

WITO · WORLD INTEROPERABLE TRUST ORGANIZATION
GENEVA · SWITZERLAND

WORKING PAPER

The Economic Trust Landscape

*A study of the instruments that create and verify trust in claims
about products, services, and people.*

DRAFT · JULY 2026

PUBLICATION INFORMATION

© 2026 World Interoperable Trust Organization.

This is a working draft circulated for consultation. It may be shared in full with colleagues and within your organisation. Please do not quote, cite, or reproduce extracts without contacting WITO. A final version is expected in 2027.

WITO is an association constituted in Geneva, Switzerland under Articles 60 et seq. of the Swiss Civil Code.

SUGGESTED CITATION

World Interoperable Trust Organization (2026). *The Economic Trust Landscape: A study of the instruments that create and verify trust in claims about products, services, and people*. Working Paper, draft, July 2026. Geneva: WITO.

AUTHOR

Robin Shaban, PhD

Robin Shaban is an economist and public policy researcher, and co-founder of the World Interoperable Trust Organization. They hold a PhD from Carleton University's School of Public Policy and Administration and an MA in economics from Queen's University.

About WITO.

WITO, the World Interoperable Trust Organization, is a neutral, non-commercial body constituted in Geneva as a not-for-profit association under Swiss law. Its purpose is to strengthen trust in claims about physical and digital objects as they move through the global economy, helping protect consumers and public health, safeguard medicines and food, uphold environmental and climate integrity, support international cooperation, and make cross-border trade more trustworthy. It does this by developing frameworks for verifiable claims and by coordinating mutual recognition between systems. WITO is grounded in open standards and open to any qualifying organisation worldwide.

Built, but not connected.

The economy runs on trusted information: the certificates, identifiers, traceability systems, credentials, and recognition arrangements that let one party rely on a claim it cannot check for itself. This report maps that infrastructure as a whole, using a dataset of 619 **instruments** – the regulations, standards, schemes, treaties, and arrangements that create or verify trust in claims about products, services, and people. A key finding from this descriptive analysis is that this **economic trust infrastructure** is extensively built but poorly connected.

The report begins with the instruments themselves. They take seven different forms, and no single form dominates: law, voluntary consensus standards, and private or NGO schemes each account for roughly a fifth of the landscape. They are authored across the public sector, NGO and multistakeholder bodies, private companies, and hybrid arrangements. They are managed by about 370 organizations, of which 309 hold just one instrument. Most instruments are voluntary, the market is the most common driver of their uptake, and more of them are global than national. Grouped by the problem they address, they divide into five domains led by product integrity. A quarter of them do not have mutual recognition with other instruments.

Sorted by function, these instruments form a seven-layer stack, from the identifiers that name a thing at the base to the regulation that compels its verification at the top. The stack is thickest in the middle, where verification is performed: conformity assessment alone accounts for 207 instruments, while the foundational and mandating layers are thin. No single body occupies the connective role that would join the layers together.

Across all the layers, authority and machinery are held by different actors. Public bodies author 63 of the 67 instruments that compel trust by law, while the operational layers beneath – conformity assessment, credentials, and traceability – are built largely by industry and non-governmental bodies. Law and the market rarely reinforce the same instrument, and governments tend to mandate where they capture the benefit directly. Illicit trade and excise is mandated 87 percent of the time, while 37 percent of product verifiability and quality instruments are mandated by law.

The connective layer that would let these instruments recognize one another is thin and almost entirely voluntary. Furthermore, the instruments that carry the most force tend to be the least interoperable. Of instruments authored by governments, 43 percent do not have mutual recognition agreements compared with 20 percent for private instruments, 13 percent for NGO or multistakeholder instruments, and 3 percent for hybrid ones. The instruments best placed to compel adoption are the least able to work with anyone else.

The report describes a landscape that is genuinely built and genuinely uncoordinated: most of it voluntary, most of it single-body, and least connected where the stakes and the

authority are highest. Two questions it does not settle are whether these instruments demonstrably work, and what they cost to comply with. What the map implies, and what a response might look like, is taken up in the companion issue paper, *Trust Infrastructure for the Economy of the Future*.

Table of Contents

Introduction.....	4
The Instruments	6
1.1 Instrument types	6
1.2 Instrument creators and owners	7
1.3 How binding are they?.....	7
1.4 What drives their uptake?	8
1.5 Geographic scope	9
1.6 Problems they address.....	9
1.7 Instrument mutual recognition.....	10
The Economic Trust Infrastructure Stack	12
Insights Across the Stack.....	13
3.1 Authority and machinery are held by different actors.....	13
3.2 Law or the market, but seldom both.....	13
3.3 Governments mandate where they capture the benefit.....	14
3.4 Interoperability in the economic trust stack	15
3.5 Fragmentation is sector-specific, not universal	18
Conclusion	20
Annex A.....	21

Trust Infrastructure

The hidden layer behind trustworthy markets.

Trustworthy information about products, services, and people is fundamental to a well-functioning economy. As the global economy becomes more complex and technologies like AI and product traceability systems become more common, creating and sharing trustworthy information has become even more important.

In this study, we undertake a preliminary examination of the world's **economic trust infrastructure**: the system of technologies, standards, laws and regulations, and other instruments that work together to create and provide trustworthy information about products, services, and people. This note maps the infrastructure using a constructed dataset of 619 **instruments** and provides descriptive insights about how it operates.

Mapping the world's economic trust infrastructure is a necessary starting point for any effort to make trust systems work better, and work better together. The global economy is entering an era of transformative technology adoption, increasing digitization, and likely more crises related to climate and a shifting balance of geopolitical power. Governments, businesses, and technology-focused non-governmental organizations must take proactive steps to ensure that the systems that support trust in markets and trade remain effective.

The paper is organized in three parts, preceded by a note on method. That note explains how the dataset was assembled and coded. Part I then profiles the instruments themselves, one characteristic at a time. Part II sorts those instruments by function into a seven-layer stack, from the identifiers that name a thing at the base to the regulation that compels its verification at the top. Part III reads a set of insights across that stack: who owns each layer, whether law or the market drives adoption, where the stack connects and where it breaks, and how fragmentation varies across sectors. A short conclusion draws the findings together, and a codebook in Annex A defines every variable and gives its full tabulation.

How the dataset was built.

The dataset covers 619 instruments that make up the economic trust infrastructure across all sectors and globally. An **instrument** is a distinct trust or standards mechanism: a government law or regulation, voluntary standard, scheme managed by companies or consortia, NGO or multistakeholder schemes, treaty, accreditation and mutual-recognition arrangements, or operating platform, that establishes or verifies trust in a claim about a

product, a service, or a person. Instruments whose primary purpose lies outside the economy, such as those governing elections or public discourse, are not included.

The dataset was assembled through an iterative, AI-assisted search of primary and authoritative sources: the texts of regulations and treaties, the catalogues of standards bodies and of accreditation and scheme operators, and the publications of governments and international organizations. The search was organized by domain and built up in successive rounds, beginning with the core of object trust, product identification, traceability, conformity assessment, and certification, and expanding outward to adjacent and broader trust domains such as digital identity, payments, cybersecurity and software supply chains, metrology, financial services, and legal and notarial trust. Each candidate instrument was recorded only with a verified, resolvable source, and entries were then deduplicated and checked against those sources.

For each instrument, the dataset records a common set of characteristics, which the next section profiles in turn. Definitions and full tabulations of every variable are provided in Annex A.

