Available Online: 16 October 2026 DOI: 10.54254/2753-7102/2026.37724

Embedded supervision for intellectual property tokenisation under the EU DLT Pilot Regime: reconciling proportionality with trade secret protection

Luxi Li

Faculty of Law & Justice, UNSW Sydney, Sydney, Australia

l15923676663@gmail.com

Abstract. The tokenisation of intellectual-property-related financial claims on Distributed Ledger Technology (DLT) promises fractional investment, programmable licensing, faster settlement and improved traceability. Yet the same ledger architecture that can make regulatory information more accessible may also create a new confidentiality problem for IP-intensive issuers. This article examines that problem within Regulation (EU) 2022/858 (the DLT Pilot Regime). It argues that the central legal question is not whether supervisors should have access to DLT data, but how supervisory access should be designed so that the information necessary for market integrity and investor protection is available without turning commercially sensitive information into unnecessarily persistent regulatory data. The article makes four interventions. First, it distinguishes the tokenised financial instrument from the underlying IP and from confidential know-how associated with that IP, avoiding a model in which trade secrets are treated as though they were themselves transferable securities. Second, drawing on the wider debate about which digital-money architecture will underpin tokenised markets, it shows that the choice of settlement asset for an IP-backed DLT instrument is analytically inseparable from the choice of supervisory architecture, because both raise the same underlying question of how much trust must be placed in a third party. Third, it reframes embedded supervision as an architecture of graduated data access rather than as unrestricted ledger visibility, and applies the Trade Secrets Directive, the General Data Protection Regulation and the EU proportionality principle to argue for a privacy-by-design model based on data minimisation, permissioned access, cryptographic commitments and, where technically mature and appropriate, zero-knowledge proofs and confidential computation. Fourth, it proposes a four-layer supervisory architecture and a graduated disclosure matrix that link the sensitivity of information to the regulatory purpose for which it is sought. The article does not contend that current EU law already mandates such technologies. Rather, it shows how the DLT Pilot Regime's existing requirements concerning direct supervisory access, proportionality of exemptions, cybersecurity and confidentiality can supply the legal basis for a less intrusive supervisory architecture that remains faithful to the experimental and technology-neutral character of the Regime.

Keywords: DLT Pilot Regime, embedded supervision, intellectual property tokenisation, trade secrets, proportionality, zero-knowledge proofs, privacy by design, financial market infrastructures

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

International securities settlement and intellectual-property financing share an unglamorous but consequential defect: both still rely, to a significant degree, on intermediated record-keeping that separates the moment a transaction is agreed from the moment it is verified, reconciled and made final [1]. Distributed Ledger Technology (DLT) is often presented as a solution to this defect because it can record ownership, execute contractual conditions and generate a single shared transaction history within one technical environment[1]. In tokenised markets, smart contracts can encode the rules governing transfers and can link the movement of an asset token to the movement of a payment token, which is said to reduce reconciliation and settlement friction considerably[2] [1]. The financial-market implications of this architecture have already attracted substantial academic and regulatory attention, including in the context of tokenised real-world assets, cross-border payments and the competition among different forms of on-chain money [1].

The next question is how this architecture interacts with Intellectual Property (IP). Patents, copyright portfolios, licensing receivables, royalty streams and other IP-related contractual claims are potentially suitable for tokenisation where the token represents a legally enforceable financial entitlement rather than merely a digital label attached to an intangible asset. Tokenisation may make such claims divisible and transferable, and may permit automated distribution of revenues to fractional holders [2]. But IP-intensive transactions differ from many conventional financial assets in one important respect: their value frequently depends on information that the issuer has strong commercial incentives to keep confidential. Pharmaceutical trial data, pricing models, unpublished technical know-how, customer-specific licensing terms and valuation assumptions can be commercially significant even where they are not themselves the tokenised financial instrument.

The regulatory problem is therefore more specific than a general conflict between "blockchain transparency" and privacy. Under Regulation (EU) 2022/858, DLT market infrastructures remain subject to the Union financial-services framework except where specific, temporary exemptions are granted, and the Regulation contains additional requirements concerning technology, cybersecurity, data integrity and supervisory cooperation[3]. In particular, where a DLT Multilateral Trading Facility (DLT MTF) receives an exemption from the transaction-reporting obligation in Article 26 of the Markets in Financial Instruments Regulation (MiFIR), the competent authority must have direct and immediate access to transaction details and is admitted to the DLT MTF as a "regulatory observer participant"[4]. The Regime therefore already contemplates technologically mediated supervisory access. The unresolved question is the scope and granularity of that access when the underlying data environment contains commercially sensitive information about IP-related transactions.

This article asks: how can embedded supervision be incorporated into DLT infrastructures used for IP-related financial instruments without creating unnecessary exposure of trade secrets and other confidential information? The argument proceeds in six steps. First, it situates IP tokenisation within the wider contest among different architectures for tokenised value transfer, drawing on the observation that on-chain assets

[1] Itai Agur and others, 'Tokenization and Financial Market Inefficiencies' (IMF Fintech Note 2025/001, International Monetary Fund, 29 January 2025) 3 https://doi.org/10.5089/9798400298905.063 accessed 20 September 2026.

[2] Agur and others (n 1) 3–4.

[3] Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology [2022] OJ L151/1, arts 1, 4–7.

[4] Regulation (EU) 2022/858 (n 3) art 4(3).

require an on-chain settlement asset whose credibility depends on institutional design rather than on cryptography alone [1]. Secondly, it clarifies what is, and is not, being tokenised and maps IP-related instruments onto the DLT Pilot Regime. Thirdly, it reconstructs embedded supervision as a form of supervisory data architecture and identifies the particular confidentiality risks generated by IP-intensive markets. Fourthly, it applies the Trade Secrets Directive, the General Data Protection Regulation (GDPR) and the EU proportionality principle, while avoiding the stronger claim that every form of direct supervisory access is unlawful. Fifthly, it develops a privacy-by-design model in which supervisors receive the information needed for a specified regulatory purpose through graduated access, cryptographic proofs and controlled disclosure. Finally, it draws out the implications of that model for ESMA guidance, for the design of DLT market infrastructures and for a possible future statutory amendment.

The article makes a methodological point as well. The DLT Pilot Regime is an experiment rather than a completed regulatory settlement. Its purpose is to allow ESMA and national competent authorities to learn how DLT affects market infrastructure and to determine whether existing legislation requires adjustment[5]. Accordingly, the appropriate legal response is not to replace supervision with privacy technology, nor to replace privacy with unrestricted supervisory access, but to redesign the interface between supervision and the ledger so that regulatory objectives are achieved with no more information than is reasonably required.

