1. Introduzione: Le cripto

Uno scenario nuovo, con eccezioni e particolarità adatte a renderlo un fenomeno rilevante dell'economia digitale . Un asset potenzialmente in grado di incidere su alcuni assetti dell'economia e della finanza di un'economia secolare, mediante l'integrazione della tecnologia nei processi finanziari ed economici. Un settore tecnologico e finanziario in evoluzione , quello delle criptovalute. Per definizione, le cripto sono valute digitali che possiedono le stesse prerogative delle monete tradizionali: scambio, deposito e investimento.[5] Ciò che le contraddistingue è il fatto che queste siano totalmente decentralizzate, quindi esenti dall'emissione, dalla garanzia e dal controllo da parte di banche centrali o autorità pubbliche. Ma quindi, come possono essere scambiate senza che ci siano enti bancari terzi per la transazione e il deposito? La risposta risiede nel loro sistema base di funzionamento, quello delle blockchain (catene di blocchi). Come riportato da IBM, la blockchain: "è un registro digitale condiviso e immutabile, che consente la registrazione delle transazioni e il tracciamento degli asset, all'interno di una rete aziendale, e fornisce una singola fonte affidabile." L'idea alla base è semplice. Un normale detentore di cripto effettua una transazione. La transazione, prima di essere raccolta e convalidata dalla catena, viene messa in sala d'attesa (mempool[1])[19] che funge da memoria temporanea. Da lì la transazione viene verificata da un nodo validatore (o minatore a seconda della pratica di consenso adottata), il quale, venendo selezionato dal computer sulla base di criteri definiti dal protocollo di consenso , accumula quante transazioni gli è possibile selezionare e "convalida" perché si formi il nuovo blocco. Il blocco viene associato a un codice crittografico univoco che include l'impronta digitale del blocco precedente, creando la catena e, una volta consentito, viene distribuito e aggiunto in modo permanente al registro di tutti i nodi. In aggiunta, ogni blocco ha un'impronta temporale che indica esattamente quando la transazione è stata inserita nella blockchain.[1][2] Questo orario mantiene le transazioni in ordine cronologico e rende i dati più sicuri, perché impedisce di modificare le informazioni registrate in passato. La pratica del consenso è ciò che rende il sistema sicuro e trasparente, e la grandezza della catena, visto che il codice crittografato si allunga e si complica a ogni blocco, è ciò che rende molto difficilmente alterabile, sebbene la sicurezza dipenda dal protocollo, dall'implementazione e dalle chiavi private . È però un punto importante da porre che di queste pratiche esistono tipologie diverse e distinte, ciascuna delle quali si distanzia sia per criteri di scelta del nodo validatore che per meccanismo da adottare per la conferma. Tra i meccanismi di consenso, le due soluzioni dominanti e più accreditate oggi sono rispettivamente la Proof of Work(PoW) e la Proof of Stake(PoS). [17]

2. PoW vs Pos

La Proof of Work è il metodo che Bitcoin usa dal 2009 e funziona sulla base della potenza di calcolo dei dispositivi utilizzati. I partecipanti, chiamati miner, gareggiano per risolvere un problema crittografico computazionale molto difficile. Devono provare tantissime combinazioni diverse fino a trovare un valore chiamato nonce[2][6]. Combinato con i dati del blocco, produce un risultato speciale, l'hash[3][16], che rispetta una regola di difficoltà. Non esiste scorciatoia matematica e l'unico modo per trovare la soluzione è provare miliardi di combinazioni al secondo, un processo che consuma enormi quantità di energia elettrica. Il miner che riesce a trovare per primo l'hash, diventa convalidatore del blocco e riceve una ricompensa in bitcoin più i costi di transazione. Più aumentano i blocchi, più la potenza computazionale ed i tempi necessari a risolvere l'hash crescono, divenendo essi stessi garanti

---

[1] **La mempool (abbreviazione di memory pool)** è l'area di memoria temporanea in cui i nodi della rete Bitcoin trattengono le transazioni non ancora confermate prima che i miner le inseriscano in un blocco della blockchain

[2] **Un nonce:** è un numero a 32 bit inserito nell'intestazione di un blocco che i miner modificano ripetutamente per risolvere il puzzle crittografico del Proof of Work. La parola deriva dall'inglese "number used only once" (numero usato una sola volta).

