Build a digital wallet or neobank

A consumer or business wallet architecture covering accounts, ledger, cards, payments, identity, fraud and notifications.

LAYER 1 / REQUIRED

Accounts and regulated partner

Provide account infrastructure and customer-funds model.

- ☐ Jurisdiction
- ☐ Account ownership
- ☐ Safeguarding or deposit protection

ClearBank — UK and EU banking infrastructure
Swan — European embedded banking
Unit — US account infrastructure
Solaris — European banking infrastructure
Increase — API-based US accounts and payment-rail access

LAYER 2 / REQUIRED

Ledger and core

Maintain balances, holds, fees and product rules.

- ☐ Real-time ledger
- ☐ Availability and auditability
- ☐ Migration and export

Thought Machine — Core and ledger
10x Banking — Cloud core
Episode Six — Ledger and wallets
Tuum — Core banking
Pismo — Cloud core, ledger and financial-product operations

LAYER 3 / REQUIRED

Cards and wallets

Issue cards and support mobile-wallet provisioning.

- ☐ Issuer and processor roles
- ☐ Tokenisation
- ☐ Card controls and disputes

Marqeta — Card issuing
Enfuce — Issuing and processing
Thredd — Issuer processing
MeaWallet — Tokenisation and wallet enablement
Lithic — Programmable cards and mobile-wallet provisioning

LAYER 4 / REQUIRED

Payments and FX

Support transfers, direct debits, local rails and currency conversion.

- ☐ Required rails
- ☐ FX model
- ☐ Returns and reconciliation

Modulr — Payments and accounts
Currencycloud — Cross-border and FX
Wise Platform — International transfers
Form3 — Payment connectivity

LAYER 5 / REQUIRED

Identity, fraud and AML

Onboard customers and manage lifecycle risk.

- ☐ Identity assurance
- ☐ Account takeover controls
- ☐ Monitoring and cases

Veriff — Identity verification
Sumsub — KYC and AML
Sardine — Fraud and AML
ComplyAdvantage — Screening and monitoring

Questions to ask providers

- ☐ Which legal entity contracts for each service and in which jurisdictions?
- ☐ Which responsibilities remain with the product operator rather than the provider?
- ☐ What are the implementation, approval, testing and migration timelines?
- ☐ How are incidents, exits, data portability and business continuity handled?
- ☐ Which capabilities are supplied by the regulated partner and which are operated by the product team?