2. Tokenised money as a precondition for tokenised value

Before an IP-backed token can be usefully analysed as a supervisory problem, it is necessary to recognise that it is, in the first instance, a payments problem. A royalty stream or a licensing receivable is only as efficient, on-chain, as the instrument used to settle it. If the cash leg of a tokenised IP transaction must still travel through a conventional correspondent-banking chain, tokenising the asset leg produces only a partial efficiency gain, because the payment leg continues to be bound by cut-off times, local business hours and multi-jurisdictional compliance screening [1]. This is why the literature on real-world-asset tokenisation increasingly treats the choice of settlement asset, not merely the choice of ledger, as a first-order design question [1].

Three architectures currently compete to supply that on-chain settlement asset: Central Bank Digital Currencies (CBDCs), stablecoins, and tokenised bank deposits [1]. Each carries a different institutional trust structure. A CBDC is a direct liability of the central bank and therefore carries essentially zero credit risk, but, at least in the retail context, its development in leading jurisdictions has recently been constrained by explicit legislative choices, most notably the prohibition on retail CBDC issuance introduced in the United States as part of the broader 2025 shift toward regulated stablecoins[6] [1]. A stablecoin is a private liability whose stability depends on the adequacy and governance of its reserve assets; it can scale quickly and interoperate easily with smart contracts, but its creditworthiness is only as strong as its issuer's reserve management and, in the event of insolvency, the priority its holders are actually given in the issuer's bankruptcy

[5] Regulation (EU) 2022/858 (n 3) recital 53; European Securities and Markets Authority, Report on the DLT Pilot Regime (ESMA70-460-111, 27 September 2022); European Securities and Markets Authority, Report on the Functioning and Review of the DLT Pilot Regime (ESMA75-117376770-460, 25 June 2025). https://www.esma.europa.eu/document/report-dlt-pilot-regime accessed 20 September 2026. https://www.esma.europa.eu/sites/default/files/2025-06/ESMA75-117376770-460_Report_on_the_functioning_and_review_of_the_DLTR_-_Art.14.pdf accessed 20 September 2026.

[6] Anti-CBDC Surveillance State Act of 2025, HR 1919, 119th Cong (2025) (passed House of Representatives, 17 July 2025) https://www.govinfo.gov/app/details/BILLS-119hr1919rh accessed 20 September 2026.

estate[7] [1]. A tokenised bank deposit is a digital representation of a conventional deposit liability, and therefore inherits the prudential regulation, deposit insurance and central-bank backstops that already apply to the issuing bank, while also potentially bearing interest[8] [1].

This taxonomy matters for the present argument for two reasons. The first is architectural: an IP-backed DLT instrument that distributes royalties automatically through a smart contract will typically need to select one of these three settlement assets, and that choice will itself be subject to the DLT Pilot Regime's requirements concerning technology, cybersecurity and data integrity discussed in Part III below[9]. The second reason is conceptual, and it is the more important one for this article. The debate about which digital-money architecture will prevail is, at bottom, a debate about where institutional trust should be located: in cryptographic and market mechanisms alone, as with unbacked cryptocurrencies; in a private issuer subject to a bespoke reserve regime, as with regulated stablecoins; or in the decades-old apparatus of prudential bank regulation, deposit insurance and lender-of-last-resort support, as with tokenised deposits[10]. That same structural choice recurs, in a different guise, when a regulator must decide how much of an IP-backed instrument's supervisory data should be verified through a bespoke cryptographic mechanism, such as a zero-knowledge proof, as against how much should simply be entrusted to the pre-existing, well-tested apparatus of direct supervisory access and professional secrecy obligations. The argument developed in Parts IV to VII below can therefore be read as an application, to supervisory data architecture, of the same institutional-design logic that has already proved decisive in the competition among CBDCs, stablecoins and tokenised deposits: newer cryptographic mechanisms are valuable precisely where they minimise unnecessary disclosure, but they should supplement, rather than replace, the settled and time-tested legal apparatus of prudential and securities regulation [1].

3. IP-related tokenisation and the scope of the DLT Pilot Regime

3.1. The object of tokenisation: IP rights, financial claims and confidential information

IP tokenisation should be separated into three legally distinct layers. The first is the underlying IP right or asset: for example, a patent, a copyright portfolio, or a contractual licence. The second is the legal or economic claim represented by the token, such as a debt claim against a Special-Purpose Vehicle (SPV), a share, a unit in a collective investment undertaking, or a transferable claim to royalties. The third is the information environment supporting valuation, compliance and servicing of that claim. The third layer may contain trade secrets even though the trade secret is not itself the object of the financial instrument.

This distinction matters because trade secrets occupy a different legal position from registered IP rights [3]. Directive (EU) 2016/943 protects undisclosed know-how and business information where it is secret,

[7] Guiding and Establishing National Innovation for US Stablecoins Act, Pub L No 119-27, 139 Stat 419 (2025) ("GENIUS Act") §§ 4, 11.

[8] European Banking Authority, Report on Tokenised Deposits (12 December 2024) 8, 10. https://www.eba.europa.eu/sites/default/files/2024-12/4b294386-1235-463f-b9b5-08f255160435/Report%20on%20Tokenised%20deposits.pdf accessed 20 September 2026.

[9] Regulation (EU) 2022/858 (n 3) art 7.

[10] Bank for International Settlements and others, Central Bank Digital Currencies: Foundational Principles and Core Features (Report, October 2020) 3 https://www.bis.org/publ/othp33.pdf accessed 20 September 2026.

commercially valuable because it is secret, and subject to reasonable steps to keep it secret[11]. A pharmaceutical trial result or a proprietary pricing formula may therefore be protected as a trade secret, but that does not make the information a transferable security. A token may instead represent a financial claim whose value is informed by such information. The legal design should consequently avoid placing the confidential information itself on the ledger merely because the token's value depends upon it.

The economic case for tokenisation is nevertheless significant. Tokenised assets can create a shared record of ownership and can use smart contracts to connect asset transfers with payment, and the resulting reduction in reconciliation and settlement friction is one reason why tokenisation has been identified as a response to structural inefficiencies in conventional financial-market infrastructure[12] [1]. For IP-related assets, the potential use cases include royalty-stream financing, tokenised claims issued by an IP-holding SPV, and programmable distribution of licensing proceeds. The regulatory question is not whether these structures are desirable in the abstract, but whether the financial claim satisfies the applicable definition of a financial instrument.

