DORRS Data

Enabling CLARITY Act–Compliant Crypto-Native Disclosures:

A Regulatory-Grade Framework for Protocol-Level Transparency

January 2026

INFO@DORRS.IO

WWW.DORRS.IO

Table of Contents

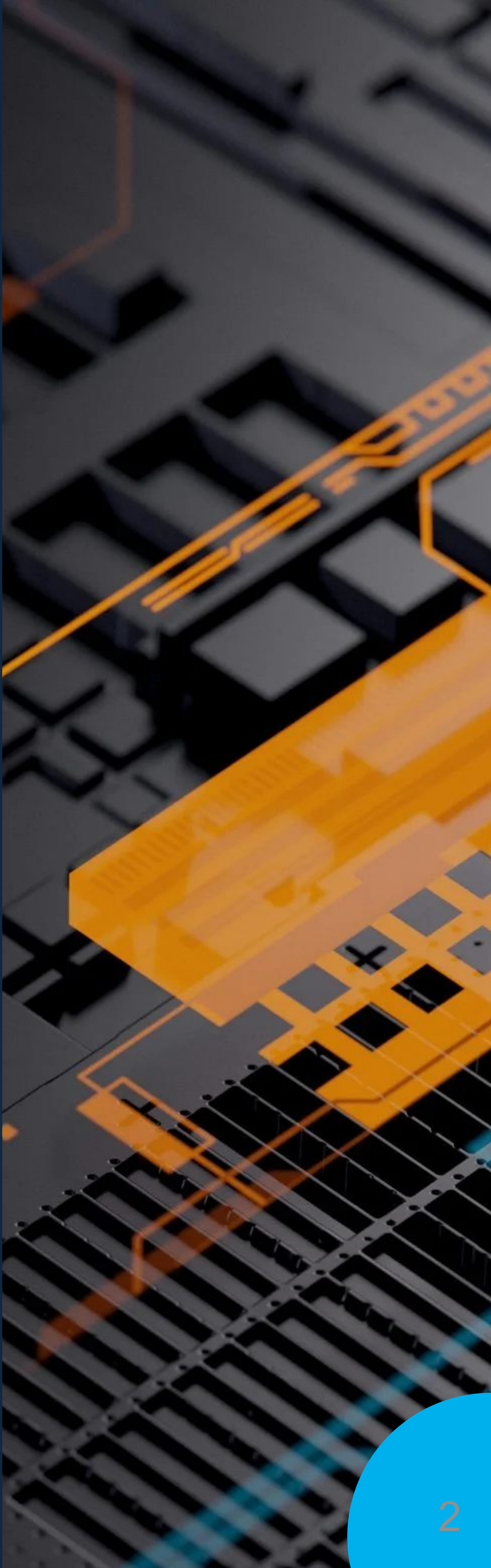


Table of Contents

Abstract

The CLARITY Act introduces a new disclosure paradigm for digital assets that function as decentralized or semi-decentralized networks rather than traditional operating companies. This white paper explains the CLARITY disclosure regime, why it is structurally distinct from EDGAR/S-1 registration, and how **DORRS (Decentralized Order Reporting & Registry System) Data** provides the purpose-built infrastructure to operationalize CLARITY-compliant, crypto-native disclosures at scale.

Executive Summary

Key Takeaway

The CLARITY Act does not modernize EDGAR—it replaces it for ancillary digital assets. DORRS is designed to implement this replacement cleanly, transparently, and in a regulator-ready form.

The **CLARITY Act** introduces a fundamentally new disclosure regime for digital assets, replacing traditional equity-style registration frameworks—such as **Form S-1**—for ancillary digital assets. Rather than forcing blockchain-based networks into corporate disclosure models designed for public companies, the Act mandates crypto-native, protocol-specific transparency disclosures that reflect how decentralized systems actually operate.

DORRS (Decentralized Order Reporting & Registry System) is purpose-built to serve as the authoritative disclosure and reference-data layer for this new regime. By cleanly separating what trades, who issued it, and how the network functions, DORRS enables regulators, auditors, market operators, and investors to consume CLARITY disclosures in a structured, verifiable, and machine-readable manner.

- Symbol identifies what trades.
- Asset Profile explains who issued it.
- CLARITY Disclosure explains how the network works, who controls it, and how it decentralizes.

