in cui si desidera andare in cambio di bitcoin e poi spendere la carta regalo direttamente nel negozio.

Biglietti aerei, hotel, giochi, carte SIM... con bitcoin e le carte regalo è possibile acquistare quasi tutto!

8.5.4 Economie circolari e Bitcoin come mezzo di scambio

Il concetto di economia circolare nasce dall'idea di ridurre al minimo i rifiuti in un'economia riutilizzando e riciclando il maggior numero possibile di prodotti e sottoprodotti.

Partendo da questo concetto, un'economia circolare Bitcoin è un'economia in cui le transazioni sono effettuate in bitcoin e in cui il denaro sotto forma di bitcoin rimane e cresce all'interno dell'economia, a beneficio dei suoi individui e delle sue imprese.

Rete Lightning: Utilizzare Bitcoin nella vita quotidiana

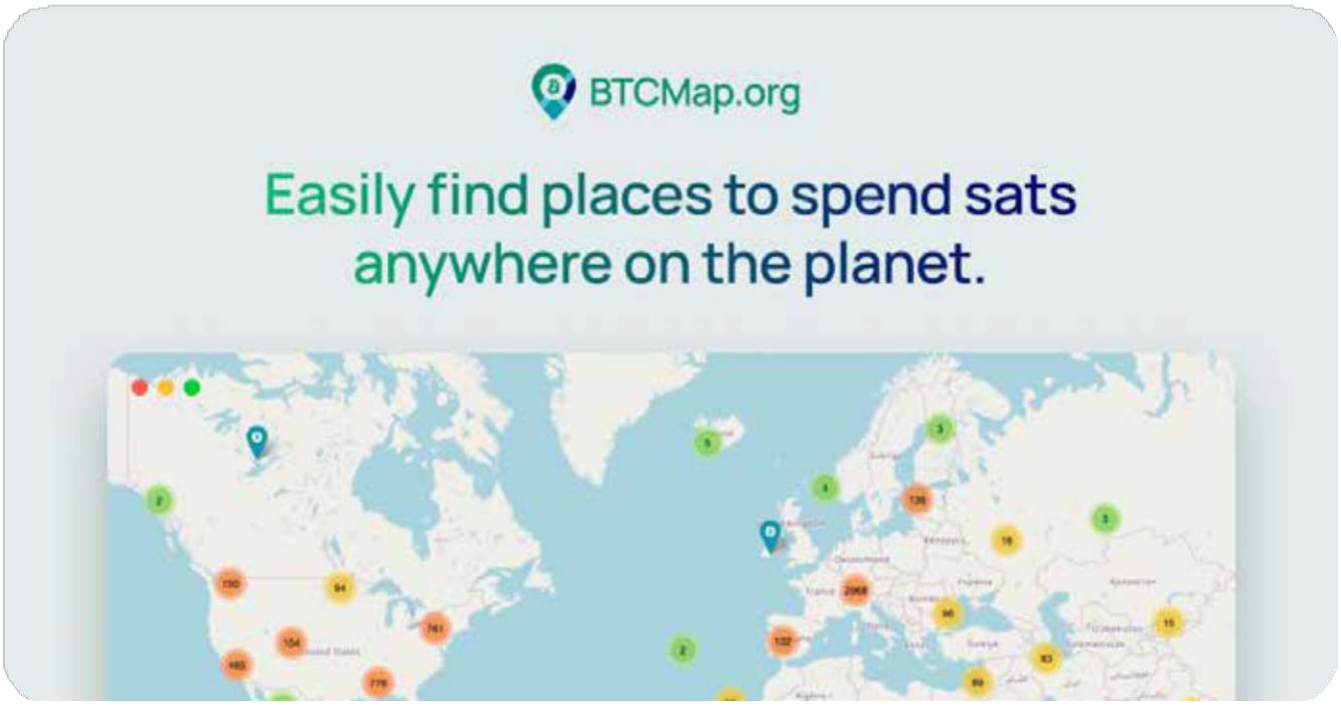
La Lightning Network consente alle economie circolari Bitcoin di prosperare in tutto il mondo grazie a un sistema di pagamento quasi istantaneo e a un'elevata velocità di trasferimento con transazioni in bitcoin a basso costo.

La prima economia circolare Bitcoin mai creata si trova ad Arnhem, nei Paesi Bassi. È stata creata molto prima che esistesse la Lightning Network, ma allora le commissioni on-chain erano davvero basse!

Il secondo è stato Bitcoin Beach, situato a El Zonte, El Salvador. Ha sfruttato la potenza della Lightning Network per fornire alla comunità, per lo più non bancaria, pagamenti digitali istantanei direttamente con i loro smartphone !

Oggi centinaia di economie circolari stanno nascendo in tutto il mondo, alimentate da Bitcoin, dalla Lightning Network e da risorse educative.

Su BTCMap.org potete anche cercare le comunità Bitcoin dove potrete incontrare altri utenti Bitcoin e trovare aziende che accettano Bitcoin. Alcuni dei nostri insegnanti e studenti hanno aggiunto imprese ed economie circolari a BTCmap.org e, una volta pronti, potrete farlo anche voi!



Risorsa: btcmap.org/communities

Al termine del Capitolo 8, avete acquisito informazioni sull'utilizzo di Bitcoin nella vostra vita quotidiana attraverso la Lightning Network. La Lightning Network rende le transazioni più rapide e accessibili, offrendo un'anteprima di come il Bitcoin continuerà a cambiare ed evolversi nei vari livelli.

Nel Capitolo 9 analizzeremo l'aspetto tecnico di Bitcoin. Dalla crittografia ai nodi, ai minatori e altro ancora, preparatevi a dare un'occhiata più da vicino a come funziona realmente Bitcoin.

Capitolo #9

Introduzione alla tecnica di Bitcoin

Libro di lavoro per studenti

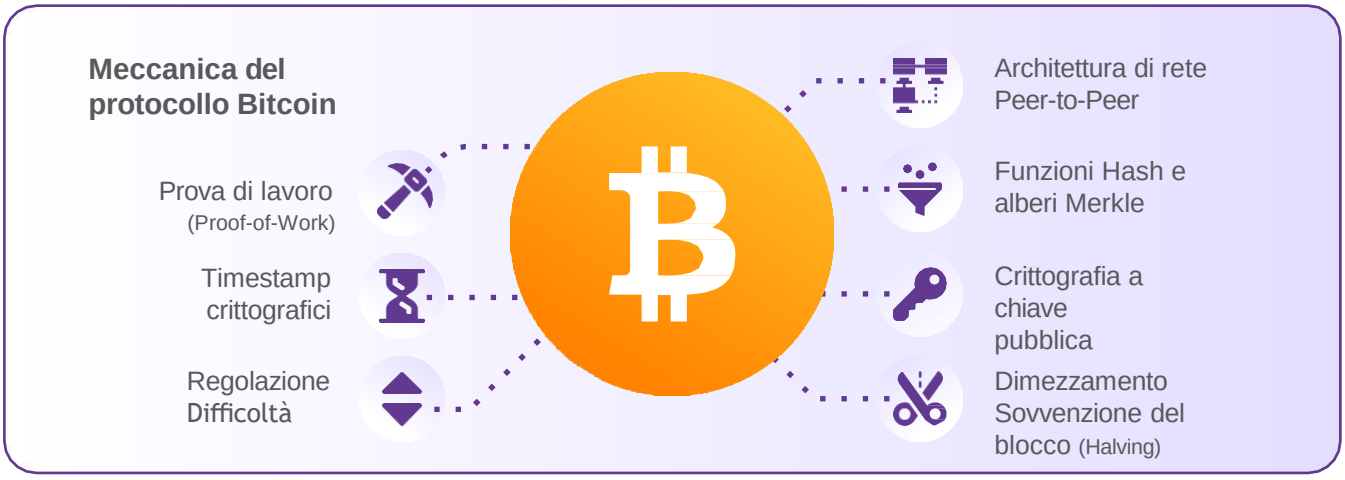
Versione italiana| 2025

Introduzione alla tecnica di Bitcoin

9.0 Introduzione

> Bitcoin non è "non regolamentato", è gestito dall'algoritmo matematico invece di essere controllato dalle burocrazie governative; non è corrotto.
>
> **Andreas M. Antonopoulos**

In questo capitolo esamineremo da vicino la tecnologia che consente alla rete Bitcoin di operare in modo completamente decentralizzato. Spiegheremo in termini semplici cosa succede quando si invia una transazione in bitcoin, come vengono elaborate le transazioni e cosa fanno i minatori e i nodi nella rete Bitcoin. In questo capitolo affronteremo alcuni concetti tecnici e impegnativi. Una cosa importante da ricordare: molte persone non capiscono come funziona Internet, eppure sono in grado di usarlo ogni giorno per inviare e-mail, contattare gli amici sui social media e persino pagare le bollette. Imparare l'aspetto tecnico del funzionamento del Bitcoin è un viaggio lungo che non tutti vogliono intraprendere, anche se decidono di usarlo come denaro. Sebbene vi incoraggiamo a continuare ad approfondire gli aspetti tecnici del Bitcoin, in questo capitolo ci concentreremo sui concetti chiave di base.



Se desiderate una comprensione tecnica più approfondita del funzionamento di Bitcoin, abbiamo incluso delle risorse nelle ultime pagine di questo libro di lavoro. Potete anche registrarvi sul nostro sito web per il Diploma Bitcoin-Edizione Tecnica per essere avvisati quando sarà pronto un corso più tecnico.

Vediamo un video che illustra il funzionamento della rete Bitcoin.

Attività: Guardare "Come funziona Bitcoin sotto il cofano".

https://youtu.be/Lx9zgZCMqXE

Come avete visto nel video, la rete Bitcoin è semplicemente un libro mastro o un registro delle transazioni memorizzato su più computer chiamati nodi. Il libro mastro di Bitcoin è pseudonimo, cioè non contiene dati personali, ma solo informazioni sulle transazioni e sugli indirizzi. Il libro mastro mostra ogni bitcoin e i suoi movimenti dall'inizio della rete, il 3 gennaio 2009.

Successivamente, daremo un'occhiata più da vicino alla tecnologia che rende possibile questo sistema.

9.1 Chiavi pubbliche e private: Sicurezza attraverso la crittografia

> Bitcoin ci offre una promessa concreta: il programma verrà eseguito esattamente come specificato.
>
> **Andreas M. Antonopoulos**

9.1.1 Crittografia Chiavi pubbliche/private

La crittografia è un modo per mantenere segrete le informazioni camuffandole in codice.

- La crittografia è il processo che consiste nel prendere le informazioni e trasformarle in un codice speciale, rendendole illeggibili a chiunque non disponga del metodo di decrittografia corretto. È come chiudere una cassaforte, dove solo chi possiede la chiave o la combinazione corretta può aprirla.
- La decrittazione, invece, è il processo che permette di prendere le informazioni criptate e renderle nuovamente leggibili, come sbloccare la cassaforte e poter leggere le informazioni al suo interno.

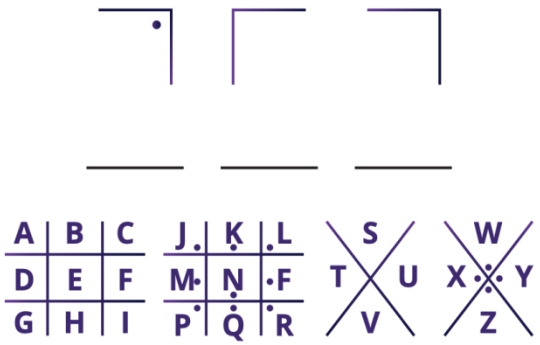
Per esempio, supponiamo che John voglia inviare ad Arel un messaggio segreto che non deve essere letto da nessun altro. I due decidono di utilizzare il metodo di crittografia Pigpen Cipher per mascherare il messaggio prima di inviarlo. Solo chi possiede il cifrario può decifrare il messaggio, rendendolo illeggibile per chiunque altro. Sebbene questo metodo non sia oggi considerato sicuro, illustra il principio della crittografia a chiave privata per l'invio di messaggi.

Come risolvere

Cifrario Pigpen

Quando si risolve il Cifrario di Pigpen, al giocatore viene dato un messaggio criptato e un cifrario. Per decifrare il messaggio, il giocatore deve trovare il simbolo del messaggio cifrato sul cifrario per trovare la lettera decifrata.

- Esempio di messaggio criptato:



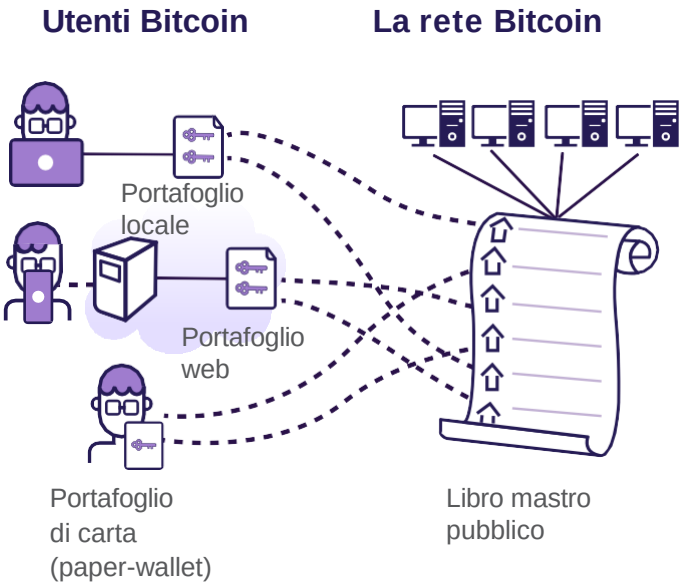
Come funziona la crittografia nelle transazioni in bitcoin?

Nella crittografia tradizionale a chiave privata, John e Arel dovrebbero innanzitutto condividere una chiave segreta, come una password o il cifrario Pigpen. John userebbe poi questa chiave per crittografare il suo messaggio prima di inviarlo ad Arel. Arel, che conosce la chiave segreta, userebbe la stessa chiave per decifrare il messaggio e leggerlo.

Tuttavia, se qualcun altro è in possesso della chiave e intercetta il messaggio, può decifrarlo e leggerlo.

Introduzione alla tecnica di Bitcoin

La **crittografia a chiave pubblica**, quella utilizzata nelle transazioni in bitcoin, ha risolto questo problema. Con la crittografia a chiave pubblica, John e Arel non hanno bisogno di condividere la password o il metodo di crittografia l'uno con l'altro. Invece, ciascuno di loro possiede due chiavi diverse: una **chiave pubblica** (che è sicuro condividere con chiunque) e una **chiave privata** (che deve essere mantenuta privata).



In questo caso quando John vuole inviare un messaggio ad Arel, può utilizzare la sua **chiave privata** per crittografare il proprio messaggio prima di inviarlo ad Arel. Quando Arel riceve il messaggio, solo lui è in grado di decifrarlo con la **chiave pubblica** di John. Chiunque altro, anche se intercettasse il messaggio, non sarebbe in grado di leggerlo. Anche le probabilità di rubare la chiave sono molto più basse, perché John e Arel non hanno bisogno di condividere la **chiave privata** tra loro.
Il vantaggio principale della crittografia a chiave pubblica rispetto a quella privata è che consente una comunicazione sicura senza che il mittente e il destinatario debbano condividere una chiave segreta (o un altro metodo di crittografia come il Pigpen Cipher), che potrebbe essere intercettata da terzi.

In Bitcoin, la crittografia a chiave pubblica non viene utilizzata per inviare messaggi criptati. Viene invece utilizzata per creare **firme digitali** uniche che rendono le transazioni in bitcoin immutabili. La **firma digitale** con **chiave privata** è un modo per dimostrare l'autenticità di una transazione bitcoin, simile a quando si scrive la propria firma su un documento fisico. Mentre chiunque può verificare la firma utilizzando la **chiave pubblica** che non può essere usata per firmare.

