



DARTE SERIES

London 3.0

The London 3.0 edition of the DARTE Series was held on 7 September 2026 at the House of Lords, London, in collaboration with the European Commission. We extend our gratitude to the Blockchain Game Alliance, DAAvern, the European Commission and the Institute of Free Technology for their support of this roundtable.

The DARTE Series, initiated by Mariana de la Roche Wills (BlackVogel) and Dr. Nina-Luisa Siedler (siedler legal), brings together regulators, practitioners, public authorities and academia for in-depth dialogue on the regulation of digital assets. Sessions result in public reports and specific calls to action. The session opened with welcome notes from Baroness Uddin and Yasmina Kazitani.

London 3.0 departed from the usual DARTE structure in one respect. Where a session normally covers three topics, this edition concentrated on a single question: financial confidentiality as a foundation of property rights and competitive markets. The topic was introduced by Dr. Agata Ferreira of the Institute of Free Technology, who set out three connected problem areas that framed the discussion.

This report consolidates the insights from the discussion. The perspectives and conclusions presented here represent the collective understanding of the topics discussed. They do not reflect the individual positions of any participant.



The opening: a presumption that was inverted

The session opened from a historical position rather than a technical one. In British legal tradition, lawful financial affairs were presumed confidential and disclosure required a specific reason. When income tax was introduced in 1799 to fund the Napoleonic wars, Parliament objected to its inquisitorial character and attached elaborate safeguards for secrecy. When the tax was restructured in 1803, it was divided into schedules according to the source of income, so that no single official held a complete picture of any taxpayer's affairs. When it was abolished in 1816, Parliament required the destruction of the identifying returns, on the reasoning that accumulated records invite abuse.

The presumption was never an absence of disclosure duties. It was an allocation of the burden. The party seeking disclosure carried it, and the party seeking confidentiality did not.

Over roughly four decades that allocation has been reversed. Reporting thresholds, suspicious activity reporting, automatic exchange of account information, beneficial ownership registers, transfer of funds rules and now cryptoasset reporting frameworks were each justified on their own terms. None of them intended the cumulative effect. Participation in the financial system now implies exposure as a standing condition, and confidentiality is the position that requires justification.

Public distributed ledgers are the end point of that trajectory. Every previous financial system, from ledger books to telegraphs to wire transfers to clearing

houses, was confidential by default with disclosure as the regulated exception. Public ledgers reversed that relationship completely. Publication is permanent, global and indiscriminate, and what is disclosed cannot be withdrawn. Information that is pseudonymous today can be attributed tomorrow, retrospectively and across the entire history.

There has never been a medium in the history of money or of communication that exposed everything about everyone to everyone else, forever.

What was not anticipated when these systems were designed was how effectively analytics would strip away the pseudonymity that made the transparency trade-off tolerable in the first place. A point from the floor qualified this. Public verifiability is itself valuable and should not be surrendered, and privacy-preserving technologies do not remove it. What changed was that the growth of compliance and reporting obligations turned public verifiability into a form of exposure that did not exist in that dimension when these systems were built.

- **Disentangling what is meant by privacy**

The analytical move that shaped the rest of the session was to stop treating privacy as one thing. Much of the apparent conflict between confidentiality and supervision dissolves once two distinctions are made:

- between the layers of the technology stack, and

- between the different things the word privacy is being used to describe.

Participants separated three kinds of confidentiality.

1. Content. Amounts, terms and counterparties. This is ordinary commercial confidentiality of the kind every financial system has always maintained.

2. Participation. Who communicates with whom, and who operates the infrastructure. This is principally a security property, because it removes the targets an attacker or a coercing party would otherwise use. Analytics firms obtain substantial information from network topology without ever breaking encryption.

3. Substance of the activity. This is semantic and circumstance-specific, and covers financial and non-financial activity alike. People vote, associate and send messages privately in ordinary life, and these are different acts subject to different considerations. This category sits outside the scope of the AML rules usually invoked to characterise all on-chain activity.

