Domitille COSSON – LDIS

Decentralization, Smart Contracts, and Transaction Privacy: Europe at the Crossroads of Blockchain Regulation and Digital Capitalism.

How can regulatory governance distort blockchain's architecture and undermine its intended technological function?

Blockchain technology has emerged over the past decade as a foundational innovation in digital infrastructure. Initially envisioned as a decentralized alternative to centralized financial and informational systems, blockchain promised transparency, individual sovereignty, and privacy protection in an era increasingly marked by surveillance and data extraction. Yet this emancipatory promise now faces a profound paradox: while blockchain seeks to decentralize control, it is increasingly absorbed into institutional frameworks of regulation, compliance, and oversight.

This thesis also integrates insights from crypto lobbying organizations that are in direct and ongoing dialogue with European regulators—providing a unique vantage point on the question of whether governance is fundamentally altering the nature of blockchain. Groups such as the European Crypto Initiative (EUCI) are in close contact with institutions in Brussels, actively contributing to the regulatory process through technical consultations, working groups, and structured feedback loops. Similarly, national institutions like the *Banque de France* and the *Autorité des Marchés Financiers* (AMF) are engaged in shaping the legal frameworks that will define the operational contours of crypto activity in Europe.

This dynamic is notably different from the United States, where crypto lobbying tends to be more politicized and adversarial. In the European context, lobbying is predominantly technical grounded in legal precision, infrastructure design, and interoperability standards rather than partisan conflict. This shift signals a maturing of the ecosystem: whereas the early crypto movement was driven by cyberpunk ideals—deeply skeptical of governance and state involvement—the current wave of industry actors is actively participating in regulatory discourse. Their aim is not to reject governance altogether, but to shape it in a way that preserves decentralization, innovation, and legal clarity.

By tracing this evolution, the thesis argues that governance is not inherently opposed to blockchain principles—but that it must be carefully designed to avoid reproducing centralization or undermining trust. The presence of technically competent lobbying, in direct conversation with regulators, provides an essential testbed for understanding how governance can be constructed to accommodate innovation without hollowing out the values that made blockchain transformative in the first place.[1]

This thesis situates itself at the intersection of technological promise and legal constraint. It draws on institutional texts, academic works and comparative legal analysis to examine the following central tension: how can governance be structured to protect legitimate public interests—financial stability, user protection, prevention of crime—without dismantling the core values of decentralization, privacy, and

[1] William O'Rorke, Interview on MiCA and French Regulatory Relations, YouTube – Video_Unhosted with Claire Balva, 2025.

programmability that define blockchain systems? **How can regulatory governance distort blockchain's architecture and undermine its intended technological function?**

First, we will explores the institutional foundations of European regulation. It shows how agencies such as the European Banking Authority and the European Central Bank have sought to protect the euro, prevent systemic financial abuse, and impose transparency standards on crypto-asset service providers. These regulatory efforts, rooted in traditional legal logic, often clash with blockchain's decentralized design. While they aim to address legitimate risks—such as fraud, consumer protection, and money laundering—they frequently impose a hierarchical model of legal accountability that is structurally incompatible with decentralized networks [2]. This section also draws on the work of Shoshana Zuboff, whose analysis of surveillance capitalism underscores the growing asymmetry of power between users and data collectors.[3] Blockchain, in this context, emerges as a counter-architecture—designed to redistribute control and restore agency in a data-driven society.

Then, we will work on the broadens the analysis by examining the unintended effects of regulation on the design of blockchain systems themselves. Focusing on MiCA II [4] and its treatment of DeFi, stablecoins, and pseudonymous systems, this section draws on comparative legal analysis between the European Union, the United States, and China. It argues that the EU's claim to technological sovereignty risks backfiring: instead of fostering innovation, the rigidity of MiCA II may trigger capital flight[5], accelerate brain drain, and concentrate market power in the hands of a few actors capable of absorbing the regulatory burden [6]. This part also integrates the reflections of Primavera De Filippi and Aaron Wright, who describe blockchain as a new form of governance where rules are enforced by code rather than institutions. While this model opens new horizons for automated and transparent regulation, it also raises complex questions about legitimacy, liability, and fairness. [7]

---

[2] EBA reports 2019–2021

[3] Shoshana Zuboff, The Age of Surveillance Capitalism, Harvard Business School Press, 2019, Chapter 3: The Discovery of Behavioral Surplus, pp. 93–136.
How Google initiated the extraction of behavioral data, turning users into a source of profit: "*You are not the customer; you are the raw material*."

[4] European Commission, MiCA II, 2024 – Licensing and whitepaper obligations for CASPs. Found in Title V – Conditions for the provision of crypto-asset services by crypto-asset service providers, particularly: Article 59: "*Obligation to obtain authorisation*"; Article 62: "*Obligations related to white paper*s"; Article 66: "*Record-keeping and transparency obligations*"

[5] Ariane Ollier-Malaterre and Shuang Wang, Blockchain in Authoritarian Contexts, 2022, Chapter 2: Blockchain in China's Rural Control Systems, pp. 65–98.

[6] EU Crypto Initiative (EUCI), Interview with Co-founder, 2025

[7] Primavera De Filippi and Aaron Wright, The Rule of Code: Blockchain and the Law, Harvard University Press, 2018, Chapter 4: Code and Governance, pp. 89–132.

And in the last Part we will answer about the proposes architectural and legal alternatives that seek to reconcile the need for oversight with blockchain's core principles. Building on the European Data Protection Board's 2025 Guidelines of preventive governance rooted in cryptographic tools, proportionality, and protocol-native enforcement. This includes technologies such as zero-knowledge proofs (ZKPs), pseudonymous digital identities, and blockchain-aware public enforcement bodies capable of detecting abuse without dismantling privacy. [8] Rather than treating regulation and innovation as opposites, this section argues for a synthesis in which legal protections are embedded in code—preserving blockchain's promise while ensuring legal compliance.[9]

At a moment when blockchain stands at a crossroads—caught between its radical potential and the pressure of institutional normalization—this thesis argues for a new regulatory posture. One that does not frame governance as an obstacle to innovation, but rather as an opportunity to rethink digital sovereignty in terms that are both legally robust and technologically coherent. [10]

Ultimately, it raises a deeper question, that we will answer at the end of this thesis: could the very architecture of blockchain one day replace traditional forms of governance altogether? If regulation continues to ignore the unique features of decentralized systems, it may not only fail to protect the public—it may destroy the technological alternatives we need most. In that case, the challenge is not only to govern blockchain, but to learn from it how governance itself can evolve.

The thesis constitutes a literature review based on key institutional and academic texts that define the regulatory environment of blockchain in Europe. It draws primarily on the 2025 Guidelines of the European Data Protection Board (EDPB)[11], the legislative proposal final for MiCA, and reports from the European Banking Authority (EBA), which advised and shaped the risk-based approach underlying MiCA II. These documents provide both the normative foundation and the technical benchmarks used throughout this section to assess whether blockchain governance can be aligned with European legal values and innovation principles.[12]

Part I. The Essential Role of Governance in Digital Capitalism to Address Cryptocurrency Sector Risks

[8] European Data Protection Board, "Guidelines 02/2025 on processing of personal data through blockchain technologies," April 2025.
[9] Ministère de l'Intelligence Artificielle, Clara Chappaz, Paris Blockchain Week Speech, 2025.
[10] William Helle, "*Web3 Identity and Surveillance Risks*," CryptoScope Journal, Volume 3, Issue 1, February 2025, pp. 24–29.
[11] European Data Protection Board, Guidelines on pseudonymisation and blockchain, 2025.
[12] European Commission, Proposal for a Regulation on Markets in Crypto-assets (MiCA), COM(2020)593 final.

In response to these tensions, regulation has emerged as a natural tool to introduce accountability into blockchain environments. Frameworks such as MiCA was designed to prevent systemic abuse, stabilize markets, and ensure that crypto-assets are not used for fraud, terrorism, or capital flight. From a legal theory perspective, this is not only legitimate—it is necessary. [13] As the EBA reports underline, unchecked anonymity can create regulatory blind spots and enable high-impact criminal behaviors. [14]

The promise of blockchain technology lies in its architecture: a decentralized, transparent, and tamper-proof infrastructure that can eliminate the need for intermediaries and empower individuals globally. However, as blockchain applications—especially cryptocurrencies—have scaled at unprecedented speed, they have also unveiled a range of systemic vulnerabilities. These include widespread fraud, regulatory evasion, data opacity, and criminal exploitation. While decentralization was designed to minimize centralized abuse, it has also inadvertently enabled a regulatory vacuum. Governance—understood both as institutional regulation and protocol-level rule enforcement—is no longer optional. It is an essential safeguard for the ecosystem's credibility, scalability, and survival in democratic societies.[15]

The European Union stands at the forefront of this transformation. Legislative instruments such as MiCA, AMLR, and GDPR reflect an emerging framework where risk mitigation, privacy protection, and legal accountability are intended to coexist. However, as this section explores, governance must be nuanced, technologically literate, and privacy-preserving to avoid undermining blockchain's foundational benefits.

1.1. Surveillance Capitalism and the Birth of Blockchain Resistance

Shoshana Zuboff theorizes the rise of a new and insidious economic order in which human experience itself becomes raw material for commercial exploitation. Surveillance capitalism, as she defines it, is not merely a business model based on advertising or data collection—it is a new form of economic domination built on the systematic extraction, commodification, and manipulation of behavioral data. Through practices pioneered by technology giants such as Google, Meta (formerly Facebook), and Amazon, human actions—search queries, geolocation, biometric information, social interactions—are converted into data flows which are then analyzed, packaged, and monetized in behavioral futures

[13] European Commission, MiCA II, 2024 – Licensing and whitepaper obligations for CASPs. Found in Title V – Conditions for the provision of crypto-asset services by crypto-asset service providers, particularly: Article 59: "*Obligation to obtain authorisation*"; Article 62: "*Obligations related to white papers";* Article 66: "*Record-keeping and transparency obligations*"
[14] European Data Protection Board, Guidelines on pseudonymisation and blockchain, 2025.
[15] Primavera De Filippi and Aaron Wright, The Rule of Code: Blockchain and the Law, Harvard University Press, 2018, Chapter 4: Code and Governance, pp. 89–132.

markets. Zuboff insists that this model operates outside the traditional boundaries of market capitalism and legal constraint. It functions through **"**unilateral surveillance operations**"**, in which users are not informed participants in a digital transaction, but "human natural resources**"** to be tracked, predicted, and nudged. The danger, according to Zuboff, is not only the erosion of privacy, but the construction of behavioral surplus economies in which human autonomy is replaced by systems of algorithmic governance, calibrated to preempt choice and reshape action.[16]

In this context, blockchain technology emerges as a powerful counter-narrative. While it was not invented as an explicit response to surveillance capitalism, its architecture and ideological foundations make it one of the most radical alternatives to the extractive logic Zuboff critiques. Blockchain redistributes trust away from centralized data collectors and toward decentralized consensus. Instead of building platforms that accumulate data behind proprietary walls, blockchain allows participants to interact in peer-to-peer environments where data control is either pseudonymous or entirely self-sovereign. In particular, blockchain's emphasis on immutability, transparency, and pseudonymity represents a structural inversion of surveillance capitalism's core mechanisms. Whereas surveillance platforms function by harvesting and centralizing vast volumes of behavioral data, blockchain systems generally aim to minimize unnecessary data collection and expose all protocol logic to public scrutiny. Users interacting on-chain typically do so under pseudonyms, and may retain custody of their private keys without yielding biometric or identity-linked information. Transactions are verified by consensus, not surveillance.[17]

From my perspective, this structural contrast is not incidental—it constitutes one of the strongest arguments in favor of blockchain's relevance in a digital environment increasingly shaped by invasive monitoring and opaque decision-making systems. Blockchain reclaims a space where data can be sovereign, where rules are open-source, and where participation does not require surrendering one's digital self.

That said, Zuboff's warnings remain deeply relevant even within blockchain environments. The risk, as she points out, is not just the centralization of data, but the normalization of asymmetry—a world in which one party sees everything, predicts everything, and governs silently. If blockchain protocols are not carefully designed, and if emerging regulations force identifiability, traceability, and surveillance back into the system, then the original promise of decentralization could collapse into a new form of

[16] Shoshana Zuboff, The Age of Surveillance Capitalism, Harvard Business School Press, 2019, Chapter 3: The Discovery of Behavioral Surplus, pp. 93–136.
How Google initiated the extraction of behavioral data, turning users into a source of profit: "*You are not the customer; you are the raw material."*
[17] William Helle, "*Web3 Identity and Surveillance Risks,"* CryptoScope Journal, Volume 3, Issue 1, February 2025, pp. 24–29.

digital control. For instance, requiring all wallets to be linked to off-chain identities, or integrating blockchain into state-level surveillance programs—as already observed in China—could turn blockchain into a new vector of behavioral regulation.[18] This is the reason why I believe the blockchain community must remain vigilant. The ideological foundation of blockchain, especially in its early iterations like Bitcoin, was rooted in skepticism toward centralized institutions, surveillance regimes, and monetary manipulation. In that sense, blockchain is not merely a neutral infrastructure—it is an architectural expression of resistance. Its survival as such depends not only on code, but on the legal, political, and cultural frameworks in which it evolves.

Zuboff's insights force us to ask hard questions: can blockchain maintain its integrity in an environment dominated by surveillance incentives? Will privacy-enhancing technologies like zero-knowledge proofs or confidential transactions be supported by legal frameworks, or banned under the suspicion of criminality? And most importantly: can we build a future where technological innovation protects human dignity, rather than eroding it under the weight of predictive monetization?

These are not hypothetical concerns. In the name of combating illicit finance, some governments propose blanket bans on privacy coins or require full KYC verification for even non-custodial wallets. Such measures, while well-intentioned, risk collapsing the distinction between surveillance for safety and surveillance as control. In doing so, they undermine what Zuboff identifies as one of the core needs of the digital citizen: the right to sanctuary—the ability to think, act, and transact without being constantly watched.[19]

In conclusion, blockchain offers more than an innovation in database architecture—it offers a vision of a different digital world, one that resists the commodification of identity and the automation of influence. This vision must be protected not only through code, but through legal resistance, institutional literacy, and the preservation of privacy as a public good.

1.2. Blockchain as a New Form of Governance - Surveillance Capitalism and the Birth of Blockchain Resistance

[18] Shoshana Zuboff, The Age of Surveillance Capitalism, Harvard Business School Press, 2019, Chapter 9: Rendition from the Depths, pp. 221–266.

[19] Shoshana Zuboff, The Age of Surveillance Capitalism, Harvard Business School Press, 2019, Chapter 9: Rendition from the Depths, pp. 221–266.
Zuboff describes how platforms capture intimate aspects of human life through ubiquitous digital infrastructures—relevant for illustrating Web3 risks in the absence of ethical governance.

