

BLOCKDEV PLC

Yugo

POLICY ON CUSTODY AND ADMINISTRATION OF CRYPTO-ASSETS ON BEHALF OF CLIENTS

Custody and Administration Policy

Field	Value
Document	Internal policy under Article 3(1), point (16)(a) of Regulation (EU) 2023/1114 (MiCA)
Legal basis	MiCA, including Article 75; Delegated Regulation (EU) 2025/305, including Article 12; applicable national law
Status	Approved by the Board of Directors
Version	V2.1
Date	27.09.2026
Document owner	Compliance Department / jointly with the Product, Operational Risk and Reporting function (CPO) and the CTO
Approving body	Board of Directors of BlockDev PLC
Scope	All clients, crypto-assets, wallets, external contractors and internal processes related to custody and administration

Version control and approval

Version	Date	Description	Prepared by	Approved
v1.0	28.05.2026	POLICY ON CUSTODY AND ADMINISTRATION OF CRYPTO-ASSETS ON BEHALF OF CLIENTS	Compliance	BoD
V2.0	29.07.2026		Compliance	BoD
V2.1	27.09.2026	Register of Supported Assets and Networks (Annex 4) with the actual assets and statuses; access review every 6 months; reconciliation through the platform's automated checks; ARTs ineligible; roles and cross-references to the Description of the Reference ICT Architecture and the related documents	Compliance / CTO	BoD

Contents

1. Purpose and scope
2. Legal basis
3. Definitions
4. Governance and responsibilities
5. Description of the custody model
6. Supported clients, assets and networks
7. Ownership and segregation of client assets
8. Register of client positions
9. Incoming transfers and crediting
10. Outgoing transfers and withdrawals
11. Controls over instructions and access
12. Reconciliation and control of discrepancies
13. Reporting to clients
14. Rights attached to crypto-assets
15. Incidents, losses and liability
16. Oversight of BitGo and other external contractors
17. Continuity, exit and return of assets

18. Reporting, records and review

Annexes

1. Purpose and scope

This Policy sets out the rules, processes and control mechanisms through which BlockDev PLC, operating under the Yugo trade name, provides the service of custody and administration of crypto-assets on behalf of clients. The Policy applies to all products, channels, wallets, operations, external contractors and employees involved in the holding, safekeeping, control, administration, transfer or return of crypto-assets, or of the means of access to them, on behalf of clients.

The Policy aims to ensure that client crypto-assets are safekept and administered in a transparent, secure, traceable and regulatory-compliant manner, with a clear distinction between the assets of clients, the assets of BlockDev PLC and the assets of other persons.

- protection of client assets and of the means of access to them;
- maintenance of an accurate internal register of client positions;
- segregation of client assets and a prohibition on their use for own account;
- daily reconciliation between the internal register, blockchain data and data from the external custody provider;
- clear rules on deposits, withdrawals, transfers, protocol forks, airdrops, incidents and the return of assets;
- effective oversight of BitGo Europe GmbH and other external contractors, where used.

2. Legal basis

The Policy has been drawn up having regard to the following regulatory framework:

- Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA), including the definition of the service in Article 3(1), point (16)(a), and the obligations under Article 75 on the custody and administration of crypto-assets on behalf of clients;
- Delegated Regulation (EU) 2025/305 on the information to be included in an application for authorisation as a crypto-asset service provider, including Article 12 on the custody and administration policy;
- Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets, to the extent applicable to transfers of crypto-assets;
- the Markets in Crypto-Assets Act (ZPKA), Ordinance No. 77 and the applicable acts of the Financial Supervision Commission (FSC);
- the rules on AML/CFT, sanctions, personal data protection, information security, DORA/ICT governance and outsourcing, to the extent applicable to the Company's activities.

