RADAR SPECIAL

No. 4 · JULY 2026

Radar in-depth report

Blockchain and digital finance

Understanding distributed ledgers, tokenisation, MiCA, DeFi, stablecoins, ETFs and digital currencies

A Radar guide to finding your way through technology, rules, infrastructure and real risks.



Gruppo Radar · Comprendere oggi. Costruire domani

by effettoantropico.life

Responsibility notice

> ☒ **What to watch — Required notice**
> This in-depth report is intended solely for information and education. It does not constitute financial, legal, tax or investment advice. Blockchain technologies, crypto-assets and related financial instruments involve technical, economic, regulatory and operational risks. Any practical decision must be assessed with qualified professionals and up-to-date sources.

*Guiding editorial principle: **blockchain is not magic**: it is an infrastructure that records, connects and makes parts of digital value verifiable. But every infrastructure needs to be understood, governed and controlled.*

Guiding question: **who records value, who holds it in custody, who controls it**, under which rules and with what risks for those who participate?

Opening

Blockchain is often presented as a sudden revolution, but its real value does not lie in the promise of replacing everything. It lies in the possibility of recording information, ownership and transactions in a shared, verifiable way that is harder to alter. This is why finance is interested in it: because finance is made of ledgers, trust, transfers of value, rules, custody and responsibility.

Understanding blockchain does not mean becoming programmers or crypto investors. It means learning to distinguish a technology from a promise, a token (a digital representation recorded on a network) from a right, a decentralised network from a controlled platform, a stablecoin from a public currency, an ETF from direct ownership, and a market rule from actual protection.

This handbook was created to offer a compass: simple in its language, rigorous in its concepts, prudent in its conclusions. Because the digital future of finance calls for understanding, discernment and responsibility, rather than blind enthusiasm.

> 📌 **Did you know? — A map**
> In this in-depth report we move through five stages: technology, financial applications, tokenisation, rules and the future. The point is not to decide whether blockchain is good or bad. It is to understand when it is useful, where it risks being misrepresented, who governs it and what responsibilities it brings with it.