The Instruments

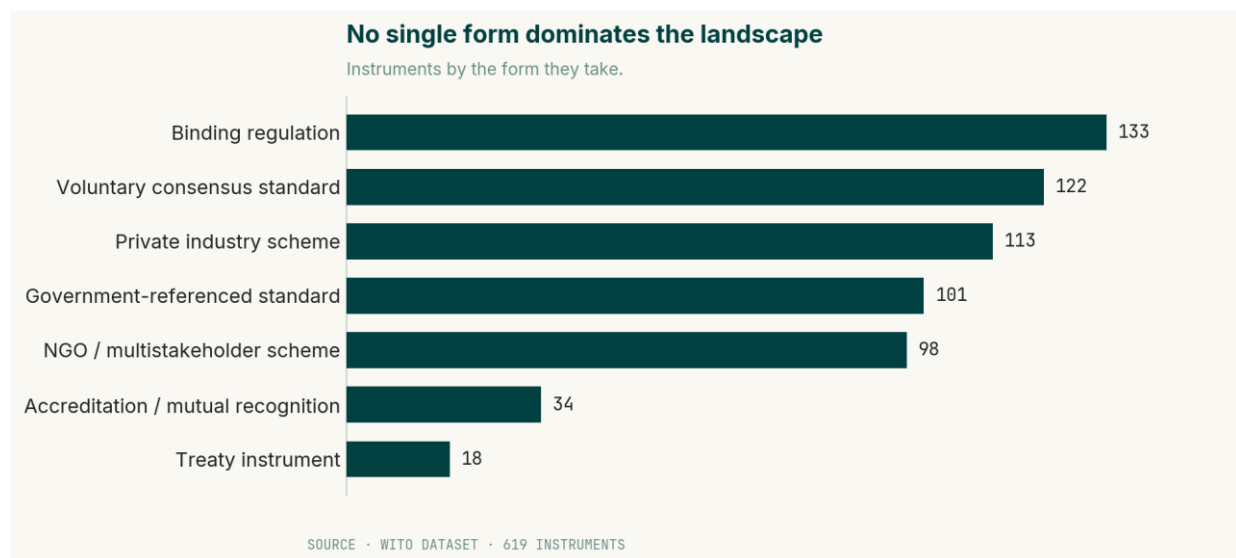
The building blocks of economic trust infrastructure.

This section profiles the 619 instruments by what form they take, who owns them, how binding they are, what drives their uptake, where they apply, what problems they address, and whether they connect to one another. These are the building blocks from which the analysis in Part II is assembled.

1.1 Instrument types

Instruments take one of seven forms. The largest group is binding regulation – law issued by a public authority – at 133 instruments. Close behind are voluntary consensus standards from standards bodies (122) and private industry schemes run by companies or consortia (113). Government-referenced standards, which are not law themselves but are operated or formally referenced by a government, account for 101; NGO or multistakeholder schemes for 98; accreditation and mutual-recognition arrangements for 34; and treaties for 18. No single form dominates. Law, consensus standards, and private or NGO schemes each make up roughly a fifth of the landscape, with trust being produced as much by industry and civil society as by the state.

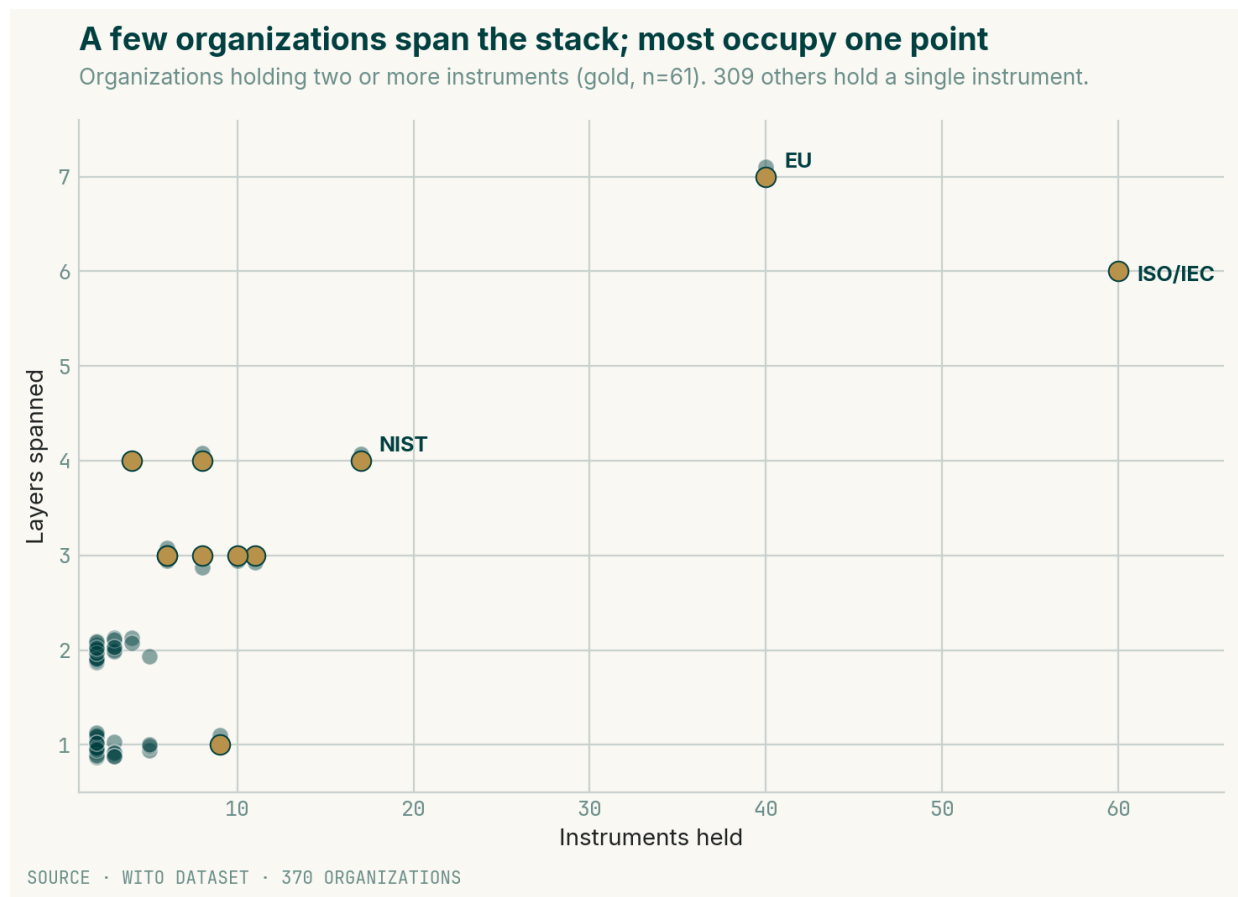
FIGURE 01 • INSTRUMENTS BY FORM



1.2 Instrument creators and owners

By the type of body that authors them, the instruments are led by the public sector (250), followed by NGO or multistakeholder bodies (163), private companies or consortia (120), and hybrid public-private arrangements (86). The 619 instruments are run by 370 organizations. A few of these have a wide portfolio of instruments: ISO and IEC together account for 60 instruments and span six of the seven functional layers described in the next section, the European Union spans all seven with 40 instruments, and NIST spans four functional layers with 17. The three largest organizations hold about 19 percent of the landscape. Against them sits a long tail: 309 of the 370 organizations appear only once, with a single instrument. The landscape is built by many hands.