[3] **L'hash:** è un codice digitale di lunghezza fissa generato dall'algoritmo crittografico SHA-256 per mettere in sicurezza e collegare i blocchi della blockchain.

di sicurezza e forza del Bitcoin. Per riscrivere la storia della blockchain (ad esempio per compiere una doppia spesa), un attaccante dovrebbe possedere più della metà della potenza di calcolo dell'intera rete (attacco del 51%), un'impresa economicamente proibitiva su una rete matura come quella di Bitcoin, dove il costo dell'hardware (ASIC[4]) e dell'energia si misura in miliardi di dollari. La PoW, in sostanza, ancora la sicurezza digitale a un costo fisico ed energetico reale ed è per questo che i sostenitori di Bitcoin la definiscono spesso "energia trasformata in verità".[3]

La Proof of Stake, invece, adottata da Ethereum in modo completo con "The Merge[5]"[15] nel settembre 2022 (dopo anni di transizione), sostituisce il lavoro computazionale con una garanzia economica diretta. Invece di far gareggiare computer che consumano molta energia, qui chi vuole aiutare a validare le transazioni mette a deposito (staking) una quantità significativa della criptovaluta nativa della rete come collaterale. I validatori vengono selezionati in modo pseudocasuale, ponderato in base alla quantità messa in stake, per proporre e attestare i blocchi. Più capacità liquida si lascia come collaterale congelato, più si acquisisce e si guadagna autorità nella convalida, prerogativa assegnata oggettivamente dal meccanismo di codice della rete . Se un validatore agisce in modo scorretto (ad esempio validando due blocchi in conflitto, un comportamento chiamato "slashing condition"), perde parte o la totalità del proprio capitale in stake. La sicurezza, quindi, non deriva dal costo esterno dell'energia ma dal costo interno del capitale a rischio, un disincentivo economico diretto dove attaccare e corrompere coesistono sullo stesso piano.[4][12]

A questo punto dovrebbe essere chiaro a tutti i lettori quanto, le implicazioni a cui sono soggetti i detentori delle rispettive reti, siano alla base estremamente diverse, tanto nelle metodologie quanto nel valore stesso della moneta. La PoW produce un costo aggiuntivo per ogni nuova moneta introdotta nel mercato che, con un mercato stabile, si avvicina al valore degli asset; potremmo quasi definirla una materia prima digitale. Da qui tutta l'analogia con la miniatura dell'oro e il suo costo di estrazione, a base dell'argomento "sound money" a favore di Bitcoin. La PoS, al contrario, non richiede un dispendio energetico esterno comparabile (le stime parlano di una riduzione di oltre il 99,9% del consumo energetico di Ethereum dopo il Merge) e distribuisce le ricompense in modo proporzionale al capitale già posseduto. È questo meccanismo che viene criticato in quanto diventa causa di tendenza verso la concentrazione di ricchezza e potere di governance. In poche parole, dalla rendita lavorativa (con costi ingenti e necessità di adoperare sistemi sempre più performanti) ad una semplice rendita di capitale (dove il più ricco continua ad essere selezionato e diventa più ricco).[23]
Queste reti, però, per quanto le più accreditate, usate e dominanti del mercato, sono solo le iniziatrici dei sistemi di convalida adottati. Da qui la diramazione è stata molto più complessa e si sono create tante sottocategorie di tipologie di reti da cui poi hanno preso vita tantissimi ecosistemi di monete. Parliamo di reti pubbliche, private, dove si è provato a dare un senso più centralizzato, autorizzate, dove è necessario essere autorizzati per parteciparvi, e infine di consorzi, gestiti da un gruppo di organizzazioni selezionate che condividono la responsabilità della rete (ideali per rapporti con responsabilità condivise come produttore-compratore).

---

[4] **I minatori ASIC (abbreviazione di Application Specific Integrated Circuit.):** Sono macchine essenziali per estrarre Bitcoin e criptovalute.

[5] **The Merge:** Importante aggiornamento di rete avvenuto il 15 settembre 2022, che ha portato con successo la transizione di Ethereum da un meccanismo di consenso Proof-of-Work (PoW) a un meccanismo Proof-of-Stake (PoS).