Part 1 - Understanding the technology

Editorial divider - Technology

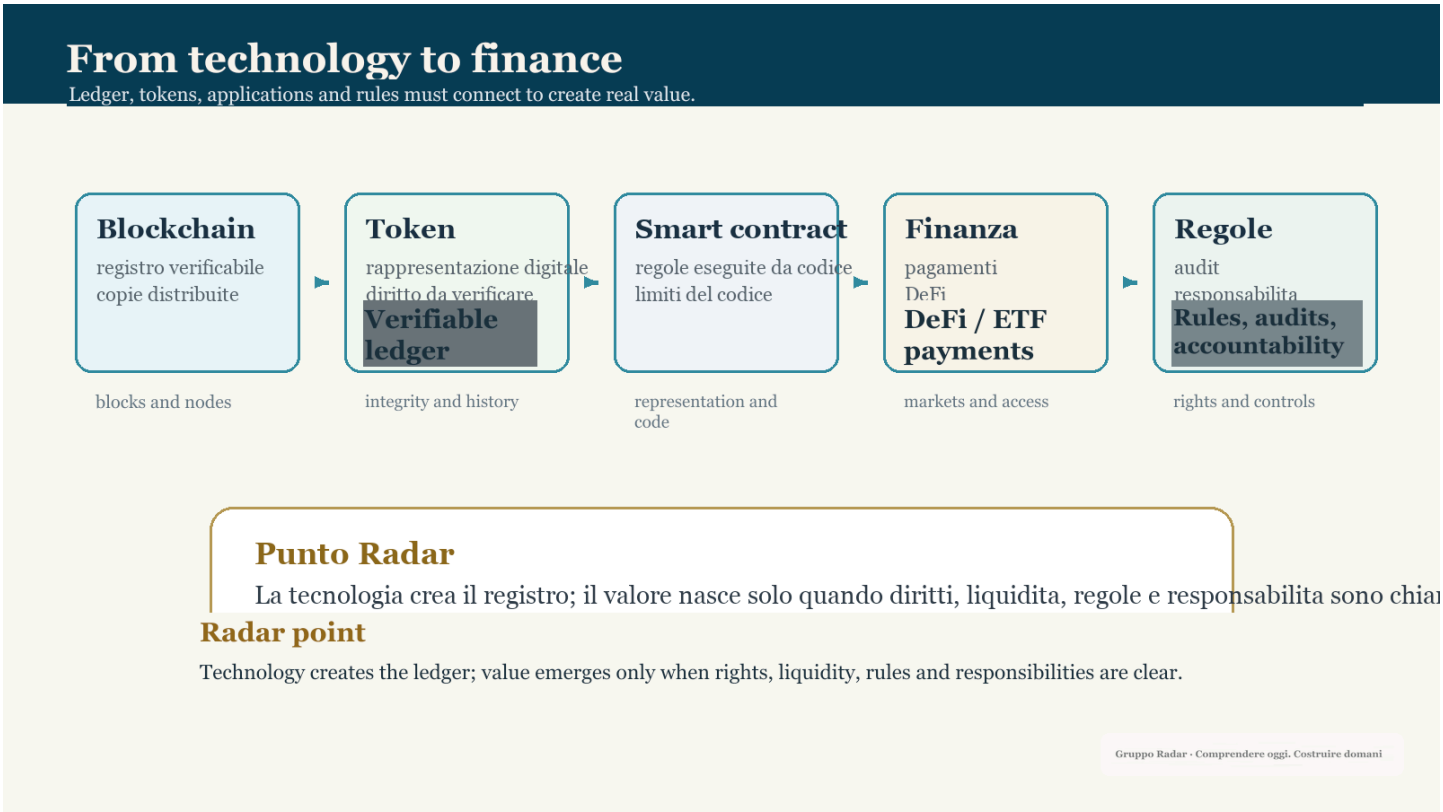


Chart 1 - from technology to finance.

Chapter 1 - Blockchain: what it actually records

A **blockchain** (a shared digital ledger linked together in blocks) is not a currency, not a single platform, and not a synonym for Bitcoin. It is a way of organizing data and transactions in a verifiable sequence, where each new block connects to the previous one through cryptographic references (mathematical techniques for protecting and verifying information).

The simplest example is a digital account book copied onto many computers. If someone tries to modify a page already recorded, the hash (the data's digital fingerprint) also changes, and the network can see that something does not add up. This does not make every abuse impossible, but it makes subsequent alterations more visible.

Traceable does not mean true. If the initial data is wrong, incomplete or entered by an unreliable party, blockchain records it in a more resilient way, but does not turn it into truth. **Blockchain protects the structure of the ledger, not the absolute truth of the real world.**

> **Radar Insight — Key**
> Blockchain does not replace trust: it redistributes it among code, the network, rules and verification. This can increase transparency and control, but it does not eliminate human responsibility.

Chapter 2 - DLT, hashes, blocks and nodes

DLT (*Distributed Ledger Technology*) is the broader family of shared ledgers. A blockchain is a DLT organised into linked blocks; not all DLTs are blockchains. This distinction avoids a frequent misunderstanding: calling any shared database a blockchain simply to give it an aura of innovation.

There are few essential components, but they need to be properly understood and clarified: **hash** (a digital fingerprint), **block** (an ordered container of data or transactions), **node** (a computer participating in the network), **chain** (the chronological connection between blocks) and **cryptography** (a set of mathematical techniques for protecting signatures, identities and data integrity).

Table - Quick technical glossary

Term	Simple explanation	Why it matters
Hash	A digital fingerprint of a piece of data	Makes it possible to check whether data has changed
Node	A computer participating in the network	Stores or verifies copies of the ledger
Block	An ordered container of transactions	Organises information over time
Chain	A link between blocks	Makes the historical sequence visible

☒ **Radar Insight — Key**
Blockchain's strength does not come from a single element, but from the combination of hashes, nodes, consensus rules and distributed copies of the ledger.

Chapter 3 - Consensus: how the network decides what is valid

Consensus (the set of rules by which a network decides which transactions to accept) is the mechanism that allows several nodes to maintain a consistent version of the ledger. It is not an ideal vote: it is a technical and economic procedure that assigns weight to those who produce, validate or propose blocks.

Proof of Work (proof of computational work) requires energy and computation; **Proof of Stake** (validation based on economic participation in the network) assigns weight to those who pledge capital as collateral;

Proof of Authority (validation entrusted to authorised parties) prioritises identity and control; consortium models (managed by several organisations) seek a balance between efficiency and mutual trust.

Decentralised does not mean without power. Even a technically distributed network can concentrate influence in validators (participants who

verify and validate network operations), developers, large holders, exchanges (trading platforms), cloud providers (providers of computing infrastructure) or foundations.