Crittografia a chiave pubblica (per ogni transazione tra due utenti):

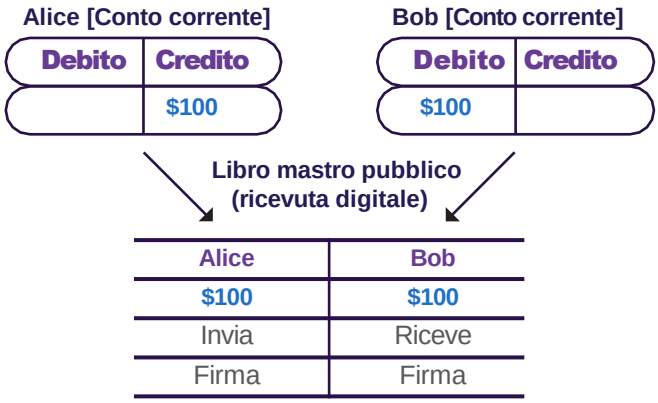
Ogni utente dispone di due chiavi: una **privata**, che viene **tenuta segreta**, e una **pubblica**, che può essere **condivisa con altri.**

La **chiave privata** serve come forma di identificazione e prova di proprietà, confermando: **"Questo indirizzo appartiene a me e ne ho il controllo".**

Le firme digitali vengono create per identificare transazioni uniche.

Firma digitale

- Le transazioni in bitcoin prevedono il trasferimento di una certa quantità di bitcoin direttamente sul conto di un'altra persona.
- La crittografia viene utilizzata per garantire che solo il vero detentore dei bitcoin ha il controllo di inviare il proprio denaro a qualcun altro. In questo modo si assicura che la proprietà sia protetta da attori malintenzionati.
- Come ulteriore misura di protezione, ogni transazione inviata in Bitcoin riceve automaticamente una **firma UNICA**. Questa **firma unica** è dotata di una tecnologia a prova di manomissione che aiuta la rete a verificare che sia stato il vero proprietario dei bitcoin, e non qualcun altro, ad inviarli.



Come funziona una vera transazione in bitcoin in termini semplici:

1. **Creazione della transazione:**

   Un utente avvia una transazione in bitcoin specificando dettagli come l'indirizzo del destinatario e l'importo in bitcoin da inviare.

2. **Generazione di firme digitali:**

   Il mittente genera una **firma digitale** unica utilizzando la propria **chiave privata**. Questa firma è un codice crittografico unico che verifica l'autenticità della transazione.

3. **Trasmissione della transazione:**

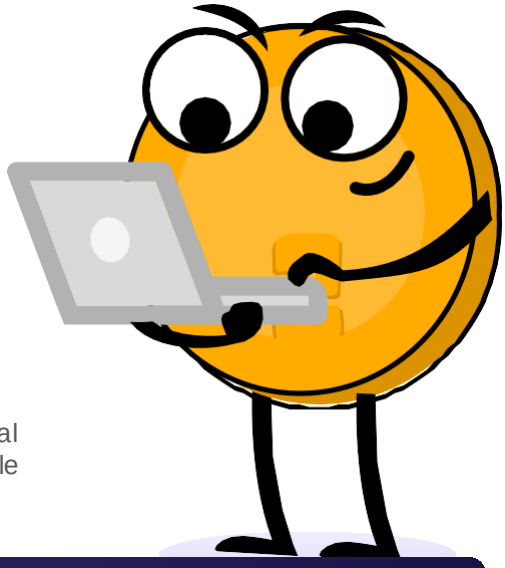
   La transazione firmata viene trasmessa alla rete Bitcoin, indicando l'intenzione di trasferire la proprietà dei bitcoin dal mittente al destinatario.

4. **Verifica in rete:**

   I nodi della rete Bitcoin ricevono la transazione e utilizzano la **chiave pubblica** del destinatario per decifrare e verificare l'integrità della transazione. Contemporaneamente, utilizzano la **chiave pubblica** del mittente per verificare la **firma digitale**.

5. **Configurazione sulla rete Bitcoin:**

   Se la verifica ha esito positivo, la transazione viene aggiunta al libro mastro, che funge da registro sicuro e trasparente di tutte le transazioni. Una volta confermata, la proprietà dei bitcoin viene ufficialmente trasferita dal mittente al destinatario.



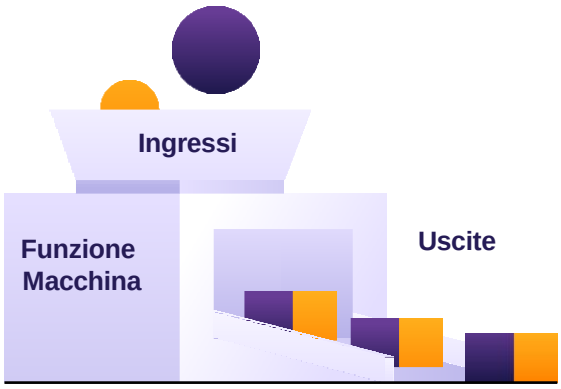
In sintesi, la firma digitale, creata con la chiave privata del mittente, serve come prova crittografica dell'autenticità e della proprietà, consentendo alla rete decentralizzata di Bitcoin di convalidare e registrare la transazione sul libro mastro.

9.1.2 Spiegazione dell'hashing

Non lasciatevi intimidire dai termini tecnici e dai concetti matematici. Siamo consapevoli che non tutti amano la matematica, ma potreste sorprendervi e vedere che anche le idee più complesse possono essere afferrate con un po' di impegno.

Che cos'è una funzione?

Una **funzione** è come una macchina che prende alcune informazioni e le trasforma in qualcosa di nuovo. Le informazioni fornite alla funzione sono chiamate **input.** Le nuove informazioni che la funzione crea sono chiamate **output.** Le funzioni aiutano i computer a svolgere compiti e a risolvere problemi.



Pensate a una ricetta per preparare un'insalata. La ricetta (o funzione) indica quali ingredienti usare e come mescolarli per ottenere l'insalata. Si possono mettere ingredienti diversi, ma la ricetta darà sempre come risultato l'insalata. Le funzioni possono essere utilizzate per rendere le cose più facili e più efficienti.

Questa ricetta è una funzione che prende gli ingredienti come elementi di **input** e genera come **output** l'insalata tagliata.

In bitcoin, le funzioni vengono utilizzate per eseguire le transazioni. Sappiamo già che le transazioni in bitcoin sono essenzialmente trasferimenti di valore (denaro) da un indirizzo a un altro. Per eseguire una transazione, vengono utilizzate diverse funzioni crittografiche per convalidare la transazione e aggiornare lo stato del libro mastro di Bitcoin.

Le funzioni utilizzate in una transazione bitcoin comprendono la verifica dell'autenticità degli input della transazione, il controllo che il mittente disponga di fondi sufficienti e l'aggiornamento dei saldi degli indirizzi interessati. Una volta verificata e aggiunta a un blocco del libro mastro, una transazione diventa parte del registro permanente di tutte le transazioni della rete.

Che cos'è una funzione unidirezionale?

Una funzione unidirezionale utilizza una serie di istruzioni per elaborare le informazioni e trasformarle in qualcosa di nuovo, come una ricetta di frullato trasforma gli ingredienti in una nuova bevanda. Ma, così come non si può smontare un frullato per riottenere gli ingredienti originali, non si può invertire la funzione unidirezionale per riottenere le informazioni originali.

La crittografia a chiave pubblica, di cui la **chiave pubblica** fa parte, si basa sull'uso di funzioni unidirezionali, che rendono difficile determinare la **chiave privata** dalla **chiave pubblica**. In teoria non è esattamente impossibile "scoprire" la **chiave privata** dalla **chiave pubblica**, ma è estremamente difficile farlo e richiederebbe una quantità spropositata di tempo e di potenza di calcolo per portare a termine questo compito.

Trovare una **chiave privata** da una **chiave pubblica** in Bitcoin è come cercare di trovare un ago in un pagliaio grande quanto un campo da calcio. L'ago rappresenta la **chiave privata** e il pagliaio tutte le possibili **chiavi private**.

Allo stesso modo, le funzioni unidirezionali sono progettate per essere irreversibili e non possono essere decifrate.

Che cos'è una funzione hash?

L'hashing è come un'impronta digitale per i dati. Si tratta di un processo che consiste nel prendere un messaggio digitale e trasformarlo in un codice a lunghezza fissa, che funge da identificatore unico.

Proprio come un'impronta digitale può identificare una persona, un hash può identificare un messaggio digitale. Gli hash sono utilizzati in molte applicazioni, tra cui le transazioni in bitcoin.

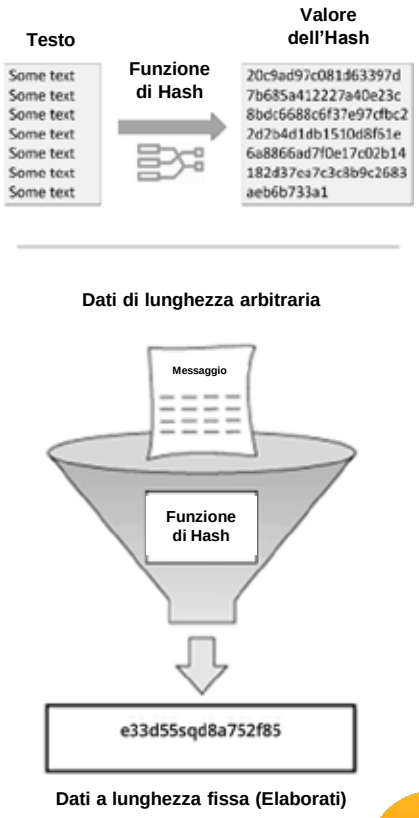
Come viene utilizzato l'hashing nelle transazioni in bitcoin

In Bitcoin, ogni transazione viene sottoposta a hash prima di essere aggiunta a un blocco del libro mastro. L'hash funge da firma per la transazione, verificando che la transazione sia valida e non sia stata manomessa. Se qualcuno cerca di cambiare anche una sola lettera della transazione, l'hash sarà completamente diverso, avvisando gli altri della modifica.

Il ruolo dell'hashing nella sicurezza

L'hash è essenziale per la sicurezza della rete Bitcoin. Utilizzando gli hash per identificare le transazioni, la rete può rilevare qualsiasi tentativo di modificare o manipolare una transazione. Questo aiuta a prevenire le frodi e a garantire che tutte le transazioni siano registrate accuratamente sul libro mastro.

Una funzione hash è un tipo di funzione unidirezionale che prende un input (denominato "messaggio" o "dati") e lo converte in una rappresentazione numerica denominata "hash". L'hash **in uscita** è unico rispetto ai dati in ingresso, quindi anche una piccola modifica dei dati **in ingresso** produce un hash completamente diverso.



Una funzione hash è come una macchina per codici segreti: prende un **messaggio** generico di qualsiasi lunghezza e lo trasforma in un codice a lunghezza fissa.

Introduzione alla tecnica di Bitcoin

Il codice appare sempre uguale per lo stesso messaggio. Se si cambia anche di poco il messaggio, il codice sarà completamente diverso. Questo aiuta i computer a ricordare le cose e a verificare se qualcosa è stato modificato.

Genera istantaneamente un hash SHA256 di qualsiasi stringa o valore di input. I codici Hash sono utilizzati come metodi unidirezionali.

Attività - Generare l'hash SHA 256 →

Il **risultato**, o hash, è sempre della stessa lunghezza, indipendentemente dalla lunghezza delle informazioni originali.

Bitcoin utilizza alcuni tipi specifici di funzione hash chiamati **SHA-256** e **RIPEMD160.** Di seguito sono riportati alcuni esempi:

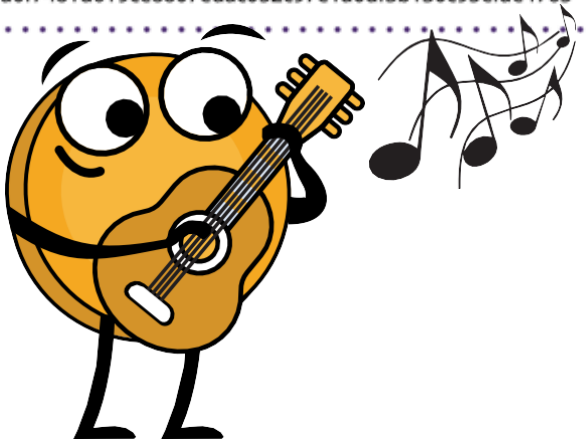
- Si noti che una piccola variazione del secondo ingresso cambia completamente l'uscita rispetto al primo.
- Il terzo ingresso è un enorme file, ma l'uscita ha la stessa lunghezza fissa degli altri due.

SHA256 hash of the string ***hello world***
B94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9

SHA256 hash of the string **hello world.**
7ddb227315f423250fc67f3be69c544628dffe41752af91c50ae0a9c49faeb87

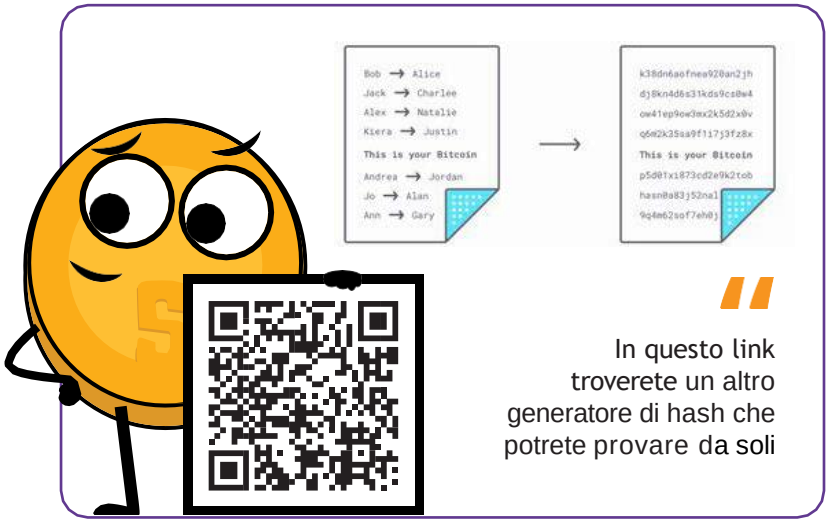
SHA256 hash of the downloadable iso file **Ubuntu 18.10**
7b9f670c749f797a0f7481d619ce8807edac052c97e1a0df3b130c95efae4765

L'hash può anche essere considerato come uno spartito musicale che cattura l'essenza di un brano. Proprio come uno spartito musicale è una rappresentazione unica di una melodia, un valore hash è una rappresentazione unica di un pezzo di dati. Confrontando la partitura di un brano musicale con l'esecuzione effettiva, un musicista può determinare se l'esecuzione è accurata. Allo stesso modo, confrontando il valore hash dei dati ricevuti con il valore hash originale, si può determinare se i dati sono stati alterati durante la trasmissione.



Proprio come una leggera deviazione in un'esecuzione musicale può provocare un suono diverso, anche la più piccola modifica ai dati originali si tradurrà in un valore di hash diverso. Questo rende l'hashing uno strumento potente per garantire l'integrità e l'autenticità di una transazione bitcoin.

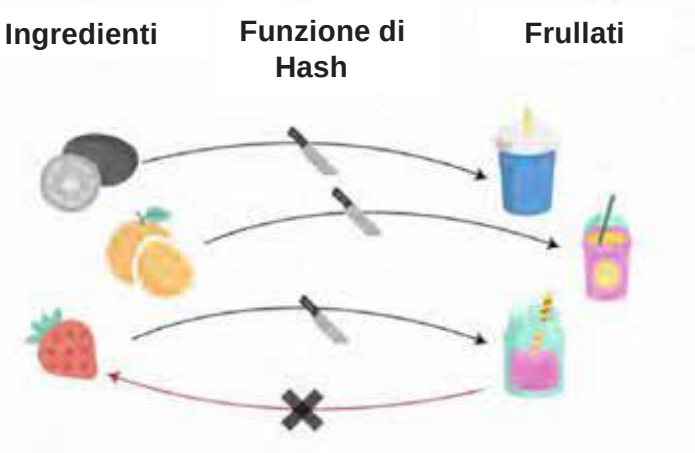
Il processo di codifica della **chiave pubblica** attraverso l'hashing viene utilizzato per migliorare la sicurezza delle informazioni convertendole in un formato a lunghezza fissa e illeggibile. Bitcoin utilizza gli algoritmi SHA-256 e Ripemd-160 per produrre indirizzi pubblici. Il risultato serve come identificatore unico per la **chiave pubblica** e contribuisce a garantire l'integrità e la sicurezza delle transazioni memorizzate nel libro mastro. Crittografando le informazioni in questa maniera diventa più difficile per le persone non autorizzate accedere e manipolare i dati.