For the purposes of the MiCA application, this document should be read together with the Policy on Outsourcing Activities to External Contractors, the Description of the Reference ICT Architecture (the "Description") and the related documents (BCP framework, DR procedures, access management, ICT providers), the internal rules under the Measures Against Money Laundering Act (MAMLA), the Business Continuity Policy and Plan, the General Terms and Conditions for Users, the complaints-handling policy and the risk management framework.

3. Definitions

Term	Meaning
CASP	A crypto-asset service provider within the meaning of MiCA.
Custody service	Custody and administration of crypto-assets on behalf of clients, including the safekeeping or control of crypto-assets or of the means of access to them.
Client assets	Crypto-assets held or administered on behalf of a client, whether in an individual or an omnibus wallet.
Means of access	Cryptographic keys, credentials, recovery components, access rights, approval rights or other means that allow the movement or control of crypto-assets.
BitGo	BitGo Europe GmbH, used as an external contractor for custody infrastructure, key safekeeping/control and technical support for wallet operations, under the applicable contract.
Internal register	The system or register of BlockDev PLC for recording client balances, movements, blocked amounts, fees and rights attached to the assets.
Reconciliation	The process of reconciling the internal register, on-chain balances, BitGo data and other applicable records.
Authorised representative	A person designated by BlockDev PLC with rights of access to, or to give instructions to, the custody infrastructure, subject to this Policy and the approval matrix.

4. Governance and responsibilities

Responsibilities under this Policy are allocated so as to ensure a clear separation between business, technology and control functions.

Body/function	Key responsibilities
Board of Directors (BoD)	Approves the Policy, material changes to the custody model, the risk appetite, the use of critical external contractors and the annual review. Receives regular reports on custody risks, incidents, reconciliation discrepancies and outsourcing risk.
Executive Director (ED)	Ensures the implementation of the Policy, the resources needed to implement it, escalation to the BoD and control over the operational functions.
Compliance	Ensures regulatory compliance, incident reviews and interaction with competent authorities.
Specialised Unit	AML/CFT, sanctions control, Travel Rule processes, review of client disclosures.
CPO (Product, Operational Risk and Reporting function)	Maintains the risk assessment for custody, outsourcing, ICT, operational risk and concentration risk, and oversees corrective measures.
CTO / ICT function	Responsible for system architecture, access rights, security, logs, change management, technical documentation and the monitoring of external ICT/custody providers.
Operations / Client Operations	Performs client onboarding, instruction processing, client communication, maintenance of statements and records, and first-level checks of transfers.
Internal audit / independent review	Periodically assesses the effectiveness of controls, records, reconciliation and outsourcing oversight, in proportion to the scale of the business.

5. Description of the custody model

BlockDev PLC provides the custody and administration service as the CASP responsible to the client. BitGo Europe GmbH is used as an external contractor for custody infrastructure, including technical key safekeeping/control, wallet infrastructure, transaction-signing support, reporting and support, where applicable.

The use of BitGo does not transfer BlockDev PLC's regulatory responsibility towards the client. BlockDev PLC remains responsible for the client relationship, the internal register of positions, disclosures, segregation, reconciliation, the approval of instructions, AML/transaction verification/Travel Rule checks, complaints, reporting and oversight of the external contractor.

Element	Role of BlockDev PLC / Yugo	Role of BitGo
Client contract	Contracting party and crypto-asset service provider to the client; provides terms, disclosures and support.	Not a contracting party to the client, unless expressly agreed otherwise.
Keys / technical custody infrastructure	Exercises oversight, controls, approvals and the instruction-submission model.	Safekeeps/controls keys and wallet infrastructure under the contract.
Internal register	Maintains the register and client positions.	Provides custody records and statements to BlockDev PLC.
Movement instructions	Validates the client instruction, AML/transaction verification/sanctions, limits and approvals.	Executes valid instructions in accordance with security procedures and applicable law.
Reconciliation	Performs daily reconciliation and investigates discrepancies.	Provides balances, transaction records and support in the event of discrepancies.
Incidents	Coordinates incident response, notifications to clients/regulators and corrective actions.	Notifies and cooperates in accordance with the contract/service levels.

