

A LEGAL TREATISE · GLOBAL EDITION



Code, Law and Capital

The Global Digital-Assets Order

KHURRAM CHUGHTAI

GLOBAL EDITION · CALL FOR INTEREST · 1 OCTOBER 2026

A LEGAL TREATISE

Code, Law and Capital

The Global Digital-Assets Order

GLOBAL EDITION

KHURRAM CHUGHTAI

JUS AND REM LIMITED

LONDON · MMXXVI

Call for interest · Detailed contents · Contents are subject to change before publication

About this edition

Code, Law and Capital: The Global Digital-Assets Order examines the relations among code, law and capital in the global order of digital assets. Code determines what an arrangement permits, records and prevents; law supplies the sources through which authority, rights, duties and remedies arise; capital directs attention to resources, incentives, claims upon future value and the distribution of gains and losses.

The comparative method follows the asset or claim, the activity undertaken, the actor involved, the infrastructure employed and the point at which practical control is exercised. It puts common questions to different legal orders without assuming that a single regulatory model fits them all. Pakistan is considered where its experience bears upon the inquiry, on the same footing as other jurisdictions.

THE INTELLIGENT-ORDER TEST

For a defined issue, jurisdiction and date, the book applies a six-condition test: **classification legibility, authority traceability, institutional executability, rights and remedy, capital intelligibility and adaptive legality.**

READERSHIP AND COMPANION EDITION

The book is written principally for judges, lawyers, regulators and policymakers, and also for technologists, economists, financial institutions, researchers and students. It is published independently of, and released jointly with, *Code, Law and Capital: The Future of Digital Assets in Pakistan* (Pakistan Library Edition).

Register your interest. This release gives readers, institutions, libraries, reviewers and prospective collaborators the shape of the book, so that they can say whether they wish to be kept informed.

To register, visit ksc-jusnrem.io and complete the short form: name, institution or practice, jurisdiction, edition, and whether you are interested as a reader, reviewer, library, translator or collaborator.

Registrations received by 31 October 2026 will be included in the first circulation of reviewer materials. Registration remains open after that date.

KSC.JUSNREM

Legal Intelligence

This book is one part of a wider body of work. KSC.JUSNREM works with legal intelligence to examine what present arrangements assume, to test how they may change, and to support correction through valid procedures. The practice, the research and a public tool are listed below.

THE PRACTICE

PRACTICE

JUSNREM Counsel & Consulting

The legal practice of KSC.JUSNREM, based in Lahore, with offices in Karachi and Islamabad.

jusnrem.com

RESEARCH

INSTITUTIONAL RECORD

KSC.JUSNREM Legal Intelligence

Published frameworks and essays on how authority, responsibility and remedy are traced when decisions are made through institutions, data, code and models.

ksc-jusnrem.io

DOCTRINE

JUS.automica

A jurisprudential research programme on how law remains law when intelligence takes part in legal functions. In development.

jus-automica.digital

PUBLIC TOOL

FREE

constitution.codes

Pakistan's constitutional history as a version-controlled record: documentary reader, the Constitution as it stood after each amendment, statute library, comparative constitutions and a judgments library.

constitution.codes

Structure at a glance

I	Foundations of the Global Digital-Asset Order	Chapters 1–3
II	Private Law, Claims and the Architecture of Capital	Chapters 4–7
III	Monetary, Financial and Fiscal Orders	Chapters 8–13
IV	Integrity, Institutions, Rights and Remedies	Chapters 14–19
V	Programmable, Decentralised and AI-Mediated Finance	Chapters 20–23
VI	Comparative Legal Orders	Chapters 24–29
VII	Global Coordination, Computational Regulation and Future Orders	Chapters 30–33

This document describes the planned contents of a work in progress. It is not legal advice, does not state the law of any jurisdiction, and must not be relied upon for any decision. Titles, section headings and order may change before publication.

WHERE THIS RELEASE LEADS

1 October 2026	Call for interest: this document, released for both editions.
From November 2026	Reviewer materials, on request, for those who register as reviewers or collaborators.
To be announced	Publication of the two editions. The order of release and the press will be announced at ksc-jusnrem.io .

REGISTRATIONS

Your details. Registrations are held by KSC.JUSNREM (JUSNREM Counsel & Consulting, Lahore) and used only to send news of the two editions and, for those who ask, reviewer materials. They are not shared with anyone else. You may withdraw at any time through the address given on the registration page, and your details will then be removed. Processing is governed by the law of Pakistan; requests from readers elsewhere, including under the EU General Data Protection Regulation, are honoured.

CODE, LAW AND CAPITAL

PART ONE

I



Foundations of the Global Digital-Asset Order

-
- 01 Code, Law and Capital: The Governing Thesis
 - 02 From Ledgers to Programmable Value: An Institutional History
 - 03 The Functional Taxonomy: Assets, Activities, Actors, Infrastructure and Control
-

OI

Code, Law and Capital: The Governing Thesis

When a digital-asset arrangement executes as programmed, how can a legal order identify who holds the right, which authority may act, and who bears the loss?

ABSTRACT

A digital-asset transfer can execute exactly as programmed without settling who held the right transferred, which institution may intervene, or who bears the loss on failure. The chapter sets out the book's governing thesis: Code as architecture and as machine-readable rule, Law as a hierarchy of sources operating through time, and Capital as claims, power and loss. It builds these into the Intelligent-Order Test of six conditions and applies it to a constructed cross-border payment. It also states the counterexamples that would limit the method.

KEYWORDS

Code, Law and Capital ♦ arrangement ♦ lawful chain ♦ Intelligent-Order Test ♦ authority traceability ♦ institutional executability ♦ rules as code

KEY DOCTRINES AND PRINCIPLES

- ♦ *Ordo non est jus*: an operative technical order is not, by that fact, legal authority
- ♦ The unit of analysis is the arrangement, not the token name
- ♦ Control must be disaggregated into information, influence, intervention capacity, authority and responsibility
- ♦ Authoritative instrument, interpretation, representation, decision and remedy must remain separate stages
- ♦ Four economic functions stay distinct: productive formation, intermediation, speculation, monetary substitution

LEADING AUTHORITIES

- ♦ UNIDROIT, Principles on Digital Assets and Private Law (2023)
- ♦ Property (Digital Assets etc) Act 2025
- ♦ UNCITRAL Model Law on Automated Contracting (2024)
- ♦ FSB, High-level Recommendations on crypto-asset activities (2023)
- ♦ OECD Crypto-Asset Reporting Framework
- ♦ Basel Committee, Prudential treatment of cryptoasset exposures

STILL OPEN

The chapter states that its joined method is a contribution only if later chapters explain concrete results or remediable gaps more precisely than single-component accounts.

01 Code, Law and Capital: The Governing Thesis

THE ARCHITECTURE OF THE CHAPTER

1.A	The problem of the global digital-asset order <i>Execution and authority · Value and enforceable rights</i>
1.B	Code as architecture, rule and instrument <i>Protocol constraints and control · Law as Code and Rules as Code</i>
1.C	Law as a hierarchy operating through time <i>Sources and competence · Commencement and review</i>
1.D	Capital as claims, power and loss <i>Productive finance and speculation · Priority and distribution</i>
1.E	Jurisprudence of Intelligent Order <i>Structural, relational and normative intelligence · Lawful chain and human responsibility</i>
1.F	The Intelligent-Order Test <i>Classification, authority and capability · Rights, capital and adaptation</i>
1.G	Method contribution and limits <i>Nearest scholarly predecessors · Evidence and counterexamples</i>

02

From Ledgers to Programmable Value: An Institutional History

How does a recorded event acquire authority over persons who did not write or operate the record, and what does that history teach about tokens and distributed ledgers?

ABSTRACT

Rapid transfer of a claim, authentication of a message and agreement among computers each fall short of a legally effective entitlement. The chapter traces the question of how a record acquires authority through four transformations: recording, transfer, intermediation and authority. It moves from accounts, registers and negotiable instruments through dematerialisation, cryptographic ledgers, native units, tokenisation, exchange failures and payment systems in India and Brazil. It concludes that changes in record-keeping rearrange dependencies rather than remove them, and that each new location of control must be visible, authorised and open to correction.

KEYWORDS

institutional memory ♦ dematerialisation ♦ settlement finality ♦ protocol-native unit ♦ tokenisation ♦ intermediation ♦ path dependence

KEY DOCTRINES AND PRINCIPLES

- ♦ A ledger entry may be declaratory evidence or constitutive of the right
- ♦ Hashes, signatures and consensus answer different questions; none amounts to legal finality
- ♦ Tokenisation may be a constitutive record, an instruction to a register, or evidence of a claim
- ♦ Code changes an institutional dependency; it rarely abolishes all dependencies
- ♦ A date may mark invention, deployment, legal recognition or adoption, rarely all four

LEADING AUTHORITIES

- ♦ UNCITRAL Model Law on Electronic Transferable Records (2017)
- ♦ UNCITRAL Model Laws on Electronic Commerce (1996) and Electronic Signatures (2001)
- ♦ CPSS-IOSCO Principles for Financial Market Infrastructures (2012)
- ♦ UNIDROIT, Principles on Digital Assets and Private Law (2023)
- ♦ BIS-CPMI, Tokenisation in the Context of Money and Other Assets (2024)
- ♦ BIS, Project Agorá report (27 May 2026)

STILL OPEN

The chapter acknowledges that its comparison of UPI and Pix should not be forced, and that adoption evidence does not show social benefit or crypto-asset use.

O2 From Ledgers to Programmable Value: An Institutional History

THE ARCHITECTURE OF THE CHAPTER

2.A	Records, claims and institutional memory <i>Accounts, registries and negotiability · Trust, intermediaries and public authority</i>
2.B	Dematerialisation and networked finance <i>Electronic securities and payment messages · Clearing, settlement and databases</i>
2.C	Cryptography and distributed ledgers <i>Hashing, signatures and consensus · Public, permissioned and hybrid systems</i>
2.D	Native assets and tokenisation <i>Protocol-native units · Representations of off-chain entitlements</i>
2.E	Cycles of intermediation and failure <i>Exchange growth and leverage · Runs, hacks and insolvencies</i>
2.F	Global adoption and exclusion <i>Payments, remittances and capital markets · Access, infrastructure and unequal costs</i>
2.G	What the history teaches legal design <i>Institutional path dependence · Continuity and disruptive dependencies</i>

03

The Functional Taxonomy: Assets, Activities, Actors, Infrastructure and Control

How can a digital-asset arrangement be described, before any legal label is applied, in terms of asset, activity, actor, infrastructure and control?

ABSTRACT

The word token can name a network unit, a debt record or a claim on an issuer, so a label cannot decide who holds what right or who can correct an error. The chapter develops five inquiries, asset or representation, activity, actor, infrastructure and control, with decisive information and risk recorded beside them. It applies them to a constructed cross-border copper token and hands the resulting facts to later legal analysis. It also confines uncertainty to four status terms, UNKNOWN, GAP, DRAFT and CONFLICT, and answers the objection that functional classification expands regulatory perimeters.

KEYWORDS

five-object taxonomy ♦ linked claim ♦ control map ♦ decisive information ♦ oracles and bridges ♦ loss absorption ♦ UNKNOWN and GAP

KEY DOCTRINES AND PRINCIPLES

- ♦ The legally operative record must be stated for each stage, with any break between records marked
- ♦ Information can be decisive without being a power to intervene
- ♦ Technical contribution, benefit, influence and attributable conduct are distinct axes, not a ladder to liability
- ♦ Control is a set of powers over a defined object, not one status
- ♦ A GAP is a finding after a bounded search, not a failure to find

LEADING AUTHORITIES

- ♦ UNIDROIT, Principles on Digital Assets and Private Law (2023)
- ♦ FSB, High-level Recommendations (2023)
- ♦ FSB, Multifunction Crypto-asset Intermediaries (2023)
- ♦ IOSCO, Policy Recommendations for DeFi (2023)
- ♦ BIS-CPMI, Tokenisation in the Context of Money and Other Assets (2024)
- ♦ ERC-20 and ERC-721 token standards

STILL OPEN

The chapter acknowledges that functional classification can quietly expand a regulatory perimeter, and that completing the map does not settle legal effect, evidence or remedy.

03 The Functional Taxonomy: Assets, Activities, Actors, Infrastructure and Control

THE ARCHITECTURE OF THE CHAPTER

3.A	Assets and representations <i>Native units and linked claims · Fungibility, uniqueness and transfer restrictions</i>
3.B	Activities across the lifecycle <i>Issuance, exchange and safeguarding · Lending, staking, validation and advice</i>
3.C	Actors and organisational relationships <i>Issuers, operators and intermediaries · Users, developers, validators and governance participants</i>
3.D	Infrastructure and dependencies <i>Ledgers, interfaces and off-chain records · Oracles, bridges, sequencers and cloud services</i>
3.E	Control and decisive information <i>Keys, pauses, upgrades and redemption · Evidence, access and intervention capacity</i>
3.F	Risk and value maps <i>Credit, liquidity and operational exposure · Revenue, funding and loss absorption</i>
3.G	Classification under uncertainty <i>UNKNOWN, GAP, DRAFT and CONFLICT · Reassessment triggers and documentary support</i>

CODE, LAW AND CAPITAL

PART TWO

II



Private Law, Claims and the Architecture of Capital

-
- 04 Property, Characterisation and the Spectrum of Digital Rights
-
- 05 Secured Transactions, Digital Collateral and Priority
-
- 06 Custody, Intermediation and Insolvency
-
- 07 Private International Law and Cross-Border Digital Claims

O4

Property, Characterisation and the Spectrum of Digital Rights

Who owns a token, and how do control, entitlement and transfer determine which claim prevails when a digital asset is stolen, sold or linked to another asset?

