**Kiến trúc & nguyên tắc vận hành**

Hệ thống xử lý theo mô hình “xếp hàng rồi mới làm”: mọi việc nặng như tạo đơn, giữ hàng, trừ/hoàn tiền đều đưa vào hàng đợi (queue) và có tiến trình nền (worker) lấy ra xử lý. Những chỗ cần chính xác tuyệt đối (cùng một sản phẩm, cùng một ví) chạy theo FIFO – vào trước, làm trước – để tránh đua tranh dữ liệu. Mọi thao tác tiền/tồn kho đều ghi dấu vết (audit) và bút toán bất biến để đối soát; các yêu cầu tạo mới mang idempotency key để lỡ lỗi mạng hay bấm lại cũng không bị ghi trùng. Tiền của đơn được giữ theo cơ chế escrow 3 ngày: người mua trả là dùng được ngay, nhưng chỉ khi hết 3 ngày không có khiếu nại (hoặc người mua xác nhận đã dùng) thì tiền mới về ví người bán.

**Tài khoản, định danh & quyền**

Người dùng có thể đăng ký (email/số điện thoại + mật khẩu) và đăng nhập (mật khẩu hoặc Google SSO), quên mật khẩu thì nhận link đặt lại. Người dùng được sửa thông tin cá nhân (tên, avatar, email/điện thoại – sửa thì phải xác thực lại; địa chỉ; số tài khoản và ngân hàng). Muốn trở thành người bán (Seller) bắt buộc phải KYC; chỉ khi KYC được duyệt mới được mở shop và đăng sản phẩm. Quyền được kiểm soát theo nguyên tắc “ít quyền đủ dùng”: Admin không được xem nội dung sản phẩm nhạy cảm (file/key/link), chỉ thấy siêu dữ liệu phục vụ quản trị.

**Luồng mua hàng 2 bước theo FIFO**

Khi người mua bấm “Mua ngay”, hệ thống soi nhanh: còn hàng không, ví còn đủ tiền không. Nếu đạt, tạo đơn ở trạng thái “đã tiếp nhận”, trả ngay thông báo kèm đường link “TẠI ĐÂY” để theo dõi, đồng thời đẩy đơn vào hàng đợi xử lý. Worker lấy đơn đầu hàng ra, kiểm tra lại tồn kho và số dư ngay tại thời điểm xử lý, giữ/khóa tạm số lượng, rồi gửi lệnh trừ tiền sang hàng đợi riêng của ví (cũng FIFO). Worker ví trừ tiền xong báo về; lúc đó đơn mới được xác nhận, mở quyền tải/hiển thị key và bắt đầu đếm escrow 3 ngày. Nếu ở bất kỳ khâu nào hết hàng hoặc trừ tiền thất bại, hệ thống nhả hàng và đánh dấu đơn thất bại; mọi thứ đều chống lặp nên không trừ hai lần.

**Escrow 3 ngày & khiếu nại**

Khi đơn đã xác nhận, hệ thống giữ tiền 3 ngày. Nếu yên ổn, hết thời gian hệ thống tự chuyển tiền cho người bán (đã trừ phí sàn); nếu người mua bấm “Đã sử dụng ok” có thể tất toán sớm. Nếu có khiếu nại, người mua mở chat gắn đúng mã đơn; escrow tạm dừng. Admin xem trao đổi và bằng chứng; nếu hợp lệ thì hoàn tiền về ví người mua và không chuyển cho người bán; nếu không hợp lệ thì đóng khiếu nại và tiếp tục đếm đến khi tự chuyển tiền.

