RESEARCH SERIES

Stablecoin Based Cards

Technical and Legal Architecture

STABLECOIN-BASED CARDS

Technical and Legal Architecture

MODEL 01 RESEARCH SERIES

SELF-CUSTODY CARD

Technical Architecture and Legal Analysis of Custody Boundary

01 ○ ACTIVE
Self-Custody Card

02
Exchange-Custodial

03
Full-Stack Issuer

04
White-Label / PM

About This Research

Stablecoin-based cards are no longer a concept: they are a functioning product in the market. Monthly crypto card spending, which stood at $100 million in January 2023, reached $1.5 billion by December 2025. On March 3, 2026, Visa expanded stablecoin settlement to more than 100 countries.

This research series examines four technical architectures in a comparative framework. For each model, the technical actors, full transaction flow, AML obligations, revenue economics, and the regulatory framework of seven jurisdictions are analyzed in detail.

Jurisdictions: EU (MiCA), UK (FSMA 2026), US (GENIUS Act), UAE (VARA), Singapore (MAS PSA), Hong Kong (Stablecoins Ordinance), and Turkey (SPK/MASAK).

Methodology and Scope

This research is based exclusively on publicly available primary sources: regulatory documents, official announcements, and company disclosures. No confidential discussions were held with any company. All data has been independently verified where possible; where verification was not possible, uncertainty is explicitly noted.

Out of scope: Specific investment advice, tax advice, individual company evaluations.

Table of Contents

Page numbers correspond to the internal pagination of the M01 content (1–36).

Abbreviations

Abbreviation	Explanation
AML	Anti-Money Laundering
AMLA	Anti-Money Laundering Authority (EU supervisory body, est. 2026)
API	Application Programming Interface
ATM	Automated Teller Machine
BIN	Bank Identification Number: first 6–8 digits of a card number
CASP	Crypto-Asset Service Provider: MiCA-licensed entity
CBUAE	Central Bank of the UAE
CDD	Customer Due Diligence
DAC8	Directive on Administrative Cooperation 8: EU crypto-asset tax reporting directive
EDD	Enhanced Due Diligence
EEA	European Economic Area
EMI	Electronic Money Institution
ERC-4337	Ethereum account abstraction standard (Paymaster-enabled)
EURC	EUR Coin: Circle's Euro-pegged stablecoin
FATF	Financial Action Task Force
FCA	Financial Conduct Authority: UK financial regulator
FX	Foreign Exchange
HKMA	Hong Kong Monetary Authority
ISO 8583	International messaging standard for card transactions
KYC	Know Your Customer
MAS	Monetary Authority of Singapore
MASAK	Financial Crimes Investigation Board: Turkey's AML authority
MiCA	Markets in Crypto-Assets Regulation: EU regulation (2023/1114)
MPC	Multi-Party Computation
OCC	Office of the Comptroller of the Currency: US national bank regulator
PEP	Politically Exposed Person
PM	Program Manager
POS	Point of Sale terminal
PSD2	Payment Services Directive 2: EU payment services directive
PSA	Payment Services Act: Singapore
SAR	Suspicious Activity Report (US)
SCA	Strong Customer Authentication
SPK	Capital Markets Board of Turkey
STR	Suspicious Transaction Report
TCMB	Central Bank of the Republic of Turkey
TFR	Transfer of Funds Regulation: EU Travel Rule
TX	Transaction (blockchain)
USDC	USD Coin: Circle's US Dollar-pegged stablecoin
VARA	Virtual Assets Regulatory Authority: Dubai/UAE crypto regulator

Stablecoin-Based Cards
Model 01: Self-Custody Card

Technical Architecture and Legal Analysis of the Custody Boundary

Current as of March 12, 2026

EXECUTIVE SUMMARY

The self-custody card model covers stablecoin payment architectures in which the private key remains with the user. This research examines three distinct technical architectures: per-swipe on-chain TX (Architecture A), batched settlement (Architecture B), and session key pull (Architecture C) — through the lens of actors, full transaction flow, and legal obligations triggered at each step. The MiCA×PSD2 dual-licensing requirement effective as of March 12, 2026, the EU Travel Rule's threshold-free application, and ESMA's still-unresolved custody interpretation constitute the model's most critical regulatory uncertainties. Jurisdictional analysis covers the EU, UK, UAE, Singapore, Hong Kong, the US, and Turkey. The research identifies material differences across the three architectures in terms of the legal defensibility of the self-custody claim and Travel Rule compliance burden.

Monthly crypto card spending, which stood at $100 million at the start of 2023, reached $1.5 billion by end of 2025: $18 billion annualized, roughly 15x growth, a ~147% compound annual growth rate (January 2023–December 2025). Over the same period, P2P stablecoin transfers grew by only 5%. Cards have become the primary engine of stablecoin adoption. On March 3, 2026, Visa and Stripe's Bridge announced plans to expand stablecoin-backed cards from 18 countries to 100+ countries by end of 2026; the program operates on Solana, Ethereum, Stellar, and Avalanche supporting USDC, EURC, PYUSD, and Paxos Global Dollar. Phantom and MetaMask users can spend across 150 million+ Visa/Mastercard acceptance points.

The most technically complex segment of this growth is the self-custody model. The claim is simple but uncompromising: the private key stays with the user, and assets are not surrendered to an intermediary. Behind this claim lie three fundamentally different technical architectures. In this research, I examine the actors, the full transaction flow from card setup to chargeback, and the legal obligations triggered at each step.