Mandatory Crypto-Native Disclosures Under the CLARITY Act

The CLARITY Act establishes a disclosure framework specifically designed for digital assets that function as networks or protocols, not as traditional operating companies. For ancillary digital assets, CLARITY replaces S-1-style registration with initial and ongoing public disclosures tailored to the technical, governance, and economic realities of blockchain systems. Issuers or responsible disclosure parties must provide transparency across the following areas:

Issuers or **responsible** disclosure parties **must** provide **transparency** across the **following** areas:

- **Team and governance structure**, including founders, key contributors, and decision-making processes
- **Token supply mechanics**, including total supply, issuance schedules, emissions, burns, and inflation controls
- **Technical operation of the blockchain or protocol**, explained in plain English
- **Control and upgrade authority**, identifying who can modify code, governance rules, or network parameters
- **Token economics and utility,** including how the token is used and incentivized
- **Custody and wallet arrangements,** including custodial options and risks
- **Trading venues and liquidity,** identifying where and how the asset trades
- **Code audits and cybersecurity reviews**, where available
- **Material risk factors,** including technical, governance, regulatory, and market risks
- **Insider and affiliate holdings,** including ownership concentration
- **A roadmap to decentralization,** describing how and when reliance on the issuer or related persons is expected to end

These disclosures are not securities registration statements. They do not require financial statements, earnings projections, or corporate valuation analysis unless otherwise material. Instead, they ensure that market participants have accurate, current, and verifiable information about protocol operation, governance, and decentralization status.

Why CLARITY ≠ EDGAR / FORM S-1

This section explains why CLARITY Act disclosures are not equivalent to, nor a substitute for, EDGAR-based securities registration statements, and why applying EDGAR/S-1 standards to CLARITY disclosures would be analytically incorrect and operationally ineffective.

Different Regulatory Objectives

EDGAR / Form S-1

The EDGAR registration framework is designed to:

- Facilitate capital formation for issuers of securities
- Provide issuer-centric financial transparency
- Support valuation, underwriting, and distribution of equity or debt
- Enable analysis of earnings, balance sheets, management discussion, and corporate risk

Core unit of disclosure: the corporate issuer.

CLARITY Act

The CLARITY Act establishes a disclosure regime designed to:

- Provide protocol-level transparency for crypto-native networks
- Inform market participants about governance, control, decentralization, and technical operation
- Protect markets without misclassifying digital networks as public companies
- Enable trading, custody, and oversight of ancillary digital assets

Core unit of disclosure: the network or protocol, not the issuer's balance sheet.

Distinct Disclosure Subjects

Dimension	EDGAR (S-1)	CLARITY Act
Primary subject	Corporate issuer	Protocol / network
Financial statements	Mandatory	Not required unless otherwise material
Capital structure	Shares, debt, dilution	Token supply mechanics, emissions, burns
Management	Officers & directors	Governance participants, DAOs, upgrade authorities
Risk disclosure	Business & market risk	Technical, governance, control, and decentralization risk
Ongoing updates	Periodic filings	Continuous, protocol-driven updates

Key distinction: CLARITY disclosures focus on how a system operates and who controls it, not on corporate profitability.

Why EDGAR Concepts Do Not Translate

A. Financial Statements Are Often Not Meaningful

Many crypto networks:

- Do not generate traditional revenue
- Issue tokens programmatically rather than through capital raises
- Rely on decentralized or algorithmic incentive mechanisms

Requiring GAAP financials in these cases would:

- Provide limited investor protection
- Create misleading comparability
- Incentivize artificial corporate wrappers

B. Governance Is Technical, Not Corporate

- Control in digital networks may be exercised through:
- Smart contracts
- Timelocks
- Multisignature wallets
- On-chain voting mechanisms