Without careful thought, the 'rule of code' could become as arbitrary and exclusionary as the flawed institutions it seeks to replace. But with the right principles, it could also redefine what it means to govern in the digital age.[20]

The challenge is not only technical, but philosophical: how do we build systems that are both automated and just, decentralized and accountable, immutable and adaptable?
Ultimately, the future of blockchain governance depends on how well we can balance the precision and efficiency of code with the ethical complexity and flexibility of human legal systems. Where law and code interact not as substitutes, but as complements. Legal systems must adapt to oversee these new digital spaces, but without stripping them of the innovations that make them valuable.
A nuanced regulatory approach should not simply transpose existing legal categories onto blockchain systems. Instead, it should aim to understand how enforcement works natively in code, and how concepts like due process, human dignity, or proportionality can be embedded in technical architectures.[21]

In my view, the regulatory community, including initiatives like MiCA, must confront this duality head-on. Blockchain can serve as a powerful tool for democratizing access and enforcing accountability through transparency, but it can also entrench new inequalities if the architecture of governance is opaque, inaccessible, or captured by a few. This concern becomes even more pressing in the context of decentralized autonomous organizations (DAOs), where collective decision-making is encoded into smart contract logic. While DAOs promise participatory and transparent governance, they also concentrate power in those who write and maintain the underlying code, or who hold governance tokens in large quantities.
Moreover, code-driven governance often lacks the procedural safeguards that legal systems have developed over centuries. There is no room for exceptions, appeals, or proportionality unless such mechanisms are explicitly coded into the protocol—an often complex and imperfect task.
This raises difficult questions about responsibility: who is liable when a smart contract leads to harm? The developer? The platform? The users who triggered it?

[20] Primavera De Filippi and Aaron Wright, Blockchain and the Law: The Rule of Code, Harvard University Press, 2018, Chapter 6: A Lex Cryptographia, pp. 210–245. Source of the sections discussing algorithmic sovereignty and the tension between state authority and decentralized self-regulation.
[21] Primavera De Filippi and Aaron Wright, Blockchain and the Law: The Rule of Code, Harvard University Press, 2018, Chapter 6: A Lex Cryptographia, pp. 210–245. Source of the sections discussing algorithmic sovereignty and the tension between state authority and decentralized self-regulation.

When governance is embedded in code, new forms of opacity arise. Unlike legal language, which is subject to interpretation, debate, and reform, smart contracts operate deterministically. If the code is flawed, incomplete, or biased, its consequences unfold automatically and sometimes irreversibly.[22]
However, De Filippi and Wright also highlight the deep tensions this model introduces.
The appeal of this model lies in its speed, efficiency, and resistance to manipulation. It reduces costs, eliminates intermediaries, and allows individuals to transact and cooperate without needing to rely on trust in a central authority. This is especially attractive in contexts where legal institutions are slow, inaccessible, or unequally applied.
Smart contracts, in this context, are more than just pieces of self-executing code. They are governance tools that define the conditions of interaction, enforce outcomes automatically, and do so with minimal need for third-party adjudication.[23]

They argue that blockchain enables a new legal architecture—one in which rules are not enforced by courts, regulators, or institutions, but by code itself. This shift from legal enforcement to technological enforcement, sometimes referred to as 'regulation by design', represents a fundamental reconfiguration of governance.
Proposed solutions include off-chain data storage combined with hashed references on-chain, or privacy-enhancing technologies like zero-knowledge proofs. These methods aim to reconcile the promise of blockchain with the requirements of legal erasure, purpose limitation, and accountability.[24]

1.3. Structural Governance Failures: Fraud and Money Laundering in Crypto Markets

Since 2021, cryptocurrency exchanges have paid record-breaking penalties for failures in AML (Anti-Money Laundering) and KYC (Know Your Customer) procedures. KuCoin, BitMEX, Binance, and FTX—each managing billions in daily volume—have been implicated in facilitating illicit financial flows, including from darknet markets and ransomware attacks. These platforms often allowed users to register with minimal identity verification, leveraging blockchain's pseudonymity to circumvent financial surveillance mechanisms. [25]

The EU's forthcoming AMLR (Anti-Money Laundering Regulation) directly responds to this threat by banning anonymous crypto accounts by 2027, and extending due diligence requirements to all crypto-

[22] Clara Chappaz, Ministry of Digital Affairs, Speech on AI and Data Governance, Paris Blockchain Week, France, 2025.
[23] Primavera De Filippi and Aaron Wright, The Rule of Code: Blockchain and the Law, Harvard University Press, 2018, Chapter 4: Code and Governance, pp. 89–132.
[24] Primavera De Filippi and Aaron Wright, Blockchain and the Law: The Rule of Code, Harvard University Press, 2018, Chapter 6: A Lex Cryptographia, pp. 210–245..
[25] Clara Chappaz, Ministry of Digital Affairs, Speech on AI and Data Governance, Paris Blockchain Week, France, 2025.

asset service providers (CASPs). This policy shift reflects a tension between financial inclusion, privacy, and national security. While regulators seek to eliminate blind spots in financial monitoring, overregulation risks pushing users toward unregulated or offshore alternatives—fragmenting the very oversight mechanisms the regulation intends to strengthen.[26]

This dynamic is particularly visible in France, where in late 2024, four individuals were indicted for laundering proceeds from narcotics trafficking via crypto wallets and mixers. [27] Transparency Gaps and Investor Vulnerability. Despite their appeal, centralized exchanges often operate with opaque custodial models, where client funds are pooled into shared wallets, with no segregation or explicit insurance. Unlike traditional finance, where bank deposits and brokerage assets are protected by frameworks such as the EU's Deposit Guarantee Scheme, retail crypto investors bear full liability in the event of insolvency. The collapse of FTX in 2022 revealed how easily billions in customer deposits could vanish when basic governance mechanisms—segregated accounts, public audits, and internal controls—were ignored. In academic and legal circles, there is growing advocacy for on-chain proof-of-reserves, real-time audit trails, and DAO-based exchange governance models as more resilient alternatives to opaque custodianship. Governance, in this case, becomes not just a question of state regulation but of protocol-level accountability, rooted in cryptographic assurances. [28]

1.4. Promotion, Misinformation, and Market Manipulation

The speculative dynamics of the crypto market have created fertile ground for influence-based manipulation, particularly through celebrity endorsements that often bypass regulatory oversight. This phenomenon reveals a structural paradox at the heart of decentralized technologies: although blockchain protocols are trustless by design, the narratives that shape their perceived legitimacy and value are highly centralized. In an environment where attention is the most valuable asset, individuals with massive reach—especially on platforms like Instagram, TikTok, or Twitter—can have disproportionate impact on market behavior, often without being subject to the same standards of disclosure or liability that apply in traditional finance. One of the most illustrative cases is that of K.Kardashian, who in 2022 was fined $1.26 million by the United States Securities and Exchange Commission (SEC) for promoting EthereumMax without properly disclosing that she had been paid for the endorsement. The case was emblematic not only because of her celebrity status, but because it exposed the ease with which a speculative asset could be propelled into the spotlight based solely on social influence, regardless of its

[26] William Helle, "*Web3 Identity and Surveillance Risks*," CryptoScope Journal, Volume 3, Issue 1, February 2025, pp. 24–29
[27] Le Parisien, "*Crypto: Enlèvements et agressions ciblent les détenteurs de portefeuilles publics*," Le Parisien, 15 January 2025, p. 3.
[28] William Helle, "*Web3 Identity and Surveillance Risks*," CryptoScope Journal, Volume 3, Issue 1, February 2025, pp. 24–29

technical merit or financial legitimacy. The token in question lacked any intrinsic utility, yet its price surged briefly following the endorsement—only to collapse after retail investors, many of whom were inexperienced, entered the market based on what they perceived as a credible recommendation. [29]

A similar situation has unfolded in Europe, one of the world's most-followed content creators. Lame has come under scrutiny for endorsing crypto-related projects in ways that, while subtle, may not meet the transparency standards expected under emerging EU advertising and financial promotion rules. As regulators struggle to catch up with the speed of social media cycles, the lack of clear disclosure frameworks for influencers promoting crypto assets poses a serious risk to consumer protection, especially for younger, tech-savvy audiences who may lack the financial literacy to discern sponsored content from genuine enthusiasm.

These cases underscore a deeper asymmetry in the so-called decentralized ecosystem. While blockchains operate without centralized control, the attention economy that surrounds them is anything but decentralized. Access to visibility, market narratives, and credibility is concentrated in a handful of figures—be they influencers, venture capitalists, or founders with large online followings. This creates a situation in which trustless systems are embedded in trust-based informational hierarchies, where signals of value are generated less by code than by visibility.

Such asymmetries give rise to coordinated disinformation risks. Unsophisticated investors, often entering the market for the first time, are vulnerable to psychological anchoring, social proof effects, and hype cycles that resemble those of traditional pump-and-dump schemes—albeit with a digital facelift. The decentralized nature of crypto platforms makes it difficult to track accountability across borders, and even more difficult to intervene in real time.

This is where governance, both regulatory and communal, becomes essential. Regulatory bodies must establish and enforce clear disclosure obligations for influencers, content creators, and platforms promoting financial products, especially in jurisdictions where crypto-assets are not yet considered fully regulated securities. At the same time, the crypto community itself must develop internal mechanisms of legitimacy—such as verified auditor endorsements, open disclosures of paid partnerships, and DAO-based moderation of promotional content—to mitigate the risks of narrative manipulation. [30]

Ultimately, this tension illustrates one of the core contradictions of Web3: technical decentralization does not automatically translate into informational or social decentralization. Without robust and

[29] EU Crypto Initiative (EUCI), AML Handbook, 2025

[30] Primavera De Filippi and Aaron Wright, Blockchain and the Law: The Rule of Code, Harvard University Press, 2018, Chapter 6: A Lex Cryptographia, pp. 210–245. Source of the sections discussing algorithmic sovereignty and the tension between state authority and decentralized self-regulation.

adaptive governance structures, both formal and informal, the space risks becoming susceptible not just to market volatility but to coordinated exploitation through influence. Protecting the long-term integrity of the crypto ecosystem will therefore require governance models that address not only financial and legal compliance, but also the cultural and communicational structures through which value is constructed and perceived.

Across the globe, the governance of smart contracts reflects radically divergent political philosophies. In China, smart contracts are increasingly embedded within a state-controlled digital infrastructure, where their programmability serves not individual autonomy but state objectives—whether in finance, public administration, or surveillance. As documented in Red Mirror, these tools are used to enforce behavioral norms and economic policy through code, transforming blockchain into a mechanism of compliance rather than liberation. By contrast, in the United States, governance remains highly fragmented, with overlapping state and federal frameworks often generating regulatory uncertainty. This disjointed environment allows for innovation but also fuels misinformation, regulatory arbitrage, and inconsistent enforcement, particularly in decentralized finance (DeFi).

The European approach sits somewhere in between: it aspires to institutionalize blockchain governance through structured legislation (e.g., MiCA) while preserving a degree of openness. However, the global governance of smart contracts reveals that decentralization is not just a technical challenge—it is a geopolitical one. The ideals of trustless interaction and autonomous execution are continually undermined by the surveillance logic in authoritarian regimes and the informational asymmetries in liberal democracies, where misinformation and opaque lobbying can distort policy design. As a result, there is no unified global path to decentralized governance. Each region encodes its own vision of control, risk, and legitimacy into the technical and legal structures that govern smart contracts. Understanding these divergences is essential for designing governance frameworks that neither overreach nor surrender to market chaos.[31]

1.5. Cybercrime and State Exploitation of Blockchain Infrastructure

North Korean state-sponsored cyber groups—particularly the Lazarus Group—have increasingly leveraged the speed, pseudonymity, and global reach of blockchain infrastructures to launder illicit funds derived from decentralized finance (DeFi) exploits, ransomware campaigns, and large-scale cyberattacks. These activities represent one of the clearest illustrations of how blockchain technology, while neutral in design, can be exploited by hostile state actors operating outside traditional financial and legal boundaries.

[31] William Helle, "*Web3 Identity and Surveillance Risks*," CryptoScope Journal, Volume 3, Issue 1, February 2025, pp. 24–29

The Lazarus Group, which has been linked to previous intrusions into SWIFT systems, attacks on major cryptocurrency exchanges, and the WannaCry ransomware campaign, has adapted its strategy to target decentralized protocols. By exploiting vulnerabilities in smart contracts or leveraging social engineering to gain access to DeFi administrative keys, the group has successfully exfiltrated hundreds of millions of dollars worth of assets. Once obtained, these funds are routed through decentralized exchanges (DEXs), coin mixers, and blockchain bridges to obfuscate origin, sever forensic traceability, and convert funds into fiat or privacy coins.

The challenge for regulators and law enforcement is profound. Unlike centralized financial institutions, which are obligated to conduct know-your-customer (KYC) checks and cooperate with suspicious transaction reporting regimes, many DeFi platforms operate without custodians, identifiable administrators, or jurisdictional anchors. This allows malicious actors to move funds across chains and platforms at a velocity and complexity that far exceed the capacities of traditional anti-money laundering (AML) systems.

In response to this escalating threat, the European Union has reinforced its commitment to cyber-resilience and financial integrity through the expansion of its Joint Cybercrime Task Force. The initiative coordinates cybercrime intelligence among member states and Europol, focusing increasingly on the intersection between cyber operations and blockchain-based laundering. Beyond the EU, emerging discussions and meeting with a diplomatic association at the german embassy with Colonel Reiberling and students,—the colonel point to the necessity of a coordinated supranational response. These discussions have coalesced around the idea of creating a "cyber-Schengen" framework: a transnational cyber-governance infrastructure enabling real-time data sharing, forensic collaboration, and traceability across borders without undermining national sovereignty.[32]

This “cyber-Schengen” concept reflects a growing recognition that digital threats no longer respect borders, and that the enforcement capabilities of any single jurisdiction—no matter how technologically advanced—are insufficient to tackle the global architecture of crypto-financed crime. The envisioned framework would facilitate joint operations between national cyber units, support blockchain forensics training, and incentivize private actors, including analytics firms and wallet providers, to collaborate on threat detection. In doing so, it would extend the logic of the Schengen Agreement—freedom of movement with shared security responsibilities—into the digital realm.

However, this ambition comes with delicate trade-offs. The fundamental strength of blockchain lies in its pseudonymity and borderless nature. Any attempt to build traceability infrastructure must be balanced

[32] Minister of Foreign Affairs of Germany, French-German Diplomatic discussion: European Military Power Dialogue, November 2024

against the legitimate privacy interests of law-abiding users, journalists, whistleblowers, and dissidents who rely on these technologies for operational security. Moreover, the centralization of surveillance capabilities in cybercrime units, especially if embedded into blockchain analytics firms or cross-chain monitoring layers, raises questions about proportionality, data protection, and long-term mission creep.

In my view, the critical question is not whether we can build enforcement capabilities that match the sophistication of actors like Lazarus, but whether we can do so without replicating the very control architectures blockchain was designed to avoid. This means building governance frameworks that are not only effective but also structurally accountable—where investigative powers are bound by clear limits, where due process is preserved, and where technological neutrality is not used as a cover for backdoor surveillance.