> ⚠️ **What to watch — Decentralised does not mean without power**
> A network can be technologically distributed yet concentrated in its governance (rules, powers and decision-making processes), liquidity, access to nodes or ability to influence updates.

> 🧠 **Radar Insight — Key**
> Consensus is blockchain's operational heart: it determines what enters the ledger. But the way consensus is designed also determines who carries more weight in the network.

Chapter 4 - Wallets, keys and custody

A **wallet** (a tool for managing keys and transactions) does not physically contain **crypto-assets** (digital assets recorded on a blockchain or DLT). It manages keys and digital signatures that allow assets recorded on the ledger to be controlled.

The **public key** (shareable information similar to an address) is used to receive or identify transactions.

The **private key** (a secret code that allows transactions to be signed) makes it possible to move assets.

The **seed phrase** (a sequence of words for recovering a wallet) is often the last possibility of recovery.

If the private key or seed phrase is lost, recovery may be impossible. If custody (key management) is entrusted to an intermediary, operational complexity decreases but counterparty risk increases (the risk that the custodian will fail to fulfil its obligations properly).

> ⚠️ **What to watch — The brutal rule of keys**
> Whoever controls the private key controls the assets. Technical freedom also increases operational responsibility.

> 🧠 **Radar Insight — Key**
> Blockchain can remove some intermediaries, but it does not remove the problem of custody: someone must always protect access, keys and responsibilities.

Chapter 5 - Public, private and consortium blockchains

Public blockchains are open and permissionless (without prior permission): anyone can read, submit transactions or participate according to the network's rules.

Private blockchains *are permissioned (with authorised access): they offer more control and often greater efficiency, but less openness.*

Consortium blockchains are managed by several organisations and can serve banks, supply chains or shared infrastructures.

The useful question is not just *"is it blockchain?"*. **The central question is: who governs the infrastructure?** We need to ask who can read, who can write, who validates, who updates the rules and who is accountable if something goes wrong.

> 🧠 **Radar Insight — Key**
> There is no single blockchain. Each architecture changes the relationship between openness, control, speed, transparency and responsibility.

Table - Public, private, consortium

Type	Access	Control	Typical use	Critical issue
Public	Open	Distributed	Bitcoin, Ethereum, DeFi	Scalability (the network's ability to handle an increase in operations), costs, governance
Private	Authorised	Central or restricted	Companies, banks	Less decentralisation
Consortium	Authorised by several parties	Shared	Supply chains, markets, institutions	Governance among participants

Part 2 - Understanding financial applications

Digital finance

Chapter 6 - Why finance looks to blockchain

Finance depends on ledgers: accounts, payments, securities, collateral, custody, identities, authorisations and transfers. Blockchain is of interest because it can

integrate recording, transfer and verification within the same digital infrastructure.

Blockchain does not always eliminate intermediaries: it often transforms them. In some cases it reduces reconciliation steps (comparisons between different ledgers); in others it creates new intermediaries: digital custodians, platforms, validators, data providers, audits and regulated entities.

The most common uses are *transfers of value, digital payments, tokenisation* (the digital representation of assets or rights), *smart contracts* (programs that execute rules), *stablecoins* (crypto-assets with a pegged value), *digital custody, audits and settlement* (the completion of a transaction through the transfer of money or securities).

> 🧠 **Radar Insight — Key**
> Finance looks to blockchain because finance is made of ledgers. But a more efficient ledger is not enough: rules, responsibilities and real markets are needed.

Chapter 7 - Bitcoin and crypto-assets

Bitcoin was the first major use case for public blockchain: a decentralised network, a digital asset and a public ledger that allows transfers without a central bank. But **blockchain does not mean Bitcoin. Bitcoin is a network; *bitcoin*, written in lower case, is the asset circulating on that network**.

Crypto-assets (digital assets based on cryptography and distributed ledgers) include different categories: **coin** (a network's native asset), **token** (a digital representation created on a network), utility token (a token linked to a use), governance token (a token carrying voting rights or influence), **stablecoin** and **security token** (a token that may represent financial instruments or economic rights).

Bitcoin can be studied as a monetary and technological innovation, but it remains a volatile asset. Fame does not eliminate market risk, operational risk, regulatory risk or custody risk.

> ⚠️ **What to watch — Famous does not mean safe**
> An asset's fame does not eliminate volatility, operational risk, regulatory risk or market risk.

> 🧠 **Radar Insight — Key**
> Bitcoin brought blockchain to the public's attention, but blockchain and crypto are not the same thing. Understanding the difference prevents many misunderstandings.