FIGURE 02 • ORGANIZATIONAL FOOTPRINT

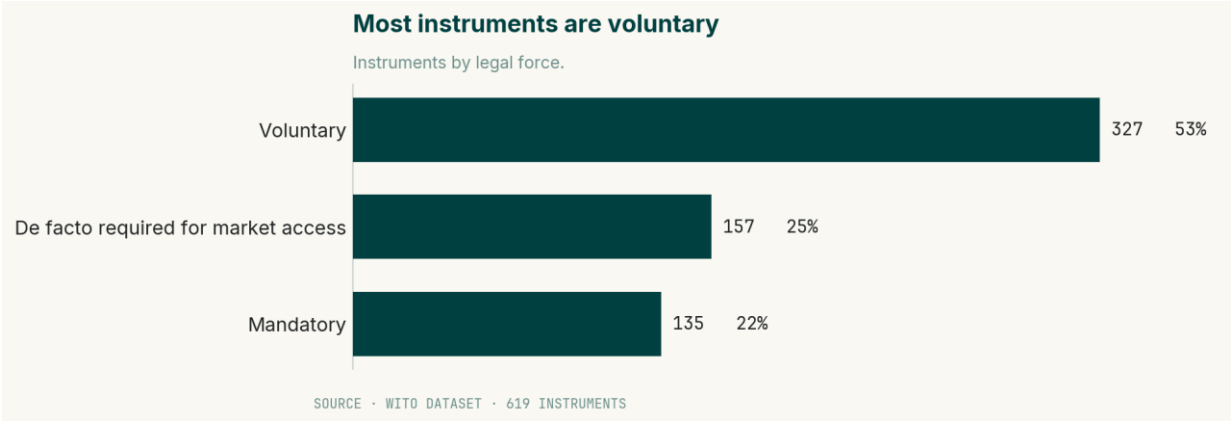


1.3 How binding are they?

Instruments differ in how much force stands behind them. Most are voluntary (327), where adoption is optional, with no legal or market gate. A large group, 157, are de facto

required for market access: they are not mandatory by law, but compliance is the price of selling into a particular market because dominant buyers or importing regimes require it. Retailer-required food-safety schemes are an example. The remaining 135 are mandatory, binding by law. Voluntary instruments are the norm, but a quarter of the landscape is effectively compulsory through the market rather than through law.

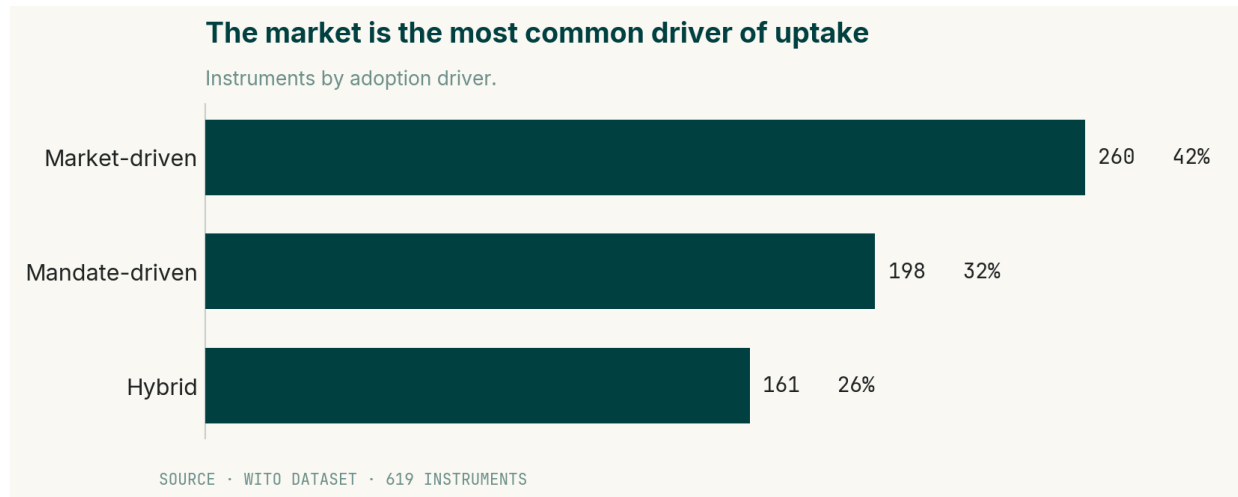
FIGURE 03 • INSTRUMENTS BY BINDINGNESS



1.4 What drives their uptake?

A related but distinct characteristic is what drives an instrument's uptake, recorded as its adoption driver. Each instrument is coded with one of three values: mandate-driven, where a law or regulation prompts its use; market-driven, where commercial demand does; and hybrid, where both apply. The value is assigned from the instrument's recorded characteristics and its verified source. Market demand is the most common driver (260 instruments), followed by legal mandate (198), with the remaining 161 coded hybrid. Adoption driver is distinct from bindingness, previously discussed, which records legal form rather than the reason for uptake. An instrument can be voluntary in form yet mandate-driven where a law points actors toward it. How the two interact is examined in Section 3.2.

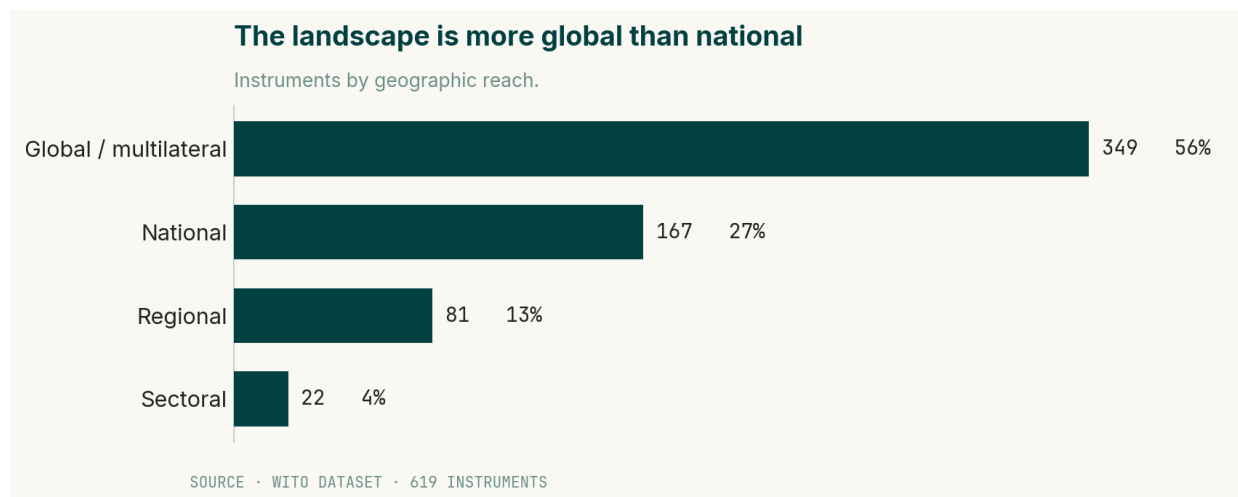
FIGURE 04 • INSTRUMENTS BY ADOPTION DRIVER



1.5 Geographic scope

By geographic reach, more than half the instruments (349) are global or multilateral, 167 are national, 81 are regional, and 22 are targeted to a specific sector. The landscape is more global than national, though, as later sections show, the national instruments carry disproportionate weight where isolation is concerned.