Ultimately, blockchain presents both a vector and a venue for geopolitical contestation. It enables financial flows that are faster than law and more agile than diplomacy. Confronting this challenge will require a blend of cryptographic forensics, international legal harmonization, and public-private coordination—what one might call a digital equivalent of arms control. Without such efforts, blockchain risks becoming not only a tool of innovation but a battleground for covert statecraft.

1.6. The EDPB's Framework: Governance Without Surveillance

In its 2025 guidelines, the European Data Protection Board (EDPB)[33] addresses in detail the unique data governance challenges raised by blockchain systems. These challenges are primarily structural. On one hand, the immutability of blockchain entries—the very feature that guarantees their reliability—conflicts directly with one of the cornerstones of the General Data Protection Regulation (GDPR): the right to erasure, or "right to be forgotten." Once data is inscribed on a public blockchain, it cannot be altered or deleted without compromising the integrity of the entire network. On the other hand, blockchain networks are often decentralized by design, operating without a central administrator or identifiable data controller. This absence of a clear legal subject makes it particularly difficult to enforce GDPR obligations, which are traditionally centered around the responsibility of an accountable data controller.

Faced with this structural misalignment, the EDPB does not propose banning blockchain systems outright. Instead, it adopts a pragmatic and technically literate position by recommending specific design principles that could allow blockchain technologies to remain compatible with European data protection law. First, the EDPB strongly advises against the direct on-chain storage of any personally identifiable information. Instead, such data should be stored off-chain in encrypted databases, with only

[33] European Data Protection Board, Guidelines on pseudonymisation and blockchain, 2025

cryptographic references—such as hashes or zero-knowledge proofs—committed to the blockchain. This approach preserves the functional advantages of blockchain while ensuring that personal data remains subject to erasure, correction, and access controls off-chain.[34]

Second, the EDPB encourages developers and deploying entities to conduct Data Protection Impact Assessments (DPIAs) before launching any blockchain-based systems that may involve the processing of personal data. These assessments serve as a critical tool to evaluate the potential risks of a project, identify mitigation strategies, and ensure that privacy protections are not treated as an afterthought but as a foundational element of system architecture.

Underlying all these recommendations is the EDPB's broader endorsement of the principle of "privacy by design." Rather than seeing privacy as an external constraint to be added after technical development, the EDPB envisions a model in which privacy is embedded directly into the codebase and architecture of blockchain protocols. In this view, compliance is not something that is retrofitted through legal disclaimers or policy documents—it is something that emerges from the system's very structure.[35]

This protocol-native approach to privacy is particularly promising because it aligns with the logic of decentralization rather than opposing it. It enables blockchain systems to offer transparency and auditability without violating fundamental rights. By advocating for cryptographic accountability over bureaucratic control, the EDPB sets a standard for what technologically coherent and rights-respecting governance can look like in the digital age.[36]

1.7. Debunking Misconceptions: Illicit Use Is Marginal, and Most Investors Are Young and Responsible

Contrary to persistent stereotypes, cryptocurrencies are not the main vehicle for money laundering. According to a 2023 report by the U.S. Treasury Department, traditional finance—including cash and conventional financial institutions—remains the primary channel for laundering illicit funds, accounting for 2% to 5% of global GDP, or an estimated $800 billion to $2 trillion annually. In comparison, only 0.34% of crypto transactions in 2023 were linked to illicit activity, a figure significantly lower than in fiat finance.[37]

[34] European Data Protection Board, Guidelines on pseudonymisation and blockchain, 2025
[35] European Data Protection Board, Guidelines on pseudonymisation and blockchain, 2025
[36] European Data Protection Board, "Guidelines 02/2025 on processing of personal data through blockchain technologies," April 2025.
[37] Journal du Coin, Analyse annuelle de la régulation crypto en France, December 2024, https://journalducoin.com, p. 8–14

Moreover, the investor base in the crypto sector is predominantly young, tech-savvy, and aligned with legitimate innovation. A joint study by KPMG and the Association for the Development of Digital Assets (ADAN) found that 57% of French crypto holders are under 35, and a significant majority actively seek alternatives to traditional financial systems. [38] These profiles indicate a shift toward long-term, innovation-driven engagement, rather than short-term speculation or illicit use.

These findings challenge the often exaggerated narrative of cryptocurrencies as a haven for crime. They call for a more differentiated and data-driven approach to regulation, targeting actual risks without stifling innovation or discouraging participation from young, legitimate investors.

1.8 Institutional Foundations: The Role of EBA and the Eurozone Stability Agenda

The European Banking Authority (EBA) has played a strategic and foundational role in shaping the regulatory architecture that culminated in the Markets in Crypto-Assets Regulation[39]. Long before the proposal was formally adopted, the EBA issued a series of technical advice papers and risk assessments highlighting systemic threats posed by unregulated crypto-assets to financial stability within the eurozone. Among its key concerns were the potential for liquidity mismatches, consumer fraud in the absence of custodial guarantees, and the use of opaque structures to bypass financial safeguards.
The EBA notably stressed the importance of legal segregation of assets—a core tenet of traditional financial regulation—which was conspicuously absent in many early crypto-exchange models. Its policy guidance emphasized the risks of pooled custodianship, insufficient capital buffers, and lack of legal recourse for retail investors in the event of insolvency. In response, MiCA formalized a risk-based regulatory perimeter whose objective was to protect both the euro and EU retail participants from systemic contagion.

A cornerstone of this architecture is MiCA tripartite classification of crypto-assets: asset-referenced tokens (ARTs), e-money tokens (EMTs), and other crypto-assets, including utility tokens. This taxonomy allowed regulators to differentiate between tokens based on their monetary function, systemic risk, and technological opacity. It also enabled a calibrated supervision regime, echoing the EBA's insistence on proportionality and sectoral specificity.
From a governance standpoint, MiCA laid the groundwork for a harmonized EU-wide licensing regime for Crypto-Asset Service Providers (CASPs), setting the stage for future convergence between traditional and crypto-financial oversight. However, some critics argue that the EBA's influence tilted

[38] LinkedIn Live Replay, KPMG & ADAN, "*Panorama 2023 de l'écosystème crypto français*", held on 18 October 2023, accessible via https://www.linkedin.com/company/adan-association.
[39] European Commission, Proposal for a Regulation on Markets in Crypto-assets (MiCA II), 2024.

the balance in favor of systemic risk mitigation at the cost of innovation, especially for small actors operating on non-custodial or decentralized infrastructures.[40]

Legal scholar [41] has been one of the most vocal European academics to address the fundamental incompatibilities between blockchain technologies and the General Data Protection Regulation. Her argument is structural: GDPR assumes a model in which there exists an identifiable data controller, who can be held accountable for compliance. Blockchain, by contrast, is premised on distributed consensus, where no single entity holds authority or control.

This architectural misalignment becomes acute when considering the GDPR's 'right to be forgotten'. Public blockchains, by design, are immutable. Even when personal data is stored in encrypted form, Finck warns that the 'encryption fallacy' offers limited protection. Advances in quantum computing could in future render today's encryption obsolete. This tension underscores a deeper challenge: how can European law evolve to accommodate code-based governance without sacrificing constitutional rights?[42]

Personally, I believe that blockchain—precisely because of its structural characteristics—has the potential to respond to Shoshana Zuboff's concerns about surveillance capitalism. It creates an alternative system of data handling where control is redistributed and transparency is inherent. In contrast to centralized data economies, blockchain offers a path toward user agency and structural resistance to surveillance-based extraction models.

In her book The Age of Surveillance Capitalism, Zuboff describes a new economic order in which personal experiences are mined, commodified, and monetized without consent. Blockchain technology emerged, in part, as a technical and ideological counter-movement to this paradigm. Rather than collecting and monetizing behavioral data, blockchain networks—at least in theory—offer transparency without surveillance, and accountability without centralized control. However, the growing effort to impose traceability obligations risks subverting the very logic of blockchain as a privacy-preserving infrastructure.

In Blockchain and the Law, the authors argue that blockchain introduces a new legal architecture, where smart contracts become automated governance systems. This transformation raises questions of legal legitimacy, responsibility, and enforceability. While blockchain reduces dependency on institutional

[40] European Commission, Proposal for a Regulation on Markets in Crypto-assets (MiCA II), 2024.

[41] Michele Finck, "*Blockchain and the General Data Protection Regulation*," Oxford Internet Institute, 2024 – GDPR–blockchain conflicts (immutability, erasure, responsibility). The existence of the legal Conflicts between Blockchain Architecture and GDPR, pp. 17–24

[42] Michele Finck, "*Blockchain and the General Data Protection Regulation,*" Oxford Internet Institute, 2024 – GDPR–blockchain conflicts (immutability, erasure, responsibility). The existence of the legal Conflicts between Blockchain Architecture and GDPR, pp. 17–24

intermediaries, it also introduces new risks: opacity of code, asymmetries of knowledge, and concentration of influence in protocol design. Their work shows that decentralization alone does not guarantee accountability. [43]

In my view, the most important challenge for regulators like the European Commission is to preserve the emancipatory potential of blockchain—its capacity to offer a rights-respecting alternative to surveillance capitalism—while building systems of governance that do not sacrifice legal protections. This implies finding a balance between innovation, accountability, and structural fairness.[44]
The European Banking Authority (EBA) played a foundational role in the construction of MiCA by advising the European Commission on the risk-based framework necessary to safeguard eurozone stability. Its early reports warned of systemic liquidity risks, consumer vulnerabilities, and the risk of crypto-asset custody without legal segregation. This justified a strict regulatory perimeter to protect the euro and promote transparency among custodians.MiCA implements a tripartite classification of crypto-assets: (1) asset-referenced tokens (ARTs), (2) e-money tokens (EMTs), and (3) utility tokens. This classification was designed to anchor investor protection and differentiate between tokens based on monetary function and technological risk. From a governance standpoint, this tripartite model echoes the EBA's insistence on differentiated supervision: e-money tokens fall under e-money institutions' oversight, ARTs under stricter collateral and redemption conditions, and utility tokens are subject to whitepaper disclosures. The goal is to formalize custody, create licensure regimes, and promote cross-border compliance through regulatory harmonization.

1.9 Regulating the Legal Architecture of Tokenization

The tokenization of assets is often praised as a cornerstone of the next financial revolution—hailed for its potential to democratize finance, streamline asset transfer, and increase liquidity across markets. It is commonly presented as a technological breakthrough, tightly linked to blockchain innovation and decentralization. However, from a legal perspective, tokenization is far from new. Jurists recognize in it an age-old phenomenon: the representation of an asset by a transferable legal instrument. The novelty lies not in the concept itself, but in its technological mediation, which now demands an equally sophisticated and integrated legal response. Tokenization is not merely a matter of code or digital infrastructure—it is a juridical operation that requires recognition, legitimacy, and structuring under the law. Both the act of tokenizing (i.e., the issuance of tokens) and the legal status of the token itself must be supported by a robust legal framework. This includes legal clarity on ownership, transfer, restitution rights, and taxation. Without such a framework, tokenization risks remaining a fragile, ambiguous

[43] Primavera De Filippi and Aaron Wright, Blockchain and the Law: The Rule of Code, Harvard University Press, 2018, Chapter 6: A Lex Cryptographia, pp. 210–245.
[44] European Commission, Proposal for a Regulation on Markets in Crypto-assets (MiCA II), 2024

practice—attractive in theory but legally unstable in practice.The first legal challenge concerns issuance**:** the creation of a token linked to an underlying asset. This act must be recognized and codified to give the token legal standing. In this respect, the MiCA Regulation already represents a substantial step forward—it provides a comprehensive regime for the issuance of asset-referenced tokens (ARTs) and e-money tokens (EMTs), regulating issuers, their obligations, guarantees, and supervisory mechanisms. However, this framework also underscores a structural contradiction with blockchain's ethos of disintermediation. By institutionalizing the role of the issuer as a mandatory legal counterparty, MiCA reintroduces central points of trust—arguably at odds with the decentralized ambitions of crypto-infrastructure. Nonetheless, legal certainty necessitates an identifiable and accountable party to guarantee the delivery, redemption, or equivalence of the underlying asset.[45]

Beyond issuance, tokenization demands a clear and enforceable regime of ownership. Tokens representing real-world assets must be considered autonomous objects of property, capable of being bought, sold, gifted, inherited, or pledged as collateral. In France, the Ordonnance of 15 October 2024 addressed this need by introducing provisions for both self-hosted tokens and those held via third-party service providers. Crucially, the ordinance also includes protections for good-faith acquirers**,** recognizing the inherently negotiable nature of tokens. Given that tokens are designed for rapid circulation with minimal verification, a legal safety net for bona fide purchasers is essential. This aligns with broader legal principles found in negotiable instruments and securities law, adapted here to the blockchain context.[46]

Perhaps the most intricate issue in tokenization arises when a conflict emerges between two claimants—one asserting rights over the token, the other over the underlying asset. This conflict becomes especially delicate when the asset is non-fungible, such as real estate or a work of art. In such cases, the token can function not merely as a promise of redemption, but as a true digital title of ownership. But this raises profound legal questions: Should someone acquiring an artwork or building in the real world be required to verify whether the asset has been tokenized? Would this undermine established legal mechanisms such as property registries or the civil law principle possession vaut titre (from the civil code) These dilemmas highlight the centrality of trust in the issuer and the need for full-reserve custodianship if non-fungible assets are to be credibly tokenized.

International private law further complicates the picture. What happens when the token is issued in a jurisdiction that recognizes tokenization, but the underlying asset is located in one that does not? The legal asymmetry can erode the rights of the token holder. A compelling analogy is found in the case Byers v Samba, where the Saudi legal system's refusal to recognize trusts led to the invalidation of the

[45] Alain Montfort, Interview on Crypto Privacy and Security, BFM Crypto, 2025
[46] Alain Montfort, Interview on Crypto Privacy and Security, BFM Crypto, 2025

trust's claims over Saudi shares. The same legal fragmentation could undermine token holders' rights if courts in the jurisdiction of the underlying asset refuse to acknowledge the legal status of the token. Tokenization, then, does not escape geopolitics: it is entangled in conflict-of-law doctrines and jurisdictional recognition battles.[47]

Another unresolved tension lies in the fiscal treatment of tokenized assets. Should taxation apply to the token itself, or to the underlying asset it represents? If tokens are treated as autonomous digital assets, they may fall under cryptocurrency-specific tax regimes. If, however, they are viewed as mere wrappers for traditional assets, the fiscal logic of the underlying applies. This divergence opens the door to regulatory arbitrage, uncertainty, and potentially abusive structuring. The issue touches on a deeper philosophical question: Can the legal and tax nature of an asset shift simply because of how it is recorded and transferred? Ultimately, there is no viable tokenization without legally robust tokens. Their quality—and by extension, the legitimacy of the tokenized economy—rests not only on cybersecurity or economic fundamentals, but on juridical integrity. That integrity must cover the issuer's credibility, the legal bond between token and asset, and the rules governing conflicts, transfers, and restitution. Without it, tokenization remains legally brittle and economically risky.