> *Reading Guide: M01: Who should read this: Developers and Web3 product managers seeking to understand the technical architecture; startups evaluating DeFi payment solutions; legal*

> *professionals focused on property rights and custody doctrine. Estimated reading time: 45–60 minutes. Most critical sections: Section 5 (Technical Constraints) and Section 10 (Legal Implications) — to understand why the self-custody model appears optimal yet is simultaneously the most constrained.*

1. The Custody Spectrum

The term "self-custody" is used in the market in vastly different ways. Understanding where a given card actually sits requires examining the full spectrum.

Model	Private Key Control	Example Structure	Self-Custody?
Full Custodial	Fully with the intermediary	Centralized exchange wallet	No
MPC-Based	Yes*	API wallet provider	Partial
Self-Custody Card ★	Yes	Smart contract / session key	Yes*
Full Non-Custodial	Fully with the user	Hardware wallet (no card)	Yes

> ** In the self-custody card model, the co-signer or session key mechanism is what distinguishes it from "fully non-custodial." The user holds the private key, but an additional approval layer is required for transactions. The regulatory significance of this distinction is addressed in Section 7.*

---

2. Actors

Eight distinct actors are involved in a self-custody card transaction. Below is a summary table followed by a detailed description of each actor and how their role differs across architectures.

Actor	Role	Sees Crypto?	License Obligation	KYC/AML
User	Asset owner	Yes; full visibility	None	None (customer)
Wallet / Smart Contract	Asset custody and signing	Yes	Varies by architecture	Indirect

Co-signer / Session Key	Approval layer	Partial	CASP / EMI (contested)	Present
Card Issuer / BIN Sponsor	Card issuance, FX, settlement	Yes; USDC side	EMI or PI license	Primary responsible party
FX Layer	USDC → Fiat conversion	Yes; bridge point	Variable	Present
Card Network	Auth, Clearing, Rules	No; fiat only	Principal Membership	None (indirect policy)
Acquirer Bank	Fiat settlement	No	Banking license	On the merchant side
Merchant / POS	Goods/service provider	No	None	None

User

The private key belongs to the user: meaning the user is the legal owner of the asset. KYC and AML obligations rest with the card issuer; the user is in the position of a customer. Depending on the architecture, the user provides active approval for each transaction (Architecture A), provides no approval at all (Architecture B), or assigns a one-time authorization at setup (Architecture C).

Wallet / Smart Contract Layer

The layer where the user's USDC is held. The wallet architecture determines which chain it operates on, which token types it supports, and how the co-signer/session key policy is enforced. Architecture A uses a smart contract wallet (Safe-style multisig); Architecture B typically uses an MPC-backed wallet; Architecture C uses a smart contract wallet operating via session key authorization.

Co-Signer / Session Key

The fundamental element distinguishing a self-custody card from fully non-custodial. Two implementations:

- Co-signer: In addition to the user's signature, the company's signature is also required. The company does not hold the private key but holds effective veto power: no transaction can proceed without its approval.
- Session key: The user grants the card issuer permission to execute transactions automatically within a defined scope (specific token, specific limit, specific duration). The user can revoke this permission at any time.

> *As of March 12, 2026, ESMA has not clarified whether a co-signer or session key structure qualifies as "custody" under MiCA Art. 3(1)(16). None of the 40+ existing CASP licenses are specifically tailored to the self-custody card model. Companies must be able to defend their legal positions in writing.*

Card Issuer / BIN Sponsor

The institution that issues the card and holds the BIN (Bank Identification Number). EMI or PI license mandatory. Primary legal responsibility for KYC/AML sits here. Sees the USDC side; either handles FX conversion itself or delegates to a separate FX layer. In some programs the card issuer also assumes the program manager role (vertical integration).

FX Layer

The point at which USDC is converted to fiat. The question of who executes this conversion is the least documented aspect of self-custody models:

- Scenario A: The card issuer receives the USDC, converts it to fiat, and forwards it to the acquirer. FX risk sits with the card issuer.
- Scenario B: An independent FX/liquidity provider. The card issuer handles only auth/clearing; conversion is with a separate actor.
- Scenario C: Card network official rate (Visa/Mastercard rate), no markup; the converting actor varies between A and B.

Card Network

Visa or Mastercard. Never sees crypto; operates entirely on fiat. Rule-setter and infrastructure provider. As of March 12, 2026, Visa carries more than 90% of crypto card volume; stablecoin-linked card spending reached an annualized run-rate of ~$4.5 billion by December 2025 (Visa Cuy Sheffield statement).

Acquirer Bank

The merchant's bank. Receives fiat settlement and pays the merchant. Never sees crypto. Manages disputes between the merchant and card issuer in the chargeback process.

Merchant / POS

No contact with crypto whatsoever. The POS terminal sees a standard card transaction: fiat authorization, fiat receipt. This zero-integration setup across 150 million+ Visa/Mastercard acceptance points is the self-custody model's strongest commercial advantage.

---

3. Full Transaction Flow

Nine stages from card setup to chargeback. Each stage covers the technical flow, architecture-specific variations, and legal obligations triggered at that step.

> *Color code: Blue box = technical step | Green border = legal obligations | Yellow border = warning*

3.1 Card Setup

Wallet Creation — *Setup*

The wallet is created when the user installs the application. The private key belongs to the user; the seed phrase is securely stored on the device or backed up by the user. In the smart contract wallet architecture, the wallet address corresponds to a smart contract defining the signing policy.