3.2. When an IP-related token becomes a DLT financial instrument

Regulation (EU) 2022/858 applies to "DLT financial instruments", defined as financial instruments that are issued, recorded, transferred and stored using DLT[13]. The relevant gateway is therefore the existing concept of a financial instrument under the Markets in Financial Instruments Directive (MiFID II), which defines a financial instrument as one of the instruments listed in Section C of Annex I to that Directive, not the label "token" and not the mere existence of an underlying IP asset[14]. An IP-related token can fall within the Regime where, for example, it constitutes a transferable security or another MiFID II financial instrument. A token that merely grants access to software or performs a non-financial utility function does not become a DLT financial instrument simply because it uses blockchain technology.

This point also limits the role of the Markets in Crypto-Assets Regulation (MiCA). Crypto-assets that qualify as financial instruments are outside the core scope of the MiCA framework, and the DLT Pilot Regime was specifically designed to facilitate the testing of DLT market infrastructures for crypto-assets that qualify as financial instruments[15]. The analysis should therefore begin with classification under MiFID II and the DLT Pilot Regime rather than assuming that all IP tokens are regulated in the same way, or that MiCA supplies a residual regulatory home for every instrument that does not fit comfortably within either framework.

Eligibility is further constrained by the Pilot Regime's quantitative thresholds. Article 3 limits, among other things, shares to issuers with a market capitalisation below EUR 500 million and bonds and other forms of securitised debt to an issue size below EUR 1 billion, subject also to aggregate market-value thresholds for the DLT market infrastructure as a whole[16]. An IP-backed structure may therefore enter the Regime through a securitised-debt or equity architecture, but the structure must be designed around the instrument actually

[11]Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) [2016] OJ L157/1, art 2(1).

[12]Agur and others (n 1) 3–4.

[13]Regulation (EU) 2022/858 (n 3) art 2(11)–(12).

[14]Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments [2014] OJ L173/349, art 4(1)(15).

[15]Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets [2023] OJ L150/40, art 2(4); Regulation (EU) 2022/858 (n 3) recitals 6–8.

[16]Regulation (EU) 2022/858 (n 3) art 3(1)–(3).

admitted to trading or recorded, not around the value of the underlying IP portfolio in isolation. A royalty stream from a single blockbuster patent could easily exceed these thresholds even where the tokenised claim itself remains modest, so careful structuring around the recorded instrument, rather than the underlying asset, is a precondition of eligibility.

3.3. What the DLT Pilot Regime actually requires

The DLT Pilot Regime is better understood as a controlled regulatory experiment than as a general exemption from securities regulation. A DLT MTF remains subject to the requirements applicable to an ordinary MTF under MiFID II, subject to specified exemptions and compensatory measures; DLT Settlement Systems (DLT SSs) and DLT Trading and Settlement Systems (DLT TSSs) are similarly connected to the existing MiFIR, MiFID II and Central Securities Depositories Regulation (CSDR) architecture[17]. The operator must also establish rules concerning access to the ledger, the validation of nodes, conflicts of interest and risk management, and must maintain information-technology and cyber arrangements that protect the integrity, security and confidentiality of data[18].

This architecture is important for the present argument because it already contains the seeds of a confidentiality-sensitive supervisory model. The Regulation does not say that every item of information relevant to an IP-backed instrument must be placed in plaintext on a distributed ledger. Nor does it make an unrestricted supervisory node a universal condition of participation. Rather, the most specific access rule arises where a DLT MTF is exempted from Article 26 MiFIR: the competent authority must have direct and immediate access to the transaction details that the DLT MTF is required to keep, and the authority is admitted as a regulatory observer participant[19]. Because the underlying MiFIR transaction-reporting regime is itself designed to give supervisors the information necessary to detect insider dealing and market manipulation under the Market Abuse Regulation (MAR), the substantive content of the transaction record that must be disclosed is already constrained by the purposes that MAR's prohibitions on insider dealing and market manipulation are designed to serve[20].

ESMA's implementation work reinforces this reading. Its 2022 report addressed technical elements of the Regime and compensatory measures concerning supervisory data, while its 2025 review identified legal and technical issues encountered by supervisors and considered how the Pilot Regime might be made more permanent[21]. The regulatory challenge is thus not to invent supervisory access where none exists, but to determine how access should be structured when transaction-level data are embedded in a DLT environment that may also contain commercially sensitive IP information.

[17]Regulation (EU) 2022/858 (n 3) arts 4–6.

[18]Regulation (EU) 2022/858 (n 3) art 7(2)–(4).

[19]Regulation (EU) 2022/858 (n 3) art 4(3).

[20]Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments [2014] OJ L173/84, art 26; Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse [2014] OJ L173/1, arts 7, 8 and 12.

[21]European Securities and Markets Authority (n 5).

4. Embedded supervision as a supervisory architecture

4.1. From periodic reporting to ledger-based supervision

Raphael Auer's embedded-supervision model provides the conceptual starting point for this article. Its central proposition is that DLT can permit compliance with regulatory objectives to be monitored automatically by reading the market's ledger, reducing the need for firms to collect, verify and deliver the same information through separate reporting pipelines [4]. Auer subsequently extended the argument to decentralised finance, emphasising that the design question is not whether a regulator can technically observe a ledger, but which observational capability is actually necessary for a given supervisory objective [4]. The innovation therefore lies less in giving regulators "more data" than in changing the relationship between the source of market data and the supervisory process.

In a conventional reporting system, the regulated entity extracts data, transforms it into a prescribed format, transmits it, and remains responsible for its accuracy. In a DLT environment, the ledger may provide a common source of transaction records, while smart contracts can constrain certain transactions before they occur. Tokenisation therefore creates an opportunity to move from ex-post reconstruction toward continuous verification. Yet embedded supervision is not synonymous with unrestricted visibility. A supervisory system can read a ledger, receive selected events, verify commitments, or request underlying records only when a defined trigger occurs.

This distinction is especially important for IP markets. The regulatory value of a data field depends on the regulatory question being asked. To detect market abuse under MAR, a supervisor may need order, execution and account-level information[22]. To verify a collateralisation threshold, it may need a proof that a condition is satisfied rather than every underlying licensing contract. To investigate a suspected manipulation event, it may need targeted access to underlying evidence, including the arrangements and procedures that a trading-venue operator is itself required to maintain under Article 16 MAR to detect and report suspicious orders and transactions[23]. A legally coherent architecture should therefore match the granularity of access to the supervisory purpose, rather than treating "full ledger visibility" as the default position from which exceptions must be justified.

