IN-DEPTH REPORT

Blockchain and Tokenization of Financial Assets

Smart contracts and the future of capital markets

Independent analysis on the evolution of blockchain in institutional finance

August 2026

Table of Contents

Executive summary

In recent years blockchain has gone from being associated almost exclusively with cryptocurrencies to becoming the object of significant investment by the world's leading financial institutions. The central theme of this transformation is **asset tokenization**: shares, bonds, funds, bank deposits and collateral (assets pledged as security) can now be represented through digital tokens, whose management is automated through smart contracts.

This report retraces the entire path of this evolution: from the failure of the pioneering project of the Australian Securities Exchange in 2016, to the current phase of technological and regulatory maturity. It analyzes the technical mechanisms of tokenization, how smart contracts work, the role of stablecoins, deposit tokens and CBDCs, and the infrastructures — oracles, bridges, staking — that make it possible to use public blockchains in finance.

A central part of the analysis is devoted to the theme of **decentralization**, showing how this is not a binary property but a multidimensional one, and comparing in detail the design choices of Bitcoin and Ethereum. The main conclusion is that institutional adoption of blockchain does not represent the affirmation of the original *trustless* paradigm, but rather an **evolution of existing financial market infrastructures**, in which trust is redistributed among computer protocols, smart contracts and regulated institutions.

> *Tokenization does not represent a revolution in the sense originally attributed to blockchain by Bitcoin, but rather a profound evolution of financial market infrastructures.*

1. Introduction

In recent years blockchain technology has gone from being regarded as a marginal innovation, closely associated with the world of cryptocurrencies, to representing one of the areas of greatest interest for the world's leading financial institutions. Investment banks, asset managers, market infrastructures and regulatory authorities are indeed assessing how to use this technology to modernize the architecture of financial markets, with the aim of reducing operating costs, increasing process efficiency and enabling the continuous, automated trading of financial instruments.

This evolution represents a significant shift compared with the perception the sector had developed in the years following the birth of Bitcoin. For over a decade blockchain was generally identified with cryptocurrencies and with the strong volatility that has characterized those markets. The numerous crises that have affected the sector, the failure of major operators and the absence of a sufficiently well-defined regulatory framework contributed to keeping traditional financial institutions in a cautious stance: the technology was often considered promising in theory, but still too immature for systemic applications in regulated markets.

In recent years this scenario has progressively changed. Regulatory developments in numerous jurisdictions, growing interest from central banks in digital currencies, the spread of stablecoins and, above all, the development of so-called **tokenization of financial assets** have brought blockchain back to the center of institutional operators' attention. In particular, traditional finance's interest concerns not so much cryptocurrencies as a new asset class, but rather the possibility of using blockchain infrastructure to digitally represent financial instruments that already exist and automate their lifecycle.

Numerous financial institutions — including large international banks, asset managers, stock exchanges and companies that manage clearing and settlement infrastructures — are investing hundreds of millions of dollars in developing blockchain-based platforms. According to the authors, this phenomenon could profoundly transform the functioning of financial markets, making continuous trading of financial instruments possible, automating numerous administrative processes and significantly reducing settlement times for transactions.

However, growing attention toward blockchain does not necessarily imply the adoption of the original philosophy that inspired the birth of Bitcoin. The project developed by Satoshi Nakamoto in 2008 aimed to create a **trustless** monetary system, that is, one capable of functioning without the need for central intermediaries. The blockchain used today by institutional finance instead pursues different aims: banks, asset managers and issuers continue to play a central role in the issuance, custody and management of financial instruments. What changes is mainly the technological infrastructure used to record asset ownership and automate certain operational processes.

In this sense, blockchain does not replace the existing financial system, but presents itself as a possible evolution of its infrastructures. The innovation does not consist in eliminating intermediaries, but rather in integrating them within a digital ecosystem characterized by greater programmability, greater interoperability and significantly shorter execution times compared with traditional architectures.

The aim of this report is to critically analyze this evolution, illustrating the principles of financial asset tokenization, the role of smart contracts, the characteristics of the main public blockchains, and the technological and systemic risks associated with their growing use in financial markets.

2. From the ASX project crisis to the new phase of tokenization

The current enthusiasm for blockchain contrasts with what happened only a few years earlier. One of the most significant episodes in the history of applying blockchain technology to financial markets is the project launched in 2016 by the **Australian Securities Exchange (ASX)**.

At the time ASX announced its intention to replace its clearing and settlement system, known as CHESS (*Clearing House Electronic Subregister System*), with a new infrastructure based on blockchain technology. The initiative was presented as a pioneering project and received enormous media attention, since it would have represented the world's first case of a major national stock exchange adopting a distributed ledger as the central infrastructure of its market.

Expectations were high: it was believed that blockchain would simplify the settlement of transactions, reduce the number of intermediaries involved in post-trading processes, improve transparency and lower operating costs for all market participants.

The project, however, quickly ran into difficulties far greater than initial expectations. During development, technical, organizational and managerial problems emerged: the platform proved unable to guarantee the performance required by a high-transaction-volume national infrastructure, while the complexity of integration with existing systems was underestimated. Added to this were governance issues and difficulties managing relationships with market participants.

AUD 170 million

Investments fully written off by ASX after the project's cancellation

After years of delays and numerous project revisions, the project was ultimately cancelled (a fate common to many software projects of a certain complexity). ASX was forced to fully write off the investments made, amounting to approximately 170 million Australian dollars, and subsequently was also fined for providing the market with information considered misleading about the project's progress. The episode was interpreted by many observers as proof that blockchain was not yet mature enough to serve as the backbone infrastructure of a major regulated market.

