RADAR WEEKLY

N. 13 · 14 SEPTEMBER 2026

The cost of trust

MiCA reshapes crypto finance as energy, rates and AI safety raise the price of capital, speed and accountability.



Gruppo Radar · Comprendere oggi. Costruire domani

by effettoantropico.life

The week in focus

For years, in the world of crypto-assets, trust depended chiefly on how well known a platform was, the reputation of a brand, or the promise that customers' funds were treated properly. A person may have a few dozen or several hundred euros in an app, use a wallet to hold or transfer value, receive a digital payment, or buy a financial product exposed to crypto without directly owning a token. The action is simple; behind it, however, are companies, accounts, keys, fees and responsibilities that often remain invisible.

Europe is trying to change this relationship. MiCA, the European regulation on markets in crypto-assets, requires those professionally offering certain services to be identifiable, to have minimum resources and to leave an auditable record of their work. It does not make crypto safe, prevent losses or turn a risky investment into a prudent one. It does, however, make an essential point clearer: who has the relationship with the customer, where their funds are held and who must answer if something goes wrong.

This is the question running through the issue: how much does it cost to turn trust into verifiable obligations, who bears that cost, and how much of it may fall, in different forms, on people, small businesses and markets?

1. Time is running out to comply

MiCA became fully applicable on 30 December 2024. To avoid shutting down overnight services that were already operating under national rules, member states were permitted a transitional period: a limited time to apply, organise and obtain — or fail to obtain — authorisation. That period could run until 1 July 2026, but for an individual operator it may end earlier, when the authority grants or refuses authorisation.

For someone opening an app or using a familiar service, the change may seem distant. In fact, it shifts the question from "do I know this name?" to "who is actually offering this service in Europe?" From 1 July, the market should no longer be read merely as a shop window of platforms. Anyone professionally offering crypto-asset services in the Union must fall within MiCA's perimeter: it may be a CASP, the company authorised to provide crypto services, or a bank or other financial institution able to carry out that activity under the conditions set by the regulation.

A narrow exception remains, often called reverse solicitation, or the exclusive initiative of the customer. Simply put, a person independently seeks out a foreign provider without that provider having advertised or promoted the service to them in the European market.

> 🧠 **Radar Insight — Regulated trust has a cost**
>
> A rule does not replace an investor's prudence. It does, however, try to make visible who is operating, with a place of business in the Union, adequate resources and a structure that can be supervised even after authorisation has been obtained.

2. Behind the app there must be an identifiable company

CASP is not the name of the app on a phone, nor the brand appearing in advertising. It is the company authorised to carry out one or more crypto-asset services: for example, holding them in custody, executing an exchange, transferring them or offering advice. Article 59 requires that the company have its registered office in a member state where it carries out at least some of its services, effective management in the Union and at least one director resident in the EU. The authorisation also specifies which services that particular entity may offer.

For a person buying small amounts through an app, this is a simple but not trivial check. In the MiCA register maintained by ESMA — the European securities and markets authority — one can look up the legal name of the company, the country that authorised it, the authority supervising it and the permitted services. It is not a way to choose the "right" token; it helps answer a more basic question: **with whom do I actually have a relationship?**

Once authorised in one member state and having complied with the prescribed procedure, a CASP may also offer its authorised services in the other countries of the Union. This is the **European passport**: not a general licence to do anything, but a way to avoid requiring the same company to start from scratch in every country, while remaining within the services it has been authorised to provide.

In Italy the change is already visible. On 30 June the Bank of Italy announced the end of the transitional period and the presence of nine authorised entities. On 7 May Consob had authorised CheckSig S.r.l. Società Benefit as the first Italian CASP, following the Bank of Italy's favourable opinion. For a person using a service, what matters is not the first-place distinction itself: it is the ability to distinguish the authorised company from a mere trading name.

> 📌 **Did you know? — A "global brand" is not the same as an "authorised EU entity"**
>
> A brand may be familiar, but it does not by itself say who holds assets in custody, executes or transfers. The ESMA register exists precisely to show the company, supervisor and authorised service, without relying only on the platform's reputation.

3. An economic cushion against fragile services

When a platform offers a service to many people, it is not enough for it to work on quiet days. It must be able to face errors, interruptions and unexpected costs without immediately passing everything on to the customer. MiCA calls this requirement **prudential safeguards**: in practice, an economic cushion the operator must maintain to have a minimum base and keep functioning in difficult moments.