Chapter 8 - Stablecoins: promised stability and actual reserves

Stablecoins are crypto-assets designed to maintain a stable value relative to a currency or a basket of assets. The **peg** (the anchoring of value) is the promise; the reserves (the assets supporting the value) are what needs to be verified.

Stablecoin does not mean safe. Stability depends on reserves, liquidity (the ability to convert quickly), governance (rules and decision-making powers), transparency, audits (independent verification) and the regulatory framework. A **depeg** (loss of the peg) shows that the promise can break.

Within the European **MiCA** *(Markets in Crypto-Assets Regulation)*, the rules for **asset-referenced tokens** (tokens other than e-money tokens that aim to maintain a stable value by reference to other values or rights, including in combination) and **e-money tokens** (tokens that aim to maintain a stable value relative to a single official currency) are central precisely because the declared stability must be supported by verifiable requirements.

Table - Stablecoins: what to check

What to check	A simple question
Reserves	What supports the stated value?
Liquidity	Can it be converted quickly?
Issuer	Who is responsible?
Audit	Who checks the reserves?
Rules	Within which regulatory framework does it operate?

> 🧠 **Radar Insight — Key**
> A stablecoin promises stability, but that stability must be verified: reserves, liquidity, governance and rules matter more than the slogan.

Chapter 9 - Smart contracts and DeFi

A smart contract (a program that executes instructions when defined conditions are met) is not intelligent in the human sense and is not automatically correct. **A smart contract does not mean a sound contract.** Code executes rules: if those rules are fragile, even automatic execution can cause harm.

DeFi (decentralised finance) is the set of financial services built on **smart contracts**: decentralised exchanges, loans, **liquidity pools** (reserves of liquidity supplied by users), **derivatives, automatic protocols and yield farming** (automatic strategies for seeking returns).

The main risks are bugs (errors in the code), cyberattacks, manipulated oracles (tampered external data providers), lost keys, opaque governance, hidden leverage, fragile liquidity and the absence of traditional protections.

> ⚠️ **What to watch — Smart does not mean wise**
> A smart contract executes rules. If those rules are wrong, incomplete or vulnerable, the outcome can be harmful even when execution is automatic.

> 🧠 **Radar Insight — Key**
> DeFi shows the power of programmable finance, but programmability does not eliminate risk: it shifts it into code, liquidity, governance and security.

Chapter 10 - Bitcoin ETFs: exposure does not mean ownership

An **ETF** (Exchange-Traded Fund, a fund traded on an exchange) provides exposure to the price of an asset without owning it directly. In the case of spot Bitcoin products, the investor buys units in a regulated financial product and does not directly control bitcoin in a wallet.

An ETF does not mean direct ownership. Custody, rights, costs, intermediaries and responsibilities change. Direct ownership requires key management; exposure through a financial product requires a broker (an intermediary that executes buy or sell orders), a regulated market, an issuer and institutional custody.

The **SEC** (Securities and Exchange Commission, the US financial markets authority) approved the listing and trading of eleven spot Bitcoin products on 10 January 2024. This approval concerns listing and trading rules; it is not a judgement on Bitcoin's value or safety.

> 🧠 **Radar Insight — Key**
> An ETF can make access to Bitcoin's price simpler, but it is not equivalent to owning Bitcoin. Custody, rights, risks and intermediaries change.

Part 3 - Understanding tokenisation

Tokenisation and rules

Chapter 11 - Tokenisation: representing value in digital form

Tokenisation is the digital representation of an asset, a right or a financial instrument through a token recorded on a blockchain or DLT. **A token does not mean ownership.** The token denotes a representation; the right depends

on the contract, applicable law, issuer, custody and the practical ability to enforce that right.

Property, bonds, shares, fund units, commodities, receivables, certificates, works of art or economic rights can be tokenised. But tokenising does not automatically make an asset liquid (easy to sell), safe or legally straightforward.

The delicate part is the bridge between the digital world and the real world: *who guarantees that the asset exists, who holds it in custody, which contract connects the token to the right, which court rules in a dispute, and which market makes an exit possible.* **Table -**

Token vs right

Type of token	What it might represent	A question to ask
Real estate	An economic, corporate or contractual interest in a property	What right do I actually have over the asset?
Financial	A regulated financial instrument or economic right	Which regulations apply?
Utility token	Access to or use of a service	Does the service exist, and is it actually useful?
Governance token	Influence over protocol decisions	Does the vote count, or is it merely symbolic?