3. Il passaggio dalla moneta digitale alla finanza decentralizzata (DeFi)

A livello cronologico, il primo sistema di blockchain è stato Bitcoin nel 2008, creato dall'anonimo e mai identificato Satoshi Nakamoto. La ragione per cui fu creato era molto semplice: risolvere il problema di trasferire denaro direttamente da una persona a un'altra senza bisogno di banche o altri intermediari. Nel fare ciò fu creato con una struttura ed un funzionamento a prova di novizio, per risultare sicuro e prevedibile (non Turing-completo[6]). Un linguaggio di codice molto intuitivo con regole di pagamento non complesse senza logiche elaborate come in un vero linguaggio di programmazione. Una democratizzazione di un mondo così tecnico come la scienza computeristica. Le regole semplici potevano includere il richiedere più firme (multisign) o far sì che un pagamento venga effettuato solo dopo una certa data (timelock).[20]

Nel 2015 qualcosa cambia. Viene introdotto Ethereum ed assistiamo per la prima volta agli smart contract. Contrariamente a Bitcoin, sono dei programmi che permettono regole complesse come in un linguaggio e si eseguono automaticamente quando vengono soddisfatte determinate condizioni, senza che nessuna delle parti coinvolte debba fidarsi dell'altra o di un intermediario terzo. Se un registro distribuito può tenere traccia in modo affidabile non solo di "chi possiede cosa" ma anche di "quali regole logiche arbitrarie governano il trasferimento di quel valore", allora diventa possibile ricostruire, in forma disintermediata e programmabile, l'intera infrastruttura dei servizi finanziari: prestiti, scambi, derivati, assicurazioni, gestione del rischio. Questo ha decretato la nascita della finanza decentralizzata (DeFi), un sistema dove dei contratti intelligenti, programmati in maniera molto complessa, si eseguono autonomamente nel momento in cui le controparti dello scambio lo consentono e i requisiti richiesti sono interamente soddisfatti. Il passaggio tra Bitcoin ed Ethereum è lo spartiacque tra le generazioni cripto. Un passaggio reale da un mezzo di scambio debole ed un asset di valore, ad un computer autonomo su cui costruire una nuova finanza. La DeFi nasce concretamente tra il 2018 e il 2020 (il periodo noto come "DeFi Summer" nel 2020[25]) e s'intende l'insieme di prodotti e servizi di carattere finanziario di cui tutti gli agenti economici possedenti crypto e connessi a Internet possono usufruire. Si tratta di un mercato autonomo, mai chiuso e senza nessun potere centrale, che possa giudicare, aggiudicare o prendere decisioni su enti terzi. I protocolli con cui prese vita furono vari, come: MakerDAO (stablecoin decentralizzate collateralizzate), Compound e Aave (prestiti e mutui peer-to-peer algoritmici) e Uniswap (scambio decentralizzato tramite pool di liquidità automatizzati, gli Automated Market Makers o AMM).[10][8] L'innovazione strutturale di questi protocolli è, per come anticipato precedentemente, la sostituzione dell'intermediario umano (la banca che valuta il merito di credito, il market maker che fornisce liquidità, la borsa che abbina domanda e offerta) con codice open source, verificabile pubblicamente ed eseguito in modo deterministico dalla rete stessa.[7][9] Bitcoin in questa dinamica così forte, entro un cambiamento di utilizzo, è rimasto schiacciato proprio a livello strutturale. La coin madre, infatti, privilegia la sicurezza, la semplicità e la resistenza alla censura sopra ogni altra proprietà. Meno complessità significa meno superficie d'attacco e meno bug negli smart contract (che nella storia di Ethereum hanno causato perdite per miliardi di dollari, dal collasso del DAO nel 2016 a innumerevoli exploit successivi). Per molti anni gli strumenti finanziari costruiti su Bitcoin sono rimasti piuttosto semplici. Un esempio potrebbe essere il portafoglio multisign, che richiede più firme per spendere i fondi come se fosse una cassetta di sicurezza con più chiavi (ognuno mette la propria chiave privata crittografata che dà accesso al contratto). Altri potrebbero essere canali di pagamento come la Lightning Network pensati per pagamenti molto veloci e di piccolo importo, e soluzioni come il wrapped Bitcoin (WBTC), che permettono di usare Bitcoin su altre reti creando token che rappresentano BTC custoditi altrove. Recentemente però, gli utenti di Bitcoin si sono adoperati per la creazione di strumenti più sofisticati

---

[6] **La programmazione di una macchina di Turing:** Significa definire una serie di regole logiche per guidare una testina che legge, scrive o cancella simboli su un nastro infinito e cambia lo stato della macchina.