In questo link troverete un altro generatore di hash che potrete provare da soli

Hashing

Una funzione di Hash riceve in ingresso qualsiasi valore e produce in uscita un codice a lunghezza fissa (Hash)



- **Deterministico.**
  Con gli stessi ingredienti si ottiene sempre lo stesso frullato (risultato).
- **Resistenza alla preimmagine.**
  Non si può incollare una fragola a un frullato.
- **Resistenza alla correlazione.**
  Cambiando un po' gli ingredienti si ottiene un un frullato completamente diverso.
- **Resistenza alle collisioni.**
  È difficile trovare ingredienti diversi per una frullati che hanno come risultato lo stesso identico.
- **Velocità e affidabilità.**
  Come gettare la frutta nel mixer: è veloce e il risultato è sicuramente un frullato.

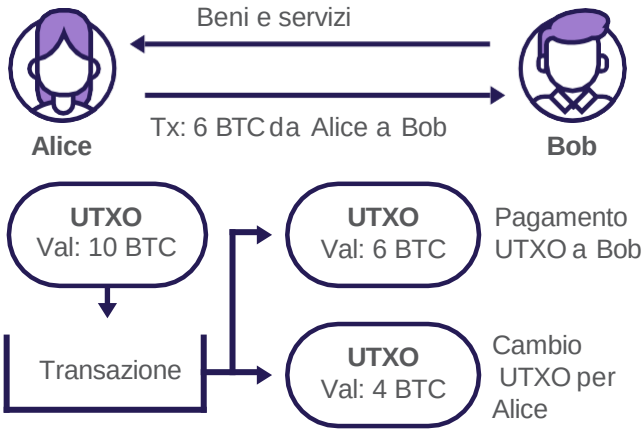
9.2 Il modello UTXO

UTXO - Uscita transazione non spesa

Introduzione alla tecnica di Bitcoin

Cosa sono gli UTXO?

In Bitcoin, le transazioni funzionano come la rottura di un pezzo d'oro più grande in pezzi più piccoli e l'invio di questi pezzi più piccoli sia ad altri che a se stessi.



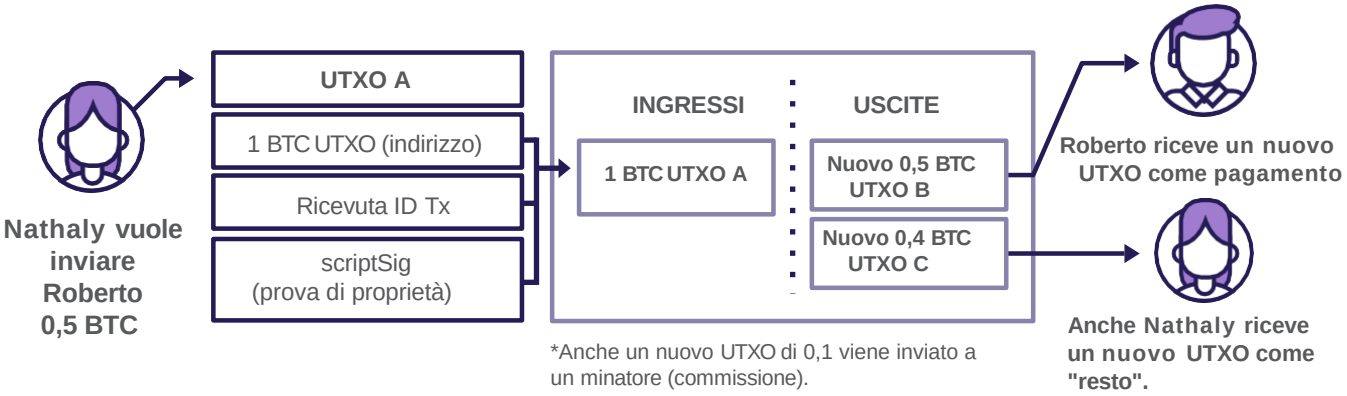
Si può pensare agli UTXO come a diverse dimensioni e pezzi di bitcoin o banconote di diverso taglio nel proprio portafoglio. Quando si spende un UTXO, questo viene ricreato in un nuovo UTXO per il destinatario, e ciò che rimane viene rispedito all'utente in un altro UTXO, noto come UTXO di "resto". È un pò come usare una banconota da 10 dollari per comprare due tazze di caffè a 6 dollari: il bar si tiene il pezzo da 10 dollari e vi dà 4 dollari di resto.

Quando si inviano bitcoin, si invia sempre l'intero importo di uno (o più) dei propri UTXO nel portafoglio Bitcoin. Cosa succede quindi ? Si invia una parte al destinatario e si riceve indietro l'importo rimanente come resto a uno dei propri nuovi indirizzi Bitcoin. Il resto ricevuto è chiamato output di transazione non speso, o UTXO, e può essere utilizzato come input per una nuova transazione futura.

Il saldo del vostro portafoglio Bitcoin è la somma di tutti i vostri UTXO. Quindi, la somma dei vostri UTXO è la somma della quantità di bitcoin posseduti.

È importante notare che **non si dovrebbe far conoscere ad altri** i propri UTXO, perché quando qualcuno li conosce, può tracciare le transazioni in bitcoin nella rete e in definitiva sapere quanto denaro si possiede.

In conclusione, ogni volta che si effettua una transazione, si utilizza uno o più UTXO esistenti per spendere bitcoin e si creano nuovi UTXO (sia per l'utente che per il destinatario).



*Anche un nuovo UTXO di 0,1 viene inviato a un minatore (commissione).

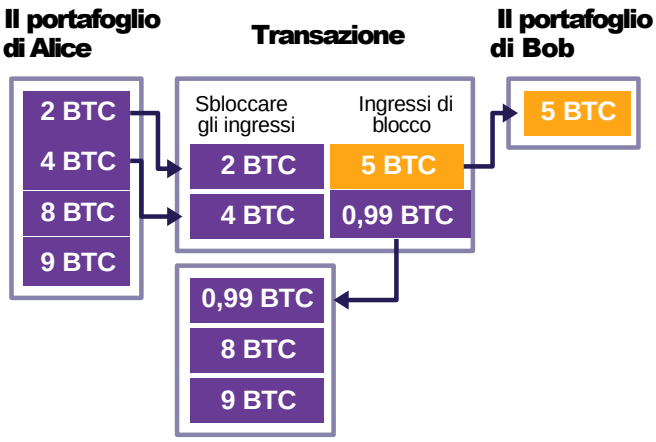
Quando viene effettuata una transazione, la quantità di bitcoin inviati viene suddivisa in più uscite, ciascuna delle quali è associata a un nuovo indirizzo Bitcoin (un nuovo UTXO).

Quando si inviano bitcoin a qualcuno, si utilizzano uno o più UTXO come fonte dei fondi (input). Questi UTXO saranno combinati, se necessario, per creare nuovi output che appartengono sia al destinatario della transazione che a voi stessi. Questi nuovi output, o UTXO, diventeranno di proprietà del destinatario e di vostra proprietà. Questi UTXO possono poi essere utilizzati come fonte di fondi in altre transazioni future. Questa catena di UTXO crea una storia trasparente e tracciabile di tutte le transazioni bitcoin sul libro mastro di Bitcoin, a partire dal primo blocco (3 gennaio 2009).

Un esempio per illustrare il funzionamento: se volete inviare due bitcoin ma avete solo un UTXO del valore di cinque bitcoin, la differenza di tre bitcoin vi viene restituita come resto. "Questo resto è un nuovo UTXO per voi, e potete spendere questo nuovo UTXO in una transazione futura.

Un altro esempio:

1. Alice vuole inviare a Bob cinque bitcoin.
2. Combina sei bitcoin da due dei suoi UTXO
3. Da questi UTXO, invia 5 bitcoin a Bob, riceve 0,99 bitcoin come resto e deve pagare una commiussione di transazione (fee) di 0,01.
4. Dopo la conferma, la transazione viene aggiunta al libro mastro di Bitcoin, aggiornando tutti i nodi che hanno una copia del libro mastro.



Se Alice tenta di utilizzare una delle sue uscite già spese per effettuare un'altra transazione, questa viene automaticamente rifiutata dai nodi. Questo perché i nodi mantengono una copia del libro mastro di Bitcoin (e di tutte le sue transazioni), quindi possono facilmente controllare il saldo degli UTXO di Alice e verificare che la transazione non sia valida.

Di seguito è riportata una schermata di una transazione reale in cui è presente un solo ingresso. Tuttavia, in un altro caso, il saldo iniziale potrebbe essere la somma di più UTXO (più ingressi). Quali osservazioni si possono fare quando si guardano le due transazioni qui sotto? Gli input corrispondono agli output? Potete descrivere i dettagli della transazione?

C'è un collegamento tra le due schermate?

E quale transazione si è verificata per prima?

9.3 Uno sguardo più da vicino ai nodi e ai minatori di Bitcoin

In questa sezione daremo uno sguardo più dettagliato a due parti (e soggetti) molto importanti della rete Bitcoin che sono state introdotte per la prima volta nel Capitolo 6. Analizzeremo:

1. **Nodi Bitcoin:**

   Controllori e validatori dei blocchi, il cui compito principale è quello di conservare una copia del libro mastro di Bitcoin, assicurandosi che tutte le transazioni siano valide e che tutti seguano le stesse regole.

   Distribuendo questo lavoro tra molte persone in tutto il mondo, Bitcoin rimane forte e saldo contro potenziali attacchi. Questi nodi aiutano a mantenere il sistema affidabile e fedele alla sua idea di decentralizzazione, in cui nessuna persona o gruppo ha troppo potere.

2. **Minatori di Bitcoin:**

   Architetti della sicurezza che utilizzano potenti computer ed energia elettrica per controllare e verificare le transazioni, assicurandosi che tutto sia sicuro. Questo lavoro contribuisce a rendere il libro mastro, o la blockchain, resistente ai malintenzionati che tentino di rovinare tutto.

Insieme, i nodi e i minatori Bitcoin lavorano come una squadra per mantenere un sistema decentralizzato, sicuro e forte, come un nuovo modo di gestire il denaro su cui le persone di tutto il mondo possono fare affidamento. Analizziamo questi ruoli in dettaglio per capire come contribuiscono all'innovativo sistema Bitcoin.

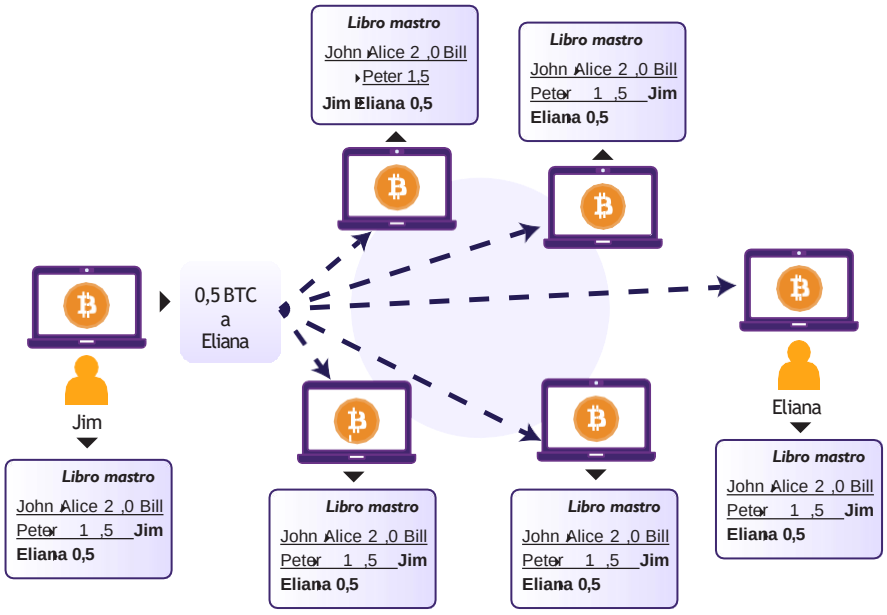
9.3.1 Cos'è un nodo Bitcoin e come si configura?

Un nodo Bitcoin può sembrare complicato, ma è semplicemente un un software che esegue una copia del libro mastro di Bitcoin.

Quando si gestisce un proprio nodo Bitcoin, si ha voce in capitolo nel definire le regole della rete Bitcoin.

Immaginate questo: se un gruppo di persone tenta di cambiare il funzionamento di Bitcoin, ad esempio alterando l'offerta totale di bitcoin, avete voce in capitolo.

Potete scegliere di non cambiare il vostro nodo con il nuovo sistema, il che è come votare per far rispettare le regole della rete che sostenete.



Immaginiamo un nodo Bitcoin come un poliziotto digitale con alcuni compiti essenziali:

1. **I guardiani della convalida:**
Un nodo Bitcoin conserva una copia digitale della blockchain, che è come un registro condiviso di tutte le transazioni bitcoin. Molti nodi in tutto il mondo detengono questo stesso registro.

2. **Hub di comunicazione:**
I nodi si connettono tra loro, creando una vasta rete di comunicazione. Condividono le informazioni, in particolare le transazioni in attesa di essere aggiunte alla blockchain, memorizzate in una sala d'attesa digitale chiamata "mempool".

3. **Controllore di qualità:**
Ogni aggiunta alla blockchain è sottoposta a un controllo. I nodi si assicurano che le transazioni siano valide, rifiutando quelle che non rispettano le regole della rete Bitcoin.

4. **Informatore Blockchain:**
Altri software, come i portafogli (wallet), possono chiedere a un nodo informazioni sulla blockchain, come i saldi dei bitcoin. I nodi fungono da centri di informazione.

5. **Accoglienza di un nuovo nodo:**
Quando un nuovo nodo vuole unirsi, i nodi esistenti forniscono generosamente una copia della blockchain. Il nuovo nodo controlla autonomamente la validità di ogni transazione, sottolineando un sistema privo di fiducia.

Attività:
Guardare il video sui nodi Bitcoin

Una delle opzioni per gestire il proprio nodo è scaricare il software Bitcoin Core e lasciargli il tempo di scaricare l'intera blockchain. Una volta pronto, lo si può lasciare acceso e, ogni 10 minuti circa, arrivano nuovi blocchi con transazioni. Il nodo controlla la loro validità e li aggiunge alla propria copia locale della blockchain.

Risorsa:
Software Bitcoin Core

La gestione di un nodo offre sovranità e indipendenza. Non si fa affidamento su altri; è il vostro corpo di polizia. A differenza del portafoglio Bitcoin, che non ha una copia della blockchain, un nodo garantisce l'autosufficienza. Invece di fidarsi degli altri per quanto riguarda i propri bitcoin (e lo stato della rete Bitcoin), il portafoglio comunica con il proprio nodo personale, rendendo la propria esperienza digitale più sicura e affidabile.

9.3.2. Cos'è un minatore di Bitcoin e come funziona l'estrazione?

> Lo scopo del mining non è la creazione di nuovi bitcoin, ma il sistema di incentivi. Il mining è il meccanismo con cui la sicurezza di Bitcoin è decentralizzata.
>
> **Andreas M. Antonopoulos**

Introduzione alla tecnica di Bitcoin

I minatori raccolgono le transazioni non confermate, formano un blocco e spendono energia per trovare un blocco valido di transazioni che **aggiungerà e proteggerà il blocco nella blockchain.**

I minatori sono in corsa per aggiungere il prossimo blocco alla blockchain. L'ambito premio è un "hash di blocco valido" abilmente nascosto tra miliardi di altri, e solo una chiave specifica assegnata dalla rete può sbloccarlo.

