STRATOS
Research

From Digital Currency to Decentralized Finance: An Introduction

A Comparative Analysis of Consensus Mechanisms, Programmable Finance, Crisis-Management Frameworks, and the Tension Between Rule of Law and Rule of Code

Cosimo Petralia

October 14, 2026

---

1. Introduction: Cryptocurrencies

Cryptocurrencies represent a new landscape, whose exceptions and peculiarities make it a relevant phenomenon of the digital economy. They are an asset potentially able to affect some of the economic and financial arrangements of a centuries-old economy by integrating technology into financial and economic processes, and they constitute a technological and financial sector that is still evolving. By definition, cryptocurrencies are digital currencies that share the functions of traditional money, namely exchange, deposit and investment [5]. What sets them apart is that they are entirely decentralized, and therefore not issued, guaranteed or controlled by central banks or public authorities. How, then, can they be exchanged without a third-party bank to handle the transaction and hold the deposit? The answer lies in the system on which they operate, the blockchain. As IBM puts it, blockchain "is a shared, immutable digital ledger, enabling the recording of transactions and the tracking of assets within a business network and providing a single source of truth." The underlying idea is simple. A crypto holder initiates a transaction. Before being collected and validated on the chain, the transaction sits in a waiting area, the mempool[1] [19], which acts as temporary memory. From there it is verified by a validator node (or by a miner, depending on the consensus mechanism adopted). The node, selected by the network according to criteria defined by the consensus protocol, gathers as many transactions as it can and "validates" them, forming a new block. The block is assigned a unique cryptographic code that incorporates the digital fingerprint of the previous block, which is what creates the chain. Once accepted, the block is distributed and permanently added to the ledger held by every node. In addition, every block carries a timestamp indicating exactly when the transaction was entered into the blockchain [1, 2]. The timestamp keeps transactions in chronological order and makes the data more secure, because it prevents information recorded in the past from being modified. The consensus mechanism is what makes the system secure and transparent, while the length of the chain, given that the encrypted code grows longer and more complex with every block, is what makes it very difficult to alter, although security depends on the protocol, on its implementation and on private keys. It is important to note, however, that consensus mechanisms come in distinct types, which differ

[1] The mempool (short for memory pool) is the temporary memory area where nodes of the Bitcoin network hold transactions that have not yet been confirmed, before miners include them in a block.

both in how the validator node is chosen and in how confirmation takes place. Among them, the two dominant and most widely established solutions today are Proof of Work (PoW) and Proof of Stake (PoS) [17].

2. PoW vs PoS

Proof of Work is the method Bitcoin has used since 2009, and it relies on the computing power of the devices involved. Participants, called miners, compete to solve a very demanding cryptographic puzzle. They must try an enormous number of combinations until they find a value called a nonce[2] [6]. Combined with the block data, this value produces a hash[3] [16] that meets a set difficulty rule. There is no mathematical shortcut, and the only way to find the solution is to try billions of combinations per second, a process that consumes enormous amounts of electricity. The first miner to find the hash becomes the validator of the block and receives a reward in bitcoin plus the transaction fees. As the number of blocks increases, the computing power and the time needed to find the hash also grow, and these in turn become guarantors of Bitcoin's security and strength. To rewrite the history of the blockchain (for example to carry out a double spend), an attacker would need more than half of the computing power of the entire network (a 51% attack), an economically prohibitive undertaking on a mature network such as Bitcoin's, where the cost of hardware (ASICs[4]) and energy is measured in billions of dollars. In essence, PoW anchors digital security to a real physical and energy cost, which is why Bitcoin supporters often describe it as "energy turned into truth" [3].

Proof of Stake, fully adopted by Ethereum with The Merge[5] [15] in September 2022 after years of transition, replaces computational work with a direct economic guarantee. Instead of having energy-intensive computers compete, anyone wishing to help validate transactions locks up (stakes) a significant amount of the network's native cryptocurrency as collateral. Validators are selected pseudo-randomly, weighted by the amount staked, to propose and attest blocks. The more liquid funds a participant locks up as collateral, the greater the authority it gains in validation, a prerogative assigned objectively by the network's code. If a validator acts improperly (for example by validating two conflicting blocks, a behaviour that falls under a "slashing condition"), it loses part or all of its staked capital. Security therefore rests on the internal cost of capital at risk, whereas in PoW it rests on the external cost of energy. This is a direct economic disincentive, because the capital needed to attack or corrupt the network is the same capital that would be lost in doing so [4, 12].