⚖️ **Legal Obligations**

> *No legal obligation has been triggered yet. Wallet creation alone does not require a license.*

Co-signer / Session Key Setup — *Setup*

- Architecture A: The smart contract is deployed with the co-signer address and policy rules (spend limit, whitelist, time restriction). Two signatures will be required for each transaction.
- Architecture B: Soft reserve policy is defined. Co-signer activates during the batch period. In MPC architecture, the company shard is created at this stage.
- Architecture C: The user creates a session key and assigns limited authorization to the card issuer address. Scope: specific token (e.g., USDC only), specific limit, specific duration. The user can revoke authorization at any time.

⚖️ **Legal Obligations**

- EU (MiCA): Whether co-signer or session key authorization constitutes "custody" remains contested. ESMA guidance awaited. Transition period ends July 1, 2026; CASP licensing obligations vary by country until then (see Section 7 for details).
- UK (FCA): FCA registration may be required for "qualifying cryptoasset" services under FSMA 2026. Sandbox active in Q1 2026.
- UAE (VARA): Co-signer structure may be classified as "custody." VASP license required under VARA Rulebook v2.0.
- Turkey: TCMB April 2021 prohibition; use of crypto as payment instrument is banned. SPK CASP Regulation and BRSA payment institution license overlap.

KYC / Identity Verification

Setup

The card issuer (or a verification service acting on its behalf) manages the KYC process: identity document, selfie, address verification. Upon approval, the card is produced and delivered. KYC data is not linked to the private key and does not affect the self-custody structure.

⚖️ **Legal Obligations**

- In all jurisdictions, the card issuer is the primary KYC responsible party. The user is in the position of a customer.
- EU: Customer identity verification (CDD) mandatory under AMLD6 and MiCA. Risk-based approach applies.
- US: FinCEN CIP (Customer Identification Program) requirements. MTL-holding issuer is responsible.
- Turkey: Identity verification mandatory under MASAK Article 5. Platform registration under Regulation No. 29.

3.2 Transaction Initiation

POS / Online Transaction Initiation

T = 0

The user inserts, taps, or enters the card online. The terminal generates a standard ISO 8583 authorization message and sends it to the Visa/Mastercard network. No crypto appears in this message: only fiat amount, card number, merchant information, and timestamp.

⚖️ **Legal Obligations**

- Crypto regulation has not yet come into play at this stage. The transaction begins under Visa/Mastercard network rules.

► Card network rules (Visa Core Rules, Mastercard Rules) define the framework to which the card issuer must adhere.

3.3 Authorization

	Balance Check + Co-signer / Session Key Approval	*0–2 seconds*

The card issuer receives the auth request. Two checks occur in parallel:

- Is the USDC balance sufficient? The USDC equivalent of the fiat amount is calculated at the current rate.
- Approval layer: Does the co-signer policy or session key scope permit this transaction?

If both checks pass, a soft reserve is created: the USDC amount corresponding to the transaction is locked, with no on-chain movement yet. The auth response returns "Approved" to the network.

- Architecture A: Co-signer signature is obtained or queued at this stage.
- Architecture B: Soft reserve is created; co-signer deferred to the batch period.
- Architecture C: Session key scope is checked. If within scope, approval is automatic.

⚖️ **Legal Obligations**

► EU (TFR / Travel Rule): The transaction is recorded at this stage. Which information is transmitted and when will be clarified in the next step.

► During the soft reserve period, the user continues to hold legal ownership of the USDC. However, the right of disposal is restricted.

► Authorization denial (insufficient balance or policy violation) falls within the card issuer's responsibility. Notification obligation to the user applies.

3.4 FX Conversion

	USDC → Fiat Conversion	*Simultaneous with auth or post-clearing*

The moment USDC is converted to fiat. Timing and responsible actor vary by architecture:

- At-spend (real-time): Rate is locked at auth. FX risk is minimal. Common in Architectures A and C.

- At-settlement (deferred): Conversion occurs post-clearing. Exchange rate risk may arise. Possible in Architecture B.

The card network's official rate is typically used as the rate reference. Whether a markup is applied varies by card program; some programs explicitly commit to "no markup."

⚖️ **Legal Obligations**

- EU: Disclosure of FX spread and rate information to the user is mandatory under MiCA and PSD2.
- The license status of the actor performing FX conversion (card issuer or separate FX layer) varies by jurisdiction.
- Turkey: TCMB foreign exchange regulations may subject crypto-fiat conversion to additional restrictions.

3.5 Clearing

	Clearing Message	*T+0 / T+1*

A clearing message is transmitted via VisaNet or Banknet. Settlement begins between the card issuer and acquirer bank. At this stage:

- The chargeback window opens; typically 60–120 days, varying by card network and transaction type.
- The transaction is recorded on both sides. Crypto still appears as a fiat record.
- The card issuer incurs a fiat liability to the acquirer.

⚖️ **Legal Obligations**

- EU (TFR): Travel Rule obligation is confirmed after clearing, before on-chain settlement. Transmission of originator and beneficiary information is mandatory.
- US (FinCEN): MSB (Money Services Business) registration requirements come into effect at the clearing stage.
- After the chargeback window opens, the dispute procedure between card issuer and user is governed by card network rules.

3.6 On-Chain Settlement

	Blockchain Transaction	*T+1 / T+2: varies by architecture*

The stage at which the three architectures diverge most clearly:

Architecture A — Per-Swipe On-Chain TX

A separate on-chain TX is sent for each transaction. USDC is transferred to the destination address (card issuer settlement address). The transaction is traceable on-chain; each spend leaves a separate record.

Architecture B — Batched Settlement

Multiple transactions are consolidated into a single batch TX. Occurs at end of day or periodically. Individual transaction traces within the batch TX may not be distinguishable.