6. Supported clients, assets and networks

The custody service is provided only for clients, assets and distributed ledger technology networks approved by BlockDev PLC following a risk assessment, an AML/CFT assessment, a technical assessment and confirmation from the custody infrastructure provider.

- Individual clients: only after successful identification, risk assessment, sanctions/politically exposed person (PEP) screening and acceptance of the client terms;
- Business clients/merchants: only after business identification, verification of the beneficial owner, sanctions/PEP screening, review of the business model and contractual approval for onboarding;
- Supported assets: only crypto-assets included in the Register of Supported Assets and Networks;

- Unsupported assets/networks: not accepted for custody; erroneous transfers are handled under the procedure for unsupported assets, with no guarantee of recovery.

If a crypto-asset already held or administered on behalf of a client becomes unsuitable for support for legal, regulatory, AML/CFT, sanctions, operational, technical, security, market or reputational reasons, BlockDev PLC may designate the relevant crypto-asset or network as unsupported or ineligible for future custody. In such a case, the Company notifies the affected clients within a reasonable time, to the extent permitted under applicable law, and stops accepting new deposits, new transfers or new operations involving that asset or network. The Company may continue to support only the actions necessary for the controlled withdrawal, return or migration of the relevant asset, subject to the applicable AML/CFT, sanctions, KYT, Travel Rule, technical and security checks. The time frame and manner of withdrawal, return or migration of such an asset are determined according to the nature of the risk, technical feasibility, the availability of the relevant network, the requirements of the external wallet/custody infrastructure provider and applicable law.

Asset category	Status	Additional conditions
Crypto-assets other than ARTs/EMTs	Eligible after internal approval	Assessment of liquidity, AML exposure, technical support and custody support.
ARTs, EMTs (incl. USDC, EURC)	Ineligible for custody and transfer (General Terms and Conditions, sections 5.3–5.4)	EMTs may form part only of the exchange services, subject to a separate regulatory basis and client documentation.
Unsupported tokens / scam tokens	Ineligible	Not credited; handled under the procedure for erroneous/unsupported deposits.

7. Ownership and segregation of client assets

Client crypto-assets are held in the name and for the account of clients and do not constitute own assets of BlockDev PLC. The Company is not entitled to use client assets for its own account, to fund operating expenses, to secure its own obligations, or for lending, restaking, staking or any other activity, except with the client's express prior consent and only if such activity is authorised and falls within the Company's regulatory scope.

- Client assets are segregated from the own assets of BlockDev PLC.
- Client positions are recorded separately for each client in the internal register.
- Where omnibus wallets are used, the entries in the register must at all times allow the rights of each client to be identified.
- Own corporate wallets, fee wallets and operational wallets are not commingled with client custody wallets.
- Every movement between client wallets, corporate wallets and operational wallets is documented and approved in accordance with the approval matrix.

Wallet type	Permitted content	Control
Segregated client wallet	Assets of a specific client	Allocation in the register + BitGo/blockchain record.
Omnibus client wallet	Assets of multiple clients	Mandatory detailed register per client and daily reconciliation.
Corporate wallet	Own assets of BlockDev PLC	Separate from client wallets; not used for client custody.
Fee wallet	Company fees after charging/collection	Separate accounting and approval for transfers.
Hold/investigation wallet	Assets with an unclear status or under review	Used only for incidents/unsupported deposits, under Compliance oversight.

8. Register of client positions

BlockDev PLC maintains an up-to-date register of client positions. The register must make it possible at any time to establish which crypto-assets are held on behalf of each client, in what amount, on which network, through which wallet/address and what movements have been made.