**Nạp tiền qua VietQR (QR sống 5 phút + bấm “ĐÃ CHUYỂN KHOẢN”)**

Mỗi yêu cầu nạp sinh một mã VietQR riêng, chỉ có hiệu lực 5 phút và hiển thị đồng hồ đếm ngược cùng cảnh báo “hết giờ là không còn tác dụng”. Người dùng quét VietQR trong app ngân hàng, kiểm tra sẵn số tài khoản nhận, số tiền, nội dung chuyển tiền (mã nhận diện), không tự sửa; chuyển xong quay lại bấm “ĐÃ CHUYỂN KHOẢN” để hệ thống bắt đầu đối soát. Hệ thống tự quét 2 lần: lần 1 ngay lập tức, lần 2 sau 5 phút để bắt giao dịch tới trễ; khớp là cộng ví ngay, không khớp thì chuyển sang chờ kiểm tra tay. Trường hợp server lỗi hoặc cần tra soát, người dùng gửi mã giao dịch/biên lai cho Admin để “Recheck” thủ công. Một giao dịch chỉ được cộng một lần; mọi dữ liệu đối soát có nhật ký để truy vết. (Một số ngân hàng có trả kèm tên/STK người nạp; hệ thống chỉ dùng để đối chiếu, không tự động hoàn ra đó nếu người dùng không yêu cầu và KYC không khớp.)

**Rút tiền T+1 ngày, duyệt thủ công có bộ lý do từ chối**

Người dùng gửi yêu cầu rút kèm số tiền, lý do, số tài khoản và tên ngân hàng (lấy từ hồ sơ). Hệ thống kiểm tra KYC, số dư và định dạng trước; nếu ổn thì chuyển sang chờ duyệt. Admin xem chi tiết, nếu phát hiện lỗi có thể tick nhiều lý do (sai số tài khoản, sai tên ngân hàng, tên chủ tài khoản không khớp KYC, số dư không đủ, vượt hạn mức/khả nghi…) rồi từ chối và trả về cho người dùng biết rõ sai chỗ nào để sửa. Nếu hợp lệ, Admin chuyển tiền thủ công trong 1 ngày làm việc và bấm “Hoàn thành”, lúc đó ví người dùng mới bị trừ và trạng thái sang “đã chi”. Cách làm này đảm bảo sổ cái trong hệ thống khớp thực tế ngân hàng.

**Chat & thông báo**

Mỗi trang sản phẩm có nút “Chat với người bán” để hỏi đáp. Nếu có sự cố sau mua, người dùng chat với Admin (cuộc hội thoại gắn mã đơn để truy nhanh). Admin có màn gửi thông báo hàng loạt (bảo trì, cảnh báo, chính sách); nhật ký gửi/nhận giúp kiểm soát việc truyền thông.

**Quản trị & màn hình Admin**

Admin có các màn chính: Dashboard (tổng quan số liệu, cảnh báo), KYC Review (duyệt/từ chối, ẩn bớt thông tin nhạy cảm), Deposits (tra cứu, recheck), Withdrawals (duyệt, hoàn thành, hoặc từ chối với danh sách lý do chuẩn), Complaints/Disputes (xử lý khiếu nại, hoàn tiền khi cần), Broadcast (gửi thông báo), Users & Shops (khóa/mở, gắn cờ), Configuration (thiết lập escrow, số lần/khoảng quét, phí sàn, hạn mức). Tất cả đều theo nguyên tắc “ít quyền đủ dùng”; Admin không được xem nội dung sản phẩm để tránh rủi ro thất thoát.

**Tính đúng–đủ–an toàn dữ liệu**

Giữ hàng/giảm kho dùng cập nhật nguyên tử để không bán vượt tồn; bút toán ví chỉ thêm không sửa để đối soát. Có hàng đợi lỗi (DLQ) và cơ chế thử lại có giãn cách để không làm hệ thống quá tải. Hàng đợi được phân vùng theo sản phẩm và ví để nơi nào cần FIFO thì đảm bảo FIFO nhưng tổng thể vẫn mở rộng tốt. Thời lượng escrow, số lần/khoảng quét, phí/hạn mức đều cấu hình được, thay đổi áp dụng ngay. Các lỗi thường gặp (rút hơn số dư, thiếu thông tin ngân hàng, định dạng sai…) đều được báo rõ ràng để người dùng tự sửa.