The same distinction clarifies where obligations attach. Data protection law addresses those who determine how personal data is processed. Financial regulation addresses intermediaries at the point of their interaction with customers. **Neither requires the underlying infrastructure to be public.**

A parallel with encryption ran through the discussion and was returned to

repeatedly. Encrypted traffic between a customer and their bank has never obstructed the bank's own obligations, and nobody proposed weakening it so that third parties could read it. Compliance and enforcement concentrate at the edges of the system, where identified regulated parties hold records, rather than in the transport layer.

Participants also proposed a change of vocabulary, from privacy to confidentiality. Privacy limits the discussion to the personal level. European commercial life is built on confidentiality, and markets do not function without it. The business dimension is lost when the word privacy is used alone.

- **What the exposure costs**

With those distinctions in place, the discussion turned to consequences. Three were identified, and they are connected rather than separate.

1. Property rights and personal security.

Digital assets have been recognised as objects of proprietary rights across a growing number of legal systems. That recognition has been silent on control over information about the asset, and on a public ledger no such control exists from the moment the asset is issued. In established categories of property, the right to exclude the general public from knowledge of the property forms part of the right itself. The consequence of its absence is that information which in any other setting would be protected as undisclosed commercial information, including trading positions, counterparties, treasury operations and

settlement patterns, is exposed to everyone, including competitors, forever and at no cost.

This is a security question as much as a privacy one. The same publicly available data is the input for large-scale address spoofing, for extortion and blackmail against identifiable holders, and for the documented rise in violent robbery and abduction of individuals targeted because their holdings are visible. No regulated institution in any jurisdiction publishes a list of customer balances. The question put to the room was why the same information is treated differently when it sits on a blockchain.

The problem extends past financial information. Distributed ledgers are already used for corporate and shareholder voting, membership and association records, credentials, identity and public registers. A permanent, universally readable record of how a person voted, whom they associate with or what credentials they hold reproduces the exposure that the secret ballot and the confidentiality of membership were established to prevent.

2. Market integrity and competition.

Because instructions are visible before they take effect, an observer can trade ahead of them, position around them or reorder them for gain. In regulated markets that conduct is front-running and a breach of the duty to act in the client's best interests. In tokenised markets it has been an accepted business model with published tooling and measurable revenue. The structural observation was that regulated markets do not police front-running primarily through

enforcement. They prevent it by not publishing the orders in the first place.

The competition effect is already visible. Serious transaction volume routes around public channels at additional cost, institutional platforms have been built confidential by default, and wholesale participants do not put balance sheet and trading activity on a ledger that broadcasts it to competitors. Participants who can afford to work around the exposure do so. Those who cannot are exposed. The market has reached its own conclusion, and it is the conventional one.

3. Neutrality of the infrastructure.

The third consequence concerns the people who operate the infrastructure rather than the people who use it. Beneath the layer of users, intermediaries and regulated activity sits the substrate that orders and settles transactions: validators, builders and relays. Markets depend on that substrate treating every transaction alike.

Exposure at that layer undermines this in two ways. Operators who can be identified can be pressured, whether through sanctions exposure, legal threat, commercial leverage or coercion, and an operator under pressure stops treating transactions equally. Operators who can see the content of pending transactions can also act on it, by reordering or trading ahead, which is the same extraction problem described above appearing one layer down.

Participants pointed to the routing of Ethereum blocks through sanctions-compliant relays following the Tornado Cash designations as the clearest

illustration. A substantial share of block production moved to relays that filtered sanctioned transactions. The protocol did not change. The operators were identifiable and jurisdictionally exposed, so shared infrastructure became selective infrastructure within weeks.

The conclusion drawn was that the pipes should be blind. Infrastructure whose operators can neither be identified nor read what they carry cannot discriminate between participants, even under instruction. Neutrality then stops being a promise that has to be trusted and becomes a property of the design.

