Orbital.

The Stablecoin Guide

Building the right infrastructure — a guide for businesses moving stablecoin payments from pilot to production.

How you consume it

Stablecoin and fiat pay-ins and payouts

Money & assets

FX, stablecoin and fiat custody make funds usable

The regulated core

Licensing, compliance and security make the payment permissible

In this guide

01 **Introduction**
Stablecoin ambition versus payment reality

02 **The hidden complexity of the stablecoin stack**
Three considerations before you build

03 **Start small, think big, scale fast**
A strategic principle

04 **The stablecoin infrastructure stack**
Eight capabilities, three tiers

05 **How the stablecoin stack shifts across three use cases**
How the payment objective translates into infrastructure requirements

06 **Define the use case. Build for what comes next.**
Build for what comes next

What's next

01

Introduction

Stablecoin ambition versus payment reality

IN THIS SECTION

End-to-end payment journey p.4

Stablecoin ambition versus payment reality

For businesses making cross-border payments, stablecoins offer the prospect of faster, more flexible ways to move value.

But accessing a stablecoin is not the same as having a complete payments solution. A wallet, custody service or connection to a blockchain network can provide an important capability; its commercial value depends on how it works with the infrastructure around it.

Consider a business collecting payments from overseas customers and paying international suppliers. Transferring a stablecoin is only one part of that process. The business also needs to identify who is paying, apply the appropriate checks, attribute funds to the right customer or invoice, and decide whether to hold or convert them. It then needs to pay the supplier in the currency or asset they require, with visibility across the journey from collection to final settlement.

Fiat to stablecoin

End-to-end payment journey

CUSTOMER PAYS IN EUR

SUPPLIER IS PAID IN USDC

01	02	03	04	05
Receive	**Check and control**	**Hold or convert**	**Payout**	**Reconcile**
€250,000 collected by SEPA	Payer verified and screened	Converted EUR to USDC	USDC sent to a supplier's verified wallet	Matched to the invoice

Visibility across the journey, from collection to final settlement

THROUGHOUT 01 Licensing · 02 Compliance · 03 Security

Stablecoin to fiat

End-to-end payment journey

CUSTOMER PAYS IN USDT

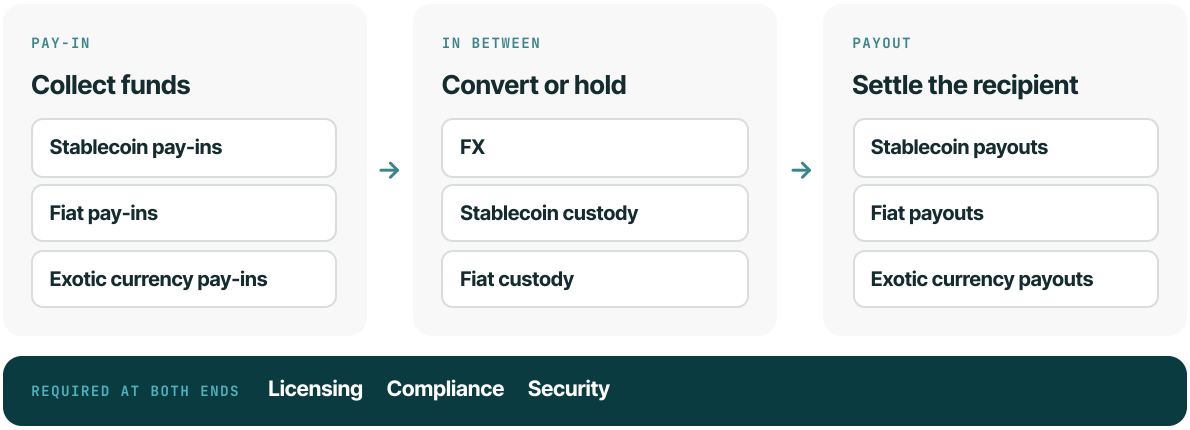
SUPPLIER IS PAID IN BRL

01	02	03	04	05
Receive	**Check and control**	**Hold or convert**	**Payout**	**Reconcile**
250,000 USDT received from a customer wallet	Wallet screened, Travel Rule data exchanged	Converted USDT to BRL	BRL paid by Pix to a supplier in Brazil	Matched to the invoice

Visibility across the journey, from collection to final settlement

Pay-in and payout are distinct parts of that journey. The ability to send stablecoins does not necessarily provide the accounts, payment methods or banking access needed to collect funds. Equally, accepting a stablecoin does not automatically enable a business to convert it, hold it for treasury purposes or settle a recipient in local currency. A functioning payments operation needs the relevant capabilities at both ends, supported by appropriate licensing, compliance, liquidity and controls.

What a payment needs, from collection to payout



Managing a business's own treasury is different from collecting customer payments, paying third parties or distributing funds on behalf of a platform's users. Each involves different participants, responsibilities and operational requirements.

PAYMENT FLOW EXAMPLES

Managing a business's own treasury



FOR EXAMPLE

A corporate holding USDC alongside EUR and moving between them

Collecting customer payments



FOR EXAMPLE

A CFD broker accepting client deposits in USDT or local currency

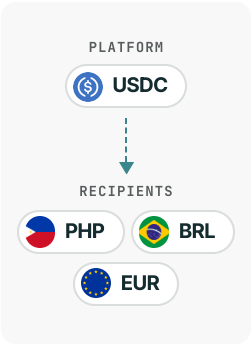
Paying third parties



FOR EXAMPLE

An importer paying suppliers in local currency abroad

Distributing funds on behalf of a platform's users



FOR EXAMPLE

A remittance firm paying out to recipients across corridors

The starting point should therefore be the payment flow the business wants to deliver, not an individual token, network or technology provider.

