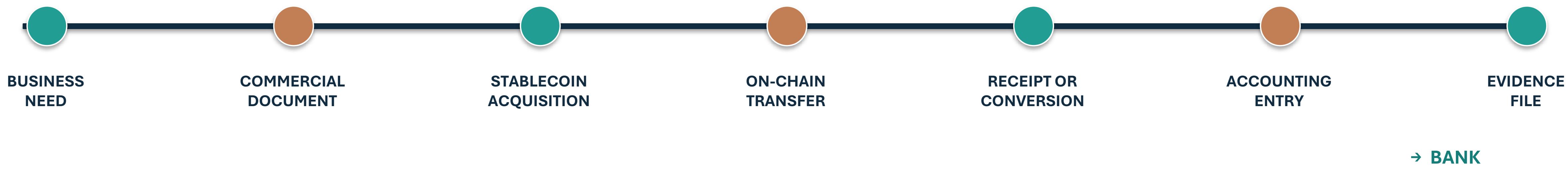
Stablecoin flows:
does your banking documentation explain, substantiate and secure your transactions?

A method for linking each flow to its business rationale, counterparties, evidence and accounting treatment.

AN END-TO-END RECONSTRUCTED TRANSACTION



A TRANSACTION THE BANK CAN UNDERSTAND

2026 EDITION

Summary

Useful banking documentation must tell the story of a transaction from end to end.
Gathering invoices, statements and screenshots is not enough. The documentation must show how each stablecoin flow relates to an identifiable business transaction, known parties and consistent evidence.

1 UNDERSTAND THE BANKING CHALLENGE

Why does a flow become difficult to assess when it is fragmented across providers, wallets, networks and documents?

2 IDENTIFY THE QUESTIONS

What is the business rationale? Who is involved? Where do the funds come from? Where do they go?

3 RECONSTRUCT THE PATH

Connect the bank account, provider, wallets, on-chain transfer and final use.

4 GATHER THE EVIDENCE

Identify the required commercial, banking, accounting and technical documents.

Reading path — continued

5 IDENTIFY THE PARTIES

Document platforms, wallet addresses, beneficiaries and relationships between the parties.

6 BUILD THE DOCUMENTATION

Organise the information into a clear, consistent package that can be produced quickly.

7 CHECK READINESS

Review the available evidence before the transaction or a bank request.

8 DECIDE

Complete documentation supports the analysis without guaranteeing acceptance of the transaction.

UNDERSTAND → MAP → DOCUMENT → IDENTIFY → ORGANISE → CHECK → DECIDE

The banking challenge of stablecoin flows

A transaction visible on a blockchain is not necessarily an understandable business transaction.
A company may have an invoice, a bank statement, a platform history and a transaction identifier. Unless these items are linked, they do not allow the transaction to be reconstructed easily.

CONTRACT OR INVOICE
Why pay?

→

BANK TRANSFER
Funds mobilised

→

PROVIDER ACCOUNT
Stablecoins acquired

→

ON-CHAIN TRANSFER
Asset, network, addresses

→

RECIPIENT WALLET
Who controls it?

WHAT THE BANK NEEDS TO RECONSTRUCT

ONE BUSINESS TRANSACTION

Need → Parties → Funds → Transfer → Destination → Accounting

The blockchain shows a transfer, not its full explanation

THE CHALLENGE IS NOT ONLY TECHNICAL

FATF standards require financial institutions to identify their customer and beneficial owner, understand the purpose and intended nature of the business relationship, and examine whether transactions are consistent with their knowledge of the customer, its business and risk profile. This due diligence may include the source of funds when necessary.[1]

THE BLOCKCHAIN SHOWS A TRANSFER, NOT ITS FULL EXPLANATION

A transaction identifier alone does not demonstrate the commercial rationale, the legal identity of the parties, control of the wallet, the origin of the euro funds, the final use, internal approval or the accounting treatment. In the European Union, transfers involving a regulated provider must be accompanied by information on the originator and beneficiary.[2] [3]

DO NOT CONFUSE

Regulatory obligation: banks and providers apply the due-diligence measures required by their jurisdiction and risk assessment. Proposed good practice: the company voluntarily links its business, banking, technical and accounting evidence. None of the texts reviewed requires a document officially called a “stablecoin flow banking documentation package”.

