

The Chargeback-Safe Architecture for Crypto Payments

A PayWicket position paper · August 2026

Executive summary

Card-payment businesses rarely fail for lack of demand — they fail on **chargebacks**. The moment a company becomes the *merchant of record* on a card network and cannot control chargeback exposure, it is one fraud wave away from a frozen account and a six-figure clawback. It is well known in the payments industry that otherwise-healthy businesses running as the merchant of record on mainstream processors have been shut down while carrying six-figure chargeback balances.

PayWicket is architected specifically so that **it is never in that seat**. We separate the risky, reversible fiat leg from the final, irreversible crypto leg, and push the reversible leg onto a **licensed, PCI-compliant on-ramp provider** purpose-built to carry it. The result: the buyer gets a familiar card checkout, the seller receives final settlement, and **PayWicket carries neither card-fraud/chargeback liability nor custody of funds**.

The analogy: the rocket booster

Think of every transaction as a launch:

- **Booster stage — the card deposit.** A licensed on-ramp provides the heavy, risky thrust of moving fiat: card verification, KYC, PCI security, fraud screening, and — critically — **chargeback liability**. This is the most dangerous stage, and it belongs to the licensed provider whose business is built to survive it.
- **Separation event — fiat becomes crypto.** The instant the card deposit converts to a stablecoin (USDC), the booster detaches. The reversible risk stays with the booster. What continues is final, irreversible value.
- **Orbit — crypto settlement.** From here the value moves as crypto: final, non-reversible, self-custodied. The seller is paid in settled USDC that **cannot be clawed back**. PayWicket is the guidance system — routing value, never holding it.

The strategic point: the dangerous stage is deliberately disconnected from the platform.

Why card businesses fail (and why this design doesn't)

Businesses that die on card rails usually share three traits:

1. They are the **merchant of record** — the card network holds *them* liable for every disputed charge.
2. Card payments are **reversible for up to ~180 days**, yet value has already been delivered.
3. When disputes spike, the processor **freezes the account and claws back**.

This architecture removes each failure mode:

Failure mode	Merchant-of-record card model	PayWicket
Card merchant of record	The business	The licensed on-ramp
Who eats a chargeback	The business	The on-ramp (KYC + priced in)
Reversible value delivered	Yes	No — crypto settlement is final
Who holds customer funds	The business / processor	Nobody — non-custodial
Card data stored	Yes (PCI burden)	None — never seen

Risk allocation

Risk	Carried by
Card fraud / chargebacks	Licensed on-ramp
PCI-DSS / card-data breach	Licensed on-ramp
Buyer identity / KYC on the card leg	Licensed on-ramp
Custody of funds	No one — non-custodial; keys stay with the wallet holder
Crypto finality / irreversibility	Buyer & seller — disclosed in Terms
Platform fee (merchant pays)	PayWicket: 0.5% on crypto-wallet payments (on-chain); 5.9% + \$1.50 on card payments, which funds the licensed card provider and KYC

PayWicket's exposure to card chargebacks and cardholder data is, by design, effectively zero.

Security posture

- **No stored card numbers.** There is no cardholder data in our systems to steal; sensitive card and identity data lives in the on-ramp's PCI-DSS Level 1 environment.
- **Non-custodial.** We do not pool or hold customer funds — there is no custodial balance to drain.
- **Hardened platform.** Server-side secrets only, signed webhooks, rate-limited endpoints, MFA-gated administration, and on-chain settlement through an audited router.

The attack surface that sinks most payment startups — stored card data plus a large custodial float — does not exist in this design.

KYC is the seatbelt, not the obstacle

Identity verification on the card leg is exactly the control that prevents buy-then-chargeback fraud. On a licensed on-ramp, that verification is the provider's responsibility, and for transactions $\leq \$1,000$ it is typically just email + card, one time, with no documents. PayWicket caps card funding at **\$1,000 per transaction** to keep buyers in the lightest-friction tier and to bound risk. The verification is the seatbelt that makes the whole model safe.

How we roll it out

- **Today:** payments run through **licensed on-ramp providers**, so PayWicket carries zero card risk, zero chargeback liability, and zero PCI surface, while buyers enjoy a familiar card checkout.
- **Ahead:** a fully embedded, "invisible-crypto" checkout is achievable under appropriate licensing and partnerships, with reserves and modern fraud controls — an evolution, never a shortcut.

Legal & disclosures

Our Terms — on PayWicket and available to merchant sites — clearly disclose that fiat-to-crypto conversion is performed by licensed third parties under their own terms, that cryptocurrency transactions are **final and irreversible**, and that once value converts to crypto the wallet holder bears the risk of their crypto funds. See paywicket.com/terms.

Conclusion

The failure that ends most card businesses is not a risk we manage — it is a risk we have **architected ourselves out of**. By disconnecting the reversible card "booster" and letting only final crypto reach orbit, PayWicket delivers a familiar card experience while carrying none of the exposure that sinks card businesses. It is a glimpse of how the future of money will flow: easy on the surface, final underneath.