In conclusion, tokenization is not merely a technological innovation but a multidimensional legal project**.** Its success depends on resolving complex issues across issuance, ownership, circulation, conflict resolution, private international law, and taxation. Each of these areas constitutes a legal construction site—un chantier juridique—that must be rigorously addressed if Europe is to provide a competitive yet secure framework for tokenized finance. A regulation-first approach, as embodied by MiCA, is a necessary starting point, but not the endpoint. Future regulatory frameworks must evolve to reflect the layered, transnational, and asset-specific challenges posed by the tokenized economy.[48]

To sum up, initial regulatory frameworks emerged primarily to address pressing threats to financial stability and security. Institutions like the European Banking Authority (EBA) and the Financial Action Task Force (FATF) emphasized the need for Anti-Money Laundering (AML) controls to combat illicit finance, terrorism financing, and fraud. These led to strong compliance expectations, with MiCA's earliest applications grounded in EBA recommendations related to the custody of crypto-assets, governance standards, and investor transparency. The goal was to regulate established actors—wallet providers, custodians, and crypto exchanges—who were onboarding millions of users without consistent investor protections. This phase of regulation largely addressed the systemic risks posed by existing players and sought to protect European financial sovereignty. MiCA responded by creating three legal

[47] Alain Montfort, Interview on Crypto Privacy and Security, BFM Crypto, 2025
[48] Clara Chappaz, Ministry of Digital Affairs, Speech on AI and Data Governance, Paris Blockchain Week, France, 2025.

categories of crypto-assets: asset-referenced tokens (ARTs), e-money tokens (EMTs), and other crypto-assets (including utility tokens). This categorization, paired with licensing requirements, whitepaper obligations, and custody rules, provided a structured response to the emerging crypto economy. For the average retail or institutional crypto investor, this phase of regulation was perceived as necessary and even welcomed—it created market certainty and legitimacy for established products

Yet as shown throughout this thesis, if these regulations are not nuanced, they risk conflating use and abuse. A functional blockchain ecosystem does not reject governance—it needs it. But that governance must be proportionate, technologically literate, and rooted in values of transparency, accountability, and respect for individual rights. Regulation should not assume that privacy equals suspicion; it should differentiate between structural safeguards and deliberate obfuscation.

Part II — How Traditional Regulatory Governance Transforms Blockchain: A Double-Edged Sword, analysis from lawyer and tech experts

After reviewing the main European regulatory frameworks—such as MiCA II, the DSA, the DMA, and EDPB guidelines—I conducted a series of interviews with legal experts, lawyers, and professionals in the field of emerging technologies. These conversations provided critical insight into how regulation, while intended to reduce systemic risk and ensure legal certainty, can also substantially alter the development pipeline of crypto projects. According to these practitioners, the current regulatory trajectory could make Europe significantly less attractive and less competitive for innovators seeking to launch blockchain-based ventures.[49]

Several interviewees pointed out that the increasing compliance burden—especially in terms of licensing and legal structure—could lead to the reallocation of strategic and financial resources toward M&A activity, not to expand or scale projects, but simply to survive within the legal environment. For smaller or early-stage crypto initiatives, this means navigating a highly resource-intensive entry point, often necessitating legal engineering just to maintain operational viability. Such constraints not only threaten to stifle grassroots innovation, but also risk triggering a brain drain, as developers and founders seek more agile jurisdictions.[50]

A further paradox arises around the regulation of privacy-preserving technologies, such as private cryptocurrencies. By bringing private money under public scrutiny without offering adequate protective alternatives, regulation may unintentionally introduce new forms of insecurity—both technical and

[49] European Commission, 2023; OECD, 2022
[50] EU Crypto Initiative (EUCI), AML Handbook, 2025 – Anonymous accounts and upcoming AML restrictions

societal. What begins as an effort to combat opacity may, in effect, undermine trust and exacerbate capital and talent flight from the European ecosystem. [51]

In this second part of the thesis, we examine how Phase II of regulatory governance operates at the level of project design itself, targeting the architecture of emerging crypto protocols, including new tokens, stablecoins, and DeFi systems. While well-intentioned, this shift toward upstream regulation poses profound risks for innovation. We will explore how these policies—despite aiming to prevent abuse—may open new fractures between regulation and competitiveness in the digital economy.[52]

2.1 Understanding MiCA II: Legal Structure, Scope, and Objectives

This understanding is grounded first and foremost in the original legislative proposal for MiCA published by the European Commission, which outlines the necessity of a Union-wide framework to regulate the issuance of crypto-assets and the provision of related services. The proposal underscores that all entities engaging in the provision of crypto-asset services—whether through centralized or hybrid systems—must apply for prior authorization from a competent national authority (Article 53), and that all token issuers not falling under exemptions must publish a compliant whitepaper prior to any offering (Article 4). Article 4 specifies that the whitepaper must include a detailed description of the crypto-asset, the issuer, the rights and obligations attached to the token, the underlying technology, and the associated risks. It must be notified to the competent authority and made publicly available before any offering, even if the token is issued for free. This provision, while grounded in transparency and consumer protection, imposes a significant bureaucratic and legal burden on projects that operate outside the traditional corporate structure. MiCA's integrated role within the EU's broader Digital Financial Strategy, alongside the DLT Pilot Regime (Regulation 2022/858), the Digital Operational Resilience Act -DORA, 2022/2554, and the Digital Euro proposal. MiCA's scope is comprehensive, covering the issuance, public offering, and admission to trading of crypto-assets, as well as the supervision and conduct requirements for CASPs. Its foundational aims also include client protection, transparency in whitepaper disclosures, and the prevention of insider dealing and market manipulation in crypto markets. [53]

Notably, MiCA is framed by Recital 22 as flexible toward decentralization, stating that crypto-assets and services provided "fully in a decentralized manner without any intermediary" fall outside its scope. Nevertheless, this clause is conceptually limited. There is a regulatory ambiguity in distinguishing

---

[51] EDPB Guidelines 05/2022; Pieranni, 2021.

[52] ESMA, 2019; European Blockchain Observatory & Forum, 2021

[53] Clara Chappaz, Speech at Paris Blockchain Week, Ministry for Artificial Intelligence, France, 2025

between what constitutes a fully decentralized system and those only partially so. In practice, most DeFi platforms would still be subject to scrutiny under CASP obligations due to their semi-permissioned architectures or reliance on front-end operators. Furthermore, Recital 11 clarifies that NFTs are excluded only when truly non-fungible. Tokenized collections or fractional NFTs are presumed fungible and therefore fall within MiCA's regulatory perimeter.

Finally, MiCA incorporates the principle of "technology neutrality" and the idea of "same activity, same risk, same rules" (Recital 9), yet this principle is not always consistently applied when evaluating the nature of DeFi governance or smart contracts vis-à-vis their centralized counterparts. As outlined in Recital 22 and substantiated in the European Commission's original MiCA proposal, fully decentralized systems are notionally exempt from the regulation. However, the boundaries between partial decentralization and protocol operator intermediation remain vague and legally uncertain. The regulation's formalistic insistence on identifiable issuers and regulated intermediaries consequently risks clashing with the protocol-native ethos of blockchain governance, which is built around anonymity, permissionless contribution, and the absence of a controlling legal person. [54]

This ambiguity has significant consequences. The lack of definitional clarity invites both over-compliance by cautious actors and under-compliance by strategic actors. Moreover, it discourages open-source experimentation, particularly for non-custodial and community-run applications. In parallel, as highlighted in the Blockchain for Europe position paper (2024), delays and legal ambiguity surrounding the licensing of crypto-asset service providers push many developers to either relocate their activity to Malta or Abu Dhabi—jurisdictions offering more agile and risk-adapted regulatory environments—or to remain in the EU in a state of non-compliance, hoping that enforcement will be light or that reforms will emerge. This erosion of regulatory certainty, paired with inconsistent application of technology-neutral principles, undermines both MiCA's credibility and its strategic potential to position the EU as a leader in digital innovation. [55]

2.2 Legal Fiction and Technological Misfit: MiCA's Compliance Burdens

Despite its progressive objectives, MiCA II introduces a model of governance that reproduces institutional hierarchies incompatible with decentralized protocols. The requirement to obtain a CASP license and to submit whitepapers to regulatory vetting presumes that each project is operated by a legally identifiable entity, with physical headquarters, management structures, and liability chains. In

[54] Clara Chappaz, Speech at Paris Blockchain Week, Ministry for Artificial Intelligence, France, 2025

[55] Clara Chappaz, Speech at Paris Blockchain Week, Ministry for Artificial Intelligence, France, 2025

contrast, decentralized protocols are often governed by anonymous communities, operate on open-source infrastructure, and intentionally avoid legal centralization.

MiCA II is triggering a regulatory exodus of crypto developers. Teams based in France, Germany, and Italy—many of whom operate with minimal funding—are relocating to jurisdictions such as Abu Dhabi, Switzerland, and Singapore, where innovation is not penalized by bureaucratic uncertainty. While the EU hoped to become a leader in Web3 regulation, it risks becoming a jurisdiction of exit, where only the wealthiest actors remain: "Small teams can't wait 18 months for a license or pay compliance lawyers €100,000. So they'll either sell to a larger platform or leave the EU entirely."[56]

Worse still, many large platforms——have already adopted a "pay-to-play" strategy: rather than structurally adapting to the regulation, they factor fines into their business model. These actors absorb sanctions without addressing the systemic governance risks that MiCA was designed to prevent. Thus, MiCA II risks entrenching oligopolistic structures: legal certainty for giants, exit for the rest.

This imbalance is further aggravated by what and several legal experts describe as a "pay-to-play loophole" embedded within the MiCA II enforcement model. While the regulation introduces sanctions for unauthorized operations or procedural breaches, these penalties are often set at levels that large actors can easily absorb. Rather than incentivizing full structural compliance—such as building internal compliance frameworks, issuing verified whitepapers, or restructuring custody practices—some platforms treat MiCA-related fines as operational overhead, strategically opting to pay administrative penalties while continuing business as usual.

From a legal-economic standpoint, this creates a system where non-compliance becomes fiscally rational for capitalized actors, and full compliance becomes unattainable for smaller, decentralized teams. More alarmingly, under prevailing interpretations of corporate income tax law in several Member States, such fines may be partially or entirely deductible as business expenses, unless explicitly prohibited by statute. The European Commission[57] warned that the absence of harmonized exclusion rules on the deductibility of regulatory sanctions risks neutralizing their deterrent effect. Unless MiCA II violations are treated as explicitly non-deductible under national fiscal codes, the regulation could

[56] EU Crypto Initiative (EUCI), Interview with Co-founder, 2025

[57] European Commission, MiCA, COM(2020)593 final – Asset-referenced tokens regulation. Covered in Title III – Asset-referenced tokens: Articles 15–36, especially: Article 15: "*Authorisation requirement*"; Article 20: "*White paper obligations*"; Article 28: "*Stabilisation mechanisms"*

paradoxically subsidize misconduct, allowing dominant actors to write off penalties while avoiding systemic changes.[58]

The combined legal and fiscal reality is therefore troubling: MiCA II, despite its promise of harmonization and accountability, may in practice create a bifurcated compliance ecosystem—one in which smaller actors exit, and larger actors externalize compliance through strategic non-compliance and fiscal optimization. This divergence undermines the credibility of the regulation and threatens the long-term legitimacy of European digital financial governance. This dual-track outcome also facilitates mergers and acquisitions, which are increasingly viewed as the only viable survival strategy for smaller crypto firms within the EU M&A activity is likely to accelerate as small and medium-sized companies, unable to shoulder the full burden of compliance, are acquired by larger players with the legal and financial infrastructure to maintain EU licenses. These consolidations, while superficially compliant, tend to centralize power and weaken the ecosystem's diversity and resilience.[59]

Some developers, unwilling to consolidate or relocate, have begun to explore grey-zone operations—choosing to operate pseudonymously, offshore, or in temporary non-compliance. According to ORWL (2025), these scenarios are not hypothetical, but already observable across the EU. Developers are performing risk analyses not just on technical vectors, but on regulatory inertia and enforcement gaps. This form of calculated non-compliance is emerging as a rational adaptation to legal regimes perceived as excessively burdensome or disconnected from operational reality.[60]

MiCA II, as it currently stands, risks reinforcing inequality in regulatory access, favoring compliance-capable incumbents while marginalizing innovation-driven challengers. Unless mechanisms are introduced to distinguish truly decentralized systems from service-based operators, and unless supervisory practices embrace proportionality and dialogue, the EU's ambition to lead in crypto governance may produce the opposite effect: regulatory overreach, legal fragmentation, and the hollowing out of the domestic crypto ecosystem.

2.3 The Legal-Ethical Dilemma of Presumed Illegality and the Criminalization of Privacy

---

[58] European Commission, MiCA, COM(2020)593 final – Asset-referenced tokens regulation. Asset-referenced tokens: Articles 15–36, especially: Article 15: "*Authorisation requirement*"; Article 20: "*White paper obligations*"; Article 28: "*Stabilisation mechanisms*"

[59] EU Crypto Initiative (EUCI), Interview with Co-founder, 2025

[60] ORWL Legal Collective, Legal Opinion on Privacy Technologies and Blockchain Regulation, 2025 – Legal presumption and anonymization under French law. See Section II – Anonymity and Legal Presumption, pp. 9–14

The criminalization of privacy-enhancing technologies within national legal frameworks represents one of the most contentious consequences of the current regulatory trajectory in Europe. Nowhere is this clearer than in the French anti-narcotics legislation, which applies a blanket presumption that the use of tools like coin mixers, stealth addresses, or anonymization protocols constitutes evidence of money laundering or illicit intent. This inversion of the burden of proof—requiring users to demonstrate their innocence—stands in direct violation of the fundamental legal principle of presumption of innocence, enshrined in Article 48 of the Charter of Fundamental Rights of the European Union.

The ORWL collective of legal scholars and practitioners based in Paris characterizes this approach as legally and operationally "superfétatoire," i.e., redundant and counterproductive. Their 2025 legal opinion argues that such presumption-based enforcement not only undermines the principle of technological neutrality but also exposes legitimate users—such as journalists, whistleblowers, or citizens under oppressive regimes—to disproportionate legal risk. Rather than addressing money laundering through forensic investigation, capacity-building in cybercrime units, and international coordination, the French model externalizes its burden onto technology itself.[61]

Moreover, ORWL warns that the combination of MiCA II's disclosure-heavy obligations and national criminal frameworks may result in developers abandoning the EU altogether. In their 2025 report, ORWL notes that pseudonymity is not a loophole, but a foundational safeguard. It allows developers to contribute to open protocols without fear of criminal liability, especially in cases where their work might intersect with privacy-preserving functionalities. If laws criminalize the architecture itself rather than its misuse, developers will either cease building within the EU or deploy anonymously via offshore proxies—thus removing both innovation and accountability from European oversight.[62]

The resulting legal climate discourages not only technical experimentation but also ethical use cases of blockchain. There exists a broad continuum of legitimate motivations for using anonymity in digital financial systems: from dissident communication and privacy-preserving donations to whistleblowing and sensitive journalism. Treating all such behavior as criminal by default endangers civil liberties while doing little to curb actual criminal operations, which adapt more quickly to surveillance than the law can evolve.