Ten years on, the context appears profoundly different. Not only has the technology changed, but above all the entire ecosystem in which it operates: supervisory authorities have progressively defined specific rules for digital assets, numerous central banks have launched experiments on digital currencies, the stablecoin market has reached significant size, and new infrastructures dedicated to the tokenization of financial instruments have emerged.

Competition has also helped accelerate this change. Cryptocurrency exchanges are no longer limited to trading digital assets, but aim to offer financial services increasingly similar to traditional ones, progressively entering the market for shares, bonds and other financial instruments. Traditional market infrastructures have therefore begun to regard blockchain no longer as an external threat, but as a technology to be integrated into their own systems in order to remain competitive.

The failure of the ASX project is therefore no longer interpreted as the failure of blockchain itself, but as the result of a technology introduced in a context that was still premature, characterized by limited

technological maturity, poor standardization and the absence of a sufficiently well-defined regulatory framework.

3. What tokenization is

The central concept of the new strategy adopted by Wall Street is the **tokenization of financial assets**. This term refers to the process by which a real asset or an economic right is digitally represented through a **token** recorded on a blockchain.

From a technical standpoint, a token is a digital unit that identifies a given property right and enables its transfer between different parties through the recording of transactions on a distributed ledger. Unlike native cryptocurrencies such as Bitcoin or Ether, a token does not necessarily constitute a new financial instrument, but rather represents the digital version of an asset that already exists.

Categories of tokenizable assets

Virtually all tradable financial instruments can be tokenized. The following table summarizes the main categories.

Category	Examples
Equity instruments	Shares, ETFs, mutual fund units, alternative funds
Debt instruments	Bonds, money market instruments, trade receivables
Deposits and liquidity	Bank deposits, collateral in repo transactions
Real assets	Commodities, real estate, real estate fund units
Derivative instruments	OTC derivatives and instruments linked to indices or commodities

Table 1. Tokenizable assets and liabilities.

Tokenization does not change the economic nature of the underlying financial instrument. A tokenized bond continues to confer the same property rights as a traditional bond; a tokenized share continues to represent a stake in the issuer's share capital. What changes is how these rights are recorded, transferred and administered.

In traditional systems, ownership of financial instruments is managed through a complex network of intermediaries made up of custodian banks, central securities depositories (CSDs), clearing houses, transfer agents, registrars and paying agents. Every transfer requires a series of reconciliations between different registries, resulting in operating costs and settlement times that, although considerably reduced in recent years, remain higher than those theoretically achievable through a distributed infrastructure.

Tokenization proposes a different paradigm: the distributed ledger becomes the single point of reference for representing ownership of financial instruments and recording transactions. In theory, this approach makes it possible to reduce the number of reconciliations, simplify the settlement process and create financial instruments that are directly programmable through smart contracts, which will be examined in the next section.

It is important to stress that tokenization does not necessarily imply the use of fully public and permissionless blockchains. Many initiatives promoted by financial institutions in fact use authorized distributed ledgers (*permissioned distributed ledger*), in which access to the validation of transactions is reserved to previously identified parties. In other cases, public blockchains such as Ethereum are used instead, on which tokens representing real financial assets are issued.

This distinction is fundamental because it highlights how tokenization does not coincide with absolute decentralization. Most projects developed by traditional finance in fact maintain strong control over issuers, intermediaries and regulatory compliance procedures, using blockchain mainly as a more efficient and programmable technological infrastructure. In other words, the innovation does not consist in eliminating trust in intermediaries, but in digitizing and automating processes through a new generation of distributed ledgers.

4. Smart contracts: the true engine of tokenization

If blockchain is the infrastructure on which tokenized financial instruments are recorded, **smart contracts** represent the mechanism that makes those instruments genuinely programmable. It is precisely this programmability, even more than the use of a distributed ledger, that constitutes the element of greatest interest for institutional finance.

Smart contracts are programs that automatically execute certain operations when predetermined conditions occur. Examples of such operations in finance include: the automatic payment of dividends, the settlement of trading transactions, the disbursement of loans, and the automatic execution of other activities normally carried out by financial intermediaries. This definition is correct, but represents only part of their real meaning.

4.1 Origin of the concept

Contrary to what is often assumed, the concept of the smart contract predates the birth of blockchain. In 1994 the cryptographer and computer scientist **Nick Szabo** introduced the idea of a contract capable of automatically executing certain clauses without requiring the intervention of an intermediary, with the aim of turning some contractual obligations into computer code. At the time, however, there was no distributed infrastructure capable of guaranteeing that the program would be executed simultaneously by all participants without the need for a central authority.

The birth of Bitcoin in 2008 solved the problem of distributed consensus, but it offered only a deliberately limited scripting language. With Ethereum, introduced in 2015, the concept of the smart contract finally found a platform flexible enough to allow complex programs to be built directly on the blockchain. From that moment on, blockchain ceased to be merely a distributed ledger of transactions and became a genuine distributed computing platform.

4.2 What a smart contract really is

From a computing standpoint, a smart contract is a **deterministic program** recorded on the blockchain and executed simultaneously by all the network's validating nodes. The adjective *deterministic* is of fundamental importance: given the same input data, every node must necessarily produce the same result. This property ensures that no node can unilaterally alter the outcome of the computation, that all participants share the same state of the system, and that the distributed ledger remains consistent.