(Ordinals, BRC-20, Stacks e RSK) consentendo di costruire applicazioni di finanza decentralizzata (DeFi) più articolate mantenendo inalterate le regole di protocollo fondamentali, così da far persistere l'unicità della coin in sicurezza e stabilità. [14]
Su Ethereum, invece, la DeFi era parte integrante. La Ethereum Virtual Machine (EVM[7])[11], come ambiente esecutivo, ha permesso fin dalla nascita di creare una finanza completa. La tecnologia smart contract, poi, è stata il vero asso nella manica. Questa, infatti, vive come singolo e come componibile, il che significa che il contratto può essere singolo o chiamare altri contratti a catena continuando a soddisfare i requisiti di ciascuno ad ogni passaggio senza ulteriori permessi da richiedere (fenomeno conosciuto come "money legos[8]"). La differenza, in sintesi, non è solo tecnica ma di filosofia di rischio. Bitcoin ottimizza per la robustezza, l'immutabilità e la prevedibilità nel lunghissimo periodo, accettando una minore espressività; Ethereum ottimizza per la flessibilità e l'innovazione finanziaria, accettando una superficie d'attacco più ampia e una maggiore complessità sistemica (con tutti i rischi che questo comporta, dagli exploit agli smart contract mal auditati, fino al rischio sistemico di liquidazioni a cascata nei protocolli di lending sovracollateralizzati).

4. Il confronto con la finanza tradizionale

Arrivati a conclusione di questa digressione, è importante per il lettore comprendere cosa rende la DeFi così diversa dalla banca tradizionale in senso stretto.Quando si discute di economia, un rapporto fondamentale necessita di essere tenuto a mente: il rapporto tripartito tra soggetti in surplus (soggetti che hanno accumulato alcuni risparmi rispetto al loro stipendio), soggetti in deficit (soggetti che necessitano di un ulteriore reddito per ovviare a spese superiori alla loro capacità utile) e banche commerciali (intermediari tra queste due controparti). Il rapporto prevede che la banca riscatti il reddito in surplus sotto forma di depositi a breve o lungo termine e che lo riassegni, sotto forma di prestiti o mutui, ad i soggetti in deficit. Questo scambio è sempre stato tanto fondamentale quanto fallace. Per ragioni strutturali, le banche, qualora s'interfacciassero con un numero troppo elevato di prelievi, per quanto solventi nel merito dei propri attivi, non potrebbero onorare tutte le richieste contemporaneamente, perché il capitale sarebbe impiegato in attività illiquide. A maggior ragione, le banche commerciali non si limitano a trasferire i depositi dei risparmiatori verso i mutuatari, ma creano attivamente nuova moneta nel momento in cui erogano un prestito, accreditando l'importo sul conto del mutuatario senza prelevare da un deposito preesistente. Ciò è stato teoricamente comprovato dallo studio del 1983 firmato da Douglas Diamond e Philip Dybvig. La loro idea si basava sull'idea dell'imitazione. Dato un contratto di deposito bancario che offre liquidità immediata a chi ne ha bisogno e un rendimento maggiore a chi può attendere, si crea una situazione socialmente efficiente, generando un equilibrio in cui la banca funziona normalmente. Lo stesso identico contratto ammette un secondo equilibrio, egualmente coerente con la razionalità individuale. Ciascun depositante, difatti, trova razionale (qualora non ci fosse sicurezza sullo stato dei depositi) ritirare anche lui immediatamente, indipendentemente dal proprio effettivo bisogno di liquidità, semplicemente per non restare tra gli ultimi quando le riserve si saranno esaurite.[13] Poiché questo secondo equilibrio è autorealizzante, la sua eliminazione richiede un intervento esterno al gioco stesso, motivo per cui il sistema bancario, in risposta alle crisi affrontate, ha sviluppato quattro architetture istituzionali, con l'obiettivo di arginare e debellare le possibili crisi future. Rispettivamente:

---

[7] **EVM:** è una piattaforma software decentralizzata che esegue contratti intelligenti e calcola le modifiche dello stato della rete su Ethereum

[8] **Money lego (o DeFi lego):** Nel settore della finanza decentralizzata (DeFi), indica la capacità dei diversi protocolli basati su blockchain, di collegarsi e integrarsi tra loro come i mattoncini del famoso gioco. Grazie agli smart contract, gli utenti possono combinare servizi finanziari diversi, come prestiti, scambi e depositi, per creare strumenti nuovi e complessi.

1. L'assicurazione dei depositi elimina l'equilibrio di panico, rendendo irrilevante, per il singolo depositante, la velocità con cui ritira i propri fondi. Un depositante che sa di recuperare comunque i propri fondi entro i limiti di garanzia non ha alcun incentivo razionale a precipitarsi allo sportello prima degli altri, e il bad equilibrium del modello di Diamond e Dybvig smette semplicemente di essere un equilibrio.
2. Il prestatore di ultima istanza trova la sua formulazione classica in Walter Bagehot, il cui trattato del 1873 rimane il riferimento canonico della materia. In tempi di panico, una banca centrale deve prestare liberamente, a tassi punitivi, contro buon collaterale. "Prestare liberamente" impedisce che una crisi di liquidità temporanea si trasformi, per mancanza di fondi disponibili, in una crisi di solvibilità permanente. Il "tasso punitivo" disincentiva il ricorso al sostegno della banca centrale in condizioni normali, limitando il rischio morale. Infine, il vincolo del "buon collaterale" assicura che l'intervento sostenga istituzioni solventi ma illiquide, non istituzioni già insolventi.
3. I requisiti di capitale, codificati a livello internazionale negli accordi di Basilea[9], impongono alle banche di detenere una quota minima di capacità utile. Proprio a fronte degli attivi ponderati per il rischio, le perdite si scarichino anzitutto sugli azionisti e non immediatamente sui depositanti. In termini pratici, questo significa che su cento unità di prestiti erogati, la banca deve aver già accantonato, sotto forma di capitale proprio, un cuscinetto sufficiente ad assorbire un deterioramento significativo del valore di quei prestiti, prima che le perdite raggiungano i depositanti.
4. La supervisione prudenziale discrezionale comprende: stress test periodici, limiti alla concentrazione del rischio, richieste di accantonamenti addizionali e interventi nella governance in caso di difficoltà. Si tratta quindi di un potere discrezionale continuo che nessuna delle altre tre istituzioni possiede, e che permette di intervenire su una situazione di rischio prima che si trasformi in crisi conclamata, non soltanto ad attenuare le conseguenze una volta manifestate.

5. Conclusione ed ultime riflessioni

Le metodologie risolutive alle crisi, non si sono create autonomamente né tantomeno come sovrastrutture burocratiche senza le quali il sistema funzionerebbe ugualmente bene, bensì sono frutto di un problema strutturale della finanza identificato empiricamente attraverso crisi specifiche e costosissime. Tale concetto è fondamentale, in quanto, se la DeFi replica fedelmente le prerogative e le funzioni della banca, allo stesso tempo, sconosce empiricamente e non applica nessuna delle quattro architetture di assorbimento delle inefficienze.

Ecco che l'assenza di discrezionalità tipica degli smart contract diventa una compressione e non un vantaggio. Da un lato elimina corruzione, conflitto d'interesse ed errore soggettivo, ma dall'altro, strutturalmente, non può annullare, nonostante le circostanze lo possano necessitare, le proprie regole settate nel codice. La Banca dei Regolamenti Internazionali (BIS) ha messo in guardia contro la non realisticità di costruire un intero sistema finanziario basato solo su operazioni automatiche. Al contrario, sostiene la tesi secondo cui, in certe situazioni, i progetti DeFi avranno bisogno di modifiche o di decisioni prese da persone (giudizio discrezionale) per risolvere problemi[18]. Nella DeFi, la fiducia, "codificata ex ante", è mediata dal codice. Questo produce un'efficienza informativa e operativa notevole in quanto esiste un solo registro condiviso e verificabile da chiunque in tempo reale.