Confidentiality at this layer is therefore a resilience and market-integrity measure rather than a concealment one, since supervision operates at the layer above, where the records and the obligations sit.

- **The case for the existing controls**

The session did not reach consensus on every point, and the counterargument was put directly and more than once.

An operator of a regulated exchange described how customer due diligence had in practice prevented transactions with illicit actors and had surfaced evidence of individuals being coerced during video identification. The checks and balances inherited from decades of financial services practice are imperfect, should be improved, and also work. In that participant's framing, they need to exist for the industry to function.

A second intervention came from an anti-money-laundering and intergovernmental perspective. Bad actors still have to be pursued. One approach

now under discussion is to strengthen confidentiality for natural persons and companies while observing markets more broadly, through public and private partnerships that examine transaction patterns rather than the individual transactions seen by a single institution. The reasoning is that each institution observes only a small share of the market and therefore misses a great deal. The question put to the room was how bad actors are still chased out of the system if confidentiality extends to the topology of the market.

The response was not that enforcement should stop. It was the encryption precedent again. Encryption was once classified alongside weapons because of its dual use, and the resolution was to move enforcement to the edges and to specific cases rather than to compromise encryption for everyone. The same principle was argued to apply here: investigate the misuse at the edges rather than degrade the substrate for every user.

A second counterweight came from the practitioner side on proportionality. Arguments about privacy coins are often conducted on the basis of their potential rather than their observed use, and liquidity is a real constraint on that potential. One participant cited a European kidnapping case where a ransom was demanded in a privacy coin, and noted that the sum involved could not realistically have been raised in cash. The point was that the assessment should be made against reality rather than against the theoretical maximum harm.

- **Why the current framing misfires**

Several participants converged on the view that the obstacle is the shape of the debate rather than any specific rule.

The debate is framed as all or nothing, a choice between transparency and accountability, and that framing conflates confidentiality with opacity. Either everything is public, or enforcement is blind. The premise was rejected.

Confidentiality is selective disclosure and control, where different actors see different things according to their entitlement, which is how financial supervision already operates.

Mass data collection does not remove exposure. It moves it. A compliance model built on bulk collection and retention recreates the same problem off-chain, in the databases held by intermediaries, vendors and analytics firms. Those databases are permanent, centralised and easy to cross-reference. The people recorded in them cannot see what they contain, and they are themselves a target for attack.

Privacy technologies are treated as one undifferentiated class, which participants identified as a failure of legal understanding rather than of the technology. Some tools hide everything from everyone. Others, such as fully homomorphic encryption, let a supervisor verify a specific fact without seeing anything else. The two are regulated the same way. Counsel reported still having to explain the difference case by case, with no settled legal framework to point to.

Optional privacy on a transparent ledger is a weakness in itself. If almost everything on a chain is visible, choosing to hide one transaction draws attention to it. The effect is the same as sending one encrypted page in a stack of plain ones. It marks the sender rather than protecting them. Encryption stopped being controversial only once it was built into the infrastructure and applied to everything by default.

The practical consequence was familiar to every firm in the room. Using a privacy tool is itself treated as a risk signal. Participants observed that MiCA and the AML framework work in practice to discourage adoption. A client who has touched a privacy tool becomes a client an exchange cannot take on, and the exchange is not permitted to ask why. One participant recalled the same asymmetry from the AML negotiations, where the permitted threshold for holding cash was set above the equivalent for crypto-assets, even though crypto-assets are far easier to trace.

Selective disclosure has no regulatory recognition and no evidentiary standard. The technology exists and is in production use, but there are competing methods offering different guarantees, and no common standard between them. Encryption took the opposite route. It became a standard first, then interoperable, and regulatory recognition followed.