- unique client identifier;
- asset ticker, full name, network/chain, contract address where applicable;
- available balance, pending deposits, pending withdrawals, blocked/frozen balances;
- transaction hash, timestamp, sender/recipient address, fee, reference to the client instruction;
- price reference, where applicable for statements;
- link to the transaction verification/Travel Rule/sanctions checks;
- audit trail of changes and manual adjustments.

A manual adjustment to the register is permitted only after documented approval by Operations, Compliance and Risk, with the original entry, the reason, the timestamp and the person who made the change being retained.

9. Incoming transfers and crediting

Incoming transfers are accepted only for supported assets and networks. Before a client position is credited, at least the following checks are performed:

- Confirmation that the asset and network are included in the Register of Supported Assets and Networks.
- Blockchain confirmations in accordance with the set confirmation thresholds.
- Transaction verification/wallet screening of the sender's address and the exposure of the transaction.
- Sanctions screening and AML/CFT risk assessment.
- Travel Rule process, where applicable.
- Matching against a client instruction/order/expected deposit, where available.
- Crediting in the internal register and notification of the client.

Situation	Action
Deposit of a supported asset from a low-risk wallet	Crediting after confirmations and automated checks.
Deposit with medium/high risk exposure in transaction verification	Hold for manual review; decision by Compliance before crediting/return/blocking.
Unsupported asset or wrong network	Not credited automatically; incident/support ticket; recovery only if technically and legally feasible.
Sanctions exposure	Immediate blocking/freezing, escalation to the MLRO and legal/regulatory assessment.

10. Outgoing transfers and withdrawals

Outgoing transfers and withdrawals are executed only on the basis of a valid client instruction, after successful checks and in compliance with the approval matrix. The Company may refuse, delay or stop a withdrawal in the event of AML/CFT, sanctions, fraud, technical, legal or regulatory risk.

- Receipt of the client instruction through an approved channel.
- Authentication and enhanced authentication of the client, where applicable.
- Verification of the available balance and of the client's entitlement to the assets.
- Check of the recipient address, its status on the list of approved addresses and its exposure in transaction verification.
- Collection/transmission of Travel Rule data, where applicable.
- Approval under the matrix according to amount, asset, risk rating and address.
- Submission of the instruction to BitGo/the custody infrastructure provider.
- On-chain monitoring, confirmation and notification to the client.
- Update of the register and archiving of evidence.

Withdrawal type	Minimum control	Escalation
Small withdrawal to an approved low-risk address	Automated checks + dual control according to limits	Operations in the event of a technical issue.
Withdrawal to a new address	Address screening + waiting/verification period + four-eyes approval	Compliance for medium/high risk.
Large withdrawal	Four eyes + Compliance review + Risk approval depending on the threshold	ED/BoD for exceptional amounts.
High-risk/sanctions exposure	Hold / refusal / freeze	MLRO and Legal; possible notification to competent authorities.
Emergency withdrawal/return of assets	Special procedure with approval by the ED + Compliance + Risk	BoD in the event of significant risk.

11. Controls over instructions and access

Access to the custody infrastructure is restricted to authorised representatives approved by management and subject to ongoing control. All access is granted on the principle of least privilege, with multi-factor authentication, individual credentials, logging and periodic review.

- shared credentials are prohibited;
- all privileged actions are logged and subject to review;
- access rights are reviewed at least every 6 months in accordance with the “Access Management” document (Section 4, Area G) and immediately upon a change of role/departure;
- a new authorised representative is added only after approval, training, a background/compliance check and entry in the Access Rights Register;
- instructions to BitGo are submitted only through the agreed security procedures;
- operations above thresholds require the four-eyes principle or higher-level escalation.