Architecture C — Session Key Issuer Pull

The card issuer pulls USDC from the user's wallet using the session key authorization. The user is not active at this stage. The pull TX is visible on-chain, but each transaction may not be a separate TX.

⚖️ **Legal Obligations**

- EU (TFR / Travel Rule): Travel Rule obligation arises in full at the moment of the on-chain TX. Originator: user (name, wallet address, identity information). Beneficiary: card issuer settlement address.
- Architecture A: Each TX is separate, so attribution is clear. Compliance is most straightforward in this model.
- Architecture B: Attribution problem for individual transactions within the batch TX. FATF Travel Rule requires that each payment be traceable to its owner; additional system design is mandatory.
- Architecture C: In the pull TX, the originator is the user and the beneficiary is the card issuer. The "voluntary transfer" interpretation is contested due to the session key authorization; obtaining a regulatory opinion is recommended in some jurisdictions.
- Self-hosted wallet rule: Under EU TFR, additional verification (wallet ownership proof) may be required for transfers to the user's own wallet.

3.7 Merchant Settlement

	Acquirer → Merchant Fiat Payment	*T+1 / T+2*

The acquirer bank pays the merchant in fiat according to the clearing message. The merchant receipt shows fiat. Crypto has never appeared on stage. From the merchant's perspective, this is a completely standard card transaction.

⚖️ **Legal Obligations**

- The acquirer–merchant relationship is governed by fiat payment regulations. Crypto regulation does not apply at this point.

3.8 ATM Withdrawal

	ATM Cash Withdrawal	*Instant*

ATM withdrawal follows the same technical flow as a card purchase. The key difference: separate limit rules apply to cash withdrawals on the clearing and settlement side. USDC is locked to cover the fiat amount withdrawn (soft reserve). ATM transactions are subject to both daily and monthly limits; these limits are set by the card issuer, independent of on-chain limits.

- Daily ATM limit: Varies by card issuer policy (e.g., $500/day)
- Monthly ATM limit: Varies by card issuer policy (e.g., $2,500/month)
- If limit exceeded: Card issuer may apply a fee or decline the transaction

⚖️ **Legal Obligations**

- The ATM operator is a third party and may apply additional fees; these are independent of card program rules.
- EU TFR: Whether ATM withdrawal falls within Travel Rule scope varies by architecture. In Architecture A, each withdrawal has a separate on-chain TX; transfer classification is stronger. In Architecture B, individual withdrawals are absorbed into the batch; attribution is difficult. ESMA's interpretation of ATM withdrawals had not been published as of March 12, 2026; the cautious approach pending that interpretation is to maintain per-withdrawal records in all architectures.

3.9 Chargeback

	Chargeback Process	*T+60 / T+120 window*

Chargeback begins when the user disputes a transaction. Dispute grounds: unauthorized transaction, undelivered goods/services, incorrect amount. In the self-custody model, the chargeback process runs simultaneously on the fiat side and the on-chain side.

Fiat Side: Card Network Process

The user notifies the card issuer of the dispute. The card issuer initiates chargeback against the acquirer bank per Visa/Mastercard rules. The acquirer forwards the dispute to the merchant. If the merchant accepts, the refund follows the path acquirer → card issuer → user. If the merchant disputes, the dispute process begins (60–120 days).

On-Chain Side: Two Scenarios (by Architecture)

Scenario A: Reimbursement from Company Treasury

When chargeback is approved, the company reimburses the user from its own reserve. No on-chain reversal. The user receives USDC or fiat. Operationally the simplest approach, but the company must maintain sufficient liquidity reserves. Common in Architecture B.

Scenario B: On-Chain Reversal

When chargeback is approved, the smart contract or session key mechanism is activated. The locked USDC is returned to the user's wallet. Verifiable and transparent on-chain, but incurs on-chain transaction cost. Possible in Architectures A and C.

> *Chargeback and cashback are entirely separate processes. Chargeback is a dispute resolution mechanism governed by card network rules. Cashback is a spending reward operating under program terms.*

- Card network rules (Visa Core Rules / Mastercard Rules): Chargeback timelines, burden of proof, and dispute procedures are determined by the card network.
- EU: If the returned USDC is treated as a new crypto transfer, Travel Rule may be retriggered.
- US: Card issuer has EFTA (Electronic Fund Transfer Act) obligations in the chargeback process. Unauthorized transaction notification must be made within 60 days.
- For reimbursements from the company treasury, the card issuer has a disclosure obligation to the user (source of refund, timeline) under the EMI license.

3.10 Cashback

	Cashback: Spending Reward	*Monthly or periodic*

Cashback is a reward provided by the program in return for the user's spending. A completely separate process from chargeback.

- Reward calculation: A percentage of the spend amount (e.g., 0.5%–3%) accrues as a reward.
- Reward currency: In some programs paid in fiat (USD/EUR), in others as an ecosystem token.
- Distribution timing: Generally at month-end or periodic. Automatically credited to the user's wallet.
- Scope restrictions: ATM withdrawals, cash-like transactions, gambling, government payments and similar categories are generally excluded from cashback.
- Monthly cap: Varies by program limit.

In programs paying cashback in an ecosystem token, who finances the token treasury is an important question. It may be funded from the protocol treasury, company reserves, or transaction fees; a metric to monitor for sustainability.

⚖️ **Legal Obligations**

- EU: Ecosystem token paid as cashback may qualify as a crypto-asset under MiCA. Depending on token type, utility token or ART/EMT classification may arise.
- Tax: Taxation of cashback income varies by jurisdiction. In some EU countries, crypto cashback is treated as taxable income.
- Turkey: Payments made in ecosystem tokens may be classified as crypto-asset transfers under MASAK.

