



Ticino
Arbitration
Centre



DIGITAL ASSETS & BLOCKCHAIN DISPUTES

SUPPLEMENTARY RULES

Effective: 1 August 2026

PREAMBLE.....	2
Article 1 – Scope of Application.....	2
Article 2 – Eligible Parties and Non-Consumer Use.....	3
Article 3 – Regulated Digital Assets and Tokenised Rights.....	3
Article 4 – Initial Technical Disclosure and Snapshot.....	4
Article 5 – Core Procedural Approach.....	6
Article 6 – Blockchain Evidence and System Records.....	6
Article 7 – Digital Asset Events, Automated Outcomes and Derived Entitlements.....	7
Article 8 – Attribution of Addresses, Transactions and Signatures.....	8
Article 9 – Control, Access and Authority.....	9
Article 10 – Blockchain Analytics and Risk-Assessment Evidence.....	10
Article 11 – Preservation Measures.....	11
Article 12 – Experts and Forensic Analysis.....	12
Article 13 – Platform Groups, Third-Party Platforms and Non-Parties.....	13
Article 14 – Illegality, Sanctions and Tainted Asset Allegations.....	14
Article 15 – Remedies.....	15
Article 16 – Safeguards.....	17
Article 17 – Entry into Force and Relationship with the TAC Arbitration Rules.....	18

PREAMBLE

These Supplementary Rules set out specific procedural and evidentiary adaptations applicable, where expressly agreed by the parties, to disputes involving digital assets, blockchain-based or distributed ledger transactions, cryptographic control mechanisms, tokenised rights, and related contractual relationships.

These Rules recognise that the technical recording, transfer, and control of digital assets may not correspond to the legal rights, obligations, and entitlements of the parties, and that arbitral proceedings must be capable of examining both technical and economic reality where necessary. The Ticino Arbitration Centre administers arbitrations concerning the rights and obligations of identifiable parties in connection with digital assets and related transactions. It does not administer, govern, or modify blockchain networks, distributed ledger systems, automated protocols, or technical infrastructure.

These Rules apply in conjunction with the TAC Arbitration Rules and regardless of the specific technical architecture, protocol, platform, or successor technology on which a digital asset, transaction, or record is maintained. They do not create a separate substantive law of digital assets and do not determine the legal characterisation of any asset, token, instrument, right, or transaction under applicable law.

Article 1 - Scope of Application

1.1 These Rules apply, in accordance with Article 69 of the TAC Arbitration Rules, only where the parties have expressly agreed to their application and where the dispute involves the determination of rights, obligations, entitlements, or liabilities in connection with digital assets, blockchain-based or distributed ledger transactions, cryptographic control mechanisms, tokenised rights, or related contractual relationships.

1.2 For the purposes of these Rules, the expression "digital assets" includes assets, rights, records, claims, units, tokens, or entitlements that are recorded, represented, transferred, controlled, evidenced, or administered through blockchain technology, distributed ledger technology, cryptographic credentials, smart contracts, token registers, custody systems, automated or self-executing code, public, private, permissioned, consortium, hybrid, or equivalent systems, or any functionally equivalent or successor technology, regardless of the specific platform, protocol, or technical architecture.

1.3 These Rules are particularly suited to disputes involving: the transfer, custody, control, valuation, access, use, tracing, attribution, liquidation, staking, delegation, governance, redemption, settlement, restoration, or replacement of digital assets or digitally recorded rights; token sale, issuance, vesting, or governance arrangements; staking, validation, liquidity, or market-making relationships; exchange, settlement, margin, liquidation, or OTC transactions; tokenised representations of real-world assets, rights, or entitlements; and disputes concerning on-chain execution, bridge transactions, cross-chain arrangements, smart contract operation, or equivalent system records.

1.4 These Rules may apply to disputes involving decentralised autonomous organisations, protocol governance, or decentralised systems only where the dispute is between identifiable persons or entities bound by an arbitration agreement. The absence of a clearly identified counterparty or an enforceable arbitration agreement is not cured by the existence of a governance mechanism, token vote, on-chain procedure, decentralised structure, automated execution, or distributed system.

1.5 These Rules do not apply solely because a payment obligation is denominated in or settled using a digital asset. Where the substance of the dispute concerns the underlying contractual relationship and no specific digital asset, technical control, tokenised right, distributed ledger record, or equivalent

system issue is in dispute, the TAC Arbitration Rules shall apply without these Supplementary Rules unless the parties have expressly agreed otherwise.

1.6 Where the parties have expressly agreed to the application of more than one set of TAC Supplementary Rules, these Rules shall govern blockchain-specific, digital-asset-specific, technical-control, cryptographic-control, and system-record issues falling within their scope. Any inconsistency between applicable Supplementary Rules shall be resolved in accordance with Articles 69.3 and 69.4 of the TAC Arbitration Rules and, where necessary, Article 69.5.

1.7 These Rules do not make applicable any other Supplementary Rules to which the parties have not expressly agreed.

Article 2 - Eligible Parties and Non-Consumer Use

2.1 These Rules are intended for disputes between parties acting in a commercial, professional, institutional, investment, or business capacity in connection with digital assets or related transactions.

2.2 These Rules do not apply to consumer disputes to the extent that applicable mandatory law restricts the use of arbitration or the application of these Rules in respect of a party acting in a consumer capacity.

2.3 The fact that a party is a natural person shall not, by itself, determine whether that party acted as a consumer or in a commercial, professional, institutional, investment, or business capacity.

2.4 Where the status of a party is disputed and may affect jurisdiction, admissibility, the application of these Rules, or the availability of mandatory protection, the Tribunal shall determine that question as a preliminary issue or at such stage as it considers appropriate, having regard to the applicable law and the circumstances of the case.

2.5 In making such determination, the Tribunal may consider all relevant circumstances, including the nature, frequency, volume, purpose, and pattern of the transactions; the use of leverage, algorithmic trading tools, automated tools, APIs, professional platforms, custody arrangements, professional trading infrastructure, or business accounts; the party's course of dealing and prior conduct; participation in liquidity provision, staking, market-making, validator operations, mining, treasury management, or similar professional activities; the existence of commercial, investment, or business objectives; and any other circumstances indicating whether the party acted for personal, domestic, non-professional, commercial, professional, institutional, investment, or business purposes.

2.6 Nothing in these Rules shall limit, exclude, or deprive any person of mandatory consumer protection applicable under the governing law, the law of the seat, or any other law mandatorily applicable to the arbitration agreement or dispute.