Control	Description	Frequency
MFA	Mandatory for all privileged/custody systems	Continuous
Access review	Review of roles, rights and active users (“Access Management” document)	Every 6 months and ad hoc
Log review	Review of privileged actions and withdrawals	Monthly or upon an incident
Training	Training on custody operations, AML, sanctions and ICT security	Before access and annually
Revocation	Immediate removal of access upon departure/role change/incident	Ad hoc

12. Reconciliation and control of discrepancies

BlockDev PLC performs a daily reconciliation between the internal register, the data from BitGo/the custody provider and the on-chain balances. Reconciliation is performed by the platform’s automated checks — reconciliation of every transfer against BitGo and the network confirmation, and a check of balances against thresholds every 5 minutes (the Description, sections 10.3 and 13.1); the reconciliation register consists of the results of the automated checks and of the manual cases where a deviation arises. The aim is to ensure that total client balances per asset do not exceed the available crypto-assets held for clients and that every movement is correctly recorded.

- At least daily reconciliation of all client assets under custody;
- intraday monitoring in the event of high volumes, significant transfers or network instability;
- every discrepancy is classified by severity and escalated;
- no withdrawal is permitted that would result in a negative client balance or a discrepancy;
- the results are archived and available for audit/regulatory review.

Formula / rule	Description
$\Sigma \text{ Client register balances} \leq \text{Custody provider / On-chain balance}$	For each asset, the total balance across clients may not exceed the holdings in the relevant custody wallet.
$\text{Client register balance} = \text{Opening balance} + \text{Deposits} - \text{Withdrawals} - \text{Fees} \pm \text{Adjustments}$	Every client balance must be traceable through the transaction history.
Pending operations register	All pending deposits/withdrawals are kept in a separate register with the date, reason and owner.

Severity	Example	Action deadline
Low	Delayed blockchain confirmation or a small rounding difference	By the next business day
Medium	Unallocated deposit or pending withdrawal beyond the standard time frame	Same day; notification to Compliance/Risk
High	Missing asset, unauthorised movement, discrepancy between the register and the custody balance	Immediate escalation to the ED, Compliance, Risk and the CTO
Critical	Loss of assets, suspected compromise, sanctions block with a significant impact	Incident procedure + notifications under applicable law

13. Reporting to clients

Clients receive a statement of position in electronic format at least once every three months and upon request. The statement must contain sufficient information to enable the client to understand their positions and movements during the relevant period.

- identification of the client and the period;

- crypto-asset, network, quantity and valuation, where applicable;
- opening and closing balance;
- deposits, withdrawals, transfers, fees and adjustments during the period;
- information on blocked/frozen/pending positions, where applicable;
- instructions for objections, complaints and client support.

Client statements do not constitute investment advice or a tax statement. Any price information is provided for reporting purposes and may depend on external market data sources.

14. Rights attached to crypto-assets

Crypto-assets may be associated with rights or events such as protocol forks, airdrops, token migrations, renamings, staking rewards, governance rights or other network events. BlockDev PLC supports only those rights or events that have been approved in advance and are technically, legally and operationally feasible.

- By default, staking, lending, borrowing, restaking and yield-generating activities are not carried out with client assets under this Policy.
- Protocol forks/airdrops are not supported automatically; the decision is taken after a risk/legal/technical assessment.
- Clients are notified of supported network events where these may affect their rights.
- Unsupported airdrops/forks may not be credited if recovery/support is not technically or legally feasible.
- Governance voting is carried out only if it is provided for in the client terms and there is a clear procedure.
- In the event of a fork, airdrop, token migration, network upgrade, protocol change or other network event, BlockDev PLC carries out a legal, regulatory, AML/CFT, sanctions, technical, operational and risk assessment of whether the event will be supported. BlockDev PLC is not obliged to support every fork, airdrop, new token, network change or right arising in connection with a supported crypto-asset. The Company may temporarily suspend or restrict deposits, withdrawals, transfers or other operations involving the affected asset where this is necessary to protect client assets, information security, regulatory compliance or technical stability. Clients are notified of material events that may affect their positions, to the extent practically possible and permitted under applicable law. Unsupported forked assets, airdropped tokens or other newly arising rights are not automatically credited to the client and may not be recoverable through the Yugo platform. If the Company decides to support a given network event, client rights are determined on the basis of the client position recorded in the internal register at the relevant time the event occurs, to the extent technically, legally and operationally possible.