In sum, the EU's current posture—where privacy design equals criminal suspicion—risks eroding trust in its legal coherence and repelling the very class of actors it needs to foster technological sovereignty.

[61] ORWL Legal Collective, Legal Opinion on Privacy Technologies and Blockchain Regulation, 2025 – Legal presumption and anonymization under French law. See Section II – Anonymity and Legal Presumption, pp. 9–14

[62] ORWL Legal Collective, Legal Opinion on Privacy Technologies and Blockchain Regulation, 2025 – Legal presumption and anonymization under French law. See Section II – Anonymity and Legal Presumption, pp. 9–14

A rights-based approach would demand proportionate, evidence-based enforcement combined with robust data governance mechanisms—not presumptive outlawing of cryptographic anonymity.Despite its aims to harmonize and stabilize the crypto market, MiCA II imposes governance burdens that are structurally misaligned with the logic of decentralized innovation. The mandate that every crypto initiative formalize itself as a licensed entity, accountable under national law, presumes that decentralization can be subordinated to institutional formalism. It fails to appreciate that the most transformative applications of blockchain operate outside traditional legal containers—by design.

A regulatory expert from the European Crypto Initiative, warns of the unintended consequence this regulatory architecture is producing: a brain drains of crypto talent and projects from the EU. In countries such as France, Germany, and Italy, developers behind open-source protocols and early-stage crypto infrastructure face mounting compliance costs and a growing legal grey zone. For these teams, the regulatory burden—waiting over a year for licensing approval, hiring legal advisors, and restructuring governance—represents a prohibitive barrier. Jurisdictions like Abu Dhabi, Singapore, and Switzerland now appear more attractive to innovators seeking regulatory clarity without compromising decentralization.[63]

Compounding this issue is the strategic behavior of large platforms that operate across multiple jurisdictions. Many of these actors have adopted what she terms a "pay-to-play" strategy. Rather than building compliance capacity or restructuring product offerings to align with MiCA II's requirements, these firms factor administrative penalties into their financial models. Fines are seen not as deterrents but as manageable costs—far cheaper than adapting their architecture. This institutional calculus is especially perverse given the current sanctioning regime. MiCA's fines, while significant on paper, are relatively modest compared to the annual revenues of dominant market players, rendering them ineffective as enforcement tools. [64]

What is more alarming is the fiscal architecture that surrounds these sanctions. Under prevailing corporate tax frameworks in several EU Member States, financial penalties paid by companies may be treated as deductible expenses unless expressly forbidden by statute. The European Commission acknowledged where it warned that the lack of harmonized rules regarding the deductibility of regulatory fines creates uneven enforcement and undermines their punitive value. In effect, large crypto

[63] EU Crypto Initiative (EUCI), Proposal for Blockchain Compliance Models, 2025.
[64] EU Crypto Initiative (EUCI), Interview Co-founder of EUCI

enterprises can not only absorb penalties—they can potentially deduct them from their tax base, turning non-compliance into a fiscally rational decision.[65]

This dual failure, regulatory underenforcement and fiscal permissiveness—leads to a structurally inequitable system. Smaller startups and decentralized collectives, which often cannot even access legal representation or capital buffers, are disproportionately driven out of the EU market or excluded from compliance altogether. In contrast, multinational platforms with in-house legal teams and financial leeway remain operational while sidestepping the spirit of MiCA II.

The cumulative effect is a compliance asymmetry that privileges multinational corporations while excluding smaller or decentralized projects. This dual-track outcome—a combination of market consolidation and innovation flight—contradicts the EU's commitment to supporting innovation, competition, and technological sovereignty in the digital economy. According to EU Crypto Initiative, one of the most foreseeable consequences of MiCA II's licensing rigidity is a wave of mergers and acquisitions (M&A) within the European crypto ecosystem. Small and medium-sized enterprises, unable to bear the regulatory and legal costs of compliance, will be forced to consolidate with larger, better-capitalized entities in order to survive. This phenomenon, already visible in preliminary deal activity tracked in France and Germany, reflects a strategic absorption of risk by major platforms and investment funds willing to shoulder compliance in exchange for market dominance. While such M&A consolidation may preserve some domestic innovation, it undermines diversity in the ecosystem and marginalizes open-source, community-driven structures. At the same time, many developers unable or unwilling to merge have begun to explore alternative jurisdictions such as Abu Dhabi, Dubai, and Malta, which offer faster, tech-aligned licensing regimes and regulatory sandboxes. Others stay in Europe but operate informally, accepting the legal uncertainty and preparing to pay regulatory fines if and when they arise. This bifurcated strategy—either leave, consolidate, or operate illegally—reflects the failure of MiCA II to accommodate the actual technical architecture and governance models of decentralized crypto networks.[66]

2.4. Criminalization of Anonymity: Legal Risks to Privacy Infrastructure

France's narcotics law presents a compelling case study of regulatory overreach. According to legal analysis by ORWL and expert lawyer W. O'Rorck, the blanket criminal presumption that use of privacy-enhancing technologies (PETs)—such as mixers, privacy coins (e.g., Monero), or encrypted wallets—constitutes intent to launder creates dangerous jurisprudence. This legal stance effectively reverses the

[65] European Commission, MiCA, COM(2020)593 final – Asset-referenced tokens regulation. Asset-referenced tokens: Articles 15–36, especially: Article 15: "*Authorisation requirement*"; Article 20: *"White paper obligations*"; Article 28: "*Stabilisation mechanisms*"
[66] EU Crypto Initiative (EUCI), Interview with Co-founder, 2025

burden of proof, eroding the principle of innocence and placing legitimate users—journalists, dissidents, and privacy advocates—under blanket suspicion. [67]

Moreover, such laws are technologically non-neutral, targeting certain tools rather than the acts committed through them. This approach stands in contradiction to EU data protection values, particularly those enshrined in the GDPR and the Charter of Fundamental Rights.

More effective form of governance would focus on investigative capacity-building: hiring cyber-forensics experts, expanding cross-border coordination, and deploying algorithmic red-flagging tools that detect laundering patterns without outlawing privacy itself. [68]

2.5. The Erosion of Pseudonymity: Privacy Concerns and Surveillance Risks

The erosion of pseudonymity under emerging regulatory regimes, particularly through MiCA II and national AML provisions, raises serious concerns for the privacy and operational security of crypto users and developers. Pseudonymity—a core design feature of blockchain systems—was never intended to provide total anonymity, but rather to decouple identity from transactional behavior while allowing accountability through cryptographic means. However, in practice, increasing requirements to link wallet addresses with off-chain identifiers such as email, phone numbers, and social media accounts (e.g. Twitter, Telegram, Discord) have created a surveillance architecture that undermines this principle. Crypto journalist highlights, [69] this convergence of blockchain and identity platforms paradoxically introduces new vulnerabilities: user accounts become traceable across ecosystems, opening doors to phishing attacks, harassment, and even physical threats. The case of David Balland from Ledger, reported by BFM Crypto following his kidnapping, starkly illustrates the physical risks associated with the forced exposure of blockchain-linked identities.[70]

The European Data Protection Board (EDPB)[71], reaffirms that pseudonymisation remains a legitimate and protected form of privacy under the GDPR—particularly when reinforced through cryptographic techniques such as zero-knowledge proofs (ZKPs), Merkle trees, or selective disclosure protocols. Yet this legal position is not reflected in enforcement practices. ORWL, a digital rights think tank based in Paris, warns that regulatory hostility to pseudonymity has created a chilling effect on developers

[67] BFM Crypto – Les Pros, 10 March 2025, segment "*Régulation et blanchiment*", intervention ORWL, p. 2–3
[68] ORWL Legal Collective, Legal Opinion on Privacy Technologies and Blockchain Regulation, 2025 – Legal presumption and anonymization under French law. See Section II – Anonymity and Legal Presumption, pp. 9–14
[69] William Helle, "*Web3 Identity and Surveillance Risks*," CryptoScope Journal, Volume 3, Issue 1, February 2025, pp. 24–29.
[70] Alain Montfort, Interview in BFM Crypto, 2025.
[71] European Data Protection Board, Guidelines on pseudonymisation and blockchain, 2025.

working on privacy-preserving tools. Their 2025 policy brief notes that treating pseudonymity as circumvention rather than compliance devalues one of the few privacy-by-design safeguards embedded in blockchain architecture. [72]

The result is a paradox: while the GDPR celebrates privacy by design, regulatory regimes inspired by MiCA II and AMLR appear to incentivize its dismantling. Instead of recognizing pseudonymity as an architectural good, it is often conflated with criminal intent—reversing the presumption of good faith that should accompany privacy-first systems. This disconnect between the legal framework and the technical paradigm threatens not only individual rights but also the credibility of European digital innovation.

2.6 Surveillance Through Identity Integration: The Collapse of Technical Neutrality

To meet regulatory expectations under MiCA II and forthcoming AMLR provisions, many blockchain-based platforms now require users to connect their wallets to centralized identity systems. This includes linking public addresses to identifiers from social media (e.g. Discord, Twitter/X, Telegram), government IDs, or biometric data. While intended to satisfy Know-Your-Customer (KYC) obligations and prevent abuse, these integrations risk collapsing the very principle of technical neutrality.

The result is a hybrid surveillance framework, where user activity is tracked simultaneously on-chain and off-chain, enabling unprecedented forms of behavioral profiling. Instead of empowering users through pseudonymity and data minimization, the system increasingly mirrors legacy platforms where identity is centralized, monetized, and vulnerable. In practice, this also creates single points of failure and attack vectors, especially as blockchain records are immutable and public.[73]

ORWL has warned that such identity linkage turns privacy-preserving users into targets. Their report from 2025 notes that crypto founders and developers have faced extortion and coercion in France due to the growing traceability of wallets, who reports an uptick in security threats related to asset visibility. BFM Crypto's special report [74] highlighted how extortion gangs monitor known wallet balances and conduct social engineering to extract information, using on-chain transparency against users. [75]

Thus, the push to integrate identity across Web2 and Web3 systems not only undermines privacy-by-design but also violates proportionality—a core principle under the GDPR. Rather than regulating

[72] ORWL Legal Collective, Legal Opinion on Privacy Technologies and Blockchain Regulation, 2025 – Legal presumption and anonymization under French law. See Section II – Anonymity and Legal Presumption, pp. 9–14
[73] William Helle, "*Web3 Identity and Surveillance Risks*," CryptoScope Journal, Volume 3, Issue 1, February 2025, pp. 24–29.
[74] Alain Montfort, Interview in BFM Crypto, 2025.
[75] ORWL Legal Collective, 2025 Legal Opinion on Privacy Technologies and Blockchain Regulation.

identity exposure with nuance, the current trajectory incentivizes full traceability, disproportionately impacting lawful users while sophisticated actors adapt through layering techniques. The EU's regulatory architecture must reconsider whether technical neutrality remains a rhetorical ideal or a binding normative standard.

2.7 Increased Criminal Risks and Capital Flight Resulting from Anonymity Removal

The consequences of dismantling anonymity in crypto ecosystems extend far beyond the philosophical or legal. They manifest in concrete threats to physical safety, capital allocation, and jurisdictional competitiveness. In France, at least seven cases of kidnapping and extortion targeting crypto holders were reported in the first quarter of 2025 alone, according to Le Parisien. In each case, the victims had visible on-chain activity linked to known wallets or usernames—a direct consequence of regulatory frameworks that mandate deanonymisation without adequate safeguards.[76]

Alain Montfort, cybersecurity expert and president of Alamosofy, explains that increased traceability has shifted the risk calculus for both users and developers. Where anonymity once served as a protective veil, forced transparency has made crypto professionals vulnerable to physical harm. In response, many have chosen to withdraw from public-facing roles or migrate to countries where privacy remains both a right and a practice.[77]

That anonymity should be understood as a form of operational security, particularly for developers of public goods and open protocols. Its removal under MiCA II and national transpositions of AMLR creates a governance environment that treats cryptographic privacy as presumptively illicit. The result is a chilling effect on development, and a growing shift of capital and talent to jurisdictions such as Malta, the UAE (Abu Dhabi and Dubai), or Singapore—locations with more permissive and innovation-aligned frameworks.[78]

Rather than reducing risk, the EU's current trajectory displaces it—pushing lawful innovation offshore and exposing its remaining actors to heightened personal and legal threats. This strategic misalignment weakens the EU's competitiveness in Web3 infrastructure, and calls into question its claim to be a privacy-forward regulatory leader.[79]

2.8 The Race to Technological Governance: State Appropriation of Blockchain

[76] Le Parisien, "*Crypto: Enlèvements et agressions ciblent les détenteurs de portefeuilles publics*," Le Parisien, 15 January 2025, p. 3
[77] Alain Montfort, Interview in BFM Crypto, 2025.
[78] ORWL Legal Collective, 2025 Legal Opinion on Privacy Technologies and Blockchain Regulation.
[79] William Helle, "*Web3 Identity and Surveillance Risks*," CryptoScope Journal, Volume 3, Issue 1, February 2025, pp. 24–29.

As the heart of today's global digital transformation lies not just a race to innovate, but a race to govern innovation—to encode political will into the infrastructures of the future. This race is most visible in the domain of blockchain, a technology initially born of resistance to central authority, but now increasingly absorbed into the strategic agendas of states. While decentralized networks were originally conceived to circumvent institutional power, they are now being reappropriated, restructured, and repurposed by governments that seek not to dismantle blockchain's potential—but to bend it to their own logic. This is the premise of what this thesis calls technological governance: a mode of sovereignty exercised not through law alone, but through protocol design, infrastructure policy, and normative defaults embedded in code. [80]

Pieranni describes a society where emerging technologies—blockchain, AI, facial recognition, and digital currency—do not exist in isolation, but operate as converging tools of governance. The Chinese state's use of blockchain in public infrastructure, from health data to supply chains to judicial records, exemplifies a profound reorientation: a decentralized architecture redirected toward hyper-centralized control. The digital yuan (e-CNY), for instance, allows for monetary programmability at the level of the individual, enabling the government to pre-define how, where, and when money can be spent. Blockchain here is no longer a tool for autonomy, but for computational sovereignty—the state's ability to automate obedience and enforce policy through smart contracts. This approach signals a fundamental transformation of blockchain's political nature. In China, code is not law in the libertarian sense; code is an extension of the Party-state. The values of transparency and immutability, often celebrated by Western blockchain communities, are not discarded—but recontextualized. They are deployed to enhance state legibility of the population, rather than to protect individuals from it. Blockchain's potential for auditability becomes a surveillance feature. Its pseudonymity is stripped away in favor of biometric-linked digital identities. Its distributed architecture becomes a ledger of centralized behavior tracking. In Pieranni's words, the result is a "Red Mirror": a reflection not of where blockchain is heading universally, but of how it may be reshaped by the ideological frameworks of powerful states.