It should now be clear how deeply the implications for holders of the two networks differ, both in their methods and in the value of the currency itself. PoW attaches a cost to every new coin introduced into the market, and in a stable market this cost approaches the coin's value, so that it could almost be called a digital commodity. Hence the analogy with gold mining and its extraction cost, which underpins the "sound money" argument for Bitcoin. PoS, by contrast, requires no comparable external energy expenditure (estimates point to a reduction of more than 99.9% in Ethereum's energy consumption after the Merge) and distributes rewards in proportion to the capital already held. This mechanism is criticized because it tends to concentrate wealth and governance power. In short, the system moves from a return on work (with heavy costs and the need for ever more powerful hardware) to a pure return on capital (where the wealthiest participants keep being selected and grow

[2] A nonce is a 32-bit number placed in the header of a block, which miners repeatedly modify in order to solve the cryptographic puzzle of Proof of Work. The term stands for "number used only once".

[3] A hash is a fixed-length digital code generated by the SHA-256 cryptographic algorithm to secure and link the blocks of the blockchain.

[4] ASIC (Application-Specific Integrated Circuit) miners are specialized machines essential for mining Bitcoin and other cryptocurrencies.

[5] The Merge was a major network upgrade, completed on 15 September 2022, that moved Ethereum from a Proof-of-Work (PoW) to a Proof-of-Stake (PoS) consensus mechanism.

wealthier) [23].

However established, widely used and dominant these two networks may be, they were only the first of the validation systems in use. From them the field has branched out considerably, producing many subcategories of networks, each of which has given rise to numerous coin ecosystems. These include public networks; private networks, which adopt a more centralized design; permissioned networks, where participation requires authorization; and consortium networks, run by a group of selected organizations that share responsibility for the network (well suited to relationships with shared responsibilities, such as those between producer and buyer).

3. The shift from digital money to decentralized finance (DeFi)

Chronologically, the first blockchain system was Bitcoin, created in 2008 by the anonymous and never identified Satoshi Nakamoto. Its purpose was simple, namely to allow money to be transferred directly from one person to another without banks or other intermediaries. To this end it was given a deliberately simple structure and operation, accessible even to non-experts, so as to be secure and predictable (it is not Turing-complete[6]). Its code language is intuitive, with uncomplicated payment rules and none of the elaborate logic found in a full programming language. It amounted to a democratization of a field as technical as computer science. These simple rules could include requiring several signatures (multisig) or allowing a payment only after a certain date (timelock) [20].

In 2015 things changed. Ethereum was launched, and with it smart contracts appeared for the first time. Unlike Bitcoin, smart contracts are programs that can encode complex rules, as a full programming language does, and that execute automatically when given conditions are met, without any party having to trust the other or a third-party intermediary. If a distributed ledger can reliably keep track not only of "who owns what" but also of "which arbitrary logical rules govern the transfer of that value", then it becomes possible to rebuild, in a disintermediated and programmable form, the entire infrastructure of financial services, including lending, trading, derivatives, insurance and risk management. This marked the birth of decentralized finance (DeFi), a system in which complex smart contracts execute autonomously as soon as the counterparties consent and all the required conditions are met. The shift from Bitcoin to Ethereum marks the watershed between generations of crypto, a genuine move from a weak medium of exchange and store of value to an autonomous computer on which a new kind of finance can be built. DeFi took concrete shape between 2018 and 2020, the latter year being known as the "DeFi Summer" [25]. The term refers to the set of financial products and services available to any economic agent who holds crypto and has an Internet connection. It is an autonomous market that never closes, with no central authority able to judge, adjudicate or make decisions affecting third parties. The first protocols included MakerDAO (decentralized collateralized stablecoins), Compound and Aave (algorithmic peer-to-peer loans and mortgages) and Uniswap (decentralized exchange through automated liquidity pools, known as Automated Market Makers or AMMs) [8, 10]. As noted above, the structural innovation of these protocols is the replacement of the human intermediary (the bank that assesses creditworthiness, the market maker that provides liquidity, the exchange that matches supply and demand) with open-source code, publicly verifiable and executed deterministically by the network itself [7, 9]. Amid this fast-moving shift in how blockchains were used, Bitcoin was held back by its own structure. The original cryptocurrency prioritizes security, simplicity and censorship resistance above every other property. Less complexity means a smaller attack surface and fewer bugs in smart contracts, which in Ethereum's history have caused losses of billions of dollars, from the collapse of The DAO in 2016 to countless later exploits. For many years the financial