FIGURE 05 • INSTRUMENTS BY GEOGRAPHIC SCOPE

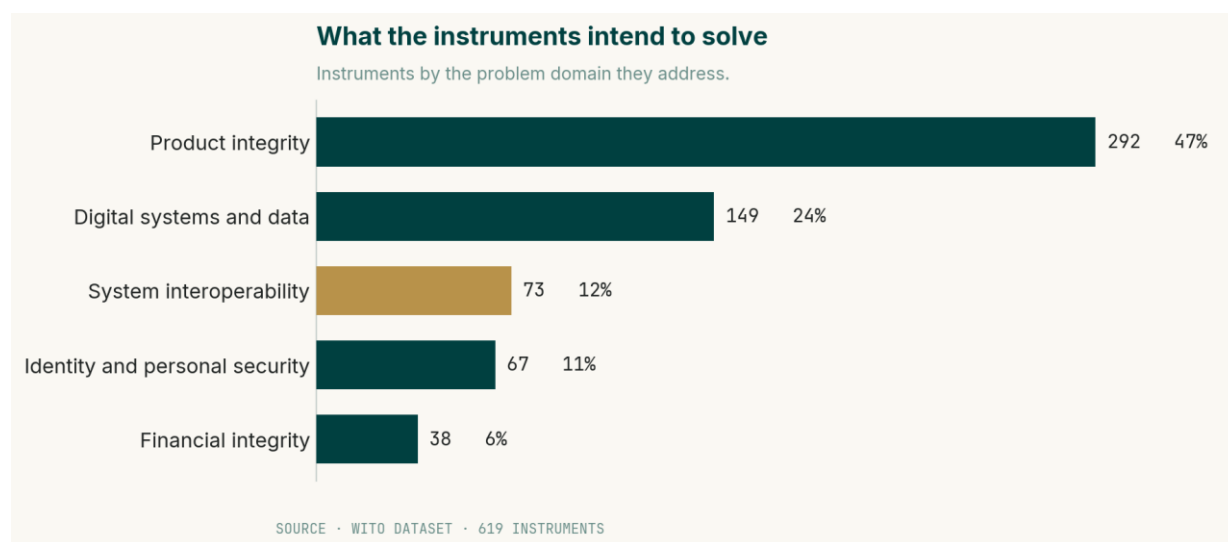


1.6 Problems they address

Grouped by the problem each instrument addresses, the landscape divides into five domains, formed by grouping twelve more specific harm families that are defined in Annex A.

- **Product integrity** is the largest, with 292 of the 619 instruments (47 percent). It covers the authenticity, safety, provenance, and lawful sourcing of physical goods, and includes product-safety regulation, food-safety and agricultural certification, anti-counterfeiting and traceability schemes, and responsible-sourcing programs.
- **Digital systems and data** follows with 149 instruments (24 percent). It covers the security and integrity of digital systems, data, and AI, and includes cybersecurity and software-supply-chain standards, data-governance and assurance frameworks, and AI management and conformity instruments.
- **System interoperability** accounts for 73 instruments (12 percent). These exist to let separate trust systems recognize one another, through shared identifiers, common data formats, and mutual-recognition arrangements.
- **Identity and personal security** accounts for 67 instruments (11 percent). It covers the verification of people and the prevention of identity fraud and impersonation, and includes national digital identity systems, electronic-signature and PKI trust services, and biometric standards.
- **Financial integrity** accounts for 38 instruments (6 percent). It covers financial crime, money laundering, and mispriced risk, and includes payment-security standards, anti-money-laundering and know-your-customer frameworks, and financial assurance and audit standards.

FIGURE 06 • PROBLEM DOMAINS

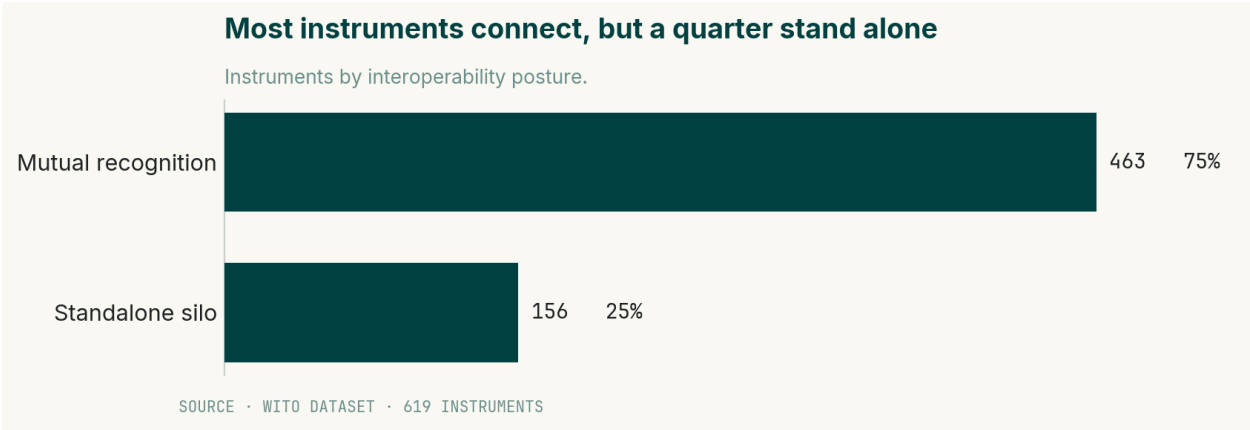


1.7 Instrument mutual recognition

The last characteristic, and the one the later analysis turns on, is interoperability posture: whether an instrument recognizes and is recognized by others, or operates on its own.

Roughly three-quarters of the instruments (463) take part in some form of mutual recognition, while a quarter (156, or 25 percent) stand alone as silos.

FIGURE 07 • INTEROPERABILITY



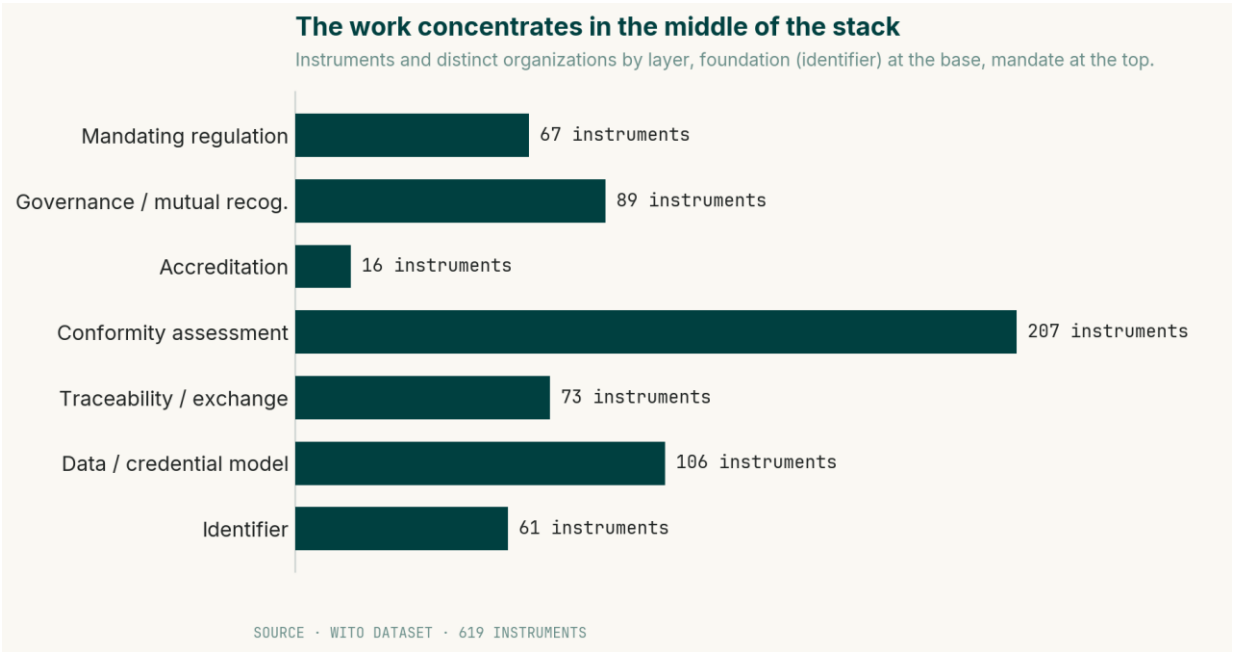
The Economic Trust Infrastructure Stack

The instruments sort into seven functional layers.