🧠 **Radar Insight — Key**
The token is a representation. The actual right depends on the contract, applicable law, issuer, custody, governance and the effective ability to enforce that right.

Chapter 12 - Real estate tokenisation: the clearest example

Imagine a property worth 1 million euros divided into 10,000 tokens of 100 euros each. Access appears to become simpler. *But the question is not how much the token costs. It is: what does it actually represent?*

Does the token grant actual ownership? Does it entitle the holder to a share in a company? Does it entitle the holder to part of the income? Who manages the property? Who pays for maintenance, taxes, expenses and insurance? Who decides whether to sell? Is there a market on which to resell the token? What happens if the issuer fails? Which law applies?

Blockchain can record the circulation of a token, but it does not replace land registries, contracts, special purpose vehicles (legal entities created to manage an asset), governance or legal protection.

⚠️ **What to watch — Bricks do not magically enter the blockchain**

Blockchain can record a token linked to a property, but it does not replace land registries, contracts, special purpose vehicles, governance, responsibility or legal protection.

🧠 **Radar Insight — Key**

A real estate token can make an economic interest more accessible, but without a clear legal structure it remains a fragile digital promise.

Part 4 - Understanding the rules

Rules

Chapter 13 - MiCA: the European framework

MiCA (Markets in Crypto-Assets Regulation) is EU Regulation 2023/1114. It creates a harmonised framework for crypto-assets and related services not already covered by traditional financial legislation.

According to the European Commission, MiCA entered into force on 29 June 2023. The rules on asset-referenced tokens (tokens linked to a basket of assets) and e-money tokens (tokens linked to an official currency and comparable to electronic money) have applied since 30 June 2024; general application began on 30 December 2024. In 2026 the Commission also launched consultations on a review of the MiCA framework, a sign that regulation remains in evolution.

Regulated does not mean guaranteed. MiCA introduces rules on transparency, white papers (information documents), authorisations, customer protection, stablecoins and CASPs, but does not eliminate volatility, fraud, poor management, technological risks or business failures.

🧠 **Radar Insight — Key**

MiCA attempts to bring order to part of the European crypto market, but regulated does not mean guaranteed, and it does not mean risk-free.

Chapter 14 - CASPs, white papers and operators' responsibilities

CASP (Crypto-Asset Service Provider) refers to operators offering services such as custody, trading platforms, crypto/currency exchange, crypto/crypto exchange, order execution, placing, advice, portfolio management and transfers on behalf of customers.

The **white paper** (an information document on the project, risks, rights, issuer, technology and economics) helps make the offering easier to understand. But the presence of a document is not equivalent to a guarantee: its content, responsibilities, limits and controls must be read.

ESMA (European Securities and Markets Authority) maintains MiCA registers covering white papers, issuers, and authorised or non-compliant CASPs. Here too, the point is not to stop at the word *"register"*: we need to verify what the record actually says.

> ⚠️ **What to watch — A white paper is not a guarantee**
> *The presence of an information document does not eliminate risk, volatility, poor management or a project's fragility. It must be read, compared and verified.*

> 🧠 **Radar Insight — Key**
> *Authorised operators broaden the scope of accountability, but readers still need to understand the product, custody, rights and risks.*

Chapter 15 - AML, KYC, the Travel Rule and audits

AML (Anti-Money Laundering) and **KYC** (Know Your Customer, verification of the customer's identity) are intended to reduce money laundering, fraud and the illicit use of platforms. The **Travel Rule** (a rule requiring information about the originator and beneficiary of transfers) extends the traceability of information to certain transfers of value.

These rules increase control and responsibility, but also raise sensitive issues: privacy (the protection of private life), surveillance, data processing, financial autonomy and the power of intermediaries.

Audits (independent checks or verifications) may cover smart contract code, stablecoin reserves, custody, governance, cybersecurity, the correspondence between a token and a real-world asset, AML/KYC procedures and data quality.

> 🧠 **Radar Insight — Key**
> Compliance increases control and traceability, but does not solve the problem of trust on its own. It shifts the weight onto operators, audits, rules and verifiable responsibilities.

Part 5 - Understanding the future

The future

Chapter 16 - CBDCs and the digital euro

A **CBDC** (Central Bank Digital Currency) is public money in digital form. Digital does not mean decentralised. A CBDC may or may not use DLT; in either case, it remains within an institutional infrastructure.