ABSTRACT

Asking who owns a token can mean asking about a credential, a ledger unit, an issuer claim, a platform credit or a right in an underlying asset. The chapter separates these objects and asks what property recognition achieves, how factual control differs from entitlement, and when a transferee defeats an earlier claimant. It compares English, Singaporean and German approaches, works through a stolen-key example and a bond-token example, and treats tracing and remedies. It concludes that a ledger transfer may change control without transferring title or an underlying registered right.

KEYWORDS

control and entitlement ♦ property recognition ♦ innocent acquirer ♦ constitutive register ♦ linked asset ♦ tracing ♦ legal finality

KEY DOCTRINES AND PRINCIPLES

- ♦ Control is a factual capacity; lawful authority must be separately established
- ♦ Technical finality and legal finality answer different questions
- ♦ A person transfers no greater proprietary rights than it has, subject to innocent-acquirer protection
- ♦ A token may refer to an off-chain asset without constituting or transferring it
- ♦ Property recognition makes a claimant visible; procedure and capacity make a judgment effective

LEADING AUTHORITIES

- ♦ UNIDROIT, Principles on Digital Assets and Private Law (2023)
- ♦ Property (Digital Assets etc) Act 2025
- ♦ ByBit Fintech Ltd v Ho Kai Xin [2023] SGHC 199
- ♦ Gesetz über elektronische Wertpapiere (Germany)
- ♦ Law Commission of England and Wales, Digital Assets: Final Report (Law Com No 412)

STILL OPEN

The chapter does not promise that every theft can be reversed, and it leaves priority of security interests, custodian insolvency and applicable law to Chapters 5, 6 and 7.

04 Property, Characterisation and the Spectrum of Digital Rights

THE ARCHITECTURE OF THE CHAPTER

4.A Objects, rights and records

Asset, key, account and underlying entitlement · Contractual, proprietary and statutory rights

4.B Property categories across legal traditions

Common-law approaches · Civil-law and mixed-system approaches

4.C Control, possession and entitlement

Factual powers and lawful authority · Multisignature, recovery and delegation

4.D Transfer and third-party protection

Acquisition and competing claims · Good faith, finality and adverse claims

4.E Linked assets and tokenised rights

Constitutive registers · Promises, representations and transfer restrictions

4.F Interference, restitution and proprietary remedies

Tracing, following and substitutes · Injunctions, delivery and compensation

4.G Harmonisation and residual domestic law

UNIDROIT Principles · Limits of functional convergence

05

Secured Transactions, Digital Collateral and Priority

When a digital asset secures a debt, which legal steps make the creditor's right effective against strangers, and how does priority allocate loss on default or insolvency?

ABSTRACT

A creditor with access to a signing key still cannot tell what the asset secures, whether the grantor could encumber it, or whether the claim outranks others. The chapter separates creation, third-party effectiveness, priority, valuation, enforcement and insolvency, and asks what signal of encumbrance a legal order recognises. It works a two-lender example in which registration-first and control-first rules produce different distributions of the same loss. It then treats haircuts, rehypothecation, automated liquidation, avoidance, netting and cross-border design, ending with the transaction dossier a creditor needs to survive failure.

KEYWORDS

digital collateral ♦ third-party effectiveness ♦ control ♦ priority ♦ rehypothecation ♦ automated liquidation ♦ close-out netting

KEY DOCTRINES AND PRINCIPLES

- ♦ Creation of a security right does not carry the creditor through to priority
- ♦ Control and registration are competing signals of encumbrance; each legal order must choose
- ♦ Code's ability to execute is not a source of enforcement authority
- ♦ Legal priority allocates realised value; it cannot make a volatile asset worth its last price
- ♦ Each collateral question needs its own connecting factor, not one law for the whole arrangement

LEADING AUTHORITIES

- ♦ UNIDROIT, Principles on Digital Assets and Private Law (2023)
- ♦ UNCITRAL Model Law on Secured Transactions (2016)
- ♦ Directive 2002/47/EC on financial collateral arrangements
- ♦ New York UCC
- ♦ UNCITRAL Legislative Guide on Insolvency Law
- ♦ Uniform Law Commission, UCC Amendments (2022)

STILL OPEN

The chapter acknowledges that control-based priority may make an encumbrance less visible to a searcher, and that reform must choose openly which signal lenders can trust.

05 Secured Transactions, Digital Collateral and Priority

THE ARCHITECTURE OF THE CHAPTER

-
- | | |
|-----|---|
| 5.A | The obligation and collateral object
<i>Native assets, issuer claims and receivables · Security assignment, pledge and title transfer</i> |
|-----|---|
-
- | | |
|-----|--|
| 5.B | Creation and third-party effectiveness
<i>Attachment, formalities and authority · Registration, possession and control</i> |
|-----|--|
-
- | | |
|-----|---|
| 5.C | Priority among competing claimants
<i>Secured creditors, purchasers and custodians · Earlier claims and adverse transfers</i> |
|-----|---|
-
- | | |
|-----|--|
| 5.D | Valuation, margin and collateral reuse
<i>Haircuts, volatility and concentration · Rehypothecation and collateral chains</i> |
|-----|--|
-
- | | |
|-----|--|
| 5.E | Enforcement and automated liquidation
<i>Default, notices and legal process · Liquidation code and judicial intervention</i> |
|-----|--|
-
- | | |
|-----|--|
| 5.F | Insolvency and avoidance
<i>Preference, fraudulent transfer and stays · Close-out netting and protected arrangements</i> |
|-----|--|
-
- | | |
|-----|--|
| 5.G | Cross-border collateral design
<i>Applicable law and connecting factors · UNCITRAL, UNIDROIT and domestic reform</i> |
|-----|--|
-

06

Custody, Intermediation and Insolvency

Does a customer's claim to assets held by a platform survive the custodian's failure, and is there anything demonstrably available to satisfy it?

ABSTRACT

A customer who sees ten units on a screen may hold a right to those units, an interest in a pool, a claim for equivalent units, or only a damages claim. The chapter follows custody from deposit through omnibus holding, subcustody and reuse to insolvency, asking what an office-holder can identify, control and return. It contrasts the *Cryptopia* and *Celsius* decisions, reviews segregation, reconciliation and proof of reserves, and works a hypothetical shortfall under two allocation rules. It concludes that custody is credible only when legal form, technical control and capital exposure reconcile at failure.

KEYWORDS

custody ♦ omnibus holding ♦ segregation ♦ reconciliation ♦ subcustody ♦ shortfall ♦ proof of reserves

KEY DOCTRINES AND PRINCIPLES

- ♦ Displayed balance and signing power do not decide the customer's position
- ♦ Address separation is evidence of allocation, not a universal title rule
- ♦ Excluding customer property from the estate answers a priority question, not a quantity question
- ♦ Consent to a use does not establish security or priority against third parties
- ♦ Freezing is distinct from ownership; blockchain speed cannot cure a misclassification

LEADING AUTHORITIES

- ♦ UNIDROIT, Principles on Digital Assets and Private Law (2023)
- ♦ Regulation (EU) 2023/1114 (MiCA)
- ♦ *Ruscoe v Cryptopia Ltd (in liquidation)* [2020] NZHC 728
- ♦ *In re Celsius Network LLC*, Case No 22-10964 (MG) (Bankr SDNY, 2023)
- ♦ UNCITRAL Model Law on Cross-Border Insolvency (1997)
- ♦ IOSCO, Policy Recommendations for Crypto and Digital Asset Markets (2023)

STILL OPEN

The chapter states that its worked shortfall is a decision tree, not a forecast, and that the rateable and bracketed allocation rules are choices rather than an existing universal priority.

o6 Custody, Intermediation and Insolvency

THE ARCHITECTURE OF THE CHAPTER

6.A	Custody models and customer expectations <i>Self-custody, hosted wallets and outsourcing · Omnibus and individually allocated holdings</i>
6.B	Terms, title and fiduciary relationships <i>Bailment, trust, agency and contract · Consent to lending, staking and reuse</i>
6.C	Segregation, reconciliation and audit <i>On-chain balances and internal ledgers · Proof of reserves and missing liabilities</i>
6.D	Outsourcing, affiliates and custody chains <i>Subcustodians and related parties · Cross-border books and control</i>
6.E	Failure and insolvency classification <i>Customer property and estate assets · Shortfalls and unsecured claims</i>
6.F	Resolution, recovery and operational continuity <i>Transfers, keys and access · Administrator powers and customer communication</i>
6.G	Case dossiers and safeguards <i>Exchange insolvencies · Evidence-based custody design</i>

07

Private International Law and Cross-Border Digital Claims

Which court may hear each cross-border digital claim, which law governs each issue, and how can a resulting order be made effective where value and records sit?

ABSTRACT

A digital transfer can touch many legal orders while no single place answers every question a claimant must ask. The chapter separates jurisdiction, contractual choice of law, proprietary connecting factors, issuer and intermediary relationships, insolvency recognition, and recognition and enforcement of orders. It tests them on a constructed custody failure spanning six fictional States. It concludes that no one situs or universal rule resolves the dispute; each connecting factor must be contestable on evidence, and the analysis is measured by the claimant's path to an effective remedy.

KEYWORDS

adjudicative jurisdiction ♦ party autonomy ♦ proprietary connecting factors ♦ account-based claims ♦ centre of main interests ♦ recognition and enforcement ♦ service and tracing

KEY DOCTRINES AND PRINCIPLES

- ♦ Jurisdiction, applicable law, insolvency and enforcement each need a separate connection
- ♦ A contract clause binds its parties and does not settle third-party priority
- ♦ Node or server location is not a self-proving situs for a proprietary contest
- ♦ Recognising a foreign insolvency, recognising its judgments and transferring an asset are distinct acts
- ♦ Relief must be framed by the control actually held by the person bound

LEADING AUTHORITIES

- ♦ Regulation (EU) No 1215/2012 (Brussels I Recast)
- ♦ Regulation (EC) No 593/2008 (Rome I)
- ♦ UNIDROIT Principles on Digital Assets and Private Law (2023)
- ♦ UNCITRAL Model Law on Cross-Border Insolvency (1997)
- ♦ Hague Convention on Recognition and Enforcement of Foreign Judgments (2019)
- ♦ Hague Convention on Choice of Court Agreements (2005)

STILL OPEN

It asks whether a factor-based approach to wholly decentralised applications, as in the Law Commission's consultation, can stay predictable to strangers who financed an asset before litigation.

07 Private International Law and Cross-Border Digital Claims

THE ARCHITECTURE OF THE CHAPTER

7.A Jurisdiction and forum

Defendant connections and harmful events · Forum clauses, consumers and interim relief

7.B Contractual choice of law

Party autonomy and mandatory rules · Standard terms and weaker parties

7.C Proprietary connecting factors

Location, control and system choice · Third-party effects and rival claimants

7.D Issuer, platform and intermediary relationships

Account-based claims · Linked registers and custody contracts

7.E Cross-border insolvency

Main proceedings, recognition and assistance · Customer claims and estate administration

7.F Recognition, evidence and enforcement

Foreign judgments and orders · Service, tracing and practical execution

7.G Convergence and reform

UNIDROIT and Law Commission work · Open questions and model solutions

CODE, LAW AND CAPITAL

PART THREE

III



Monetary, Financial and Fiscal Orders

-
- | | |
|----|--|
| 08 | Money, Monetary Sovereignty and Payment Infrastructure |
|----|--|
-
- | | |
|----|--|
| 09 | Stablecoins: Reserves, Redemption and Resolution |
|----|--|
-
- | | |
|----|---|
| 10 | Securities, Derivatives and Tokenised Market Infrastructure |
|----|---|
-
- | | |
|----|---|
| 11 | Banking, Deposit-Taking and Prudential Exposure |
|----|---|
-
- | | |
|----|--|
| 12 | The Fiscal Order: Taxation, Accounting and Reporting |
|----|--|
-
- | | |
|----|---|
| 13 | Market Conduct, Disclosure and Consumer and Investor Protection |
|----|---|

08

Money, Monetary Sovereignty and Payment Infrastructure

Which claim does a payee actually receive, and when is it final, when digital money and payment infrastructure alter the chain from instruction to settlement?