The smart contract thus becomes an integral part of the blockchain and inherits its main characteristics: immutability, transparency, verifiability, traceability and distributed execution. It is worth noting that the term "contract" can be misleading: in most cases the smart contract **does not replace the legal contract**, but rather automates its execution. The legal contract continues to exist; the smart contract implements the operational logic needed so that certain clauses are applied automatically. In other words, code does not replace law, but automates its application.

4.3 A state machine

From a software engineering standpoint, a smart contract can be interpreted as a **finite state machine (FSM)**. Every financial instrument in fact goes through a succession of states during its lifecycle: for example, a bond may evolve according to the sequence illustrated below.

Figure 1. Lifecycle of a tokenized bond as a finite state machine.

Each transition between two states is triggered automatically when a given event occurs. The smart contract controls these transitions by applying the rules defined at the time the instrument was issued: in practice, the bond's behavior becomes an integral part of the instrument itself. This is probably the main innovation introduced by tokenization.

4.4 Smart contracts in financial markets

In traditional financial markets a single transaction generally involves numerous parties: custodian bank, broker, clearing house, central securities depository (CSD), transfer agent, registrar, paying agent, fund administrator and management company. Each of them performs specific operational activities, many of which simply consist in applying perfectly codifiable rules. Smart contracts therefore make it possible to embed these rules directly into the financial instrument.

For example, a tokenized bond could:

- automatically calculate interest;
- check the coupon payment date;
- automatically transfer money to investors;
- update the register of holders;
- carry out the final redemption at maturity.

Similarly, a tokenized ETF could:

- periodically check the composition of the index;
- automatically calculate the new portfolio;
- generate rebalancing orders;
- update the net asset value (NAV).

The same principle can be applied to mutual funds, syndicated loans, repo transactions, OTC derivatives and numerous other instruments. It is precisely this programmability that represents one of the main reasons for the interest the financial world shows today toward blockchain.

4.5 The economic advantages

The introduction of smart contracts produces advantages that go well beyond simple automation. Among the main benefits are:

- reduced settlement times;
- fewer reconciliations between different systems;
- elimination of numerous manual processes;
- reduction of operational errors;

- greater transparency of transactions;
- reduced operational risk;
- the possibility of round-the-clock continuous trading.

From an economic standpoint, financial instruments thus cease to be simple digital representations of a property right and become **programmable financial instruments** (*programmable financial assets*). This transformation could profoundly change how market infrastructures function in the coming years.

4.6 The limits of smart contracts

Full automation, however, introduces new critical issues. A program executes exclusively what has been written in the code: if the code contains an error, that error will be automatically replicated by every node in the network. Moreover, once deployed on the blockchain, a smart contract can be very difficult to modify — a substantial difference compared with traditional information systems, where software errors can generally be corrected through centralized updates. In the case of blockchain, fixing the issue may require new versions of the contract or, in more extreme cases, changes to the network protocol.

There is also a second, even more significant problem: automation eliminates the discretion that characterizes many operational decisions today. During a financial crisis, for example, a bank may decide to give a counterparty more time before enforcing collateral; a smart contract does not have this flexibility and, if the specified conditions are met, will automatically execute the planned action. For this reason the International Monetary Fund and the European Central Bank have pointed out that excessive automation could amplify systemic risk, especially when it concerns critical processes such as transaction settlement or margin calls.

5. Stablecoins and tokenized money

The tokenization of financial instruments inevitably also requires the availability of a form of **digital money** with which to settle transactions. In a traditional market, in fact, every trade involves two simultaneous transfers: that of ownership of the financial instrument and that of money. If the first is tokenized while the second continues to use traditional banking circuits, the advantages of blockchain are inevitably limited. For this reason the most developed segment of tokenization today concerns **tokenized money**.

Form of tokenized money	Issuer	Main characteristics
Stablecoins	Private entities	Pegged to the value of a legal-tender currency; instant transfers, operate 24/7
Deposit tokens	Commercial banks	Tokenized bank deposits; retain a direct link with the existing banking system
CBDC	Central banks	Central bank digital currencies; still under study or in pilot phase in most jurisdictions

Table 2. Examples of tokenized money (existing or under development).

Stablecoins are today the most developed market: they allow virtually instant transfers and can be used twenty-four hours a day, seven days a week, overcoming the time limits of traditional payment systems. Their spread is one of the factors that has helped reignite financial institutions' interest in blockchain, since it makes it possible to envisage an ecosystem in which financial instruments and money are settled on the same distributed infrastructure.

Numerous banks are also experimenting with **deposit tokens**, which have the advantage of maintaining a direct relationship with the traditional banking system and the existing regulatory framework. **CBDCs**, on the other hand, are still under study or in pilot phase in most jurisdictions, and their development is proceeding at different speeds depending on the choices of the respective central banks.

From an economic standpoint, tokenized money represents the natural complement to asset tokenization: without a natively digital form of payment, the settlement process would continue to depend on external infrastructures, limiting much of the benefit expected from the new architecture of financial markets.

6. Tokenized money market funds and new digital financial instruments

One of the most interesting developments of tokenization concerns **tokenized money market funds** (*Tokenized Money Market Funds — TMMF*), today considered one of the most mature applications of blockchain in the financial sector.

Traditional money market funds invest mainly in short-term instruments characterized by high credit quality and low market risk, such as government securities, bank deposits and commercial paper, with the aim of offering investors a relatively stable return while maintaining a high level of liquidity. Tokenization does not change the fund's investment policy, but affects how units are issued, transferred and administered: each unit is represented by a token recorded on the blockchain, while the investor continues to hold the same economic right over the fund's assets.