This leads to a critical insight: blockchain's architecture is not politically neutral. Its deployment depends not only on code, but on the governance models that surround and interpret it. As this thesis argues, the race to technological governance is also a race to define the meaning of blockchain itself. Will it remain a tool of financial emancipation, individual privacy, and voluntary coordination? Or will it evolve into an invisible infrastructure for digital conformity? China's example shows that the same technical features—immutability, traceability, programmability—can serve either freedom or control, depending on the hands that shape their use.

[80] Simone Pieranni, Red Mirror: Invention of China, Laterza, 2021, Chapter 5: Control Through Technology, pp. 152–176.

For Europe, the challenge is urgent. As frameworks like MiCA II and the Digital Services Act come into force, the EU is not just regulating blockchain—it is participating in this global contest over what blockchain will become. The decisions made today about identity verification, custody, transaction surveillance, and the permissibility of privacy-enhancing technologies (like zero-knowledge proofs or decentralized identifiers) will determine whether the European model offers a counterweight to the Chinese paradigm—or quietly converges with it. The risk is not only one of overregulation, but of infrastructural mimicry: importing the logic of surveillance while believing we are defending liberal values.

The Red Mirror should not be read as distant science fiction. It is a live prototype of what happens when governance infiltrates infrastructure without checks, when political aims override cryptographic neutrality, and when public institutions embrace programmable systems not to serve citizens, but to predict and shape them. It is also a cautionary tale: if Europe fails to articulate a coherent ethical framework for blockchain governance—rooted in data minimization, open access, self-sovereignty, and civic participation—then the technology's future may be dictated by the very regimes it was designed to resist.

Thus, the race to technological governance is not merely about regulation. It is about defining the architectural values of the digital public sphere. Europe still has the opportunity to propose a model that respects privacy without forfeiting oversight, that ensures security without collapsing into control, and that uses blockchain not to mirror power, but to redistribute it. But to do so, it must first recognize the stakes of this race—and ensure it is running in the right direction.[81]

The Rule of Code, anticipated this phenomenon: the law can be embedded in code, but so can authoritarianism. Blockchain is not inherently liberating—it can encode surveillance, hierarchy, and coercion just as easily as transparency and consensus. The crucial variable lies in governance.[82]

Against this backdrop, the EU often claims to offer a third path between U.S. deregulation and Chinese techno-authoritarianism. But this ambition remains structurally incomplete. In attempting to codify all aspects of crypto governance—from wallet traceability to licensing regimes—without integrating constitutional protections and proportionality constraints, the EU risks replicating some of the very pathologies it seeks to avoid. MiCA II's architecture mirrors many of the compliance demands found in

[81] Simone Pieranni, Red Mirror: Invention of China, Laterza, 2021, Chapter 5: Control Through Technology, pp. 152–176.
[82] Primavera De Filippi and Aaron Wright, Blockchain and the Law: The Rule of Code, Harvard University Press, 2018, Chapter 6: A Lex Cryptographia, pp. 210–245.

corporate regulation, but fails to distinguish between centralized exchanges and decentralized protocol communities.

If Europe wishes to avoid becoming a digital sovereignty paradox—championing open systems while constraining them through bureaucratic legalism—it must reassess its alignment with the values embedded in blockchain technology: permissionless access, distributed trust, and programmable accountability. Without this recalibration, its regulatory posture may pave the way not for innovation, but for codified stagnation.[83]

To sum up there are laws that exist and are emerging—but which change the value proposition of blockchain: The second wave of legislation, including MiCA II and AMLR, expands beyond regulating existing actors. It now aims to regulate the design and logic of new crypto projects themselves—including DeFi protocols, DAOs, privacy coins, and decentralized governance mechanisms. While these regulations claim to protect users and macroeconomic stability (e.g. shielding the euro from speculative crypto-currency inflation), they introduce unintended consequences.

For example, long licensing delays and vague thresholds discourage innovation and push small actors out of the market. According to both the EBA and critics like ORWL, these laws attempt to regulate highly dynamic ecosystems with frameworks modeled on traditional finance. The result is a shift from regulating how crypto is used to regulating how it is built, which undermines blockchain's core principles—decentralization, pseudonymity, and open-source governance. [84]

Furthermore, concerns over stablecoin-induced inflationary pressure on the euro have led to regulatory overreach. While economic stability is a legitimate goal, imposing severe controls on algorithmic stablecoins and DeFi collateral systems risks stagnating innovation and may prevent the euro itself from participating in competitive programmable finance.

2.9 Global Governance Models: Europe vs. United States vs. China

In the second phase of regulatory governance, Europe stands at a crossroads. MiCA II's ambition is to shape the future of blockchain in line with European values—accountability, consumer protection, and financial stability. However, this ambition must be analyzed in light of competing global governance strategies.

[83] Clara Chappaz, Ministry of Digital Affairs, Speech on AI and Data Governance, Paris Blockchain Week, France, 2025.
[84] ORWL Legal Collective, 2025 Legal Opinion on Privacy Technologies and Blockchain Regulation

The European Union's model, based on MiCA II and AMLR, imposes strict licensing, transparency obligations, and technological neutrality. While designed to shield the euro and create a trusted crypto ecosystem, these laws tend to reproduce traditional finance's structures within decentralized systems—often ignoring the very logic of decentralization. The result is a compliance-heavy environment that disproportionately affects small teams and open-source protocols. Many developers face licensing processes lasting 12–18 months and compliance costs exceeding €100,000—forcing them either to abandon their projects or seek jurisdictions abroad. This phenomenon contributes to a growing 'jurisdictional arbitrage' whereby promising European startups relocate to innovation-friendly hubs like Abu Dhabi, Dubai, or Singapore. [85]

In contrast, the United States offers a fragmented but more permissive approach. Despite the lack of a unified federal regulatory framework, and ongoing tension between agencies like the SEC and CFTC, the U.S. remains attractive to builders due to its vibrant venture ecosystem, active developer communities, and relative regulatory flexibility. Enforcement is often ex-post and litigation-driven, allowing innovation to thrive at the margins. Yet, the absence of clarity has led to high-profile lawsuits (e.g., Ripple, Coinbase) and considerable legal uncertainty. Nevertheless, the country remains a magnet for Web3 talent because regulatory barriers are lower at the launch stage.

The Chinese model, on the other hand, exemplifies digital authoritarianism. While cryptocurrencies are banned, blockchain is actively embraced for centralized administrative control. As Pieranni describes in 'Red Mirror', blockchain in China is used for immutable land registries, surveillance-compatible supply chains, and programmable CBDCs (e-CNY) that offer zero anonymity. Ariane Ollier-Malaterre's sociological account illustrates how surveillance becomes internalized in daily life, eroding autonomy. Xiaowei Wang [86] goes further, showing how blockchain is weaponized in rural areas for food traceability and behavioral analytics. These insights reflect a state-appropriated version of blockchain that subverts its emancipatory potential. [87]

Europe's position, often described as a 'third way', is thus problematic. Rather than offering a genuine alternative to U.S. deregulation or Chinese authoritarianism, it risks combining the burdens of both:

[85] Clara Chappaz, Ministry of Digital Affairs, Speech on AI and Data Governance, Paris Blockchain Week, France, 2025.
[86] Ariane Ollier-Malaterre and Shuang Wang, Blockchain in Authoritarian Contexts, 2022, Chapter 2: Blockchain in China's Rural Control Systems, pp. 65–98.
[87] Simone Pieranni, Red Mirror: Invention of China, Laterza, 2021, Chapter 5: Control Through Technology, pp. 152–176.

legal rigidity without the innovative freedom of the U.S., and surveillance mechanisms without the economic scale of China. [88]

2.10 The Structural Consequences of MiCA II: Concentration, Compliance Arbitrage, and Innovation Drain

The effects of MiCA II extend beyond licensing burdens. The regulation inadvertently promotes market centralization. Large actors adopt a 'pay-to-play' strategy—factoring fines into business models while avoiding architectural reform. Meanwhile, smaller projects are priced out of the system or forced into consolidation. This has resulted in an ongoing wave of mergers and acquisitions across France and Germany, where small protocol teams are bought out by compliance-capable incumbents. What appears as regulatory harmonization is, in reality, ecosystem consolidation.[89]

Another unintended consequence is fiscal optimization of non-compliance. As the European Commission warned the lack of harmonized rules around the deductibility of regulatory sanctions enables platforms to deduct MiCA-related fines as operational costs. This transforms enforcement into a budgetable risk rather than a structural deterrent, fundamentally undermining the legitimacy of the regulation. [90]

Finally, capital flight and talent drain have become structural issues. Developers unwilling to restructure protocols or undergo regulatory filtering are choosing to launch projects offshore. This trend is particularly visible in sectors like DeFi and privacy coins, where architectural anonymity or open governance makes MiCA II compliance nearly impossible. The rise of Abu Dhabi and Singapore as havens for crypto builders is not incidental—it reflects a systemic rejection of the European model. Unless corrected, the EU's claim to technological sovereignty may be reduced to paper, while sovereignty in practice shifts eastward.

---

[88] Simone Pieranni, Red Mirror: Invention of China, Laterza, 2021, Chapter 5: Control Through Technology, pp. 152–176.

[89] EU Crypto Initiative (EUCI), AML Handbook, 2025 – Anonymous accounts and upcoming AML restrictions

[90] European Commission, MiCA, COM(2020)593 final – Asset-referenced tokens regulation. Asset-referenced tokens: Articles 15–36, especially: Article 15: "*Authorisation requirement*"; Article 20: "*White paper obligations*"; Article 28: "*Stabilisation mechanisms*"

2.11. A Unified Framework, Yet Fragmented Reality: MiCA's Incomplete Harmonization

The Markets in Crypto-Assets (MiCA) Regulation represents a historic step toward establishing a unified legal framework across the European Union. It introduces three pillars of regulation: the issuance of crypto-assets and stablecoins, the provision of services such as custody and exchange, and the prevention of market abuse. The overarching goal is to transform 27 fragmented regulatory regimes into a cohesive European market for digital assets.

Yet despite its harmonizing intent, MiCA's implementation reveals a persistent fragmentation—not in legal texts, but in regulatory practice. National competent authorities (NCAs) interpret and apply the regulation with varying degrees of rigor, flexibility, and speed. Countries like Malta and the Baltic states have adopted a more opportunistic strategy, granting licenses in as little as four months, compared to over a year in France or Germany. This divergence creates strategic arbitrage: crypto firms select jurisdictions based not on legal substance, but on timelines, procedural clarity, and regulator posture.

Such divergences compromise MiCA's original promise of a level playing field, and instead foster regulatory competition across the Union. The practical consequence is a fractured market in which the choice of jurisdiction becomes a complex equation involving legal certainty, reputation, geographic proximity to target markets, and administrative burden.

2.12. The case of France as a Cautious Overachiever: Discipline Without Agility

France presents a paradox in the MiCA implementation landscape. On the one hand, it is one of the most diligent countries in terms of regulatory compliance. With over 130 registered Prestataires de Services sur Actifs Numériques (PSAN)[91], France hosts one of the largest populations of regulated crypto service providers in the EU. The Autorité des marchés financiers (AMF) is widely viewed as benevolent and transparent, processing all applications and avoiding arbitrary rejections—unlike the UK's Financial Conduct Authority, which has drawn criticism for mass rejections without explanation. Yet this commitment to procedural integrity comes at a cost. The AMF tends to delay action pending final guidelines from ESMA or the EBA, leading to considerable bureaucratic inertia. Resource limitations, exacerbated by delayed budget allocations, further hinder its ability to swiftly process high volumes of license applications. Moreover, crypto founders in France often exhibit an unusual psychological deference to the regulator. Unlike banks or investment funds, which do not hesitate to challenge regulators in court, many crypto actors fear retaliation or blacklisting. This chilling effect undermines the assertion of procedural rights, despite the existence of legal remedies, as demonstrated by the successful legal challenges mounted by law firms like ORWL. Post-license supervision only compounds

[91] William O'Rorke, Interview on MiCA and French Regulatory Relations, YouTube – Video_Unhosted with Claire Balva, 2025

the burden. Firms are subject to surprise on-site inspections lasting up to twelve weeks, audits targeting anti-money laundering (AML) controls, and narrowly focused compliance verifications. These impose significant organizational costs: internal reallocation of staff, exposure to sanctions, and administrative overload.

2.13. Market Reshaped: Specialization, Dissuasion, and Strategic Migration

As MiCA settles into national legal systems, the European crypto market is undergoing a process of specialization reminiscent of what occurred with investment funds. Jurisdictions such as Luxembourg and Ireland, long known for their fund expertise, are now positioning themselves as crypto hubs. This specialization affects both the geography of projects and their internal structuring. Firms may benefit from efficient licensing processes but face hidden costs such as limited local talent pools or lower institutional credibility.

More critically, the burden of regulatory compliance acts as a structural filter. Projects involving complex infrastructure (e.g., centralized exchanges or custodians) increasingly require legal counsel from inception—"you can't build a bank without a lawyer" becomes equally true for regulated crypto infrastructure. This raises the entry threshold and creates a bifurcated market: on one side, well-capitalized firms operating under heavy regulation; on the other, lighter, often borderline-regulated actors focused on distribution or software.

Finally, the factors guiding jurisdictional choice transcend regulatory texts. Legal clarity is necessary, but not sufficient. Project leaders also weigh access to banking services, the quality of the local legal ecosystem, staff availability, and cultural proximity to markets. Paradoxically, jurisdictions that are initially too permissive can backfire: sudden regulatory reversals—such as mass license cancellations in the Baltics—can force firms to relocate abruptly, threatening operational stability and investor confidence.[92]

Part III — Empirical and Practical Solutions to Preserve Blockchain's Foundational Ethos

This third section explores preventive solutions grounded in architectural design and proportionality, alongside technological advancements—such as clean digital identities and secure-by-design infrastructures—intended to reduce the need for heavy-handed regulatory controls.

3.1. The Need for Proportionate Regulation: Preserving the Ethos of Blockchain

[92] William O'Rorke, Interview on MiCA and French Regulatory Relations, YouTube – Video_Unhosted with Claire Balva, 2025

While targeted regulation is essential to prevent abuse and protect users, there is a growing concern—both among legal scholars and industry practitioners—that excessive or ill-adapted regulatory pressure could erode the very foundations that make blockchain transformative. Decentralization, transparency, and open access are not marginal attributes of blockchain—they are its core architectural principles. When regulatory frameworks attempt to impose institutional structures designed for centralized systems onto decentralized protocols, the result is often legal friction, technical incoherence, and economic deterrence. [93]

While the intent behind the European regulatory push—especially through instruments like MiCA is legitimate, the execution sometimes reflects a profound misunderstanding of how blockchain technologies operate. He emphasized that many regulatory texts are drafted through analogies with traditional finance, overlooking the specificities of decentralized architectures. For instance, requirements to identify a responsible legal entity, or to submit a complete whitepaper prior to any public token issuance, may appear reasonable on paper, but they become inapplicable or even absurd in the context of community-governed DAOs or open-source smart contracts developed without centralized coordination.[94]

This gap between legal theory and technical implementation has tangible consequences. It creates high compliance costs that only well-capitalized actors can afford to absorb. Smaller teams, developers, and innovators are either pushed to relocate to jurisdictions with more agile frameworks—such as Abu Dhabi, Singapore, or Switzerland—or they withdraw from the European market entirely. In both cases, Europe loses a portion of the creative energy and intellectual capital that could have otherwise contributed to building a sovereign and ethically grounded Web3 ecosystem.