ABSTRACT

A displayed transfer or credited balance does not itself establish discharge of a debt, finality of settlement or a right to redeem. The chapter follows the payment chain from unit of account to settlement asset, comparing cash, bank deposits, e-money, native tokens, currency-referenced tokens, CBDCs and wholesale tokenised settlement. It works a constructed Indonesia–Kenya payment through provisional credit, principal risk and conversion, and examines currency substitution and remittance costs. It concludes that any claimed improvement must be shown against complete alternative routes, including conventional instant-payment systems.

KEYWORDS

legal tender ♦ unit of account ♦ settlement asset ♦ finality ♦ delivery versus payment ♦ CBDC ♦ monetary sovereignty

KEY DOCTRINES AND PRINCIPLES

- ♦ Read the liability rather than the screen
- ♦ Unit of account and settlement asset are different questions
- ♦ System finality and private-law discharge need not coincide
- ♦ Compare complete routes by total cost, time, certainty and remedy
- ♦ Foreign or new does not itself demonstrate harm to monetary sovereignty

LEADING AUTHORITIES

- ♦ CPMI-IOSCO Principles for Financial Market Infrastructures (2012)
- ♦ Directive 2009/110/EC (electronic money)
- ♦ Regulation (EU) 2023/1114 (MiCA)
- ♦ Directive 98/26/EC (settlement finality)
- ♦ Bank of Jamaica (Amendment) Act 2022
- ♦ Bahamian Dollar Digital Currency Regulations 2021

STILL OPEN

It recognises that no universal optimum exists among retail, wholesale and intermediary CBDC designs, which depends on local payment quality, banking structure and public mandate.

08 Money, Monetary Sovereignty and Payment Infrastructure

THE ARCHITECTURE OF THE CHAPTER

8.A	Monetary concepts and legal categories <i>Tender, debt discharge and payment acceptance · Unit of account and settlement assets</i>
8.B	Public and private digital money <i>Central-bank money, bank deposits and e-money · Native tokens and stablecoins</i>
8.C	Payments, clearing and settlement <i>Messaging, execution and finality · Delivery versus payment and payment versus payment</i>
8.D	Tokenised deposits and wholesale systems <i>Programmable settlement platforms · Interoperability and access rules</i>
8.E	CBDCs and public design choices <i>Retail, wholesale and intermediary models · Privacy, resilience and public accountability</i>
8.F	Currency substitution and capital movements <i>Dollarisation, monetary transmission and liquidity · Exchange restrictions and cross-border payments</i>
8.G	Payments, inclusion and public value <i>Remittances, merchant costs and accessibility · Competition, interoperability and exclusion</i>

09

Stablecoins: Reserves, Redemption and Resolution

What makes a stablecoin's promise of stability legally and economically credible when redemption, reserve access and resolution are tested at the same moment?

ABSTRACT

A stablecoin's trading price does not show who must pay a holder, from which assets, or when. The chapter separates design, issuer and user claims, reserve quality and custody, redemption access, governance dependencies, runs and resolution. It works a constructed token, Meridian, through a weekend payment-bank outage and then a genuine reserve loss, showing that delay and deficit call for different remedies. It compares the FSB baseline with regimes in the European Union, Hong Kong, the United States and Singapore, and concludes that reserves, claims, channels and failure process cannot substitute for one another.

KEYWORDS

stablecoin ♦ reserve assets ♦ redemption ♦ segregation ♦ attestation ♦ depeg ♦ resolution

KEY DOCTRINES AND PRINCIPLES

- ♦ Price, asset value, legal entitlement and payment time answer different questions
- ♦ A profitable arbitrage price is not a right to compel the issuer to pay
- ♦ Segregation asks whose assets the reserve is when the issuer fails
- ♦ A supervisory recovery plan must be executable through named institutions and legal powers
- ♦ Enacted-but-prospective law is distinct from operative law and from policy consultation

LEADING AUTHORITIES

- ♦ Regulation (EU) 2023/1114 (MiCA), Titles III and IV
- ♦ FSB High-level Recommendations for Global Stablecoin Arrangements (2023)
- ♦ GENIUS Act, Pub L No 119-27
- ♦ Hong Kong Stablecoins Ordinance
- ♦ MAS stablecoin framework and 2026 Payment Services Act consultation
- ♦ IMF-FSB Synthesis Paper (2023)

STILL OPEN

It leaves open whether any qualifying final GENIUS Act regulation issued earlier, noting the official materials examined establish no exhaustive negative.

09 Stablecoins: Reserves, Redemption and Resolution

THE ARCHITECTURE OF THE CHAPTER

9.A	Designs and promises <i>Fiat-backed, crypto-collateralised and algorithmic structures · Issuer and user claims</i>
9.B	Reserve assets and custody <i>Quality, liquidity, concentration and segregation · Attestations, audits and ownership</i>
9.C	Redemption rights and distribution <i>Direct and intermediary access · Fees, timing, suspensions and minimums</i>
9.D	Governance and operational dependencies <i>Banks, custodians, oracles and administrators · Conflicts and concentration</i>
9.E	Runs, depegging and contagion <i>Liquidity spirals and collateral sales · Market structure and interconnected exposure</i>
9.F	Supervision, recovery and resolution <i>Licensing, safeguards and intervention · Insolvency, priority and cross-border coordination</i>
9.G	Comparative stablecoin regimes <i>FSB baseline · Domestic implementation and divergence</i>

IO

Securities, Derivatives and Tokenised Market Infrastructure

When does a digital arrangement create a security or derivative obligation, and how must market infrastructure keep the token aligned with the legally operative record?

ABSTRACT

Tokenisation can change how securities are issued, traded, cleared and settled without merging those functions into one event. The chapter examines the statutory perimeter for shares, debt, collective investments, investment contracts and derivatives, then issuance, disclosure, trading-venue roles, vertical integration, registers and settlement. A worked tokenised bond shows how a ledger entry can be final while the registrar rejects the transfer. Comparing the European Union, Brazil and the United States, it concludes that classification follows enacted law applied to actual rights, and that investors need an enforceable claim against an answerable person.

KEYWORDS

investment contract ♦ financial instrument ♦ tokenised securities ♦ authoritative register ♦ delivery versus payment ♦ vertical integration ♦ DLT Pilot Regime

KEY DOCTRINES AND PRINCIPLES

- ♦ The first question is what the holder can demand, against whom, under which instrument
- ♦ Functional inquiry collects the facts; enacted law selects their legal significance
- ♦ Ledger persistence, legal finality and payment availability are distinct
- ♦ A protocol atomic swap does not include the registrar's constitutive decision
- ♦ A conflict is not resolved by publishing code if the operator controls data feeds and collateral

LEADING AUTHORITIES

- ♦ Directive 2014/65/EU (MiFID II), annex I, section C
- ♦ Regulation (EU) 2023/1114 (MiCA)
- ♦ SEC v W J Howey Co, 328 US 293 (1946)
- ♦ Lei 6.385/1976 and CVM Guidance Opinion 40 (2022)
- ♦ Regulation (EU) 2022/858 (DLT Pilot Regime)
- ♦ SEC v Ripple Labs Inc, No 20-cv-10832 (SDNY)

STILL OPEN

It treats the SEC's August 2026 Regulation Crypto Assets proposal as unresolved, so tailored offering exemptions remain a proposal rather than law.

10 Securities, Derivatives and Tokenised Market Infrastructure

THE ARCHITECTURE OF THE CHAPTER

10.A Investment rights and statutory tests

Shares, debt, collective investment and investment contracts · Economic substance and legal form

10.B Issuance, distribution and disclosure

Public offers, private placements and admission · Issuer obligations and intermediary responsibility

10.C Derivatives and structured exposure

Futures, options, swaps and synthetic assets · Leverage, margin and retail access

10.D Trading platforms and market organisation

Exchange, brokerage and dealer functions · Vertical integration and conflicts

10.E Tokenised securities and registers

Constitutive records and transfer agents · Corporate actions and settlement assets

10.F Clearing, settlement and systemic dependencies

Netting, collateral and finality · DLT pilots, interoperability and operational risk

10.G Comparative perimeter disputes

Enforcement, judgments and legislation · IOSCO baseline and residual differences

II

Banking, Deposit-Taking and Prudential Exposure

How do tokenised deposits, custody and own-account crypto exposures reach a bank's balance sheet, and which protection and prudential rules actually apply on failure?

ABSTRACT

A bank may hold, safeguard, lend against or issue tokens, and each activity creates a different claim and route of loss. The chapter builds an exposure ledger covering deposit status, deposit insurance, Basel prudential groups, capital, liquidity, outsourcing, stress and resolution. It applies the ledger to a hypothetical Meridian Bank, showing that a modest own-account holding can coexist with serious loss through a collateralised loan, frozen custody or a redemption run. It concludes that international standards bind only through domestic instruments, and that protection depends on the legally qualifying liability.

KEYWORDS

tokenised deposit ♦ segregated custody ♦ Basel SCO60 ♦ deposit insurance ♦ Group 2 exposure ♦ outsourcing ♦ resolution

KEY DOCTRINES AND PRINCIPLES

- ♦ Follow what the bank owes, owns, controls or depends upon
- ♦ A prudential group is not a property-law category
- ♦ Liquidity support and loss absorption answer different questions
- ♦ Legal right to collateral, prudential recognition of it and stressed proceeds are three values
- ♦ Custody value and the bank's loss-bearing position must not be conflated

LEADING AUTHORITIES

- ♦ Basel Committee SCO60: Cryptoasset exposures
- ♦ Basel Committee DIS55: Cryptoasset exposures
- ♦ Directive 2014/49/EU (deposit guarantee schemes)
- ♦ EBA assessment of tokenised deposits (December 2024)
- ♦ PRA letter on tokenised assets and cryptoasset exposures (May 2026)
- ♦ FDIC proposal of 7 April 2026

STILL OPEN

It treats whether capital standards displace risk to less supervised providers or reduce it as competing empirical hypotheses requiring matched observations.

II Banking, Deposit-Taking and Prudential Exposure

THE ARCHITECTURE OF THE CHAPTER

- 11.A Bank activities and claims**
Deposit-taking, issuance, custody and brokerage · Own-account positions and lending
-
- 11.B Tokenised deposits and depositor protection**
Deposit status and transfer mechanisms · Insurance exclusions and resolution
-
- 11.C Crypto-asset prudential classification**
Basel exposure groups and conditions · Domestic implementation and exceptions
-
- 11.D Capital, liquidity and concentration**
Credit, market and operational capital · Large exposures, liquidity and collateral
-
- 11.E Counterparty, custody and outsourcing**
Service providers and subcustodians · Governance, due diligence and recovery
-
- 11.F Stress, contagion and resolution**
Bank runs, interconnectedness and fire sales · Liquidity support and loss allocation
-
- 11.G Supervisory information and limits**
Exposure reporting and scenario testing · Data quality, perimeter and proportionality
-

I2

The Fiscal Order: Taxation, Accounting and Reporting

How can tax, accounting and information reporting be connected to a valid charge, reliable evidence and a challengeable assessment when digital-asset transfers are visible but fiscally opaque?

ABSTRACT

A ledger shows movements between addresses without identifying the taxpayer, consideration or cost, so reporting begins rather than completes a tax inquiry. The chapter treats substantive tax, financial accounting and information reporting as separate systems. It examines taxable events, mining and staking receipts, residence and source, valuation, the OECD Crypto-Asset Reporting Framework, and taxpayer rights. A worked designer's transaction across States R, S and P separates income, gain and loss. It concludes that reports are investigatory inputs, and that assessments must remain contestable and capable of correction across borders.

KEYWORDS

taxable event ♦ capital and revenue ♦ staking rewards ♦ CARF ♦ residence and source ♦ fair value ♦ assessment

KEY DOCTRINES AND PRINCIPLES

- ♦ An international reporting standard operates only through domestic legislation and exchange arrangements
- ♦ Book gain, fair-value movement and taxable gain are not automatically equal
- ♦ Reporting intermediaries are not tax creditors
- ♦ Network geography is a poor substitute for fiscal connection
- ♦ A data match must be tested before an adverse decision

LEADING AUTHORITIES

- ♦ OECD Crypto-Asset Reporting Framework and 2023 CRS update
- ♦ Council Directive (EU) 2023/2226 (DAC8)
- ♦ Case C-264/14 Skatteverket v Hedqvist
- ♦ IRS Revenue Ruling 2023-14
- ♦ IFRS Interpretations Committee agenda decision (2019)
- ♦ FASB ASU 2023-08

STILL OPEN

It states that no aggregate revenue gain or compliance yield is asserted, because comparable validated evidence of assessed, collected and reversed amounts is lacking.