> USD 16 billion

Assets in tokenized money market funds in 2025, according to the Financial Times — growing rapidly compared with the few billion of previous years

One of the most innovative aspects consists in the possibility of directly integrating numerous administrative functions into the smart contract. For example, the contract can:

- automatically calculate the unit's value;
- distribute accrued yield on a daily basis;
- register new subscribers;
- update the number of units outstanding;
- verify compliance with regulatory limits;
- automatically manage redemptions.

In traditional systems these operations normally require the coordinated involvement of the management company, the fund administrator, the custodian bank and the transfer agent. Tokenization instead makes it possible to embed a significant part of these activities directly in the instrument's application logic.

It is important to note, however, that the fund continues to be managed by an authorized company subject to the supervision of the competent authorities: blockchain therefore does not eliminate the role of the management company, but makes the administrative process more efficient. This distinction is fundamental to understanding the approach adopted by traditional finance — tokenization does not replace the existing regulatory framework, but digitizes financial instruments while keeping the fundamental principles of supervision, custody and investor protection unchanged.

7. Collateral tokenization

Among the applications considered most promising by market infrastructures is collateral tokenization. In most financial transactions one of the counterparties provides financial assets as a guarantee of fulfillment of its obligations: government securities, corporate bonds, shares, fund units or cash.

Collateral is used daily in numerous markets:

- repurchase agreements (repo);
- OTC derivatives;
- secured financing;
- securities lending;
- clearing operations at clearing houses.

In current systems the transfer of collateral requires a series of administrative and accounting checks involving custodians, clearing houses and custodian banks. This process, while extremely reliable, inevitably involves operational lead times and ties up capital that could be used in other transactions.

Tokenization radically changes this paradigm: collateral is represented by tokens recorded on the blockchain, and the smart contract automatically checks the existence of the guarantee, its updated value, compliance with required margins and the possible release of the guarantee at the end of the transaction. In theory, the transfer of collateral can take place at the same time as the execution of the transaction, significantly reducing settlement times.

This is precisely one of the areas in which market infrastructures see the greatest potential for blockchain. The Depository Trust & Clearing Corporation (DTCC), the main post-trade infrastructure of the U.S. market, is developing platforms aimed at tokenizing the instruments held in its system, with the goal of increasing efficiency in collateral management.

From an economic standpoint, the main benefit consists in the possibility of increasing the speed of collateral circulation (*collateral velocity*): the same financial asset could be reused more quickly in successive transactions, reducing the overall amount of capital needed for the financial system to function.

Naturally, this advantage also introduces new critical issues. Greater circulation speed in fact implies greater interconnection among market participants and could amplify the effects of any liquidity crises. For this reason, collateral tokenization represents at the same time one of the main efficiency factors and one of the possible sources of systemic risk.

8. Tokenized shares and the new market infrastructures

The application of tokenization to shares probably represents the most visible evolution for investors. In theory, every share issued by a company could be represented by a digital token recorded on a blockchain, which would continue to confer the same economic and administrative rights as a traditional share:

- the right to dividends;
- voting rights;
- the right to participate in capital increases;
- the right to a share of liquidation proceeds.

Only the infrastructure through which these rights are recorded and transferred would change.

Numerous market infrastructures are already developing platforms dedicated to this new model. In particular, Nasdaq is studying systems in which shares could be issued and traded directly on blockchain infrastructures, enabling automated management of the main corporate actions, such as dividend distribution, stock splits, capital increases and extraordinary transactions.

From an operational standpoint, one of the main advantages concerns the possibility of integrating the entire lifecycle of the share within the smart contract. The issuer could directly program:

- dividend payment;
- the ex-dividend date;
- the exercise period for option rights;
- the management of shareholder meetings;
- the automatic updating of the shareholder register.

This would reduce the need to maintain separate registries at multiple intermediaries.

A further theoretical advantage consists in the possibility of extending trading beyond the current opening hours of stock exchanges: while today trading is limited to market sessions, a blockchain platform could allow the transfer of tokens twenty-four hours a day.

It is necessary, however, to distinguish between technical and regulatory feasibility. Technology (even current technology) does indeed allow continuous trading, but this does not mean that supervisory authorities, market infrastructures or issuers will necessarily decide to adopt a round-the-clock operating model: the definition of trading hours remains an organizational and regulatory choice, independent of blockchain's technological capabilities.

Here too the difference between technological innovation and institutional transformation clearly emerges. Blockchain makes new operating models possible, but their actual adoption depends on the decisions of market operators, supervisory authorities and the regulatory framework within which these markets will continue to operate.

9. Oracles, bridges and staking: the new elements of blockchain infrastructure

When a blockchain is described as "decentralized" one tends to imagine a completely autonomous infrastructure, capable of functioning without any connection to the outside world. In reality, modern public blockchains, especially those intended to host complex financial applications, depend on a series of additional infrastructural components that play an essential role in their functioning.

Among these, particular importance is held by **oracles**, **bridges** and the **staking** system: three elements that, although often overlooked in popular descriptions of blockchain, today constitute some of the main points of attention from the standpoint of security and decentralization. Understanding how they work is essential to correctly assess the opportunities offered by tokenization and, at the same time, the new risks introduced by the use of public blockchains as financial market infrastructure.

9.1 Oracles: the link between blockchain and the real world

A blockchain can be regarded, from a computing standpoint, as a **closed system**: all the nodes in the network share the same ledger and can only process information already present within it. This ensures consistency and security, but also entails a fundamental limitation — blockchain **does not know what happens in the outside world**.

