Alveare Finanziario

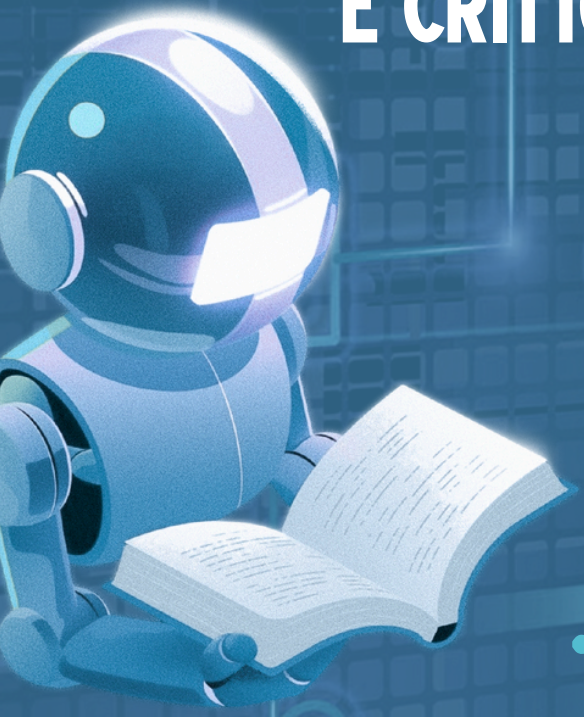
FORMAZIONE BLOCKCHAIN

CONTENUTO GRATUITO

ISPIRATO DA
"CERTIFICACIÓN BLOCKCHAIN 2026"
DI SEBASTIAN ÁLVAREZ HERRERA

MODULO 1

EVOLUZIONE DEL DENARO, INTERNET E CRITTOGRAFIA.



Prefazione

Parlare di blockchain nel 2026 non è più una scelta avveniristica. È una necessità.

Chi si occupa di finanza, anche a livello personale, sa già che il sistema monetario sta attraversando una fase di trasformazione profonda. Le regole che hanno governato il denaro per secoli si stanno riscrivendo, e chi arriva preparato a questa transizione avrà un vantaggio concreto rispetto a chi aspetta che le cose si stabilizzino da sole. Le cose non si stabilizzeranno. Continueranno a cambiare.

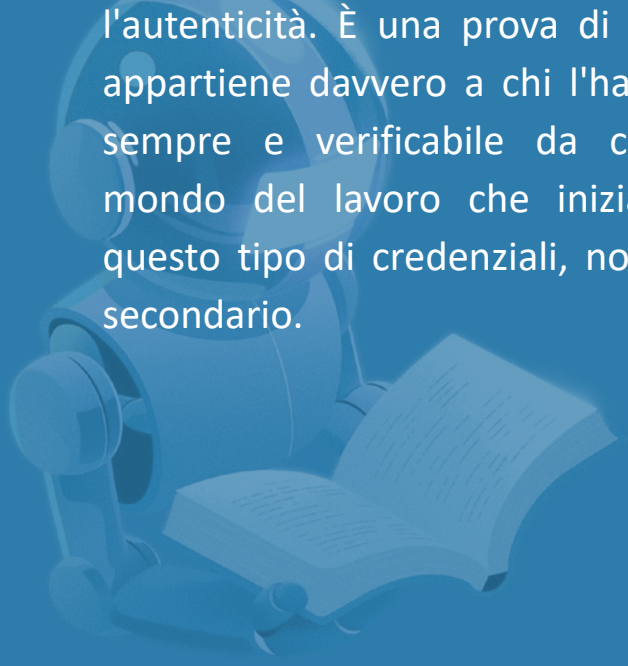
In Alveare Finanziario crediamo da sempre che la cultura finanziaria non sia un privilegio riservato a chi lavora in una banca o ha una laurea in economia. È uno strumento che appartiene a tutti, e il compito di chi la conosce è trasmetterla nel modo più chiaro possibile.

È con questo spirito che abbiamo scelto di tradurre e adattare per il pubblico italiano il lavoro di Sebastián Álvarez Herrera, formatore e consulente con anni di esperienza sul campo tra blockchain, criptovalute e trading istituzionale. Un materiale che in lingua spagnola ha già accompagnato migliaia di persone in questo percorso, e che oggi mettiamo a disposizione di chi vuole affrontarlo nella propria lingua.