12 The Fiscal Order: Taxation, Accounting and Reporting

THE ARCHITECTURE OF THE CHAPTER

12.A	Taxable events and legal characterisation <i>Disposal, exchange, income and business receipts · Capital, revenue and consumption-tax distinctions</i>
12.B	Mining, staking, lending and rewards <i>Accrual, realisation and receipt · Costs, deductions and losses</i>
12.C	Residence, source and cross-border exposure <i>Individuals, entities and permanent establishments · Withholding, treaties and double taxation</i>
12.D	Valuation, records and accounting <i>Fair value, cost, impairment and disclosures · Missing histories, fees and exchange rates</i>
12.E	CARF, CRS and domestic reporting <i>Covered persons, transactions and due diligence · Implementation, commencement and exchange relationships</i>
12.F	Administration, enforcement and taxpayer rights <i>Assessment, penalties, appeals and limitation · Information powers, privacy and proportionality</i>
12.G	Fiscal policy and distribution <i>Compliance costs and revenue evidence · Neutrality, incentives and avoidance</i>

I3

Market Conduct, Disclosure and Consumer and Investor Protection

At which point in a customer's journey does each disclosure, conduct and redress device operate, whom does it bind, and what loss can it prevent or repair?

ABSTRACT

A person meeting a digital-asset product passes from promotion to entry, participation, exit and complaint, and each protective device operates at a different point and binds a different actor. The chapter examines information asymmetry, promotions, suitability and appropriateness, conflicts, market abuse and redress, testing them against a constructed platform, Meridian. It concludes that every duty must be traced to an identified legal source, and that warnings, bans and licences should be judged by user understanding, loss, complaint outcomes and displacement rather than by their existence. It closes with a four-file dossier method.

KEYWORDS

information asymmetry ♦ Financial promotions ♦ suitability and appropriateness ♦ conflicts of interest ♦ market abuse surveillance ♦ complaints and redress ♦ displacement effects

KEY DOCTRINES AND PRINCIPLES

- ♦ The relevant risk is an arrangement, not an asset label
- ♦ Suitability and appropriateness answer different questions and attach to different triggers
- ♦ Disclosure assists a decision only if it reaches the person in time to affect it
- ♦ Detection is a reason to investigate, not a substitute for proof
- ♦ Protection must be assessed after the transaction as well as before it

LEADING AUTHORITIES

- ♦ Regulation (EU) 2023/1114 (MiCA)
- ♦ IOSCO, Policy Recommendations for Crypto and Digital Asset Markets (November 2023)
- ♦ FCA, PS23/6: Financial Promotion Rules for Cryptoassets (2023)
- ♦ FTC Endorsement Guides
- ♦ SFC Hong Kong, virtual-asset trading platform requirements and FAQs
- ♦ CFPB, Complaint Bulletin on crypto-assets (10 November 2022)

STILL OPEN

The chapter acknowledges that no cited source supplies a global causal estimate of protection, so comparative claims about outcomes remain dependent on cohort, denominator and period.

13 Market Conduct, Disclosure and Consumer and Investor Protection

THE ARCHITECTURE OF THE CHAPTER

13.A	Information asymmetry and product design <i>Risk, complexity and behavioural design · Retail, professional and vulnerable users</i>
13.B	Promotions, disclosure and representations <i>Claims, endorsements and incentives · Reserve, yield and decentralisation statements</i>
13.C	Suitability, appropriateness and access <i>Advice, assessments and restrictions · Financial inclusion and proportionality</i>
13.D	Conflicts and fair dealing <i>Proprietary trading, order handling and listing · Related parties and fee structures</i>
13.E	Market abuse and surveillance <i>Manipulation, insider information and wash trading · On-chain and off-chain detection limits</i>
13.F	Complaints, redress and collective recovery <i>Internal complaints, ombuds mechanisms and litigation · Compensation schemes and uninsured losses</i>
13.G	Evidence of protection and residual gaps <i>IOSCO recommendations · Domestic outcomes and displacement effects</i>

PART FOUR

IV



Integrity, Institutions, Rights and Remedies

-
- | | |
|----|---|
| 14 | Financial Integrity: AML/CFT, Sanctions and Cross-Border Compliance |
|----|---|
-
- | | |
|----|---|
| 15 | Data Protection, Identity, Cybersecurity and Operational Resilience |
|----|---|
-
- | | |
|----|--|
| 16 | Electronic Transactions, Signatures and Automated Acts |
|----|--|
-
- | | |
|----|---|
| 17 | Electronic Evidence, Forensics and Adjudication |
|----|---|
-
- | | |
|----|---|
| 18 | Institutional Architecture, Capability and Coordination |
|----|---|
-
- | | |
|----|--|
| 19 | Enforcement, Courts, Review and Remedies |
|----|--|

I4

Financial Integrity: AML/CFT, Sanctions and Cross-Border Compliance

How far do AML/CFT, Travel Rule and sanctions duties attach to particular persons and functions in digital-asset transfers, and what evidence and remedies must accompany each intervention?

ABSTRACT

A ledger can be visible to everyone while the institution asked to know who paid whom learns little, and suspicion alone confers no power to restrain property. The chapter traces how FATF standards become enforceable only through domestic instruments, then tests which actors (custodial exchanges, banks, issuers, DeFi operators, software authors, validators, self-hosted wallet users) carry which duties. It examines customer due diligence, the Travel Rule, sanctions blocking and delisting, and cross-border recovery, and works a constructed EU transfer. It concludes that each intervention must keep its source, actor, evidence and route of correction.

KEYWORDS

FATF standards ♦ VASP perimeter ♦ Travel Rule ♦ unhosted wallets ♦ sanctions blocking ♦ customer due diligence ♦ false positives

KEY DOCTRINES AND PRINCIPLES

- ♦ FATF Recommendations are standards addressed to states; enforceability comes from the domestic instrument
- ♦ Duties attach to a regulated function and a person able to perform it
- ♦ Suspicion that starts an inquiry is distinct from proof that justifies deprivation
- ♦ Blocking, rejecting and reporting are distinct; so are correction, licence and delisting
- ♦ Practical incapacity does not extinguish an enacted duty; it may require redesign or cessation

LEADING AUTHORITIES

- ♦ FATF Recommendations (updated June 2026), including Recommendations 10 and 15 and Interpretive Note
- ♦ FATF, Updated Guidance for a Risk-Based Approach to VAs and VASPs (2021)
- ♦ Regulation (EU) 2023/1113
- ♦ FinCEN guidance FIN-2019-G001 (9 May 2019)
- ♦ OFAC, Sanctions Compliance Guidance for the Virtual Currency Industry (2021), FAQs 646 and 1196
- ♦ OFSI, UK Financial Sanctions: General Guidance

STILL OPEN

The chapter states that the hardest case lies between operator and code, where several actors each hold part of the power needed to provide a service, and their duties must be established separately.

14 Financial Integrity: AML/CFT, Sanctions and Cross-Border Compliance

THE ARCHITECTURE OF THE CHAPTER

14.A	Sources, powers and regulated functions <i>FATF standards and domestic implementation · VASPs, financial institutions and excluded functions</i>
14.B	Risk assessment and customer due diligence <i>Beneficial ownership, enhanced checks and monitoring · Proportionality, access and documentation</i>
14.C	The Travel Rule and information exchange <i>Originator, beneficiary and counterparty data · Interoperability and cross-border restrictions</i>
14.D	Unhosted wallets, DeFi and offshore providers <i>Control and responsible persons · Geographical reach and practical capacity</i>
14.E	Sanctions screening, blocking and remedies <i>Targeted persons, assets and services · Licensing, exemptions, delisting and review</i>
14.F	Investigation, confiscation and international assistance <i>Suspicious reports, financial intelligence and evidence · Seizure, restraint and cross-border cooperation</i>
14.G	Implementation outcomes and safeguards <i>Mutual evaluations and targeted updates · Effectiveness, false positives and contestability</i>

15

Data Protection, Identity, Cybersecurity and Operational Resilience

How can identity, personal-data, security and resilience duties be applied to permanent, replicated ledger architectures without collapsing their separate legal questions or leaving affected people without correction or relief?

ABSTRACT

A tokenised payment can settle correctly while exposing the people whose identities it verifies or stranding those who cannot reach their assets during an outage. The chapter separates verification, authentication and authorisation, then works through controllers and processors, ledger metadata, data-subject rights, transfers, key management, concentrated cloud dependencies and incident duties. It compares GDPR, LGPD, the Singapore PDPA, DORA, NIST guidance and New York Part 500 as sources of differing force, and tests a lifecycle map on a constructed breach-and-outage scenario. It concludes that accountability lies in whether affected people can obtain an explanation and test the correction.

KEYWORDS

pseudonymity ♦ controllers and processors ♦ data minimisation ♦ key recovery ♦ concentrated dependencies ♦ operational resilience ♦ incident notification

KEY DOCTRINES AND PRINCIPLES

- ♦ Verification, authentication and authorisation answer different questions
- ♦ Pseudonymity is contextual; identifiability is relational and evidence-based
- ♦ A correction transaction is evidence of correction, not necessarily a cure for continuing exposure
- ♦ Irrecoverability, delegated recovery and shared recovery allocate loss differently and cannot be presented as equivalent
- ♦ A service-restoration target and a data-recovery target answer different questions

LEADING AUTHORITIES

- ♦ Regulation (EU) 2016/679 (GDPR)
- ♦ Lei No 13.709/2018 (Brazil, LGPD)
- ♦ Personal Data Protection Act 2012 (Singapore)
- ♦ Regulation (EU) 2022/2554 (DORA)
- ♦ NIST Cybersecurity Framework 2.0
- ♦ 23 NYCRR Part 500
- ♦ EDPB Guidelines 9/2022 on Personal Data Breach Notification

STILL OPEN

The chapter acknowledges that the sources compared differ in force and reach, so its comparison illuminates questions every arrangement must ask without making any jurisdiction's answer universal.

15 Data Protection, Identity, Cybersecurity and Operational Resilience

THE ARCHITECTURE OF THE CHAPTER

15.A	Identity, attribution and access <i>Pseudonymity, verification and credentials · Identity providers, exclusion and recovery</i>
15.B	Personal data and ledger architecture <i>Controllers, processors and joint arrangements · Public metadata, linkability and persistent records</i>
15.C	Rights, safeguards and cross-border transfers <i>Access, rectification, objection and erasure · Data minimisation, retention and transfer mechanisms</i>
15.D	Security and key management <i>Authentication, key lifecycle and recovery · Threat models and security assurance</i>
15.E	Outsourcing and concentrated dependencies <i>Cloud services, custody and critical providers · Contracts, audit access and exit</i>
15.F	Operational resilience and incident duties <i>Continuity, testing, reporting and recovery · Bridges, oracles and settlement disruption</i>
15.G	Cyber incidents and accountability <i>Investigation, disclosure and compensation · Supervisory learning and proportionality</i>

I6

Electronic Transactions, Signatures and Automated Acts

When does an electronic or automated act have legal effect, to whom is it attributable, and who bears the loss when the system produces the wrong result?

ABSTRACT

An electronic trace shows that a message was sent or a token moved, but not whether a formality was met, who authorised the system, or who must restore value after an error. The chapter separates five questions: recognition of electronic form, authentication, attribution, consent and capacity, and remedy. It applies UNCITRAL texts as comparative instruments, alongside eIDAS and the UK Electronic Trade Documents Act 2023, to signatures, receipt, transferable records and automated contracting. A worked cross-border sale with a feed error shows that form, attribution, consent and remedy can each receive a different answer.

KEYWORDS

functional equivalence ♦ technology neutrality ♦ attribution ♦ transferable electronic records ♦ automated contracting ♦ input error ♦ mandatory law

KEY DOCTRINES AND PRINCIPLES

- ♦ Functional equivalence is formality-specific and begins from the purpose of the formality
- ♦ Authentication concerns source; attribution concerns whose act the law treats it as
- ♦ A key is an object of control, not a legal person
- ♦ Execution proves the program's transition; it does not conclusively establish discharge
- ♦ A model law is a legislative proposal, not an enacted rule

LEADING AUTHORITIES

- ♦ UNCITRAL Model Law on Electronic Commerce (1996)
- ♦ UNCITRAL Model Law on Electronic Signatures (2001)
- ♦ United Nations Convention on the Use of Electronic Communications in International Contracts (2005)
- ♦ UNCITRAL Model Law on Electronic Transferable Records (2017)
- ♦ UNCITRAL Model Law on Automated Contracting (2024)
- ♦ Regulation (EU) No 910/2014 (eIDAS)
- ♦ Electronic Trade Documents Act 2023 (UK)

STILL OPEN

The chapter accepts that technology neutrality may conceal unequal reliability and unequal access, and treats that objection as valid.

16 Electronic Transactions, Signatures and Automated Acts

THE ARCHITECTURE OF THE CHAPTER

-
- 16.A **Recognition and functional equivalence**
Writing, originals and retention · Non-discrimination and technology neutrality

 - 16.B **Signatures, authentication and authority**
Electronic signatures and cryptographic credentials · Reliability, intention, delegation and misuse

 - 16.C **Dispatch, receipt and electronic records**
Time, place and acknowledgments · Integrity, accessibility and retention

 - 16.D **Transferable electronic records**
Control, singularity and integrity · Transfer of rights and underlying instruments

 - 16.E **Automated formation and performance**
Electronic agents and machine outputs · Attribution, disclosures and party autonomy

 - 16.F **Errors, unexpected outcomes and mandatory law**
Input errors, coding faults and dynamic information · Consumer protections and non-excludable duties

 - 16.G **Cross-border recognition and implementation**
UNCITRAL texts and domestic enactments · Reservations, exclusions and applicable law

I7

Electronic Evidence, Forensics and Adjudication

How should a court connect blockchain records, platform data and analytics to a legal finding, and what must be preserved, disclosed and explained before that finding meets the governing burden?