4.2. The DLT Pilot Regime's regulatory-observer mechanism

Article 4(3) of Regulation (EU) 2022/858 is particularly significant. Where an exemption from Article 26 MiFIR is granted, the DLT MTF must keep transaction records containing the relevant details and must ensure that competent authorities have direct and immediate access to those details; the competent authority is admitted as a regulatory observer participant[24]. This is close to an embedded-supervision architecture, but it is narrower than the proposition that the regulator should possess a full, unfiltered copy of every item of commercial information associated with the token.

The provision also demonstrates why a blanket privacy objection would be too broad. The DLT Pilot Regime deliberately prioritises immediate supervisory access to transaction information in the context of a

[22]Regulation (EU) No 600/2014 (n 20) art 26.

[23]Regulation (EU) No 596/2014 (n 20) art 16.

[24]Regulation (EU) 2022/858 (n 3) art 4(3).

particular exemption. The legal issue is therefore one of scope, purpose and architecture. Where the required transaction record itself contains no trade secret, direct access may create little additional confidentiality risk. Where the DLT implementation stores additional data beyond what is legally required for transaction reporting, however, the operator should not assume that the statutory requirement to provide access to transaction data also authorises unrestricted access to unrelated confidential information.

That distinction can be expressed as a data-governance principle: the supervisory interface should expose the regulatory record, not necessarily the entire information environment in which the regulatory record is produced. This is the point at which embedded supervision and privacy by design become complementary rather than opposing concepts, and it is also the point at which the institutional-trust analysis developed in Part II becomes operative: the regulator does not need cryptographic assurance for information it is already entitled to see directly under Article 4(3), and cryptographic techniques should instead be reserved for information that lies outside the required transaction record.

4.3. Why IP-intensive markets create a special confidentiality problem

IP-related markets intensify the problem because the information surrounding an instrument can itself have economic value. A royalty-backed security may depend on confidential licensing schedules; a patent-backed financing may depend on non-public valuation assumptions; and a technology-transfer transaction may involve technical know-how that is not disclosed in the patent register. If such information is unnecessarily replicated across nodes or incorporated into persistent transaction metadata, the ledger can transform a regulatory disclosure into a durable commercial information store.

DLT's immutability also changes the risk profile [5]. Conventional confidential filings can be corrected, restricted, archived or deleted according to applicable retention rules. A ledger record, by contrast, may remain accessible to authorised nodes or other participants long after the immediate supervisory purpose has expired. The legal problem is not that immutability automatically destroys secrecy. Rather, immutability makes initial data minimisation and access control more important, because a later attempt to cure over-disclosure may be technically difficult or, on a public or widely permissioned chain, practically impossible.

The DLT Pilot Regime itself recognises the need for confidentiality and cybersecurity. Its recital 41 and Article 7 require information-technology and cyber arrangements that ensure, among other things, the integrity, security and confidentiality of data[25]. The Regulation therefore supplies an internal regulatory basis for treating confidentiality as part of DLT market-infrastructure design, rather than as an external concern that must be sacrificed to supervisory efficiency.

5. Trade secret protection, data protection law and the limits of disclosure

5.1. Article 2(1) of the Trade Secrets Directive

Directive (EU) 2016/943 defines a trade secret cumulatively. The information must be secret in the relevant sense, have commercial value because it is secret, and have been subject to reasonable steps to keep it secret[26]. This definition creates an important analytical constraint on the present argument. It would be incorrect to say that any disclosure to a regulator automatically destroys trade-secret status. The Directive itself contemplates lawful acquisition, use and disclosure in specified circumstances, and a controlled

[25]Regulation (EU) 2022/858 (n 3) recital 41 and art 7(4).

[26]Directive (EU) 2016/943 (n 11) art 2(1).

disclosure to an authority under confidentiality obligations is not equivalent to publication to competitors. At the same time, the "reasonable steps" requirement gives the technical design of tokenisation legal significance. If a firm voluntarily places plaintext trade-secret information on a ledger accessible to a large group of network participants when the same regulatory purpose could be achieved by keeping the information off-chain, that design choice may complicate a later argument that adequate secrecy measures were taken. The better conclusion is therefore conditional: ledger disclosure does not automatically forfeit trade-secret protection, but an architecture that unnecessarily multiplies access may weaken the holder's ability to demonstrate reasonable steps to maintain secrecy within the meaning of Article 2(1)(c) of the Directive[27].

This distinction materially improves upon a simple conflict model. The Trade Secrets Directive does not create an absolute right to keep all commercially sensitive information from regulators. Instead, it creates a protected legal interest in secrecy, subject to lawful disclosure and other statutory conditions. The regulatory design question is accordingly whether supervisory access can be targeted and secured while preserving the secrecy measures required by Article 2(1)(c).

5.2. Regulatory confidentiality is not a substitute for data minimisation

Professional-secrecy obligations can reduce the risk of secondary disclosure, but they do not solve the architectural problem created by excessive collection. Even where a competent authority is legally bound to protect confidential information, the information has still been copied into another institutional environment, becomes subject to the regulator's retention and cybersecurity arrangements, and may become relevant to future administrative, judicial or supervisory processes.

The DLT Pilot Regime consequently should not be interpreted on the assumption that regulatory secrecy eliminates the need for technical confidentiality. Article 7 requires the DLT infrastructure itself to maintain data confidentiality and accessibility, while the Regulation's broader supervisory framework requires cooperation and reporting between operators, competent authorities and ESMA[28]. These obligations point toward layered controls rather than a binary choice between transparency and secrecy.

A particularly important safeguard is purpose limitation at the system-design level. A supervisory node should be configured to receive only the classes of data that are necessary for a defined regulatory function. Where an automated compliance condition can be expressed as a mathematical predicate, such as "the collateralisation ratio exceeds the required threshold", the regulatory system should consider whether verification of the predicate can substitute for disclosure of the underlying confidential inputs. The legal advantage is not that the regulator becomes blind, but that the regulator receives evidence proportionate to the regulatory question.

5.3. The General Data Protection Regulation as a complementary, not merely analogous, source of principle

The confidentiality problem addressed in this article is conceptually distinct from the protection of personal data, because trade secrets are commercial rather than personal information. Nevertheless, where an IP-related DLT infrastructure processes personal data, for example the identity of licensees, inventors or beneficial owners recorded on the ledger for anti-money-laundering purposes, the GDPR applies directly and supplies more than a loose analogy for the privacy-by-design model proposed here. Article 5(1)(c) GDPR requires that

[27]Directive (EU) 2016/943 (n 11) art 2(1)(c).