- **Two structural problems beyond this discussion**

The EU digital regulation programme, including the Digital Services Act and the Digital Markets Act, already identifies

highly centralised, privately owned and opaque digital technologies as a risk, and already targets mass data collection and aggregation. Extracting the principles from that programme points toward decentralised, privacy-preserving technology as the answer. However, the anti-money-laundering framework is built in a separate silo and points in the opposite direction. Firms are being asked to satisfy both at once and the two do not fit together. Getting the silos to talk to each other was identified as a precondition for progress.

- **The decentralisation paradigm.**

A related argument held that the difficulty is not primarily legal. Every attempt to bring decentralised infrastructure under supervision by monitoring, disclosure or reporting reintroduces a central point, and the attack vectors participants had been describing throughout the session are all centralised ones. Regulation that is fear-driven produces that result. Regulation that is principle-driven, which was identified as the historical strength of common law, can adapt across technologies because the principles, including confidentiality, survive changes in how they are implemented.

- **Digital identity.**

The forthcoming European Digital Identity Wallet was raised as a significant development, with a business wallet to follow. Several limits were noted. Implementation is not harmonised, with Member States building separate solutions. The qualified ledger requirements point to permissioned rather than public infrastructure. And access is uneven: a long-term resident who is a

third-country national may be unable to obtain national electronic identity credentials at all, which makes the wallet an access barrier as well as an enabler. Decentralised digital identity was raised as the direction that resolves more of these problems than it creates.

- **The distance between this room and the legislature**

The most direct challenge of the session came from the parliamentary side, and it was addressed to the industry rather than to the regulators.

The gap between the technical discussion in the room and the discussion that produces legislation is wide, and legislators do not reach the level of detail at which these questions are decided. Parliamentary groups operate in their own silos and do not reliably coordinate, which mirrors the regulatory silos identified earlier in the session. Public attention to data holding has been episodic and has followed specific controversies, and the default in practice has been opt-out rather than opt-in, with very few people ever exercising a deliberate choice. Concerns were raised about facial recognition and the misidentification of Black and Asian individuals, and about the credibility of the proposition that individuals will ever own their own data.

A further observation was that the obstacle may be political rather than technical. Policymakers may not want to facilitate this level of protection, and the Tornado Cash case illustrated how a legitimate use is displaced in public debate by the illicit one. Moving the position at the top is what filters down. Repeated discussions with individual

regulatory authorities will not achieve the same effect.

The point made to the industry was practical. This forum is valuable for debate and it should also produce proposals specific enough to be carried into a legislature. A standing invitation was extended to supply them.

- **Points of agreement**

Participants agreed on the following.

1. There is a clear need for confidentiality in financial systems, given the systemic erosion of financial privacy and the realities of public ledgers.
2. Privacy-preserving technologies should be understood as security-preserving, resilience-preserving and neutrality-preserving, and should not be treated as a category of concern in themselves. Their development and support matters, particularly in light of current digital threats.
3. The debate should continue, with active support for the development of these technologies.
4. Further education is needed, among policymakers and industry alike, on the benefits of these technologies and the needs they address.

Two further propositions advanced during the session attracted support. Permanent public exposure should be treated as a security and

consumer-protection question and not only a privacy one, so that measures reducing exposure are assessed as protective rather than as suspicious. And supervisory and standard-setting bodies should state that the use of privacy-preserving technology is not of itself a high-risk indicator, where an institution can evidence equivalent or better outcomes.

- **Conclusion**

The roundtable closed on a reframing. Confidentiality is the conservative position and total exposure is the radical one. Permanent public exposure on public ledgers is a design choice without precedent in the history of money or of communication, and it affects the resilience, safety and credible neutrality of decentralised digital infrastructure.

Encryption became part of internet infrastructure because commerce required it for safety and integrity, and because it unlocked the opportunities of online commerce. The same case was made here. As distributed ledger technology matures and handles higher-value and higher-volume activity, privacy-preserving technology should become standard infrastructure. Supporting it now is what protects market integrity, consumers and competition.