ABSTRACT

A transaction graph can make a dispute look continuous while the legal links between transfer, control, identity, authority and entitlement remain unproved. The chapter begins from the proposition to be proved and the forum's burden, then follows collection, chain of custody, authentication, hearsay, address clustering, error rates, expert evidence, disclosure and confidentiality. It compares US federal rules, eIDAS, the UNCITRAL model law, English and Indian evidence statutes, and tests an inference ledger on a constructed custody failure. It concludes that a finding must state which question was decided and which links remain open.

KEYWORDS

proposition map ♦ chain of custody ♦ authentication and admissibility ♦ address clustering ♦ expert evidence ♦ disclosure ♦ inference ledger

KEY DOCTRINES AND PRINCIPLES

- ♦ Transfer, operational control, identity, authority and entitlement are five distinct objects
- ♦ The burden governs the final decision; it cannot repair a broken link in the chain
- ♦ Authentication is proposition specific; admissibility is neither endorsement nor a measure of weight
- ♦ A clustering output is a conditional statement under stated assumptions, not an identification
- ♦ Disclosure must suffice to test the decisive step, without unlimited access to unrelated data

LEADING AUTHORITIES

- ♦ UNCITRAL Model Law on Electronic Commerce
- ♦ Regulation (EU) No 910/2014 (eIDAS)
- ♦ Federal Rules of Evidence (US)
- ♦ Bharatiya Sakshya Adhiniyam 2023 (India)
- ♦ Civil Evidence Act 1995 (England and Wales)
- ♦ *Ruscoe v Cryptopia Ltd (in liquidation)* [2020] NZHC 728
- ♦ OSC staff review of QuadrigaCX (2020)

STILL OPEN

The chapter states that a method travels only with its procedural status, and that neither the QuadrigaCX review nor Ruscoe supplies the facts or precedent for its constructed Meridian dispute.

17 Electronic Evidence, Forensics and Adjudication

THE ARCHITECTURE OF THE CHAPTER

- 17.A Questions to be proved**
Transfer, control, identity and entitlement · Civil, criminal and administrative standards

- 17.B Collection, preservation and provenance**
Device records, logs and ledger data · Chain of custody, timestamps and reproducibility

- 17.C Authentication and admissibility**
Electronic-record rules · Hearsay, business records and certificates

- 17.D Attribution and blockchain analytics**
Address clustering, labels and tracing · Probability, error rates and alternative explanations

- 17.E Expert evidence and intelligibility**
Qualifications, methods and limitations · Court-appointed and party experts

- 17.F Disclosure, fairness and sensitive information**
Access to underlying data and tools · Privilege, privacy and security restrictions

- 17.G Judgments, orders and evidential learning**
Findings, reasons and procedural posture · Reusable forensic standards

I8

Institutional Architecture, Capability and Coordination

What must be shown before a public body's response to a digital-asset failure is executable: a competent institution, an operative instrument, capacity to establish facts, and a reviewable procedure?

ABSTRACT

A statute may name a regulator that has no validly appointed decision maker, no lawful route to the books and no staff able to reconcile chain transfers with customer claims. The chapter defines institutional executability as competence, an operative instrument, capacity and procedure, and applies it to mandates, regulatory overlap, resources, decision files, coordination models, information gateways and transition. It compares MiCA, the UK, Hong Kong, Brazil and Singapore, and completes a mandate-and-capability matrix for a custodial redemption shortfall. It concludes that identifying the link that fails is more useful than adding another committee or platform.

KEYWORDS

institutional executability ♦ competent authority ♦ lawful chain ♦ regulatory overlap ♦ lawful gateway ♦ coordination models ♦ transition and commencement

KEY DOCTRINES AND PRINCIPLES

- ♦ Institutional executability joins competence, instrument, capacity and procedure
- ♦ International recommendations cannot supply a missing domestic appointment or coercive power
- ♦ Referral can accelerate an authorised act but cannot give authority to an actor who lacks it
- ♦ Purchased analytics or a private risk score cannot decide whether a legal test is met
- ♦ The unit of analysis is the decision and its lawful path, not the institutional chart

LEADING AUTHORITIES

- ♦ Regulation (EU) 2023/1114 (MiCA)
- ♦ FSB, High-level Recommendations (17 July 2023)
- ♦ FSB, Thematic Review (16 October 2025)
- ♦ Brazil, Law No 14,478/2022 and Decree No 11,563/2023
- ♦ Bank of England and FCA, Approach to Joint Regulation of Systemic Stablecoin Issuers (30 June 2026)
- ♦ Hong Kong Stablecoins Ordinance (commenced 1 August 2025)

STILL OPEN

The chapter acknowledges that its matrix states no jurisdiction's law and that a blank answer signals an unresolved question, not illegality or institutional readiness.

18 Institutional Architecture, Capability and Coordination

THE ARCHITECTURE OF THE CHAPTER

- 18.A Competence and institutional mandate**
Constitutional, statutory and delegated authority · Appointments, delegations and independence
-
- 18.B Regulatory allocation and overlap**
Central banks, financial regulators and tax authorities · Integrity, data, competition and consumer bodies
-
- 18.C Operational capacity and resources**
Staff, expertise, budgets and systems · Supervisory tools, procurement and evidence access
-
- 18.D Decision procedures and accountability**
Consultation, reasons and records · Conflicts, oversight and review
-
- 18.E Coordination and information sharing**
Domestic arrangements and cross-border colleges · Lawful gateways, security and escalation
-
- 18.F Lawful transition and implementation**
Commencement, savings and staged obligations · Legacy firms, proportionality and continuity
-
- 18.G Measuring institutional executability**
Lawful chain diagnostics · Outcomes, learning and adaptive legality
-

19

Enforcement, Courts, Review and Remedies

What must connect a right, a public decision or a judgment to an act that actually delivers relief when transfers are irreversible, custodians are unreachable and controllers are abroad?

ABSTRACT

A ledger may preserve a transfer while its recipient is unknown, and an authority may announce a freeze that nobody in its jurisdiction can execute. The chapter sets out the lawful chain from valid instrument to executable remedy: public inspection and intervention, administrative sanction and review, civil claims, criminal process, urgent and proprietary relief, and remedies under technical constraint. It tests the chain against a constructed custody scenario involving a licensed provider and 100 deposited units. It concludes that technical feasibility is never sufficient for legal entitlement, and that outcomes should be judged by recovery actually delivered.

KEYWORDS

lawful chain ♦ proportionality ♦ interim measures ♦ freezing order ♦ tracing ♦ delivery order ♦ execution

KEY DOCTRINES AND PRINCIPLES

- ♦ Each coercive step needs its own legal basis; one power does not imply another
- ♦ Proportionality compares an intervention with narrower effective steps, including harm to undisputed holders
- ♦ Preventive supervision, suspension and penalty solve different problems and are not interchangeable
- ♦ Finality of a network is not a defence to claims against persons who caused loss
- ♦ Technical feasibility is necessary for an order but never sufficient to establish entitlement

LEADING AUTHORITIES

- ♦ Regulation (EU) 2023/1114 (MiCA)
- ♦ UNIDROIT, Principles on Digital Assets and Private Law (2023)
- ♦ UNCITRAL Model Law on Cross-Border Insolvency (1997)
- ♦ Federal Rules of Civil Procedure (United States), r 65
- ♦ Payment Services Act 2019 (Singapore)
- ♦ Financial Services and Markets Act 2000 (UK)

STILL OPEN

The chapter states that its Meridian case is assumed for analysis, and that the outcome measures it proposes are observations to be verified, not a composite score deciding future cases.

19 Enforcement, Courts, Review and Remedies

THE ARCHITECTURE OF THE CHAPTER

19.A	Public powers and procedural limits <i>Inspection, information demands and intervention · Notice, hearing, reasons and proportionality</i>
19.B	Administrative sanctions and review <i>Licence conditions, suspension and penalties · Appeal, judicial review and interim protection</i>
19.C	Civil claims and collective routes <i>Contract, tort, fiduciary and proprietary claims · Representative actions and alternative dispute resolution</i>
19.D	Criminal investigation and prosecution <i>Offences, intent, jurisdiction and proof · Search, seizure, confiscation and defence</i>
19.E	Urgent and proprietary remedies <i>Freezing, disclosure, injunctions and tracing · Delivery, recovery and third-party interests</i>
19.F	Remedies under technical constraints <i>Irreversible transfers, lost keys and governance powers · Compensation, substitutes and access restoration</i>
19.G	Effectiveness, rights and feedback <i>Outcome measures and distribution · Published reasons and institutional learning</i>

V



Programmable, Decentralised and AI-Mediated Finance

20	Smart Legal Contracts and Programmable Performance
21	Decentralised Finance: Control, Intermediation and Market Risk
22	DAOs: Organisation, Governance and Liability
23	AI Agents and Algorithmic Finance

20

Smart Legal Contracts and Programmable Performance

When a contract is partly performed by software, how are formation, meaning, attribution and remedy kept apart so that an executed transfer is not mistaken for a legal outcome?

ABSTRACT

Software can release payment before anyone has established what the parties agreed or who authorised the release. The chapter analyses a constructed cross-border escrow in three layers: technical execution, the human and organisational acts that gave the program a role, and legal effect. It examines interfaces and versions, keys and authority, precedence clauses, oracles, timing, coding errors and mistake, mandatory rules, and pause or reversal powers. It concludes that automation gives reliable performance only within a bounded task, and that an identifiable promise and a contestable, executable correction must remain.

KEYWORDS

smart legal contract ♦ oracle ♦ attribution ♦ precedence clause ♦ mistake ♦ dynamic information ♦ pause mechanism

KEY DOCTRINES AND PRINCIPLES

- ♦ A ledger event proves execution, not consent, authority or legal entitlement
- ♦ Attribution is kept separate from validity and liability
- ♦ Code is unambiguous about what it does, but not self-interpreting as the parties' meaning
- ♦ An oracle reports according to a method; it does not turn a fact into legal truth
- ♦ Technical capacity to reverse or pause does not create the contractual entitlement to do so

LEADING AUTHORITIES

- ♦ *Quoine Pte Ltd v B2C2 Ltd* [2020] SGCA(I) 2
- ♦ UNCITRAL Model Law on Automated Contracting (2024)
- ♦ UNCITRAL Model Law on Electronic Commerce (1996)
- ♦ UN Convention on the Use of Electronic Communications in International Contracts (2005)
- ♦ UNIDROIT, Principles on Digital Assets and Private Law (2023)
- ♦ UK Law Commission, Smart Legal Contracts: Advice to Government (Law Com No 401, 2021)

STILL OPEN

The chapter says its escrow is constructed and that Quoine is Singapore authority, comparative elsewhere, so the international models and cases give no universal rule of enforcement.

20 Smart Legal Contracts and Programmable Performance

THE ARCHITECTURE OF THE CHAPTER

20.A The three layers of the transaction

Technical execution · Communication, authorisation and legal effect

20.B Formation, capacity and consent

Interfaces, terms and deployment · Keys, authority and participation

20.C Text, code and interpretation

Precedence clauses and incorporated programs · Versions, dependencies and dynamic inputs

20.D Oracles, contingencies and performance

External facts and discretionary inputs · Time, conditions and partial performance

20.E Errors, breaches and unauthorised outcomes

Coding defects, exploit and mistake · Illegality, frustration and mandatory rules

20.F Remedies, correction and governance

Damages, restitution and injunctions · Upgrade, pause and reversal mechanisms

20.G Drafting, assurance and residual risk

Testing, audits and change control · Hybrid contract documentation

21

Decentralised Finance: Control, Intermediation and Market Risk

Who performed the financial function and controlled its decisive dependencies when a decentralised-finance loss arose, and what duty and remedy, if any, follow from that control?

ABSTRACT

Decentralised finance removes the dealer at the moment of execution without showing who designed the market, controls its dependencies or bears the loss when an input fails. The chapter treats "decentralised" as a proposition to be tested layer by layer, applying the five-object map to exchange, lending, governance, infrastructure and access. It works through an arithmetic liquidation stress exercise and a constructed control dossier, then separates factual control from duty, breach and remedy. It concludes that evidence of control starts the legal inquiry without finishing it, and that mixed findings serve better than one verdict.