Il libro che hai tra le mani nasce da un percorso di certificazione blockchain costruito per chi ha già una certa familiarità con il mondo della finanza, ma non ha mai avuto l'occasione di addentrarsi nel funzionamento tecnico delle criptovalute, degli smart contract o della finanza decentralizzata. Non troverai qui formule inaccessibili o lunghe digressioni accademiche.

Troverai invece un percorso strutturato, che parte dall'origine del denaro, passa per la storia di internet e della crittografia, e arriva ai concetti fondamentali della blockchain con la stessa logica progressiva di un buon corso di formazione professionale.

Chi completa il percorso ha la possibilità di sostenere un esame finale di certificazione. La certificazione ottenuta non è un semplice attestato: viene registrata in modo immutabile sulla blockchain, il che significa che nessuno potrà alterarla, revocarla o metterne in dubbio l'autenticità. È una prova di competenza che appartiene davvero a chi l'ha conseguita, per sempre e verificabile da chiunque. In un mondo del lavoro che inizia a riconoscere questo tipo di credenziali, non è un dettaglio secondario.



Il nostro invito è semplice: affronta questo manuale come faresti con qualsiasi disciplina che vale la pena imparare. Con metodo, senza fretta, e con la consapevolezza che ogni concetto che comprendi oggi ti mette in una posizione migliore per le decisioni di domani. Non serve diventare sviluppatori o miners. Serve capire come funziona il mondo in cui i tuoi soldi e i tuoi investimenti si muovono.
La blockchain non è il futuro. È già il presente. E il momento giusto per capirla è adesso.

Alveare Finanziario

Storia ed evoluzione del denaro

Per addentrarci nella storia e nell'evoluzione del denaro, dobbiamo innanzitutto comprenderne l'origine e la funzione all'interno della società.

Il denaro è qualsiasi bene o attività generalmente accettato come mezzo di pagamento dagli agenti economici per i loro scambi. Nasce per ovviare alla scarsa efficienza del baratto, che iniziò ad essere utilizzato nel Neolitico con i primi insediamenti umani. Agli albori delle società umane, la generazione di eccedenze era praticamente nulla, poiché l'essere umano cacciava solo per soddisfare i propri bisogni immediati. Allo stesso modo, conservare i prodotti durante l'inverno era praticamente impossibile a causa dello stile di vita esistente in quelle comunità, la cui caratteristica principale era il nomadismo.

Sebbene i cacciatori e i raccoglitori si spostassero alla ricerca di viveri e di rifugi migliori, la necessità veramente pressante iniziò durante il Neolitico.

A partire da quell'epoca, l'aumento della popolazione costrinse a sviluppare nuovi mezzi per sostenere le società, come l'agricoltura e l'allevamento, il che generò la necessità di immagazzinare grandi quantità di cibo per i periodi di carestia. Così, le eccedenze degli anni in cui si era avuto un buon raccolto venivano scambiate con altri prodotti di popoli lontani, dando così origine al commercio. Per la conservazione di questi beni venivano utilizzate tecniche come l'essiccazione, l'affumicatura, la salatura e la stagionatura. A seconda delle zone geografiche se ne utilizzavano alcune piuttosto che altre. Ad esempio, in Africa si ricorreva all'essiccazione, mentre nel nord Europa si affumicavano gli alimenti e nelle zone costiere era comune la salatura.

Chi ha inventato il denaro?

Sebbene il baratto, all'epoca, fosse un fattore trainante di enorme importanza per il commercio e le società, con il passare del tempo smise di essere considerato una pratica praticabile. Fondamentalmente, presentava due problemi. Da un lato, affinché uno scambio potesse avvenire, era necessario che entrambe le parti avessero bisogno del prodotto offerto dall'altra. In altre parole, se una persona aveva un surplus di pelli e aveva bisogno di grano, doveva trovare un produttore di grano che fosse necessariamente interessato all'acquisto di pelli, cosa che non sempre accadeva. D'altra parte, il baratto non era in grado di definire il valore reale delle merci, ad esempio, quale quantità di lana equivalesse a due brocche di vino o se una mucca valesse quanto un cammello.