Article 67 requires the higher of a minimum threshold and one quarter of the previous year's fixed overheads, reviewed annually. The thresholds in Annex IV are €50,000, €125,000 or €150,000, depending on the type of service. Own funds are the firm's resources, not money paid in by customers. An operator may use own funds, an insurance policy covering specific risks, or a comparable guarantee, including in combination.

An example makes the rule clearer. If a small company has annual fixed costs of €800,000 for staff, IT systems, rent, security and insurance, one quarter of those costs is €200,000. Even if its service were subject to a €150,000 threshold, it would have to maintain the higher amount, €200,000. For someone using the app, this is not a personal savings pot or a guarantee that the purchased token will retain its value. It does, however, reduce the risk that the service was built without an economic base proportionate to the work it claims to perform.

An insurance policy is not a generic detail. It must cover risks such as errors, omissions and operational interruptions and, when the business model requires it, gross negligence in the custody of customers' funds and crypto-assets as well. The other side deserves attention: more capital, staff and insurance may translate into higher costs. These could be absorbed by the company's margins, appear in fees or the spread — the difference between the purchase and sale price — or result in a narrower offering. This is a possibility to watch, not an effect already demonstrated.

> 🧠 **Radar Insight — The higher of the nominal minimum and one quarter of fixed overheads**
>
> The €50,000, €125,000 and €150,000 thresholds do not tell the whole story. If the organisation grows, the rule also looks at what it costs to maintain: the cushion must grow with the service the firm has decided to offer.

For a large platform the expense can be spread across many users; for a small business it may weigh more heavily. This is not a condemnation of scale or proof that smaller firms will disappear. It is the concrete cost of a promise: continuing to answer to customers even when the service does not run as expected.

4. The €500 in the app is not the platform's property

The distinction to keep clear here is between three different things: traditional money paid in by a person before a purchase; crypto-assets they may have held in custody; and the assets of the firm offering the service. They may appear within the same digital experience, but must not be confused.

Article 70 requires CASPs receiving customers' funds, other than electronic money tokens, to protect customers' ownership rights and not use those funds for their own account. By the end of the business day following receipt, the money must be placed with a bank or central bank in an identifiable account separate from the firm's funds. This mandatory separation, called segregation of funds, prevents the platform from mixing customer money with its own and using it to pay expenses, salaries or debts.

Imagine €500 loaded into an app before buying a crypto-asset. That €500 should not become a financial shortcut for the company; it must be kept distinct from its resources. If the person then buys a token, the type of risk changes: price fluctuations, the difficulty of selling or quickly converting a crypto-asset without a significant loss, or a technical problem with the token do not disappear because the initial money was separated. The rule protects against confusion between the customer and the intermediary; it does not guarantee a return or prevent every loss. A clarification in the ESMA–Commission Q&A of 18 February 2026 adds a small but concrete detail: the CASP cannot retain interest earned on customers' funds deposited with a credit institution; it must be passed on to the customer. The Q&A helps interpret the rules, but does not replace the definitive interpretation of the Court of Justice of the European Union.

> ⚠️ **To watch — Protection does not mean a guarantee of capital**
>
> Keeping funds separate reduces a platform-related risk. It does not eliminate token price fluctuations, illiquidity — the difficulty of selling or quickly converting a crypto-asset without a significant loss — partial or total losses, or technical risks. Where relevant, MiCA also requires clarity about what does not exist: an automatic deposit guarantee or automatic compensation for the investment.

5. Behind a reliable app are people, controls and understandable costs

Capital is only part of the story. Behind an app that promises to hold, transfer or exchange value there must be responsible people, protected IT systems, procedures for managing an error and a way to continue serving customers during an interruption. MiCA requires all this to be documented: who leads the firm, what expertise they possess, how risks are managed, how ICT systems — the technologies and data that make the service work — are protected, and how decisions can be reconstructed.

For someone using a service, part of this work should be visible: understandable costs and conditions, declared fees, a readable difference between purchase and sale prices, and clear custody agreements. A small investor must be able to understand what they pay; a family using a wallet or a transfer service must be able to know the rules and costs under which digital money is moved; a small business must consider that staff, security, insurance and controls are real costs for the provider, not words on the back of a contract.