2.7 Where a claim or defence is advanced by or against a successor, heir, legal representative, guardian, insolvency administrator, liquidator, estate representative, or other person claiming through or on behalf of a party or account holder, the Tribunal may require evidence of that person's status, authority, and entitlement under applicable law. Nothing in these Rules shall create succession, representation, proprietary, or account-access rights not recognised by applicable law or the arbitration agreement.

Article 3 - Regulated Digital Assets and Tokenised Rights

3.1 Where the dispute involves a digital asset that may constitute, represent, evidence, reference, or be linked to a financial instrument, security, share, equity interest, debt instrument, derivative, collective investment interest, electronic money, deposit, corporate interest, partnership interest, receivable, commodity, contractual right, real-world asset, carbon credit, or other regulated or legally recognised right or instrument under applicable law, the Tribunal may take into account the regulatory status or

classification of that asset or right to the extent relevant to the determination of the rights and obligations in dispute, the applicable law, jurisdiction, admissibility, or the lawfulness of the relief sought.

3.2 These Rules do not determine whether a digital asset, token, right, claim, instrument, transaction, or arrangement constitutes a financial instrument, security, share, derivative, collective investment interest, electronic money, deposit, corporate interest, partnership interest, proprietary right, contractual right, or any other regulated or legally recognised category. That question shall be determined by the Tribunal in accordance with applicable law and, where appropriate, addressed as a preliminary issue.

3.3 Where a dispute involves a tokenised representation of a real-world asset, right, or entitlement, including tokenised shares, equity interests, debt instruments, receivables, real estate interests, commodities, carbon credits, or similar instruments, the Tribunal may take into account: on-chain records, distributed ledger records, token ledger entries, and custody records; corporate registers, cap tables, shareholder or member registers, account records, and contractual records; vesting schedules, lock-up arrangements, treasury records, corporate actions, restructurings, mergers, conversions, substitutions, and register reconciliation; valuation materials; applicable corporate, property, financial-market, and regulatory law; and any restriction arising from mandatory law, insolvency, sanctions, asset freezing, registration requirements, transfer restrictions, or regulatory requirements.

3.4 The Tribunal shall not, by application of these Rules alone, create, confirm, transfer, extinguish, perfect, register, or validate any proprietary, corporate, regulatory, financial-market, or other rights that are not established by applicable law or the agreement of the parties.

3.5 Where applicable mandatory law governs the form, registration, transfer, perfection, custody, holding, settlement, recognition, or enforcement of an asset or interest represented by or linked to a digital asset, the Tribunal shall take that law into account in determining any remedy.

3.6 Nothing in these Rules shall authorise the Tribunal to grant relief that would be contrary to mandatory law, including applicable laws or regulations concerning securities, financial instruments, payment services, electronic money, collective investment schemes, insolvency, sanctions, asset freezing, anti-money laundering, corporate capital maintenance, registration, transfer restrictions, or public policy.

3.7 Where a dispute involves a wrapped, bridged, synthetic, collateral-backed, reserve-backed, redeemable, asset-referenced, or equivalent digital asset, the Tribunal may take into account the legal and contractual relationship between the digital asset and any underlying asset, reserve, custodian, issuer, bridge, redemption mechanism, collateral arrangement, backing structure, or related entitlement. These Rules shall not by themselves determine whether the holder has a proprietary claim, contractual claim, redemption right, security interest, or other entitlement to the underlying asset or reserve.

Article 4 - Initial Technical Disclosure and Snapshot

4.1 Within a time limit determined by the Centre before the constitution of the Tribunal, and thereafter by the Tribunal, each party shall provide a concise and coherent description of the technical arrangements, assets, systems, and relationships relevant to the determination of the dispute.

4.2 Such description shall include, to the extent reasonably available and relevant:

- (a) the digital assets, tokens, tokenised rights, or digitally recorded rights in dispute, including their type and the system on which they are recorded;
- (b) relevant wallet addresses, account identifiers, smart contract addresses, custody identifiers, token registers, system identifiers, or equivalent technical references;

- (c) the roles, access rights, and authority of relevant persons or systems with respect to those assets, accounts, wallets, contracts, records, or systems;
- (d) relevant transaction history, transfer records, on-chain activity, custody records, platform records, exchange records, internal ledger records, or equivalent system records for the period in dispute;
- (e) any applicable custody arrangements, platform accounts, exchange accounts, third-party access, multisignature arrangements, smart contract permissions, governance mechanisms, recovery mechanisms, or equivalent control arrangements;
- (f) the identity and role, to the extent reasonably available, of any person or entity involved in the operation, custody, settlement, fiat payment channel, compliance review, access restriction, technical administration, platform infrastructure, liquidity provision, omnibus account structure, prime brokerage arrangement, white-label arrangement, or contractual transfer relevant to the dispute;
- (g) any known restrictions, freezes, regulatory holds, technical limitations, loss of access, compromise, pending transactions, or material changes affecting the assets, records, accounts, wallets, smart contracts, or systems.

4.3 Each party shall provide, or indicate the availability of, a snapshot of the relevant technical state as at a reference date to be determined by the Centre before the constitution of the Tribunal, and thereafter by the Tribunal. The snapshot shall record, to the extent relevant and reasonably available: wallet balances, token balances, or other asset positions; smart contract state; custody records, platform account balances, exchange account balances, token register entries, or internal ledger positions; pending transactions; known restrictions; and material changes affecting the relevant digital assets, records, accounts, wallets, contracts, or systems.

4.4 The Centre before the constitution of the Tribunal, and thereafter the Tribunal, may determine the form, source, method, and timing of any snapshot, including whether it should be prepared or verified by a party, an independent expert, a custodian, an exchange, a platform, a registrar, a transfer agent, or another appropriate source.

4.5 Each party shall indicate whether any digital asset, wallet, smart contract, custody arrangement, account, technical permission, token register, or arrangement relevant to the dispute has been created, modified, transferred, bridged, converted, restricted, reconfigured, or restructured after the occurrence of the events giving rise to the dispute, or after the party became aware of a potential dispute. Where such action is not reasonably explained, the Tribunal may take it into account as an adverse factor in assessing the evidence, drawing inferences, or allocating costs.

4.6 Where disclosure under this Article is incomplete, inconsistent, or evasive, the Tribunal may draw appropriate inferences. Before the constitution of the Tribunal, the Centre may note any apparent deficiencies in such disclosure for the consideration of the Tribunal upon its constitution. The Centre shall not draw evidentiary inferences or determine entitlement, attribution, control, authority, credibility, or intent.