Per risolvere questa situazione, si prese un prodotto come valore di riferimento, un elemento che servisse a regolare gli scambi. In un primo momento, si utilizzarono il bestiame o il grano come elementi di riferimento per gli scambi. Successivamente, questi elementi si evolsero in altri più facili da gestire, come l'oro, l'argento o i sacchetti di sale. In particolare, l'uso del sale come elemento di pagamento per il lavoro svolto ha dato origine al termine "salario".

Qual’è l’origine del denaro?

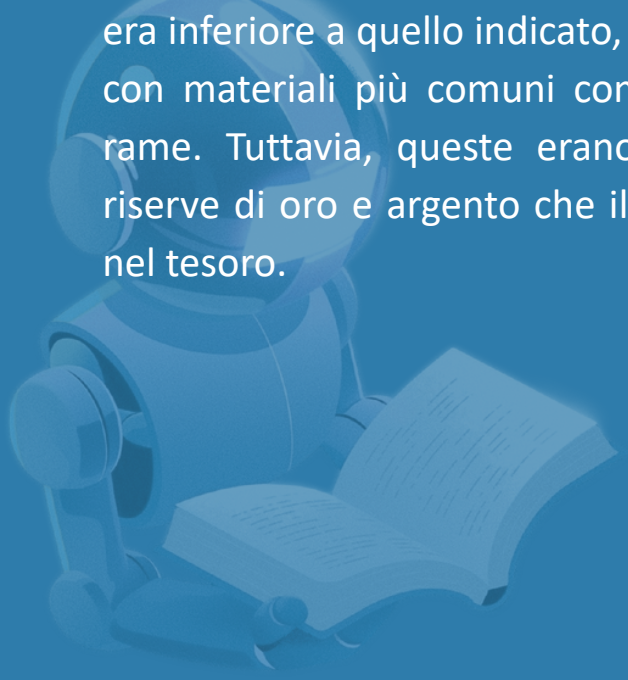
Secondo lo storico greco Erodoto, le prime monete metalliche sorsero in Asia Minore, nell'VIII secolo a.C., quando il re Lidio Gige si propose di semplificare la riscossione delle tasse e la loro conservazione.

Lo sviluppo delle attività commerciali, soprattutto attraverso l'Impero Romano, favorì l'utilizzo delle monete metalliche. Da allora, erano gli Stati ad avere il monopolio della coniazione delle monete. Queste erano solite avere un sigillo inciso: la figura di un dio, il busto di un imperatore o qualche altro simbolo caratteristico di quella società. Questi marchi garantivano sia la purezza che il peso del materiale con cui la moneta era stata fabbricata. In generale, si preferiva l'uso dell'oro e dell'argento rispetto ad altri materiali per la loro incorruttibilità e il loro valore.

Come erano le prime monete?

Le monete con la composizione più stabile nacquero nell'antica Grecia. Queste pesavano solitamente tra i 65 e i 67 grammi ed erano, principalmente, d'argento. La dracma divenne la moneta universale in quanto quella con il maggior valore intrinseco.

Il problema sorse quando le riserve di metalli preziosi cominciarono a scarseggiare. Fu allora che lo Stato dovette creare la moneta a corso legale, ovvero un tipo di moneta il cui valore era inferiore a quello indicato, poiché realizzata con materiali più comuni come il bronzo o il rame. Tuttavia, queste erano garantite dalle riserve di oro e argento che il paese custodiva nel tesoro.



Caratteristiche della prima carta moneta

Nei secoli XV e XVI si utilizzavano ancora monete d'oro e d'argento nelle grandi transazioni, ma né per le strade né nelle case era possibile custodirle in modo sicuro. Gli orafi disponevano di casseforti e custodie per tenere al sicuro oggetti di valore e denaro, così iniziarono a offrire questo servizio a terzi. Le persone portavano il proprio oro agli orafi affinché lo custodissero e, in cambio, questi emettevano dei certificati nominativi che ne attestavano il possesso. In questo modo, il proprietario, presentando il certificato, poteva ritirare le monete d'argento o d'oro quando ne aveva bisogno per effettuare una transazione.

Con il passare del tempo, questi certificati vennero utilizzati progressivamente per effettuare pagamenti senza bisogno di ricorrere al metallo che li garantiva, dando origine al sistema della carta moneta, ciò che oggi conosciamo come banconote.