The **digital euro** (the ECB's digital euro project) is neither a cryptocurrency nor a private stablecoin: it would be a digital form of cash issued by a central bank, intended to complement cash and existing payment solutions. The ECB states that the project moved into its next phase in October 2025 and aims to be ready for a possible first issuance in 2029, if the necessary EU legislation is adopted during 2026.

The central discussion concerns online/offline payments, privacy, inclusion, the role of intermediaries, central control and the relationship with banks and private infrastructures. The important point is prudence: the ECB itself speaks of a possible issuance and notes that no final decision has yet been taken.

> ⚠️ **What to watch — Digital does not mean decentralised**
> A public digital currency can modernise payments, but it remains within an institutional, centralised infrastructure.

> 🧠 **Radar Insight — Key**
> The future of digital money does not run through crypto alone: it also runs through central banks, rules and the relationship between efficiency, privacy and control.

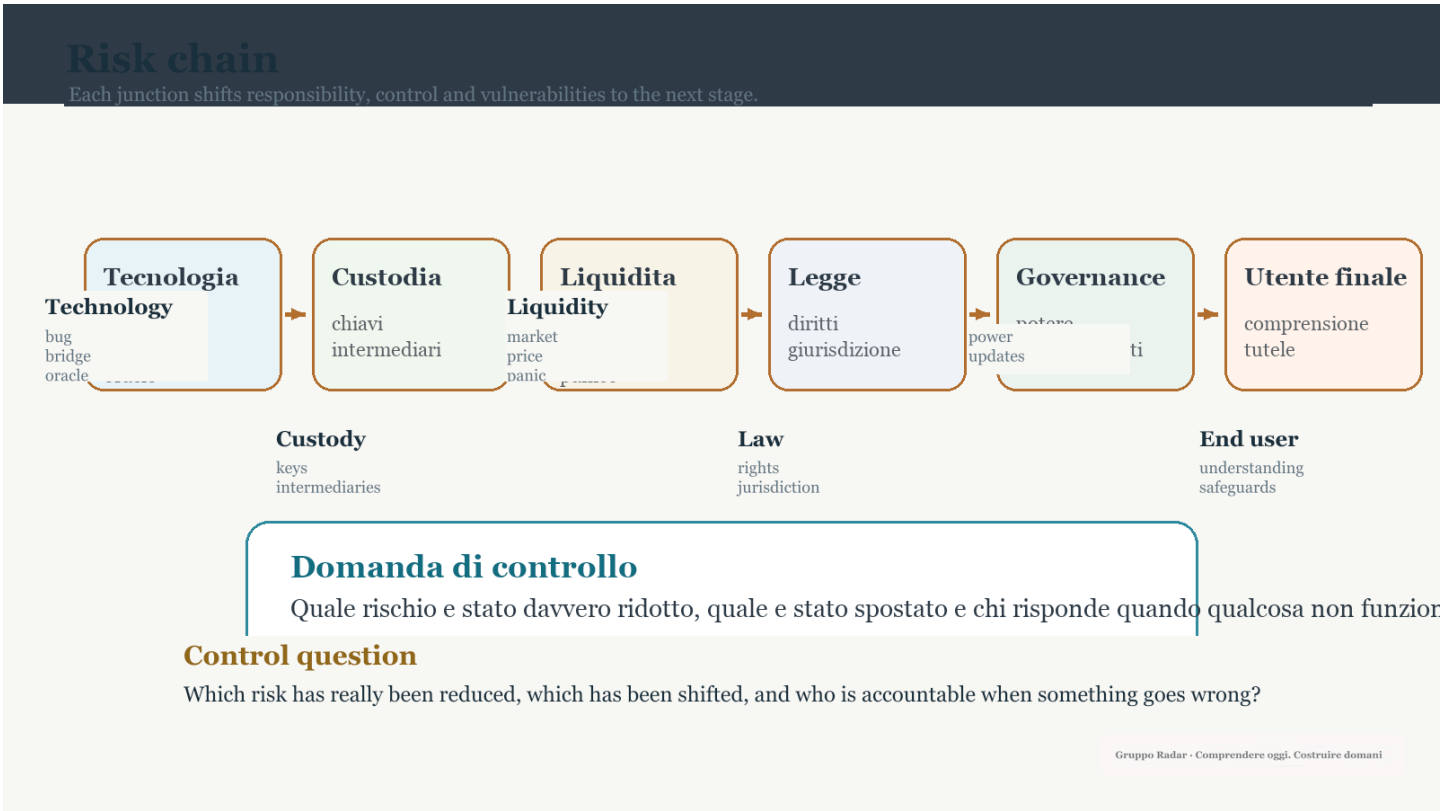


Chart 2 - the chain of risk.