The instruments profiled above perform different jobs. Some name a thing; some describe it; some move that description along a chain; some test it against a standard; some vouch for the testers; some coordinate across schemes and jurisdictions; and some compel the rest by law. Sorted by function, the 619 instruments fall into seven layers that build on one another, a dependency ladder that runs from the identifier that names an object at the base to the regulation that compels its verification at the top.

The stack is thickest in the middle, where verification is performed. Conformity assessment alone accounts for 207 instruments, and the foundational and mandating layers are comparatively thin. This stack is the organizing framework for this study.

FIGURE 08 • THE TRUST STACK

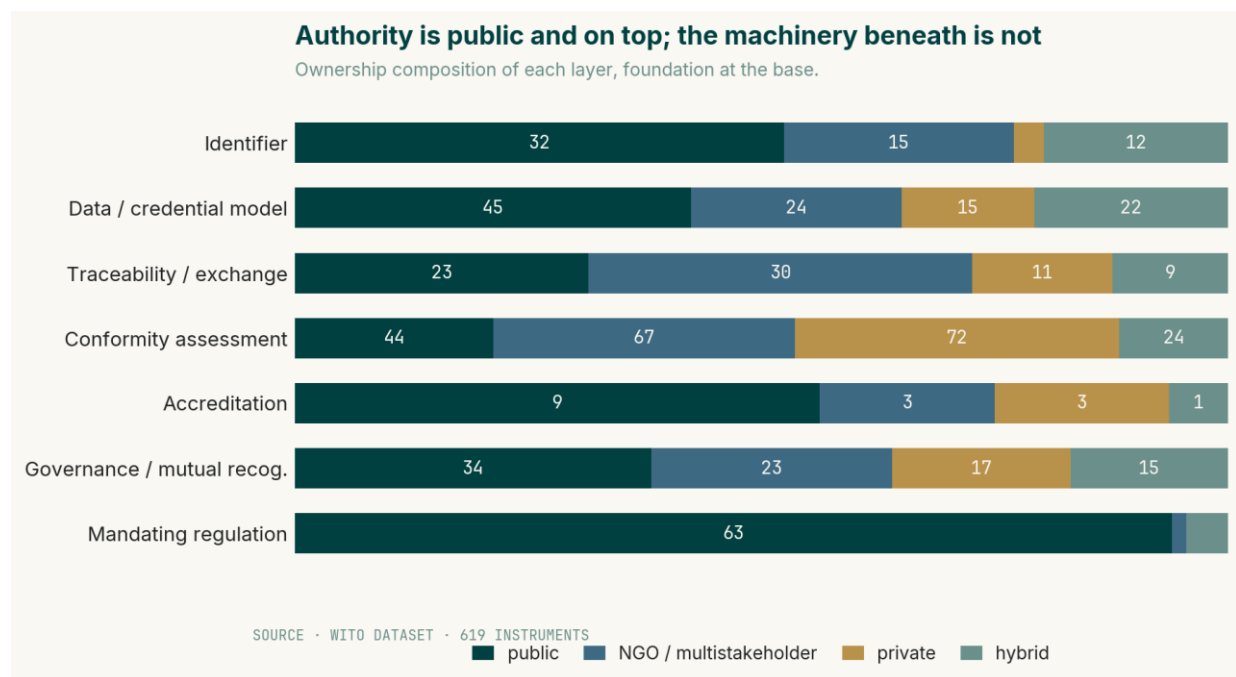


Insights Across the Stack

3.1 Authority and machinery are held by different actors.

Public bodies author 63 of the 67 mandating-regulation instruments, and are largely absent from the operational layers beneath, where industry and NGO or multistakeholder bodies build the conformity, credential, and traceability mechanisms. Authority to compel sits with the public sector, and the machinery of verification is built by everyone else.

FIGURE 09 • OWNERSHIP BY LAYER



3.2 Law or the market, but seldom both

This section compares two related but distinct variables. Bindingness records the legal force of an instrument: whether it is mandatory by law, de facto required for market access, or voluntary. Adoption driver records why actors take it up: because law or regulation prompts its use (mandate-driven), because the market demands it, or because

both forces are relevant. The distinction matters because an instrument can be voluntary in form but still be mandate-driven if a law or regulation points actors toward it.

For example, the Codex Alimentarius traceability principles are voluntary guidelines. Codex has no power to compel anyone and following them is optional. Yet their uptake is driven by law, because the World Trade Organization's Agreement on Sanitary and Phytosanitary Measures treats Codex as the international benchmark for food safety, and many national regulations write its standards directly into their own rules. The instrument is therefore voluntary in bindingness but mandate-driven in adoption, steered into use by the legal framework around it rather than by any force of its own.

Across the dataset, an instrument's legal force and the driver coded for its uptake line up closely. Mandate-driven instruments are 128 mandatory against just 15 voluntary, and market-driven instruments 212 voluntary against 2 mandatory. Almost none of the 135 mandatory instruments is market-driven, and few of the 327 voluntary ones are mandate-driven. The landscape sorts into a largely mandated track and a largely voluntary, market-led track, with little occupying the middle ground where a voluntary instrument is nonetheless carried into use by regulation, as with Codex above, or a mandatory one owes its uptake to the market.

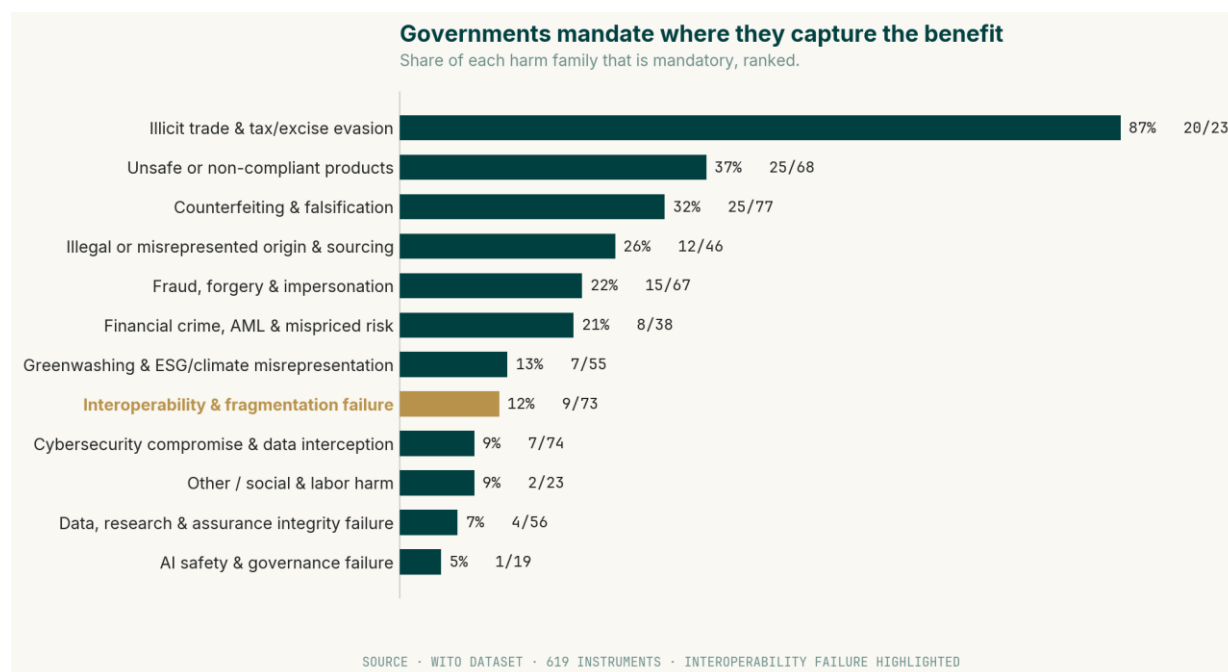
Adoption driver	Mandatory	De facto (market access)	Voluntary	Total
Mandate-driven	128	55	15	198
Hybrid	5	56	100	161
Market-driven	2	46	212	260
Total	135	157	327	619

Table 1. Instruments by bindingness (columns) and adoption driver (rows). Source: WITO dataset, 619 instruments.