C'è poi una differenza più sottile, di natura quasi epistemologica. La finanza tradizionale si basa su un modello di fiducia "sociale e legale" le regole sono ineseguibili in modo diverso da come sono scritte, il che elimina il rischio di arbitrarietà discrezionale (nessuno può decidere unilateralmente di

[9]**Accordi di Basilea:** Sono linee guida internazionali sulla vigilanza e sui requisiti di capitale delle banche. Definiti dal Comitato di Basilea, servono a garantire la stabilità del sistema finanziario globale, evitando che gli istituti di credito falliscano in caso di gravi crisi.

congelare i tuoi fondi o cambiare le condizioni di un prestito già in essere) ma elimina anche la flessibilità correttiva che un giudice umano, o un intervento regolamentare, può offrire di fronte a un evento imprevisto o a un'ingiustizia palese. È il classico compromesso tra "rule of law" discrezionale e "rule of code" deterministico, e non è affatto scontato quale dei due modelli produca, nel lungo periodo, maggiore stabilità sistemica ed equità distributiva, è anzi precisamente il tipo di tensione teorica che rende interessante, dal punto di vista della ricerca, l'analisi della "finanza decentralizzata" come esperimento istituzionale reale su scala globale.
Esiste quindi un percorso non necessariamente divisivo tra le due visioni di finanza. Al contrario, uno scambio costruttivo in cui i risvolti positivi dell'una possano essere integrati nell'altra. Del resto, il Financial Stability Board (FSB) sostiene che la DeFi presenti rischi simili a quelli della finanza tradizionale, anche se quei rischi possono apparire in modo diverso sulla base della tecnologia adoperata. Al momento le connessioni tra DeFi e sistema finanziario tradizionale sono limitate, ma potrebbero crescere, qualora la DeFi si espandesse. [27][22][24]
Allo stesso tempo, il Fondo Monetario Internazionale (FMI), ritiene che, per ora, i rischi che le criptovalute e la DeFi pongono alla stabilità finanziaria non siano ancora tali da minacciare l'intero sistema. È d'obbligo però sottolineare, che il fenomeno è globale e le regole in molti Paesi sono insufficienti, perciò va monitorato con particolare attenzione.[26] Concludo citando il padre di tutto ciò che è stato discusso in questa sede, Satoshi Nakamoto: "'If you don't believe me or don't get it, I don't have time to try to convince you, sorry"(Se non ci credi o non lo capisci, non ho tempo per cercare di convincerti, mi dispiace). [21]

Bibliography

1. Admin. 2020. "Blockchain: Cos'è Un Blocco E Com'è Fatto." Knobs, April. https://knobs.it/blockchain-cose-un-blocco-e-come-fatto/.
2. Amazon Web Services. 2026. "Cos'è La Tecnologia Blockchain?" Amazon Web Services, Inc., August 20. https://aws.amazon.com/it/what-is/blockchain/.
3. Aranzulla, Salvatore. 2026. "Come Funziona Il Mining." Salvatore Aranzulla, Aranzulla.it. https://www.aranzulla.it/come-funziona-il-mining-1293103.html.
4. Beech, Elena. 2025. "What Is Ethereum? Explaining ETH, Smart Contracts, DeFi and More." Exp.Science. https://www.exp.science/education/what-is-ethereum-explaining-eth-smart-contracts-defi.
5. Borsaitaliana.It. 2026a. "Borsa Italiana." https://www.borsaitaliana.it/borsa/glossario/criptovaluta.html.
6. Brown, Jefreda R., and Yarilet Perez. 2019. "Nonce." Investopedia. https://www.investopedia.com/terms/n/nonce.asp.
7. BSEtec. 2024. "Ethereum and Its Implication for DeFi- How Ethereum and DeFi Are Synonymous." BSEtec, April 2. https://www.bsetec.com/blog/ethereum-and-its-implication-for-defi-how-ethereum-and-defi-are-synonymous/.