Calls to Action regarding transparency as a market-integrity and competition problem

The key calls to action from the discussion are:

1. On the legal status of confidentiality

- Holders should have a protectable interest in information about the asset. International harmonisation projects and national law reform commissions should address the question directly. The point is conservative rather than novel.
- Confidentiality of ledger information should be the default, with disclosure defined for specific circumstances: to a counterparty, a supervisor, an auditor or a court, rather than to everyone by default.
- The degree of confidentiality required should be settled through proportionality analysis, using principles already established across legal systems. Is the exposure necessary to a legitimate objective, is it the least intrusive means available, and is generalised permanent publication proportionate where targeted disclosure would serve?
- Where ledger records engage civic and non-financial interests, including voting, association and credentials, confidentiality should be a design requirement and not an optional feature.

2. On supervision and compliance

- Align the standard with how financial markets already operate: no indiscriminate exposure to everyone, targeted disclosure to those entitled to it, with the obligation concentrated on regulated intermediaries and the records they handle. The infrastructure ledger should be confidential by default, in the same way that the payment message layer beneath a bank transfer is not published.
- Supervisory and standard-setting bodies should confirm that the use of privacy-preserving technology is not of itself a high-risk indicator, consistent with the risk-based approach those standards already rest on.
- Issue guidance clarifying that legitimate disclosure is circumstance-specific: triggered by a defined event or lawful request, held by the party that owes the duty, and limited to the fact required. Disclosure that is standing, indiscriminate and blanket, whether built into the infrastructure or reconstructed off-chain through bulk collection, meets no proportionality standard.

- Meet regulatory objectives through verifiability by regulated intermediaries, using zero-knowledge and comparable techniques, rather than through infrastructure that exposes everything permanently and retrospectively.
- 3. On market structure**
- Support technical solutions that do not broadcast instructions before execution, and the routing of transaction orders through confidential channels. An order that is not published cannot be traded ahead of.
 - Treat confidentiality as a property of the neutrality and operational resilience of market infrastructure. The question is whether the infrastructure can continue to treat participants equally under pressure or under adversarial conditions. Measures protecting the privacy of technical operators should be recognised as resilience measures.
- 4. On standards and process**
- Establish a joint supervisor and industry group to define minimum evidentiary verifiability artefacts. The scope should be narrow and configurable, and the practical outcome would be industry guidance.
 - Remove the obstacles to the development of privacy-preserving technology, including the exposure of developers to liability for the act of building it.
 - Produce proposals specific enough to be carried into a legislature, rather than positions addressed to regulators alone.

We thank all participants of the London 3.0 DARTE event for contributing to the discussion:

Agata Ferreira (Institute of Free Technology), Aaron Sanchez (Exponential Science), Albi Rodriguez (Garrigues), Alexander Sefi (Amina Group), Alexandra Lloyd (YouHodler), Amélie Arras (Zumo), Eva Wong (Parity), Fela Bankole, James Newell (GSR), Jessica Maria Rota, Joanna Jenkins (Frame), Joey Garcia (Xapo Bank), Jörn Erbguth (Blockchain and Data Protection Consultant), Juan Ibañez (MiCA Crypto Alliance), Lewis McLellan (OMFIF), Louise McKenna-Mayes, Magnus Jones (Nordic Blockchain Association), Baroness Manzila Uddin (House of Lords), Marc Taverner, Mariana de la Roche (BlackVogel / DAAvern), Martha Chavarría Romero (Croma Legal), Maurício Magaldi (Input Output), Mohammad Alauthman (Anglia Ruskin University), Nina Siedler (siedler legal / DAAvern), Rachel Nyasani (Pembroke Privacy), Raido Saar (Comply Once), Rav Kumar (Incrededa), Robin Davies (Intellect EU), Sibabrata Banerjee (Incrededa), Simon McFeely (Finvisor), Siva Kumar, Soledad Contreras (Coindesk), Tabish Zaman (Anglia Ruskin University), Tiburcio Sanz (Taxbit), Yasmina Boubnider (BGA), and Zornitsa Daskalova (Zodia).