That does not mean building every capability before the first payment. Businesses can begin with a focused, evolve, they should be able to introduce relevant currencies, networks, markets and payment flows without rebuilding the entire operating model.

This guide explores what that foundation requires: the complexity behind stablecoin payments, the eight

02

The hidden complexity of the stablecoin stack

Three considerations before you build

IN THIS SECTION

Building beyond the initial requirement p.7

Managing integration and operational complexity p.8

Designing for both collection and settlement p.8

The hidden complexity of the stablecoin stack

The complexity of stablecoin payments lies less in any single component than in making the whole operation work together. Businesses need to connect the technology that moves funds with the permissions, banking relationships, liquidity and controls that make those funds usable.

Building or buying individual capabilities can meet an immediate requirement. The gaps often become visible later: when a business adds a new currency, serves a different customer group or needs to settle recipients through another payment route. Three considerations are particularly important when designing the infrastructure.

The question is not whether the first solution works. It is whether the foundation can accommodate what the business needs next.

Building beyond the initial requirement

A component can perform its intended role well without supporting the complete payment journey. Wallet and custody infrastructure, for example, can enable businesses to hold and move stablecoins. Collections, conversion and settlement may also require banking access, on- and off-ramps, liquidity, compliance controls and payout capabilities.

The same distinction applies to an initial use case. Infrastructure that supports one payment flow may need additional capabilities when the business introduces new counterparties, currencies or markets. A treasury setup for managing a company's own funds, for instance, may not support collecting payments from customers or distributing funds to third parties.

WHAT WALLET INFRASTRUCTURE ALONE DOESN'T COVER

FOR EXAMPLE

Wallet & custody infrastructure

ALSO REQUIRED

- ✓ Banking access
- ✓ On & off-ramps
- ✓ Liquidity
- ✓ Compliance controls
- ✓ Payout capabilities

Managing integration and operational complexity

Using specialist providers is not inherently a weakness. Many payment operations depend on a combination of proprietary technology and external partners. What matters is how those capabilities are connected and who takes responsibility for the overall flow.

Each additional provider can introduce another integration, onboarding process, set of controls and source of transaction data. A payment may complete successfully on-chain while conversion, account reconciliation or final fiat settlement still requires intervention elsewhere.

Without coordinated orchestration and visibility, these dependencies can become a fragmented “Frankenstack”: individually capable services that are difficult to operate as one payment system. As volumes and requirements grow, teams can spend more time managing hand-offs, resolving exceptions and assembling records across systems, increasing the risk of communication errors between systems, technical failures and operational disruption.

Designing for both collection and settlement

Pay-in and payout serve different purposes and need to be assessed separately. A collection flow needs to support how customers or counterparties send funds, how those funds are attributed to the correct party, and how they are screened and reconciled. A payout flow needs to deliver funds to the intended recipient through the appropriate asset, currency and settlement route.

Strength in one does not automatically establish coverage in the other. Broad payout reach, for example, does not necessarily mean a provider can collect local-currency payments in the same markets. Similarly, stablecoin acceptance does not establish whether funds can be held for treasury management or converted and paid out in the recipient’s preferred currency.

Businesses therefore need to map both sides of the transaction and the processes connecting them, against their intended use case. That provides a clearer basis for assessing infrastructure than a list of individual features alone.

03

Start small, think big, scale fast

A strategic principle

IN THIS SECTION

Phase 01 · Start small p.10

Phase 02 · Think big p.11

Phase 03 · Scale fast p.11

Start small, think big, scale fast

Businesses do not need to launch every stablecoin capability at once. A focused starting point can help establish commercial value, test the payment journey and build operational experience. But a narrow initial scope should not mean a narrow infrastructure foundation.

The strategic principle is to separate what the business needs to launch today from what its infrastructure should enable tomorrow.

PHASE 01 · THE LAUNCH

Start small

Define the use case

Begin with a specific payment requirement rather than a broad ambition to "adopt stablecoins". That could mean collecting payments from overseas customers, moving funds between group entities or paying suppliers in a particular corridor.

Define who is paying, who is receiving, which currencies or assets are involved, and what happens to funds between collection and settlement. Establish what success looks like: faster settlement, greater treasury flexibility, less manual processing or better access to a particular payment route.

A controlled launch allows the business to validate both demand and execution. The aim is not simply to demonstrate that funds can move, but to confirm that the complete flow—from onboarding and screening to conversion, reconciliation and settlement—works as intended.

PHASE 02 · THE INFRASTRUCTURE

Think big

Preserve optionality

Starting with one use case should not lock the business into one currency, network or operating model. Infrastructure decisions should account for plausible next steps: additional markets, different recipient types, new collection methods or the ability to hold both fiat and stablecoins for treasury management.

Preserving optionality does not mean supporting every token or blockchain from day one. It means understanding how relevant capabilities can be added, what dependencies they introduce and whether the underlying platform can accommodate them.

Licensing, compliance and security, the regulated core, should form part of that foundation from the outset, alongside the FX and custody arrangements that make funds usable. These are not features to add after volumes grow; they help determine which customers, markets and payment flows the business can support.

PHASE 03 · THE GROWTH

Scale fast

Once the initial use case is established, expansion should build on the existing infrastructure rather than require a separate stack for each new flow. Connected orchestration, controls and transaction records can reduce the need to repeat integrations or create additional manual processes.