3.3 Governments mandate where they capture the benefit

The share of instruments that are mandated varies sharply by the harm they address, and the pattern is telling. Illicit trade and excise, where the state collects the revenue directly, is mandated 87 percent of the time. Diffuse coordination harms are left to voluntary action: cybersecurity is mandated 9 percent of the time, and interoperability and fragmentation failure, the third-largest harm family in the whole dataset, is mandated just 12 percent of the time.

FIGURE 10 • WHAT GETS MANDATED



3.4 Interoperability in the economic trust stack

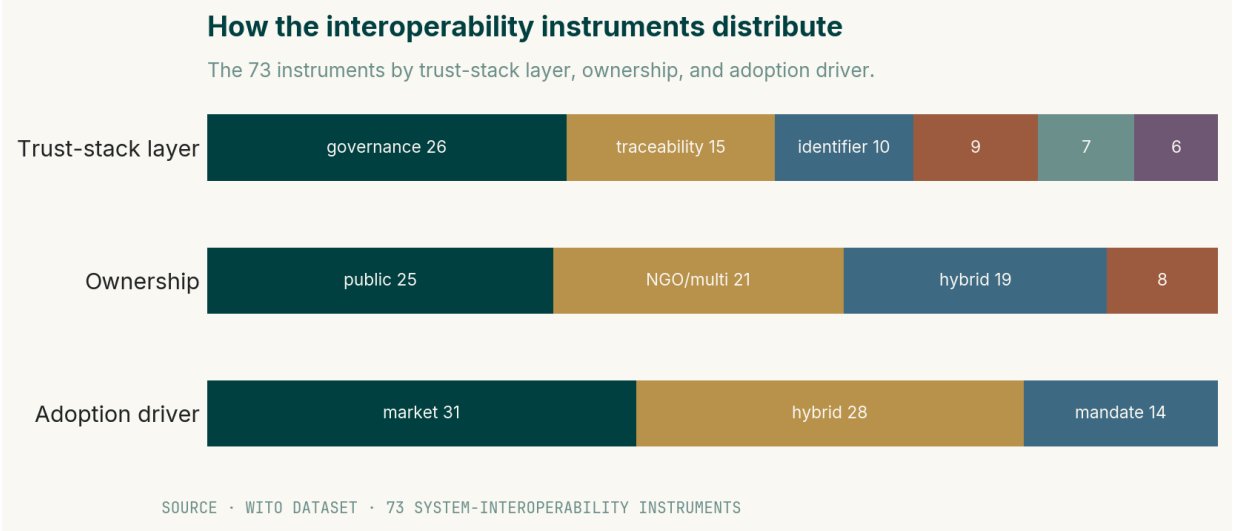
3.4.1 The connective layer is thin and mostly voluntary

One of the five problem domains, system interoperability, comprises 73 instruments that exist to let separate trust systems, schemes, and jurisdictions recognize one another through shared identifiers, common data formats, and mutual-recognition arrangements. They include shared identifiers that let separate systems reference the same object, such as the GS1 keys and the Digital Object Identifier; common data and credential formats that let claims move across systems, such as the ISO/IEC biometric formats and the ISO 8583 payment message standard; exchange protocols that let traceability data travel along a chain, such as the Codex tracing principles and the GDST seafood standard; benchmarking arrangements that let duplicate certification schemes recognize common baselines, such as the Global Food Safety Initiative; and mutual-recognition and cross-border frameworks that let one authority's decisions be accepted by another, such as IAF, ILAC, the World Customs Organization, eIDAS, and the ICAO Digital Travel Credential.

These 73 instruments sit in the middle and upper layers of the stack, concentrated in governance and mutual recognition (26) and traceability and exchange (15), with the remainder in identifiers (10), data and credential models (9), conformity assessment (7), and mandating regulation (6). Ownership is balanced: 25 are public, 21 NGO or multistakeholder, 19 hybrid, and 8 private. It is also the most fragmented domain in the dataset at the organization level, with 67 distinct owners across 73 instruments. Almost every instrument has a different owner.

The connecting work is rarely compelled. Only 14 of the 73 interoperability instruments are mandate-driven, and only 3 take the form of binding regulations themselves, while 54 are voluntary. In other parts of the stack, law requires instruments to be used, but when the task is to make one trust system accept another's decisions, uptake is left almost entirely to voluntary agreement, even where public bodies take part. The main tool for the work is the mutual-recognition arrangement, of which the dataset holds 34, about half of them (15) aimed at connecting systems together. The weakness is not that these tools are absent, but that they usually remain optional.