---

4. Three Technical Architectures

Three different architectures lie behind the same self-custody claim. As you read the following, you should be able to identify which model you are using.

Architecture A — Per-Swipe On-Chain TX

Each card transaction corresponds directly to an on-chain transaction. 1 swipe = 1 blockchain TX.

Technical Architecture

- Wallet: Smart contract (Safe-style multisig); user + co-signer signature required
- Per transaction: Two signatures obtained → on-chain TX broadcast → USDC delivered to destination address
- Co-signer policy: Spend limit, whitelist, time restriction defined within the smart contract
- Blockchain: L2 or dedicated chain preferred for low gas + fast finality
- Settlement: USDC or e-money token (EUR-pegged stablecoin)
- FX: At spend, card network official rate
- Chargeback: From company treasury or on-chain reversal (Scenario A or B)
- Cashback: Fiat or ecosystem token if applicable, periodic

Identification Criteria: If you are using this model:

- You can see a blockchain TX for each transaction
- Your wallet is a smart contract address (not an EOA)
- Co-signer approval on every transaction; you may occasionally notice auth latency
- Your spending history is fully traceable in a block explorer

Assessment

Architecture A is the architecture that most robustly satisfies the self-custody claim. Because each transaction is a separate TX, Travel Rule attribution is clear and the user can independently verify their spending history on-chain. The cost is latency: waiting for smart contract finality is occasionally noticeable in a POS environment. Despite co-signer audit costs and gas requirements per transaction (minimal on L2), I consider this architecture to hold the strongest legal defensibility position.

Architecture B — Batched Settlement

There is no on-chain transaction at the time of spending. Transactions occurring within a given period are settled as a batch TX.

Technical Architecture

- Wallet: Typically MPC; company also holds a shard
- At spend: Soft reserve, USDC locked, no on-chain TX
- At settlement: Multiple transactions in a single batch TX
- Co-signer: Activates at batch time, not per transaction
- Blockchain: EVM-compatible networks common

- FX: At settlement or at spend (varies by program)
- Chargeback: Typically from company treasury (Scenario A)
- Cashback: Fiat or ecosystem token if applicable, periodic

Identification Criteria: If you are using this model:

- You cannot see individual on-chain TXs corresponding to your transactions
- You pay no gas or very low gas
- Wallet infrastructure is provided by the company; there may be no seed phrase or the company holds a shard
- Auth is very fast; no on-chain waiting

Assessment

Architecture B's operational appeal is high: near-zero gas, instant auth, scaling ease. But MPC's company-held shard makes this the weakest self-custody legal argument of all three. The company holds part of the private key; under FATF and MiCA frameworks this carries the risk of being classified as custody. In my view, building a strong self-custody legal argument for Architecture B is very difficult; companies marketing this model as "self-custody" risk misleading consumers.

Architecture C — Session Key Issuer Pull

The user grants the card issuer limited, revocable authorization at setup. For each transaction, the card issuer automatically pulls USDC within the scope of this authorization.

Technical Architecture

- Wallet: Session key-enabled smart contract wallet
- Setup: User assigns limited authorization to card issuer address (token: USDC only, limit, duration)
- Per transaction: Card issuer pulls USDC using session key authorization; user does not provide active approval
- Authorization control: User can revoke session key at any time
- Blockchain: Low-cost network (L2 or dedicated chain)
- FX: Card issuer pulls USDC, executes conversion, sends fiat to acquirer
- Chargeback: Ecosystem token compensation or on-chain reversal (Scenario A or B)
- Cashback: Ecosystem token, periodic and automatic

Identification Criteria: If you are using this model:

- You granted authorization once at setup; no approval prompts since then
- The card issuer address appears in the session key list in your wallet
- You can revoke authorization from the application settings
- Cashback arrives automatically as an ecosystem token

Assessment

Architecture C is the smoothest solution from a user experience perspective: one-time authorization at setup, zero approval steps thereafter. The revocability of authorization keeps the self-custody argument alive. If session key scope is well-designed (USDC only, specific limit, specific duration), this architecture's legal defensibility is competitive with Architecture A. The critical question is: how broadly is the pull authorization scoped? The wider the scope, the weaker the self-custody argument and the stronger the custody interpretation. These boundaries must be clearly stated in the contract.

Architecture Comparison

Criterion

Architecture A	Architecture B	Architecture C	On-chain timing
Per transaction	Periodic batch	Pull at spend	User signature
Per transaction	None	Setup only	Wallet architecture
Smart contract (multisig)	MPC	Session key + smart contract	Transparency
Full; every TX on-chain	Partial; batch visible	Pull TX on-chain	Self-custody strength
High	Limited by MPC	High (revocable)	Travel Rule
Clear; each TX separate	Attribution problem	Additional design needed	User experience
Medium	Easy	Easiest	Gas cost
Per TX (low)	Amortized in batch	Low	Smart contract risk
High	Low	Medium	Chargeback mechanism
Treasury or on-chain	Treasury	Ecosystem token or on-chain	Cashback

Fiat or token, periodic	Fiat or token, periodic	Ecosystem token, automatic	Ecosystem token, automatic

The legal and technical framework of the self-custody card model has significantly clarified by 2026; however, three structural barriers stand in the way of mass adoption: oracle security and price slippage, gas cost and user experience, and cross-chain balance management. This section addresses each barrier from both technical and practical perspectives.

5. Technical Constraints and Scalability Challenges

There are two critical time points in a self-custody card transaction: (1) when the authorization message is sent at POS: the card network approves the fiat amount; (2) when the on-chain TX is broadcast, at which point stablecoin reserve is burned or spent. The time between these two points can range from milliseconds to several seconds. This interval is the primary source of price risk.