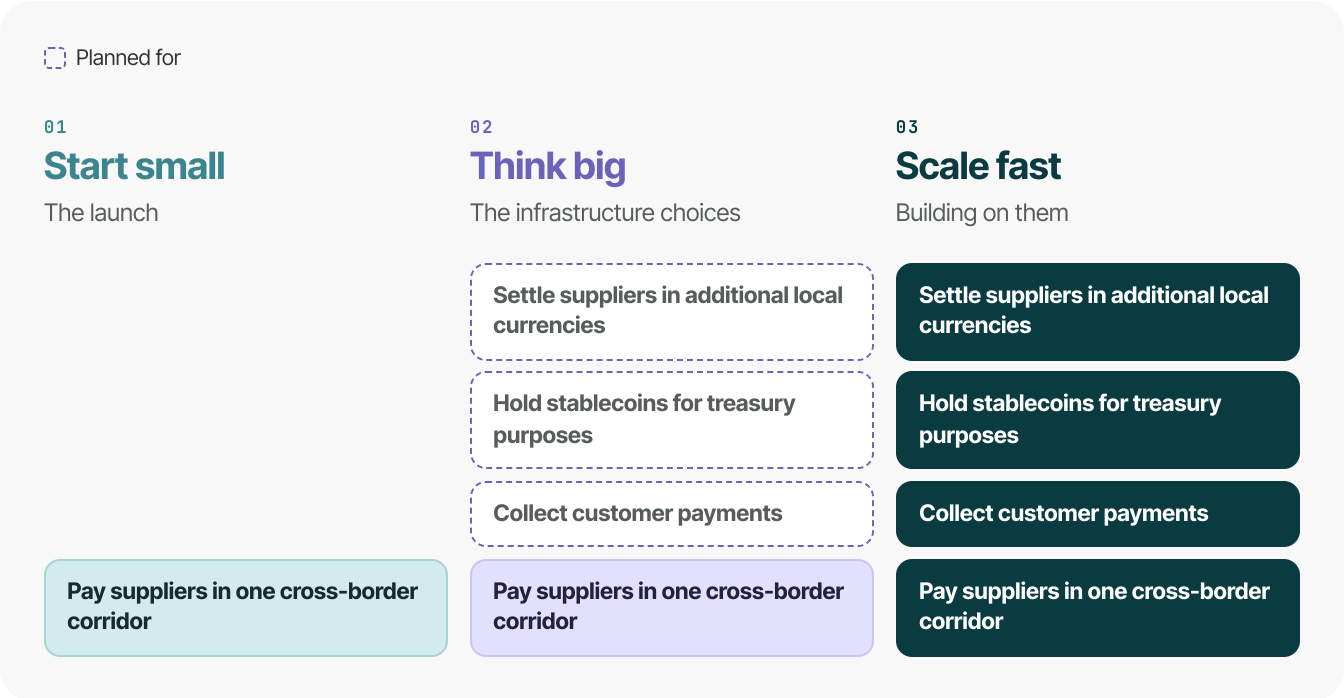
The goal is not to own every component in-house. It is to have a dependable operating model in which responsibilities are clear, specialist capabilities work together and teams retain visibility across the payment journey.

Scaling fast also does not mean bypassing the checks required for a new market, asset or customer group. It means having a foundation that makes those changes easier to assess and implement, without redesigning

THE PROGRESSION AT A GLANCE

Start small	Think big	Scale fast
Identify one commercially valuable payment requirement	Plan for relevant currencies, assets, markets and participant types	Extend the existing integration where capabilities and permissions allow
Launch a controlled, end-to-end use case	Embed the regulated core of licensing, compliance and security, plus FX and custody, in the foundation	Add payment routes and use cases through connected infrastructure
Validate demand, operational performance and business value	Preserve choice as customer needs and the market evolve	Limit vendor sprawl, duplicated processes and manual hand-offs

A business might begin by paying suppliers in one cross-border corridor. Over time, it may also want to collect customer payments, hold stablecoins for treasury purposes or settle suppliers in additional local currencies. The initial launch can remain focused while the infrastructure is selected with those potential requirements in mind.



04

The stablecoin infrastructure stack

Eight capabilities, three tiers

IN THIS SECTION

Overview of the stack p.14

The regulated core: licensing, compliance, security p.16

Money & assets: FX, stablecoin and fiat custody p.19

How you consume it: pay-ins and payouts p.23

Build or partner? p.24

The stablecoin infrastructure stack

Starting small without limiting future growth depends on the infrastructure underneath the initial use case. A stablecoin payment operation needs more than the ability to transfer an asset. It needs a regulated core that makes the payment permissible, money and asset capabilities that make funds usable, and the products through which a business actually collects and pays.

Eight connected capabilities, grouped into those three tiers, provide the framework for assessing that foundation. Each performs a different role, but their value comes from how they work together.