When the service is advice or portfolio management, Article 81 requires knowledge of the customer's experience, objectives, risk tolerance and capacity to bear losses. These are the appropriateness and suitability assessments: different checks, but both intended to understand whether the proposed service and risk are consistent with the person in front of the provider. Someone claiming to offer independent advice cannot then secretly be paid by a third party to steer the customer towards a product; these payments or benefits are third-party inducements and may be accepted only within the prescribed limits, when they genuinely improve the service and do not compromise its independence. Article 75 requires a custody agreement setting out conditions, costs and charges. Article 66 requires prices, costs and fees to be published visibly. They may look like details, but they are what allows a person to compare a service and a supervisor to understand how it operates.

> ⚠️ **To watch — Where do the costs go?**
>
> More technology, specialist staff, insurance and controls may favour large operators able to spread the expense across many customers. The European passport can also reduce duplication and make the market easier to compare. Concentration is not a foregone conclusion: it must be measured by looking at fees, spreads, service quality and the room left for specialist firms.

6. What changes for citizens, savers, businesses and funds

People who do not invest directly

Someone who does not buy crypto-assets receives no new obligation from MiCA and does not automatically see their current account change. They may nevertheless encounter the regulation indirectly: through digital payments, related services, an employer using a crypto provider, or a financial product distributed to the public. The possible effect is a more identifiable, sometimes more expensive offering, and a clearer separation between whoever advertises a brand and whoever is responsible for the service.

People who buy or hold crypto through an app

For a private saver who buys or holds crypto through an app, the most useful check comes before choosing a token: look in the ESMA register for the authorised European company and authorised service. Custody, executing an exchange, transferring and providing advice are different activities. Knowing which of these activities one is using helps establish whom to hold accountable for a problem. Segregation of funds and cost transparency protect the relationship with the intermediary; they do not guarantee the value of the asset purchased, eliminate illiquidity — the difficulty of selling or quickly converting a crypto-asset without a significant loss — or automatically trigger deposit guarantees or investor compensation.

Stablecoins, wallets and transfers

A stablecoin is a crypto-asset designed to maintain a stable value relative to a currency or another asset. Designed does not mean risk-free. For a family, a worker paid through digital services or a professional receiving transfers, it is useful to distinguish the token, the service and the intermediary. The token is the digital unit; the service allows it to be held, transferred or exchanged; the intermediary is the entity that may perform that service or control the means of access. A self-custody wallet is not a deposit with a platform. A stablecoin is neither the company that issues it nor the app

that makes it usable. The concrete question remains: who manages the keys, the transfer or the customer relationship?

Small businesses and professionals

A small business receiving payments or using a crypto provider encounters a service that, to remain in the market, must sustain capital or insurance, cybersecurity, competent people, business continuity and documentation. Some of those expenses may remain in margins, reach fees and spreads, or appear in additional services. We do not yet know to what extent this will happen, or whether it will happen in the same way for everyone. That is precisely why the financial conditions should be understandable, not hidden behind a familiar name.

Advisers, managers and financial products

For advisers and managers, appropriateness, suitability, costs, inducements and documentation define the customer relationship. Explaining risk does not make a crypto-asset prudent; it does, however, make it possible to check whether a proposal was consistent with what the person said they knew, their objectives and the service provided.

A boundary deserves particular care for anyone accessing crypto through a fund or a product distributed to the public. MiCA does not automatically replace the rules governing financial instruments, harmonised funds or other investment funds. The abbreviations MiFID II, UCITS/OICVM and AIFMD remain in the sources because they identify these different perimeters, but what matters to the citizen is the translation: a fund or product with crypto exposure continues to follow its own distribution and protection rules. MiCA may cover part of the infrastructure used — the issuer, custody, execution or the CASP — without automatically turning that product into an investment protected in every respect.

> 📌 **Did you know? — Who is affected and how**
>
> Anyone directly using a crypto service should be able to identify the company, authorisation and service. Families and small businesses may feel the effects in the offering and its costs, without their relationship with their bank automatically changing. MiCA is not a guarantee of token value and does not replace the rules specific to funds, financial products or deposits.