[6]Programming a Turing machine means defining a set of logical rules that guide a head which reads, writes or erases symbols on an infinite tape and changes the state of the machine.

instruments built on Bitcoin remained fairly simple. One example is the multisig wallet, which requires several signatures to spend funds, much like a safe deposit box with several keys (each party contributes its own cryptographic private key, which grants access to the contract). Others include payment channels such as the Lightning Network, designed for very fast, small-value payments, and solutions such as wrapped Bitcoin (WBTC), which allow Bitcoin to be used on other networks through tokens that represent BTC held elsewhere. More recently, however, the Bitcoin community has developed more sophisticated tools (Ordinals, BRC-20, Stacks and RSK) that make it possible to build more elaborate DeFi applications while leaving the core protocol rules unchanged, thus preserving the coin's distinctive security and stability [14].

On Ethereum, by contrast, DeFi was an integral part of the design from the start. As an execution environment, the Ethereum Virtual Machine (EVM)[7] [11] has made it possible from the outset to build a complete financial system. Smart contracts were the decisive advantage. They can operate individually or be composed, meaning that a contract can stand alone or call other contracts in sequence, satisfying the requirements of each at every step without requesting further permissions (a property known as "money legos"[8]). In short, the difference extends beyond technology to the philosophy of risk. Bitcoin optimizes for robustness, immutability and predictability over the very long run, accepting lower expressiveness; Ethereum optimizes for flexibility and financial innovation, accepting a broader attack surface and greater systemic complexity, with all the risks this entails, from exploits and poorly audited smart contracts to the systemic risk of cascading liquidations in overcollateralized lending protocols.

4. Comparison with traditional finance

With this background in place, it is important to understand what makes DeFi so different from a traditional bank in the strict sense. A fundamental relationship in economics is the three-way link between surplus units (agents who have accumulated savings out of their income), deficit units (agents who need additional funds because their expenses exceed their available income) and commercial banks, which intermediate between the two. The bank collects surplus funds as short- or long-term deposits and reallocates them to deficit units as loans or mortgages. This exchange has always been as fundamental as it is flawed. For structural reasons, a bank facing too many withdrawals at once cannot honour them all simultaneously, however solvent its assets may be, because its capital is tied up in illiquid assets. This is all the more true because commercial banks do more than transfer savers' deposits to borrowers. They actively create new money when they grant a loan, crediting the amount to the borrower's account without drawing on any pre-existing deposit. This was demonstrated theoretically in the 1983 study by Douglas Diamond and Philip Dybvig. Their argument rests on the idea of imitation. A deposit contract that offers immediate liquidity to those who need it and a higher return to those who can wait produces a socially efficient outcome, an equilibrium in which the bank operates normally. The very same contract admits a second equilibrium, equally consistent with individual rationality. If there is uncertainty about the state of the deposits, each depositor finds it rational to withdraw immediately as well, whatever their actual need for liquidity, simply to avoid being among the last in line when reserves run out [13]. Since this second equilibrium is self-fulfilling, eliminating it requires an intervention external to the game itself. This is why, in response to past crises, the banking system has developed four institutional architectures aimed at containing and preventing future ones.

[7] The Ethereum Virtual Machine (EVM) is the decentralized software environment that executes smart contracts and computes changes to the state of the Ethereum network.