Chapter 17 - Institutional tokenization and the future of markets

Banks, exchanges, depositories, funds and institutions are studying DLT and tokenization for financial instruments, settlement, custody, payments and

markets. The most transformative aspect may not be “buying crypto”, but making certain infrastructures of traditional finance programmable and more efficient.

The most relevant areas are tokenised bonds, tokenised funds, faster settlement, digital collateral, programmable payments, continuous auditing, shared infrastructures and interoperability (the ability of different systems to communicate and work together).

The **BIS** (Bank for International Settlements) emphasises that tokenisation and unified ledgers can work better when settlement (final settlement) and central bank money remain integrated: trust and payment finality are not minor details.

> 🧠 **Radar Insight — Key**
> Institutional tokenisation does not erase traditional finance: it can change its infrastructure, timing, costs, responsibilities and controls.

Chapter 18 - Open risks: technology, markets, law and society

Technical risks include bugs, attacks, vulnerable bridges (connections between blockchains), manipulable oracles, poorly written smart contracts and lost keys. Economic risks include volatility, fragile liquidity, leverage (the use of debt or amplified exposure), market panic, unsound stablecoins and unsustainable returns.

Legal risks concern unclear rights, uncertain jurisdiction, issuer failure, non-compliant tokens and poorly defined responsibility. Social risks include surveillance, digital exclusion, concentration of power, dependence on private infrastructures and a false sense of control.

The promise of efficiency must always be read alongside the critical question: *which risks are reduced? Which are shifted, and which become less visible?*

> ⚠️ **What to watch — Risk does not disappear: it changes form**
> When a technology promises efficiency, we must always ask which risks are reduced, which are shifted and which become less visible.

> 🧠 **Radar Insight — Key**
> Understanding how blockchain works is not enough. We need to understand who governs it, what it promises, what it actually guarantees and what happens when something goes wrong.

Chapter 19 - Critical questions before believing in a project

The most useful page of a Radar in-depth report is the one that slows the decision and encourages reflection and critical thinking. Before believing in a project, curiosity must be turned into verifiable questions.

This checklist (a list of checks) is not intended to make us always say no. It is intended to prevent words such as decentralization, tokenization, return, stable coin or regulated from being used as cognitive shortcuts.

- Who governs this network?
- Who can change the rules?
- Who holds the assets in custody?
- What right do I actually have?
- What happens if I lose the key?
- What happens if the issuer fails?
- Is there a real market on which to sell?
- Where does the promised return come from?
- Has the code been audited?
- Is the operator authorized?
- Is the product regulated, or merely presented as such?
- Which risks am I not seeing?
- Who benefits from my participation?
- What can I verify independently?

> 🧠 **Radar Insight — Key**
> The most important question is not “what return does it offer?”, but “what am I actually buying, who controls it, and what risks am I taking?”

Chapter 20 - Editorial conclusion

Blockchain should neither be idolized nor rejected on principle. It needs to be understood. It is a technology that can change how we record value, trust and rights, but every practical application must be assessed in its technical, economic and legal context.

The initial question remains the compass: *who records, who holds in custody, who governs, who controls, who is accountable?* Without these answers, the word blockchain can become a new form of opacity. The digital future of finance will be built not only by those who possess technology, but by those able to combine innovation, responsibility, transparency and discernment.

🧠 Radar Insight — Final key

Blockchain can become an infrastructure of trust only if it remains understandable, verifiable, accountable and governed by comprehensible rules. Without understanding, even the most advanced technology becomes a new form of opacity.

Glossary and progressive vocabulary

Brief definitions, designed to let you reread the document without having to consult an external technical source.

Term	Simple definition
Blockchain	A shared digital ledger, organised into interconnected blocks.
DLT	Distributed ledger technology, a broader family than blockchains.
Node	A computer that stores, sends or verifies network data.
Block	An ordered container of data or transactions.
Hash	A digital fingerprint that changes if the data changes.
Consensus	The rules by which the network decides what is valid.
Proof of Work	Consensus based on computational work and resource consumption.
Proof of Stake	Consensus based on capital pledged as collateral within the network.
Proof of Authority	Consensus entrusted to identified, authorised parties.
Wallet	A tool for managing keys and signing transactions.
Public key	Shareable information, similar to an address.
Private key	A secret code that allows assets to be controlled and transactions to be signed.
Seed phrase	A sequence of words used to recover a wallet.
Mining	The validation process typical of Proof of Work.
Staking	Economic participation used in some Proof of Stake networks.
Smart contract	A program that executes rules when defined conditions are met.