KEYWORDS

decentralised finance ♦ control dossier ♦ liquidation ♦ oracle ♦ constant-product pool ♦ responsible persons ♦ bad debt

KEY DOCTRINES AND PRINCIPLES

- ♦ "Decentralised" is tested at each layer, not accepted as a legal classification
- ♦ Factual control does not entail a duty, breach, causation or an available remedy
- ♦ Executable price, realisable price and the price used to value a claim can diverge
- ♦ A liquidation spread is not, without more, damage, profit or unjust enrichment
- ♦ International policy instruments cannot establish an offence or duty without a domestic source

LEADING AUTHORITIES

- ♦ FSB, The Financial Stability Risks of Decentralised Finance (16 February 2023)
- ♦ IOSCO, Final Report with Policy Recommendations for Decentralized Finance (DeFi) (December 2023)
- ♦ IOSCO, Policy Recommendations for Crypto and Digital Asset Markets (November 2023)
- ♦ FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs (2021)
- ♦ FATF, Targeted Report on Regulatory Challenges from Decentralised Finance (21 July 2026)
- ♦ FSB, High-level Recommendations for Crypto-asset Activities and Markets (17 July 2023)

STILL OPEN

The chapter states that its Meridian dossier and stress simulation are constructed examples, and that where law cannot reach a risk without overbroad attribution the response is lawful reform, not retrospective liability.

2I Decentralised Finance: Control, Intermediation and Market Risk

THE ARCHITECTURE OF THE CHAPTER

21.A	DeFi functions and architecture <i>Exchange, lending, staking and synthetic exposure · Protocols, interfaces and intermediaries</i>
21.B	Liquidity pools and price formation <i>Automated market makers and arbitrage · Fees, liquidity provision and impermanent loss</i>
21.C	Collateral, lending and liquidation <i>Overcollateralisation, leverage and reuse · Oracle prices, liquidators and cascades</i>
21.D	Governance and concentrated powers <i>Admin keys, upgrades, treasuries and voting · Delegation, insiders and emergency controls</i>
21.E	Infrastructure, dependencies and extraction <i>Oracles, bridges, sequencers and MEV · Front ends, hosting and access</i>
21.F	Perimeters, responsible persons and duties <i>Financial integrity, conduct and prudential functions · IOSCO recommendations and domestic law</i>
21.G	Failure, intervention and adaptation <i>Exploits, bad debt and market disruption · Recovery, user rights and lawful correction</i>

22

DAOs: Organisation, Governance and Liability

When a DAO's vote is visible but its legal author is not, how do form, treasury authority and liability decide who can be called to account?

ABSTRACT

A decentralised autonomous organisation can make a decision visible without making its legal author evident. The chapter examines purpose and membership, on-chain and off-chain constitutions, unincorporated and incorporated forms, governance procedure and capture, authority in external transactions, duties and member exposure, and remedies on dispute and insolvency. It tests these through a constructed treasury grant approved by a concentrated delegate, before and after incorporation. It concludes that a wrapper changes the reachable estate and route to decision without making a captured vote independent or a deficient treasury adequate.

KEYWORDS

DAO ♦ legal wrapper ♦ treasury ♦ delegation ♦ capture ♦ ratification ♦ fiduciary duty

KEY DOCTRINES AND PRINCIPLES

- ♦ Neither decentralisation nor a wrapper by itself decides participants' legal responsibility
- ♦ Asset control, contractual authority and organisational office are allocated separately
- ♦ Duties attach to decisions and relationships, not to possession of a token
- ♦ An accurate tally shows a programmed threshold was passed, not a valid disposition
- ♦ Classification, service, substantive violation and execution against assets are separate inquiries

LEADING AUTHORITIES

- ♦ *Commodity Futures Trading Commission v Ooki DAO*, No 3:22-cv-05416-WHO (ND Cal, 8 June 2023)
- ♦ Law Commission of England and Wales, *Decentralised Autonomous Organisations: Scoping Paper* (July 2024)
- ♦ Partnership Act 1890
- ♦ Companies Act 2006
- ♦ Wyoming Statutes, Title 17, ch 31 (DAO supplement)
- ♦ Cayman Islands Foundation Companies Act (2025 Revision)

STILL OPEN

The chapter acknowledges that entity-centred reform has a limit: naming a defendant may leave the decisive power and fund elsewhere, and its Meridian Commons case rests on stated assumptions.

22 DAOs: Organisation, Governance and Liability

THE ARCHITECTURE OF THE CHAPTER

22.A The organisation behind the label

Purpose, membership and coordination · On-chain and off-chain arrangements

22.B Personality and legal forms

Unincorporated associations, partnerships and companies · Foundations and specialised wrappers

22.C Governance rights and procedures

Proposals, voting, delegation and quorum · Participation, concentration and capture

22.D Authority, agency and external transactions

Representatives, signatures and treasury control · Counterparty reliance and ratification

22.E Duties, responsibility and member exposure

Fiduciary, contractual and statutory duties · Passive holders, operators and contributors

22.F Disputes, remedies and insolvency

Member challenges, minority protection and exit · Asset recovery and creditor claims

22.G Comparative organisational reform

Law Commission work and adopted regimes · Adaptation without fictitious autonomy

23

AI Agents and Algorithmic Finance

When an AI agent can use tools to advise, trade and transfer at machine speed, how are capability, authority, oversight, fault, evidence and remedy tied to human decisions?

ABSTRACT

An AI system that can invoke an order-entry or signing interface acts faster than a supervisor can read the record, yet it confers no legal personality or agency. The chapter treats an agent as a configured system and separates six inquiries: capability, authority, oversight, fault, evidence and remedy. It covers mandates and credentials, formation and reliance, model risk, records and market interaction, and it works through a constructed incident in which an altered bulletin redirects a fund's agent. It concludes that a narrow mandate, pre-trade barriers and available competent people are conditions of lawful automation.

KEYWORDS

AI agent ♦ mandate ♦ tool permissions ♦ human oversight ♦ prompt injection ♦ kill switch ♦ apparent authority

KEY DOCTRINES AND PRINCIPLES

- ♦ Authentication shows which credential was accepted; authority depends on the mandate and its grantor
- ♦ "Human in the loop" describes workflow placement, not effective control
- ♦ Meaningful oversight requires understanding, detection, timely intervention and explanation
- ♦ A machine-generated rationale is not necessarily the cause of the order it explains
- ♦ Control points and received benefits are evidence for responsibility, not proof of it

LEADING AUTHORITIES

- ♦ MiFID II (Directive 2014/65/EU)
- ♦ Securities Exchange Act Rule 15c3-5, 17 CFR 240.15c3-5
- ♦ UNCITRAL Model Law on Automated Contracting (2024)
- ♦ Regulation (EU) 2024/1689 (Artificial Intelligence Act)
- ♦ FINRA Regulatory Notice 24-09
- ♦ NIST, AI Risk Management Framework (AI RMF 1.0)

STILL OPEN

The chapter asks whether people can govern decisions made at a speed they cannot match, and answers that they can only if the mandate is narrow and the barrier acts before exposure; otherwise the use case should be declined.

23 AI Agents and Algorithmic Finance

THE ARCHITECTURE OF THE CHAPTER

23.A	Capabilities and financial roles <i>Advice, trading, compliance and execution · Fixed automation and adaptive models</i>
23.B	Authority, delegation and limits <i>Mandates, credentials and tool permissions · Capacity, attribution and apparent authority</i>
23.C	Formation, reliance and unexpected outputs <i>Agent communications and commitments · Error, misrepresentation and third-party reliance</i>
23.D	Governance and human responsibility <i>Oversight, competence, escalation and intervention · Reasons, contestability and accountability</i>
23.E	Model risk and market interaction <i>Hallucination, drift, adversarial inputs and correlated behaviour · Feedback loops and manipulation</i>
23.F	Records, assurance and liability <i>Models, prompts, logs and version histories · Causation, insurance and allocation of loss</i>
23.G	Regulatory adaptation and lawful experimentation <i>Sandboxes, procurement and standards · Review triggers and evolving duties</i>

VI

Comparative Legal Orders

-
- | | |
|----|--|
| 24 | The United States: Federalism, Perimeters and Institutional Conflict |
|----|--|
-
- | | |
|----|---|
| 25 | The European Union: A Supranational Digital Financial Order |
|----|---|
-
- | | |
|----|--|
| 26 | The United Kingdom: Property, Permissions and Legal Transition |
|----|--|
-
- | | |
|----|---|
| 27 | Asia-Pacific: Diverse Legal Orders and Digital Financial Strategies |
|----|---|
-
- | | |
|----|---|
| 28 | The Gulf and Middle East: Financial Centres, Islamic Finance and Digital Assets |
|----|---|
-
- | | |
|----|--|
| 29 | Africa and Latin America: Monetary Choice, Market Development and Legal Protection |
|----|--|

24

The United States: Federalism, Perimeters and Institutional Conflict

Where does each federal, state and judicial source of authority attach to a US digital-asset arrangement, and who carries the loss when the institutions meet at a boundary?

ABSTRACT

Digital-asset governance in the United States is a problem of divided authority: federal securities, commodities, banking, payments, sanctions and tax law meet state licensing, commercial, trust and insolvency law. The chapter fixes a legal-status cut-off of 28 September 2026 and builds a dated authority map. It then examines classification, state commercial law and Article 12, stablecoin and custody rules, integrity obligations and litigation postures such as Ripple, Coinbase and Celsius. It concludes with four common-case tests, and argues that the lawful chain cannot be presumed from a bill or the abundance of rules.

KEYWORDS

federalism ♦ authority map ♦ pre-emption ♦ investment contract ♦ controllable electronic records ♦ payment stablecoin ♦ custody

KEY DOCTRINES AND PRINCIPLES

- ♦ Classification concerns arrangements and transactions, not only objects
- ♦ A statute, an agency interpretation and an unadvanced bill have different makers and legal effect
- ♦ Federal permission to provide a service does not establish segregation or priority of customer assets
- ♦ Control is a technical criterion; it cannot create an external entitlement
- ♦ Public sanction of a custodian does not automatically restore customer property

LEADING AUTHORITIES

- ♦ SEC v W J Howey Co
- ♦ Loper Bright Enterprises v Raimondo, 603 US 369 (2024)
- ♦ GENIUS Act, Pub L No 119-27 (18 July 2025)
- ♦ SEC, Securities Act Release No 33-11412 (17 March 2026)
- ♦ UCC Article 12 (2022 amendments) and Delaware Code tit 6
- ♦ In re Celsius Network LLC, No 22-10964 (Bankr SDNY, 4 January 2023)

STILL OPEN

The chapter states that its authority map is deliberately incomplete as a claims register, and that a Canadian comparison would need matched statutes, provincial rules and judgments assembled for the same four cases.

24 The United States: Federalism, Perimeters and Institutional Conflict

THE ARCHITECTURE OF THE CHAPTER

24.A	Constitutional and institutional allocation <i>Federal agencies and state powers · Pre-emption, coordination and judicial control</i>
24.B	Asset and market classification <i>Securities, commodities, payments and banking · Statutory tests and contested interpretations</i>
24.C	Property, security and commercial law <i>State law and UCC amendments · Control, transfer and creditor priority</i>
24.D	Stablecoins, custody and prudential rules <i>Issuer permissions and customer protection · Bank and non-bank structures</i>
24.E	Integrity, fiscal and conduct obligations <i>AML, sanctions and tax · Promotions, fraud and market abuse</i>
24.F	Litigation, enforcement and remedies <i>Procedural posture, appeals and settlements · Insolvency recovery and private actions</i>
24.G	Institutional and capital assessment <i>Capability, information and coordination · Distribution, innovation and risk migration</i>

25

The European Union: A Supranational Digital Financial Order

What does the EU's common crypto-asset text achieve when it meets national property, insolvency and enforcement institutions in custody failure, redemption and cross-border supervision?

ABSTRACT

A Union-wide permission can coexist with a contested title to customer assets, and a directly stated redemption right can fail for want of records, reserves or an executable proceeding. The chapter tests MiCA and adjacent instruments against four matched situations: custody failure, a security-like token, a redemption demand and a cross-border service. It separates legal force from institutional completion and common conduct duties from national private-law recovery. It concludes that harmonised text, authorisation, supervisory practice and private recovery are distinct propositions, each needing its own evidence.

KEYWORDS

source hierarchy ♦ MiCA perimeter ♦ legal segregation ♦ redemption right ♦ passporting ♦ transitional period ♦ institutional executability

KEY DOCTRINES AND PRINCIPLES

- ♦ Direct applicability is not institutional self-execution
- ♦ MiCA excludes crypto-assets that qualify as financial instruments; classification follows rights, not labels
- ♦ A Union register evidences status; it does not guarantee solvency or customer ownership
- ♦ Common conduct duties do not produce uniform private-law recovery
- ♦ Textual alignment, authorisation, supervisory practice and recovery are separate claims

LEADING AUTHORITIES

- ♦ Regulation (EU) 2023/1114 (MiCA)
- ♦ Regulation (EU) 2022/858 (DLT Pilot Regulation)
- ♦ Regulation (EU) 2022/2554 (DORA)
- ♦ Regulation (EU) 2023/1113 (transfer information)
- ♦ Council Directive (EU) 2023/2226 (DAC8)
- ♦ Treaty on the Functioning of the European Union

STILL OPEN

Whether consistent supervisory practice and consistent private recovery follow from harmonised text remains unshown without evidence of resources, decisions and actual proceedings.