[8] In decentralized finance, "money legos" (or "DeFi legos") refers to the ability of different blockchain protocols to connect and integrate with one another like the bricks of the well-known toy. Through smart contracts, users can combine different financial services, such as lending, trading and deposits, to create new and complex instruments.

1. Deposit insurance eliminates the panic equilibrium by making the speed at which an individual depositor withdraws their funds irrelevant. A depositor who knows they will recover their funds in any case, within the limits of the guarantee, has no rational incentive to rush to the bank ahead of others, and the bad equilibrium of the Diamond and Dybvig model simply stops being an equilibrium.
2. The lender of last resort finds its classic formulation in Walter Bagehot, whose 1873 treatise remains the canonical reference on the subject. In times of panic, a central bank must lend freely, at penalty rates, against good collateral. "Lending freely" prevents a temporary liquidity crisis from turning, for lack of available funds, into a permanent solvency crisis. The "penalty rate" discourages recourse to central bank support in normal conditions, limiting moral hazard. Finally, the "good collateral" requirement ensures that the intervention supports solvent but illiquid institutions, and not institutions that are already insolvent.
3. Capital requirements, codified internationally in the Basel Accords[9], oblige banks to hold a minimum amount of capital against their risk-weighted assets, so that losses are borne first by shareholders and reach depositors only afterwards. In practical terms, for every hundred units of loans granted, the bank must already have set aside, as equity, a cushion large enough to absorb a significant deterioration in the value of those loans before losses reach depositors.
4. Discretionary prudential supervision comprises periodic stress tests, limits on risk concentration, requests for additional provisions and intervention in governance when a bank is in difficulty. It is a continuous discretionary power that none of the other three architectures possesses, and it allows authorities to act on a risk before it becomes a full-blown crisis, in addition to mitigating its consequences once it has materialized.

5. Conclusion and final remarks

These crisis-resolution tools are the response to a structural problem of finance, identified empirically through specific and extremely costly crises, and the system would not work equally well without them. This point is fundamental. While DeFi faithfully replicates the prerogatives and functions of a bank, in practice it disregards, and does not apply, any of the four architectures for absorbing these inefficiencies.

The absence of discretion typical of smart contracts therefore turns out to be a constraint. On the one hand it eliminates corruption, conflicts of interest and subjective error; on the other, by its very structure, it cannot override the rules written into the code, even when circumstances require it. The Bank for International Settlements (BIS) has warned that building an entire financial system solely on automated operations is unrealistic, and argues that in certain situations DeFi projects will need modifications or decisions taken by people (discretionary judgement) to solve problems [18]. In DeFi, trust is "coded ex ante" and mediated by code. This yields remarkable informational and operational efficiency, since there is a single ledger, shared and verifiable by anyone in real time.

There is also a subtler difference, of an almost epistemological nature. Traditional finance rests on a model of "social and legal" trust. The rules cannot be executed in any way other than as they are written, which eliminates the risk of discretionary arbitrariness (no one can unilaterally decide to freeze your funds or change the terms of an existing loan) but also eliminates the corrective flexibility that a human judge, or a regulatory intervention, can offer in the face of an unforeseen event or a blatant injustice. It is the classic trade-off between discretionary "rule of law" and deterministic "rule of code". Which of the two models produces greater systemic stability and distributive fairness in the long run is far

[9]The Basel Accords are international standards on banking supervision and bank capital requirements, set by the Basel Committee on Banking Supervision to safeguard the stability of the global financial system by preventing credit institutions from failing during severe crises.

from obvious, and this is precisely the kind of theoretical tension that makes “decentralized finance”, as a real institutional experiment on a global scale, worth studying.

The two visions of finance therefore need not be opposed. A constructive exchange is possible, in which the strengths of one can be integrated into the other. The Financial Stability Board (FSB) holds that DeFi presents risks similar to those of traditional finance, although they may manifest differently depending on the technology used. Links between DeFi and the traditional financial system are currently limited, but they could grow if DeFi expands [22, 24, 27].