SOURCES
1. Financial Action Task Force — The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation — updated October 2025, Recommendation 10. Link
2. European Parliament and Council of the European Union — Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets — 31 May 2023. Link
3. European Banking Authority — Guidelines on information requirements in relation to transfers of funds and certain crypto-assets under Regulation (EU) 2023/1113 — 4 July 2024. Link

What the bank needs to understand

The bank does not examine only a transfer: it seeks to understand the transaction behind it.
Useful documentation must answer five questions quickly. The depth of the checks depends on the jurisdiction, the customer profile, the nature of the transaction and the institution's risk assessment.

1 WHO IS INVOLVED?

- Company, directors, beneficial owners
- Supplier, customer, providers
- Wallet controller
- Ultimate economic beneficiary

2 WHY?

- Business need
- Contract, purchase order or invoice
- Relationship between the parties
- Intended final use

3 WHAT AND HOW MUCH?

- Fiat amount
- Stablecoin and network
- Fees and differences
- Expected frequency

4 THROUGH WHICH PATH?

- Bank account
- Acquisition provider
- Wallets and transfer
- Conversion or use

5 IS IT CONSISTENT?

- Declared business activity
- Transaction profile
- Commercial documents
- Accounting and approvals

Common principles, but no universal questionnaire

FATF

Customer and beneficial-owner identification, purpose of the relationship, consistency with the business activity and risk profile, and source of funds when necessary.[1]

FRANCE

Ongoing due diligence; enhanced review of a complex, unusually large transaction or one with no apparent economic rationale.[2]

WAEMU

Amount and nature of transactions, source and destination of funds, economic rationale and consistency with the information held on the customer.[3]

UNITED STATES / UNITED KINGDOM

Understanding the nature and purpose of the relationship and the expected transactions. The FCA considers blockchain analysis without off-chain information insufficient.[4,5]

WHAT THIS GUIDE ADDS FOR STABLECOIN FLOWS

The texts do not all prescribe documentation organised in the same way. This guide proposes a transaction record linking the parties, business rationale, flow of funds, evidence and accounting. It is a documentation good practice, not a universal regulatory form.

SOURCES

1. Financial Action Task Force — The FATF Recommendations — updated October 2025, Recommendation 10. Link
2. French Republic — Monetary and Financial Code, Articles L. 561-5, L. 561-5-1, L. 561-6, L. 561-10-2 and R. 561-12-1 — consolidated version consulted on 28 July 2026. Link
3. BCEAO — Instruction No. 003-03-2025 of 18 March 2025 on customer identification, identity verification and customer due diligence by financial institutions — published on 1 April 2025. Link
4. Federal Financial Institutions Examination Council — BSA/AML Examination Manual: Customer Due Diligence — Overview — consulted on 28 July 2026. Link
5. Financial Conduct Authority — Financial Crime Guide, FCG 3: Money laundering and terrorist financing — updated 29 November 2024. Link

End-to-end mapping of the flows

Mapping a flow means aligning the movement of value with the movement of evidence.

BUSINESS LOGIC	Need →	Contract / order →	Invoice →	Expected payment →	Receipt			
MOVEMENT OF VALUE	Bank account →	Transfer to provider →	Acquisition →	Sending wallet →	On-chain transaction →	Receiving wallet →	Conversion / use →	Final asset
MOVEMENT OF EVIDENCE	Rationale →	Bank reference →	Buy order →	Proof of control →	TxID + network →	Beneficiary →	Statement / evidence →	Accounting entry

WHAT AN EXECUTIVE SHOULD REMEMBER A blockchain screenshot is not a complete map: each movement of value must be linkable to evidence.