Beyond the economic risks, overregulation also poses a structural threat to the principle of autonomous governance, which is one of blockchain's most promising contributions. By encoding rules directly into protocols, blockchain allows for trustless coordination, algorithmic enforcement, and peer-to-peer accountability. If regulators insist on overriding this logic through external, top-down mechanisms—especially ones that lack proportionality or technological nuance—they risk neutralizing the unique governance capacity that blockchain makes possible.

This is why it is crucial for regulatory frameworks to adopt a model that is not only proportionate in scope but also aware of the architectural and functional differences between centralized and decentralized systems. Such a model would distinguish between actors based on their risk profiles and

[93] William Helle, *"Web3 Identity and Surveillance Risks,"* CryptoScope Journal, Volume 3, Issue 1, February 2025, pp. 24–29
[94] William Helle, "*Web3 Identity and Surveillance Risks*," CryptoScope Journal, Volume 3, Issue 1, February 2025, pp. 24–29

levels of influence rather than their form. For example, a centralized exchange handling billions in daily transactions should not be treated the same way as a small developer deploying a liquidity pool or NFT minting contract.[95]

In doing so, regulation can remain responsive to real threats—such as fraud, terrorist financing, or systemic instability—without placing an undue burden on innovation or suppressing the collective experimentation that defines the crypto ecosystem. This approach is not about deregulation, but about intelligent differentiation, which aligns enforcement efforts with the actual structure and behavior of the systems in question.

This tension—between protective oversight and technological autonomy—forms the central axis of this thesis. It invites a deeper reflection on how legal regimes such as MiCA, AMLR, and GDPR are not simply "applying" to blockchain, but actively reshaping its boundaries, its design logic, and its future governance potential. The challenge ahead is not whether blockchain will be regulated, but whether that regulation will allow it to fulfill its original promise without being hollowed out in the process. [96]

3.2. Securing Transactions through Cryptographic Integrity

One of the most direct and technically coherent responses to regulatory challenges is the reinforcement of privacy and auditability via cryptographic primitives. Hashing algorithms, digital signatures, and Merkle trees provide mathematical guarantees of data integrity while enabling verifiable proofs without revealing underlying personal data. For example, zero-knowledge proofs (ZKPs) allow a user to demonstrate possession of certain information—such as compliance with KYC thresholds or access rights—without exposing the information itself.

The European Data Protection Board (EDPB) interplay between blockchain and personal data protection, clearly endorses such techniques. The EDPB specifically recommends that on-chain data should be minimized or replaced by off-chain storage of personal information, with cryptographic commitments (e.g., hashes, ZKPs, digital signatures) linking back to it. These recommendations are grounded in the GDPR's Articles 5 and 25, especially emphasizing the principles of data minimization, storage limitation, and privacy by design.[97]

The EDPB further stresses that cryptographic privacy mechanisms should not be viewed as obstacles to regulation but as opportunities to embed compliance at the architectural level. This marks a sharp departure from repressive frameworks such as the anonymity ban planned under the AMLR by 2027,

[95] EU Crypto Initiative (EUCI), AML Handbook, 2025.
[96] Alain Montfort, Interview in BFM Crypto, 2025.
[97] European Data Protection Board, "Guidelines 02/2025 on processing of personal data through blockchain technologies," April 2025.

which the EDPB does not endorse in its guidelines. Instead, the Board suggests proactive risk mitigation through cryptographic governance (e.g., selective disclosure, contextual access management, and data custodianship models) that ensures compliance without undermining pseudonymity. By treating blockchain not as a threat to data protection but as a system capable of embodying it, the EDPB positions itself as one of the few EU-level institutions advocating for regulatory innovation grounded in technical literacy. In this view, compliance is not merely a matter of identity revelation but of auditability, accountability, and proportionality—values that blockchain, if properly implemented, can fulfill by design.[98]

This architecture aligns directly with the GDPR's privacy-by-design principle (Art. 25), while preserving blockchain's native immutability and transparency. By leveraging ZKPs and commitment schemes, projects can create compliance layers that do not compromise user anonymity or decentralized control. the reinforcement of privacy and auditability via cryptographic primitives. Hashing algorithms, digital signatures, and Merkle trees provide mathematical guarantees of data integrity while enabling verifiable proofs without revealing underlying personal data. For example, zero-knowledge proofs (ZKPs) allow a user to demonstrate possession of certain information—such as compliance with KYC thresholds or access rights—without exposing the information itself.

The European Data Protection Board (EDPB) endorses such mechanisms in its 2025 Guidelines, recommending off-chain storage of personal data combined with cryptographic commitments on-chain. This architecture aligns with the GDPR's privacy-by-design principle (Art. 25), while preserving blockchain's native immutability and transparency. By leveraging ZKPs and commitment schemes, projects can create compliance layers that do not compromise user anonymity or decentralized control.[99]

3.3 Privacy-Preserving Digital Identity Frameworks

Digital identity is a cornerstone of both compliance and usability in decentralized systems. However, traditional KYC systems often rely on centralized identity verification processes that conflict with blockchain's decentralized ethos. One of the most ambitious initiatives to address this dilemma is Worldcoin, co-founded by Sam Altman, which proposes a global proof-of-personhood system using biometric verification (notably iris scanning). The aim is to ensure that behind every digital wallet or on-chain address, there is a unique human user, and not a swarm of sybil bots or exploitative identity

[98] European Data Protection Board, Guidelines on pseudonymisation and blockchain, 2025.
[99] European Data Protection Board, Guidelines on pseudonymisation and blockchain, 2025.

farms. While controversial, this logic tackles a real issue in Web3: guaranteeing civil uniqueness while preserving scalability and fairness in on-chain governance. [100]

Nonetheless, the project has been met with institutional skepticism. Indonesia, for instance, suspended its biometric data collection pilot with Worldcoin in 2023 over concerns about data security, identity exploitation, and insufficient regulatory clarity on biometric consent (Reuters, Aug. 2023). Critics warn that such systems risk becoming honeypots for biometric surveillance. But from a privacy engineering standpoint, the intent behind Worldcoin—distributing a non-replicable digital ID—is not to centralize control, but to prevent fake identities from dominating decentralized ecosystems.

Moreover, it is worth reminding that in Europe, individuals already routinely share verified identity documents with banks, health insurance providers, and fintech platforms. The real challenge is not the existence of identity disclosure, but the architecture and control mechanisms surrounding that data. The Privacy-preserving digital identity systems—such as those built with ZKPs and DIDs—can reconcile the need for compliance with the right to privacy.[101]

Thus, rather than rejecting identity outright, the blockchain community should focus on developing modular, consent-based identity layers that empower users. These systems should enable compliance where necessary, while protecting users from surveillance and misuse—aligning with the principles of self-sovereignty, contextual consent, and cryptographic verification.

The EU's eIDAS 2.0 initiative has opened the door to compatibility between DIDs and legal digital identity under European law. Combining such frameworks with ZKPs allows for a pseudonymous yet verifiable presence in crypto ecosystems. This approach meets regulatory needs for authentication without exposing the user's core identity. It enables, for instance, age verification or country-specific access restrictions without unnecessary personal data collection. [102]

Projects such as Polygon ID, zkKYC, and Veramo demonstrate how identity can be cryptographically verified, locally stored, and contextually disclosed. These solutions allow for selective compliance that respects privacy, and they stand as viable pathways for reconciling MiCA II and GDPR requirements.

3.4 Strengthening Digital Hygiene and Operational Security

In addition to system-level privacy protections, user-level security remains essential to reducing exposure in a transparent ecosystem. The necessity of strong digital hygiene practices is necessary:

[100] BFM Crypto – Les Pros, 10 March 2025, segment "*Régulation et blanchiment*", intervention ORWL, p. 2–3.
[101] European Data Protection Board, Guidelines on pseudonymisation and blockchain, 2025.
[102] ORWL Legal Collective, 2025 Legal Opinion on Privacy Technologies and Blockchain Regulation

multi-signature wallets, hardware key storage, address randomization, and network segmentation can reduce the likelihood of targeted attacks. These measures serve as non-negotiable building blocks of operational security in environments where on-chain activity is inherently transparent and, if left unmanaged, traceable to real-world individuals. [103]

The European Data Protection Board (EDPB), in its 2025 Guidelines, explicitly recognizes that data minimization and user-driven control over exposure are crucial to ensuring blockchain's compatibility with the GDPR. This reinforces the argument that digital hygiene practices are not only cybersecurity imperatives but also extensions of fundamental rights such as the right to informational self-determination. In its recommendations, the EDPB encourages developers and platforms to adopt privacy-by-default settings and to embed data protection impact assessments (DPIAs) directly into protocol design and frontend user flows.

In this light, digital hygiene should not be treated as a user responsibility alone, but as a co-regulated space where protocol developers, regulators, and end-users share the burden of minimizing risk. Rather than focusing exclusively on identity traceability, European policy could shift its enforcement attention to whether platforms have implemented strong defaults, granular user consent mechanisms, and resilience protocols that reflect best practices in secure cryptographic ecosystems.

Furthermore, platforms must abandon practices that expose wallet addresses in publicly indexed formats or bind them to personal identifiers. As BFM Crypto has reported, extortion and wallet tracing attacks in 2025 have exploited predictable wallet structures and insufficient user awareness. Enforcing security-by-default policies, offering opt-in pseudonymity, and minimizing off-chain identity leaks are critical risk mitigation steps.[104]

3.5. Embedding Governance in Code: Protocol-Level Regulation

As De Filippi and Wright (2018) argue, blockchain introduces a new regulatory modality: governance by design. Smart contracts and DAOs can enforce rules ex-ante, reducing the need for ex-post penalties. Protocols like Aave, MakerDAO, or Optimism have already embedded governance constraints—such as treasury approvals, rate limits, and transparency audits—directly into smart contracts. [105]

This mode of governance aligns more closely with the preventative regulatory philosophy promoted by the European Data Protection Board (EDPB) in its 2025 Guidelines, which emphasize embedding compliance into system architecture rather than relying on top-down enforcement. The EDPB promotes

[103] Alain Montfort, Interview in BFM Crypto, 2025.
[104] Alain Montfort, Interview in BFM Crypto, 2025.
[105] Primavera De Filippi and Aaron Wright, Blockchain and the Law: The Rule of Code, Harvard University Press, 2018, Chapter 6: A Lex Cryptographia, pp. 210–245.

cryptographic accountability—such as the use of zero-knowledge proofs, hashed credentials, and selective disclosure—as a way to uphold privacy while ensuring auditability.

This vision stands in direct contrast with the repressive trajectory suggested under MiCA II and the upcoming AMLR provisions, where identification and traceability are often mandated irrespective of technical design. Rather than leveraging blockchain's ability to self-enforce via programmable constraints, MiCA II presumes that compliance can only be assured through exogenous bureaucratic oversight. The result is a missed opportunity to innovate governance itself.

Embedding compliance into protocol logic offers a middle path: regulators could stipulate functional outcomes (e.g., no sanctioned entity can access a service) and allow developers to implement these rules using privacy-preserving cryptographic tools. Such flexibility respects the principles of proportionality and technological neutrality articulated in both the GDPR and the EDPB's guidance.

Ultimately, while MiCA II focuses on command-and-control licensing, the regulatory model proposed by both De Filippi and Wright and supported by the EDPB suggests a future in which blockchain protocols do not just comply with regulation—they operationalize it natively, transparently, and proportionally.[106]

Rather than imposing top-down compliance, regulators could require that certain functions (e.g. user onboarding, stablecoin minting) include auditable controls written in code. This would preserve decentralization while achieving regulatory goals in a natively compatible way. For instance, privacy-preserving AML checks could be handled via zk-SNARKs that prove no sanctioned addresses are involved in a transaction.

Embedding compliance in code creates a more enforceable, scalable, and user-aligned system than purely paper-based regulation. It also opens the door for automated supervision, where regulators can audit outcomes through cryptographic transparency rather than account-level monitoring.

3.7 A Convergent Path Forward

To preserve blockchain's foundational values while addressing legitimate concerns of financial security, consumer protection, and market integrity, the EU must rethink its regulatory posture. Rather than forcing blockchain into existing legal templates, the goal should be to evolve law in tandem with the technology—privileging transparency, resilience, and user empowerment. This implies the creation of a multi-layered regulatory ecosystem in which preventive mechanisms—such as cryptographic

[106] Primavera De Filippi and Aaron Wright, Blockchain and the Law: The Rule of Code, Harvard University Press, 2018, Chapter 6: A Lex Cryptographia, pp. 210–245.

accountability, smart contract transparency, and decentralized reputation systems—operate in parallel to traditional supervisory authorities. One of the key institutional innovations is a publicly funded European cybersecurity police force oriented toward blockchain integrity, capable of tracking illicit behavior without dismantling anonymity or decentralization. [107]

This approach resonates with the European Data Protection Board (EDPB) Guidelines 01/2025, which emphasize the importance of embedding data protection principles into blockchain design rather than imposing external, static legal mandates. According to the EDPB, proportionality, purpose limitation, and data minimization must remain functional anchors—even in blockchain systems. Rather than defaulting to identity-based enforcement, the EU could focus on designing interoperable privacy standards and behavioral anomaly detection systems that maintain pseudonymity by default. This would represent a more precise and technologically literate alternative to sweeping traceability mandates.[108]

Ultimately, the path forward involves abandoning the rigid hierarchy of command-and-control licensing in favor of adaptive compliance frameworks that scale with technological change. Europe must treat blockchain not only as a subject of regulation, but as an opportunity to reinvent how governance itself is distributed, verified, and protected.

The future of digital governance lies not in choosing between privacy and compliance, but in designing systems that can do both. By leveraging cryptographic techniques, decentralized enforcement, and code-embedded rules, Europe can lead not just in regulation, but in innovation.

3.8 Establishing a Cybersecurity-Focused Public Infrastructure

"There is a need to construct a transnational cybersecurity infrastructure tailored to the borderless nature of blockchain technologies". [109] The traditional national enforcement frameworks are increasingly ineffective in responding to the decentralized and transjurisdictional dynamics of crypto-assets, smart contracts, and decentralized applications. Drawing a parallel with the long-standing debate on European military integration, Reiberling highlighted that smaller EU states are often in favor of supranational coordination—not merely for deterrence, but to gain access to resources, intelligence, and institutional stability offered by larger member states. This logic, he argued, applies equally to cybersecurity: without shared enforcement tools, smaller nations remain disproportionately vulnerable.