[28]Regulation (EU) 2022/858 (n 3) arts 7 and 12.

personal data be adequate, relevant and limited to what is necessary in relation to the purposes for which it personal data be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed, a principle usually described as data minimisation[29]. Article 25 GDPR requires the controller to implement appropriate technical and organisational measures, such as pseudonymisation, designed to implement data-protection principles effectively, both at the time of determining the means of processing and at the time of the processing itself; this is the statutory source of the phrase "data protection by design and by default", from which the wider concept of "privacy by design" used in this article is derived[30]. The Charter of Fundamental Rights independently protects personal data under Article 8, alongside intellectual property under Article 17(2) and the freedom to conduct a business under Article 16[31].

The relevance of the GDPR to this article is therefore twofold. First, where an IP-related DLT infrastructure does process personal data, Articles 5(1)(c) and 25 GDPR impose an independent, directly applicable legal requirement to minimise data collection and to embed data-protection safeguards into the technical architecture, reinforcing rather than merely paralleling the confidentiality obligations under Article 7 of the DLT Pilot Regime. Secondly, and more generally, the GDPR demonstrates that EU law already possesses a mature statutory vocabulary and enforcement infrastructure for translating an abstract principle of minimisation into binding technical design obligations. That vocabulary, and the accumulated supervisory practice built around it, is a more secure legal foundation for the privacy-by-design model proposed in Part VII than an appeal to technological best practice alone.

6. Proportionality: from abstract principle to supervisory design

6.1. The correct constitutional framework

The starting point of this analysis is not to overstate the role of Article 5(4) of the Treaty on European Union (TEU). Article 5 TEU states the principles of conferral, subsidiarity and proportionality, and Article 5(4) provides that, under the principle of proportionality, the content and form of Union action must not exceed what is necessary to achieve the objectives of the Treaties[32]. It is therefore a constitutional constraint on Union action. It should not be presented as though every technical decision by every national competent authority is automatically an act governed directly by Article 5(4) in the same way as an EU legislative measure.

Nevertheless, proportionality is highly relevant to the DLT Pilot Regime because the Regulation itself expressly incorporates proportionality into its own design. The Regulation states that its objectives should be achieved consistently with proportionality, and specific exemptions must be proportionate and justified by the use of DLT[33]. The proportionality inquiry is therefore both constitutional in a general sense and internal to the statutory architecture of the Regime.

The familiar approach of the Court of Justice of the European Union (CJEU) can be structured around suitability, necessity and proportionality in the strict sense [6]. Fedesa confirms the proportionality principle in EU law while recognising a degree of legislative discretion where complex policy choices

[29]Regulation (EU) 2016/679 (n 29) art 25.Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L19/1, art 5(1)(c).

[30]Regulation (EU) 2016/679 (n 29) art 25.

[31]Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 8, 16 and 17.

[32]Consolidated version of the Treaty on European Union [2012] OJ C326/13, art 5(4).

[33]Regulation (EU) 2022/858 (n 3) recital 55 and arts 4(4), 5(10) and 7.

are involved[34]. Digital Rights Ireland demonstrates that measures involving large-scale access to information must be assessed against the availability of safeguards and the extent of the interference[35]. Schrems II confirms that this proportionality analysis extends to the transfer of information to institutions whose subsequent handling of that information the data subject cannot fully control, a consideration directly relevant to any regulatory architecture that copies commercially sensitive information into a supervisory authority's own systems[36]. In the present context, the question is not whether supervision is legitimate; it plainly is. The question is whether the same supervisory objective can be achieved with less intrusive access to commercially sensitive information.

6.2. Suitability

Direct access to transaction data is suitable for many DLT market-supervision purposes. A supervisor cannot effectively monitor market integrity if it cannot obtain reliable information about orders and transactions. The DLT Pilot Regime itself recognises this by requiring direct and immediate access to relevant transaction details where the Article 26 MiFIR exemption is used[37]. Ledger-based supervision can also reduce reconciliation costs and improve the timeliness of supervisory information, which is central to Auer's embedded-supervision model [4].

The suitability stage therefore does not resolve the confidentiality problem. A measure may be suitable while still being unnecessary or excessive. The fact that a full ledger can provide more information than a targeted supervisory feed does not establish that all of that information is needed to satisfy the objectives of MiFID II, MiFIR, MAR or CSDR[38].

6.3. Necessity and the least-intrusive supervisory interface

Necessity is where privacy-preserving architecture becomes legally significant. Suppose a DLT MTF must demonstrate that a portfolio backing a tokenised IP debt instrument maintains a specified collateralisation ratio. Three supervisory designs are possible. The first gives the regulator plaintext access to every underlying licensing contract and valuation input. The second gives the regulator a structured data feed containing only the variables required to calculate the ratio. The third gives the regulator a cryptographic proof that the ratio exceeds the prescribed threshold, with the underlying evidence retained off-chain and available under a targeted disclosure procedure.

If all three designs are technically reliable and legally auditable, the first is difficult to justify as necessary merely because it is administratively convenient. The relevant test is not whether full access makes supervision easier, but whether less intrusive access can achieve the same regulatory objective. This is consistent with the DLT Pilot Regime's own requirement that exemptions and compensatory measures be

[34]Case C-331/88 The Queen v Minister of Agriculture, Fisheries and Food, ex parte Fedesa [1990] ECR I-4023, ECLI:EU:C:1990:391.

[35]Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others ECLI:EU:C:2014:238.

[36]Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ECLI:EU:C:2020:559.

[37]Regulation (EU) 2022/858 (n 3) art 4(3).

[38]Directive 2014/65/EU (n 14); Regulation (EU) No 600/2014 (n 20); Regulation (EU) No 596/2014 (n 20); Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories [2014] OJ L257/1.

proportionate to the use of DLT[39].

Necessity should, however, be assessed dynamically. Zero-knowledge proofs are not a universal replacement for underlying evidence. A supervisor conducting a market-abuse investigation under Articles 8 and 12 MAR may need transaction histories, communications or other evidence that cannot be compressed into a single compliance predicate.[40] The proposed model therefore uses a hierarchy: proof-based verification for routine conditions; structured disclosure for defined supervisory needs; and full underlying disclosure only where a legal trigger, such as a formal investigation or enforcement procedure, justifies it.

6.4. Proportionality stricto sensu

The final balancing stage asks whether the benefits of a supervisory measure justify its interference with protected interests. For IP-intensive financial markets, the relevant interests include the commercial value of secrecy, the freedom to conduct a business, and the protection of property, including intellectual property. Article 17(2) of the Charter expressly recognises intellectual property as protected property, while Article 16 protects the freedom to conduct a business, and Article 8 protects personal data where it is present in the same information environment[41].

The balancing exercise should not be framed as "trade secrets versus financial stability". Such a formulation treats the interests as if one must defeat the other. The more defensible approach is institutional design: financial stability and market integrity are protected by ensuring that the regulator can verify the relevant conditions, while trade-secret interests are protected by limiting the quantity, persistence and distribution of information needed to perform that verification.