15. Incidents, losses and liability

An incident is any event that may lead to a loss, an unauthorised movement, unavailability, incorrect recording, a compromise of access or a regulatory breach in connection with client crypto-assets or the means of access to them.

Incident type	Examples	Initial action
Security incident	Compromised credentials, unauthorised access, suspected key compromise	Immediate freezing/deactivation of access, incident bridge, notification of the CTO/Compliance/Risk.
Transaction incident	Wrong address, duplicate withdrawal, unauthorised withdrawal	Stop/hold if possible, on-chain tracing, client support, legal/regulatory assessment.
Provider incident	BitGo outage, delayed withdrawal, data inconsistency	Escalation under the service levels, alternative process, assessment of the impact on clients.
Register/ reconciliation incident	Discrepancy between the register and the custody balance	Suspension of the affected operations, investigation, notification of management.
AML/sanctions incident	Sanctions exposure or suspicious transaction	Escalation to the MLRO, freezing/refusal where necessary, reporting assessment.

In the event of a loss of client crypto-assets or means of access, BlockDev PLC investigates the incident and determines the cause, the persons/systems responsible, the extent of the impact on clients, the necessary compensatory or corrective actions and the applicable notifications to clients, external providers, insurers and competent authorities.

For the purposes of this Policy, a “system failure” includes any failure, interruption, unavailability or malfunction of hardware, software, telecommunication lines, cloud infrastructure, API integrations, wallet/custody infrastructure, an external provider, a blockchain node, a KYT/Travel Rule system or any other critical technological or operational system used by BlockDev PLC or by its external provider.

In the event of a system failure, the Company applies its procedures for incident management, business continuity, reconciliation, client notification, temporary suspension of operations and return/migration of assets, where this is necessary to protect client crypto-assets.

Where a system failure affects BitGo Europe GmbH or another external wallet/custody infrastructure provider, BlockDev PLC activates the applicable escalation mechanisms, requests information and assistance from the provider, assesses the impact on client assets, documents the event and takes measures to contain the risk, including the temporary suspension of deposits, withdrawals or new operations, where necessary.

The liability of BlockDev PLC to clients is governed by the client terms and applicable law. Contracts with external contractors must provide, to the extent possible, for back-to-back protection, incident reporting, audit rights and assistance with claims.

16. Oversight of BitGo and other external contractors

BitGo Europe GmbH is treated as an external contractor performing a critical function, insofar as it provides custody infrastructure for client assets. Oversight is carried out in accordance with the Policy on Outsourcing Activities to External Contractors, the "ICT Providers" document (register, BitGo sheet — scenarios S1/S2/S3, concentration map) and this Policy.

- prior due diligence assessment;
- assessment of regulatory status, jurisdiction, financial capacity, security controls, continuity/disaster recovery and subcontracting;
- a written contract covering service levels, confidentiality, data protection, audit/access rights, incident notification, termination and exit clauses;
- ongoing monitoring at least once a year and on an ad hoc basis upon an incident/material change;
- assessment of concentration risk and an exit/migration plan;
- maintenance of the outsourcing register and the evidence file.

Control over the external contractor	Minimum frequency
Review of service levels and incidents	Monthly/quarterly depending on criticality
Risk reassessment	At least annually
Review of access rights and representatives	Every 6 months ("Access Management" document)
Review of continuity/disaster recovery evidence	Annually
Exit plan test / simulation exercise (test BC1 under the BCP framework)	Annually or upon a material change
Review of subcontractors	Upon notification or a material change

17. Continuity, exit and return of assets

BlockDev PLC maintains procedures for returning client crypto-assets as soon as possible upon ordinary termination, an extraordinary event, the cessation of business, or the termination/unavailability of BitGo or another custody provider.