Immaginate un enorme pagliaio pieno di milioni di chiavi, ognuna delle quali rappresenta un hash di blocco unico. La rete ha scelto una chiave specifica per sbloccare una preziosa ricompensa. I minatori rovistano nel pagliaio, provando ogni chiave nella serratura, ma solo un minatore fortunato scoprirà la corrispondenza perfetta.

Una volta che un minatore trova l'hash corretto del blocco, lo condivide con la rete, insieme al blocco di nuove transazioni da lui creato. Gli altri minatori verificano la soluzione per assicurarsi che sia quella giusta. Se tutto è corretto, il blocco viene aggiunto alla blockchain, creando un registro pubblico e sicuro.

I minatori guadagnano ricompense per i loro sforzi in due modi:

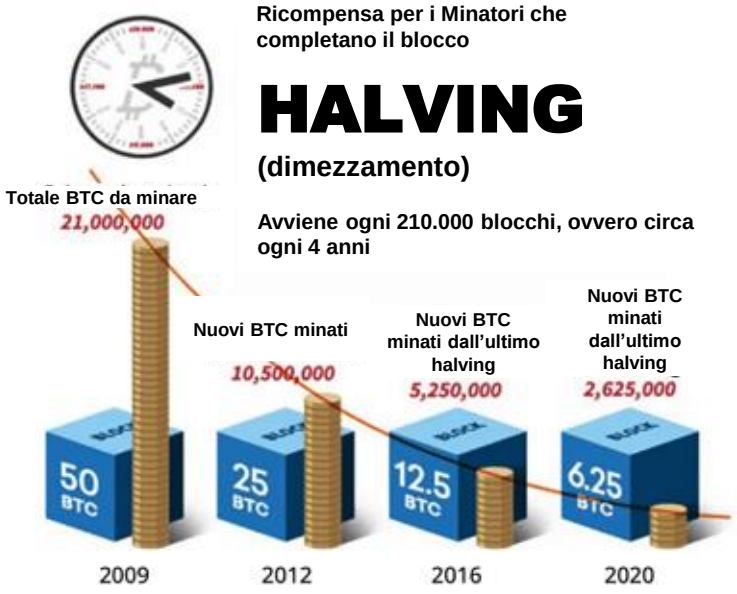
1. Ricompensa Blocco
2. Commissioni delle transazioni (fee)

I premi di blocco sono nuovi bitcoin immessi in circolazione ad ogni blocco aggiunto alla blockchain. Le commissioni di transazione sono piccoli pagamenti in bitcoin che gli utenti effettuano per far sì che le loro transazioni vengano elaborate più velocemente e con priorità dal miner. I minatori possono scegliere quali transazioni includere nel blocco che estraggono, dando solitamente la preferenza a quelle con commissioni di transazione più elevate.

Dimezzamento di Bitcoin (halving)

Il dimezzamento di bitcoin è una parte essenziale dell'universo Bitcoin che contribuisce a mantenerne la scarsità e il valore nel tempo. Come è noto, esiste una scorta fissa di 21.000.000 bitcoin in totale. Questa riserva non è completamente disponibile dal giorno del lancio del Bitcoin. Al contrario, questa fornitura entra nell'universo Bitcoin in modo graduale.

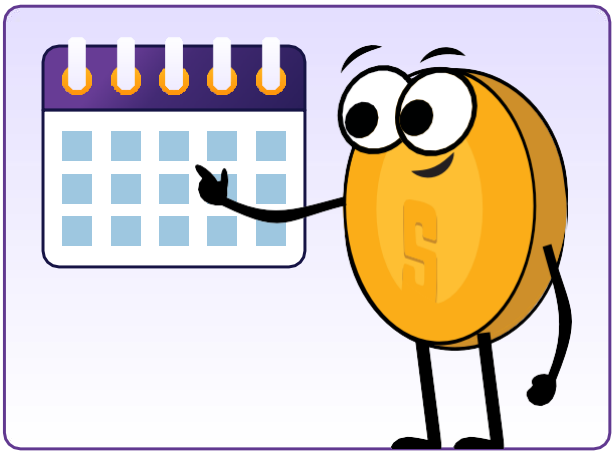
Satoshi Nakamoto ha progettato un sistema di ricompensa per blocchi per distribuire nuovi bitcoin senza un'autorità centrale. Agli albori del Bitcoin, i minatori ricevevano una ricompensa di 50 bitcoin per ogni blocco estratto, motivandoli ad investire in attrezzature potenti e in elettricità per le loro operazioni di mining.



Per mantenere la rete stabile e gestire l'offerta di nuovi bitcoin, la ricompensa dei blocchi viene dimezzata ogni 210.000 blocchi circa. Questo evento, chiamato "halving" (dimezzamento), diminuisce il numero di nuovi bitcoin che entrano in circolazione e continua a motivare i minatori a proteggere la rete e a sostenere la sua decentralizzazione. Storicamente, gli eventi di dimezzamento hanno portato a significativi aumenti di prezzo nel mercato dei Bitcoin a causa della riduzione dell'offerta di nuovi bitcoin in circolazione.

L'offerta circolante si riferisce alla quantità totale di una valuta. Nel caso del Bitcoin, l'offerta circolante totale è il numero di monete che sono state estratte e che sono in circolazione in un dato momento, escludendo le monete che sono andate perse per sempre.

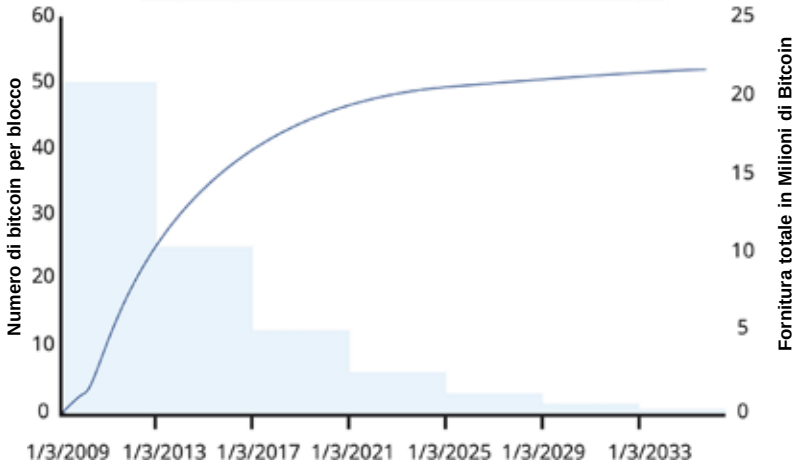
Durante ogni evento di dimezzamento, i minatori ricevono meno ricompense in bitcoin, il che riduce il tasso di emissione di nuove monete. La riduzione delle ricompense per il mining non implica necessariamente un minor guadagno per i minatori, che possono anche guadagnare commissioni di transazione per verificare le transazioni e aggiungerle alla blockchain, compensando così la diminuzione delle ricompense per il mining.
Gli eventi di dimezzamento sono pre-programmati nel protocollo Bitcoin, rendendo il programma di fornitura dei bitcoin prevedibile e trasparente.



Il **programma di fornitura di Bitcoin** è il piano predeterminato e pubblico per il rilascio di nuovi bitcoin in circolazione, progettato per mantenere la scarsità di Bitcoin nel tempo.

La seguente tabella illustra i dettagli dei prossimi eventi di dimezzamento per Bitcoin, tra cui la data prevista per il prossimo evento di dimezzamento, il numero di blocco in cui si verificherà l'evento di dimezzamento, le ricompense del blocco (per blocco estratto) durante l'evento di dimezzamento e la percentuale della fornitura totale che verrà estratta.

Previsione della produzione di Bitcoin



Evento	Data prevista	Blocco	Ricompensa del blocco	Percentuale estratta
Quarto dimezzamento	2024	840,000	3.125	96.875 %
Quinto dimezzamento	2028	1,050,000	1.5625	98.4375 %
Sesto dimezzamento	2032	1,260,000	0.78125	99.21875 %

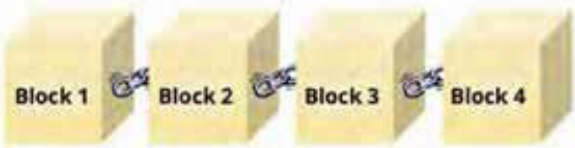
Introduzione alla tecnica di Bitcoin

Man mano che vengono estratti altri bitcoin, l'offerta in circolazione e la percentuale dell'offerta totale che è stata estratta continueranno ad aumentare fino a raggiungere l'offerta totale di 21.000.000. La riduzione dell'offerta, unita all'aumento della domanda, può far aumentare il prezzo del Bitcoin (misurato in dollari). Ciò favorisce gli early adopters e motiva i minatori a continuare a proteggere la rete e a contribuire con la loro potenza di calcolo e le loro risorse.

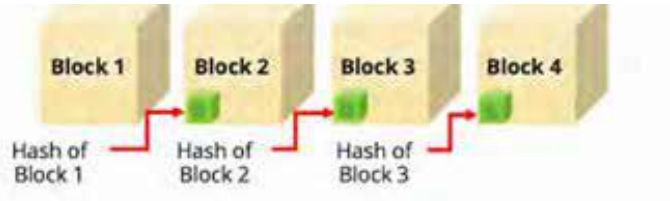
Bitcoin: percentuale di fornitura minata rispetto a 21M

Che cos'è un hash di blocco valido in Bitcoin?

In Bitcoin un hash di blocco valido è come un codice speciale che i minatori cercano di trovare. È un numero unico che aiuta a tenere traccia di ogni blocco nella blockchain che memorizza le informazioni sulle transazioni. I blocchi si collegano in una catena dal primo (blocco genesi) all'ultimo, creando una registrazione pubblica di tutte le transazioni. L'hash del blocco è fondamentale perché collega ogni blocco a quello precedente, rendendo facile per chiunque controllare la storia delle transazioni. È un po' come un'impronta digitale per ogni blocco, che garantisce la correttezza e la sicurezza delle informazioni; l'hash del blocco è un modo per verificare che i dati contenuti nel blocco non siano stati modificati.



I blocchi sono collegati tra loro da una relazione specifica. Ovvero un blocco contiene un'impronta digitale che è un valore di hash del blocco precedente. La funzione di hash può condensare un messaggio arbitrario (le informazioni del blocco) in una dimensione fissa (ad esempio 160 bit) e produce un'impronta digitale del messaggio.

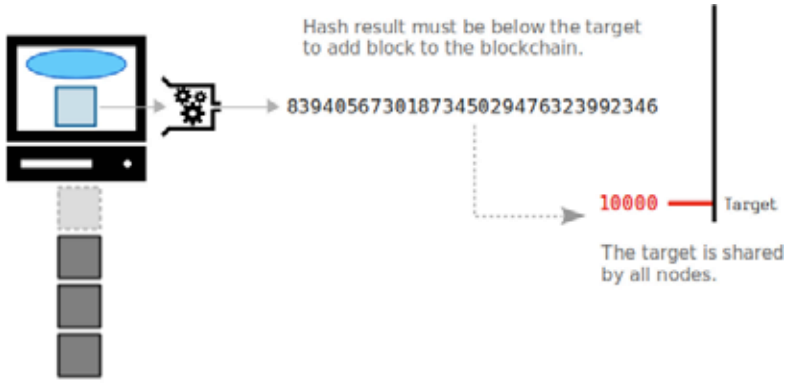


Satoshi Nakamoto, il creatore di Bitcoin, ha estratto il blocco iniziale, che conteneva un totale di 50 bitcoin.

La corsa per estrarre un blocco

I minatori si impegnano in una gara per scoprire l'hash del blocco che si allinea con l'obiettivo (un numero speciale) stabilito dalla rete. Il minatore che per primo riesce a scoprire l'hash corretto del blocco ha la possibilità di aggiungerlo alla blockchain e di assegnargli l'ID hash corrispondente. Questa soluzione serve a convalidare l'autenticità del blocco.

Il mining può essere paragonato a una gara in cui l'obiettivo è raggiungere il traguardo nel minor tempo possibile. Il grado di difficoltà nel trovare l'hash del blocco viene regolato periodicamente, assicurando che ogni blocco continui a essere estratto in circa 10 minuti (man mano che i minatori si aggiungono e se ne vanno). Questo meccanismo è chiamato "aggiustamento della difficoltà".



Supponiamo che il numero target stabilito dalla rete Bitcoin sia 1.000. I minatori dovrebbero usare la loro potenza di calcolo e la loro energia per cercare un hash di blocco (un numero specifico) inferiore a 1.000. Il primo minatore che trova un hash del blocco inferiore a 1.000 aggiunge il nuovo blocco alla blockchain e viene ricompensato con bitcoin.

Il livello di difficoltà nel mining di Bitcoin misura quanto sia difficile trovare un hash di blocco valido che soddisfi l'obiettivo fissato dalla rete. Viene regolato ogni 2016 blocchi, o all'incirca ogni due settimane, per garantire che i blocchi vengano aggiunti alla blockchain a un ritmo costante. Il livello di difficoltà è espresso come numero e più alto è il livello di difficoltà, più è difficile trovare un hash di blocco valido.

Ad esempio, consideriamo due hash diversi:

- **Hash 1:** 0000A1mINgF0RbL0cK5wItHth3hAy5tAcK
  Livello di difficoltà: 1
- **Hash 2:** 000000A1mINgF0RbL0cK5wItHth3hAy5tAcK
  Livello di difficoltà: 2

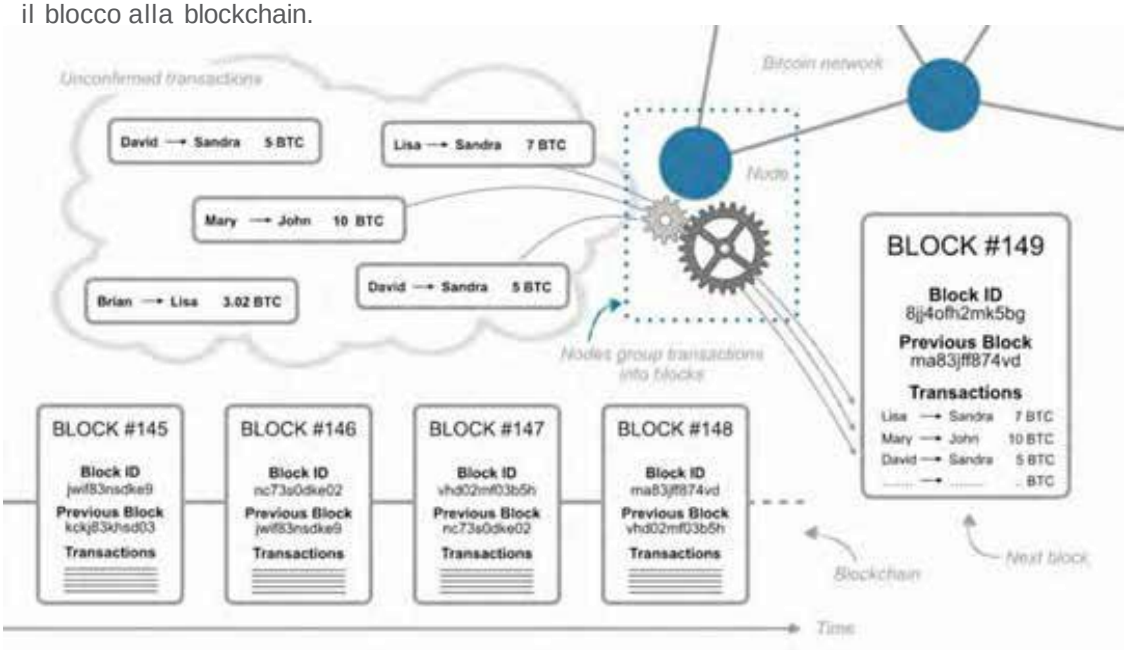
In questo esempio l'hash 2 ha un livello di difficoltà più alto rispetto all'hash 1 perché è un hash con più zeri all'inizio. Per i minatori sarebbe più difficile trovare l'hash 2 ripetto all'hash 1 perché i loro computer dovrebbero fare più lavoro.