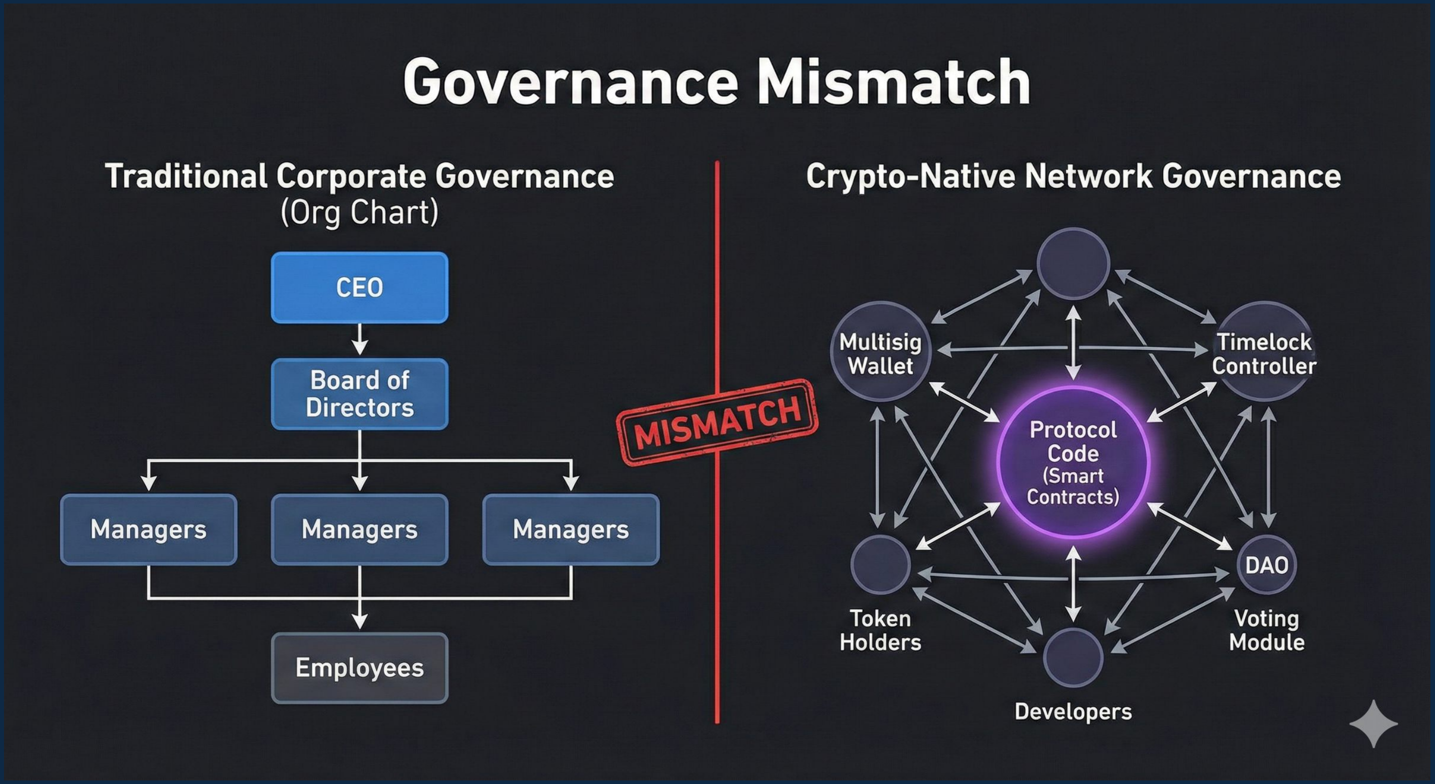
There may be no board, no officers, and no centralized decision-maker. EDGAR does not capture:

- Upgrade authority
- Emergency controls
- Admin keys
- Delegated governance power

CLARITY explicitly requires disclosure of these technical control mechanisms.

The "Governance Mismatch" (Org Chart vs. Network Map)

This split-screen diagram highlights the fundamental difference in control structures. It shows why applying corporate governance models (like an org chart) to decentralized networks (a map of smart contracts and technical controls) is a "mismatch."



Decentralization Is Not an EDGAR Concept

EDGAR assumes:

- A continuing issuer
- Ongoing managerial responsibility
- Corporate accountability structures

CLARITY requires:

- Disclosure of current decentralization stage
- A roadmap to reduced issuer reliance
- Identification of residual centralized controls
- This concept has no analogue in S-1 or 10-K frameworks.

Control & Upgrade Authority as a Material Disclosure

Under CLARITY:

- Who can change code is a material disclosure
- Who can pause or upgrade a protocol is a market-integrity concern
- Who controls admin keys may matter more than who owns equity

EDGAR does not require disclosure of:

- Smart-contract upgrade rights
- On-chain control mechanisms
- Emergency pause authorities

CLARITY makes these disclosures mandatory.