- Identification of the affected clients, assets, wallets and balances.
- Freezing of non-essential movements, if necessary to protect clients.
- Reconciliation before return or migration.
- Notification of clients of actions, time frames and instructions.
- Execution of withdrawals/migration to client addresses or to an approved alternative provider.
- Confirmation, closing of the register and final statement.
- Report to management and, where applicable, to competent authorities.

Scenario	Main approach
Termination by a client	Return/withdrawal after identification/AML/transaction verification checks and settlement of fees.
Discontinuation of the custody product	Advance notice, alternative provider or withdrawal to a client address.
BitGo outage	Escalation under the service levels, temporary suspension of the affected operations, client communication.
Termination of the relationship with BitGo	Exit plan, migration to an approved alternative or return to clients.
Cessation of Yugo's business	Orderly wind-down plan, priority for returning client assets, communication with the regulator.

18. Reporting, records and review

All records relating to the custody service are kept in a secure and reproducible format for the period required by applicable law and internal policies. The records must be sufficient to evidence client rights, the execution of instructions, checks, approvals, reconciliation, incidents and regulatory compliance.

- client instructions and consents;
- evidence of client/business identification, AML/transaction verification, sanctions and Travel Rule checks;
- register records and statement history;
- BitGo/provider reports, on-chain hashes and wallet records;
- approval and access logs;
- reconciliation and discrepancy reports;
- incident reports, root cause analyses and evidence of corrective measures;
- outsourcing due diligence and ongoing monitoring records.

This Policy is reviewed at least once a year and whenever a material change occurs, including:

- a change in the custody model;
- a change concerning BitGo Europe GmbH or another external wallet/custody infrastructure provider;
- the addition or removal of a supported crypto-asset or network;
- a material incident, system failure or loss of client assets;
- a material reconciliation discrepancy;
- a change in applicable law, regulatory expectations or guidance from a competent authority;
- a change to the internal register, the ICT architecture, the access procedures or the approval matrix;
- findings of an internal audit, independent review, supervisory inspection or BCP/DRP test.

All material changes are documented, assessed by Compliance, the Risk function and the CTO/ICT function, and submitted to the Board of Directors for approval, where applicable.

Annex 1: RACI matrix (responsibility assignment matrix)

Process	Responsible	Accountable	Consulted	Informed
Approval of the custody policy	Compliance / Risk / CTO	BoD	Legal, Operations	All relevant functions
Addition of a new asset/network	Risk + CTO + Compliance	ED/BoD if the risk is material	Operations, Liquidity	Client support
Withdrawal approval	Operations	ED/Delegated approver	Compliance/Risk upon alerts	Client
Daily reconciliation	Operations/Finance	CPO (Product, Operational Risk and Reporting function)	CTO, Compliance	ED in the event of discrepancies
Incident response	CTO/Compliance/Risk	ED	Legal, Provider, Operations	BoD/FSC where applicable
Oversight of BitGo	Risk/CTO/Compliance	ED	Legal, Operations	BoD

Annex 2: Approval matrix for withdrawals and instructions

Operation category	Threshold/condition	Required approval	Additional checks
Low-value withdrawal	Up to an internally approved threshold, to an approved low-risk address	Dual control by Operations	Automated transaction verification/sanctions checks
Medium-value withdrawal	Above the low threshold or to a new address	Operations + Compliance	Address verification, transaction verification, waiting period if necessary
High-value withdrawal	Above the high threshold or unusual activity	Operations + Compliance + Risk + ED	Manual review of sender/recipient, enhanced due diligence
Sanctions/high-risk exposure	Sanctions match or high-risk alert in transaction verification	Specialised Unit; Compliance where necessary	Hold/freeze/refusal/reporting assessment

Operation category	Threshold/condition	Required approval	Additional checks
Emergency return of assets	Cessation of business/provider incident/client protection	ED + Compliance + Risk; notification to the BoD	Reconciliation and evidence pack

