

From Digital Currency to Decentralized Finance: Blockchain, Banking, and the Institutional Design of Financial Trust

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 8, 2026

1. Introduction: Crypto

A new scenario, with exceptions and peculiarities suited to making it the new revolutionary wave of the century. An asset capable of shaking the foundations and the core dogmas of a centuries-old economy, through the integration of technology into financial and economic processes. A world at the cutting edge, that of cryptocurrencies. By definition, crypto are digital currencies that hold those prerogatives proper to traditional money: exchange, deposit and investment [5]. What sets them apart is the fact that they are entirely decentralized, and therefore free from issuance, guarantee and control by central banks or public authorities. But then, how can they be exchanged without third-party banking entities for the transaction and the deposit? The answer lies in their basic operating system, that of blockchains. As reported by IBM, the blockchain “is a shared and immutable digital ledger which allows transactions to be recorded and assets to be tracked within a business network, and provides a single reliable source”. The underlying idea is simple. An ordinary crypto holder makes a transaction. Before being collected and validated by the chain, the transaction is placed in a waiting room (the mempool¹) [18] which acts as temporary memory. From there the transaction is verified by a validator node (or a miner, depending on the consensus practice adopted) which, being selected by the computer on the basis of objective, meritocratic and transparent criteria, gathers as many transactions as it is able to select and “validates” them so that the new block is formed. The block is associated with a unique cryptographic code that includes the digital fingerprint of the previous block, creating the chain and, once allowed, it is distributed and permanently added to the ledger of all nodes.

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

In addition, every block carries a timestamp indicating exactly when the transaction was entered into the blockchain [1, 2]. This time record keeps transactions in chronological order and makes the data more secure, because it prevents information recorded in the past from being modified. The consensus practice is what makes the system secure and transparent, and the size of the chain, given that the encrypted code grows longer and more complicated with every block, is what makes hacking virtually extremely difficult. It is, however, an important point to raise that these practices come in different and distinct types, each of which differs both in the criteria for choosing the validator node and in the mechanism to be adopted for confirmation. Among consensus mechanisms, the two dominant and most widely credited solutions today are, respectively, 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 works on the basis of the computing power of the devices employed. The participants, called miners, compete to solve a very difficult computational cryptographic problem. They have to try a great many different combinations until they find a value called a nonce² [6]. Combined with the block data, it produces a special result, the hash³ [16], which complies with a 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 miner who manages to find the hash first becomes the validator of the block and receives a reward in bitcoin plus the transaction fees. The more the blocks increase, the more the computing power and the time needed to solve the hash grow, themselves becoming 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 have to hold 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 (ASIC⁴) and energy is measured in billions of dollars. PoW, in essence, anchors digital security to a real physical and energy cost, and this is why Bitcoin supporters often define it as "energy turned into truth" [3].

Proof of Stake, on the other hand, adopted by Ethereum in full with "The Merge"⁵ [15] in September 2022 (after years of transition), replaces computational work with a direct economic guarantee. Instead of making energy-hungry computers compete, here whoever wants to help validate transactions puts on deposit (staking) a significant amount of the network's native cryptocurrency as collateral. Validators are selected pseudo-randomly, weighted by the amount put in stake, to propose and attest blocks. The more liquid capacity one leaves as frozen collateral, the more authority one acquires and earns in validation, a prerogative assigned objectively by the network's code mechanism. If a validator acts improperly (for example by validating two conflicting blocks, a behaviour called a "slashing condition"), it loses part or all of its staked capital. Security, then, does not derive from the external cost of energy but from the internal cost of capital at risk, a direct economic disincentive where attacking and corrupting coexist on the same plane [4, 12].

At this point it should be clear to all readers how deeply different, at their root, the impli-

²A 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 word comes from the English "number used only once".

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

⁴ASIC miners (short for Application Specific Integrated Circuit) are machines essential for mining Bitcoin and cryptocurrencies.

⁵The Merge: a major network upgrade that took place on 15 September 2022, which successfully carried Ethereum's transition from a Proof-of-Work (PoW) consensus mechanism to a Proof-of-Stake (PoS) one.

cations faced by the holders of the respective networks are, as much in their methodologies as in the very value of the currency. PoW produces an additional cost for every new coin introduced into the market which, with a stable market, comes close to the value of the assets; we could almost call it a digital commodity. Hence the whole analogy with the mining of gold and its extraction cost, at the basis of the “sound money” argument in favour of Bitcoin. PoS, by contrast, does not require a comparable external energy expenditure (estimates speak of a reduction of over 99.9% in Ethereum’s energy consumption after the Merge) and distributes rewards in proportion to the capital already held. It is this mechanism that is criticized, in that it becomes a cause of a tendency towards the concentration of wealth and governance power. In short, from a return on labour (with heavy costs and the need to employ ever more performing systems) to a simple return on capital (where the richest keeps being selected and becomes richer) [21].