Continuous Technical Disclosure vs Periodic Reporting

EDGAR

- Periodic
- Event-driven (e.g., Form 8-K)
- Focused on corporate changes

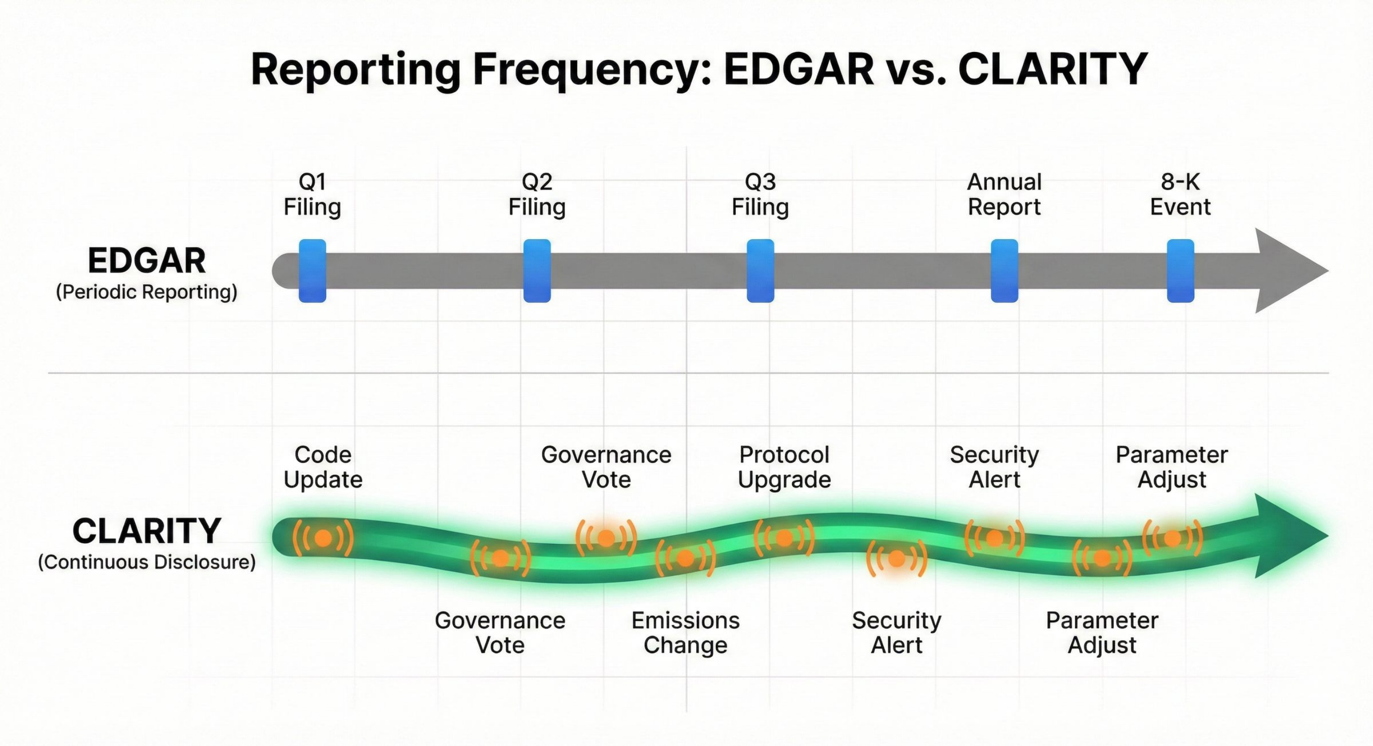
CLARITY

- Continuous and iterative
- Driven by protocol changes (code, governance, tokenomics)
- Updated when:
  - Governance authority shifts
  - Token supply mechanics change
  - Control is reduced or transferred

CLARITY disclosures function more like system documentation than financial reporting.

The "Reporting Frequency" Timeline (Continuous vs. Periodic)

This visual contrasts the static, periodic nature of traditional EDGAR filings with the continuous, event-driven disclosures required for crypto-native protocols under the CLARITY Act.