4.7 Nothing in this Article shall require the disclosure of private keys, seed phrases, recovery phrases, passkeys, or equivalent credentials in a manner that creates a disproportionate security risk. The Tribunal may order secure preservation, independent verification, escrow, attestation, secure inspection, restricted disclosure, expert review, or other protective arrangements where appropriate.

4.8 The application of these Supplementary Rules does not, by itself, displace the Expedited Procedure under Article 45 of the TAC Arbitration Rules. The Centre shall assess the suitability of the Expedited Procedure at the earliest practicable stage, having regard in particular to the expected scope of technical disclosure and snapshots, the number of relevant networks, systems, accounts, or platforms, the volume and form of technical data, the need for blockchain analytics, forensic or expert evidence, preservation measures, non-party involvement, and sanctions or regulatory issues. After constitution, the Tribunal

may, after consulting the parties, invite the Centre to determine under Article 45.2 of the TAC Arbitration Rules that the standard procedure is more appropriate. Suitability may be reconsidered as the arbitration develops.

Article 5 - Core Procedural Approach

5.1 The Tribunal may assess the rights, obligations, and entitlements of the parties having regard to both the technical record and the underlying legal, commercial, economic, and operational reality of the relevant arrangement, irrespective of its formal or technical structure.

5.2 The existence of automated execution, smart contract logic, technical permissions, cryptographic signatures, distributed ledger entries, on-chain records, governance action, token vote, protocol action, automated liquidation, slashing event, token migration, airdrop, redemption event, or equivalent system event shall not, in itself, determine the legal rights and obligations of the parties. The Tribunal shall assess such technical matters as part of the overall factual and legal record.

5.3 Technical control over a digital asset, including control of cryptographic credentials, wallet access, account access, smart contract permissions, governance permissions, administrative functions, or custody arrangements, may be a significant evidentiary indicator of rights, authority, responsibility, access, or entitlement in relation to that asset, but does not automatically establish legal ownership, legal entitlement, authority, consent, or liability.

5.4 The Tribunal may assess rights and obligations in connection with digital assets that are distributed across multiple addresses, systems, protocols, accounts, wallets, custodians, or arrangements, and need not identify a single point of control where the evidence supports a divided, shared, delegated, layered, functional, temporary, conditional, automated, or governance-based allocation of rights, authority, control, or responsibilities.

5.5 The Tribunal may take into account a party's past access to, or authority over, a system, smart contract, account, wallet, credential, protocol function, or asset where such access or authority is material to the dispute, even where that access or authority has been revoked, transferred, restricted, delegated, automated, or modified.

5.6 The Tribunal may distinguish between technical execution, legal authority, contractual entitlement, economic benefit, custody, possession, access, control, beneficial interest, proprietary interest, and regulatory status.

5.7 Where a digital asset, digitally recorded right, transaction, or record is maintained, administered, or executed through a private, permissioned, consortium-based, membership-based, or hybrid system, the Tribunal may take into account the applicable membership rules, governance rules, validator or node permissions, access-control rules, transaction-inclusion rules, administrative authority, system-operation records, and any related contractual or technical arrangements. The Tribunal shall not determine the internal governance of such a system beyond what is necessary for the resolution of the dispute between the parties.

Article 6 - Blockchain Evidence and System Records

6.1 The Tribunal may admit and consider any material it deems relevant to the determination of the dispute, including transaction records and hashes; wallet address histories and token balances; smart contract event logs, state records, and execution outputs; distributed ledger records, validator records, node records, and block data; custody platform records, exchange account records, internal ledger records, and account records; bridge transaction records and cross-chain records; governance records, voting records, and protocol logs; oracle outputs and off-chain data feeds incorporated into on-chain

systems; API logs, system logs, cryptographic signatures, transaction confirmations, forensic tracing reports, and technical analysis.

6.2 The Tribunal shall determine the relevance, reliability, materiality, and weight of each item of technical evidence having regard to: the integrity and immutability of the underlying record; the method and source of extraction or production; the date of the record and any possibility of modification; the limitations of the system that generated the record; the extent to which the record is sufficiently identified, reproducible, and capable of being tested or verified; and the opportunity of the parties to examine, respond to, and challenge the evidence.

6.3 On-chain records, distributed ledger records, and equivalent system records are admissible as evidence of the occurrence and technical content of recorded transactions, states, balances, events, or permissions, subject to the Tribunal's determination of their relevance and weight. They are not presumed to be conclusive of the legal rights or obligations of the parties.

6.4 A public blockchain record, distributed ledger record, or equivalent system record may be relied upon without requiring production of the entire underlying system record, provided that the Tribunal is satisfied that the record is sufficiently identified, reproducible, and capable of being tested or verified.

6.5 Where a party relies on a record generated by a private, permissioned, custodial, exchange-based, platform-based, or internal system, the Tribunal may require that party to provide information sufficient to assess the reliability, integrity, completeness, provenance, and limitations of the record.

6.6 Where technical evidence cannot reasonably be produced in native electronic form, the Tribunal may direct the manner in which it shall be submitted, preserved, inspected, authenticated, and recorded, having regard to the nature of the evidence, procedural fairness, confidentiality, cybersecurity, data protection, and the efficient conduct of the arbitration.

6.7 The Tribunal may also admit and consider price feeds, mark prices, index values, reference-market data, order book records, execution records, routing records, transaction-ordering records, mempool records, priority-fee records, slippage records, internalisation records, related-party execution records, MEV-related records, liquidation engine records, margin call records, timestamp records, block timestamp data, validator, miner, sequencer, finality, settlement-layer, and challenge-period records, and records concerning the source, calculation, adjustment, integrity, timing, sequence, or effect of any price, liquidation, transfer, settlement, or execution relevant to the dispute.

6.8 The Tribunal may also admit and consider reserve attestations, reserve records, redemption records, eligibility lists, distribution records, claim records, token migration records, swap records, redenomination records, slashing records, validator performance records, corporate action records, royalty mechanism records, application-layer records, collateral records, lending records, rehypothecation records, title-transfer records, close-out records, encumbrance records, liability records, proof-of-liabilities materials, reserve-to-liability reconciliation records, escrow records, condition-satisfaction records, gas, nonce, and broadcast records, and records concerning the source, calculation, adjustment, integrity, timing, sequence, or effect of any event, distribution, redemption, penalty, allocation, entitlement, collateral, reserve, liability, condition, or custody arrangement relevant to the dispute.

6.9 Where the authenticity, integrity, completeness, provenance, inclusion, exclusion, sequencing, or reconciliation of a transaction, record, batch, block, ledger entry, account entry, smart contract event, platform record, or equivalent system record is disputed, the Tribunal may require the production, explanation, verification, or expert review of contextual or surrounding records, including records not themselves directly in dispute, to the extent necessary to determine the reliability or meaning of the disputed record. The Tribunal may limit the scope, time period, form, redaction, anonymisation, confidentiality protections, or expert-only access applicable to such records.