These networks, however, for all that they are the most credited, used and dominant on the market, are only the initiators of the validation systems adopted. From there the branching has been far more complex, and so many subcategories of network types have been created, from which a great many coin ecosystems have then come to life. We are talking about public networks, private ones, where an attempt has been made to give a more centralized sense to them, permissioned ones, where authorization is required in order to take part, and finally consortia, run by a group of selected organizations that share responsibility for the network (ideal for relationships with shared responsibility such as producer-buyer).

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

Chronologically, the first blockchain system was Bitcoin in 2008, created by the anonymous and never identified Satoshi Nakamoto. The reason it was created was very simple: to solve the problem of transferring money directly from one person to another without the need for banks or other intermediaries. In doing so it was built with a structure and a way of working that were novice-proof, so as to be secure and predictable (not Turing-complete⁶). A very intuitive code language with uncomplicated payment rules, without elaborate logic of the kind found in a real programming language. A democratization of a world as technical as computer science. The simple rules could include requiring several signatures (multisign) or ensuring that a payment is made only after a certain date (timelock) [19].

In 2015 something changes. Ethereum is introduced and we witness smart contracts for the first time. Contrary to Bitcoin, these are programs that allow complex rules as in a language and execute automatically when certain conditions are met, without any of the parties involved 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: loans, exchanges, derivatives, insurance, risk management. This decreed the birth of decentralized finance (DeFi), a system where smart contracts, programmed in a very complex manner, execute autonomously the moment the counterparties to the exchange allow it and the required conditions are entirely satisfied. The shift from Bitcoin to Ethereum is the watershed between crypto generations. A real move from a weak medium of exchange and a store of value, to an autonomous computer on which to build a new finance. DeFi comes into being concretely between 2018 and 2020 (the period known as the “DeFi Summer” in 2020) and is understood as the set of financial products and services that all economic agents holding crypto and connected to the Internet can make use of. It is an autonomous market, never closed and with no central power that can judge, adjudicate or take decisions over third parties. The protocols it came to life with were various, such as: MakerDAO (collateralized decentral-

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

ized stablecoins), Compound and Aave (algorithmic peer-to-peer loans and mortgages) and Uniswap (decentralized exchange through automated liquidity pools, the Automated Market Makers or AMMs) [8, 10]. The structural innovation of these protocols is, as anticipated above, 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]. Within such a powerful dynamic, and within a change of use, Bitcoin was left crushed precisely at the structural level. The mother coin, in fact, privileges security, simplicity and censorship resistance above every other property. Less complexity means less 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 instruments built on Bitcoin remained fairly simple. One example might be the multisign wallet, which requires several signatures to spend the funds, as if it were a safe deposit box with several keys (each person puts in their own encrypted private key, which gives access to the contract). Others might be 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 by creating tokens that represent BTC held elsewhere. Recently, however, Bitcoin users have worked on the creation of more sophisticated instruments (Ordinals, BRC-20, Stacks and RSK), making it possible to build more elaborate decentralized finance (DeFi) applications while leaving the fundamental protocol rules unchanged, so that the coin’s uniqueness in security and stability persists [14].

On Ethereum, by contrast, DeFi was an integral part. The Ethereum Virtual Machine (EVM⁷) [11], as an execution environment, has made it possible from the very beginning to create a complete finance. Smart contract technology, then, was the real ace up the sleeve. It in fact lives both as a single unit and as a composable one, which means that the contract can stand alone or call other contracts in a chain, continuing to satisfy the requirements of each at every step with no further permissions to request (a phenomenon known as “money legos”⁸). The difference, in short, is not only technical but one of risk philosophy. 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 to poorly audited smart contracts, up to the systemic risk of cascading liquidations in overcollateralized lending protocols).

4. The comparison with traditional finance

Having come to the end of this digression, it is important for the reader to understand what makes DeFi so different from the traditional bank in the strict sense. When discussing economics, one fundamental relationship needs to be kept in mind: the tripartite relationship between surplus units (units that have accumulated some savings relative to their salary), deficit units (units that need additional income to cope with expenses exceeding their usable capacity) and commercial banks (intermediaries between these two counterparties). The relationship provides for the bank to collect the surplus income in the form of short- or long-term deposits and to reallocate it, in the form of loans or mortgages, to the deficit units. This exchange has always been as fundamental as it is flawed. For structural reasons, banks, were they to face too high a number of withdrawals, however solvent they might be on the merits of their own assets, could not honour all the requests at the same time, because the

⁷EVM: a decentralized software platform that executes smart contracts and computes the changes to the state of the network on Ethereum.