Trovando un hash di blocco valido, un miner dimostra di aver svolto il lavoro necessario per aggiungere il nuovo blocco alla blockchain e riceve una ricompensa in bitcoin, più le commissioni di transazione, per il suo sforzo. Il Proof-of-Work (PoW) è il metodo utilizzato dalla rete Bitcoin per convalidare le transazioni e aggiungere nuovi blocchi alla blockchain.

Il PoW mantiene il Bitcoin sicuro rendendo difficile per chiunque abbia intenzioni malevole prenderne il controllo.

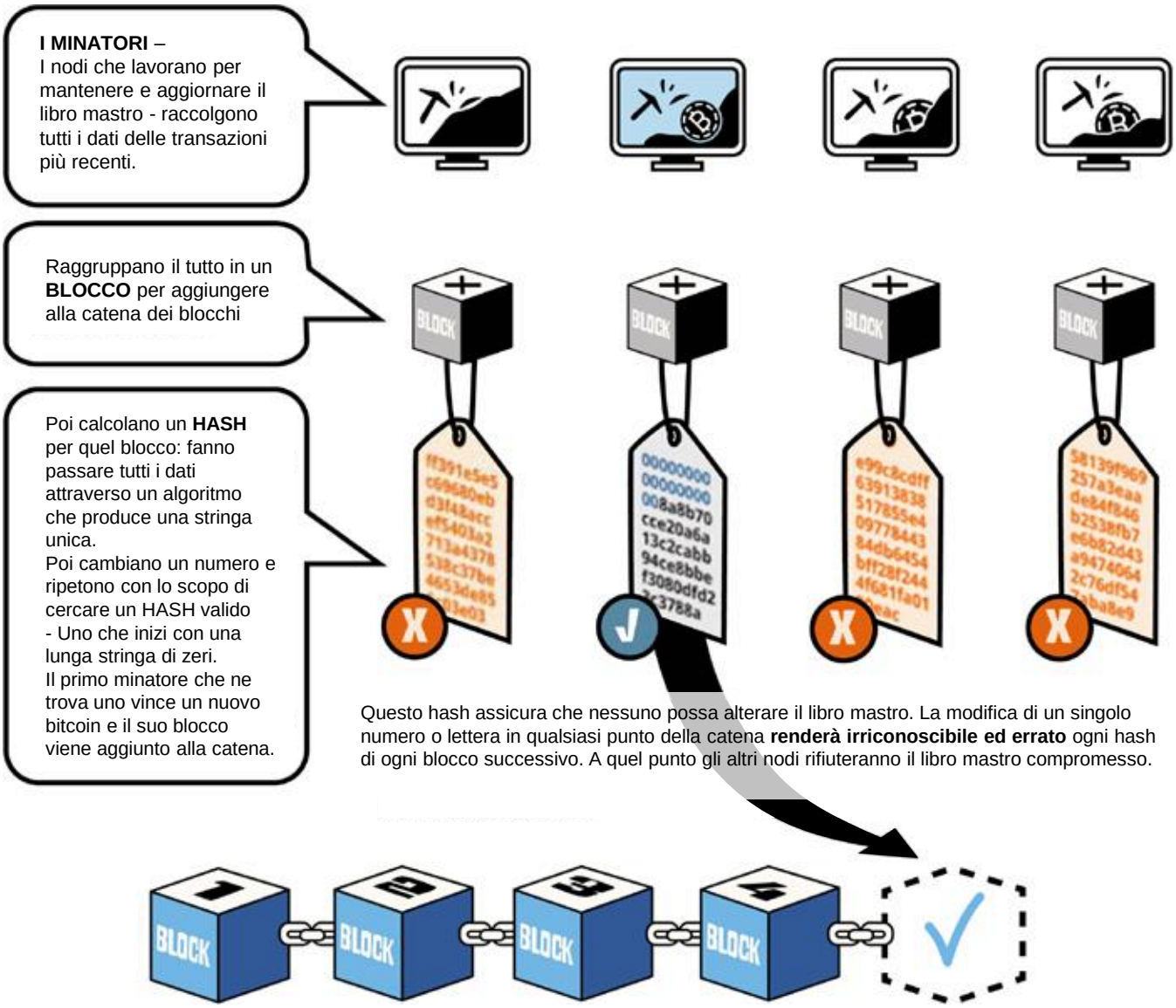
In sintesi, i compiti dei minatori consistono in:

1. **Accorpamento delle transazioni in blocchi:**
   Mentre i nodi verificano le transazioni appena create che sono in attesa nel "Mempool", i minatori selezionano un sottoinsieme di queste da includere nel loro blocco candidato.
2. **Prova di lavoro (PoW):**
   I minatori fanno a gara per trovare l'hash del blocco valido.
3. **Trasmissione di blocchi validi:**
   Dopo aver individuato il blockhash valido, propagano il nuovo blocco alla rete.
4. **Guadagnare premi:**
   Infine, ricevono i bitcoin appena creati e le commissioni di transazione per aver aggiunto con successo il blocco alla blockchain.



Più minatori possono lavorare contemporaneamente alla creazione di nuovi blocchi. Il primo minatore che scopre un hash del blocco che soddisfa l'obiettivo fissato dalla rete lo annuncia alla rete stessa; gli altri minatori controllano quindi le transazioni nel blocco candidato di quel minatore per assicurarsi che siano valide. Se le transazioni sono valide, il blocco viene aggiunto alla blockchain. Gli altri blocchi creati dagli altri minatori in quel momento non vengono aggiunti e vengono scartati. Questo processo contribuisce a mantenere il consenso all'interno della rete e a evitare che ci sia una doppia spesa.

Un blocco candidato è un insieme di transazioni considerate per l'aggiunta alla blockchain ma non ancora aggiunte.



9.4 Che cos'è la Mempool?

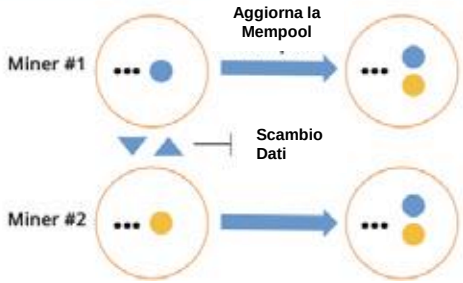
La "Mempool" o Pool (letteralmente “piscina” intesa come zona) di memoria è come una sala d'attesa per le transazioni nella rete Bitcoin. Quando si effettua una transazione, questa viene trasmessa alla Mempool prima di essere verificata, selezionata e aggiunta alla blockchain.

Immaginate di essere in fila in un ristorante. Il vostro nome viene aggiunto a un elenco di persone in attesa di un tavolo. Quando si libera un tavolo, il padrone di casa chiama il vostro nome e vi fa accomodare. Allo stesso modo, una transazione in bitcoin viene aggiunta alla Mempool quando viene effettuata e viene confermata e aggiunta alla blockchain quando un miner la include in un blocco. Nella mempool, l’ordine di scelta peró non é temporale, ma in ordine di valore delle commissioni dalla piú alta alla piú bassa, quindi le transazioni con commissioni piú alte passano davanti alle transazioni con commissioni inferiori, ovvero saranno scelte prima.

La mempool é dove le transazioni rimangono in attesa di essere incluse in un blocco per essere confermate.

Quando un nodo riceve per la prima volta una transazione da un peer, deve verificare che la transazione sia legittima. Nessuno vuole transazioni errate o ingannevoli.

La **sincronizzazione della mempool** consente ai nodi di condividere le proprie transazioni con altri nodi inviando un messaggio contenente una lista di transazioni verificate nella mempool.



La funzione principale della **mempool** é di :

1. Trasmettere le transazioni non confermate

2. Fornisce ai minatori le transazioni da minare.

Accettare le transazioni nella mempool comporta le seguenti attività:

- Ho già questa transazione?
- C'è un conflitto con un'altra transazione presente nella mempool?
- I **bitcoin** in ingresso sono sufficienti per i **bitcoin** in uscita?
- Le firme dimostrano che le uscite precedenti possono essere spese?
- **Ci sono commissioni sufficienti ?**

Come vengono verificate le transazioni e aggiunte alla Mempool?

Quando nuove transazioni vengono trasmesse alla rete Bitcoin, i nodi le verificano per assicurarsi che siano valide e che i fondi non siano stati spesi in precedenza. Una volta verificate le transazioni, i nodi le aggiungono alla loro Mempool. I nodi condivideranno poi le transazioni con altri nodi per effettuare una doppia verifica. Infine, se la maggioranza dei nodi è d'accordo, le transazioni vengono rese disponibili ai minatori per essere selezionate e inserite in un blocco.

Tuttavia, ci sono diverse ragioni per cui una transazione potrebbe non essere confermata dopo 72 ore:

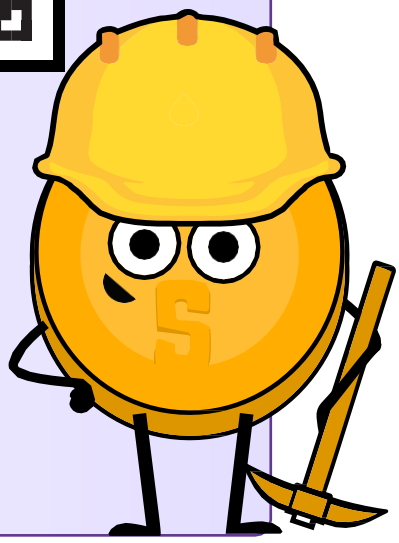
1. **Basse commissioni di transazione:**
   Le transazioni con una commissione (fee) bassa potrebbero non essere elaborate abbastanza velocemente, poiché i minatori sono più propensi a scegliere le transazioni con tariffe più elevate da includere nei loro blocchi.
2. **Congestione della rete:**
   Se la rete è congestionata, può verificarsi un ritardo nella accettazione delle transazioni, anche se queste hanno un costo elevato.
3. **Tentativo di doppia spesa:**
   Se un utente malintenzionato tenta di spendere due volte, la sua transazione viene rifiutata dalla rete.
4. **Dati errati o incompleti:**
   Se una transazione contiene dati errati o incompleti, sarà rifiutata dalla rete.
5. **Transazione non corretta:**
   Se una transazione non é corretta, è rifiutata dalla rete.

Per evitare che le transazioni vengano rifiutate, si consiglia di includere una commissione sufficientemente alta per garantire che la transazione venga elaborata in modo tempestivo e di controllare due volte che tutti i dati della transazione siano corretti prima di inviarla.

Attività: Mempool

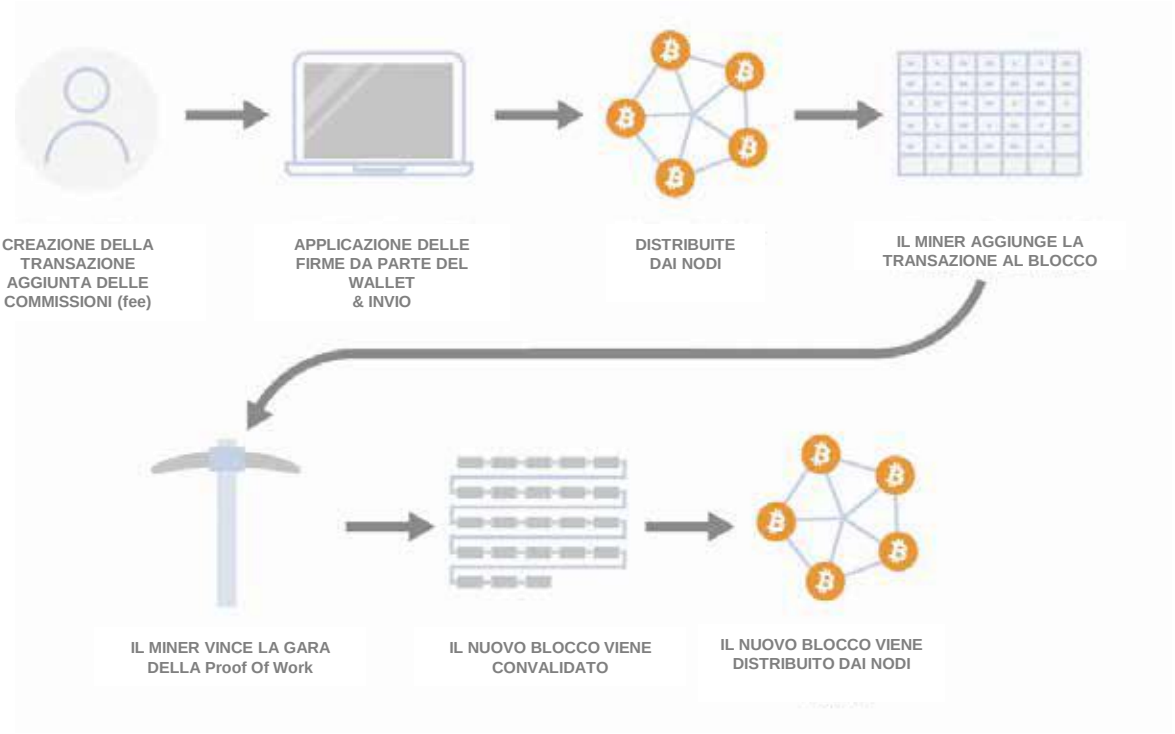
1. Scansionate il seguente **codice QR:**
2. Esaminare i vari elementi visualizzati sulla pagina, tra cui i blocchi più recenti, le transazioni concluse, il numero di transazioni, l'utilizzo della memoria e il valore approssimativo dell'intero blocco. Rispondere alle domande:

- Qual'è stato l'ultimo blocco estratto?
- Quante transazioni sono state incluse in quel blocco?
- Qual'è il valore totale scambiato in bitcoin?
- Qual'era la dimensione in megabyte del blocco?
- Con quanti zeri inizia il nonce del blocco?
- Quanti bitcoin ha guadagnato il miner in totale?
- Qual'è il valore totale delle commissioni ricevute dal miner per l'aggiunta delle transazioni alla rete?
- Scegliere una delle transazioni di valore più elevato del blocco. A quanti indirizzi Bitcoin è stato distribuito l'importo?



9.5 Come funzionano le transazioni Bitcoin dall'inizio alla fine

1. Adam vuole inviare bitcoin a Gerardo. Sceglie uno dei suoi UTXO, crea una transazione e aggiunge tutti i dettagli necessari, tra cui la quantità di bitcoin che vuole inviare, l'indirizzo di Gerardo per la ricezione e un importo superiore alla media delle commissioni di transazione.
2. Dopo un controllo finale per verificare che tutti i dettagli siano corretti, Adam utilizza la sua chiave privata per firmare la transazione.
3. Adam trasmette la transazione alla rete Bitcoin.



Da: Stevenot, Ted, "Cos'è un nodo bitcoin e come funziona?". Unchained Capital, 17, gennaio, 2023, https://unchained.com/blog/what-is-a-bitcoin-node/

4. I nodi della rete ricevono la transazione e ne verificano la validità in base alle regole del consenso (ad esempio controllando se la firma di Adam è valida e se ha fondi sufficienti per effettuare la transazione).
5. La transazione viene contrassegnata come valida e i nodi la propagano ad altri nodi della rete, aggiungendola alla Mempool.
6. Poiché Adam ha scelto una tariffa di transazione abbastanza alta, quasi tutti i minatori includono la sua transazione nei loro blocchi.

7. Proof-of-Work: I minatori fanno a gara e cercano di estrarre il loro blocco trovando l'hash del blocco valido. Uno dei minatori trova l'hash e trasmette il blocco alla rete.