Accordingly, the strongest legal claim is not that a full-data supervisory interface is per se ultra vires. The stronger and more defensible proposition is that, where a less intrusive architecture can deliver equivalent supervisory assurance, a requirement for indiscriminate access to commercially sensitive information is vulnerable to a proportionality challenge. The burden is therefore shifted toward justification of data granularity rather than toward a categorical prohibition of supervisory access.

7. Privacy-by-design embedded supervision

7.1. A four-layer architecture

This article proposes a four-layer model for IP-related DLT market infrastructures. Layer 1 is the public or participant-facing ledger layer, containing only the information necessary for transfer, settlement and legally required transparency. Layer 2 is a permissioned supervisory layer through which the competent authority receives the transaction data it is legally entitled to access under Article 4(3) of the DLT Pilot Regime[42]. Layer 3 is a privacy-preserving compliance layer, in which cryptographic commitments, zero-knowledge proofs or confidential computations demonstrate compliance with specified rules. Layer 4 is a protected evidence layer holding the underlying confidential contracts, valuation models and technical records off-chain, subject to targeted disclosure.

[39]Regulation (EU) 2022/858 (n 3) arts 4(4) and 5(10).

[40]Regulation (EU) No 596/2014 (n 20) arts 8 and 12.

[41]Charter of Fundamental Rights of the European Union (n 31) arts 8, 16 and 17.

[42]Regulation (EU) 2022/858 (n 3) art 4(3).

This architecture separates "verification" from "inspection". Routine supervision is based on verifiable compliance states. Inspection of underlying evidence remains possible, but it is triggered by a defined supervisory purpose rather than by the mere existence of a tokenised instrument. The model therefore preserves the central insight of embedded supervision, namely automatic and continuous monitoring, while rejecting the assumption that automatic monitoring requires automatic disclosure of every input [4].

7.2. Zero-knowledge proofs

Zero-Knowledge Proofs (ZKPs) are particularly suitable where the regulatory requirement can be expressed as a verifiable proposition [7]. In a simplified example, an issuer could prove that the value of eligible collateral exceeds a required threshold without revealing the complete valuation dataset to every participant in the market. The same logic could support range proofs, eligibility conditions or concentration limits [8]. Auer's work is useful here because it treats the ledger as a source from which compliance can be monitored; ZKPs extend that insight by asking whether the compliance statement itself can be verified without exposing all underlying data [4].

Yet ZKPs should be treated as a compliance tool, not as a legal conclusion. EU financial law does not currently provide a general rule stating that a valid zero-knowledge proof automatically satisfies every reporting or supervisory obligation. The legal architecture must therefore specify which regulatory predicates can be proved, what cryptographic standards are acceptable, how proof systems are audited, and when the underlying evidence must be disclosed.

The most important use of ZKPs in the present context is consequently not "absolute privacy". It is minimisation, in the same sense used by Article 5(1)(c) GDPR[43]. The regulator receives the minimum information required to establish a specified fact, while the issuer retains the confidential inputs under controlled access. This better matches the proportionality principle discussed in Part VI because the supervisory information becomes function-specific rather than exhaustive.

7.3. Confidential computation, off-chain storage and permissioned access

Fully Homomorphic Encryption (FHE) and other confidential-computation techniques may complement ZKPs where the supervisory task requires computation over sensitive inputs rather than proof of a simple predicate.

In principle, encrypted values can be processed without first exposing the plaintext to the computing environment [9]. The legal importance of such tools is that they can reduce the number of environments in which confidential information must be readable, a consideration that is analytically similar to the way blockchain-based payment infrastructures were themselves designed to reduce the number of intermediary banks that must handle a payment message before final settlement [1].

However, the article does not treat FHE as a mature universal solution. Computational cost, implementation complexity, key management and auditability can make some applications unsuitable. A publishable regulatory framework should therefore be technology-neutral: the law should specify the confidentiality and assurance outcomes required, while allowing different cryptographic implementations to compete to satisfy those outcomes, an approach consistent with the technology-neutral orientation that NIST's own technical overview of blockchain technology attributes to sound distributed-ledger governance[44].

[43]Regulation (EU) 2016/679 (n 29) art 5(1)(c).

[44]Dylan Yaga, Peter Mell, Nik Roby and Karen Scarfone, Blockchain Technology Overview (NISTIR 8202, National Institute of Standards and Technology, October 2018) https://doi.org/10.6028/NIST.IR.8202 accessed 20 September 2026.

Off-chain storage is similarly important. The DLT ledger should record the minimum commitment or state necessary to establish the legal and financial position of the token. The detailed licensing contract, valuation model or technical file can remain in a secure repository governed by contractual and regulatory access rules. The ledger can then contain a cryptographic commitment to the off-chain record, allowing a later disclosure to be checked against the state that existed at the relevant time. This preserves auditability without making the entire evidence set permanently visible.

Permissioned ledger governance should reinforce this architecture. The DLT Pilot Regime already requires rules concerning access to the distributed ledger and the participation of validating nodes[45]. A regulatory observer node should therefore be logically separated from validation functions and configured according to the supervisor's statutory purpose. Access logs, role-based permissions, cryptographic key separation and independent security audits should be treated as part of the market infrastructure's regulatory controls rather than as optional technical features.

7.4. A graduated disclosure matrix

The following matrix summarises the proposed relationship between supervisory purpose, preferred data form, the location of underlying data, and the trigger that escalates access to fuller disclosure[46].

Table 1. Tiered supervisory access: data forms and escalation triggers

Supervisory purpose	Preferred data form	Underlying data	Escalation trigger
Routine transaction monitoring	Structured transaction record / direct observer access	Retained by operator	Anomaly or formal request
Threshold / collateral verification	ZK proof or limited structured variables	Off-chain evidence	Proof failure or investigation
AML / KYC eligibility	Credential or compliance assertion	Identity records held by authorised entity[47]	Regulatory or legal trigger
Market-abuse investigation	Targeted transaction history and evidence[48]	Full relevant evidence set	Formal supervisory investigation
Cyber / operational incident	Incident metadata and forensic evidence[49]	Protected technical logs	Material incident / audit

The matrix illustrates the central design principle. Direct access is retained where the Regulation expressly requires it, while additional confidential information is not automatically exposed merely because it exists within the same technical environment. The model also preserves supervisory escalation: a proof failure, anomaly, material incident or formal investigation can unlock additional evidence under defined legal controls (see Table 1).

[45]Regulation (EU) 2022/858 (n 3) art 7(2).