7. When the intermediary seems to disappear

DeFi, or decentralised finance, brings together financial services built on programs executed on blockchains, often without the counter or traditional bank to which we are accustomed. For a person using a website or app, the experience can seem as simple as that of an ordinary platform. Yet the phrase “it is decentralised” alone does not say who can change the rules, hold a key or interrupt a service.

A smart contract is a program that automatically executes rules written in code. A bridge is a link that moves or represents value between networks; a sidechain is a network connected to the main one; the front end is the website or app through which a person interacts with the service.

There may also be keys controlled by someone, governance that approves updates, fees collected by an entity and automatic limits set by an operator. The useful questions therefore remain very concrete: who holds the keys? Who updates the code? Who manages the website? Who collects the money? Who can stop an exceptional withdrawal?

MiCA chiefly organises the identifiable intermediary. It does not settle the debate about genuinely decentralised protocols, which the European Commission will have to assess in the future application of the regulation. It does, however, prevent the word “decentralised” becoming an automatic answer when someone professionally offers a service to the public.

This week’s Liquid/SideSwap case shows why these distinctions are needed. In its post-mortem of 9 September, SideSwap attributes the origin of the incident to a consensus bug in the Elements software underlying the Liquid Network, which it says allowed approximately 4,000 L-BTC unsupported by deposits to be created. According to the company, the peg-out service — the process by which value returns from the Liquid network to Bitcoin — treated those L-BTC as an ordinary order, releasing approximately 3,996 BTC. SideSwap says none of its own keys, wallets or systems was compromised; it nevertheless acknowledges that an online authorisation key, an automatic payment and the absence of thresholds, rate controls and human review turned a protocol defect into an actual loss.

This is SideSwap’s reconstruction and acceptance of responsibility. It nevertheless shows that a network can be distributed while containing very concrete points at which a person or organisation decides whether a withdrawal occurs automatically, under what limits and with what controls. On 10 September SideSwap markets reopened; the update of 11 September says peg-ins were available again and peg-outs remained

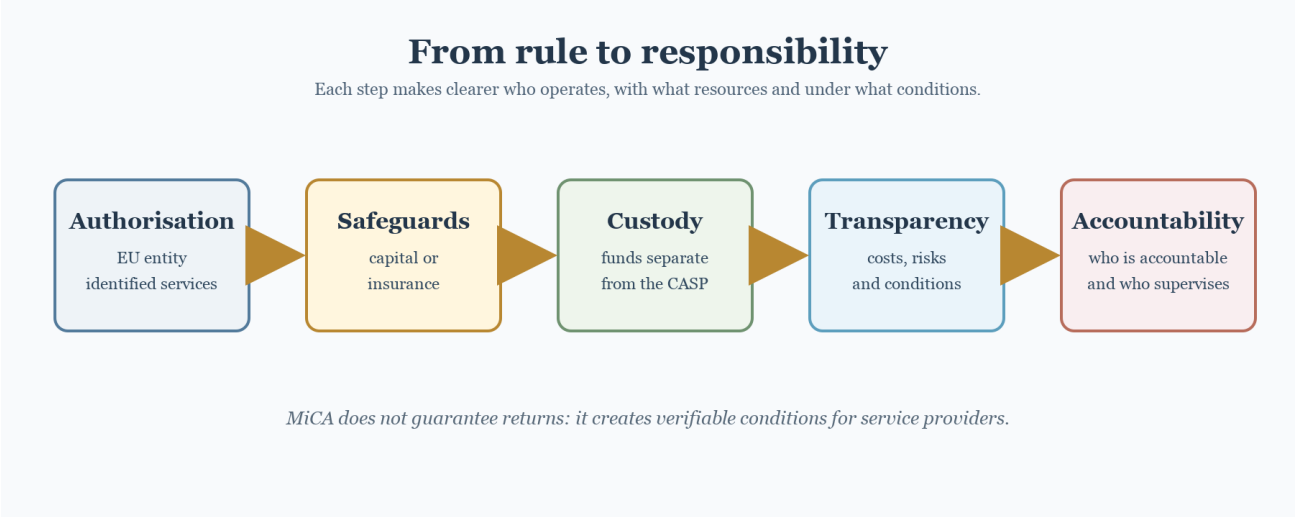
closed while the security review continued. The status of the peg and any reimbursements remains an open process.