5.1 Oracle Security and Price Slippage

For fiat-pegged stablecoins like USDC, the 1:1 peg theoretically eliminates this risk; however, during peg stress events (USDC briefly fell to $0.87 during the Silicon Valley Bank crisis) or liquidity crunches, price slippage becomes a real risk. Who bears the delta between the authorization lock price and the on-chain burn price?

> *For fiat-pegged stablecoins like USDC, the 1:1 peg theoretically eliminates this risk; however, during peg stress events (USDC briefly fell to $0.87 during the Silicon Valley Bank crisis) or liquidity crunches, price slippage becomes a real risk. Who bears the delta between the authorization lock price and the on-chain burn price?*

Risk distribution by architecture

Architecture A (Per-TX signature): The user approves at authorization; price difference is minimal. However, if the user delays approval, the authorization timeout (typically 30 seconds) may expire and cancel the transaction. Risk sharing between user and issuer is determined by contract.

- Architecture B (Batch settlement): Soft reserve is created at authorization; on-chain TX is deferred. Price slippage accumulates on the issuer's balance sheet until the batch period. Large volatility events carry batch loss risk. Industry practice: issuer keeps 0.1–0.5% excess over authorization amount in reserve (over-collateralization buffer).
- Architecture C (Session key): The card issuer pulls USDC from the user's wallet. Even if the session key spend limit is fixed, oracle price deviation can cause over-spending loss for the issuer. Example: a $50-limit session key authorizes $49.80; if the USDC/USD rate moves to $0.995 at the on-chain TX moment, the issuer loses $0.25. This delta compounds across millions of transactions.

- Architecture C (Session key): The card issuer pulls USDC from the user's wallet. Even with a fixed session key spend limit, oracle price deviation can cause over-spending loss for the issuer. Example: a $50-limit session key authorizes $49.80; if the USDC/USD rate moves to $0.995 at the on-chain TX moment, the issuer loses $0.25. This delta compounds across millions of transactions.

Industry-standard solutions combine decentralized oracle networks like Chainlink Data Feeds or Pyth Network with the card processor's internal pricing. Two-layer approach: primary oracle provides on-chain price, processor's circuit breaker suspends the transaction if deviation exceeds 0.5%. Gnosis Pay is a field-tested example of this architecture.

Flash loan attacks and oracle manipulation have caused billions in losses in DeFi protocols. A self-custody card oracle faces the same attack vectors. The card issuer's oracle selection and circuit breaker threshold must be clearly stated in the user agreement.

The most practical barrier to mass adoption of the self-custody card is this question: must the user hold the network's native token (ETH, SOL, AVAX) in their wallet for gas fees on every coffee purchase? In 2020, the answer was "yes." In 2026, the answer has changed: but whether it has become standard is debatable.

5.2 Gas, Paymaster and Gasless UX

Ethereum's ERC-4337 Account Abstraction standard made the "Paymaster" concept possible. A Paymaster is a smart contract that pays gas fees on behalf of the user and deducts the equivalent from the user's USDC. Result: the user can execute transactions without holding any ETH in their wallet.

Gasless UX: User is unaware of gas fees. Card issuer or sponsor covers Paymaster cost, embedding it in FX spread or subscription fee.

Sponsored transactions: Card issuer can sponsor a set number of transactions per user per month at no cost (e.g., first 30 transactions gasless). Beyond that, cost is passed to the user.

Solana and other chains: On Solana, gas (transaction fee) is very low (~$0.00025) and USDC payment is supported instead of SOL: no Paymaster needed. This is the primary source of UX advantage for Solana-based self-custody cards.

- Gnosis Pay (on Gnosis Chain) has been running a gasless architecture since 2024 where users cover all gas fees with EURe (Euro stablecoin). The user holds a single token; ETH or xDAI is unnecessary. This model is setting the industry standard for 2026.
- Sponsored transactions: The card issuer can sponsor a set number of transactions per user per month at no cost (e.g., first 30 transactions gasless). Beyond that, cost is passed to the user.

- A user transitioning from a banking experience to crypto must not need to understand or manage the concept of "gas fee." As of 2026, gasless UX has become table stakes for self-custody card programs: not a differentiator but a baseline expectation. Programs without Paymaster integration will struggle to grow outside the premium segment.

> *Gnosis Pay (on Gnosis Chain) has been running a gasless architecture since 2024 where the user covers all gas fees with EURe (Euro stablecoin). The user holds a single token; ETH or xDAI is unnecessary. This model is setting the 2026 industry standard.*

5.3 Cross-Chain Balance Management and Chain Abstraction

Can a user holding funds on Base (Coinbase L2) spend with the same card at a merchant running on Polygon? As of 2026, technically possible but operationally complex. This problem is called "chain abstraction": the ability for a user to spend without knowing which chain their funds are on.

Minimum requirements for mass adoption

Circle CCTP (Cross-Chain Transfer Protocol): Moves USDC natively between two chains via mint/burn. Theoretical latency 15–20 seconds; too long for the card authorization window. This latency is reduced to zero with pre-funded bridge liquidity.

Chain abstraction layers (Particle Network, Socket Protocol, Biconomy): Display balances across different chains as a single "spendable balance." User doesn't know which chain they're on; the cheapest/fastest bridge is automatically selected in the background.

L2-first architecture: Ethereum L2s such as Optimism, Base, Arbitrum offer both low gas and high finality speed. Some issuers adopt a single-chain policy by moving users to L2: eliminating complexity but restricting flexibility.