A smart contract, for example, is not able to know on its own what the current price of a share is, what the Euribor rate is, the daily gold fixing, whether a ship has reached its destination port, whether a bond has paid a coupon, what the euro/dollar exchange rate is, or whether a central bank has changed official rates.

To obtain this information, it is necessary to resort to an **oracle** (*oracle*): a software infrastructure that gathers data from the outside world, verifies its reliability according to predetermined procedures, and makes it available to smart contracts. The oracle thus plays the role of an **information bridge** between two environments that, by their nature, cannot communicate directly. Conceptually, a smart contract can be seen as a decision-making engine, while the oracle represents the sensor that provides it with the information needed to make those decisions.

For example, take a bond indexed to Euribor: the smart contract is perfectly capable of calculating the coupon amount, but does not know the value of Euribor. The oracle reads the rate published daily by the competent authority, transmits it to the blockchain and makes it available to the smart contract, which can then proceed with the interest calculation. The same principle applies to numerous financial applications: derivatives, parametric insurance, index-linked funds, collateral management, commodity-linked instruments and climate-linked instruments.

It is clear that the reliability of the smart contract depends directly on the quality of the information received: an oracle that transmits incorrect or manipulated data can compromise the correct functioning of the entire system. For this reason, oracles today represent one of the main trust assumptions (*trust assumptions*) of public blockchains. In recent years systems have been developed that try to reduce this risk by simultaneously collecting data from numerous independent sources and automatically calculating a consensus value — this does not completely eliminate the problem, but significantly reduces its probability.

From an architectural standpoint, therefore, a fully decentralized blockchain is not by itself sufficient to guarantee an entirely decentralized system: if external information comes from a limited number of oracles, part of the trust inevitably becomes concentrated in those parties.

9.2 Bridges: connecting different blockchains

A second essential element consists of **bridges**. Blockchains are generally designed as independent ecosystems: Bitcoin, Ethereum, Solana, Avalanche and other networks do not automatically share their internal state, and a token existing on Ethereum cannot be transferred directly to the Bitcoin blockchain. Bridges are used to allow the transfer of assets between different blockchains.

How this works can be described in simplified form through four phases:

- the user deposits the token on the origin blockchain;
- the bridge locks that token, preventing further transfers;
- an equivalent new token is created (minted) on the destination blockchain;
- when the user wants to return to the original blockchain, the synthetic token is destroyed (burned) and the original one is unlocked.

It would be more intuitive for the bridge to destroy the original token and create a new one on the destination network. But a problem would then arise when the reverse operation had to be carried out: returning to the original network. The bridge in fact does not have control over the creation of the original tokens, meaning it does not have the rights to trigger execution of the smart contract that creates tokens on the original network. The process would therefore get stuck. On the destination network, instead, the bridge presents the "locked" tokens as collateral for the issuance of the new ones, which turns out to be adequate collateral because the old tokens can no longer circulate, even though they continue to exist and hold value. This creates a security problem – as we will see shortly – which is why native "cross-chain" tokens were invented. One example is the Omnichain Fungible Token (OFT) standard developed by LayerZero. Here the token is designed from the outset to exist across multiple blockchains, and can therefore be destroyed on one blockchain and recreated on another, avoiding the main problem of "double circulation."

From an economic standpoint, the bridge does not really transfer the token, but rather transfers the economic right it represents. This distinction is fundamental: the correct functioning of the entire process depends on the bridge itself, and if the bridge is compromised, the link between the two blockchains also fails.

Historically, bridges have been one of the main targets of cyberattacks. Many of the most serious cryptocurrency thefts of recent years have concerned precisely vulnerabilities present in bridges rather than in the underlying blockchain protocols. The reason is intuitive: while compromising a public blockchain generally requires enormous economic resources, attacking a bridge means striking a much smaller piece of infrastructure that often holds assets of extremely high value. From a systemic standpoint, therefore, bridges represent one of the main points of risk concentration in the entire blockchain ecosystem.

9.3 Staking and Proof-of-Stake consensus

A third fundamental element concerns the mechanism of **staking**, closely linked to the functioning of blockchains based on **Proof-of-Stake (PoS)** consensus. To understand its meaning it is useful to compare it with the system used by Bitcoin, which protects its network through **Proof-of-Work (PoW)**, in which thousands of computers compete to solve complex cryptographic problems: security derives from the enormous amount of energy and computing power needed to alter the blockchain.

Ethereum, on the other hand, has used Proof-of-Stake since September 2022. In this model, security does not derive from energy consumption but from the economic capital pledged by participants (validators), who deposit network tokens as collateral. If the validator behaves correctly it receives compensation in the form of new network fees; if instead it attempts to alter the protocol or violates the rules in place, part of the deposited capital can be confiscated — a mechanism known as **slashing**.

From an economic standpoint, Proof-of-Stake replaces the energy cost of Proof-of-Work with a capital risk: the incentive to behave correctly therefore derives from the possibility of losing the capital invested.

9.4 The concentration of staking

In theory, Proof-of-Stake favors open participation. In practice, however, the phenomenon is more complex: most investors do not have the technical skills needed to directly run a validator node, and many therefore prefer to delegate their tokens to large specialized operators. This is how **liquid staking** platforms arise, gathering the tokens of thousands of investors and using them collectively to take part in the validation process.

This model improves the economic efficiency of the system but inevitably produces a certain concentration of validation power: a significant share of staking tends to concentrate among a relatively limited number of operators, such as Lido. From a decentralization standpoint, this phenomenon represents one of the most discussed aspects of the current Ethereum ecosystem: the blockchain continues to be distributed among thousands of nodes, but the economic power associated with the validation process can be significantly more concentrated.