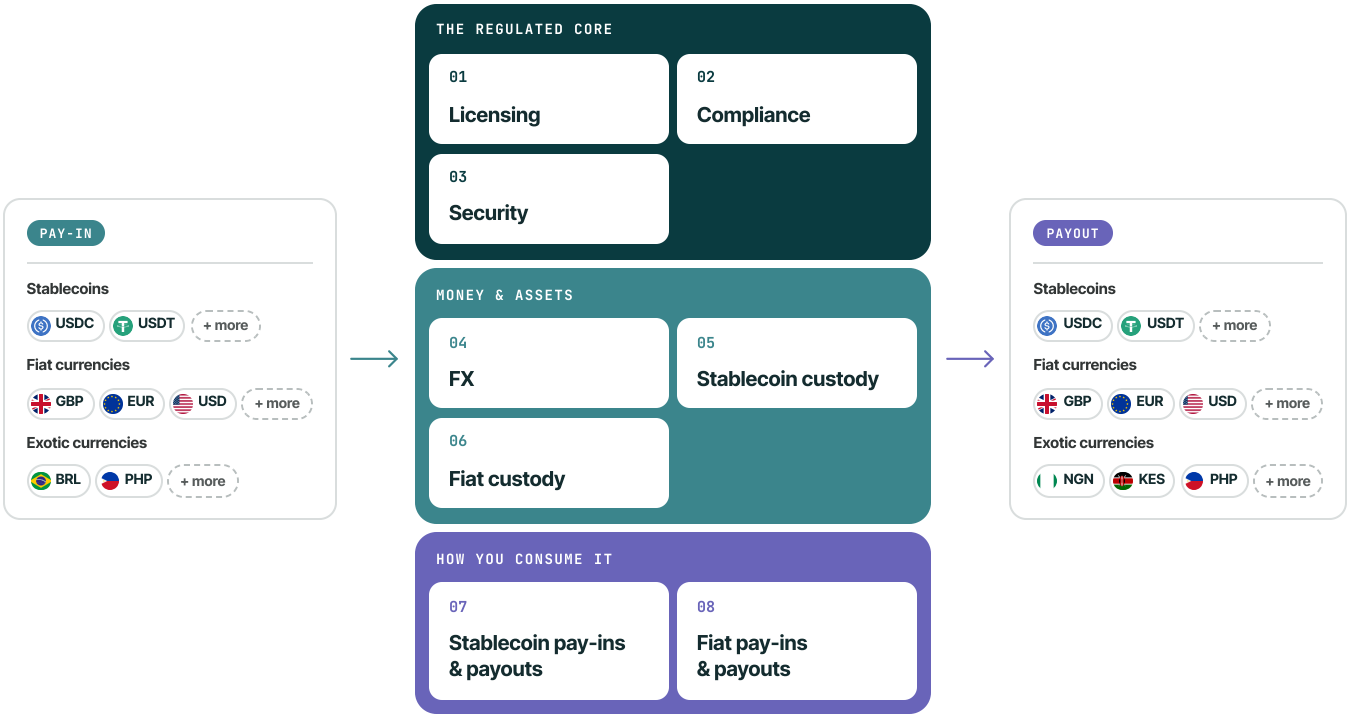
Businesses do not necessarily need to build each capability themselves. They do need to understand which capabilities are available, who is responsible for them and what would be required to extend them.

> **Orchestration connects these capabilities into one operating flow, coordinating routing, controls, transaction status and reconciliation across collection, conversion, custody and payout.**

THE INFRASTRUCTURE BEHIND MAKING REAL-TIME STABLECOIN PAYMENTS

Access to a token or custody service does not, on its own, create a complete payments solution.

A complete payment proposition draws on eight connected capabilities. Which are used—and how they connect—depends on how funds are received, held, converted and paid out.



TIER 1

The regulated core: licensing, compliance and security

The first three capabilities determine whether a payment flow can be offered at all, and to whom. Everything else in the stack depends on them.

01

THE REGULATED CORE

Licensing

Licensing establishes the regulatory permissions for the intended payment activities across the relevant jurisdictions. A stablecoin payment typically has two legs, a fiat leg and a crypto leg, and each usually requires its own authorisation. The requirements depend on the services offered, the participants involved and how funds are received, held and paid out.

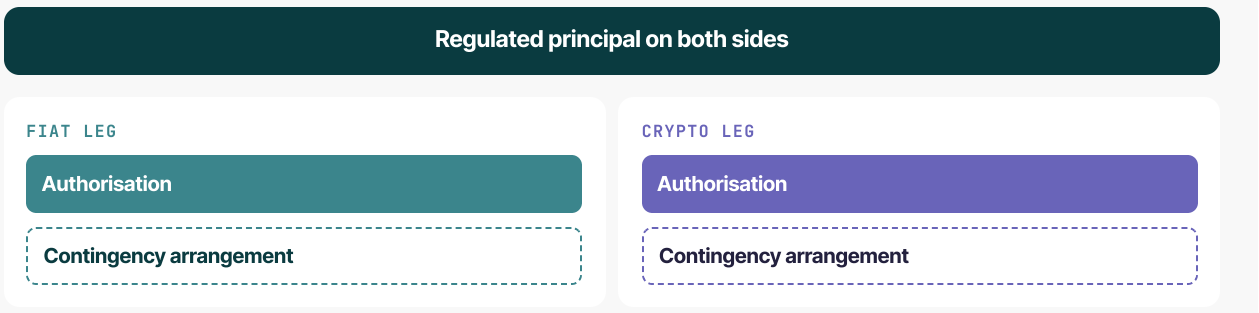
The important question is who acts as the regulated principal for each activity. Businesses should understand which entity is responsible for receiving, converting, holding and paying out funds, and how those responsibilities are coordinated across the payment journey. They should also assess the contingency arrangements that support continuity if a regulatory permission, banking relationship or payment route changes.

Regulatory permission alone does not make a payment flow operational. It must connect with the banking relationships, accounts, controls and payment rails needed to deliver the service in practice. A business should assess whether a provider's infrastructure supports its specific payment flows in the jurisdictions and currencies it operates, rather than simply whether the provider holds a licence in a particular jurisdiction.

BUILD CONSIDERATION

Obtaining and operationalising permissions involves regulatory applications, governance, capital, compliance resources and supporting partnerships. Timing and cost vary by jurisdiction and activity; pending approvals should not be treated as available capability.

WHO'S RESPONSIBLE AT EACH STEP



02

THE REGULATED CORE

Compliance

Compliance covers customer onboarding, KYC/KYB, sanctions and jurisdiction screening, KYT on deposits and payouts, AML monitoring, and Travel Rule information exchange with counterparties. Records support oversight and auditability.

Accountability is the key consideration. A provider acting as the compliance-accountable party screens every payment under its own framework, while the client remains responsible for meeting its own applicable obligations. As volumes and customer models develop, these controls need to scale without becoming a growing burden of manual reviews, and businesses should be able to reflect their particular customers and payment flows within the provider's framework.

Beyond a provider's underlying compliance controls, client-configurable monitoring rules can give businesses greater oversight. Orbital Assure is one example of this approach, allowing clients to establish additional rules within the Orbital portal, on top of Orbital's existing controls, while retaining the platform's underlying safeguards.