Cross-chain bridge smart contracts are the most frequently hacked structures in DeFi history (over $2 billion in losses from bridge hacks 2022–2024). Choosing a cross-chain solution for a self-custody card requires balancing both UX and security. The card issuer's choice of bridge protocol must be disclosed to the user.

The majority of self-custody card programs in the market operate on a single-chain policy. Cross-chain spending is not yet widespread; chain abstraction layers are in a pilot phase. The table is expected to change from a 2027 perspective; however, the standard is unclear today. The question "which chain does this card work on?" remains valid in the user's purchase decision.

Existing solutions

- Circle CCTP (Cross-Chain Transfer Protocol): Moves USDC natively between two chains via mint/burn. Theoretical latency 15–20 seconds; too long for the card authorization window. This latency is reduced to zero with pre-funded bridge liquidity.

- AML obligations in the self-custody card program are concentrated on the card issuer. The user's private key ownership does not eliminate the platform's AML responsibility. On the contrary, the on-chain-based transaction traceability requires additional system design.

> *Standard CDD (Customer Due Diligence)*

Identity verification, address confirmation, and risk profiling are mandatory for each user. In a self-custody card, KYC data is not linked to the private key but the card issuer must know its customer. Standard CDD is sufficient for low-risk users.

Current state: March 12, 2026

EDD is triggered under certain conditions:

---

6. AML Compliance Obligations

AML obligations in a self-custody card program are concentrated on the card issuer. The user's private key ownership does not eliminate the platform's AML responsibility. On the contrary, on-chain-based transaction traceability requires additional system design.

6.1 Customer Due Diligence (CDD / EDD)

Standard CDD (Customer Due Diligence)

Identity verification, address confirmation, and risk profiling are mandatory for each user. In a self-custody card, KYC data is not linked to the private key but the card issuer must know its customer. Standard CDD is sufficient for low-risk users.

Enhanced Due Diligence (EDD)

EDD is triggered under certain conditions:

- PEP (Politically Exposed Person): EDD mandatory if the user is a politically exposed person.
- High-risk country: Additional verification for users from FATF grey/black-listed countries.
- Unusual transaction volume: EDD is triggered by sudden volume spikes inconsistent with the user profile.
- Self-hosted wallet: Under EU TFR, wallet ownership proof may be required for transfers to the user's own wallet.

6.2 Transaction Monitoring

The card issuer must build transaction monitoring infrastructure on both the fiat and on-chain sides. Two layers:

Fiat Side

Merchant category, amount, geography, and transaction frequency are monitored via ISO 8583 messages. Unusual patterns (e.g., high volume at midnight, new merchant categories, rapid consecutive transactions) are caught by the rules engine.

On-Chain Side

Blockchain analytics integration is required. Monitored criteria:

- USDC from mixer/tumbler services: High-risk source.
- Interaction with sanctioned addresses: OFAC, EU Sanctions, UK OFSI.
- Funds from dark markets or exploits: Monitored via Chainalysis, Elliptic, or similar tools.
- Multiple wallet transfers in a short period: Possible structuring signal.

> *In Architectures A and C, each transaction is a separate TX, making on-chain monitoring clearer. In Architecture B, source-destination attribution within batch TXs reduces monitoring quality.*

6.3 Suspicious Transaction Reporting (STR / SAR)

Suspicious situations detected by the monitoring system must be reported to the relevant financial intelligence unit:

- EU: Each member state's FIU (Financial Intelligence Unit). Tipping-off prohibition under AMLD6.
- UK: National Crime Agency (NCA) ELMER sistemi.
- US: SAR (Suspicious Activity Report) to FinCEN, within 30 days.
- UAE: Notification to CBUAE and VARA. VARA Rulebook v2.0 details AML reporting procedures.
- Turkey: Suspicious transaction report to MASAK. Reporting obligation for crypto platforms under Regulation No. 29.

6.4 Sanctions Screening

Real-time sanctions screening is mandatory for each transaction. Lists to screen:

- OFAC (SDN List): US sanctions list. Claims global scope; applicable to all US-connected transactions.
- EU Consolidated Sanctions List: EU sanctions list.
- UK OFSI: Independent UK list, diverged from EU list post-Brexit.
- UN Sanctions: UN sanctions list.
- VARA Sanctions List: UAE-specific list.

Screening must cover both user identity and on-chain wallet address. OFAC's 2023 listing of Tornado Cash demonstrated that smart contract address screening has also become mandatory.

6.5 Actor-Based AML Responsibility Allocation

Actor	AML Obligation	Scope	Architecture-Specific Difference
Card Issuer	Primary	CDD, EDD, STR, sanctions, TX monitoring	Same across all architectures
Co-signer / Session Key	Contested	CASP obligation may arise depending on MiCA custody interpretation	Clearer in Architectures A and C
Blockchain Analytics	Tool (not an actor)	On-chain source verification, sanctions screening	Attribution limited in Architecture B
Card Network	Indirect	Network rules mandate AML policy	Same across all architectures
User	None (customer)	KYC process participation, obligation to provide accurate information	Same across all architectures

6.6 AMLA: The New EU AML Supervisory Authority

From January 1, 2026, the EU's AML/CFT supervisory powers were transferred from EBA to AMLA (Anti-Money Laundering Authority). AMLA's operational timeline: risk assessment methodology to be completed in 2026; selection process for directly supervised entities to begin in 2027; direct supervision of 40 major financial institutions (including crypto) to commence in 2028.

"New payment channels" are explicitly on AMLA's priority list: self-custody card programs may fall within this category.