25 The European Union: A Supranational Digital Financial Order

THE ARCHITECTURE OF THE CHAPTER

25.A	Supranational competence and source hierarchy <i>Regulations, directives and technical standards · EU bodies, national authorities and courts</i>
25.B	MiCA scope and boundaries <i>Asset categories, issuers and services · Excluded instruments and adjacent regimes</i>
25.C	Financial instruments and market infrastructure <i>Securities law and DLT arrangements · Settlement records and investor rights</i>
25.D	Stablecoins, safeguards and supervision <i>Reserve, redemption and governance · Significance, prudential duties and distribution</i>
25.E	Operational, data and integrity layers <i>DORA, GDPR and transfer information · Outsourcing, identity and cross-border duties</i>
25.F	Fiscal, private law and national variation <i>DAC8, domestic taxation and reporting · Property, security and insolvency</i>
25.G	Implementation, enforcement and assessment <i>Commencement, transition and guidance · Capability, review and distributional outcomes</i>

26

The United Kingdom: Property, Permissions and Legal Transition

How do enacted property law, existing registration and promotion rules, and a not-yet-commenced permission regime combine to decide who bears loss when a UK crypto platform fails?

ABSTRACT

Courts recognised proprietary rights in cryptoassets before Parliament acted, while the wider regulatory regime has been enacted but awaits principal commencement. The chapter follows one constructed case, an exporter paid in a sterling-referenced token, through property, priority, permission, evidence and remedy. It separates what the Property (Digital Assets etc) Act 2025 does from what it leaves open, and dates each regulatory source by legal status. It concludes that the UK answers some questions of legal certainty and leaves others to implementation and adjudication.

KEYWORDS

personal property ♦ customer entitlement ♦ segregation ♦ Part 4A permission ♦ financial promotions ♦ transition and commencement ♦ systemic stablecoin

KEY DOCTRINES AND PRINCIPLES

- ♦ Section 1 removes a two-category barrier; it is not a digital-property code
- ♦ Registration for one purpose is not authorisation for every activity
- ♦ A rule not yet in force cannot ground a present regulatory breach
- ♦ Recognition of property rights does not cure an evidential break in tracing
- ♦ A blockchain entry is evidence of protocol state, not of legal entitlement

LEADING AUTHORITIES

- ♦ Property (Digital Assets etc) Act 2025
- ♦ Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026, SI 2026/102
- ♦ AA v Persons Unknown [2019] EWHC 3556 (Comm)
- ♦ D'Aloia v Persons Unknown Category A [2024] EWHC 2342 (Ch)
- ♦ Wilden v Person Unknown (High Court, 5 June 2026)
- ♦ Money Laundering Regulations 2017, SI 2017/692

STILL OPEN

Whether existing platforms can reorganise custody and records in time for authorisation, and whether the FCA can assess the volume of applications, is left to implementation.

26 The United Kingdom: Property, Permissions and Legal Transition

THE ARCHITECTURE OF THE CHAPTER

26.A	Legal sources and territorial distinctions <i>Legislation, common law and regulatory rules · England and Wales Scotland and Northern Ireland</i>
26.B	Property recognition and reform <i>Property Act 2025 · Law Commission reports and judicial developments</i>
26.C	Security, custody and insolvency <i>Customer entitlement and creditor priority · Segregation, records and recovery</i>
26.D	Financial permissions and transition <i>Regulated activities, promotions and authorisation · Commencement, savings and implementation stages</i>
26.E	Stablecoins, payments and prudential design <i>Issuer, payment and bank functions · Reserve, redemption and systemic oversight</i>
26.F	Integrity, fiscal and evidence <i>AML, sanctions, reporting and tax · Electronic records and judicial proof</i>
26.G	Courts, coordination and comparative assessment <i>Case law review and institutional capacity · International reach and legal certainty</i>

27

Asia-Pacific: Diverse Legal Orders and Digital Financial Strategies

When the same platform failure is put to six Asia-Pacific legal orders, which protections address custody, redemption, collateral and enforcement, and where does each chain break?

ABSTRACT

The same token can be a payment instrument in one system, an issuer obligation in another and an impermissible substitute for public money in a third. The chapter compares Singapore, Hong Kong, Japan, Australia, India and mainland China through one constructed case: an exporter paid through a dollar-referenced token, a platform that stops withdrawals and a lender claiming collateral. It labels each source as operative law, guidance, proposal or pilot at 28 September 2026. It finds no regional ranking, only differing links between supervision, entitlement and remedy.

KEYWORDS

dollar-referenced token ♦ safeguarding ♦ electronic payment instrument ♦ source-status matrix ♦ asset retention ♦ public digital money ♦ Intelligent-Order Test

KEY DOCTRINES AND PRINCIPLES

- ♦ Permission is not a single switch: exchange, safeguarding and redemption need separate bases
- ♦ A tax or integrity registration confers no approval to market the conduct
- ♦ A segregation duty has value before litigation but does not by itself deliver recovery
- ♦ A pilot is not evidence of a liquid market or a surviving claim
- ♦ Standards and recommendations are not self-executing customer remedies

LEADING AUTHORITIES

- ♦ Payment Services Act 2019 (Singapore)
- ♦ Stablecoins Ordinance (Hong Kong)
- ♦ Payment Services Act (Japan), 2025 amendment
- ♦ Corporations Amendment (Digital Assets Framework) Act 2026 (Cth)
- ♦ Income-tax Act 1961 (India)
- ♦ UNIDROIT Principles on Digital Assets and Private Law (2023)

STILL OPEN

Whether the matched-case method yields more than a list of differences is treated as the strongest objection, answered by holding the loss mechanism constant.

27 Asia-Pacific: Diverse Legal Orders and Digital Financial Strategies

THE ARCHITECTURE OF THE CHAPTER

27.A	Comparative selection and legal diversity <i>Common, civil and mixed traditions · Permissions, restrictions and institutional choices</i>
27.B	Singapore and Hong Kong <i>Service permissions and monetary authorities · Tokenised markets, stablecoins and custody</i>
27.C	Japan and Australia <i>Private-law protections and market supervision · Banking, payments and licensing boundaries</i>
27.D	India and mainland China <i>Fiscal and integrity rules · Restrictions, public payments and monetary strategy</i>
27.E	Shared private-law and failure problems <i>Title, custody, collateral and insolvency · Cross-border customers and enforcement</i>
27.F	Regional capital and operational dependencies <i>Financial-centre strategies, payments and access · Data infrastructure and foreign exposure</i>
27.G	Comparative findings and limits <i>Institutional executability and remedies · Policy transfer and contextual constraints</i>

28

The Gulf and Middle East: Financial Centres, Islamic Finance and Digital Assets

How do layered Gulf jurisdictions and Islamic-finance governance shape the rights and losses of an investor in a tokenised sukuk paid for with a payment token?

ABSTRACT

A digital-asset firm can be incorporated in one financial centre, custody tokens in another and settle in a token issued by a third person, so that no single location answers which law constitutes the investor's claim. The chapter maps the UAE, Bahrain, Saudi Arabia and Qatar, then distinguishes scholarly opinion, standard, regulatory recognition and contract. It follows a hypothetical Crescent Equipment Sukuk through issuer, custodian, payment-token issuer and equipment register. It concludes that approval of a structure does not establish title, reserves or recourse when a participant fails.

KEYWORDS

layered jurisdiction ♦ financial zones ♦ shari'ah governance ♦ sukuk ♦ payment token ♦ māl ♦ gharar

KEY DOCTRINES AND PRINCIPLES

- ♦ A licence approves identified activities; it does not decide property in the underlying asset
- ♦ Shari'ah assessment, standard, regulatory recognition and contract are four distinct sources
- ♦ Guidance explains supervisory expectations without creating the duty alleged
- ♦ Sukuk metadata cannot perform the conveyance the structure presupposes
- ♦ Technical pause or upgrade power is not a legal entitlement to defer redemption

LEADING AUTHORITIES

- ♦ UAE Central Bank Payment Token Services Regulation
- ♦ VARA Regulations (Dubai)
- ♦ Financial Action Task Force Recommendation 15
- ♦ AAOIFI Shari'ah Standard 17 (investment sukuk)
- ♦ IFSB-10 and IFSB-31
- ♦ UNIDROIT Principles on Digital Assets and Private Law

STILL OPEN

The chapter does not decide scholarly disputes on currency exchange, delay or permissible uncertainty, and asks only that they be attached to the actual transaction.

28 The Gulf and Middle East: Financial Centres, Islamic Finance and Digital Assets

THE ARCHITECTURE OF THE CHAPTER

28.A	Layered jurisdiction and regulatory allocation <i>Domestic authorities and financial zones · Monetary, payment and market mandates</i>
28.B	UAE financial and digital-asset regimes <i>Federal, emirate and free-zone structures · Permissions, custody and supervision</i>
28.C	Other Gulf and Middle Eastern comparisons <i>Bahrain, Saudi Arabia and selected jurisdictions · Markets, payments and institutional strategies</i>
28.D	Islamic-finance methods and sources <i>Standards, supervisory recognition and scholarly disagreement · Maal, rights, exchange and uncertainty</i>
28.E	Tokenised products and substantive compliance <i>Sukuk, commodities and asset-linked structures · Ownership, risk sharing and enforceable recourse</i>
28.F	Capital hubs, integrity and cross-border exposure <i>Reserve, custody, tax and information duties · International customers and enforcement</i>
28.G	Comparative outcomes and adaptive capacity <i>Institutions, infrastructure and human oversight · Transferability and contextual limits</i>

29

Africa and Latin America: Monetary Choice, Market Development and Legal Protection

Can claims that digital assets make remittances cheap, inclusive and monetarily resilient be sustained across six African and Latin American legal orders once payment rails and private remedies are examined?

ABSTRACT

A household receiving a cross-border payment must be able to convert, store value and, if an intermediary fails, recover it. The chapter examines South Africa, Nigeria, Kenya, Brazil, Mexico and El Salvador, each dated at 28 September 2026 and each tested against the existing payment rail and monetary baseline. It distinguishes operative rules from drafts, incubation status and announcements, and treats licence counts and transaction volumes as measures of supervision or use only. It concludes that evidence must follow the proposition claimed, from net amount received to redress.

KEYWORDS

monetary baseline ♦ conduct licensing ♦ mobile money ♦ instant payment rail ♦ legal tender ♦ remittance cost ♦ analytical parity

KEY DOCTRINES AND PRINCIPLES

- ♦ Compare an arrangement against the rail users actually use, not an imagined cash-only economy
- ♦ A licence count shows implementation of a programme, not safety or a direct proprietary claim
- ♦ Legal time is part of transaction risk: drafts and future commencements are not operative protection
- ♦ The evidential burden follows the proposition: price, inclusion, capital formation, resilience or fiscal prudence
- ♦ Regulatory authorisation cannot by itself settle priority after failure

LEADING AUTHORITIES

- ♦ Financial Advisory and Intermediary Services Act, crypto-asset declaration (South Africa, 2022)
- ♦ Kenya Virtual Asset Service Providers Act, No 20 of 2025
- ♦ Banco de México Circular 4/2019
- ♦ Resolutions BCB 519, 520 and 521 (Brazil)
- ♦ El Salvador Bitcoin Law (2021) and 2025 amendment
- ♦ UNIDROIT Principles on Digital Assets and Private Law

STILL OPEN

Where an operative regulation, legal entitlement or comparable outcome cannot be verified, the chapter leaves the answer open rather than filling it with a policy claim.

29 Africa and Latin America: Monetary Choice, Market Development and Legal Protection

THE ARCHITECTURE OF THE CHAPTER

29.A	Selection, diversity and analytical parity <i>Monetary institutions and legal traditions · Case selection and evidential limits</i>
29.B	Southern and West African approaches <i>South Africa and Nigeria · Permissions, restrictions and institutional change</i>
29.C	East African payments and market development <i>Kenya and selected comparisons · Mobile money, digital assets and user protection</i>
29.D	Latin American financial regulation <i>Brazil and Mexico · Market permissions, fiscal duties and institutional allocation</i>
29.E	Monetary experiments and legal change <i>El Salvador and other selected cases · Tender policy, public exposure and transition</i>
29.F	Private rights, integrity and remedies <i>Custody, collateral and cross-border claims · Information powers, access and consumer redress</i>
29.G	Development, distribution and comparison <i>Remittances, inclusion, energy and infrastructure · Evidence, counterfactuals and adaptive legality</i>

CODE, LAW AND CAPITAL

PART SEVEN

VII



Global Coordination, Computational Regulation and Future Orders

30 Public International Law and the Digital-Asset Order

31 Global Standards and Transnational Coordination

32 Human-Governed Machine-Readable Regulation

33 Future Orders: Strategic, Anticipatory and Evolutionary Legal Intelligence

30

Public International Law and the Digital-Asset Order

Which public authority may act on a cross-border digital-asset measure, what has its state promised internationally, and where can the measure be contested?