> ⚠️ **To watch — Liquid shows where control reappears**
>
> Protocol, federation, bridge, authorisation key, peg-out service and wallet are not the same thing. The incident does not prove that all DeFi is unsafe; it invites us to follow value at the points where it moves from an automatic rule to a decision, threshold or managed interface.

In the United States the regulatory frontier is different and still open. At the close of this issue, the Senate's official schedule indicates that cloture — the step that closes debate on the motion to proceed — on the Digital Asset Market Clarity Act, H.R. 3633, will ripen on Tuesday 15 September at 2:15 p.m. Washington time. The text and Senator Cynthia Lummis's update also address when protocols that are not truly decentralised should be identifiable in relation to the CFTC, the US authority overseeing derivatives and many commodity markets, and the Bank Secrecy Act, the body of US rules on traceability and anti-money-laundering controls.

Europe regulates the CASP and its operation in the single market; in the United States the text is still before Congress. For someone using these services, the question remains the same on both sides of the Atlantic: does decentralisation truly distribute power and responsibility, or does it describe only the technical architecture?

A diagram for reading regulated trust



Editorial diagram: the requirements do not eliminate risk, but make the service easier to understand and challenge.

The diagram does not confirm that every authorised operator is sound or that every customer is protected from loss. It shows where the rule tries to make the steps identifiable: who enters the market, with what resources, how they treat funds and information, what they declare, and who can be called to account.

8. Markets — energy enters the cost of capital

The week's signal is not an isolated price. The IEA, the International Energy Agency, an intergovernmental organisation that analyses energy markets, production, consumption, prices and security of supply, reports that global oil production fell by 1.6 million barrels a day in August, to 100.1 million, with more than 10 million barrels a day of Gulf production still offline because of security risks. The average North Sea Dated price rose by $7.61 a barrel in August, to $91, before reaching $113.48 on 9 September. This is the threshold that makes the chain concrete: lower supply and more fragile routes → crude above $100 → higher energy, transport and production costs → pressure on inflation, rates and capital.

US data show the point of contact with the real economy, but do not establish a simple causal link. The August PPI rose 0.4% for the month and 5.4% for the year; final goods rose 1.1% for the month. The CPI rose 0.4% for the month and 3.4% for the year, while the energy index recorded +16.3% over twelve months. These readings describe a period wider than the shock of the final days: they do not therefore prove that the latest crude movement alone had already produced those figures. They do, however, show upstream and consumer pressure becoming visible together again.

In Europe the ECB has already taken a decision: on 10 September it raised its three key rates by 25 basis points, to 2.50% for the deposit facility, 2.65% for main refinancing operations and 2.90% for marginal lending from 16 September. The ECB connects renewed inflationary pressures to the Middle East conflict and forecasts average inflation of 3.0% in 2026, 2.5% in 2027 and 2.1% in 2028; it also makes clear that it is not committing to a predetermined path. At the closing date, the Fed has not yet taken its next decision: we therefore do not turn market expectations into a rise already adopted.

For households and businesses, the pass-through of higher costs is neither automatic nor the same for everyone. It can arrive through bills, fuel, transport, production costs, mortgages, credit and returns demanded on investments. For AI and digital infrastructure the problem is double: *data centres and networks require large amounts of energy and capital. When both become more expensive, the minimum return needed to justify a project changes.*

> ⚠️ **To watch — From the news to the instalment**
>
> Oil, inflation and rates do not pass through at one speed or to the same extent. The verified fact is the simultaneous return of energy and monetary pressure; the next question is how businesses, banks and households will distribute the cost among margins, prices, credit and deferred investment.

9. AI — speed has an economic cost

The debate on pacing — the rate at which the most advanced AI models are developed and deployed — is not only about safety in the abstract. In his essay of 12 September, Dario Amodei proposes advancing models at a pace that leaves time for safeguards, alignment — checks on model behaviour against declared objectives — and third-party controls; he does not call for training or research to stop. His proposal includes external evaluators with ongoing access, coordination between companies and, eventually, global coordination. This is a proposal by the author and Anthropic for the practices the company says it intends to adopt, not a rule already binding on the entire sector.

The economic cost of that choice is concrete even before it becomes law. Longer release times, audits, safety measures, dedicated staff and more testing can shift revenue, increase costs and change the use of data centres already financed. The opposite effect is possible: more credible controls may reduce the risk of costly incidents, regulatory blocks or loss of trust. For an investor, therefore, the question is not only how quickly a model grows, but what speed of deployment can be sustained without moving risks and costs outside the income statement.