Without integrated compliance, controls can become inconsistent across providers, and teams may struggle to reconstruct decisions or investigate activity.

BUILD CONSIDERATION

Screening tools are only one input. Building the operating capability also requires rule configuration, testing, case management, record keeping and people to manage alerts and exceptions.

EVERY PAYMENT, SCREENED

- A **Onboarding, KYC/KYB**
- B **Sanctions & jurisdiction screening**
- C **KYT on deposits and payouts**
- D **AML monitoring**
- E **Travel Rule exchange**
- F **Records for oversight**

ORBITAL ASSURE

Your own rules, set in the Orbital portal

03

THE REGULATED CORE

Security

Security protects access to systems, keys and funds. It spans custody technology and key management, user permissions and approval policies, and the control frameworks that demonstrate those protections work.

Businesses should look for independent evidence rather than assurances: audited controls such as SOC 2 Type 2 and ISO 27001, alignment with frameworks such as DORA and the NIST Cybersecurity Framework, and external security ratings. For regulated clients, a provider's security posture also feeds into their own outsourcing and operational resilience obligations.

BUILD CONSIDERATION

Security is a continuous programme rather than a one-off purchase. It requires penetration testing, audits and certifications, access reviews, incident response and the people to run them.

CERTIFICATIONS & FRAMEWORKS

SOC 2 Type 2
AUDITED CONTROLS

ISO 27001
AUDITED CONTROLS

DORA
FRAMEWORK ALIGNMENT

NIST CSF
FRAMEWORK ALIGNMENT

TIER 2

Money and assets: FX, stablecoin custody and fiat custody

The next three capabilities determine what a business can do with funds once they arrive: convert them, hold them and keep them safe.

04

MONEY & ASSETS

FX

FX connects stablecoins to the currencies businesses and their recipients actually use. It covers conversion between fiat currencies and between fiat and stablecoins, along with access to the liquidity needed to execute at size.

Execution quality matters as much as currency coverage. Businesses should understand whether the provider acts as principal or routes to third parties, whether quotes are live and executable or only indicative, how slippage is handled and how quickly converted funds settle. This is particularly important for exotic currencies, where market depth and settlement cycles vary widely. An OTC desk can matter for larger tickets and out-of-hours flows.

Receipt does not always need to trigger immediate conversion. A business may want to retain stablecoins for future payments, manage liquidity across assets or convert funds according to its treasury requirements.

Without reliable FX, a business may be able to receive stablecoins but lack a practical way to settle recipients in the currency they need, at a predictable price.

BUILD CONSIDERATION

Establishing this capability requires liquidity relationships with market makers, a dealing function, pricing and risk controls, and settlement processes, not simply access to an exchange rate.

WHAT TO CHECK WHEN CHOOSING A CONVERSION PROVIDER

Check	LOOK FOR	VERSUS
Execution	**Principal**	Routed
Quotes	**Executable**	Indicative
Slippage	**Defined**	Unclear
Settlement	**Fast**	Variable

ON RECEIPT

05

MONEY & ASSETS

Stablecoin custody

Stablecoin custody supports secure asset holding, wallet management, access permissions, fund segregation and on-chain settlement across the networks and tokens a business uses.

The custody model determines where assets sit, who can authorise their movement and how client assets are treated. Businesses should establish who is the custodian of record, whether assets are held in named vaults segregated per client, and which regulatory authorisation the custody arrangement relies on. They should assess those arrangements alongside the technology, such as MPC, used to secure keys and transactions.

Network and token coverage sits here too. More chains are not automatically better: each additional asset or network can introduce liquidity, compliance, technical and reconciliation requirements. The aim is to support the routes that matter today while retaining a practical path to add others, and to understand any dependencies on particular issuers and redemption arrangements.

Without appropriate arrangements, businesses may lack the permissions, segregation or operational visibility needed to manage digital assets securely.

BUILD CONSIDERATION

The work includes configuring wallet structures and approval policies, managing access, establishing recovery procedures, integrating and maintaining each network, and connecting balances to internal records. Buying wallet technology does not remove the need to design those processes.

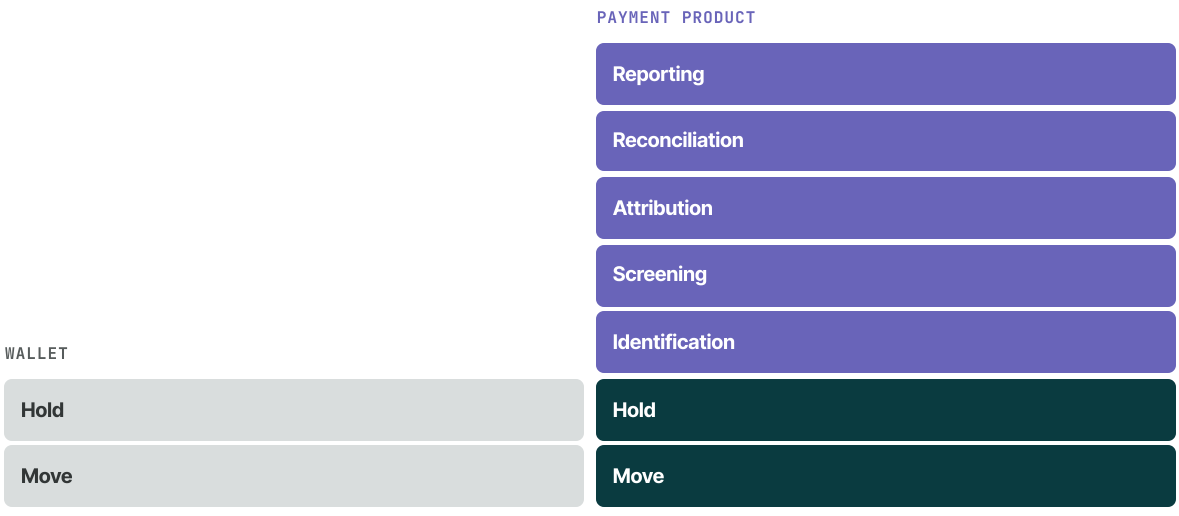
Where do wallets fit?