ABSTRACT

A digital-asset network can span several states, yet technical reach does not enlarge a state's legal reach. The chapter separates prescription, adjudication and enforcement, then tests each measure against monetary, trade, investment, sanctions and state-responsibility rules. It applies them to a constructed freeze that involves a platform, issuer, exporter and financing bank across four states. Its conclusion is that every claim needs a source, a connection, evidence and a forum, and that remedy follows obligation and claimant rather than the visibility of a transaction on a ledger.

KEYWORDS

jurisdiction ♦ enforcement ♦ capital controls ♦ GATS ♦ investment protection ♦ state responsibility ♦ legal address

KEY DOCTRINES AND PRINCIPLES

- ♦ Prescription, adjudication and enforcement are separate powers and are analysed separately
- ♦ Technical capacity, such as holding an upgrade key, is not legal authority
- ♦ IMF Articles distinguish current payments from capital movements; a token label decides neither
- ♦ Digital form does not settle treaty classification; schedules and function do
- ♦ Token ownership alone does not establish a protected investment or a forum with consent

LEADING AUTHORITIES

- ♦ IMF Articles of Agreement
- ♦ General Agreement on Trade in Services (GATS)
- ♦ ICSID Convention
- ♦ ILC Articles on Responsibility of States for Internationally Wrongful Acts
- ♦ Budapest Convention on Cybercrime
- ♦ *Nicaragua v United States* [1986] ICJ Rep 14

STILL OPEN

The chapter does not treat its jurisdiction-and-obligation map as yielding an obligation in every row; it is a method for a defined measure and leaves conflicting sovereign policies unresolved where they genuinely disagree.

30 Public International Law and the Digital-Asset Order

THE ARCHITECTURE OF THE CHAPTER

-
- | | |
|------|---|
| 30.A | Jurisdiction in networked activity
<i>Territorial, nationality and effects connections · Prescription, adjudication and enforcement</i> |
|------|---|
-
- | | |
|------|--|
| 30.B | Sovereignty and monetary measures
<i>Payment restrictions, capital controls and public money · International obligations and domestic discretion</i> |
|------|--|
-
- | | |
|------|--|
| 30.C | Trade, services and digital commerce
<i>Market access, non-discrimination and exceptions · Digital services and treaty scope</i> |
|------|--|
-
- | | |
|------|---|
| 30.D | Investment protection and digital claims
<i>Protected investment, investor and territorial links · Regulation, expropriation and fair treatment</i> |
|------|---|
-
- | | |
|------|--|
| 30.E | Sanctions, cooperation and conflict
<i>Extraterritorial measures and competing duties · Countermeasures, assistance and legal limits</i> |
|------|--|
-
- | | |
|------|--|
| 30.F | State responsibility and public digital infrastructure
<i>Attribution, breach and causation · State entities, contractors and remedies</i> |
|------|--|
-
- | | |
|------|---|
| 30.G | Dispute resolution and institutional adaptation
<i>Treaty forums, domestic courts and coordination · Legitimacy, fragmentation and reform</i> |
|------|---|
-

31

Global Standards and Transnational Coordination

Does convergence of international standards make cross-border digital-asset arrangements more intelligible and answerable, or merely export formal duties to institutions unable to perform them?

ABSTRACT

International instruments on digital assets are numerous, but each has its own maker, mandate, addressee, legal form and route into domestic law, so their density is an unreliable measure of governance. The chapter classifies the FSB, IOSCO, FATF, Basel, OECD, UNIDROIT and UNCITRAL texts by legal force. It then follows them through supervisory cooperation, information gateways and a dated comparative implementation dashboard. It concludes that convergence has value only where capacity, safeguards, reciprocal information routes and remedies keep pace with the exported text.

KEYWORDS

legal force ♦ standard setters ♦ implementation ♦ information gateways ♦ perimeter divergence ♦ effectiveness ♦ policy space

KEY DOCTRINES AND PRINCIPLES

- ♦ An international recommendation does not become a command to a private person by being influential
- ♦ Same activity, same risk, same regulation is a starting discipline, not an instruction to erase differences
- ♦ A register or reporting rule proves a duty or permission, not the standard's purpose achieved
- ♦ Cooperation arrangements cannot enlarge a statute or erase a duty of secrecy
- ♦ Convergence is accurate only where each step in a transaction's legal chain is compatible

LEADING AUTHORITIES

- ♦ FSB high-level recommendations on crypto-asset activities and global stablecoins (17 July 2023)
- ♦ FATF Recommendation 15 and Interpretive Note
- ♦ Basel Framework, SCO60
- ♦ OECD Crypto-Asset Reporting Framework (CARF)
- ♦ UNIDROIT Principles on Digital Assets and Private Law (2023)
- ♦ UNCITRAL Model Law on Electronic Transferable Records (2017)

STILL OPEN

The chapter states that its standards map and dashboard are revisable instruments of judgment, that the dashboard's capacity column is not an audited conclusion that a regime works, and that its costs are analytic risks rather than measured totals.

31 Global Standards and Transnational Coordination

THE ARCHITECTURE OF THE CHAPTER

31.A	Institutions, mandates and legal force <i>Standard setters, model laws and private-law principles · Treaties, domestic incorporation and voluntary compliance</i>
31.B	Financial stability and market integrity <i>FSB and IOSCO frameworks · Risk equivalence and perimeter divergence</i>
31.C	Integrity, prudential and fiscal coordination <i>FATF, Basel and OECD · Overlapping actors, reporting and safeguards</i>
31.D	Private law and electronic transactions <i>UNIDROIT and UNCITRAL · Adoption, implementation and residual domestic rules</i>
31.E	Supervisory cooperation and information gateways <i>Colleges, memoranda, assistance and referrals · Confidentiality, accountability and review</i>
31.F	Implementation, monitoring and capacity <i>Peer reviews, mutual evaluations and technical assistance · Resources, transition and measurable effectiveness</i>
31.G	Legitimacy, participation and adaptive convergence <i>Representation, policy space and accountability · Feedback, revision and plural legal orders</i>

32

Human-Governed Machine-Readable Regulation

When may a computational representation of digital-asset regulation assist a legal decision without acquiring authority it does not possess?

ABSTRACT

A data system can reproduce regulatory language, calculate a threshold or flag a breach, yet none of this establishes that the instrument is valid, the facts proven or the institution empowered. The chapter separates five layers: authoritative instrument, interpretation, computational representation, administrative decision and remedy. It sets out a source-to-rule traceability schema, four typed uncertainty states, and controls for versioning, review and vendor dependence. A constructed dispute over a draft custody definition tests them, and the chapter concludes that correction must run backward to source and forward to remedy.

KEYWORDS

Rules as Code ♦ Law as Code ♦ traceability schema ♦ temporal validity ♦ UNKNOWN, GAP, DRAFT, CONFLICT ♦ human reasons ♦ vendor dependence

KEY DOCTRINES AND PRINCIPLES

- ♦ Law as Code concerns sources; Rules as Code concerns operable representation; neither enacts law
- ♦ Instrument, interpretation, representation, decision and remedy are separate layers
- ♦ A human approver needs authority, the record, time and power to depart from output
- ♦ Running the latest rule against stored records silently rewrites legal history
- ♦ An unresolved state cannot itself supply a finding of breach or suspend a decision indefinitely

LEADING AUTHORITIES

- ♦ OECD Crypto-Asset Reporting Framework XML schema
- ♦ LegalRuleML Core Specification 1.0 and W3C PROV-O
- ♦ Administrative Review Tribunal Act 2024 (Cth)
- ♦ Canada, Directive on Automated Decision-Making
- ♦ Regulation (EU) 2016/679 (GDPR)
- ♦ Regulation (EU) 2024/1689 (EU AI Act)

STILL OPEN

The chapter states that it cannot announce a universal ban or permission on automated decisions, and that its schema and disputed decision are analytical devices rather than claims that any jurisdiction has adopted them.

32 Human-Governed Machine-Readable Regulation

THE ARCHITECTURE OF THE CHAPTER

32.A	Representation and authority <i>Law as Code and Rules as Code · Sources, interpretation, models, decisions and remedies</i>
32.B	Source provenance and temporal validity <i>Instrument, issuer, hierarchy and commencement · Amendment, repeal, savings and versioning</i>
32.C	Translation, interpretation and uncertainty <i>Definitions, thresholds, exceptions and discretion · UNKNOWN, GAP, DRAFT and CONFLICT states</i>
32.D	Validation, assurance and institutional ownership <i>Test cases, audits and change control · Competent review and model responsibility</i>
32.E	Administrative decisions and human reasons <i>Assisted workflows, delegated powers and approval · Contestability, explanation and access to records</i>
32.F	Rights, security and operational constraints <i>Data minimisation, discrimination and accessibility · Resilience, procurement and vendor dependence</i>
32.G	Revision, correction and remedy <i>Challenge, suspension and rollback · Measured learning and lawful change</i>

33

Future Orders: Strategic, Anticipatory and Evolutionary Legal Intelligence

How can legal institutions prepare for technological change while keeping knowledge, authority and responsibility distinct, and revise the rules lawfully as outcomes are observed?

ABSTRACT

Waiting for every technical possibility to become an injury leaves an order unprepared, while treating an imagined future as proof of need invites exceptional power. The chapter develops Strategic, Anticipatory and Evolutionary Legal Intelligence and applies the Intelligent-Order Test. It builds four conditional trajectories, a table of leading indicators with competing explanations, and a lawful reassessment loop of observe, classify, test, justify, act and review. It concludes that foresight prepares lawful options but confers no authority, and that adaptation must preserve the lawful chain.

KEYWORDS

Strategic Legal Intelligence ♦ Anticipatory Legal Intelligence ♦ Evolutionary Legal Intelligence ♦ Intelligent-Order Test ♦ scenarios ♦ leading indicators ♦ lawful reassessment

KEY DOCTRINES AND PRINCIPLES

- ♦ Demonstrated capability, emerging signal and speculative possibility are distinct evidential states
- ♦ A scenario is a conditional account with counterforces and a disconfirming indicator, not a forecast
- ♦ An agency cannot cure a missing power by calling its intervention an experiment
- ♦ A threshold prompts inquiry or triggers an already valid rule; it is not a self-executing command
- ♦ Adaptive legality requires the other five conditions to survive change

LEADING AUTHORITIES

- ♦ FSB Thematic Review (16 October 2025)
- ♦ FSB high-level recommendations on crypto-asset activities and global stablecoins (17 July 2023)
- ♦ UNIDROIT Principles on Digital Assets and Private Law (2023)
- ♦ UNCITRAL Model Law on Automated Contracting (2024)
- ♦ *In re Celsius Network LLC*, Case No 22-10964 (Bankr SDNY, 4 January 2023)
- ♦ IMF Country Report 25/58 (El Salvador)

STILL OPEN

The chapter leaves open how conflict rules should locate a digital claim whose record, operator and holder sit in different places, and which forms of tokenised money can preserve public monetary purposes.

33 Future Orders: Strategic, Anticipatory and Evolutionary Legal Intelligence

THE ARCHITECTURE OF THE CHAPTER

33.A	Strategic legal intelligence <i>System dependencies, institutional direction and capacity · Distribution, public value and constitutional limits</i>
33.B	Anticipatory legal intelligence <i>Horizon scanning, uncertainty and signals · Scenario construction and stress testing</i>
33.C	Evolutionary legal intelligence <i>Feedback, outcomes and institutional memory · Revision, experiments and safeguards</i>
33.D	Four alternative global trajectories <i>Interoperable regulated tokenisation and fragmented orders · Private monetary concentration and AI-mediated finance</i>
33.E	Indicators, thresholds and competing explanations <i>Adoption, exposure, incidents and recovery · False signals, data gaps and causal limits</i>
33.F	The lawful reassessment loop <i>Observe, classify, test, justify, act and review · Valid instruments, competent bodies and remedies</i>
33.G	The global order as a continuing legal project <i>Comparative findings and unresolved questions · Research agenda and institutional responsibility</i>

STATUS OF THIS RELEASE

This release comprises the planned contents of the Global Edition. Chapter titles and section headings follow the Author’s manuscript as locked on 30 September 2026. The text of the chapters is not released here.

This document describes the planned contents of a work in progress. It is not legal advice, does not state the law of any jurisdiction, and must not be relied upon for any decision. Titles, section headings and order may change before publication.

FORTHCOMING AND BETA PROJECTS

BETA	budget.codes Pakistan’s tax and budget law as executable code. Free public beta.
BETA	JUS.smart A public beta research environment for tracing institutional acts through authority, evidence, reasons and remedy (jus-smart.digital).
FORTHCOMING	Sovereign OS A prototype of the Sovereign Governance Intelligence Engine.
FORTHCOMING	JUSNREM.LEGAL A free legal resource and Pakistani Legal Intelligence Engine, with machine-readable laws and Rules-as-Code (RaC) legal maps.
FORTHCOMING	JUSNREM Codex A register of the treatises, doctrines and applied frameworks of the work.

These projects are in development. Their scope, names and availability may change.

JUS AND REM LIMITED

London · ksc-jusnrem.io · jus-atomica.digital

© Khurram Chughtai 2026. All rights reserved.