[46]Regulation (EU) 2022/858 (n 3) art 4(3).

[47]Regulation (EU) 2016/679 (n 29).

[48]Regulation (EU) No 596/2014 (n 20) arts 8 and 12.

[49]Regulation (EU) 2022/858 (n 3) art 7.

8. The money side of the ledger: choosing a settlement asset for IP-backed DLT instruments

The analysis in Parts IV to VII concerns the confidentiality of information about a tokenised IP claim. It is worth returning briefly to the point made in Part II, because the choice of settlement asset for that same instrument raises a structurally similar institutional question and has direct consequences for the supervisory architecture proposed above.

Where an IP-backed DLT instrument settles in a stablecoin, the supervisor's confidence in the finality of a royalty distribution depends on the adequacy of the stablecoin issuer's reserves and on the priority that stablecoin holders would actually receive in the issuer's insolvency, a question that remains only partially resolved even under the most developed statutory frameworks currently in force[50] [1]. Where the same instrument settles in a tokenised bank deposit, the supervisor's confidence instead rests on the prudential regulation, deposit insurance and resolution regime that already apply to the issuing bank, an architecture that commentators addressing tokenised deposits directly have identified as more time-tested than a bespoke stability mechanism designed and operated by a single private issuer[51] [1]. A CBDC-settled instrument would rest the same confidence directly on the central bank's own balance sheet, although the practical availability of that option for cross-border, privately issued IP instruments will depend on jurisdiction-specific policy choices of the kind that have recently narrowed the role of retail CBDCs in some major markets [1].

This is not a marginal technical detail. Where the settlement leg of an IP-backed instrument depends on a privately issued stablecoin whose reserve adequacy is not directly supervised in the same manner as a bank's balance sheet, the case for direct, unmediated supervisory access to the settlement data becomes correspondingly stronger, because there is no equivalent prudential backstop standing behind the payment leg of the transaction. Conversely, where the settlement leg uses a tokenised deposit issued by a prudentially regulated bank, part of the supervisory assurance that would otherwise have to be reconstructed from ledger data is already supplied by the bank's existing regulatory relationship with its own supervisor, which arguably reduces the marginal need for additional, IP-specific ledger visibility over the payment leg itself[52] [1]. A privacy-by-design supervisory architecture for IP tokenisation should therefore treat the choice of settlement asset as an input into the proportionality analysis developed in Part VI, rather than as a question that belongs to an entirely separate area of payments law.

9. Regulatory implications and recommendations

9.1. ESMA should develop outcome-based guidance on supervisory data

ESMA should clarify the relationship between the transaction records that must be directly accessible under the DLT Pilot Regime and additional data that an operator may hold in the same technical environment. The objective should be to distinguish legally required supervisory data from optional business or IP data. ESMA's existing work on supervisory data and the functioning of the DLT Pilot Regime provides a natural institutional basis for this clarification[53].

[50]GENIUS Act (n 7) §§ 4 and 11.

[51]European Banking Authority (n 8) 8, 10.

[52]European Banking Authority (n 8) 10.

[53]European Securities and Markets Authority (n 5).

Such guidance should adopt a functional taxonomy. "Required supervisory data" would cover the information expressly required by MiFIR, MiFID II, the DLT Pilot Regime and applicable market-abuse rules[54]. "Supporting confidential data" would include valuation models, licensing agreements and technical records that may substantiate a compliance assertion but are not themselves part of the routine supervisory record. The latter should normally remain off-chain or behind a controlled disclosure layer.

9.2. Supervisory technology should be assessed by assurance, not novelty

Regulators should avoid prescribing a single cryptographic technology. Instead, accreditation should focus on measurable outcomes: completeness of the relevant supervisory record; integrity of the data source; resistance to tampering; proof-system soundness; auditability; key-management security; and a legally enforceable route to underlying evidence when required. This approach is consistent with the technology-neutral orientation of EU financial-services legislation and with the DLT Pilot Regime's emphasis on adapting regulation without weakening investor protection, market integrity or financial stability[55].

A technology-neutral approach is especially important because the technical trade-offs differ across use cases. ZKPs may be efficient for discrete compliance predicates; confidential computation may be more suitable for certain aggregate calculations; and ordinary encryption with controlled access may remain the best solution for other records. The legal requirement should be confidentiality proportionate to risk, not technological novelty, an approach that mirrors the way blockchain-based payment experiments more generally strained at scale and produced volatile fee dynamics precisely when a single technical mechanism was expected to solve every problem at once[56] [1].

9.3. The Trade Secrets Directive should inform infrastructure design

IP-intensive issuers should be able to demonstrate reasonable steps to maintain secrecy through their DLT governance documentation. Those steps should include data classification, decisions about what is stored on-chain, access-control policies, retention rules, cryptographic protection, incident response and procedures for targeted regulatory disclosure. This would make the "reasonable steps" requirement in Article 2(1)(c) of the Trade Secrets Directive operationally visible rather than leaving it to post-dispute inference[57].

At the same time, regulators should recognise that lawful supervisory disclosure is compatible with trade-secret protection where appropriate confidentiality safeguards are maintained. The aim is therefore not to create a safe harbour that immunises all DLT operators from trade-secret obligations, but to align regulatory expectations with demonstrable secrecy controls.

9.4. A future statutory amendment should codify the principle, not the algorithm

If the Pilot Regime becomes permanent, as ESMA's 2025 review already contemplates[58], the EU legislature should consider an explicit principle of privacy-preserving supervision for DLT market infrastructures. The

[54]Regulation (EU) No 600/2014 (n 20); Directive 2014/65/EU (n 14); Regulation (EU) 2022/858 (n 3); Regulation (EU) No 596/2014 (n 20).

[55]Regulation (EU) 2022/858 (n 3) recital 6 and arts 4–7.

[56]Bank for International Settlements, Annual Economic Report 2018 (June 2018) 99–101 https://www.bis.org/publ/arpdf/ar2018e.pdf accessed 20 September 2026.

[57]Directive (EU) 2016/943 (n 11) art 2(1)(c).

[58]European Securities and Markets Authority (n 5).

provision should require that supervisory access be adequate to meet applicable regulatory objectives and proportionate to the sensitivity of the information, while permitting cryptographic proofs, confidential computation and other equivalent technical mechanisms, in a manner analogous to the way Article 25 GDPR already requires data-protection safeguards to be built into processing systems by design rather than added afterwards[59].

An algorithm-specific statutory safe harbour would be premature. Technology changes faster than legislation, and a statutory reference to a particular ZKP construction or encryption scheme could quickly become obsolete. A better legislative formulation would recognise certified privacy-preserving supervisory mechanisms as equivalent where they provide the regulator with demonstrable assurance and preserve a legally enforceable route to underlying evidence.