This does not mean that Ethereum is centralized: it means rather that decentralization must be assessed by considering not only the number of nodes, but also the distribution of capital, protocol governance and the functioning of complementary infrastructures.

The following chart summarizes the number of additional components — beyond the base protocol — on which the operational security of the two main ecosystems currently depends:

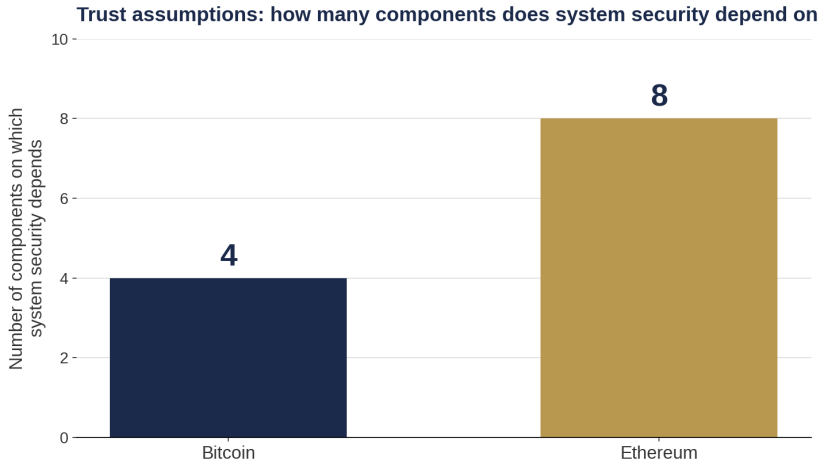

Figure 1. Indicative number of infrastructural components on which the ecosystem's operational security depends (protocol, oracles, bridges, staking, RPC providers, layer 2, cloud, DeFi).

This does not mean that PoW-based networks are exempt from concentration risk either. For example, the Bitcoin network sees the participation of so-called mining pools, i.e. consortia of validators that take care of the integrity of the network itself.

9.5 Concentration in mining

In theory, Bitcoin is designed so that every miner can independently take part in validating blocks. Each participant contributes its own computing power (*hash rate*) and competes with all the others to solve the cryptographic puzzle. The probability of finding the block is proportional to the computing power held. In an ideal system, thousands of small independent miners should contribute to the network's security. In practice, however, this model presents an economic problem.

Suppose a small miner holds 0.01% of the world's hash rate. Statistically it will find about:

$$144 \times 0.0001 \approx 0.0144$$

blocks per day.

In other words, it could go several months without finding any block, only to suddenly find one. The expected value of the return is correct, but its variance is enormous.

For a business that has to pay for electricity, staff and depreciation of ASICs (special machines designed to carry out *hash* computations as efficiently as possible), this uncertainty is difficult to sustain.

To reduce this volatility, **mining pools** emerged. A mining pool gathers the computing power of thousands of miners. When the pool finds a block, the reward is distributed among all participants in proportion to the hash rate they contributed. From a statistical standpoint, the average return does not change. What changes drastically, however, is the risk. Instead of receiving a very large reward once every several months, the miner receives small payments practically every day. From an economic standpoint, this is a form of risk mutualization.

This solution, however, introduces a new risk. Over the years, most of the world's hash rate has become concentrated in a few large mining pools. For example (the values change continuously), it can happen that:

Mining Pool	Hash Rate
Pool A	28%
Pool B	22%
Pool C	18%
Pool D	11%

The top four pools can therefore control almost 80% of the network's computing power. This means that the block-construction process is much more concentrated than the total number of miners would suggest.

Here a fundamental difference emerges. In PoS, when tokens are delegated to a staking operator the validator takes part directly in consensus, the delegated capital increases its validation power, and a growing share of staking can become concentrated among a few operators. Concentration therefore concerns the capital that determines consensus.

In PoW, by contrast, concentration among a few mining pools presents a subtler situation. The consortium does not own the miners' ASICs. It simply coordinates their work. An individual miner can switch consortium within minutes. Consequently, concentration is less rigid than in PoS. The consortium's power derives from the fact that many miners voluntarily choose to cooperate.

The real risk arises when one or a few consortia control more than 50% of the hash rate. In theory they could: censor transactions, slow down the confirmation of certain blocks, carry out double-spending attacks, and temporarily prevent the finalization of certain transactions.

It is important, however, to clarify a point that is often misunderstood. Not even with 51% of the hash rate can a mining pool create bitcoin out of nothing, change monetary policy, alter the (roughly) 21 million BTC cap, or – finally – appropriate bitcoin belonging to other users. It can influence the consensus process, but it cannot arbitrarily rewrite the protocol's rules. However, these risks are – in part – mitigated by the fact that

Bitcoin has a mechanism of economic self-defense. Miners have invested billions of dollars (often with debt) in infrastructure and ASICs. A successful attack that undermined trust in the network would trigger a collapse in the price of bitcoin and, consequently, a drastic reduction in the economic value of mining activity and of their investments. Economic incentives therefore push large consortia to behave properly. Moreover, since miners can switch pools with relative ease, a pool that adopted hostile behavior would risk rapidly losing much of its hash rate.

Aspect	*Proof-of-Work*	*Proof-of-Stake*
Source of power	Computing power (hash rate)	Capital at stake
Main concentration risk	Mining pools	Large staking operators
Ease of migration	High: the miner can switch pools quickly	More limited: depends on the protocol and unbonding periods
Investment required	ASICs and energy	Blockchain tokens
Economic incentive	Block reward and fees	Staking rewards and fees

Table 3. Comparison between PoW and PoS.