Come si è evoluto il valore del denaro nel tempo?

Dal XIX secolo, il sistema monetario dominante era il sistema aureo, in base al quale il valore di un'unità monetaria era fissato in funzione di una quantità specifica di oro, finché, nel 1944, con gli accordi di Bretton Woods, il sistema monetario cambiò con l'emergere di due nuovi protagonisti: il dollaro e l'oro. In questo modo, è stata stabilita la convertibilità della valuta statunitense in oro – al tasso di 35 dollari per 1 oncia d'oro – e delle altre valute in dollari. Nel 1971, il presidente degli Stati Uniti, Richard Nixon, ha posto fine al sistema aureo, dando così inizio alla fluttuazione delle valute.

Da allora utilizziamo un sistema fiduciario in cui il denaro non ha un valore intrinseco ed è controllato ed emesso dalle banche centrali di ciascun paese, nonché da altri organismi sovranazionali come la Banca Centrale Europea per i paesi dell'eurozona.

Pertanto, il denaro (cartaceo, monetario o digitale) non ha oggi alcun sostegno in termini di metalli preziosi, ma il suo valore si basa sulla fiducia di ogni individuo che esso sarà accettato come mezzo di pagamento dagli altri. Senza quella fiducia reciproca e quell'accettazione sociale, le banconote che utilizziamo oggi sarebbero, letteralmente, carta straccia.

Storia ed evoluzione di Internet

Nascita di Internet: si tratta della pubblicazione dell'RFC-1 (Request For Comments n.1), documento che descrive il protocollo utilizzato dai dispositivi impiegati per interconnettere la prima rete informatica, ARPANET (Rete dell'Agenzia per la Ricerca sui Progetti Avanzati). Nell'ottobre dello stesso anno fu inviato un messaggio da un computer all'altro: Charly Kline, uno studente dell'UCLA, digitò un messaggio che diceva “login”, il quale dovette percorrere circa 500 km per arrivare al destinatario. Fu in quel momento che il professor Leonard Kleinrock dell'Università di Stanford ricevette il messaggio, anche se arrivarono solo le vocali ‘O’ e “I”.
Internet è definita come una rete mondiale in cui i dispositivi sono collegati ad essa e utilizzano un linguaggio comune.

Un sito web è come un libro, le pagine web sono come le pagine del libro e l'ipertesto è ciò che dà forma ai paragrafi, alle immagini e ai riferimenti (noti come link) ad altre pagine web.

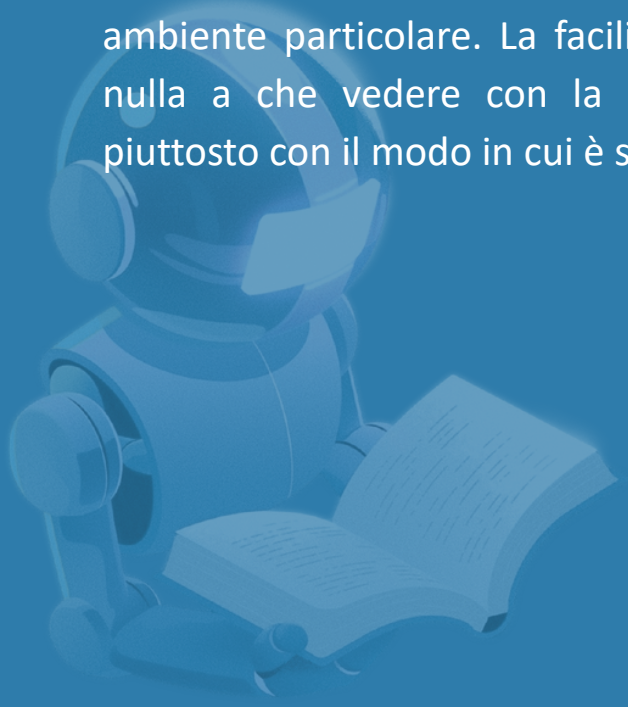
Oggi conosciamo solo 6 o 7 browser web, tra cui Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Brave, ecc. Ma per arrivare a questo, Internet ha dovuto attraversare un lungo processo di evoluzione. Nel 1993, Mosaic fu il primo browser lanciato sul mercato. Poi, nel 1995, apparve Opera, un altro browser che prometteva di soppiantare Mosaic. Qualche anno dopo, nel 1995, fece la sua comparsa Internet Explorer, uno dei browser più iconici a livello mondiale. Solo nel 2003 è apparso Safari, il browser per Macintosh. Un anno dopo ha fatto la sua apparizione Firefox, un browser molto più veloce ed efficiente rispetto ai precedenti.