Wallets enable businesses to receive and move digital assets and, depending on the custody model, manage access to holdings. In a B2B payment operation, they sit underneath the products businesses actually use, and connect with compliance, FX, fiat custody and fiat settlement.

The right setup depends on the use case. A corporate treasury wallet serves a different purpose from dedicated wallets used to identify customer receipts or support platform payouts.

Businesses should ask who needs to control funds, which assets and networks are required, how receipts are attributed, and how funds will be held, converted or distributed. The objective is not a wallet that does everything, but a payment product built on wallet infrastructure that fits a controlled, end-to-end payment journey.

A WALLET VERSUS A PRODUCT



Each transaction arrives in the business's records ready to use.

CONNECTED TO Compliance FX Fiat custody Fiat settlement

06

MONEY & ASSETS

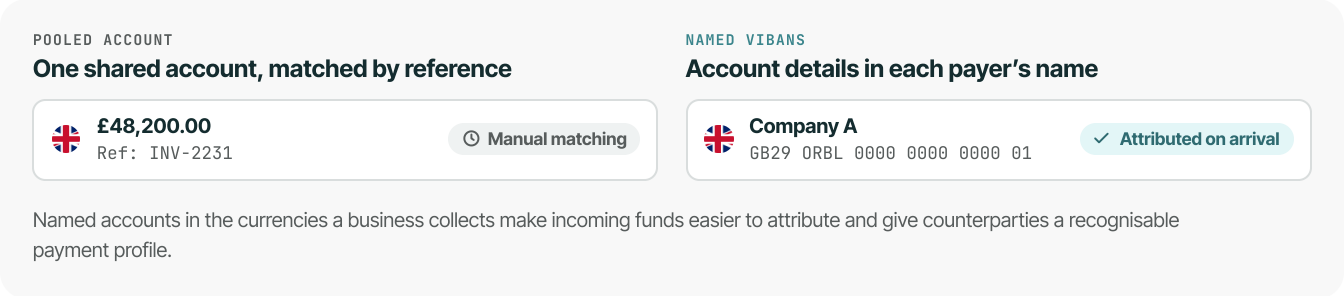
Fiat custody

Fiat custody covers how client money is held: the accounts that receive and store fiat balances, how those funds are safeguarded and which banks sit behind them.

Businesses should establish whether funds are safeguarded under an e-money or payment licence, whether client money is ever pooled with the provider's own funds, and whether balances are spread across multiple banks to avoid a single point of failure. Account structure matters operationally too. First-name IBANs or vIBANs in the currencies a business collects make incoming funds easier to attribute and give counterparties a recognisable payment profile.

Holding fiat and stablecoin balances side by side gives treasury teams the flexibility to decide when to convert or pay out, rather than having every receipt trigger an immediate transaction.

Without robust fiat custody, the safety of client money can depend on a single banking relationship, and incoming funds can be difficult to identify and reconcile.



Named accounts in the currencies a business collects make incoming funds easier to attribute and give counterparties a recognisable payment profile.

BUILD CONSIDERATION

Establishing this capability requires safeguarding arrangements, banking onboarding across multiple institutions, account structures for each currency and the reconciliation processes behind them.

How you consume it: stablecoin and fiat pay-ins and payouts

The final two capabilities are where the stack meets the business: the products through which customers and counterparties pay in, and through which recipients are paid.

Businesses may access them through an API, a web platform or assisted execution through an OTC desk, depending on their teams and requirements. Engineering teams may need programmable workflows, while treasury teams need visibility and execution tools that do not require development work.

- **API integration** — Embed payments into your systems
- **Web platform** — Manage payments without integration
- **CSV uploads** — Initiate multiple payouts in one upload
- **OTC desk** — Tailored FX for complex transactions

HOW YOU CONSUME IT

07 Stablecoin pay-ins and payouts

Stablecoin pay-ins and payouts turn wallet infrastructure into a usable payment product. On the collection side, that means giving customers simple ways to pay, such as payment links, embedded payment pages or dedicated receiving addresses, with each receipt attributed to the right customer or invoice and reconciled automatically. On the payout side, it means paying many recipients at once, in the stablecoins and on the networks they use.

The difference between a product and a wallet matters. A wallet can hold and move assets. A payment product also handles identification, screening, attribution, reconciliation and reporting, so each transaction arrives in the business's records ready to use.

Without this capability, teams may need to match on-chain transactions to customers manually, manage transfers between providers and resolve exceptions by hand.

BUILD CONSIDERATION

Developing this capability involves more than connecting to a blockchain. It requires address management, payment link and page infrastructure, bulk payout tooling, transaction-status tracking, reconciliation and exception handling, all maintained as networks change.

HOW BUSINESSES ACCEPT AND PAYOUT STABLECOINS

PAY-INS

Accept stablecoins

- **Receive by link** — Share a payment link; the customer pays from any wallet
- **Embedded payment pages** — A hosted checkout inside your own site or app
- **Binance Pay** — Customers pay directly from their Binance account
- **Dedicated customer wallets** — A unique deposit address per customer, reconciled automatically
- **Shopping cart plugins** — Add stablecoin checkout to an existing e-commerce store

PAYOUTS

Payout stablecoins

- **Web platform** — Send single payments manually from the dashboard
- **Mass payouts** — Pay many recipients at once from a CSV file
- **API** — Trigger payouts directly from your own systems
- **Binance Pay** — Pay recipients straight to their Binance account
- **OTC desk** — Tailored exchange requests for large or bespoke payouts

08

HOW YOU CONSUME IT

Fiat pay-ins and payouts

Fiat pay-ins and payouts connect the stablecoin flow to the banking system: collecting local currency from customers and settling recipients through the rails they use, such as SWIFT, SEPA, TARGET2, Fedwire, Faster Payments, CHAPS and BACS.