⁸Money lego (or DeFi lego): in the field of decentralized finance (DeFi), it indicates the ability of the various blockchain-based protocols to connect and integrate with one another like the bricks of the famous game. Thanks to smart contracts, users can combine different financial services, such as loans, exchanges and deposits, to create new and complex instruments.

capital would be employed in illiquid activities. All the more so since commercial banks do not limit themselves to transferring savers' deposits to borrowers, but actively create new money the moment they grant a loan, crediting the amount to the borrower's account without drawing on a pre-existing deposit. This was theoretically demonstrated by the 1983 study signed by Douglas Diamond and Philip Dybvig. Their idea was based on the idea of imitation. Given a bank deposit contract that offers immediate liquidity to those who need it and a higher return to those who can wait, a socially efficient situation is created, generating an equilibrium in which the bank works normally. That very same contract admits a second equilibrium, equally consistent with individual rationality. Each depositor, in fact, finds it rational (were there no certainty about the state of the deposits) to withdraw immediately as well, regardless of their own actual need for liquidity, simply so as not to remain among the last when the reserves have run out [13]. Since this second equilibrium is self-fulfilling, eliminating it requires an intervention external to the game itself, which is why the banking system, in response to the crises it has faced, has developed four institutional architectures, with the aim of containing and eradicating possible future crises. Respectively:

1. Deposit insurance eliminates the panic equilibrium by making the speed with which the single depositor withdraws their funds irrelevant. A depositor who knows they will recover their funds anyway, within the limits of the guarantee, has no rational incentive to rush to the counter ahead of the 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 matter. 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" constraint ensures that the intervention supports solvent but illiquid institutions, not institutions that are already insolvent.
3. Capital requirements, codified at the international level in the Basel accords⁹, oblige banks to hold a minimum share of usable capacity. Precisely against risk-weighted assets, losses fall first on shareholders and not immediately on depositors. In practical terms, this means that for every hundred units of loans granted, the bank must already have set aside, in the form of own capital, a cushion sufficient to absorb a significant deterioration in the value of those loans, before the losses reach the depositors.
4. Discretionary prudential supervision comprises periodic stress tests, limits on risk concentration, requests for additional provisions and interventions in governance in case of difficulty. It is therefore a continuous discretionary power that none of the other three institutions possesses, and one that makes it possible to intervene in a risk situation before it turns into a full-blown crisis, not merely to mitigate the consequences once they have appeared.

5. Conclusion and final reflections

The methods for resolving crises did not create themselves, nor did they arise as bureaucratic superstructures without which the system would work equally well; they are the fruit of a structural problem of finance identified empirically through specific and extremely costly crises. This concept is fundamental, because if DeFi faithfully replicates the prerogatives and the functions of the bank, at the same time it empirically ignores and does not apply any of the four architectures for absorbing inefficiencies.

⁹Basel accords: international guidelines on banking supervision and on the capital requirements of banks. Defined by the Basel Committee, they serve to guarantee the stability of the global financial system, preventing credit institutions from failing in the event of severe crises.

And so the absence of discretion typical of smart contracts becomes a constraint and not an advantage. On one side it eliminates corruption, conflict of interest and subjective error, but on the other, structurally, it cannot override its own rules as set in the code, even when circumstances might require it. In DeFi, trust, “coded ex ante”, is mediated by the code. This produces a remarkable informational and operational efficiency, in that there is a single ledger, shared and verifiable by anyone in real time.

There is then a subtler difference, of an almost epistemological nature. Traditional finance is based on a model of “social and legal” trust. The rules are unenforceable in any way other than how they are written, which eliminates the risk of discretionary arbitrariness (no one can unilaterally decide to freeze your funds or change the conditions of a loan already in place) 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”, and it is by no means obvious which of the two models produces, in the long run, greater systemic stability and distributive fairness; it is indeed precisely the kind of theoretical tension that makes the analysis of “decentralized finance”, as a real institutional experiment on a global scale, interesting from the point of view of research.

There is therefore a path that is not necessarily divisive between the two visions of finance. On the contrary, a constructive exchange in which the positive aspects of one can be integrated into the other. After all, I believe that these two systems can coexist because, for better or worse, however similar they are, they address different audiences and with different purposes [20, 22].

I therefore place great trust and expectations in it; I maintain that it is a frontier to keep an eye on, because it shakes up a little the systemic rigidity of what is taken for granted. I will close by quoting the father of everything that has been 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” [19].

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-explainin-g-eth-smart-contracts-defi>, 2025.
- [5] Borsaitaliana.It. Borsa Italiana. <https://www.borsaitaliana.it/borsa/glossario/criptoaluta.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/criptoalute-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] Mempool.Space. The Mempool Open Source Project. Accessed August 31, 2026. <https://mempool.space/docs/faq#what-is-a-mempool>, n.d.
- [19] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>, 2008.
- [20] PostFinance. Comprendere La DeFi: Opportunità, Rischi E Applicazioni Della Finanza Decentralizzata. <https://www.postfinance.ch/it/blog/guida-semplce-e-chiar-a-agli-investimenti/comprendere-defi.html>, 2025.
- [21] 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.
- [22] 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.