Nel 2008 è nato Chrome, uno dei browser che ha avuto una grande presenza nonostante la sua breve vita, con un ruolo di primo piano nell'evoluzione del web.

Internet non si è evoluto solo nella sua struttura, come nel caso dei browser, ma anche nel modo in cui vi si naviga. Agli albori del web, più propriamente chiamato web 1.0, potevamo solo fruire di contenuti: si trattava di informazioni che ricevevamo senza alcuna possibilità di interagire con esse. Poi è arrivato il Web 2.0 con blog, forum, commenti e, più tardi, i social network. Era ed è il Web che ci permette fondamentalmente di condividere le informazioni. Il Web 3.0 è il prossimo cambiamento che non solo permette la ricerca di informazioni e l'interazione, ma si assocerà a un concetto di personalizzazione. Un flusso di informazioni, contenuti e pubblicità adattato ai nostri gusti personali.

Oggi Internet è tutto ed è presente ovunque, è come la luce, l'acqua, è presente 24 ore al giorno. Attualmente su Internet si trova ogni tipo di informazione, i media ci bombardano continuamente di informazioni, ecco perché è estremamente importante dare un senso e un buon uso a tali informazioni, ecco perché si parla di “intossicazione da informazione”.

Nasce così il concetto di usabilità, che si riferisce all'efficacia, all'efficienza e alla soddisfazione con cui un gruppo specifico di utenti può svolgere una serie di compiti in un ambiente particolare. La facilità d'uso non ha nulla a che vedere con la complessità, ma piuttosto con il modo in cui è strutturato.



Crittografia

La crittografia è una tecnica utilizzata per proteggere i dati e impedire che terzi non autorizzati possano accedere a informazioni preziose o alterarle a proprio vantaggio o a danno di altri.

Una delle tecniche più antiche utilizzate per proteggere le informazioni è la crittografia. Questa tecnica è antica quanto la scrittura. E uno dei tanti esempi che troviamo sul suo utilizzo è l'interessante caso della storia della macchina Enigma, utilizzata dai nazisti durante la Seconda Guerra Mondiale per cifrare i messaggi sul fronte di battaglia.

La parola crittografia deriva dal greco κριπτός (kryptós = coperto, nascosto), γραφειν (grafein = scrivere) e dal suffisso -ia (usato per creare sostantivi astratti). Il messaggio cifrato in sé è visibile. È leggibile, ma il suo significato è nascosto.

Quindi, possiamo dire che attraverso la crittografia una persona può nascondere un testo o un'informazione, in modo che solo il mittente e il destinatario possano interpretarlo. Con il crescente boom e lo sviluppo dell'informatica, questa è stata ampiamente diffusa e modificata per il suo utilizzo. Ora si basa su complessi algoritmi matematici che si occupano di cifrare i messaggi. Hanno il compito di garantire la riservatezza tra le parti e l'integrità delle informazioni. A sua volta, offre l'autenticazione sia del mittente che del destinatario, garantendo che né il mittente né il destinatario possano negare l'autenticità del messaggio. Infine, garantisce che il messaggio sia nuovo, ovvero che non sia una ripetizione.

Le basi della crittografia informatica sono stabilite negli articoli “A Mathematical Theory of Communication” del 1948 e “Communication Theory of Secrecy Systems” del 1949.

Entrambi pubblicati da Claude Shannon, che getta le basi della teoria dell'informazione e della crittografia moderna. "New directions of Cryptography", sviluppato da Whitfield Diffie e Martin Hellman nel 1976, introduce il concetto di crittografia a chiave pubblica.
Il consolidamento della crittografia arriva nel 1977 con la pubblicazione dell' algoritmo RSA, sviluppato dai matematici Ron Rivest, Adi Shamir e Len Adleman.

Crittografia e sicurezza

Oggi la crittografia è uno dei pilastri fondamentali su cui si basa la tecnologia blockchain. Essa consente il funzionamento della rete, garantisce i meccanismi di consenso tra gli utenti e l'integrità della blockchain.