Annex 3: Minimum registers

Register	Content	Owner
Client positions register	Client positions, balances, assets, networks, transaction history, pending/blocked amounts	Operations / Finance
Register of supported assets and networks	Approved assets, networks, contract addresses, confirmation thresholds, risk notes	Risk / CTO / Compliance
Access rights register	Authorised representatives, roles, rights, two-factor authentication status, date of approval/review/revocation	CTO
Withdrawals register	Instructions, approvals, transaction verification checks, transaction hashes, status, exceptions	Operations
Reconciliation register	Results of the daily reconciliation, discrepancies, actions, confirmation	Finance / Risk
Incident register	Incidents, severity, root cause, actions, notifications, closure	Risk / Compliance / CTO
Outsourcing register	BitGo and other providers, services, criticality, due diligence, service levels, reviews, exit plan	Risk / Compliance

Annex 4: Register of Supported Assets and Networks (as at 27.09.2026)

Asset	MiCA type	Network	Technical integration	Offered for custody/transfer	Confirmation threshold	Status
ETH	Crypto-asset other than ART/EMT	Ethereum Mainnet	Yes (BitGo)	Yes	As per the platform configuration	Active
BTC	Crypto-asset other than ART/EMT	Bitcoin Mainnet	Pending (new-asset procedure)	After integration and go-live approval	—	Approved, not active
LTC	Crypto-asset other than ART/EMT	Litecoin Mainnet	Pending	After integration	—	Approved, not active
XRP	Crypto-asset other than ART/EMT	XRP Ledger	Pending	After integration	—	Approved, not active
XLM	Crypto-asset other than ART/EMT	Stellar Mainnet	Pending	After integration	—	Approved, not active
SOL	Crypto-asset other than ART/EMT	Solana Mainnet	Pending	After integration	—	Approved, not active
BCH	Crypto-asset other than ART/EMT	Bitcoin Cash Mainnet	Pending	After integration	—	Approved, not active
LINK	Crypto-asset other than ART/EMT (ERC-20)	Ethereum Mainnet	Pending	After integration	—	Approved, not active
USDC	EMT	Ethereum Mainnet, Polygon	Yes (technical)	No — outside the scope of custody/transfer (exchange only)	—	Excluded (General Terms and Conditions, section 5.3)
POL	Crypto-asset	Polygon	Yes, for network fees only	No — deactivated for client flows	—	Internal use

Technical integration does not mean that an asset is offered; the activation of an asset follows the procedure in the Description, section 10.3 (entry in this register after due diligence and approval → registration in BitGo and in the platform configuration → test → balance checks → go-live approval by the CTO and Compliance → update of the register). ARTs are not supported (General Terms and Conditions, section 5.4). The register is updated whenever an asset/network is added or removed and is reviewed together with the Description.

Annex 5: Daily reconciliation checklist

- Extraction of the current balances from BitGo/the custody provider for all client wallets.
- Extraction of the internal balances from the register by client, asset and network.

- Comparison of total client balances with the balances at the custody provider/on-chain.
- Identification of pending deposits, pending withdrawals and blocked/frozen amounts.
- Investigation of all differences and classification by severity.
- Obtaining confirmation from Operations/Finance and escalating exceptions to Risk/Compliance.
- Archiving of the evidence pack: exports, screenshots, hashes, confirmation, exception requests.

Annex 7: Sources and regulatory references

- Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA), in particular Article 3(1), point (16)(a), and Article 75.
- Delegated Regulation (EU) 2025/305 on the information in an application for authorisation as a crypto-asset service provider, in particular Article 12.
- Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets.
- Markets in Crypto-Assets Act (ZPKA) and Ordinance No. 77, to the extent applicable.
- FSC letter, outgoing Ref. No. PF-22-22-1, concerning the application of BlockDev PLC and the additional information requested regarding BitGo/custody and Article 12 of Delegated Regulation (EU) 2025/305.