10. Public blockchains: how decentralized are they really?

Numerous financial institutions have chosen to develop their tokenization projects using public blockchains, in particular Ethereum. Some critical points should not be overlooked, however: such infrastructures depend on networks of distributed validators and can be exposed to cyber vulnerabilities that have caused significant losses in various protocols within the ecosystem. For this reason some large banks, such as JPMorgan, prefer to develop private distributed ledgers, maintaining direct control over the infrastructure.

The question of decentralization is probably one of the most debated topics in the entire blockchain sector. In common usage a blockchain is often simply described as "decentralized" or "centralized," but this classification is overly simplistic: decentralization is not in fact an absolute property, but a set of characteristics concerning different aspects of the infrastructure.

At least five fundamental dimensions can be distinguished:

Dimension	Definition
Consensus	The way in which transactions are validated
Protocol governance	The process through which software updates are decided
Code development	Normally entrusted to groups of developers with highly specialized skills
Economic distribution	The allocation of tokens and validation power
External infrastructures	Oracles, bridges, staking services, wallets and cloud providers that make the blockchain practically usable

Table 4. The different dimensions of decentralization.

A network can therefore be highly decentralized in some respects and significantly more concentrated in others. Ethereum represents a particularly interesting example of this trade-off: from a consensus standpoint the network involves thousands of geographically distributed validators, but from a development standpoint the evolution of the protocol is influenced by a relatively small number of highly qualified developers and by the Ethereum Foundation, which plays an important role in coordinating the technical evolution of the ecosystem.

Many of the applications built on top of Ethereum also depend on specialized infrastructures, such as oracles, bridges and staking platforms, which introduce further elements of concentration. Consequently, simply defining Ethereum as "decentralized" does not give a complete picture of reality: the network certainly shows a high degree of distribution compared with traditional financial systems, but it continues to depend on numerous parties that carry out functions essential to its operation.

This observation is particularly relevant to the comparison between Bitcoin and Ethereum developed in the following section, where it will become clear how different design choices have led to the emergence of two profoundly different models of decentralization.

11. Is Bitcoin really the only fully decentralized blockchain?

The growing adoption of blockchain by institutional finance has brought back to the center of the debate a question that has accompanied this sector ever since the birth of Ethereum (in 2016): **does a genuinely decentralized blockchain exist today, or do all networks, to varying degrees, present elements of centralization?**

The answer depends above all on the meaning attributed to the term *decentralization*. If this term is understood as the absence of any party able to unilaterally alter the network's functioning, censor transactions or arbitrarily alter the history of the ledger, then Bitcoin still represents today the closest reference to that ideal. If, on the other hand, decentralization is considered as a multidimensional concept, encompassing governance, software development, economic distribution, external infrastructures and the capacity for protocol evolution, the picture is inevitably more nuanced.

To understand this distinction it is necessary to analyze the different design choices adopted by Bitcoin and Ethereum.

11.1 Bitcoin's design philosophy

Bitcoin was created with an extremely specific goal: to create an electronic monetary system functioning without central banks or fiduciary intermediaries. The entire project reflects this purpose — the architecture is deliberately simple, the scripting language is limited, changes to the protocol are introduced with extreme caution, and the attack surface is kept as small as possible. Every new feature is evaluated mainly in terms of its impact on network security.

This approach has entailed numerous trade-offs: Bitcoin does not have complex smart contracts, does not allow decentralized applications comparable to those built on Ethereum, and its programmability is limited, so much so that many applications must be built outside the main blockchain. However, it is precisely this simplicity that constitutes one of the reasons for its extraordinary robustness: after more than fifteen years of continuous operation, the Bitcoin blockchain has never suffered a compromise of its consensus protocol.

The network is today distributed among thousands of independent nodes located in numerous countries, while the software development process is characterized by a high level of consensus among developers, economic operators and the community of users. The absence of a foundation governing the project represents one of the main differences compared with many other blockchains: changes are adopted only when a very large part of the ecosystem voluntarily decides to install the new software, and as a result decision-making power is extremely distributed.

11.2 Ethereum's approach

Ethereum was created with a profoundly different philosophy: the goal is not to create a digital currency, but to build a universal platform for decentralized applications. To achieve this, the protocol incorporates a general-purpose virtual machine (the Ethereum Virtual Machine) that allows the execution of arbitrarily complex smart contracts — a choice that has fostered an extraordinarily rapid development of the ecosystem.

Built on Ethereum today are:

- decentralized finance (DeFi) protocols;
- stablecoins;

- tokenized funds;
- NFTs;
- digital identity systems;
- insurance applications;
- tokenization platforms.

Programmability therefore represents the network's main strength, but it inevitably entails greater complexity: every new functional layer increases the number of possible vulnerabilities. Smart contracts must be audited, oracles must be reliable, bridges must be secure, and staking platforms must operate correctly. As a result, the security of the entire ecosystem does not depend exclusively on the Ethereum protocol, but also on the set of infrastructures built on top of it.

This does not necessarily constitute a flaw: it is rather the natural consequence of the goal being pursued. Ethereum chose to maximize programmability; Bitcoin instead favored simplicity.

11.3 A technical comparison

The differences can be summarized in the following table.