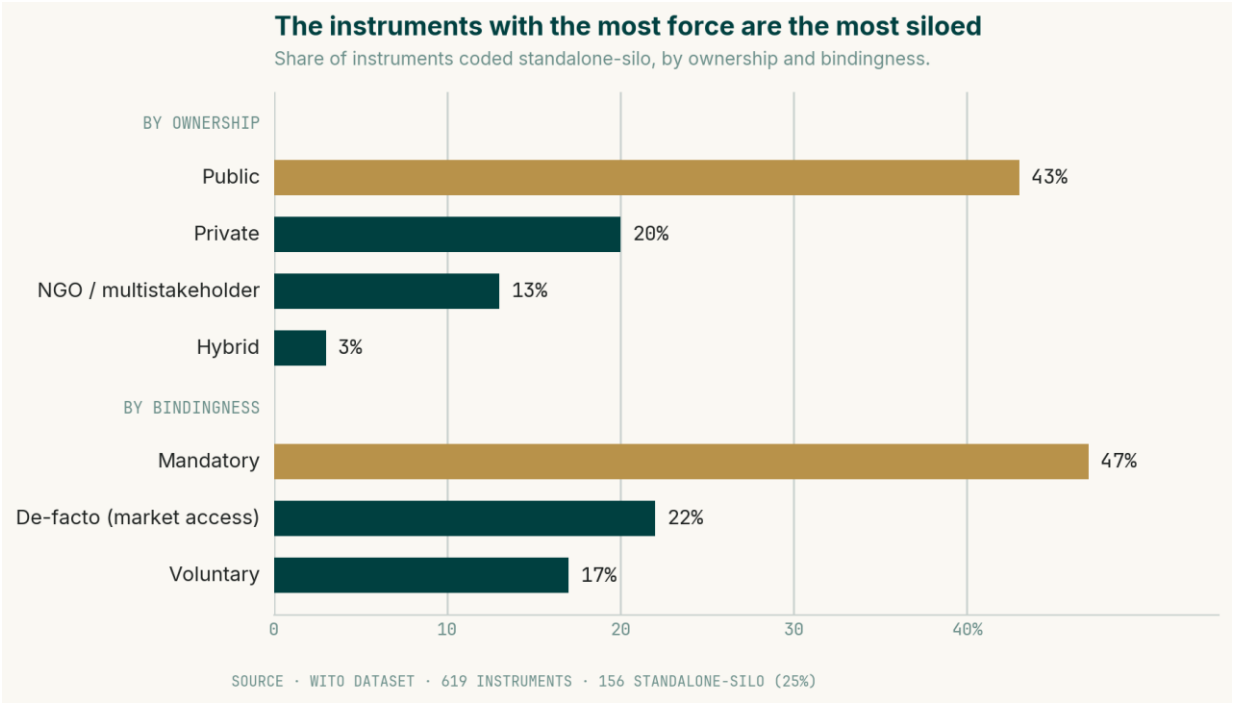
FIGURE 11 · SYSTEM INTEROPERABILITY



3.4.2 The instruments with the most authority are the least interoperable

Across the whole dataset, roughly a quarter of the instruments (156 of 619) operate with no mutual recognition of or by any other instrument. The remaining 463 take part in some form of mutual recognition. That isolation concentrates in the instruments that carry the most authority. Public instruments are the most likely to stand alone: 43 percent are siloed, compared with 20 percent of private instruments, 13 percent of NGO or multistakeholder instruments, and 3 percent of hybrid public-private ones. The same pattern appears by legal force: 47 percent of mandatory instruments are siloed, compared with 22 percent of those required only for market access and 17 percent of voluntary ones. Governments, which are best placed to compel adoption, are the least likely to build recognition into their instruments. Instruments built by coordinating coalitions, or adopted through persuasion rather than compulsion, are the most likely to have mutual recognition.

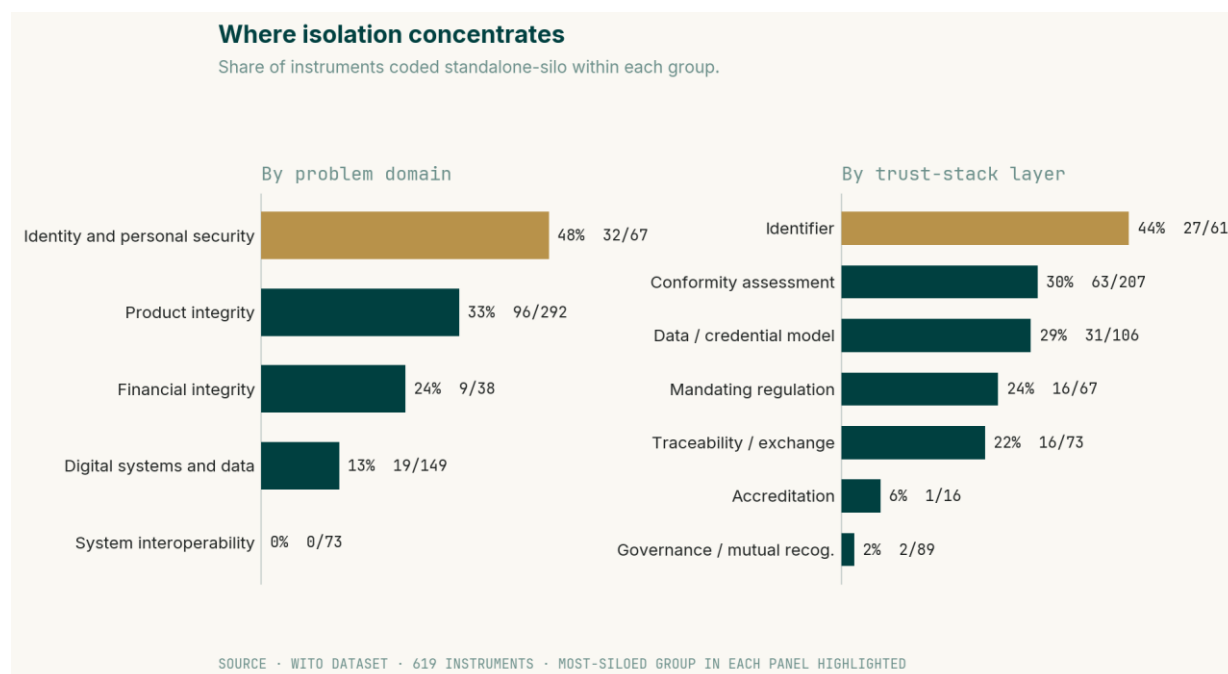
FIGURE 12 · FORCE AND ISOLATION



3.4.3 Where the isolation sits: the foundation and national systems

By problem domain, lack of mutual recognition is highest in identity and personal security, where 32 of 67 instruments (48 percent) are isolated. Product integrity is next, at 96 of 292 (33 percent), followed by financial integrity at 24 percent and digital systems and data at 13 percent. System interoperability sits at zero, because instruments whose purpose is recognition are, by definition, not silos. By trust-stack layer, isolation is highest at the identifier layer where 27 of 61 instruments (44 percent) stand alone. It then falls sharply in the coordinating layers to 2 percent in governance and mutual recognition and 6 percent in accreditation. The layers built to coordinate are the most connected, while the layer that names the object, where a shared reference should matter most, is the most fragmented.

FIGURE 13 · WHERE ISOLATION CONCENTRATES



The isolation also has a geography. Of the 107 public instruments coded as standalone silos, 103 have national scope. The pattern is structural rather than incidental: when a government makes an instrument mandatory, it usually builds it for its own jurisdiction and legal order, and mutual recognition with other jurisdictions is a separate, later step that most of these instruments have not taken. The dataset shows this across three families of instrument:

- **National digital identity systems**, among them Aadhaar in India, Singpass in Singapore, My Number in Japan, gov.br in Brazil, UAE PASS, Nafath in Saudi Arabia, VNeID in Vietnam, PhilSys in the Philippines, and Mexico's biometric CURP.
- **National conformity and product-certification marks**, including China Compulsory Certification, Saudi Arabia's SABER, Nigeria's SONCAP, India's BIS and ISI schemes, Indonesia's SNI, South Africa's NRCS, and Kenya's KEBS verification.
- **National pharmaceutical serialization systems**, including Korea's KPIS, China's NMPA drug traceability code, India's Schedule H2 and DAVA export system, and Russia's MDLP.

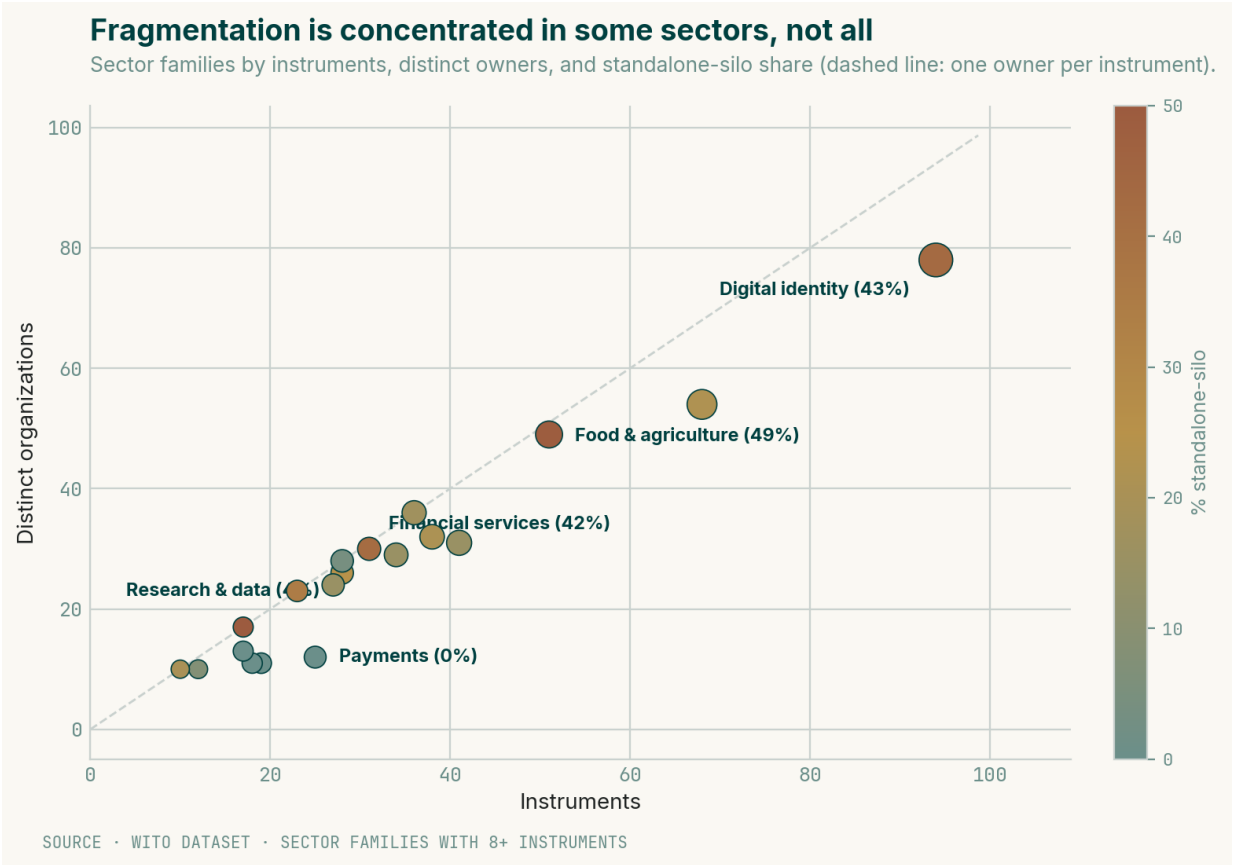
In each case the instrument serves the government's needs within its own borders, and the cost of reconciling these systems falls on the parties that must satisfy several at once, and on any later effort to make them recognize one another.