8. I nodi ricevono il blocco appena estratto e ne verificano la validità. Questo include la convalida di tutte le transazioni all'interno del blocco e la garanzia che il requisito della Proof-of-Work sia soddisfatto.

9. La maggioranza dei nodi concorda sulla validità del blocco e lo aggiunge alla blockchain. Gerardo riceve i bitcoin inviati al suo indirizzo di ricezione.

10. Man mano che altri blocchi vengono aggiunti alla blockchain nell'ora successiva, il numero di conferme della transazione cresce. Con l'aumentare del numero di conferme della transazione, Gerardo acquisisce maggiore confidenza nel suo successo e nella sua natura irreversibile.

In sintesi, il mittente firma la transazione con la propria chiave privata, i nodi verificano gli UTXO della transazione e i minatori aggiungono la transazione verificata alla blockchain. Il destinatario può quindi accedere ai bitcoin utilizzando la propria chiave privata. Una volta che un blocco è stato estratto, tutte le transazioni in esso incluse sono considerate concluse e gli UTXO utilizzati come input in queste transazioni sono considerati esauriti e non saranno più utilizzati.

Con la conclusione di questo capitolo, avete acquisito preziose nozioni sui concetti fondamentali del funzionamento di Bitcoin. Abbiamo affrontato aspetti essenziali, dalle basi del denaro all'aspetto tecnico della tecnologia Bitcoin. Nel prossimo capitolo, faremo il punto della situazione. Il capitolo 10 ci aspetta, dove approfondiremo la domanda più importante: "Perché Bitcoin ?".

Capitolo #10

Perché Bitcoin?

Libro di lavoro per studenti

Versione italiana| 2025

Perché Bitcoin?

> Bitcoin è molto più di una moneta; è una rivoluzione che restituisce il potere al popolo, offrendo una un sapore di pace e libertà in un mondo affamato di potenziamento.
>
> **Il mio primo Bitcoin**

In questo capitolo conclusivo, riassumeremo le lezioni apprese durante il nostro viaggio, porremo e discuteremo alcune domande importanti ed esploreremo il futuro di Bitcoin.

Bitcoin non è solo una tecnologia, ma un tipo di rete che alimenta una nuova forma di denaro la cui offerta non può essere modificata da nessun singolo soggetto. L'umanità non ha mai avuto una forma di denaro con un'offerta fissa e senza controllo centralizzato. Se adottato su larga scala, Bitcoin è uno strumento che sblocca un movimento di cambiamento positivo che può trasformare la vita delle persone in tutto il mondo. Rappresenta una rivoluzione pacifica verso la libertà collettiva e l'equità, aprendo nuove opportunità per l'umanità grazie alla creazione di un sistema monetario globale e condiviso.

Come sistema globale decentralizzato, Bitcoin consente una maggiore libertà finanziaria, spostando il potere da pochi a molti. Fornisce una piattaforma sicura e resistente alla censura per l'archiviazione e il trasferimento di valore, consentendo agli individui di assumere il controllo della propria ricchezza e di proteggere il proprio potere d'acquisto. Questo è particolarmente importante nell'attuale clima di incertezza economica, in cui il sistema finanziario tradizionale sta affrontando sfide senza precedenti.

Attività: Guardare il video

Le possibilità di cambiamento positivo sono immense, per questo vi invitiamo a guardare questo video per saperne di più.

In seguito, esamineremo un'altra forma di valuta digitale, denominata Central Bank Digital Currency (CBDC) e valuteremo gli aspetti che le differiscono o le accomunano a Bitcoin.

10.1 Cosa sono le valute digitali delle banche centrali (CBDC) e chi le controlla ?

Le Central Bank Digital Currencies, o CBDC, sono versioni digitali della normale moneta elettronica. Le CBDC seguono le stesse regole della moneta normale, dove un'autorità centrale, come il governo, può creare più offerta e quindi ridurre il potere d'acquisto dei cittadini. Tuttavia, le CBDC forniscono ai governi nuovi e potenti strumenti per controllare l'utilizzo di tale denaro da parte dei cittadini di tutto il mondo.

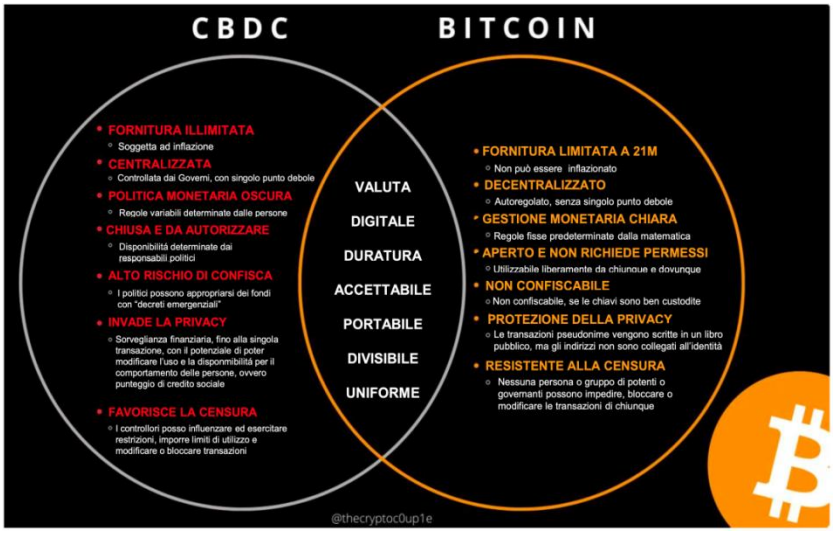
Secondo una ricerca della Human Rights Foundation (HRF), 119 dei 193 governi di tutto il mondo stanno studiando, testando o utilizzando le CBDC.

Potete verificare se il vostro Paese sta sperimentando i CBDC sul tracker CBDC della Fondazione per i Diritti Umani all'indirizzo **https://cbdctracker.hrf.org/home o https://cbdctracker.org/.**

Quindi, cosa rende le CBDC differenti rispetto alla normale moneta di conto, oltre al fatto di essere digitali? È fondamentale capire che, a differenza del normale denaro liquido sotto forma di carta o monete, le CBDC consentono al governo di controllare digitalmente i titoli di credito. E controllare ogni transazione a livello globale. Ciò significa che il governo può bloccare alcune transazioni o addirittura congelare l'intero conto nel caso in cui reputi l'utente sospetto o dubbio il modo in cui utilizzi il proprio denaro.

Per esempio, immaginate di voler inviare denaro a un familiare che ha bisogno di aiuto, e che si trovi all'estero. Il vostro governo locale potrebbe rifiutare la transazione perché è in conflitto con i leader del Paese dove si trova il vostro famigliare. Oppure immaginate di andare al negozio per comprare qualcosa che vi piace, ma di non poterlo fare perché avete espresso la vostra opinione, contraria al governo, sui social media.

Le CBDC danno ai governi il potere illimitato di controllare l'uso del denaro in tutto il mondo, limitando la capacità degli individui di spendere il denaro in base alle proprie scelte. Alcuni sostengono addirittura che le CBDC consentirebbero ai governi potenti di imporre a livello centrale politiche tirranniche su scala globale con il semplice tocco di un interruttore, senza la necessità di agenti umani incaricati dell'applicazione.



Sia le CBDC che il Bitcoin sono digitali, ma al di là di questa comunanza, rappresentano forme di denaro molto diverse con filosofie distinte, che portano a risultati molto diversi per l'umanità.

10.2 La filosofia di Bitcoin

Nei capitoli 6 e 9 abbiamo scoperto che i singoli individui che gestiscono un nodo contribuiscono a mantenere sicure le regole di Bitcoin. Si tratta di una cosa importante perché, per la prima volta, persone come noi possono far parte di un team che garantisce la protezione delle regole del nostro sistema monetario. Queste regole includono il fatto che c'è solo una quantità limitata di denaro e che nessuna singola parte può cambiare queste regole. È un'opportunità unica per le persone normali di contribuire a mantenere il nostro denaro sicuro e affidabile.

La filosofia di Bitcoin riguarda il potenziamento, la libertà, l'indipendenza finanziaria, il pensiero critico e il concetto che tutti noi dovremmo avere voce in capitolo sulle regole del sistema che scegliamo per noi stessi. A differenza del sistema monetario controllato da potenti partiti centrali, Bitcoin funziona su una rete in cui nessun singolo partito ha il controllo. Ciò significa che, a differenza di altri tipi di denaro come le CBDC, nessuno può privarvi della vostra proprietà o impedirvi di spendere il vostro denaro come volete.

Nel mondo finanziario, avere più ricchezza significa avere più influenza e controllo. Al contrario, Bitcoin opera in un modo tale da basarsi sul potere delle persone. È come un team in cui ognuno, indipendentemente dalla quantità di denaro che possiede, gioca un ruolo cruciale nel sistema. Immaginatelo come una forza collettiva, dove le vostre dimensioni finanziarie non significano automaticamente il controllo di tutto. Bitcoin è costruito su regole immutabili e, in questa armonia, è come se l'umanità stessa avesse il controllo del sistema. Non sono pochi pezzi grossi a comandare; siamo tutti noi a lavorare insieme, come una comunità resiliente, che guida il corso di Bitcoin senza che una singola autorità gli dica cosa fare.

Mentre nel sistema fiat sono i potenti a dettare le regole, nell'ecosistema Bitcoin è la forza collettiva degli individui a sostenere la rete. Nessuna singola entità, indipendentemente dalla ricchezza, può dettare il percorso dell'ecosistema Bitcoin. Si tratta di un'inversione della tradizionale dinamica del potere, in cui la resistenza del sistema non è nelle mani di pochi ma nel potere collettivo di ogni partecipante.

L'idea principale è quella di creare un sistema sicuro, chiaro ed equo in cui tutti possano accedere al denaro globale in modo paritario.

Attività: Discussione in classe - Avete il diritto di controllare il vostro denaro?

1. Il denaro è una necessità e un diritto umano? E perché?
2. Se non potete spendere i vostri soldi come volete, inviarli a chi volete o portarli con voi in un nuovo Paese, sono davvero vostri? E perché?
3. Perché il baratto ha smesso di essere utilizzato? Qual è il problema della doppia coincidenza dei desideri?
4. Qual è stato l'evento storico di maggior impatto per voi? Perché è importante capire lo shock di Nixon e la sua rilevanza per tutti i giorni nostri?
5. In che modo la moneta con un'offerta fissa è diversa dalle valute tradizionali?

6. Quando è stato creato Bitcoin, da chi, per quale scopo e in che modo questo scopo ha definito la concetto di sistema decentralizzato?
7. Qual è la differenza tra un portafoglio con e senza custodia ? Qual è il vostro portafoglio preferito ?
8. Cosa sapete della rete Lightning? Per quale tipo di transazioni la utilizzereste ?
9. Perché la gestione del proprio nodo supporta la rete ?
10. In che modo il controllo del proprio denaro vi dà potere nella vita quotidiana e nella pianificazione del futuro?
11. In che modo la libertà finanziaria può migliorare la vostra capacità di contribuire positivamente alla vostra comunità o società?

10.3 I vantaggi di Bitcoin

L'"iperbitcoinizzazione" è un futuro teorico in cui il Bitcoin diventa il sistema monetario globale dominante. Ciò significherebbe che il Bitcoin verrebbe utilizzato da tutti, ovunque e per qualsiasi cosa, dall'acquisto di caffé al pagamento di bollette e persino all'acquisto di proprietà.

Il crescente interesse per il Bitcoin da parte di individui, aziende, Paesi e governi evidenzia il potenziale impatto della sua adozione diffusa sull'economia e sulla società. Ecco alcuni dei benefici di un mondo iperbitcoinizzato:

1. **Un futuro auto-sovrano:**

   Un futuro auto-sovrano è quello in cui gli individui di tutto il mondo hanno il pieno controllo della propria identità digitale e dei propri beni. Questo potrebbe portare a una maggiore inclusione finanziaria, libertà, privacy e sicurezza, contribuendo così ad aumentare il benessere umano, l'abbondanza e la felicità generale.

2. **Una riserva di valore affidabile:**

   La scarsità digitale del Bitcoin lo rende un deposito di valore affidabile, il che potrebbe incoraggiare un maggior numero di persone a utilizzarlo come mezzo di risparmio per il futuro.

3. **Cambiamenti nella politica monetaria:**

   Se il Bitcoin venisse adottato su larga scala, potrebbe annullare la capacità dei governi di controllare l'offerta di moneta attraverso i tradizionali strumenti di politica monetaria. L'adozione di massa del Bitcoin aumenterebbe potenzialmente il potere d'acquisto delle persone e incoraggerebbe la società a orientarsi verso attività a bassa preferenza di tempo.

4. **Maggiore trasparenza e tracciabilità:**

   La registrazione a prova di manomissione e immutabile di tutte le transazioni sulla blockchain potrebbe aumentare la trasparenza e la responsabilità in vari settori e industrie. Attualmente, entità potenti hanno la possibilità di spostare trilioni di dollari in tutto il mondo senza una chiara visibilità sulla destinazione di questi fondi o sul loro utilizzo. Fornendo un registro aperto e verificabile delle transazioni finanziarie, Bitcoin potrebbe garantire che il movimento di capitali diventi più responsabile e accessibile al pubblico.

Perché Bitcoin?

5

Una rivoluzione nel mercato delle rimesse:

Il mercato delle rimesse prevede il trasferimento di fondi da una parte all'altra, spesso attraverso i confini internazionali. Nonostante il calo dei costi, le rimesse rimangono relativamente costose rispetto ai trasferimenti bancari nazionali, soprattutto per gli importi più piccoli. La Lightning Network offre transazioni veloci e a basso costo, rendendola adatta al mercato delle rimesse e affrontando i costi elevati e le altre sfide associate alle rimesse, come i tempi di regolamento lenti e le restrizioni sugli orari di lavoro.

6

Energia abbondante:

Quando c'è molta energia accessibile, le società funzionano bene e molte industrie e comunità possono soddisfare il crescente bisogno di energia nelle case, nelle aziende e nelle nuove tecnologie. Il mining di Bitcoin incentiva i minatori a utilizzare l'energia in eccesso che di solito andrebbe sprecata, proveniente da fonti energetiche sostenibili come l'energia solare, eolica e idroelettrica. I minatori di Bitcoin utilizzano questo surplus di energia per creare nuovi bitcoin attraverso le attività di mining, proteggere la rete e restituire l'energia in eccesso creata alla rete energetica che la società utilizza quando è necessaria.

10.4 Un futuro di responsabilità

Il Bitcoin è denaro.

Il denaro aiuta le persone a comunicare quali attività, beni e servizi sono più importanti all'interno della società. Come abbiamo visto in questo corso, quando il denaro è controllato da autorità centralizzate, viene manipolato.

Uno degli errori che l'umanità continua a ripetere nel corso della storia è la manipolazione del denaro, che si ripercuote negativamente su individui, famiglie, imprese, governi e, in ultima analisi, sulla prosperità umana globale.

Togliendo il controllo del denaro dalle mani di soggetti centralizzati e utilizzando invece denaro con un'offerta fissa che nessun singolo soggetto può cambiare, creiamo un mondo differente - un mondo in cui non dobbiamo confidare che l'uomo faccia la cosa giusta, ma piuttosto un mondo in cui l'uomo non è in grado di fare la cosa sbagliata.

Questo è un mondo fondamentalmente differente.

E tu, caro studente, puoi partecipare alla creazione di questo mondo. Utilizzando Bitcoin, gestendo il tuo nodo e aiutando i tuoi coetanei a conoscere meglio il futuro del denaro, voterai per un mondo differente.

Attività: Discussione finale in classe - Come è cambiata la vostra prospettiva?

Rispondete alle cinque domande qui sotto:

Perché abbiamo bisogno del denaro ?

Che cos'è il denaro?

Perché Bitcoin?

Chi controlla il denaro?

Che cosa dà al denaro il suo "valore"?