Article 7 - Digital Asset Events, Automated Outcomes and Derived Entitlements

7.1 The Tribunal may take into account any event, action, output, distribution, restriction, or change affecting a digital asset, digitally recorded right, account, wallet, smart contract, protocol, token register, custody arrangement, or equivalent system, including forks, airdrops, token migrations, swaps, redenominations, redemptions, depegs, slashing events, liquidations, governance actions, corporate actions, smart contract outputs, bridge events, oracle events, royalty mechanisms, application-layer restrictions or bypasses, and equivalent or successor events.

7.2 The technical occurrence of such event, action, output, distribution, restriction, or change shall not, by itself, determine its legal effect, contractual validity, entitlement, allocation, finality, or compliance with the parties' legal obligations.

7.3 The Tribunal may determine, by reference to the applicable law, the arbitration agreement, the parties' contract, the technical record, and the evidence as a whole:

- (a) whether a party was entitled to receive, retain, transfer, replace, redeem, or benefit from any asset, token, distribution, reward, forked asset, airdrop, migrated asset, wrapped asset, redemption right, corporate action, royalty, or other derived benefit;
- (b) the relevant record date, snapshot date, eligibility period, valuation date, cut-off time, migration period, redemption period, voting period, finality time, settlement time, challenge period, timeout, expiry time, inclusion time, settlement-layer reference time, or other reference period;
- (c) whether the event or outcome resulted from ordinary protocol operation, contractual performance, contractual breach, breach of duty, error, manipulation, unauthorised access, technical failure, or other relevant cause as determined under applicable law;
- (d) whether a digital asset, token, right, or entitlement is the same as, a successor to, a substitute for, a migrated form of, a converted form of, or economically equivalent to another digital asset, token, right, or entitlement for the purposes of the parties' rights and obligations;
- (e) whether the resulting loss, gain, distribution, penalty, dilution, shortfall, benefit, or entitlement should be allocated between the parties.

7.4 Where a party relies on a fork, airdrop, token migration, swap, redenomination, liquidation, slashing event, governance action, smart contract output, oracle output, depeg, redemption event, corporate action, royalty mechanism, application-layer restriction or bypass, or similar event, the Tribunal may require that party to provide a coherent explanation of the technical, contractual, economic, and legal basis on which the party asserts entitlement, non-entitlement, liability, or absence of liability.

7.5 Where the release, transfer, redemption, liquidation, insurance coverage, escrow release, margin call, milestone payment, distribution, or other outcome depends on the satisfaction of an off-chain condition, contractual milestone, parameter, threshold, certification, registry entry, approval, delivery, audit, performance event, or equivalent fact, the Tribunal may determine whether such condition, trigger, threshold, milestone, or fact was satisfied by reference to the applicable law, the arbitration agreement, the parties' contract, the technical record, off-chain records, expert evidence, and the evidence as a whole.

7.6 A party relying on the satisfaction or non-satisfaction of such condition, trigger, threshold, milestone, or fact may be required by the Tribunal to identify the source of the condition, the relevant contractual or technical mechanism, the applicable record date or trigger time, the evidence relied upon, and any contrary technical or off-chain records. Technical execution, non-execution, oracle output, system state, or escrow state shall not, by itself, be conclusive of whether the relevant condition, trigger, threshold, milestone, or fact was satisfied for legal or contractual purposes.

7.7 Where such explanation is incomplete, inconsistent, or evasive, the Tribunal may draw appropriate inferences, provided that the party has had a reasonable opportunity to respond.

Article 8 - Attribution of Addresses, Transactions and Signatures

8.1 A blockchain address, wallet identifier, account, smart contract address, cryptographic credential, token balance, or system record shall not, by itself, conclusively identify a natural person or legal entity or establish the identity, authority, legal capacity, ownership, entitlement, consent, responsibility, or liability of any person.

8.2 A cryptographic signature, on-chain authorisation, transaction approval, or system instruction may demonstrate control of the relevant cryptographic credential or technical permission at the time of signing, authorisation, approval, or instruction. It does not, by itself, establish the identity of the person who exercised that control, the authority of that person to act, or the consent of the party whose rights may be affected.

8.3 The Tribunal may attribute a wallet, address, account, transaction, signature, instruction, technical permission, or automated execution to a party or other person by reference to the evidence as a whole.

8.4 In determining attribution, the Tribunal may take into account, without limitation:

- (a) prior communications, instructions, admissions, confirmations, or course of dealing linking a party to an address, account, wallet, transaction, or system;
- (b) custody arrangements, KYC or onboarding records, platform account information, exchange records, internal records, transaction reports, access logs, or account records;
- (c) control over devices, credentials, accounts, wallets, smart contracts, APIs, recovery mechanisms, administrative functions, custody instructions, or governance permissions;
- (d) transaction patterns, funding sources, withdrawal destinations, clustering analysis, behavioural indicators, or other forensic indicators;
- (e) financial flows, beneficial use, economic benefit, assumption of risk, or connection to a party's known activity;
- (f) the timing, sequence, structure, and commercial rationale of relevant transactions;
- (g) any credible alternative explanation provided by a party.

8.5 Where a party asserts that it did not control, authorise, or direct a relevant address, account, wallet, transaction, signature, instruction, or system action, the Tribunal may require that party to provide a coherent explanation of the relevant technical circumstances and may draw appropriate inferences from an insufficient or inconsistent explanation.

8.6 Where authority to act has been delegated through API credentials, automated systems, trading tools, delegated signing arrangements, asset management arrangements, custody instructions, or equivalent technical mechanisms, the Tribunal may assess the scope, limits, and revocation of such delegated authority by reference to the parties' agreement, instructions, mandate, permissions, and course of dealing.

8.7 The loss, destruction, compromise, or unavailability of cryptographic credentials does not by itself establish or negate a party's rights, obligations, authority, responsibility, or liability. The Tribunal shall assess such circumstances in the context of the evidence as a whole.

8.8 Attribution based on forensic clustering, behavioural analysis, risk scoring, analytical outputs, or similar indirect methods shall be assessed together with the evidence as a whole and shall not, by itself, require the Tribunal to find identity, authority, ownership, control, consent, responsibility, or liability.