Direct rail access can shorten settlement times and reduce the number of intermediaries that can delay or reject a payment. Businesses should also check how same-currency pay-ins are matched, which statement and reporting formats are available, what cut-offs and limits apply, and whether on- and off-ramping between fiat and stablecoins can run through local accounts.

Coverage should be assessed against the actual payment journey. Broad payout reach does not necessarily mean a provider can collect local-currency payments in the same markets.

Without this capability, a business may move stablecoins efficiently yet still depend on slow or fragmented banking arrangements at either end of the flow.

BUILD CONSIDERATION

Establishing direct rail access requires banking partnerships, scheme or sponsored access, payment operations, and processes for returns, recalls and investigations.

PAYMENT RAILS

Cross-border

SWIFT

Regional

SEPA TARGET2

Local

Faster Payments (UK) Fedwire (US) ACH (US) PIX (BR) InstaPay (PH)

Build or partner?

Understanding the build commitment

The cost of assembling these eight capabilities is not just the initial technology spend.

It includes regulatory work, partner onboarding, specialist staff, integrations, security assurance and the ongoing effort of operating the payment service.

A meaningful build-versus-partner assessment should therefore compare both launch requirements and continuing responsibilities: what must be developed, which permissions and relationships are needed, who will operate the controls, and how much work each new use case introduces.

What building it yourself involves

CAPABILITY	RESPONSIBILITIES TO BUILD AND RUN
THE REGULATED CORE	
01 Licensing	Regulatory applications · Governance · Capital · Compliance resources · Supporting partnerships
02 Compliance	Rule configuration · Testing · Case management · Record keeping · Alert & exception staff
03 Security	Penetration testing · Audits & certifications · Access reviews · Incident response · Security staff
MONEY & ASSETS	
04 FX	Market-maker liquidity · Dealing function · Pricing & risk controls · Settlement processes
05 Stablecoin custody	Wallet structures · Approval policies · Access management · Recovery procedures · Network integrations · Links to internal records
06 Fiat custody	Safeguarding arrangements · Multi-bank onboarding · Per-currency accounts · Reconciliation processes
HOW YOU CONSUME IT	
07 Stablecoin pay-ins & payouts	Address management · Payment links & pages · Bulk payout tooling · Status tracking · Reconciliation · Exception handling
08 Fiat pay-ins & payouts	Banking partnerships · Scheme or sponsored access · Payment operations · Returns, recalls & investigations

The scope of work depends on the payment use case, existing capabilities and operating model.

WITH A PAYMENTS PARTNER

One partner, one integration

Your business

ONE INTEGRATION

ONE PARTNER

- Licensing
- Compliance
- Security
- FX
- Stablecoin custody
- Fiat custody
- Stablecoin pay-ins & payouts
- Fiat pay-ins & payouts

05

How the stablecoin stack shifts across three use cases

How the payment objective translates into infrastructure requirements

IN THIS SECTION

Commodities p.27

Remittance firms p.27

Regulated merchants p.28

How the stablecoin stack shifts across three use cases

The infrastructure required should be determined by the payment use case. A commodity trader settling a large supplier payment has different priorities from a remittance firm processing thousands of transfers or an account-based merchant managing customer deposits and withdrawals.

These examples show how the payment objective translates into infrastructure requirements and why no single component can meet every need.

USE CASE ONE

Commodities

Commodity traders may need to move high-value payments across borders, including to suppliers in markets where access to US dollars is constrained or correspondent banking introduces delays.

THE OBJECTIVE

To settle trades faster, improve payment certainty and reduce the time capital spends in transit.

WHAT IT REQUIRES

Reliable large-ticket liquidity, the ability to settle in the recipient's required currency, and appropriate counterparty due diligence across the jurisdictions involved.

For these large-ticket flows, execution quality, settlement speed and certainty can matter more than transaction throughput. The infrastructure must support the size and timing of the payment, not simply the ability to transfer a stablecoin.

That makes licensing, compliance, FX, fiat payouts and coordinated execution central to the use case. The payment is only complete when the supplier receives usable funds in the agreed asset or currency.

USE CASE TWO

Remittance firms

Remittance firms handle high volumes of lower-value payments across multiple corridors. They want to reduce reliance on pre-funded accounts and move settlement funds outside traditional banking hours.

Stablecoins can support the payout leg, whether funds go directly to a recipient's wallet or to a payout partner that completes delivery locally. Where the recipient needs local currency, however, final delivery still depends on the partner's liquidity, operating hours and payment rails.

The infrastructure therefore needs to sustain payout volumes while giving the remittance firm visibility and control over compliance. Using a provider's screening tools does not remove the firm's responsibility to meet its own applicable obligations.

CONTROLS MIGHT INCLUDE

Payout caps | Holds on first payments | Beneficiary verification

Depending on the payment flow and risk assessment, controls might include payout caps, additional checks or holds on first payments to new beneficiaries, and beneficiary verification before funds are released. These controls need to work alongside the provider's safeguards, with clear records of decisions and exceptions.

USE CASE THREE

Regulated merchants

One relevant merchant use case is regulated, account-based businesses whose customers fund a balance and later withdraw from it. These businesses may want to offer stablecoin deposits and withdrawals while retaining control over customer identity, sources of funds and payment risk.