Scrivete le domande poste dagli studenti che sono state selezionate nel Capitolo 1 e rispondete.

1. **Tornate alla prima attività del Capitolo 1 e confrontate le nuove risposte con quelle precedenti.**
2. **Confrontate e discutete le risposte e le domande originali. È cambiato qualcosa?**
3. **Ponetevi questa domanda finale: Qual è il mio prossimo passo? E come posso usare questa nuova conoscenza per potenziare me stesso?**

Se siete pronti a fare il passo successivo, date un'occhiata alle risorse aggiuntive nella sezione seguente, in cui abbiamo selezionato le migliori risorse per ulteriore apprendimento e successo.

Risorse aggiuntive

1. Perché usare Bitcoin?

a **"Il caso rialzista del Bitcoin" di Vijay Boyapati:**

Questo articolo spiega perché il Bitcoin è un bene prezioso e perché ha il potenziale per diventare una valuta globale dominante. L'autore illustra gli aspetti tecnici ed economici del Bitcoin che lo rendono una forte opportunità di investimento.

b **"Perché Bitcoin è importante" di Aleks Svetski (1 ora):**

Questo video illustra l'importanza di Bitcoin come asset digitale decentralizzato e il suo impatto sull'attuale sistema finanziario. Lo speaker esplora il potenziale di Bitcoin per portare la libertà finanziaria alle persone di tutto il mondo.

c **"Perché Bitcoin" di Wiz:**

Questo articolo fornisce una panoramica dei vantaggi dell'utilizzo del Bitcoin come valuta e riserva di valore. Evidenzia la natura decentralizzata del Bitcoin e il modo in cui consente una maggiore libertà e sicurezza finanziaria.

2. Che cos'è Bitcoin?

a **"Come funziona il Bitcoin sotto il cofano" di CuriousInventor:**

https://www.youtube.com/watch?v=Lx9zgZCMqXE Questo video fornisce una spiegazione dettagliata degli aspetti tecnici di Bitcoin e del suo funzionamento.

b **"Cos'è il Bitcoin" di Greg Walker:**

Questo articolo fornisce una spiegazione completa di cosa sia il bitcoin, compresa la sua storia, la sua tecnologia e la sua differenza rispetto alle valute tradizionali.

c **"Bitcoin - La genesi" di RT (30 minuti):**

Questo video racconta la creazione e i primi giorni di Bitcoin. Esplora le motivazioni del misterioso creatore, Satoshi Nakamoto, e come si è evoluto il concetto di Bitcoin.

3. Approfondimento:

a **"Lo standard Bitcoin" (1 ora e 40 minuti):**

Questo audiolibro esplora il contesto economico e storico che ha portato alla creazione del Bitcoin. Illustra i vantaggi di una moneta decentralizzata e il potenziale del Bitcoin di diventare uno standard globale.

b **"Introduzione al pensiero austriaco di Bitcoin" (1 ora):**

Questa audio-lezione tratta della Scuola austriaca di economia e del suo rapporto con il concetto di Bitcoin. Fornisce uno sguardo approfondito sui principi economici alla base del Bitcoin e sul suo allineamento con il pensiero austriaco.

c **"Bambini Bitcoin"**

di Naomi Wambui - **https://bitcoinbabies.com/**
Twitter: **@btcbabies - @ngachanaomi1**
Una risorsa gratuita in formato PDF che ha lo scopo di fornire alle madri conoscenze essenziali su alimentazione, Bitcoin e benessere mentale generale.

d **Sessioni BTC**

Un canale YouTube di formazione solo su Bitcoin con tutorial e guide utili:
https://www.youtube.com/@BTCSessions

4. Corsi:

a **L'estate dei Bitcoin**

https://www.summerofbitcoin.org/: Un programma di stage estivo globale e online incentrato sull'introduzione di studenti universitari allo sviluppo e alla progettazione open-source di Bitcoin.

b Laboratori Chaincode

https://learning.chaincode.com/#FOSS: corsi online e un programma di residenza che consente agli studenti di apprendere le competenze necessarie per lavorare allo sviluppo del protocollo Bitcoin.

c Accademia Saylor

Istruzione gratuita in più discipline: **https://www.saylor.org/**

5. Autori importanti

a Alex Gladstein: *Controllate il vostro privilegio finanziario*

b Alex Swan: *Terapia dell'incontro con il terreno: Prospettive, caratteristiche e applicazioni*

c Amanda Cavaleri: *Bitcoin e il sogno americano: La nuova tecnologia monetaria che supera il nostro divario politico*

d Anita Posch: *Imparare il Bitcoin: diventare finanziariamente sovrani*

e Eric Yakes: *La settima proprietà: Bitcoin e la rivoluzione monetaria*

f Jeff Booth: *Il prezzo del domani: Perché la definizione è la chiave per un futuro di abbondanza*

g Jimmy Song: *Il piccolo libro dei Bitcoin: Perché il Bitcoin è importante per la vostra libertà, le vostre finanze e il vostro futuro*

h Nik Bhatia: Il *denaro a strati: Dall'oro e dal dollaro al Bitcoin e alle valute digitali delle banche centrali*

i Robert Breedlove: *Grazie a Dio per il Bitcoin: La creazione, la corruzione e la redenzione del denaro*

j Lyn Alden: *Soldi rotti*

6. Autori citati

a Inventore Curioso:

https://www.youtube.com/@CuriousInventor

b Anil Patel:

Twitter: @anilsaidso

7. Altre risorse:

1 **Bitcoin.org:** Il sito web ufficiale del protocollo Bitcoin.

2 **Bitcointalk.org:** Bitcointalk is a forum where users can discute di argomenti relativi a Bitcoin, pone domande e condivide informazioni. È un luogo ideale per imparare da altri appassionati ed esperti di Bitcoin.

3 **Bitcoincore.org:** È il software originale di Bitcoin ed è ancora ampiamente utilizzato da molti utenti e sviluppatori. Fornisce un potente insieme di strumenti per interagire con la rete Bitcoin e costruire applicazioni Bitcoin.

4 **Bitcoinwiki.org:** Si tratta di una risorsa guidata dalla comunità che fornisce una guida completa a tutto ciò che riguarda il Bitcoin. Copre tutto, dagli aspetti tecnici del Bitcoin alla sua storia e ai casi d'uso.

5 **Bitcoinmagazine.com:** È una pubblicazione online che tratta notizie e approfondimenti relativi al Bitcoin e alle altre criptovalute. È un ottimo modo per rimanere aggiornati sugli ultimi sviluppi dell'ecosistema Bitcoin.

6 **Bitcoin.Design:** Un archivio open-source di elementi di design legati al bitcoin per illustrazioni, siti web, modelli e icone.

7 **NOSTR:** https://nostr.com/ - Social media in cui i dati sono effettivamente di vostra proprietà.

8 **Simple X:** https://simplex.chat/ - Un protocollo applicativo privato e decentralizzato.

9 **Creare un nodo Bitcoin:** Raspberry Pi DIY di Keith Mukai: https://github.com/kdmukai/raspi4_bitcoin_node_tutorial?tab=readme-ov-file

10 **Come scegliere un portafoglio Bitcoin:** https://bitcoin.org/en/choose-your-wallet - Utilizzate le conoscenze appena acquisite per scegliere il portafoglio giusto per voi.

11 **BitcoinIcons.com:** - https://bitcoinicons.com/ - Una raccolta di icone Bitcoin gratuite.

12 **Bitcoin For Local Business:** https://bitcoinforlocalbusiness.com/ - Una serie di strumenti per aiutarvi a condividere il valore dei Bitcoin con le vostre attività commerciali locali preferite.

13 **Mempool.Space:** https://mempool.space/ - An progetto Mempool open source che presenta anche dati e grafici di Lightning Network.

Capitolo Concetti chiave

Capitolo 1:

Introduzione al corso:

Esplora gli obiettivi e le aspettative del corso per il **Diploma Bitcoin**.

Attività di Riflessione - Definire il denaro:

Impegnarsi in un esercizio riflessivo fornendo filtri di informazioni, risposte a domande chiave sul denaro.

Discussione in classe - Perché abbiamo bisogno del denaro:

- Partecipare a una discussione in classe sulla necessità fondamentale del denaro.
- Condividere e confrontare le prospettive individuali sull'importanza del denaro.
- Gettare le basi per comprendere il ruolo del denaro nei sistemi economici.

Capitolo 2:

Capire il denaro:

- Esplorare la definizione fondamentale e il concetto di denaro.
- Discutere le diverse prospettive all'interno della classe per comprendere la natura multiforme del denaro.

Funzioni, proprietà e tipi:

- Approfondire le funzioni, le proprietà e i tipi di denaro.
- Riconoscere l'importanza di questi aspetti in l'acquisizione e l'utilizzo del denaro.

Psicologia del denaro:

- Comprendere gli aspetti psicologici del denaro, tra cui la scarsità, la preferenza temporale e gli scambi.
- Impegnarsi nell'attività "Preferenza temporale" per mettere in relazione gli elementi psicologici con scenari di vita reale.

Capitolo 3:

Introduzione alla storia del denaro Evoluzione:

Esplorare la storia e l'evoluzione del denaro. Capire come le antiche forme di commercio abbiano portato allo sviluppo della moneta che usiamo oggi.

Rivoluzione della moneta digitale:

- Scoprite l'attuale apice dell'evoluzione del denaro: la moneta digitale.
- Comprendere come esista solo in forma elettronica, consentendo transazioni istantanee e a basso costo a livello globale.
- Scoprite il ruolo significativo che Bitcoin ha svolto nel risolvere le prime sfide delle valute digitali, rendendole pronte per l'uso a livello mondiale.

Evoluzione della moneta:

Esplorate il passaggio da forme antiche come conchiglie e perline alla nascita delle monete e della cartamoneta. Seguite il viaggio dalla carta alla plastica, svelando l'evoluzione della moneta nel corso della storia.

Attività del gioco del baratto:

Partecipate a un'esperienza pratica di baratto per comprendere le sfide dello scambio diretto e apprezzare la necessità di un sistema più efficiente.

Capitolo 4:

Origini della moneta Fiat:

Esplorare le origini della moneta elettronica attraverso una breve panoramica storica, comprendendo come sia diventata una forma di moneta dominante.

Attività bancaria a riserva frazionaria:

Partecipate all'attività sul sistema bancario a riserva frazionaria per capire come funziona questo sistema, evidenziando la sua dipendenza dal debito e le implicazioni per l'economia in generale.

Il Sistema Fiat:

Cogliere gli aspetti fondamentali del sistema monetario, compresa la sua natura di sistema monetario per decreto, il ruolo delle banche a riserva frazionaria e gli attori chiave che controllano questo sistema.

Capitolo 5:

Diminuzione del potere d'acquisto:

Comprendere il concetto di inflazione monetaria e il suo impatto sul potere d'acquisto. Partecipare all'attività Effects of Inflation: Un'attività d'asta per sperimentare in prima persona gli effetti dell'infilazione.

Le conseguenze del sistema Fiat Attività:

Partecipare all'attività: Conseguenze del sistema monetario fiat, che fa luce sulle ripercussioni più ampie dell'attuale quadro monetario.

Valute digitali delle banche centrali (CBDC):

Esplora il panorama in evoluzione delle valute digitali delle banche centrali (CBDC) e il loro potenziale impatto sul futuro del denaro.

Carico del debito globale e disuguaglianza sociale:

Esplorare il duplice impatto dell'onere del debito globale e della disuguaglianza sociale. Riconoscere le conseguenze individuali e sociali, sottolineando la perdita del potere d'acquisto e il crescente divario di ricchezza.

I Cypherpunk e Decentramento:

Scoprite la storia dei Cypherpunk e le motivazioni che li hanno spinti a cercare una valuta decentralizzata. Differenziate tra sistemi centralizzati e decentralizzati, traendo spunti da una breve storia delle valute digitali.

Capitolo 6:

Satoshi Nakamoto e la creazione di Bitcoin:

Esplora la misteriosa figura di Satoshi Nakamoto e la storia delle origini del Bitcoin, comprendendo le motivazioni iniziali del suo sviluppo.

Attività di classe - Costruzione del consenso:

Impegnarsi nella costruzione del consenso nella attività della rete Peer-to-Peer che permette di capire come si ottiene il consenso all'interno della rete Bitcoin.

Abbracciare la responsabilità personale:

Enfatizzare il concetto di responsabilità personale nel contesto di Bitcoin, incoraggiando la comprensione dei ruoli individuali e della responsabilità all'interno dell'ecosistema decentralizzato.

Come funziona il Bitcoin:

Uno sguardo ai meccanismi di Bitcoin, compreso il meccanismo di consenso di Nakamoto. Identificare gli attori principali della rete Bitcoin, come i minatori, i nodi, gli utenti, gli sviluppatori e i progetti, e comprendere le dinamiche di collaborazione tra di loro.

Bitcoin come moneta digitale solida:

Esaminare il ruolo di Bitcoin come moneta digitale solida, discutendo la sua evoluzione, le sue funzioni e le sue proprietà, e partecipare a una discussione di classe sulla qualificazione di Bitcoin come moneta solida.

Capitolo Concetti chiave

Capitolo 7:

Transazioni Peer-to-Peer:

Partecipate alle transazioni decentralizzate per sperimentare i principi fondamentali degli scambi di Bitcoin.

Impostazione di un portafoglio Bitcoin:

Imparate i passi essenziali per scaricare, creare chiavi e fare il backup di un portafoglio Bitcoin per transazioni sicure.

Risparmiare e Fare le Proprie Ricerche:

Comprendere il risparmio in Bitcoin come riserva di valore e l'importanza di una ricerca indipendente per prendere decisioni informate.

Tipi di portafogli Bitcoin:

Differenziare tra portafogli open source, closed source, custodiali e non custodiali, comprendendo il ruolo delle chiavi nella sicurezza.

Acquisire Bitcoin:

Esplorare metodi come le transazioni e gli scambi peer-to-peer, discutendo i problemi di privacy legati ai processi KYC.

Capitolo 8:

Introduzione alla rete Lightning:

Riconoscere l'evoluzione del Bitcoin attraverso tecnologie come la Lightning Network, che ne potenziano le capacità.

Impostazione di un portafoglio Lightning:

Scoprite i passaggi essenziali per configurare un portafoglio Bitcoin Lightning, che facilita transazioni più veloci e scalabili.

Attività pratica:

Partecipate a una staffetta pratica di portafogli Lightning, promuovendo una comprensione dinamica delle transazioni della rete Lightning.

Tipi di portafogli Lightning:

Differenziazione tra portafogli Lightning open source, closed source, custodial e non custodial per le diverse preferenze degli utenti.

Transazioni lightining:

Esplora il processo di invio e ricezione delle transazioni Lightning, sottolineando la velocità e l'efficienza della rete Lightning.

Capitolo 9:

Il libro mastro di Bitcoin:

Comprendere il concetto di libro mastro decentralizzato facilitato da nodi e minatori, che garantisce trasparenza e sicurezza.

Il modello UTXO:

Cogliere il modello Unspent Transaction Output come aspetto fondamentale del processo di transazione di Bitcoin.

Chiavi pubbliche e private:

Esplora l'importanza della sicurezza crittografica nelle transazioni Bitcoin attraverso le chiavi pubbliche e private, insieme a un'attività di dimostrazione dell'hashing SHA 256.

Nodi e minatori Bitcoin:

Approfondisce il ruolo dei nodi e dei minatori nel mantenimento della rete Bitcoin, affrontando aspetti come l'emissione, la scarsità, il dimezzamento e la difficoltà.

Come funzionano le transazioni in Bitcoin:

Approfondite l'intero ciclo di vita di una transazione Bitcoin, coinvolgendo il mittente, il destinatario, i nodi, i minatori e la mempool, con un'attività dedicata alla mempool.

Capitolo 10:

Basi filosofiche del Bitcoin:

Esplora la filosofia alla base del Bitcoin, comprendendo come sia emerso come risposta alle sfide economiche, con particolare attenzione al suo impatto sulla libertà finanziaria e a come si differenzia dalle valute tradizionali.