Article 9 - Control, Access and Authority

9.1 The Tribunal may assess the control, access, and authority of a party or person in relation to a digital asset, digitally recorded right, technical system, account, wallet, smart contract, protocol, custody arrangement, or equivalent mechanism by reference to the functional reality of the arrangement, including where relevant the role of that person in any platform, custody, settlement, exchange, liquidity, payment, or service structure assessed under [Article 13](#).

9.2 Relevant mechanisms may include, without limitation:

- (a) the ability to initiate, approve, block, reverse, prevent, modify, administer, or influence a transaction, balance, asset, account, wallet, smart contract, protocol, custody arrangement, or digitally recorded right;
- (b) private keys, seed phrases, recovery phrases, passkeys, or equivalent credentials;
- (c) multisignature arrangements, threshold signatures, delegated signing authority, multi-party computation arrangements, co-signing rights, or equivalent access mechanisms;
- (d) custody accounts, exchange accounts, omnibus accounts, sub-accounts, trading accounts, margin accounts, treasury accounts, platform accounts, or internal ledger accounts;
- (e) smart contract permissions, administrative keys, upgrade keys, governance keys, validator rights, oracle permissions, protocol-level permissions, token issuance rights, or rights to modify parameters;
- (f) governance rights, voting rights, upgrade rights, delegation rights, staking rights, validation rights, or protocol participation rights;
- (g) recovery, freezing, whitelisting, blacklisting, access-control, withdrawal- control, account-restriction, or asset-restriction mechanisms;
- (h) API access, automated trading systems, bots, algorithmic trading tools, or other technical interfaces;
- (i) custody arrangements, delegation structures, treasury management arrangements, operational access, or other practical mechanisms of control.

9.3 Formal technical designation, including registered ownership of a wallet address, nominal holder of credentials, account label, system role, or apparent technical title, shall not be determinative where the functional reality of control, access, or authority points to a different conclusion.

9.4 The Tribunal may determine that control over a digital asset, digitally recorded right, or technical system is exercised by more than one person and need not identify a single person exercising exclusive control where the evidence supports a shared, divided, delegated, layered, temporary, conditional, automated, or functional allocation of control.

9.5 Where a party fails to provide a coherent explanation of the technical control, access, or authority arrangements relevant to the dispute following a request by the Tribunal, the Tribunal may draw appropriate adverse inferences.

9.6 Nothing in this Article shall make technical control conclusive of legal ownership, legal entitlement, authority, consent, or liability.

Article 10 - Blockchain Analytics and Risk-Assessment Evidence

10.1 The Tribunal may admit and consider materials produced by forensic tracing tools, blockchain analytics platforms, transaction tracing tools, sanctions-screening databases, transaction-monitoring systems, risk-scoring systems, compliance tools, risk-assessment systems, intelligence tools, and equivalent analytical systems.

10.2 The Tribunal shall determine the relevance, reliability, and weight of such materials having regard to all relevant circumstances, including the source, methodology, transparency, date, version, limitations, assumptions, data inputs, confidence level, scope of the query, conflicting outputs from alternative analytical sources, and the extent to which the material can be tested, explained, examined, responded to, or challenged.

10.3 A party relying on such material shall identify, to the extent reasonably possible, the nature of the tool or system used, the date and version of the analysis, the relevant inputs, assumptions, query scope, and the conclusion relied upon.

10.4 A party may challenge the methodology, assumptions, reliability, limitations, or weight of any analytical, screening, intelligence, or risk-assessment material relied upon by another party.

10.5 Where the methodology or source data of an analytical system cannot be fully disclosed because of confidentiality, security, legal, regulatory, or proprietary restrictions, the Tribunal may adopt protective measures, require summary disclosure, appoint an expert, limit reliance on the material, or determine the appropriate weight to be given to it.

10.6 A risk score, risk classification, screening result, sanctions match, clustering output, wallet attribution, taint analysis, or other analytical conclusion shall not by itself constitute a legal determination of ownership, control, identity, illegality, sanctions status, taint, liability, authority, consent, or entitlement.

10.7 Where a tool or system relied upon under this Article is an AI-Assisted Tool within Article 38.1 of the TAC Arbitration Rules, Article 38 of the TAC Arbitration Rules applies in addition to this Article. The disclosure required by [Article 10.3](#) is additional to any targeted disclosure directed under Article 38.5 of the TAC Arbitration Rules, but the same information need not be produced twice.

Article 11 - Preservation Measures

11.1 The Emergency Arbitrator or the Tribunal may order any measure necessary to preserve the integrity of a digital asset, digitally recorded right, technical arrangement, credential, record, system, evidentiary record, or technical state pending determination of the dispute.

11.2 Such measures may include, without limitation:

- (a) suspension, restriction, or preservation of transfers or transactions in respect of specified digital assets, accounts, wallets, contracts, or systems;
- (b) prohibition on the use, transfer, bridging, staking, delegation, liquidation, conversion, disposal, or modification of relevant assets or rights;
- (c) prohibition on changes to multisignature configurations, smart contract permissions, administrative permissions, governance rights, recovery mechanisms, custody instructions, access rights, account permissions, or smart contract configurations;
- (d) preservation of transaction records, wallet histories, custody records, platform logs, access data, system records, token registers, smart contract states, account records, devices, credentials, or transaction histories;
- (e) preservation of a wallet, account, token balance, custody balance, smart contract state, token register entry, or system state as at a relevant date or time;
- (f) delivery or escrow of relevant credentials or access information to a neutral third party, independent expert, or secure arrangement, to the extent permitted by applicable law and subject to appropriate security safeguards;
- (g) secure preservation, attestation, escrow, independent verification, restricted disclosure, or expert review of credentials, records, or control mechanisms where appropriate;

(h) orders to maintain, restore, or refrain from altering the status quo pending determination of the dispute.

11.3 A party shall promptly inform the Emergency Arbitrator or the Tribunal, as applicable, of any material change affecting the digital assets, digitally recorded rights, wallets, accounts, credentials, systems, arrangements, or records subject to a measure ordered under this Article.

11.4 Any action taken in breach of a measure ordered under this Article may be treated by the Tribunal as a procedural violation and may give rise to adverse inferences or consequences in the allocation of costs.

11.5 Any measure ordered under this Article shall not impose direct obligations on any person, platform, protocol, network, validator, custodian, exchange, wallet provider, registrar, transfer agent, or other entity that is not bound by the arbitration agreement, unless permitted by applicable law. Such measures may direct a party to take or refrain from taking action within that party's legal power or control, including with respect to digital assets, accounts, credentials, records, systems, or technical arrangements accessible to that party.

11.6 The Emergency Arbitrator or the Tribunal shall take into account any security, regulatory, operational, market, custody, liquidity, volatility, enforcement, or technical risk arising from a proposed preservation measure.