The International Monetary Fund (IMF), for its part, considers that the risks cryptocurrencies and DeFi currently pose to financial stability are not yet large enough to threaten the system as a whole. It should be stressed, however, that the phenomenon is global and that regulation in many countries remains insufficient, so it needs to be monitored with particular care [26]. I close by quoting the father of everything discussed here, Satoshi Nakamoto: “If you don’t believe me or don’t get it, I don’t have time to try to convince you, sorry” [21].

References

[1] Admin. Blockchain: Cos'è Un Blocco E Com'è Fatto. Knobs, April. https://knobs.it/blockchain-cose-un-blocco-e-come-fatto/, 2020.

[2] Amazon Web Services. Cos'è La Tecnologia Blockchain? Amazon Web Services, Inc., August 20. https://aws.amazon.com/it/what-is/blockchain/, 2026.

[3] Salvatore Aranzulla. Come Funziona Il Mining. Salvatore Aranzulla, Aranzulla.it. https://www.aranzulla.it/come-funziona-il-mining-1293103.html, 2026.

[4] Elena Beech. 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, 2025.

[5] Borsaitaliana.It. Borsa Italiana. https://www.borsaitaliana.it/borsa/glossario/criptovaluta.html, 2026.

[6] Jefreda R. Brown and Yarilet Perez. Nonce. Investopedia. https://www.investopedia.com/terms/n/nonce.asp, 2019.

[7] BSEtec. 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/, 2024.

[8] Vitalik Buterin. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum Foundation. https://ethereum.org/en/whitepaper/, 2014.

[9] Crypto.Com. 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, 2026.

[10] Roberto Culicchi and Rosario Albanese. 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/, 2021.

[11] Cyfrin.Io. Cyfrin Glossary: Ethereum Virtual Machine (EVM). https://www.cyfrin.io/glossary/ethereum-virtual-machine-evm, 2025.

[12] Katie Di Mento. Proof of Work Vs. Proof of Stake: Understanding the Difference. Blockdaemon.Com. https://www.blockdaemon.com/blog/proof-of-work-vs-proof-of-stake-whats-the-difference, 2019.

[13] Douglas W. Diamond and Philip H. Dybvig. Bank Runs, Deposit Insurance, and Liquidity. *Journal of Political Economy*, 91(3):401–419, 1983. https://www.minneapolisfed.org/research/quarterly-review/bank-runs-deposit-insurance-and-liquidity.

[14] Ethereum Community. Finanza Decentralizzata (DeFi). Ethereum.Org. https://ethereum.org/it/defi/, 2026.

[15] Ethereum.Org. The Merge. Ethereum.Org. https://ethereum.org/roadmap/merge/, 2025.

[16] Finst Team. Cosa È L'hashing? Accademia Cripto. Finst.Com, Finst, June 13. https://finst.com/it/learn/articles/what-is-hashing, 2025.

[17] Finst Team. 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, 2026.

[18] Hyun Song Shin. BIS Quarterly Review. December, 2021.

[19] Mempool.Space. The Mempool Open Source Project. Accessed August 31, 2026. https://mempool.space/docs/faq#what-is-a-mempool, n.d.

[20] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, 2008.

[21] Satoshi Nakamoto. Re: Scalability and Transaction Rate. Satoshi Nakamoto Institute (Bitcointalk post archive), July 29. https://satoshi.nakamotoinstitute.org/posts/bitcointalk/287/, 2010.

[22] PostFinance. 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, 2025.

[23] Rohan Reddy. 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, 2022.

[24] Alessandro Ricci. DeFi Vs Traditional Finance: What Is the Difference? Scaling Parrots, September 28. https://www.scalingparrots.com/en/defi-vs-traditional-finance-the-difference/, 2023.

[25] RugDoc IO | #1 DeFi Safety & Education Community. What Was the DeFi Summer: Find out What It Means. January 28. https://rugdoc.io/wiki/docs/defi-summer-definition/, 2026.

[26] The Crypto Ecosystem and Financial Stability Challenges. In Global Financial Stability Report. IMF. https://www.imf.org/-/media/Files/Publications/GFSR/2021/October/English/ch2.ashx, 2021.

[27] The Financial Stability Risks of Decentralised Finance. In Financial Stability Board. https://www.fsb.org/uploads/P160223.pdf, 2023.