The flow record

IDENTITIES

- Initiating company
- Economic counterparty
- Ultimate beneficiary
- Providers and wallet controllers

VALUE

- Fiat amount
- Stablecoin amount
- Fees and differences
- Amount received

TECHNICAL DATA

- Stablecoin and network
- Addresses
- Transaction identifier
- Dates and intermediate transfers

RECONCILIATION

- Contract or invoice
- Bank reference
- Provider reference
- Accounting reference and differences

INFORMATION DOES NOT ALWAYS TRAVEL WITH VALUE

Identification data does not always appear directly on the blockchain. In the European Union, the relevant providers retain and transmit certain information; additional checks may be required for self-hosted addresses, particularly above €1,000.[1] In the United Kingdom, the FCA expects applicants for registration to map the complete path of funds and crypto-assets.[2] In WAEMU, fiat-payment data supports the documentation but is not sufficient to reconstruct the on-chain transfer.[3] Consequence: combine banking data, provider data and on-chain evidence in one package.

SOURCES

1. European Parliament and Council of the European Union — Regulation (EU) 2023/1113 — 31 May 2023, notably Articles 14, 16 and 26. Link
2. Financial Conduct Authority — Cryptoassets: What we expect to see in your application for registration — 22 March 2023, updated 30 June 2026. Link
3. BCEAO — Instruction No. 001-01-2024 of 23 January 2024 on payment services in WAEMU — notably Article 56. Link

Three consistency checks

CONSISTENT TRANSACTION

PARTIES

Do the names on the contract, provider account, wallet and proof of receipt refer to the same party or to an explainable relationship?

AMOUNTS

Is the difference between the fiat amount and the amount received explained by fees, the rate or execution terms?

DATES

Do the order, transfer, acquisition, transaction and receipt form a consistent timeline?

Documents and evidence to assemble

Useful evidence must explain a specific stage of the flow and be linkable to the other evidence.
Banking documentation is not strengthened by the number of files it contains. It becomes useful when each document answers a question and every item can be linked to the same transaction.

1 — BUSINESS AND COMMERCIAL

Why was the transaction carried out?

- Contract or agreement
- Purchase order, invoice or funding request
- Description of the goods or service
- Identity of the counterparty
- Proof of delivery or performance
- Explanation for using the stablecoin

2 — BANKING AND PROVIDER

How were the funds mobilised and converted?

- Transfer instruction and statement
- Payment reference
- Provider statement
- Purchase or conversion order
- Amount, rate and fees
- Withdrawal or transfer confirmation

Technical, accounting and internal evidence

3 — ON-CHAIN

What happened on the network?

- Stablecoin and token contract
- Network and addresses
- Transaction identifier
- Amount, fees, date and time
- Intermediate transactions
- Explorer link and available export

4 — ACCOUNTING AND INTERNAL

How did the company approve, control and record the transaction?

- Internal approval
- Initiator and approver
- Accounting entry
- Valuation method and source
- Treatment of fees and differences
- Reconciliation record and exceptions

The pivot document — the flow reconciliation sheet

Unique reference → Business purpose → Counterparty → Amounts and dates → Providers and wallets → On-chain transaction → Accounting entry → Attachments

IDENTIFIABLE

Source, issuer, date and transaction visible.

LINKABLE

Common reference to the contract, payment, transaction or entry.

CONSISTENT

Parties, dates and amounts match or are explained.

ACCESSIBLE

Readable format and access restricted to authorised persons.

RETENTION AND SECURITY

FATF recommends at least five years for financial institutions.[1] The European regulation requires five years for the relevant providers.[2] In France, accounting documents and supporting records are retained for ten years.[3] In WAEMU, the 2023 uniform law provides for ten years for financial institutions.[4] These rules do not create a single retention period for every item in the documentation. Good practice: maintain a retention schedule by category, jurisdiction, period, owner and deletion date. The documentation must never contain a private key or recovery phrase.