Characteristic	Bitcoin	Ethereum
Main goal	Decentralized currency	Programmable platform
Consensus	Proof-of-Work	Proof-of-Stake
Smart contracts	Very limited	Fully featured
Scripting language	Minimal	General purpose
Attack surface	Reduced	Larger
Oracles	Generally not required	Fundamental
Bridges	Limited use	Widely used
Governance	Highly distributed	More coordinated
Updates	Very conservative	More frequent
Application ecosystem	Limited	Very extensive

Table 5. A comparison of the main characteristics of Bitcoin and Ethereum.

The table shows how Bitcoin and Ethereum do not represent two versions of the same technology, but rather two different design trade-offs. Bitcoin maximizes security, immutability and censorship resistance; Ethereum maximizes flexibility, innovation and programmability. Both pursue different goals.

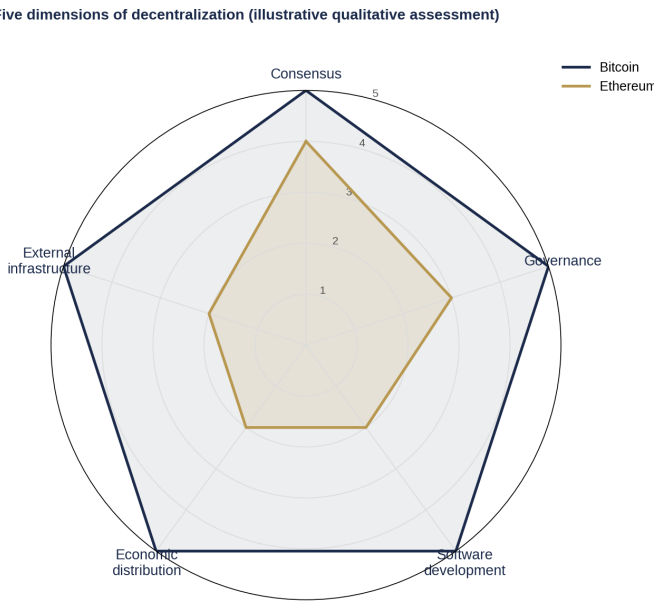

Figure 2. Qualitative and illustrative comparison between Bitcoin and Ethereum across the five dimensions of decentralization discussed in the previous chapter (1-5 scale, indicative assessment based on the qualitative analysis in this report).

11.4 A critical assessment

In light of the foregoing considerations, a more general reflection can be made. If one considers only the consensus protocol, both networks can be considered highly decentralized. If, however, one examines the entire operational ecosystem, substantial differences emerge.

Ecosystem	Components it depends on
Bitcoin	Protocol · Miners · Nodes · Developers
Ethereum	Smart contracts · Oracles · Bridges · Staking platforms · RPC providers · Layer 2 · Cloud services · DeFi infrastructures

Every new component inevitably introduces new trust assumptions (*trust assumptions*). For this reason many researchers believe that Bitcoin still represents today the most decentralized public blockchain. This does not imply that Ethereum is centralized: it simply means that the overall level of decentralization must be assessed by considering the entire architecture and not just the consensus protocol.

Bitcoin remains the system closest to the original ideal of decentralization conceived by Satoshi Nakamoto, while Ethereum represents a trade-off between decentralization and programmability, chosen to enable a much broader application ecosystem.

12. Conclusions

The interest shown today by Wall Street (and by financial operators in general) toward blockchain represents one of the most significant changes in the recent evolution of financial markets. After a long phase during which this technology had been identified almost exclusively with cryptocurrencies, attention has progressively shifted toward the possibility of using distributed ledgers and smart contracts to modernize existing financial infrastructures.

The central theme of this transformation is the **asset tokenization**. Shares, bonds, mutual funds, money market instruments, bank deposits and collateral can be represented through digital tokens, enabling more efficient management of their lifecycle. Blockchain thus becomes a platform on which to record ownership of financial instruments, while smart contracts automate numerous operational functions, from dividend payments to the management of corporate actions, to transaction settlement.

The potential benefits are significant. Reduced settlement times, fewer reconciliations between different registries, the programmability of financial instruments and the possibility of continuous trading could profoundly change how capital markets function.

However, this evolution also introduces new critical issues. Automation does not eliminate risk, but shifts it from human behavior to software: smart contracts must be correct, oracles must provide reliable data, bridges must be secure, and staking platforms must avoid excessive concentration of validation power. Moreover, the increase in operational speed could amplify the propagation of financial shocks, making the transmission of liquidity crises among highly interconnected operators faster.

The analysis of decentralization also shows how it is necessary to move beyond a simplistic view that distinguishes blockchains only between "centralized" and "decentralized". Decentralization is a multidimensional property involving consensus, governance, software development, economic distribution and external infrastructures. From this point of view, Bitcoin and Ethereum represent two profoundly different models: the former favors security, immutability and censorship resistance, while the latter accepts greater complexity in order to offer a highly programmable platform.

Probably the most important point to emerge from this analysis, however, concerns the very nature of the blockchain adopted by traditional finance. Large institutions are not embracing the original paradigm of **trustless finance**, in which intermediaries are eliminated. On the contrary, banks, asset managers, central depositories, issuers and supervisory authorities will continue to play an essential role. Blockchain is being used as a new technological infrastructure on which to build more efficient markets, while maintaining the existing institutional and regulatory framework.

In this sense, tokenization does not represent a revolution in the sense originally attributed to blockchain by Bitcoin, but rather a profound **evolution of financial market infrastructures**. Trust is not eliminated: it is redistributed among computer protocols, smart contracts and financial institutions, giving rise to a hybrid model in which technological innovation and regulation coexist. This, more than the spread of cryptocurrencies, is probably the transformation destined to characterize the next decade of financial markets.