Audit & Assurance Differences

EDGAR Audits

- Financial statement audits
- Internal controls over financial reporting (ICFR)
- Corporate accounting systems

CLARITY Reviews

- Code audits
- Security reviews
- Governance-process assessments
- Disclosure completeness and accuracy

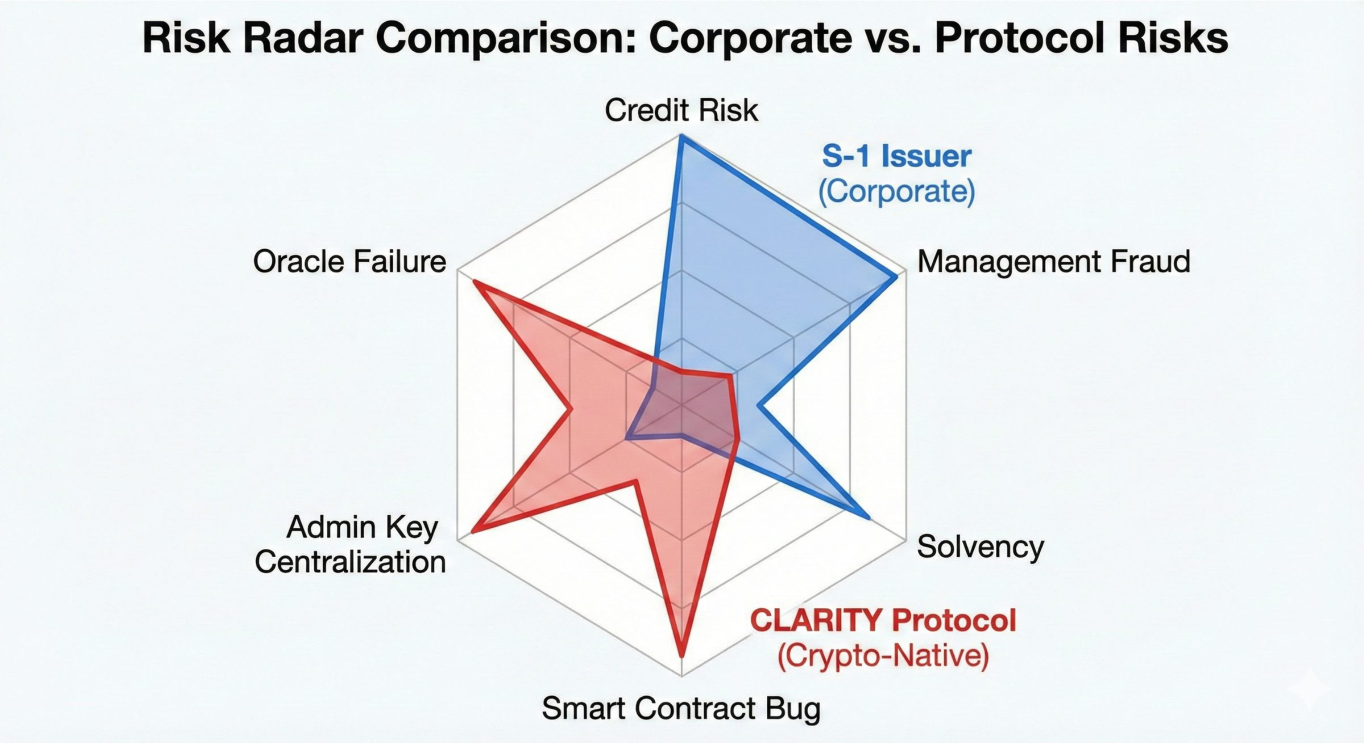
These are distinct assurance disciplines and should not be conflated.

Investor Protection Is Achieved Differently

Risk Type	EDGAR Mitigation	CLARITY Mitigation
Issuer insolvency	Financials, MD&A	Token supply mechanics, custody risks
Management misconduct	Board oversight	Governance transparency, control disclosure
Market manipulation	Trading disclosures	Liquidity sources, control rights
Operational failure	Business risk	Code audits, admin-key disclosure
CLARITY protects investors by exposing **technical and governance** risk, not by replicating equity disclosure.		

The "Risk Radar" Comparison

This radar chart overlays the distinct risk profiles of a traditional corporate issuer versus a crypto-native protocol. It visually demonstrates that the risks are fundamentally different, with protocols facing technical risks (like smart contract bugs) that are not captured by traditional corporate disclosures.



Why DORRS Is the Natural CLARITY Infrastructure Layer

Architectural Separation of Concerns

DORRS implements CLARITY by enforcing a **three-layer disclosure** architecture:

1. **Symbol** – What trades (identifiers, markets, trading attributes)
2. **Asset Profile** – Who issued it (issuer, legal, service providers)
3. **CLARITY Disclosure** – How the network works, who controls it, and how it decentralizes

This separation is intentional, auditable, and aligned with Congressional intent.