10. Limitations and directions for future research

This article has three principal limitations, each of which suggests a direction for further work. First, the analysis is doctrinal rather than empirical: it does not measure the actual frequency with which DLT MTF operators currently store IP-related confidential information on-chain, and a systematic survey of live DLT Pilot Regime authorisations, of the kind ESMA is well placed to conduct as part of its ongoing review of the Regime, would allow the proportionality analysis in Part VI to be tested against observed practice rather than against a hypothetical collateral-verification example[60]. Secondly, the article treats zero-knowledge proofs and confidential computation largely as legal design categories rather than as fully specified cryptographic protocols; a technical implementation study, ideally conducted jointly by legal scholars and cryptographers, would be needed before any of the specific mechanisms proposed in Part VII could be recommended for supervisory accreditation. Thirdly, the comparative analysis in Part II and Part VIII draws primarily on the contest among CBDCs, stablecoins and tokenised deposits as it has developed in the United States and the European Union; further research could usefully examine whether jurisdictions that have pursued wholesale CBDC projects more aggressively, for example through multi-central-bank experiments of the kind conducted before the 2025 shift in US policy, would support a different allocation of institutional trust for the settlement leg of an IP-backed DLT instrument[61] [1]. None of these limitations undermines the central claim of the article, which is architectural and proportionality-based rather than empirical, but they mark the boundary of what doctrinal analysis alone can establish.

11. Conclusion

The DLT Pilot Regime creates a useful laboratory for testing a new relationship between financial supervision and market infrastructure. For IP-related financial instruments, that relationship exposes a distinctive tension. The same DLT architecture that can reduce information asymmetry and improve supervisory timeliness can also make confidential information more persistent and more widely accessible than is necessary for the regulatory task.

[59]Regulation (EU) 2016/679 (n 29) art 25.

[60]European Securities and Markets Authority (n 5).

[61]Bank for International Settlements, "Project mBridge Reaches Minimum Viable Product Stage and Invites Further International Participation" (Media Release, 5 June 2024) https://www.bis.org/media-releases/20240605-project-mbridge-reaches-minimum-viable-product-stage-and-invites-further-international accessed 20 September 2026.

The solution is not to reject embedded supervision. Auer's insight remains compelling: where the ledger can provide reliable evidence of market activity and compliance, supervision can be integrated into the infrastructure rather than reconstructed through repetitive reporting [4]. Nor is the solution to treat trade-secret protection as an absolute bar to regulatory access. The DLT Pilot Regime expressly requires direct and immediate access to relevant transaction details in specified circumstances, and financial-market regulation necessarily depends upon effective supervisory powers.

The appropriate reconciliation is architectural, and it is, in an important sense, the same reconciliation that the wider tokenised-money literature has already reached by a different route. Just as the most durable form of tokenised money is likely to be the one that inherits, rather than replaces, the decades of prudential regulation, deposit insurance and central-bank support that already underpin conventional bank deposits[62] [1], the most durable supervisory architecture for tokenised IP claims is likely to be the one that inherits, rather than replaces, the existing legal apparatus of transaction reporting, professional secrecy, trade-secret protection and data-protection law, while using new cryptographic tools only where they genuinely reduce unnecessary disclosure. The supervisory interface should distinguish transaction data from confidential supporting evidence; use permissioned access and role-based controls; retain detailed IP information off-chain where possible; use cryptographic commitments and, where appropriate, zero-knowledge proofs or confidential computation for routine compliance verification; and reserve full evidentiary disclosure for defined supervisory triggers. This model preserves the real-time character of embedded supervision while reducing unnecessary disclosure.

Legally, the argument is therefore one of proportionality and institutional design rather than categorical invalidity. Article 5(4) TEU, the Charter, the Trade Secrets Directive, the GDPR and the DLT Pilot Regime point toward a supervisory architecture in which regulatory objectives are pursued effectively but not through indiscriminate data collection[63]. The Pilot Regime itself already requires proportionality, cybersecurity, confidentiality and appropriate access arrangements. The next step is to make those principles explicit in the technical design of DLT market infrastructures, and to do so before, rather than after, IP-intensive issuers have already committed to ledger architectures that cannot easily be redesigned once large volumes of confidential information have been recorded.

If the European Union can develop such an approach, IP-related tokenisation need not choose between market integrity and commercial secrecy. The more significant regulatory innovation would be to make the two objectives mutually reinforcing: a market in which compliance is continuously verifiable, while the commercially valuable information that supports the market remains confidential unless and until disclosure is legally justified.

References

[1] Buckley, R. P. (2026). The contest between central bank digital currencies, stablecoins, and tokenized deposits: Which will likely win, and why? *Capital Markets Law Journal, 21*(2), kmag012. https://doi.org/10.1093/cmlj/kmag012

[2] De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press. https://doi.org/10.4159/9780674985933

[62]European Banking Authority (n 8) 8, 10.

[63]Treaty on European Union (n 32) art 5(4); Charter of Fundamental Rights of the European Union (n 31); Directive (EU) 2016/943 (n 11); Regulation (EU) 2016/679 (n 29); Regulation (EU) 2022/858 (n 3).

[3] Lemley, M. A. (2008). The surprising virtues of treating trade secrets as IP rights. *Stanford Law Review, 61*(2), 311–354.

[4] Auer, R. (2019). Embedded supervision: How to build regulation into decentralised finance (BIS Working Paper No 811, September 2019, revised May 2022; also issued as CESifo Working Paper No 9771, May 2022). https://www.bis.org/publ/work811.pdf; https://www.ifo.de/DocDL/cesifo1_wp9771.pdf

[5] Finck, M. (2018). *Blockchain regulation and governance in Europe*. Cambridge University Press. https://doi.org/10.1017/9781108609708

[6] Barak, A. (2012). *Proportionality: Constitutional rights and their limitations*. Cambridge University Press. https://doi.org/10.1017/CBO9781139035293

[7] Goldwasser, S., Micali, S., & Rackoff, C. (1985). The knowledge complexity of interactive proof-systems. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing* (pp. 291–304). ACM. https://doi.org/10.1145/22145.22178

[8] Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., & Maxwell, G. (2018). Bulletproofs: Short proofs for confidential transactions and more. In *2018 IEEE Symposium on Security and Privacy* (pp. 315–334). IEEE. https://doi.org/10.1109/SP.2018.00020

[9] Gentry, C. (2009). *A fully homomorphic encryption scheme* (PhD dissertation, Stanford University). https://crypto.stanford.edu/craig/craig-thesis.pdf