8. Buterin, Vitalik. 2014. “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.” *Ethereum Foundation*. https://ethereum.org/en/whitepaper/.
9. Crypto.Com. 2026b. “Cosa Sono Gli Smart Contract Nella Blockchain E Come Funzionano?” March 9. https://crypto.com/it/crypto/learn/what-are-smart-contracts-in-blockchain-and-how-do-they-work.
10. Culicchi, Roberto, and Rosario Albanese. 2021. “Cos’è La Finanza Decentralizzata (DEFI)? Vantaggi E Rischi.” Agenda Digitale, December 8. https://www.agendadigitale.eu/cittadinanza-digitale/pagamenti-digitali/criptovalute-e-finanza-decentralizzata-e-tutto-oro-quel-che-luccica-vantaggi-e-rischi/.
11. Cyfrin.Io. 2025a. “Cyfrin Glossary: Ethereum Virtual Machine (EVM).” https://www.cyfrin.io/glossary/ethereum-virtual-machine-evm.
12. Di Mento, Katie. 2019. “Proof of Work Vs. Proof of Stake: Understanding the Difference - Blockdaemon.” Blockdaemon.Com. https://www.blockdaemon.com/blog/proof-of-work-vs-proof-of-stake-whats-the-difference.
13. Diamond, Douglas W., and Philip H. Dybvig. 1983. “Bank Runs, Deposit Insurance, and Liquidity.” *Journal of Political Economy* 91 (3): 401–19. https://www.minneapolisfed.org/research/quarterly-review/bank-runs-deposit-insurance-and-liquidity.
14. Ethereum Community. 2026. “Finanza Decentralizzata (DeFi).” Ethereum.Org. https://ethereum.org/it/defi/.
15. Ethereum.Org. 2025b. “The Merge | Ethereum.Org.” https://ethereum.org/roadmap/merge/.
16. Finst Team. 2025. “Cosa È L’hashing? | Accademia Cripto.” Finst.Com, Finst, June 13. https://finst.com/it/learn/articles/what-is-hashing.
17. Finst Team. 2026. “Cos’è Un Protocollo Crypto E Come Funziona? | Accademia Cripto.” Finst.Com, Finst, April 10. https://finst.com/it/learn/articles/what-is-a-crypto-protocol.
18. Hyun Song Shin. 2021. In *BIS Quarterly Review*. December.
19. Mempool.Space. n.d. “The Mempool Open Source Project®.” Accessed August 31, 2026. https://mempool.space/docs/faq#what-is-a-mempool.
20. Nakamoto, Satoshi. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf.
21. Nakamoto, Satoshi. 2010. "Re: Scalability and Transaction Rate." Satoshi Nakamoto Institute (archivio dei post Bitcointalk), July 29. https://satoshi.nakamotoinstitute.org/posts/bitcointalk/287/.
22. PostFinance. 2025c. “Comprendere La DeFi: Opportunità, Rischi E Applicazioni Della Finanza Decentralizzata.”

https://www.postfinance.ch/it/blog/guida-semplice-e-chiara-agli-investimenti/comprendere-defi.html.

23. Reddy, Rohan. 2022. “Proof of Work Vs. Proof of Stake: Why Their Differences Matter.” Globalxetfs.Com. https://www.globalxetfs.com/articles/proof-of-work-vs-proof-of-stake-why-their-differences-matter.
24. Ricci, Alessandro. 2023. “DeFi Vs Traditional Finance: What Is the Difference?” Scaling Parrots, September 28. https://www.scalingparrots.com/en/defi-vs-traditional-finance-the-difference/.
25. RugDoc IO | #1 DeFi Safety & Education Community. 2026c. “What Was the DeFi Summer: Find out What It Means.” January 28. https://rugdoc.io/wiki/docs/defi-summer-definition/.
26. “The Crypto Ecosystem and Financial Stability Challenges.” 2021. In *Global Financial Stability Report*. IMF. https://www.imf.org/-/media/Files/Publications/GFSR/2021/October/English/ch2.ashx.
27. “The Financial Stability Risks of Decentralised Finance.” 2023. In *Financial Stability Board*. https://www.fsb.org/uploads/P160223.pdf.