11.7 An administrative measure of the Centre under Article 5 of the TAC Arbitration Rules is binding for the administration of the arbitration. The Emergency Arbitrator or Tribunal shall frame any preservation measure under this Article consistently with that administrative measure. The Centre's measure shall not determine the factual or legal basis, necessity, proportionality, or adjudicative effect of the requested preservation measure. The Centre and the Emergency Arbitrator or Tribunal may coordinate their actions within their respective functions, subject to Article 5.7 of the TAC Arbitration Rules.

11.8 Where an administrative measure of the Centre makes a requested preservation measure unlawful, impossible, incapable of implementation, or incompatible with the continued administration of the arbitration, the Emergency Arbitrator or Tribunal shall, to the extent it remains lawfully able to act, deny, defer, modify, replace, or structure the measure in any lawful and practicable manner, including through alternative preservation steps, evidentiary measures, substitute relief, or monetary security. No order under this Article may require the Centre to disregard, reverse, or act inconsistently with a measure under Article 5 of the TAC Arbitration Rules, or to continue or resume an administration that the Centre has suspended, declined, or terminated.

Article 12 - Experts and Forensic Analysis

12.1 The Tribunal may appoint independent experts, including blockchain forensic analysts, cybersecurity experts, technical systems experts, valuation experts, accounting experts, financial analysts, custody experts, regulatory specialists, or other technical or financial experts, where appropriate to the determination of the dispute.

12.2 The Tribunal may rely on expert analysis in examining transaction histories, wallet attribution, asset flows, smart contract behaviour, protocol operations, custody records, exchange records, system integrity, sanctions screening, asset taint, valuation, technical feasibility, and the technical or financial operation of complex digital asset arrangements.

12.3 The parties shall be given a reasonable opportunity to comment on the expert's mandate and findings and may examine tribunal-appointed experts where appropriate.

12.4 The Tribunal shall not delegate adjudicative findings to the expert. The expert may analyse data, records, flows, systems, tools, technical structures, and regulatory or financial materials, but the

Tribunal shall determine jurisdiction, admissibility, attribution, control, entitlement, ownership, liability, legal characterisation, credibility, inference, remedy, and costs.

12.5 Expert mandates shall be clearly defined, with particular care in relation to the scope of transaction tracing, asset attribution, technical analysis, valuation, sanctions screening, regulatory classification, technical feasibility, pricing methodology, event analysis, and delegated authority, so as to limit the mandate to matters necessary for the determination of the dispute.

12.6 Where appropriate, the Tribunal may direct experts appointed by the parties to confer and identify areas of agreement and disagreement.

Article 13 - Platform Groups, Third-Party Platforms and Non-Parties

13.1 The Tribunal may take into account the role of any platform, system, service provider, person, or entity involved in the provision, operation, administration, support, settlement, custody, payment, compliance review, access control, liquidity, or technical infrastructure of a digital asset service, whether or not that person or entity is a party to the arbitration.

13.2 Where a digital asset service is provided, operated, administered, supported, or presented to users through more than one person or entity, the Tribunal may take into account the functional role of each such person or entity in relation to the disputed assets, accounts, transactions, records, restrictions, access, custody, settlement, fiat payment channels, compliance review, liquidity provision, technical operation, or user relationship.

13.3 For the purposes of [Article 13.2](#), relevant structures may include, without limitation, exchange groups, custody arrangements, wallet infrastructure providers, bridge operators, protocol interfaces, fiat on-ramp or off-ramp providers, payment processors, staking services, validator or node operators, liquidity providers, market makers, prime brokerage arrangements, omnibus account structures, white-label platforms, contractual novation or onboarding structures, token issuers, administrators, trustees, nominees, registrars, transfer agents, analytics providers, API providers, execution layer providers, technology layer providers, or other platform or service structures.

13.4 A party that relies on the separate role, responsibility, or legal identity of another person or entity involved in such a service may be required by the Tribunal to provide a coherent explanation of the relevant operational, contractual, technical, regulatory, custody, payment, settlement, liquidity, compliance, or platform structure, to the extent such information is reasonably available to that party or to any person or entity within that party's control or with which that party has a contractual relationship.

13.5 Where such explanation is incomplete, inconsistent, or evasive, the Tribunal may draw appropriate inferences, including in relation to control, access, authority, responsibility, attribution, reliance, conflict of interest, or the allocation of risk as between the parties to the arbitration.

13.6 Where the Tribunal considers that a finding concerning the role, conduct, records, confirmations, or evidence of a person or entity not party to the arbitration may be material to the determination of the dispute, the Tribunal may, after consulting the parties, invite such person or entity to provide written observations, records, confirmations, or evidence on a limited basis as determined by the Tribunal, subject to any confidentiality, data protection, security, regulatory, or protective measures the Tribunal considers appropriate.

13.7 Such participation shall not make that person or entity a party to the arbitration and shall not confer any procedural rights beyond those expressly granted by the Tribunal.

13.8 The Tribunal may order a party to request, obtain, preserve, or produce records, confirmations, or cooperation from a third-party platform, custodian, exchange, registrar, transfer agent, wallet provider, payment provider, liquidity provider, prime broker, white-label operator, API provider, execution layer

provider, technology layer provider, or other person or entity where such request, production, or cooperation is within that party's legal power or control.

13.9 The Tribunal shall not order a person or entity not bound by the arbitration agreement to take any technical, operational, legal, or administrative action, and nothing in these Rules shall impose direct obligations on any person or entity not bound by the arbitration agreement, unless permitted by applicable law. Where the performance of a remedy depends on the cooperation of a non-party platform or service provider, the Tribunal shall frame any order as an obligation on a party to take steps within that party's legal power or control.

Article 14 - Illegality, Sanctions and Tainted Asset Allegations

14.1 Where issues arise during the arbitration indicating that the digital assets, digitally recorded rights, transactions, wallets, addresses, accounts, systems, or arrangements in dispute may involve or be associated with illegality, fraud, theft, hacking, unauthorised access, market abuse, sanctions, designated persons or addresses, asset freezing, money laundering, terrorist financing, evasion of regulatory restrictions, stolen, misappropriated, or fraudulently obtained assets, assets subject to regulatory freezes, enforcement actions, court orders, insolvency restrictions, or other conduct contrary to mandatory law or public policy, the Tribunal may address such issues to the extent necessary for the proper determination of the dispute.