The infrastructure needs to connect the verified customer with the funding source and intended withdrawal destination. Depending on the sector and jurisdiction, this may include a closed-loop approach, with withdrawals returned to the original verified payment method, alongside documented reasons for holds, rejections and releases. For example, the UK Gambling Commission strongly recommends closed-loop payment systems for gambling operators.



Stablecoin payments add an identity challenge: a wallet address alone does not establish who controls it. Merchants therefore need processes that link relevant wallets to customers, screen payment activity and apply controls to both deposits and withdrawals.

Underneath those controls, the payment operation also needs stablecoin and fiat custody, FX, and pay-in and payout products that support the right tokens and networks. Coordinating these capabilities through one provider can simplify the operating model, but the essential requirement is a clear, auditable connection between the customer, the funds and the payment decision.

Capability by use case

CAPABILITY	Commodities	Remittance firms	Regulated merchants
01 **Licensing**	**A regulated principal on both legs of trade settlement, across the jurisdictions involved**	Permissions covering fiat-to-stablecoin conversion and cross-border payouts, with redundancy on each leg	A regulated provider acting as principal for customer deposits and withdrawals
02 **Compliance**	**Risk-based enhanced due diligence on counterparties, sanctions screening and wallet checks for high-value flows**	Provider screening on each payout, alongside the firm's own rules for payout caps, new beneficiaries, transaction velocity and prohibited corridors, with Travel Rule data exchanged	Provider screening alongside the merchant's own deposit and withdrawal rules, verification that funds come from the customer, Travel Rule support and recorded reasons for holds, rejections and releases
03 **Security**	Approval policies and audited key management suited to large-ticket transactions	Access controls and audited security for high-frequency outbound flows	Independently audited controls that support the merchant's own regulatory and outsourcing obligations
04 **FX**	**Principal liquidity and live, executable quotes for large conversions, with OTC execution and fast settlement in exotic currencies**	Fiat-to-stablecoin conversion that can reduce reliance on pre-funded accounts, with round-the-clock settlement	Control over when customer funds are converted, at live, executable rates
05 **Stablecoin custody**	Segregated vaults and approval controls, with a choice of issuer and network for settlement certainty	Wallet structures for high-frequency outbound flows, on the networks recipients and payout partners use	Segregated client holdings across the approved tokens and chains customers use
06 **Fiat custody**	First-name IBANs or vIBANs for collections where required, with safeguarded balances	Safeguarded corridor funding balances held across multiple banks	Safeguarded fiat balances held alongside stablecoins for treasury management
07 **Stablecoin pay-ins & payouts**	Direct stablecoin settlement to suppliers' wallets, reconciled to each trade	Mass payouts to recipients' wallets and payout partners, across corridors and chains	Dedicated, auto-reconciled deposit addresses per customer, with withdrawals directed to verified destinations

06

Define the use case. Build for what comes next.

IN THIS SECTION

Define the journey p.30

Assess end to end p.30

Look beyond launch p.30

1

DEFINE THE JOURNEY

A stablecoin strategy should begin with a business objective - not a token, blockchain or custody product. Whether the priority is collecting international payments, managing treasury, paying suppliers or distributing funds through a platform, the first task is to define the payment journey and the outcome it needs to deliver.

2

ASSESS END TO END

From there, assess the infrastructure required to make that journey work end to end. How will funds enter? Who needs to be verified? Will balances be held in fiat, stablecoins or both? How will funds be converted, controlled and reconciled? What does the recipient need to receive?

The questions that shape your stack

01 **How will funds enter?**

02 **Who needs to be verified?**

03 **Will balances be held in fiat, stablecoins or both?**

04 **How will funds be converted, controlled and reconciled?**

05 **What does the recipient need to receive?**

3

LOOK BEYOND LAUNCH

Then look beyond the initial launch. A solution that works for one corridor or payment flow should provide a foundation for relevant expansion, not become a constraint when the business adds customers, currencies, markets or use cases. The aim is not to build every capability at once, but to make infrastructure decisions that preserve choice.

Start small
with a clearly defined use case.

Think big
about the capabilities you may need next.

Scale fast
by building on infrastructure designed to support that progression.

Stablecoins are ready for business payments but only if the infrastructure is.

→ WHAT'S NEXT

What's your stablecoin strategy?

Whether you are exploring your first use case or expanding an existing payment operation, start with a clear view of what your business needs today and what it may need tomorrow.

Orbital brings fiat and stablecoin payments together in one infrastructure platform, combining a regulated core of licensing, compliance and security with FX, stablecoin and fiat custody, and pay-in and payout products for both. Supporting more than $12 billion in annual payment volume, with regulatory permissions across multiple jurisdictions, Orbital helps businesses manage complex international payments without building separate fiat and stablecoin infrastructure.

Map out your stablecoin payment strategy

Request a Call with a Specialist →

Orbital.

The Stablecoin Guide

Orbital.

media@getorbital.com www.getorbital.com

Disclaimer

This guide is produced by Pay Perform Technologies Ltd and is meant for general informational purposes only. No representations or warranties are made as to the accuracy, reliability, completeness, or timeliness of the data or content provided.

Information about Orbital provided herein is intended to inform eligible corporate customers about Orbital's services and does not constitute financial or investment advice. The availability of particular Orbital's services is subject to jurisdictional and regulatory limitations, compliance approval and signing of definitive service agreement. Orbital does not recommend buying or selling any particular digital assets and makes no representation on the suitability or reliability of any such asset. Cryptocurrencies are highly volatile and carry significant risks, including potential total loss. Stablecoins carry risks related to issuer solvency, reserve adequacy, and evolving regulatory frameworks.

Orbital is the trading name representing the Pay Perform group of traditional financial and digital asset service providers. Regulatory status of Orbital's services differs per jurisdiction, and you may not be protected by government or regulatory protection schemes. Please see Legal Disclosures for more information.