SOURCES

1. Financial Action Task Force — The FATF Recommendations — version amended June 2026, Recommendation 11. Link
2. European Parliament and Council of the European Union — Regulation (EU) 2023/1113 — 31 May 2023, Article 26. Link
3. French Republic — Commercial Code, Article L. 123-22 — version in force consulted on 28 July 2026. Link
4. WAEMU Council of Ministers — Uniform Law on AML/CFT/CPF — March 2023, Article 23. Link

Providers, wallets and counterparties

A wallet address is not an identity, and a trading name is not always the entity providing the service.
The documentation must separately identify the provider used, the person controlling each wallet and the economic counterparty to the transaction.
These three elements must then be linked.

1 — THE PROVIDER

Who actually provides the service?
- Legal name and trading name
- Country, registration, authority
- Status and services covered
- Signing entity and account holder
- Role: purchase, conversion, custody or transfer

2 — THE WALLET

Who controls the address used?
- Network and full address
- Custodial or self-hosted wallet
- Declared controller and role
- Verification method and date
- Persons authorised to initiate or approve

3 — THE COUNTERPARTY

Who receives the funds economically?
- Legal name, country and activity
- Relationship with the company
- Contract or invoice
- Ultimate beneficiary
- Provided wallet and any third party
- Applicable sanctions checks

Three links to document

PROVIDER

Legal entity
+ service used

SERVICE

COUNTERPARTY

Economic beneficiary
+ contractual relationship

ATTRIBUTION

WALLET

Address + controller
+ network

Does the registered entity actually provide the service used?

Why does the address belong to the counterparty, its provider or an authorised third party?

Do the address, network, amount and TxID match the instructions and evidence?

CONSISTENT FILE

INFORMATION TO COMPLETE

ESCALATE BEFORE EXECUTION

Status, self-hosted addresses and sanctions

PROVIDER STATUS

ESMA's MiCA register lists, among others, authorised providers and entities reported as non-compliant.[1 2] In the United Kingdom, FCA registration is an AML requirement, not an endorsement.[3] Implementation remains uneven across jurisdictions.[4] Retain dated evidence of the register check and its limitations.

SELF-HOSTED ADDRESS

EBA guidelines provide for specific measures for these transfers.[5] For the company: who controls the address, for which transaction and based on what evidence? An address received by email is not always sufficient.

SANCTIONS

Where US rules apply, OFAC treats virtual currencies like traditional currencies and recommends a risk-based approach.[6] European, national and foreign sanctions regimes must be determined separately.

SOURCES

1. ESMA — Public Statement: MiCA transitional period ends — 23 June 2026. Link
2. ESMA — Markets in Crypto-Assets Regulation: Interim MiCA Register — update consulted on 24 July 2026. Link
3. Financial Conduct Authority — Cryptoassets: AML/CTF regime — updated 12 February 2026. Link
4. Financial Action Task Force — Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs — 26 June 2025. Link
5. European Banking Authority — Guidelines on information requirements in relation to transfers of funds and certain crypto-assets — 4 July 2024. Link
6. Office of Foreign Assets Control — Sanctions Compliance Guidance for the Virtual Currency Industry — 15 October 2021. Link

How to build the banking documentation package

The documentation must be prepared during the transaction, not reconstructed urgently after a bank request.

The method uses two levels: a permanent file common to all flows, and a transaction file for each transaction or homogeneous series. A reconciliation sheet links the two.

PERMANENT FILE

What changes infrequently

- Identity, activity, directors and beneficial owners
- Responsibilities and usage policy
- Authorised providers, wallets, stablecoins and networks
- Approval, retention procedures and bank contacts

RECONCILIATION SHEET

Unique reference • purpose • counterparty • amount • dates • provider • stablecoin • network • wallets • TxID • entry • evidence • approval

TRANSACTION FILE

What is assembled for each flow

- Contract and business rationale
- Bank instruction and acquisition
- On-chain transfer and receipt
- Conversion or final use
- Accounting, approvals and differences

The six-step method — 1 to 3

1 FRAME

Purpose, parties, amount, stablecoin, network, providers, wallets, path and authorised persons.