14.2 The Tribunal may, as a preliminary issue or at any stage of the proceedings, adopt procedural measures in response to such issues, including:

- (a) inviting further submissions from the parties;
- (b) requiring limited or targeted production of evidence, including analytics, screening, tracing, custody, source-of-funds, source-of-assets, or compliance materials;
- (c) directing a snapshot, preservation measure, or technical or forensic report;
- (d) requiring explanation of the origin, source, movement, control, access, status, or economic effect of assets, accounts, wallets, transactions, or systems;
- (e) preserving assets, records, accounts, wallets, credentials, or system states;
- (f) staying, sequencing, or limiting parts of the proceedings;
- (g) addressing the regulatory status, origin, legitimacy, or lawfulness of the assets, rights, transactions, or arrangements as a threshold question;
- (h) limiting, refusing, or conditioning relief that may give effect to conduct contrary to mandatory law or public policy.

14.3 The Tribunal shall not grant relief that would give effect to arrangements or conduct contrary to sanctions regimes applicable to the relevant party, transaction, asset, performance, or relief, asset-freezing measures, anti-money laundering obligations, regulatory restrictions, insolvency restrictions, securities or financial-market laws, mandatory law, or public policy, or that would enable a party to benefit from theft, fraud, hacking, unauthorised access, money laundering, sanctions evasion, market abuse, or other unlawful conduct. This shall not prevent the Tribunal from granting relief available under applicable law to a party seeking recovery, restitution, compensation, or other remedy in respect of assets or rights affected by such conduct.

14.4 The Tribunal is not under a duty to conduct independent investigations into alleged illegality, sanctions violations, tainted assets, theft, fraud, hacking, money laundering, market abuse, or regulatory violations beyond the matters raised by the parties or reasonably apparent from the record. Article 35 of the TAC Arbitration Rules applies to the conduct of the proceedings in connection with any such issues.

14.5 A blockchain analytics output, risk score, screening flag, sanctions match, clustering output, taint analysis, or equivalent analytical result indicating a potential sanctions, illegality, attribution, or taint concern shall not, by itself, be determinative. The Tribunal shall assess the legal and evidentiary significance of such material in accordance with [Article 10](#).

14.6 Nothing in these Rules shall require a party to disclose information protected by legal privilege or equivalent protections. Such protections shall not, by themselves, prevent the Tribunal from requiring disclosure of non-privileged facts concerning the existence, origin, movement, control, access, status, or economic effects of assets, wallets, accounts, transactions, or systems.

14.7 Where a party relies on an inconsistent, overlapping, or conflicting regulatory, sanctions, asset-freezing, insolvency, supervisory, enforcement, or other mandatory rule or obligation, the party shall identify the rule or obligation, its legal source, the jurisdictional connection relied upon, the person, transaction, asset, record, disclosure, performance, or relief to which it is said to apply, and its nature, scope, duration, and practical effect. The Tribunal shall determine whether and to what extent the rule or obligation applies, having particular regard to the mandatory law of the seat in procedural matters and, where relevant, to any law mandatorily applicable to the relevant person, transaction, asset, record, disclosure, performance, or relief. The Tribunal may take the rule or obligation into account in determining jurisdiction, admissibility, procedure, liability, relief, timing of performance, and allocation of risk. Where it is relied upon as a defence to liability or relief, the Tribunal may consider its scope, duration, practical necessity, proportionality, and effect. The Tribunal shall not require a party to act contrary to a mandatory rule that it determines to be applicable. A mere assertion unsupported by a sufficient explanation of applicability and practical effect shall not excuse non-compliance. The Tribunal may instead order a lawful alternative, protective measure, substitute evidence, substitute performance, monetary relief, or another appropriate measure.

14.8 Where a party relies on market integrity, platform stability, system integrity, liquidity protection, orderly settlement, client-asset protection, reserve protection, protocol security, or similar grounds as a justification for suspending, restricting, reversing, modifying, delaying, liquidating, allocating, haircutting, or otherwise affecting digital assets, accounts, transactions, positions, redemptions, withdrawals, or entitlements, the Tribunal may require that party to identify the contractual, technical, regulatory, or factual basis of the measure. The Tribunal may take into account the scope, duration, necessity, proportionality, consistency, non-discriminatory application, conflict of interest, available alternatives, notice given, and effect of the measure in determining liability, relief, compensation, valuation, and allocation of risk.

14.9 Article 5 of the TAC Arbitration Rules governs institutional compliance with sanctions and mandatory restrictions and the lawful administration of the arbitration. This Article governs the Tribunal's evidentiary, procedural, and remedial assessment of sanctions, asset-freezing, illegality, and tainted-asset issues arising in the determination of the dispute.

14.10 An administrative measure or compliance determination of the Centre under Article 5 of the TAC Arbitration Rules is binding for the administration of the arbitration but does not bind the Tribunal in determining sanctions status, illegality, taint, jurisdiction, admissibility, liability, or relief. The Tribunal shall determine those matters independently in accordance with applicable law and the evidence properly before it. The fact that the Centre has taken, declined, modified, or lifted an administrative measure shall not, by itself, constitute evidence or give rise to a presumption in the Tribunal's adjudicative analysis.

Article 15 - Remedies

15.1 The Tribunal may grant any remedy consistent with the TAC Arbitration Rules and applicable law, including:

- (a) declarations as to the rights, entitlements, obligations, liabilities, access, authority, responsibility, or control of the parties in connection with digital assets, digitally recorded rights, or related arrangements;
- (b) declarations that a technical arrangement, designation, record, signature, wallet, account, custody arrangement, smart contract, or control mechanism does not reflect the underlying legal rights or obligations of the parties;
- (c) orders requiring a party to transfer, return, deliver, restore, replace, or procure the transfer or return of digital assets or digitally recorded rights within that party's legal power or control;
- (d) orders requiring a party to take any technical step within that party's legal power or control necessary to give effect to the Tribunal's findings, including initiating, signing, countersigning, co-signing, authorising, approving, revoking, or refraining from initiating a transaction, instruction, or technical action;
- (e) orders requiring a party to provide, restore, modify, or refrain from modifying access, permissions, confirmations, records, smart contract parameters, custody instructions, technical configurations, or account settings, to the extent within that party's legal power or control;
- (f) orders requiring a party to cooperate with a custodian, exchange, registrar, transfer agent, platform, wallet provider, or other person in relation to access, transfer, correction, restoration, preservation, verification, or implementation of the Award, to the extent within that party's legal power or control;
- (g) monetary compensation, restitution, disgorgement, account of profits, interest, or costs;
- (h) any other measure appropriate to give effect to the Tribunal's findings.