Il futuro di Bitcoin:

Approfondite la potenziale traiettoria e gli sviluppi futuri del Bitcoin come valuta digitale rivoluzionaria.

Riflessioni su Diploma:

- Riassumere i punti chiave del Diploma Bitcoin, incoraggiando gli studenti a riflettere sul loro percorso e sulle conoscenze acquisite.
- Le attività comprendono la visione di un video sul tema "Perché Bitcoin?" e la rivisitazione delle domande del Capitolo 1 per valutare la crescita personale nella comprensione.

Glossario

Attacco al 51%: Un tipo di attacco a una rete blockchain in cui una singola entità o un gruppo controlla la maggioranza della potenza di calcolo della rete, consentendo di manipolare le transazioni e potenzialmente interrompere la rete.

Stagione delle Altcoin: un periodo di tempo in cui le criptovalute alternative registrano aumenti di prezzo significativi, spesso a causa dell'aumento dell'interesse e dell'adozione da parte degli investitori.

Altcoins: Valute digitali ad esclusione del Bitcoin.

Atomic Swap: Uno scambio peer-to-peer di una criptovaluta con un'altra senza la necessità di un scambio o intermediario centralizzato.

Asta: Processo attraverso il quale beni o attività vengono venduti al miglior offerente.

Baratto: Lo scambio di beni e servizi senza l'uso di denaro.

Paniere di beni: Un insieme di beni o servizi utilizzato per misurare le variazioni del costo della vita.

Bitcoin: una moneta/sistema digitale che consente alle persone di inviarsi denaro a vicenda senza utilizzare una banca.

Blockchain Explorer: Uno strumento utilizzato per visualizzare ed esplorare la blockchain, che consente agli utenti di visualizzare i singoli blocchi, le transazioni e gli indirizzi dei portafogli.

Ricompensa del blocco: La quantità di nuovi bitcoin che vengono assegnati ai minatori per l'aggiunta di un nuovo blocco alla blockchain.

Blockchain: Un registro pubblico di tutte le transazioni in bitcoin avvenute.

BTC: l'unità di misura utilizzata per i bitcoin. Una moneta digitale che può essere utilizzata per effettuare acquisti o scambi.

Controlli sui capitali: Restrizioni al movimento di denaro attraverso le frontiere.

Banca centrale (Fed): Istituzione di proprietà del governo che gestisce la politica monetaria di un paese.

Centralizzazione: La concentrazione del potere o del controllo in un'unica entità.

Sistema centralizzato: Un sistema in cui il potere o il controllo sono concentrati in un'unica entità.

Conservazione a freddo: Un metodo per conservare i bitcoin al riparo dal rischio di hacker o altre minacce online.

Moneta-merce: Oggetti che hanno valore di per sé e sono utilizzati come mezzo di scambio, come l'oro o l'argento.

Conferma: Il processo di elaborazione di una transazione da parte della rete, che è altamente improbabile che possa essere annullata. I "minatori" del metodo verificano l'autenticità delle transazioni con il loro hardware e software. Si consiglia di attendere almeno sei conferme per evitare la possibilità una doppia spesa.

Meccanismo di consenso: Un metodo utilizzato nella tecnologia blockchain per convalidare le transazioni e garantire l'integrità della blockchain.

Scambio di criptovalute: Una piattaforma in cui gli utenti possono acquistare, vendere e scambiare criptovalute con altre criptovalute.

Portafoglio di criptovalute: Un programma software che memorizza le chiavi private e consente agli utenti di inviare, ricevere e gestire le proprie criptovalute.

Crittografia: Una branca della matematica che aiuta a creare sistemi sicuri.

Svalutazione: Riduzione del valore di una moneta, spesso attraverso la riduzione della quantità di metallo prezioso in una moneta.

Debito: denaro dovuto a qualcun altro.

Decentramento: La distribuzione del potere e del controllo all'interno di una rete piuttosto che la presenza di un'autorità centrale.

Organizzazione autonoma decentralizzata (DAO): Un'organizzazione o una rete governata da contratti intelligenti ed eseguita su una blockchain senza un'autorità centrale o una struttura di gestione.

Finanza decentralizzata (DeFi): Un movimento all'interno dell'industria delle criptovalute per creare una finanza decentralizzata. Prodotti e servizi finanziari che operano su una blockchain senza controllo centrale.

Sistema decentralizzato: Un sistema in cui il potere o il controllo sono distribuiti tra più entità.

Digital Asset: rappresentazione digitale di un valore che può essere scambiato o utilizzato come riserva di valore, come i bitcoin.

Libro mastro distribuito: Un database distribuito su una rete di computer invece di essere memorizzato in una posizione centrale.

Doppia coincidenza di desideri: Il fenomeno per cui due parti in un'economia di baratto hanno entrambe ciò che l'altra parte vuole e vogliono ciò che l'altra parte ha.

Doppia spesa: Quando una persona cerca di inviare i propri bitcoin a due destinatari diversi nello stesso momento.

Transazione di polvere: Una transazione che invia una quantità molto piccola di bitcoin, troppo piccola per essere economicamente redditizia.

Glossario

Tasso di cambio: Il valore di una valuta rispetto a un'altra.

FOMO: Fear of missing out, un termine usato per descrivere la sensazione di ansia o di rammarico per la possibilità di perdere qualcosa su un'opportunità vantaggiosa nel mercato delle criptovalute.

FUD: Fear, uncertainty, and doubt (paura, incertezza e dubbio), un termine usato per descrivere voci o informazioni negative che possono provocare il panico o il declino del mercato.

PIL: Prodotto interno lordo, il valore totale dei beni e dei servizi prodotti in un Paese in un determinato periodo di tempo.

Hard Fork: una modifica al protocollo Bitcoin che crea una nuova versione della blockchain che non è compatibile con la versione precedente (cioè, ad esempio, Bitcoin Cash).

Portafoglio hardware: Un dispositivo fisico utilizzato per memorizzare le chiavi private e gestire le criptovalute, che offre una maggiore sicurezza rispetto ai portafogli software.

Funzione Hash: Una funzione matematica che prende in input dati di qualsiasi dimensione e restituisce una stringa di dimensione fissa di
caratteri, comunemente utilizzati nella crittografia e nella tecnologia blockchain.

Tasso di hash: Un modo per misurare la potenza di elaborazione della rete Bitcoin.

HODL: termine usato nella comunità delle criptovalute per descrivere il possesso di criptovalute a lungo termine. piuttosto che venderlo o scambiarlo.

Portafoglio caldo: Un portafoglio Bitcoin collegato a Internet, che consente di accedere facilmente ai bitcoin.

Importazioni: Beni e servizi prodotti in un altro Paese e venduti sul mercato nazionale.

Inflazione: Un aumento del livello generale dei prezzi di beni e servizi in un'economia.

Initial Coin Offering (ICO): Metodo di raccolta fondi in cui una nuova criptovaluta viene venduta agli investitori in cambio di una criptovaluta più consolidata, come il Bitcoin.

Protocollo Layer-1: Il livello sottostante di una rete blockchain che gestisce gli aspetti fondamentali del consenso, della convalida delle transazioni e dell'archiviazione dei dati.

Protocollo di livello 2: Un livello secondario costruito in cima a una rete blockchain di livello 1, spesso utilizzato per potenziare la rete blockchain migliorando scalabilità, velocità e funzionalità.

Libro mastro: Un registro delle transazioni finanziarie.

Rete Lightning: Un protocollo di pagamento di livello 2 che consente transazioni in bitcoin più rapide ed economiche utilizzando canali a catena per le transazioni più piccole.

Mezzi di scambio: Oggetti o sistemi che sono ampiamente accettati in cambio di beni e servizi.

Albero di Merkle: Una struttura di dati ad albero utilizzata nella blockchain di Bitcoin per verificare in modo efficiente l'integrità di grandi insiemi di dati.

Pool minerario (mining pool): Un gruppo di minatori che lavorano insieme per aumentare le loro possibilità di trovare nuovi blocchi e di ottenere un'immagine di qualità e guadagnare quindi più bitcoin.

Mining: Il processo di utilizzo dell'hardware del computer per eseguire calcoli matematici per la rete Bitcoin. per controllare le transazioni e aumentare la sicurezza.

Politica monetaria e fiscale: Le politiche di una banca centrale e di un governo, rispettivamente, che influenzano la politica monetaria e fiscale modificando l'offerta di moneta e i tassi di interesse in un'economia.

Offerta di moneta: La quantità totale di denaro in circolazione in un'economia.

Portafoglio multi-firma (Multisig): Un portafoglio che richiede più firme o approvazioni prima che una transazione possa essere eseguita, garantendo maggiore sicurezza e controllo.

Multi-firma: Una funzione di sicurezza che richiede più di una chiave privata per autorizzare una transazione bitcoin.

Rete: Un gruppo di entità interconnesse.

Rete di nodi: Una rete di computer o dispositivi collegati che supportano e mantengono la rete Bitcoin.

Nodo: Un computer o un dispositivo connesso alla rete Bitcoin che partecipa alla verifica e alla trasmissione delle transazioni.

Gettone (Token) non fungibile (NFT): Un tipo di asset digitale che rappresenta un oggetto unico o irripetibile, spesso utilizzati per rappresentare opere d'arte, oggetti da collezione o altri oggetti unici.

Nonce: Un numero casuale aggiunto all'intestazione di un blocco per creare un hash che soddisfi l'obiettivo di difficoltà.

Blocco orfano: Un blocco non incluso nella catena principale della blockchain perché invalidato da una catena concorrente più lunga.

Portafoglio cartaceo: (anche noto come “paper wallet”) Una copia stampata delle chiavi private e pubbliche di un utente, utilizzata per conservare e gestire le offline di criptovaluta.

Peer-to-Peer (P2P): Una rete decentralizzata in cui i partecipanti interagiscono direttamente tra loro anziché attraverso un'autorità centrale.

Glossario

Peg: tasso di cambio fisso tra due valute in cui una è ancorata al valore di un'altra.

Blockchain privata: Una blockchain controllata da una singola organizzazione anziché essere decentralizzata.

Chiave privata: Un dato segreto che dimostra il diritto di una persona a spendere bitcoin da uno specifico portafoglio attraverso una firma crittografica.

Proof-of-Stake (PoS): Un meccanismo di consenso utilizzato in alcune reti blockchain che richiede agli utenti di possedere una certa quantità di criptovaluta per partecipare alla convalida delle transazioni.

Proof-of-Work (PoW): Un meccanismo di consenso che richiede agli utenti di eseguire una certa quantità di calcoli e lavoro per partecipare alla rete.

Blockchain pubblica: Una blockchain aperta a chiunque possa partecipare e verificare le transazioni, rendendola decentralizzata.

Chiave pubblica: Un identificativo univoco utilizzato per ricevere bitcoin, derivato dalla chiave privata di un utente attraverso un processo matematico.

Chiave pubblica/indirizzo bitcoin: Una password/numero pubblico utilizzato per ricevere bitcoin.

Libro mastro pubblico: Un database decentralizzato che tiene un registro pubblico di tutte le transazioni sulla rete Bitcoin.

Potere d'acquisto: la capacità del denaro di acquistare beni e servizi.

Frase di recupero/Parola chiave di partenza: una serie di 12, 18 o 24 parole che può essere utilizzata per generare più coppie di chiavi private e pubbliche. Queste possono essere utilizzate per ripristinare un portafoglio Bitcoin.

Rapporto di riserva: La percentuale di depositi che una banca deve detenere come riserve.

Restrizione bancaria: Restrizioni o limitazioni ai servizi bancari o all'accesso ai servizi bancari.

Satoshi Nakamoto: Lo pseudonimo utilizzato dall'anonimo creatore (o creatori) di Bitcoin.

Satoshi: la più piccola unità di Bitcoin, pari a 1/100.000.000 di un bitcoin. Prende il nome dal creatore di Bitcoin, Satoshi Nakamoto.

Satoshis per Byte (sat/b): Unità utilizzata per misurare l'importo della commissione di transazione bitcoin pagata per byte di dati di transazione.

SegWit (Segregated Witness): Un aggiornamento del protocollo Bitcoin che modifica il modo in cui i dati vengono memorizzati sulla blockchain, consentendo di aumentare la capacità e ridurre le commissioni di transazione.

Sidechain: Una blockchain collegata a un'altra blockchain, che consente il trasferimento di beni o informazioni tra le due catene.

Firma: Meccanismo matematico che consente di dimostrare la proprietà.

Smart Contract: un contratto autoesecutivo con i termini dell'accordo scritti nel codice.

Soft Fork: una modifica al protocollo Bitcoin che è retrocompatibile con le versioni precedenti del sistema software.

Stablecoin: tipo di criptovaluta progettata per mantenere un valore stabile, spesso agganciato a un tasso di cambio valuta o altra attività.

Domanda e offerta: Il principio economico secondo cui il prezzo di un bene o di un servizio è determinato dall'interazione tra la quantità di beni o servizi forniti e la quantità richiesta.

Valore temporale del denaro: Il principio secondo cui il denaro vale di più nel presente che nel futuro.

Token: Un'unità di valore creata su una blockchain, spesso utilizzata per rappresentare un'attività o un'utilità specifica all'interno di un'azienda o di un particolare ecosistema.

Tokenizzazione: Il processo di creazione di una rappresentazione digitale di un bene o di una classe di beni su una blockchain, che consente la proprietà frazionata e la trasferibilità.

Coppia di trading: Un insieme di due valute o attività che possono essere scambiate l'una con l'altra in una borsa di criptovalute.

Tassa di transazione: Una piccola somma di bitcoin pagata dal mittente di una transazione, che incentiva i minatori a includere la transazione in un blocco e ad aggiungerla alla blockchain.

ID transazione: Una stringa di numeri e lettere che riporta i dettagli di un trasferimento di bitcoin (come l'importo inviato, gli indirizzi del mittente e del destinatario e la data del trasferimento) sulla catena di blocchi Bitcoin.

Transazione: Trasferimento di bitcoin da un indirizzo a un altro sulla rete Bitcoin.

Senza fiducia: Un sistema o una transazione che non richiede la fiducia in una terza parte o in un intermediario, ma che si affida alla sicurezza e alla trasparenza della tecnologia sottostante.

Glossario

Autenticazione a due fattori (2FA): Una misura di sicurezza che richiede due metodi di autenticazione, in genere una password e un codice o un dispositivo separato, per accedere a un account o completare una transazione.

Unbanked: Individui o comunità che non hanno accesso ai servizi bancari tradizionali.

Unità di conto: Unità di misura standard utilizzata per esprimere il valore di beni e servizi.

Volatilità: Il grado di variazione del prezzo di un'attività nel tempo.

Indirizzo del portafoglio: Un identificativo univoco utilizzato per inviare e ricevere bitcoin sulla rete Bitcoin, tipicamente rappresentato come una stringa di lettere e numeri.

Backup del portafoglio: Una copia delle chiavi private e delle frasi di recupero/parole chiave di un portafoglio Bitcoin, che può essere utilizzata per ripristinare l'accesso al portafoglio in caso di perdita o furto dell'originale.

Portafoglio: Un contenitore virtuale per i bitcoin, simile a un portafoglio fisico, che contiene le chiavi private che consentono di spendere i bitcoin ad esso assegnati nella blockchain.

Balena: Un individuo o un'organizzazione che detiene una quantità significativa di criptovaluta, in grado di influenzare il mercato ed I prezzi di mercato attraverso grandi scambi.

White Hat Hacker: (Letteralmente: Hacker dal cappello bianco) Un hacker etico che utilizza le proprie competenze per identificare e risolvere le vulnerabilità dei computer.
sistemi e reti.

Whitepaper: Un rapporto che spiega il problema e la soluzione che un progetto blockchain o una criptovaluta sta cercando di affrontare.

XBT e BTC: abbreviazioni di bitcoin.

Versione italiana | 2025