DORRS is designed to:

- Preserve EDGAR-style disclosures where securities are involved
- Provide a separate, structured disclosure layer for CLARITY-covered assets
- Prevent commingling of issuer financial data with protocol governance data

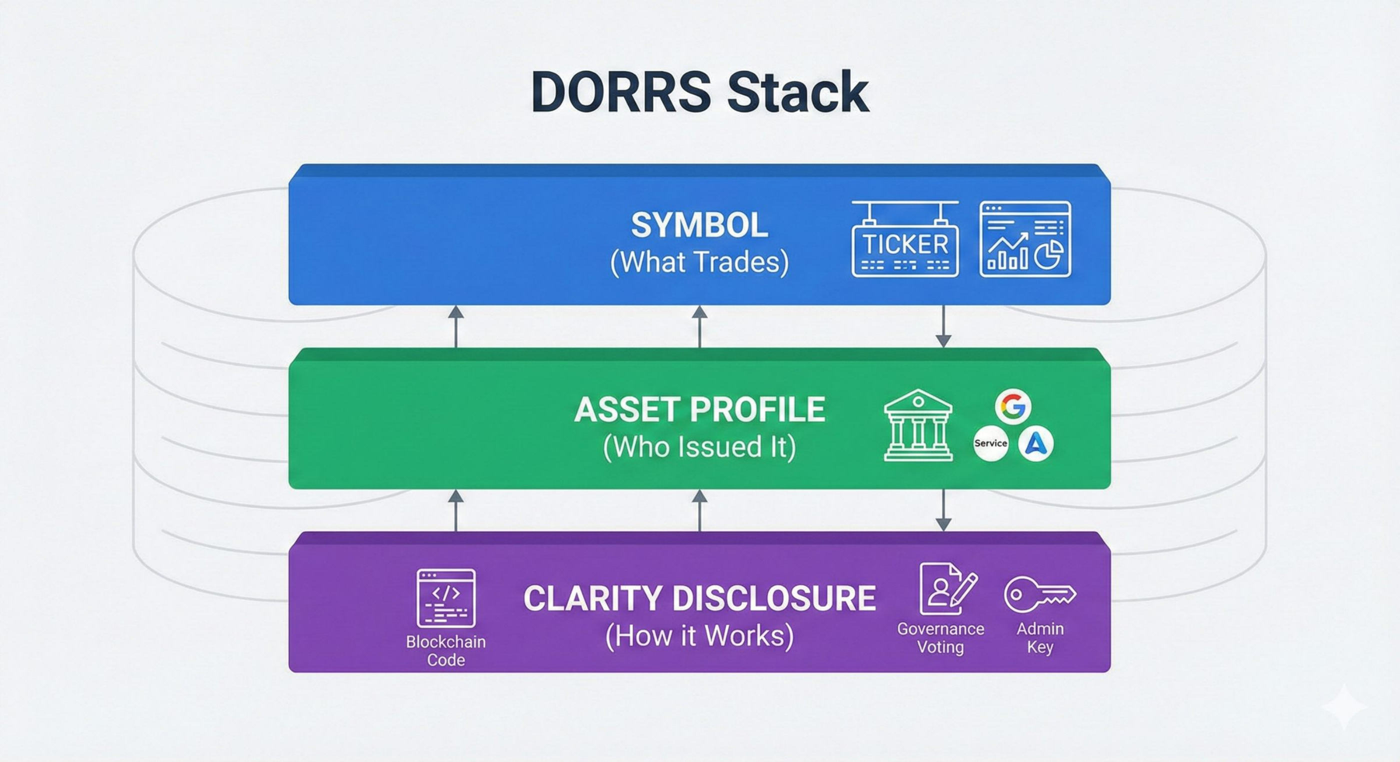
This architecture:

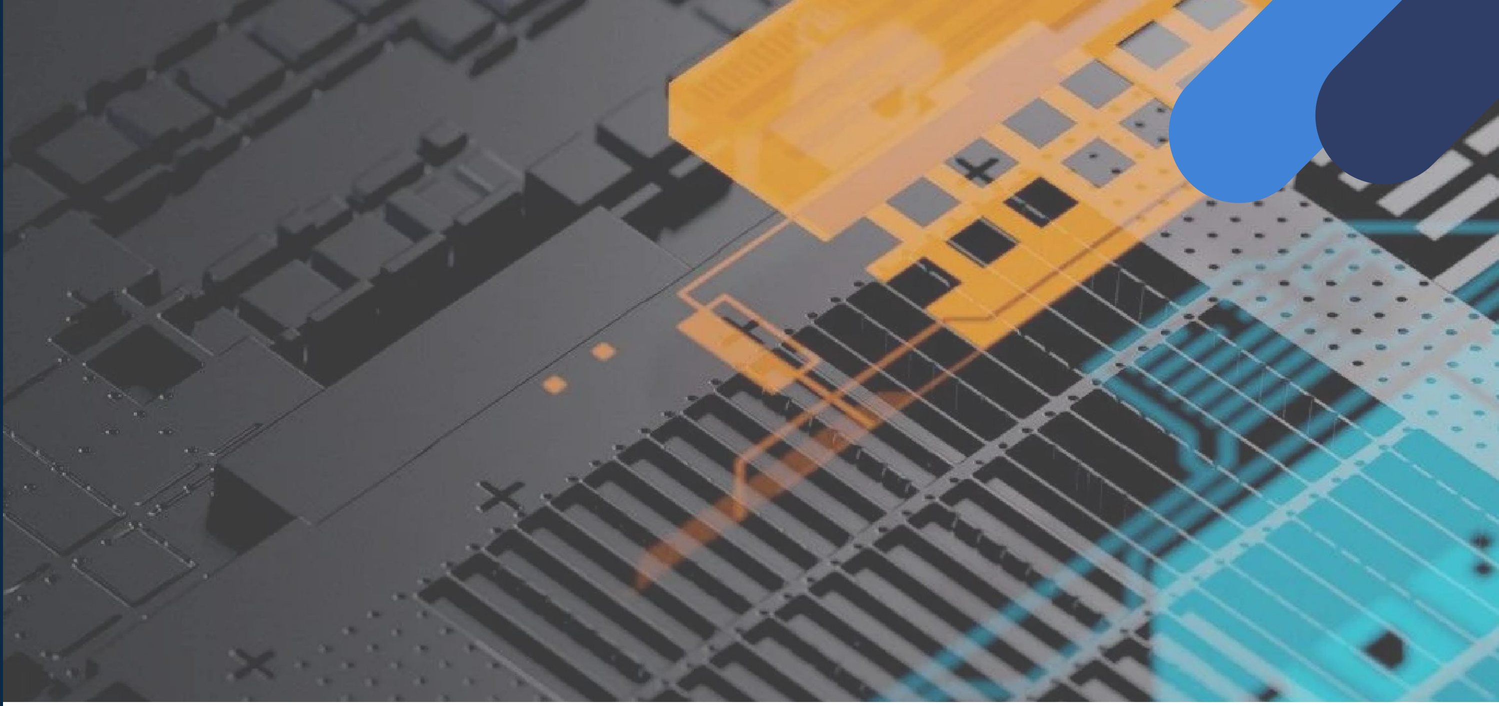
- Avoids misclassification of networks as public companies
- Supports examiner clarity and auditability
- Enables machine-readable regulatory oversight
- Aligns with Congressional intent behind the CLARITY Act

Why DORRS Is the Natural CLARITY Infrastructure Layer

The "DORRS Stack" (Layered Architecture)

This diagram illustrates the core infrastructure proposed in the paper. It separates the "what" (symbol), the "who" (asset profile/issuer), and the "how" (CLARITY disclosure/protocol) to prevent the commingling of data.





Conclusion

EDGAR answers: “Who is the company and how does it perform financially?”

CLARITY answers: “How does this digital network work, who controls it, and how does it become decentralized?”

Evaluating CLARITY disclosures using EDGAR standards would:

- Miss material protocol risks
- Create false equivalence with public companies

Undermine regulatory clarity rather than enhance it For these reasons:

- CLARITY disclosures must be treated as a distinct regulatory disclosure regime, and DORRS provides the purpose-built data, workflow, and reference architecture to operationalize that regime at scale.

Contact

DORRS Data LLC

1603 Capitol Ave Ste 415

Cheyenne, WY 82001

Email: info@dorrs.io