According to Reiberling, the inherently international character of smart contracts—automatically executing transactions across global nodes—produces legal effects and potential violations that no

[107] Clara Chappaz, Speech at Paris Blockchain Week, Ministry for Artificial Intelligence, France, 2025
[108] European Data Protection Board, Guidelines on pseudonymisation and blockchain, 2025.
[109] Minister of Foreign Affairs of Germany, French-German Diplomatic discussion: European Military Power Dialogue, November 2024

single country can regulate alone. Consequently, he advocates the creation of an international cyber-police force, comparable to Interpol, but specifically adapted to blockchain infrastructure. Its mandate would include monitoring decentralized financial flows, tracing illicit activities across jurisdictions, and coordinating interventions in real time—especially when actors exploit fragmented or uneven regulatory environments within the EU.

This proposal aligns with the concerns expressed by the European Crypto Initiative (EUCI), whose co-founder noted that under MiCA II, administrative fines are often too low to dissuade large, well-capitalized crypto actors. Many of these projects either absorb penalties as the cost of doing business or restructure through mergers and acquisitions to maintain superficial compliance while continuing to operate in gray legal zones. Rather than relying exclusively on such monetary sanctions, Reiberling stressed the necessity of equipping European institutions with preventive intelligence capabilities: systems to proactively monitor and track suspicious crypto projects internally, before harm materializes.

Yet despite its strategic rationale, the project of supranational cyber enforcement faces political resistance from key EU powers, notably France and Germany. Their reluctance reflects a deep concern for national sovereignty and the legal complexities of delegating investigatory powers to international bodies. This divergence creates an institutional imbalance: while smaller states call for alignment and shared infrastructure, larger countries hesitate—delaying the emergence of a cohesive digital security framework.

In conclusion, Reiberling positions the issue as one of sovereignty in the digital age. Just as NATO was conceived to safeguard territorial integrity, a next-generation enforcement structure is now needed to protect the integrity of Europe's digital and financial systems. Blockchain violations—by design—transcend borders; preventing them requires a governance infrastructure that is equally global, interoperable, and equipped for the complexity of twenty-first-century threats.[110]

Current enforcement models rely heavily on centralized regulators and reactive penalties. However, national police forces remain under-equipped and under-trained to address the specificity of crypto-related cybercrime. As blockchain ecosystems introduce new challenges—from anonymous liquidity pools to cross-border flash loan exploits—traditional enforcement agencies lack the technical tools, interoperability, and forensic training to respond effectively.

These challenges cannot be met solely by increasing licensing obligations or broadening identification requirements. Instead, he suggests the establishment of a European-level cyber-police force, analogous to Interpol, but specifically dedicated to blockchain and digital asset enforcement. Such an entity could

[110] Minister of Foreign Affairs of Germany, French-German Diplomatic discussion: European Military Power Dialogue, November 2024

be co-funded through transaction levies or public cybersecurity budgets and would be tasked with detecting illicit activity based not on identity exposure, but on behavioral and technical anomaly detection.[111]

Efforts to address blockchain-related crime cannot rely solely on expanding licensing requirements or mandating broader identity verification measures. While these regulatory tools may serve as basic entry barriers, they remain insufficient in capturing the full complexity of decentralized and pseudonymous ecosystems. Traditional compliance mechanisms operate on the assumption that actors are known, localized, and hierarchically structured—assumptions that simply do not hold in the context of permissionless blockchains, decentralized finance (DeFi), or anonymized liquidity protocols. As such, enforcement strategies based on identity disclosure risk both inefficiency and overreach, potentially criminalizing legitimate privacy-preserving behaviors while failing to detect actual illicit activity.

To address this gap, legal-tech experts and institutional observers—have called for the creation of a European-level cybersecurity enforcement entity. This proposed body would function analogously to Interpol, but with a mandate specifically tailored to the technical and operational realities of blockchain and digital assets. Rather than relying on identity-based enforcement, such an institution would be tasked with detecting illegal activity through behavioral analytics, code-level traceability, and anomaly detection techniques. This would allow for a form of "ethical surveillance"—one that respects privacy and decentralization while enabling effective risk identification and intervention.[112]

The funding model for this enforcement architecture could draw from transaction levies built into on-chain activity or from mandatory cybersecurity insurance premiums imposed on regulated actors. These financial mechanisms would internalize the costs of monitoring systemic risk and ensure sustainable public oversight. Importantly, this approach would allow public authorities to move beyond static licensing regimes and instead develop dynamic, data-informed responses that evolve alongside technological change.

This vision is rooted in a broader rethinking of how institutions govern digital space. As the European Data Protection Board repeatedly emphasizes, the future of data governance must rest on the principles of proportionality and prevention. Blanket surveillance, or the dismantling of pseudonymity, contradicts these values and threatens to erode trust in public institutions. A more effective alternative lies in institutional adaptation: the development of enforcement bodies that are not only legally competent but also technically embedded within the digital environments they regulate. This entails equipping public

[111] Clara Chappaz, Speech at Paris Blockchain Week, Ministry for Artificial Intelligence, France, 2025
[112] William Helle, "*Web3 Identity and Surveillance Risks*," CryptoScope Journal, Volume 3, Issue 1, February 2025, pp. 24–29.

infrastructure with the forensic capabilities, interoperability frameworks, and collaborative protocols required to navigate the high-speed, high-complexity world of blockchain-based finance.

Ultimately, the criminal misuse of blockchain technologies should not justify a regression into surveillance-heavy, centralized legal paradigms. Rather, it should catalyze a new generation of technologically literate, proportionately empowered public actors, capable of addressing crime without compromising the foundational values of Web3—privacy, decentralization, and user sovereignty. The emergence of such a public enforcement infrastructure would represent not only a regulatory innovation but also a profound evolution in the relationship between law, technology, and society.[113]

The funding for such initiatives could come from transaction levies or mandatory cybersecurity insurance. Instead of enforcing legality via licensing alone, the EU could expand its toolkit to include ethical surveillance—focused not on identity, but on behavioral anomalies and technical signatures. This would help address money laundering and scams without dismantling blockchain's privacy layer.

3.9. A Regulatory Geography of Europe: Project Flight and Competition Between Supervisory Authorities

While MiCA [114]was designed to harmonize crypto-asset regulation across the European Union, a new form of disparity has emerged—not textual, but operational. According to William O'Rorke, crypto entrepreneurs no longer select their jurisdiction based on the legal texts themselves, now largely unified within the EU, but rather on the behavior and efficiency of local regulators. The decisive factor is not what the law says, but how the regulator acts: whether they are crypto-friendly, responsive, flexible, or conversely, cautious, slow, and rigid.[115]

This has triggered a dynamic of regulatory competition. Malta, for example, has reportedly granted the first MiCA licenses within just four months, while by early 2025, the French regulator (AMF) had not issued a single one. Such agility is no coincidence: Maltese legal professionals recognize a proactive national strategy, built on investments in human resources, flexible interpretation of the texts, and a historical positioning as a jurisdiction open to financial innovation.

The consequence is clear: there is a growing risk of "project flight"—particularly from France—toward more welcoming or faster jurisdictions. For non-European crypto projects, such as those based in the

[113] ORWL Legal Collective, 2025 Legal Opinion on Privacy Technologies and Blockchain Regulation
[114] European Commission, MiCA II, 2024 – Licensing and whitepaper obligations for CASPs. Found in Title V – Conditions for the provision of crypto-asset services by crypto-asset service providers, particularly: Article 59: "*Obligation to obtain authorisation*"; Article 62: "*Obligations related to white papers*"; Article 66: "*Record-keeping and transparency obligations*"
[115] William O'Rorke, Interview on MiCA and French Regulatory Relations, YouTube – Video_Unhosted with Claire Balva, 2025.

U.S. or Asia, the decision is often purely strategic, reduced to an Excel sheet: processing time, legal climate, compliance costs. If France does not improve its responsiveness, it may see its entrepreneurs, innovators, and investors migrate to more agile hubs like Malta, Cyprus, or Ireland.

However, this dynamic comes with its own risks. Regulatory havens that initially attract projects may later reverse course. The Baltic countries serve as a cautionary tale: after a period of regulatory laxity, authorities in these jurisdictions abruptly revoked the registration of numerous virtual asset service providers (VASP or prestataires de services sur actifs numériques – PSAN in French law), destabilizing the local ecosystems. According to the EDPB, VASPs are entities that provide services such as custody, exchange, or transfer of digital assets and are subject to both AMLR and data protection obligations, especially when handling personally identifiable information in blockchain.

Projects are therefore confronted with a dilemma: should they optimize for short-term attractiveness or long-term stability? The rational choice becomes a balance between regulatory clarity, speed, and the risk of future reversals. This reality underlines the need for not just harmonized legal frameworks, but also harmonized institutional practices—if Europe wants to remain a leading and credible jurisdiction in the global crypto economy.[116]

[116] William O'Rorke, Interview on MiCA and French Regulatory Relations, YouTube – Video_Unhosted with Claire Balva, 2025.

APPENDIX

I. Academic Books

[1] Shoshana Zuboff, The Age of Surveillance Capitalism, Harvard Business School Press, 2019, Chapter 3: The Discovery of Behavioral Surplus, pp. 93–136.
How Google initiated the extraction of behavioral data, turning users into a source of profit: "You are not the customer; you are the raw material." It provides the conceptual foundation for digital capitalism discussed in the thesis.

[2] Shoshana Zuboff, The Age of Surveillance Capitalism, Harvard Business School Press, 2019, Chapter 9: Rendition from the Depths, pp. 221–266.
Zuboff describes how platforms capture intimate aspects of human life through ubiquitous digital infrastructures—relevant for illustrating Web3 risks in the absence of ethical governance.

[3] Primavera De Filippi and Aaron Wright, The Rule of Code: Blockchain and the Law, Harvard University Press, 2018, Chapter 4: Code and Governance, pp. 89–132.
Used in the thesis to explain embedded governance mechanisms (DAOs, smart contracts) as an alternative organizational model to traditional legal systems.

[4] Primavera De Filippi and Aaron Wright, Blockchain and the Law: The Rule of Code, Harvard University Press, 2018, Chapter 6: A Lex Cryptographia, pp. 210–245.
Source of the sections discussing algorithmic sovereignty and the tension between state authority and decentralized self-regulation.

[5] Ariane Ollier-Malaterre and Shuang Wang, Blockchain in Authoritarian Contexts, 2022, Chapter 2: Blockchain in China's Rural Control Systems, pp. 65–98.
Cited to show how blockchain can enhance state control rather than individual freedom, as seen in the Chinese use of blockchain technologies.

[6] Simone Pieranni, Red Mirror: Invention of China, Laterza, 2021, Chapter 5: Control Through Technology, pp. 152–176.
Analyzed in the section on state surveillance applied to digital identity and blockchain infrastructures.

II. EU and Regulatory Reports

[7] European Commission, MiCA II, 2024 – Licensing and whitepaper obligations for CASPs. Found in Title V – Conditions for the provision of crypto-asset services by crypto-asset service providers, particularly: Article 59: "*Obligation to obtain authorisation*"; Article 62: "*Obligations related to white paper*s"; Article 66: "*Record-keeping and transparency obligations*".

[8] European Commission, MiCA, COM(2020)593 final – Asset-referenced tokens regulation. Covered in Title III – Asset-referenced tokens: Articles 15–36, especially: Article 15: "*Authorisation requirement*"; Article 20: "*White paper obligations*"; Article 28: "*Stabilisation mechanisms*". This forms the legal basis for early stablecoin regulation you used in Part I.

[9] European Data Protection Board (EDPB), Guidelines 02/2025 on Processing of Personal Data through Blockchain Technologies – Data minimisation, DPIA, decentralised processing roles. Relevant sections: Section 2.3: Explains decentralised roles (controllers/processors); Section 4.1: "*Data Protection Impact Assessments*"; Section 4.2: "*Data minimisation techniques and zero-knowledge proofs*". Used in Part II.6 to support privacy-by-design and GDPR tension analysis.

[10] European Data Protection Board (EDPB), Guidelines on Pseudonymisation and Blockchain, 2025 – Pseudonymisation and privacy in DLTs. Focused in Section 2.4: Pseudonymisation and distributed ledger technologies. For the critique of the erosion of pseudonymity in Part II.2.

[11] EU Crypto Initiative (EUCI), AML Handbook, 2025 – Anonymous accounts and upcoming AML restrictions. Part I.1 corresponds to the 2027 ban on anonymous wallets and enhanced scrutiny of privacy protocols. While the full handbook was not uploaded, Chapter 5 – Risk-Based Supervision for VASPs, notably the section calling for mandatory KYC procedures for all wallet types including mixers and stealth addresses.

[12] ORWL Legal Collective, Legal Opinion on Privacy Technologies and Blockchain Regulation, 2025 – Legal presumption and anonymization under French law. See Section II – Anonymity and Legal Presumption, pp. 9–14. Cited in Part I.1 and II.1 for the critique of technological discrimination and the reversal of the burden of proof in narcotics cases.

[13] Michele Finck, "*Blockchain and the General Data Protection Regulation*," Oxford Internet Institute, 2024 – GDPR–blockchain conflicts (immutability, erasure, responsibility). The existence of the legal Conflicts between Blockchain Architecture and GDPR, pp. 17–24. Used in Part II.6 to illustrate structural incompatibilities between DLTs and data subject rights.

III. Interviews, Speeches & Testimonies

[14] William O'Rorke, Interview on MiCA and French Regulatory Relations, YouTube – Video_Unhosted with Claire Balva, 2025.

[15] EU Crypto Initiative (EUCI), Interview with Co-founder, 2025.

[16] Clara Chappaz, Speech at Paris Blockchain Week, Ministry for Artificial Intelligence, France, 2025.

[17] Alain Montfort, Interview on Crypto Privacy and Security, BFM Crypto, 2025.

[18] Minister of Foreign Affairs of Germany, French-German Diplomatic discussion: European Military Power Dialogue, November 2024.

IV. Press Articles and Media

[19] Le Parisien, "*Crypto: Enlèvements et agressions ciblent les détenteurs de portefeuilles publics*," Le Parisien, 15 January 2025, p. 3.

[20] Journal du Coin, *Analyse annuelle de la régulation crypto en France*, December 2024, https://journalducoin.com, p. 8–14.

[21] BFM Crypto – Les Pros, 10 March 2025, segment *"Régulation et blanchiment*", intervention ORWL, p. 2–3.

[22] LinkedIn Live Replay, KPMG & ADAN, "*Panorama 2023 de l'écosystème crypto français*", held on 18 October 2023, accessible via https://www.linkedin.com/company/adan-association.

[23] William Helle, "*Web3 Identity and Surveillance Risks*," CryptoScope Journal, Volume 3, Issue 1, February 2025, pp. 24–29.