We do not use a single stock-market session as proof. In the same period, the energy shock and rate expectations affect technology stocks alongside the AI debate. The correct formulation is more restrained: the possibility of technical, regulatory or voluntary limits on deployment enters the financial variables to be assessed; it has not been shown to explain a market movement on its own.

10. Technology geopolitics — safety or containmen

In Amodei's text, safety and strategic competition are explicitly intertwined. The plan proposes capability-based evaluations and limits, but links the possibility of slowing down in democratic jurisdictions to maintaining an advantage over projects associated with authoritarian regimes; it also identifies controls on advanced chips, compute, model weights and distillation techniques — the systematic extraction of capabilities

from a model through its responses. This is the author's position, not neutral proof that every restriction is necessary or proportionate.

Here the Radar question opens: when does controlling access to chips, compute, weights or distillation techniques reduce a concrete risk, and when does it chiefly protect a strategic advantage? The two motives can coexist, but are not interchangeable. Calling both "safety" without distinguishing interests, evidence and parties would make the debate less transparent, not safer.

11. Italy observatory

Among the primary sources verified this week, no separate Italian development emerges that is material enough to change the picture; the concrete development remains the MiCA implementation already described. This is a review limited to official sources relevant to the issue's themes, not an assertion that the Italian system is standing still.

Final Radar reading

MiCA makes visible a cost that in crypto finance was often left in the background: capital, insurance, custody, people and procedures needed to make an intermediary identifiable and accountable. For someone with a few euros in an app, a family using a wallet or a small business receiving a payment, the difference is not abstract: being able to recognise with whom one has a relationship and which protections actually exist. DeFi reminds us that this question does not disappear when software is distributed: it must be followed through protocol, governance, bridges, keys, interfaces and automation.

The week expands the same lesson. Energy shows the physical cost of the system; rates, the financial cost; AI pacing, the cost of speed and safety; geopolitics, the risk that limits and rules also become instruments of strategic advantage. Behind each of these steps is a question concerning people and organisations: who finances control, who sets the thresholds, who absorbs errors, and who remains responsible when the system accelerates?

For this reason, the signal to watch is not only how many MiCA authorisations will be issued, how far oil will rise or how quickly models will advance. It is whether the costs of trust, energy and safety will be made understandable, distributed in a verifiable way and discussed before they become merely a price already passed on to citizens, businesses and markets.

Primary sources and method

- Regulation (EU) 2023/1114 — MiCA, particularly Articles 2, 59, 66, 67, 70, 75 and 81 and Annex IV.
- ESMA — MiCA page and central register, accessed 14 September 2026.
- ESMA — Article 59, authorisation.
- ESMA — Article 67, prudential requirements.
- ESMA — Article 70, custody of funds and crypto-assets.
- ESMA Q&A 2486 — interest on customer funds, Commission reply of 18 February 2026.
- ESMA — Article 81, advice and portfolio management.
- Bank of Italy — entities operating in crypto-assets under MiCAR, including its communication of 30 June 2026.
- Consob — first CASP authorisation for CheckSig, 7 May 2026.
- SideSwap — post-mortem of the 6 September Liquid incident and update of 10–11 September. Attributions concerning the sequence and responsibility are presented as SideSwap's statements.
- U.S. Senate Daily Press — H.R. 3633, procedural status accessed 14 September 2026.
- Senator Cynthia Lummis — update on the text, 10 September 2026.
- IEA — Oil Market Report, September 2026.
- BLS — Producer Price Index, August 2026.
- BLS — Consumer Price Index, August 2026.
- ECB — monetary policy decisions, 10 September 2026.
- Dario Amodei — We Must Pace the Frontier, the author's proposal of 12 September 2026.
- Anthropic — Frontier Safety Roadmap, for the context of the initiatives declared by the company.

© 2026 Barbara Gattobigio · Gruppo Radar

Comprendere oggi. Costruire domani · by effettoantropico.life

All rights reserved on original content. Free access does not authorize reproduction or republication without consent, except as permitted by law. Third-party materials remain the property of their respective owners. To share this issue, use the link to the article.