3.5 Fragmentation is sector-specific, not universal

Fragmentation – the number of distinct organizations offering a specific type of instrument – is uneven. It is worst in digital identity, food, and financial services, and

almost absent in payments. Digital identity carries 94 instruments across 78 distinct organizations, and 40 of them (43 percent) stand alone with no mutual recognition. Food and financial services follow the same shape. Payments is the counterexample: 25 instruments across just 12 owners, consolidated onto shared, mutually recognized systems. The state of payments instruments shows that fragmentation is not inevitable, and that when the parties are brought together their systems can connect.

FIGURE 14 • FRAGMENTATION BY SECTOR



Findings from the Trust Landscape

What the dataset shows.

The dataset describes a landscape that is extensively built but poorly connected. The instruments that create economic trust are many, they span seven layers, and they are the work of hundreds of separate organizations. However, they are only loosely joined to one another. A quarter operate in isolation, recognized by no other instrument, and the layer whose job is to connect the rest is the thinnest and most voluntary part of the whole stack. No single body holds that connecting role.

Where the disconnection sits is the clearest finding. It is not spread evenly, and it is greatest among the instruments that carry the most authority: those that are public, mandatory, and national are the least able to work with other instruments. This follows from how the landscape is built. Governments require trust systems where they gain a direct benefit and leave the rest to voluntary effort, so the work of connecting systems falls to whoever chooses to take it on. Even so, the problem is not the same everywhere. Some sectors are badly fragmented and one, payments, is not, which shows the disconnection can be closed where stakeholders set out to close it.

Two questions this note does not settle, and that further work should, are whether these instruments actually work and what they cost to comply with. This research found published effectiveness evidence for fewer than half of them, and compliance costs are rarely disclosed. The wider implications of these findings, and the questions they raise for stakeholders, are matters for future work.

Codebook: variables, definitions, and tabulations

Every variable used in the analysis is defined here, with its categories and their counts across the 619 instruments. Category labels are the coded values used in the register.

Problem domain

The problem an instrument addresses, formed by grouping the twelve harm families into five domains.

Product integrity aggregates counterfeiting, unsafe products, illegal or misrepresented origin, illicit trade and excise, greenwashing, and social and labour harm. Digital systems and data aggregates cybersecurity, data and research integrity, and AI safety. The other three domains each map to a single harm family.

Category	Count
Product integrity	292
Digital systems and data	149
System interoperability	73
Identity and personal security	67
Financial integrity	38

Harm family

The disaggregated primary public harm an instrument exists to prevent (twelve categories).

Each instrument is assigned to exactly one of twelve harm families, the primary public harm it exists to prevent, from which the five problem domains are aggregated. Coding was model-assisted and run as a single batched pass: each instrument was classified independently from fields already in the register, required to return one value from the fixed list through a structured tool, with no web search, and each returned a confidence. All 619 were coded, with high confidence on 604 and medium on 15; medium-confidence and edge cases were reviewed by hand. The taxonomy is an analytic construction for this note, not an official scheme.

Category	Count
Counterfeiting & falsification	77
Cybersecurity compromise & data interception	74
Interoperability & fragmentation failure	73
Unsafe or non-compliant products	68
Fraud, forgery & impersonation	67

Data, research & assurance integrity failure	56
Greenwashing & ESG/climate misrepresentation	55
Illegal or misrepresented origin & sourcing	46
Financial crime, AML & mispriced risk	38
Other / social & labour harm	23
Illicit trade & tax/excise evasion	23
AI safety & governance failure	19

Trust-stack layer

The functional layer of the trust stack an instrument occupies, from naming a thing at the base to compelling its verification by law at the top.

Category	Count
conformity-assessment-certification	207
data-credential-model	106
governance-mutual-recognition	89
traceability-exchange-protocol	73
mandating-regulation	67
identifier	61
accreditation	16

Instrument type

The form the instrument takes.

Category	Count
binding-regulation	133
voluntary-consensus-standard	122
private-industry-scheme	113
govt-referenced-standard	101
NGO-multistakeholder-scheme	98
accreditation-or-mutual-recognition-arrangement	34
treaty-instrument	18

Ownership (author or origin)

The type of body that authored or owns the instrument: public (a government, regulator, or public international body), NGO or multistakeholder, private (a company or consortium), or hybrid (a public-private arrangement).

Category	Count
public	250
NGO-multistakeholder	163
private	120
hybrid	86

Bindingness

The legal force with which the instrument applies: mandatory (binding by law), de-facto required for market access (compliance is the price of selling into a market), or voluntary.

Category	Count
voluntary	327
de-facto-required-for-market-access	157
mandatory	135

Adoption driver

What drives uptake of the instrument: legal mandate, market demand, or a hybrid of the two.

Category	Count
market-driven	260
mandate-driven	198
hybrid	161

Interoperability posture

Whether the instrument recognizes or interoperates with others (mutual-recognition) or operates in isolation (standalone-silo). This variable underlies the standalone-silo shares reported in the note.

Category	Count
mutual-recognition	463
standalone-silo	156

Geographic scope

The geographic reach of the instrument.

Category	Count
global-multilateral	349
national	167
regional	81
sectoral	22

Sector family

The coded sector of the instrument, from a controlled list.

Category	Count
Digital identity & civil registration	94
Cross-sector conformity assessment & accreditation	68
Food, agriculture & beverages	51
Consumer & manufactured products	41
Cybersecurity & software supply chain	38
Minerals, metals & responsible sourcing	36
Trade, customs & logistics	34
Financial services & AML	31
Energy, carbon & environmental claims	28
Research & data integrity	28
Legal, notarial & e-commerce	27
Payments & cards	25
Pharmaceuticals & medical devices	23
Internet infrastructure & Web PKI	19
AI trust & safety	18
Tobacco & excise goods	17
Metrology & measurement	17
Seafood & fisheries	12
Forestry & timber	10
Content & media integrity	1
Other / unclear	1