15.2 Any declaration or remedy concerning a digital asset, digitally recorded right, technical arrangement, related entitlement, wallet, account, address, system, platform, protocol, smart contract, or technical control mechanism shall be made as between the parties to the arbitration, unless the person or entity affected is bound by the arbitration agreement, has been joined to the arbitration, or the applicable law permits such relief.

15.3 An order under [Article 15.1\(d\)](#), [Article 15.1\(e\)](#), or [Article 15.1\(f\)](#) shall not impose direct technical, operational, legal, or administrative obligations on any person or entity that is not bound by the arbitration agreement.

15.4 Where a transfer, restoration, reversal, access measure, correction, signature, permission change, smart contract modification, cooperation measure, or other act cannot lawfully or effectively be performed because it depends on a person or entity not bound by the arbitration agreement, because the relevant system or protocol does not permit it, because the digital asset is technically irreversible, inaccessible, irrecoverable, transferred, dissipated, lost, compromised, mixed, bridged, frozen, or rendered inaccessible, or because performance is prevented or restricted by an applicable insolvency, regulatory, sanctions, asset-freezing, sovereign immunity or analogous state-based immunity, or other mandatory regime, the Tribunal may grant monetary compensation or any other remedy available against a party to the arbitration.

15.5 In determining monetary compensation or valuation, the Tribunal may take into account the relevant date or period, market data, liquidity, volatility, transfer restrictions, custody restrictions, regulatory restrictions, loss of access, loss of opportunity, loss of use, staking rewards, income, distributions, dilution, price manipulation, market disruption, forks, airdrops, token migrations, swaps, redenominations, redemptions, depegs, slashing events, corporate actions, governance actions, royalty mechanisms, reserve shortfalls, regulatory changes, and any other relevant circumstance.

15.6 Where relief involves more than one asset, record, register, account, wallet, smart contract, corporate record, contractual obligation, or technical action, the Tribunal may structure the relief on a

staged, conditional, coordinated, or sequential basis, provided that such relief is directed only at parties to the arbitration and is consistent with applicable law.

15.7 The Tribunal may determine that different valuation dates or methods are appropriate for different assets, claims, losses, benefits, rights, remedies, events, or periods.

15.8 For the purposes of determining the amount in dispute, fees, or advances under Article 55.10 and Article 56 of the TAC Arbitration Rules, a party asserting a claim involving a digital asset or digitally recorded right shall state a reasonable monetary value in a currency accepted by the Centre and identify the valuation date, source, method, and material assumptions used. Unless the Centre determines otherwise, the relevant date shall be the date of commencement or, for a claim submitted later, the date on which that claim is submitted. The Centre may determine another date, source, method, or value where volatility, liquidity, market disruption, transfer or custody restrictions, forks, airdrops, staking rewards, or other circumstances make the stated value unrepresentative or impracticable. A determination by the Centre for fee or advance purposes is administrative only, may be revised, and does not bind the Tribunal in determining valuation, liability, damages, relief, interest, or costs.

Article 16 - Safeguards

16.1 The Tribunal shall ensure that each party has a reasonable opportunity to respond to any technical material, analytics output, expert finding, attribution evidence, valuation evidence, screening result, other evidence, or material evidentiary inference or presumption on which the Tribunal may rely.

16.2 The Tribunal shall take appropriate measures to protect confidentiality, cybersecurity, data protection, privilege, trade secrets, private information, commercially sensitive information, and the security of digital assets, credentials, accounts, wallets, systems, and records.

16.3 Nothing in these Rules shall require the disclosure of private keys, seed phrases, recovery phrases, passkeys, or equivalent credentials in a manner that creates a disproportionate risk of loss, unauthorised access, dissipation, compromise, or misuse. The Tribunal may adopt alternative protective measures, including independent verification, attestation, escrow, secure inspection, restricted disclosure, expert review, or other protective arrangements. The Tribunal may also adopt protective measures for view keys, zero-knowledge proofs, selective disclosures, cryptographic attestations, confidential transaction records, or equivalent privacy-preserving evidence.

16.4 Nothing in these Rules shall require the disclosure of information protected by legal privilege or equivalent protections. Legal privilege or equivalent protections shall not, by themselves, prevent the Tribunal from requiring disclosure of non-privileged facts concerning the existence, technical operation, control, access, movement, status, or economic effects of a digital asset arrangement, wallet, account, transaction, record, or system.

16.5 The Tribunal shall not give effect to any transaction, arrangement, technical state, system record, or claim, or grant any relief, that would be contrary to mandatory law, applicable sanctions regimes, asset-freezing measures, or public policy.

16.6 The heightened sensitivity of digital asset evidence, including wallet addresses, cryptographic credentials, transaction histories, custody records, account records, analytics outputs, and system records, shall be taken into account by the Tribunal and the Centre in determining appropriate confidentiality, cybersecurity, data protection, access, and protective measures under the TAC Arbitration Rules.

16.7 The Tribunal shall, in its Award, identify the principal facts and circumstances on which any material evidentiary inference, attribution finding, control finding, authority finding, ownership finding, entitlement finding, technical determination, feasibility finding, illegality finding, sanctions finding, taint finding, valuation finding, or remedy is based.

16.8 Technical records, analytics outputs, signatures, wallet control, account control, system records, or automated execution shall not be legally conclusive solely by reason of their technical form where further analysis is required under the applicable law, the arbitration agreement, or the evidence as a whole.

16.9 Where the conditions of Article 43 of the TAC Arbitration Rules are satisfied, the Tribunal may summarily dismiss, or determine as a preliminary issue, a claim, defence, or discrete question concerning the legal characterisation, attribution, control, authority, entitlement, or effect of a digital asset, technical record, automated outcome, or the relationship between an on-chain or system record and an off-chain legal or contractual arrangement. This paragraph does not create a separate standard from Article 43 of the TAC Arbitration Rules.

Article 17 - Entry into Force and Relationship with the TAC Arbitration Rules

17.1 These Supplementary Rules enter into force on 1 August 2026.

17.2 These Supplementary Rules apply only where the parties have expressly agreed to their application in accordance with Article 69 of the TAC Arbitration Rules.

17.3 When applicable, these Supplementary Rules shall apply in conjunction with the TAC Arbitration Rules and shall prevail over them to the extent of any inconsistency, subject to the arbitration agreement and applicable mandatory law.

17.4 The version of these Supplementary Rules in force on the date of commencement of the arbitration shall apply throughout the arbitration. A later revision shall not apply.

17.5 A superseded version of these Supplementary Rules may not be selected for an arbitration commenced after that version ceased to be in force. If the arbitration agreement expressly requires a superseded version, the Centre shall decline to administer the arbitration unless the parties amend that requirement.