2 OPEN

Assign a unique internal reference used in the sheet, file, approval, accounting and communications.

3 COLLECT

Operations: contract. Treasury: transfer, acquisition and payment. Compliance: parties and sanctions. Accounting: entry and reconciliation.

SOURCES

1. Federal Financial Institutions Examination Council — BSA/AML Examination Manual: Customer Due Diligence — Overview — consulted on 28 July 2026. Link

The six-step method — 4 to 6

4 RECONCILE

Compare parties, amounts, dates, references, wallets, fees, final use and entry. Explain every difference.

5 VALIDATE OR ESCALATE

Validate if the file is consistent; complete it if evidence is missing; escalate inconsistencies, sanctions issues or an uncertain beneficiary.[1]

6 FINALISE AND UPDATE

Finalise the sheet, retain original formats, record the approval, identify versions and update the permanent file.[1]

SOURCES

1. Federal Financial Institutions Examination Council — BSA/AML Examination Manual: Customer Due Diligence — Overview — consulted on 28 July 2026. Link

The bank response pack

1 — SUMMARY

One page: purpose, parties, flow of funds and accounting treatment.

2 — KEY EVIDENCE

Contract, transfer, provider statement, on-chain transaction, receipt and entry.

3 — SUPPORTING DOCUMENTS

Providers, wallets, internal controls and checks performed.

A PROPOSED METHOD, NOT A UNIVERSAL FORMAT

The FCA expects applicants for registration to provide complete, current, reviewed and approved documents, together with a flow-of-funds map covering the full cycle and third parties, without imposing a single format.[2] FATF recommendations are implemented through each national framework.[3] None of the sources reviewed establishes a universal banking-documentation model for every company using stablecoins.

SOURCES

2. Financial Conduct Authority — Cryptoassets: What we expect to see in your application for registration — 22 March 2023, updated 30 June 2026. Link

3. Financial Action Task Force — The FATF Recommendations — updated June 2026. Link

Preparation and decision checklist

OBJECTIVE — Identify missing information before executing the flow or responding to the bank.
A transaction is ready when its purpose, parties, path and evidence can be explained without contradiction.
This checklist is an internal method proposed by the guide. It replaces neither the checks required by the applicable jurisdictions nor the bank's own analysis.

1. BUSINESS NEED

- The business need is explained.
- The contract, purchase order or invoice is available.
- The relationship between the parties is identifiable.
- The amount and frequency are consistent with the business activity.
- The use of the stablecoin can be explained.
- The source and destination of the funds are documented.

☐ Yes ☐ Partial ☐ No

2. PARTIES

- Company and counterparty are legally identified.
- Ultimate beneficiary is known or the relationship is explained.
- The entity providing each service is identified.
- Provider status is checked in the relevant register.[1 2]
- Each wallet is attributed to a person, company or provider.
- Applicable sanctions checks have been performed.

☐ Yes ☐ Partial ☐ No

SOURCES

1. ESMA — Public Statement: MiCA transitional period ends — 23 June 2026. Link
2. ESMA — Interim MiCA Register — latest update consulted: 24 July 2026. Link

Checklist — flow of funds and evidence consistency

3. FLOW OF FUNDS

- Starting point in fiat money is identified.
- Stablecoin acquisition is documented.
- Stablecoin and network are stated.
- Sending and receiving wallets are recorded.
- Transaction identifier is retained.
- Intermediate transfers are explained.
- Receipt, conversion or final use is demonstrated.[3]