Term	Simple definition
Token	A digital representation of an asset, right, function or utility.
Coin	A blockchain's native asset, such as bitcoin on the Bitcoin network.
Crypto-asset	A digital asset based on cryptography and distributed ledgers.
Stablecoin	A crypto-asset designed to maintain a stable value relative to a reference.
Peg	The stated anchoring of value.
Depeg	The loss of the stated peg.
DeFi	Decentralised finance built on smart contracts.
TVL	Total Value Locked, the total value locked in a protocol.
Liquidity pool	A reserve of liquidity supplied to a protocol by users.
Oracle	An external source that brings data into a smart contract.
Bridge	A technical connection between different networks or blockchains.
Layer 1	The underlying blockchain on which native transactions are recorded.
Layer 2	A solution built on top of a blockchain to increase efficiency or scalability.
Tokenisation	A digital representation of an asset, right or financial instrument.
Real-world asset	An asset or right that exists outside the blockchain.
Security token	A token that may represent a regulated financial instrument or economic right.

Term	Simple definition
Utility token	A token that gives access to a service or function.
Governance token	A token used to vote on or influence protocol decisions.
ETF	An exchange-traded fund that provides exposure to an asset or index.
Custody	The management of keys or assets by oneself or an intermediary.
Self-custody	The user's independent custody of their keys.
CASP	A crypto-asset service provider under MiCA.

MiCA	The European regulation on markets in crypto-assets.
AML	Anti-money laundering: rules against money laundering and illicit financing.
KYC	Verification of the customer's identity.
Travel Rule	A rule requiring information about the originator and beneficiary of transfers.
CBDC	A digital currency issued by a central bank.
Digital euro	The ECB's digital euro project, distinct from crypto and private stablecoins.
Audit	An independent check or verification.
White paper	An information document on the project, risks, rights and issuer.
Interoperability	The ability of different systems to communicate and work together.
Governance	The set of rules, powers and decision-making processes.

Methodological notes

This in-depth report uses a Radar reading criterion: separating technology, promise, rights, markets and responsibility. Regulatory and institutional information should be read as a snapshot current at the time of writing and may change over time. For this reason, the most sensitive references must be checked against official sources before any public reuse.

Editorial snapshot: 6 July 2026. The document contains no operational, investment, tax or legal recommendations. References to MiCA, the SEC and the digital euro are presented as informational context verified against official or institutional sources.

> 🧠 **Radar Insight — The Radar method**
>
> The selection favours concepts that help distinguish signal from noise: what the technology records, which right the token represents, who governs the infrastructure, which rules apply and which risks remain unresolved.

Essential sources and useful references

NIST - Blockchain Technology Overview, NISTIR 8202, 2018: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

European Commission - Crypto-assets, page updated on 20 May 2026; MiCA framework and 2026 consultations: https://finance.ec.europa.eu/digital-finance/crypto-assets_en

EUR-Lex - Regulation (EU) 2023/1114, Markets in Crypto-Assets Regulation (MiCA): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1114

ESMA - Markets in Crypto-Assets Regulation (MiCA), registers and implementation measures: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica

FATF - Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 2021: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

FATF - Virtual Assets topic page: preventive measures, licensing, travel rule: https://www.fatf-gafi.org/en/topics/virtual-assets.html

ECB - Digital euro, project status and FAQs updated in 2026: https://www.ecb.europa.eu/euro/digital_euro/html/index.en.html

SEC - Order Granting Accelerated Approval for Bitcoin-Based Commodity-Based Trust Shares and Trust Units, 10 January 2024: https://www.sec.gov/files/rules/sro/nysearca/2024/34-99306.pdf

BIS - Annual Economic Report 2023, Blueprint for the future monetary system: tokenization and unified ledger: https://www.bis.org/publ/arpdf/ar2023e3.htm

🧠 Radar Insight — The key to sources

Institutional sources do not remove the need for judgement: they help verify dates, scope and definitions. The editorial interpretation remains oriented towards prudence and understanding.

© 2026 Barbara Gattobigio · Gruppo Radar

Comprendere oggi. Costruire domani · by effettoantropico.life All rights reserved for original content. Free access does not authorise reproduction or republication without consent, except for uses permitted by law. Third-party materials remain the property of their respective rights holders. To share this issue, use the link to the article.