Per garantire che nessun soggetto esterno possa accedere ai dati, si utilizzano la crittografia a chiave pubblica (crittografia asimmetrica) e la crittografia a chiave segreta (crittografia simmetrica), che approfondiremo più avanti. La crittografia a chiave pubblica genera un hash che semplifica la distribuzione delle informazioni, mentre la chiave privata crittografa e decrittografa le informazioni tra il mittente e il destinatario.

In Bitcoin, la chiave pubblica si ottiene tramite la chiave privata, ma il processo inverso è impossibile da realizzare. Cioè, non è possibile ottenere la chiave privata a partire dalla chiave pubblica.

La chiave pubblica, dopo alcune modifiche successive, è l'indirizzo che possiamo condividere con tutti i membri della comunità affinché ci inviino denaro. O, nel caso specifico, quella che useremo per altri utenti della comunità per effettuare loro un pagamento. Non esiste alcun rischio di furto, poiché i fondi sono accessibili solo tramite la chiave privata.

La chiave privata è simile a un PIN o a una password che utilizziamo per accedere a diverse pagine web, ma che in questo caso è crittografata, aggiungendo molta più sicurezza. Ciò significa che inseriremo una serie di termini o parole che verranno crittografati e proteggeranno il wallet. Solo noi possediamo queste parole, quindi dobbiamo conservarle in modo sicuro e non condividerle con nessuno. In questo modo potremo accedere ai nostri fondi in qualsiasi momento. La tecnologia Blockchain fa ampio uso della crittografia in tutta la sua struttura operativa.

Tipi di crittografia

Come accennato all'inizio, la crittografia può essere simmetrica o asimmetrica, a seconda del tipo di chiave utilizzata. Vediamo questo aspetto più nel dettaglio.

Simmetrica

Questo è il tipo di crittografia che è stato utilizzato sin dagli albori della storia e per moltissimo tempo. È anche chiamata crittografia a chiave privata o a chiave singola. Per metterla in pratica e poter cifrare e decifrare un messaggio, si utilizza un'unica chiave che sia il mittente che il destinatario devono conoscere in anticipo. Questo è il punto debole di questo metodo, poiché c'è una maggiore probabilità che una terza parte intercetti la chiave quando il mittente la trasmette al destinatario.

Nella crittografia simmetrica è necessario utilizzare una chiave molto difficile da indovinare, poiché i computer attuali sono in grado di indovinare le chiavi molto rapidamente.

Pertanto, dobbiamo considerare che, poiché gli algoritmi crittografici sono pubblici, è necessario garantire che la loro sicurezza dipenda dalla loro complessità interna e dalla lunghezza della password, per evitare attacchi.

Asimmetrica

Conosciuta anche come crittografia a chiave pubblica. Questo metodo utilizza due chiavi, una pubblica e una privata; pertanto non è necessario conoscere una chiave in anticipo. La chiave pubblica può essere inviata e resa nota a chiunque, mentre la chiave privata è quella che non deve essere condivisa con nessuno. Quando un mittente desidera inviare un messaggio, utilizza la chiave pubblica per cifrarlo e lo invia. E solo il destinatario con la sua chiave privata può decifrare il messaggio.

La crittografia asimmetrica offre un livello di sicurezza straordinario, al punto che nemmeno la persona che ha crittografato il messaggio può decifrarlo senza la chiave privata.

Questo è il metodo utilizzato nelle criptovalute ed è un elemento fondamentale nella blockchain per poter effettuare operazioni e scambi di informazioni tra pari in totale sicurezza e senza bisogno di fidarsi l'uno dell'altro.

Ibrida

È un metodo che utilizza sia la crittografia simmetrica che quella asimmetrica. Impiegando la crittografia a chiave pubblica per condividere una chiave per la crittografia simmetrica.

Conoscendo i concetti di base della crittografia simmetrica e della crittografia asimmetrica, possiamo renderci conto di quale sia la loro principale differenza. La sicurezza offerta dalla prima è di livello molto basso rispetto a quella offerta dalla seconda. Tuttavia, la velocità con cui la crittografia simmetrica crittografa e decrittografa un messaggio è superiore a quella della crittografia asimmetrica. Da qui nasce la crittografia ibrida.