☐ Yes ☐ Partial ☐ No

4. EVIDENCE CONSISTENCY

- Names are consistent across the documents.
- Amount differences are explained.
- Timeline is logical.
- Banking, technical and accounting references are reconciled.
- Accounting entry is linked to the transaction.
- Internal approvals are identifiable.
- Documents are readable, dated and accessible.[4]

☐ Yes ☐ Partial ☐ No

SOURCES

3. Financial Conduct Authority — Cryptoassets: What we expect to see in your application for registration — consulted on 28 July 2026. Link

4. BCEAO — Instruction No. 003-03-2025 on customer identification, identity verification and customer due diligence — 18 March 2025. Link

Checklist — red flags and decision

5. RED FLAGS AND CONTROLS

- No unexplained wallet change.
- No unidentified beneficiary or intermediary.
- No provider presented as authorised without verification.
- No sanctions result left without analysis.
- No material contradiction remains unresolved.
- No private key or recovery phrase is stored in the file.[5] [6]

☐ Yes ☐ Partial ☐ No

READY

Key checks completed; inconsistencies explained. Finalise internal approval and retain the documentation.

TO COMPLETE

Evidence is missing, with no major red flag. Obtain the additional information before execution or submission.

SUSPEND AND ESCALATE

Identity, source/destination, status, sanctions, wallet or contradictions remain unexplained.

SOURCES

5. European Banking Authority — Guidelines on information requirements in relation to transfers of funds and certain crypto-assets — 4 July 2024. Link
6. Office of Foreign Assets Control — Sanctions Compliance Guidance for the Virtual Currency Industry — 15 October 2021. Link

Conclusion: understand, control and decide

OBJECTIVE — Decide on facts, without confusing documentation quality with automatic acceptance by the bank.

Strong banking documentation does not make a transaction acceptable by default. It makes the transaction understandable, controllable and subject to a fact-based decision. The quality of the documentation depends less on the number of documents collected than on the continuity of the demonstration.

1 EXPLAIN

Need, contract, parties, stablecoin and final use.

→

2 RECONSTRUCT

Account, provider, acquisition, wallets, transfer and receipt.

→

3 DEMONSTRATE

Documents, statements, TxID, receipt and accounting.

→

4 CONTROL

Parties, amounts, dates, providers, wallets and approvals.

→

5 DECIDE

Can the company stand behind and explain the transaction?

Three possible decisions

EXECUTE AND DOCUMENT

Clear purpose, identified parties, known path and consistent evidence. Approve under internal procedures, finalise the sheet and retain the documentation.

COMPLETE BEFORE EXECUTION

Evidence is missing or a difference remains insufficiently explained, with no critical red flag. Defer until the information is obtained.

SUSPEND OR ABANDON

Identity, wallet control, source/destination, provider status, sanctions or a major inconsistency remain unresolved. Suspend, escalate and abandon if necessary.

What the documentation enables — and what it does not guarantee

WHAT THE DOCUMENTATION ENABLES

- Make the transaction easier to understand
- Reduce document searches
- Accelerate a response to the bank
- Reveal inconsistencies
- Demonstrate the controls performed
- Link treasury, compliance and accounting

WHAT IT DOES NOT GUARANTEE

- Acceptance of the flow by the bank
- Opening or maintaining the relationship
- No request for additional information
- Compliance in every jurisdiction
- Provider quality or solvency
- Absence of stablecoin, network or counterparty risk

THE EXECUTIVE'S FINAL TEST

- Can we explain the transaction in one minute?
- Can we demonstrate the complete flow of funds?
- Can we produce the key evidence immediately?
- Can we justify the decision despite the identified risks? If any answer is no, the documentation is not complete.

SOURCES

1. Financial Action Task Force — The FATF Recommendations — version amended June 2026. Link
2. ESMA — Markets in Crypto-Assets Regulation: Interim MiCA Register — consulted on 28 July 2026 ; Public Statement: MiCA transitional period ends — 23 June 2026. Link
3. Financial Conduct Authority — Cryptoassets: AML/CTF regime — updated 12 February 2026. Link