> *Practical outcome: The 2026–2027 period is a transition during which AMLA takes over EBA rules and develops its own methodology. During this period, existing AMLD6 obligations remain in force. After 2028, large-scale self-custody programs may come under direct AMLA supervision.*

6.7 FATF Stablecoin Report: March 3, 2026

FATF published its "Targeted Report on Stablecoins and Unhosted Wallets" on March 3, 2026. Key findings: stablecoins accounted for 84% of illicit virtual asset transactions in 2025; the number of stablecoins in circulation exceeded 250, with market capitalization surpassing $300 billion. FATF encouraged stablecoin issuers to implement measures enabling them to technically freeze, burn, and claw back assets in the secondary market.

> *Impact on the self-custody model: FATF's focus on unhosted wallets questions the AML monitoring capacity of card issuers in self-custody card programs. In Architecture A, every TX is traceable; in Architecture B, batch attribution weakness overlaps with FATF's unhosted wallet concerns. Architecture A or C should be preferred for the compliance argument.*

---

7. Regulatory Framework — As of March 12, 2026

Technical architecture alone is insufficient to run a self-custody card program. Seven different jurisdictions, seven different license and compliance frameworks.

7.1 European Union

MiCA: CASP License

MiCA has been fully in force since December 2024. As of March 12, 2026, more than 40 CASP licenses have been issued. Transition period varies by country: Netherlands completed in July 2025, Italy in December 2025. Final deadline for remaining countries: July 1, 2026; unlicensed operation is not possible after this date. Minimum capital: EUR 125,000 for custody and exchange, EUR 150,000 for trading platform.

Three different positions emerge on the custody interpretation for self-custody cards:

- Interpretation A: Since no private key is held, outside MiCA scope; CASP license may not be required
- Interpretation B: Co-signer/session key = control = CASP license mandatory
- Interpretation C: CASP + PI/EMI dual license; from March 2, 2026, both MiCA and PSD2 required for EMT custody/transfer (see below)

MiCA × PSD2 Dual License: In Force March 2, 2026: CRITICAL

EBA's June 2025 No-Action Letter and February 12, 2026 Opinion (EBA/OP/2026/01) provide a framework: they envisage that CASPs holding or transferring EMT (such as USDC, EURC, PYUSD) may be classified as payment service providers under PSD2. However, the EBA Opinion is not binding law: it is advisory. How national competent authorities (NCAs) apply this interpretation may vary by country. Three possible scenarios from March 2, 2026:

- Scenario 1 (Continuation): CASP has obtained PI/EMI license or is partnered with a licensed PSP. May continue operations.
- Scenario 2 (Conditional continuation): CASP has completed PSD2 application but license not yet obtained. May continue temporarily at NCA's discretion: but cannot onboard new EMT payment customers or conduct marketing.
- Scenario 3 (Suspension): No application or conditions not met. NCA halts activity; customer offboarding mandatory.

Direct impact on self-custody card programs:

- Architecture C (Session Key Pull): Card issuer pulls USDC from user wallet → EMT transfer → PSD2 payment service. Card issuer must have PI/EMI license or work with a licensed PSP.
- Architectures A and B: USDC transfer at settlement step → same obligation. Card issuer license check mandatory.
- Exemption: Crypto-fiat conversion (exchange) does not fall within PSD2 scope. First-party transfers between own wallets are contested.
- Cumulative capital burden: MiCA €125,000 + PSD2 PI €125,000 = minimum €250,000 combined capital. No compensation mechanism.
- Strong Customer Authentication (SCA) and fraud reporting: Fully mandatory from March 2, 2026. Cannot be deferred even during the transition period.

> *EBA long-term solution proposal: Payment service-related provisions should be added to MiCA in the PSD3/PSR process; this would eliminate the dual-license requirement for EMT activities. Process ongoing; EU Commission report expected throughout 2026. ECB Working Paper (March 3, 2026): warning that stablecoin growth will erode EU bank deposits and weaken monetary policy transmission; risk "significantly" increases if dollar-denominated stablecoins gain dominance in Europe. Finding: rising stablecoin interest reduces retail deposits and constrains corporate credit.*

> *Since the growth of the self-custody card model directly feeds this debate, monitoring EU regulators' stance is critical.*

AB Travel Rule (TFR)

In force threshold-free since December 30, 2024; full identity information required on every transfer. Additional verification required for self-hosted wallets. In Architecture A, attribution is clear; in Architecture B, batch attribution problem; in Architecture C, pull TX interpretation is contested: considered alongside EBA's EMT transfer interpretation.

DAC8

In force from January 1, 2026. All crypto transactions of EU-resident users will be reported to national tax authorities by CASPs. First reporting in 2027 (for 2026 transactions). Each on-chain TX in self-custody card programs falls within DAC8 reporting scope.

7.2 United Kingdom

FSMA 2026 (Cryptoassets) enacted in February 2026, effective October 2027. FCA sandbox launched Q1 2026. An independent regime from the EU. MiCA does not apply; separate FCA registration mandatory. Custody definition interpreted under FCA's "qualifying cryptoasset" framework. CP26/4 consultation period closed March 12, 2026; Policy Statement expected mid-2026. FCA's announced license application window: September 30, 2026 – February 28, 2027. Existing AML/MLR registration does not automatically convert to the new regime; registered firms must reapply during this window.

7.3 United Arab Emirates

- Dubai; VARA Rulebook v2.0 (June 2025): VASP license mandatory. Custody interpreted broadly.
- Abu Dhabi; ADGM/FSRA: Innovation-friendly approach; MTF and custody licenses available.
- CBUAE PTSR (August 2025): Separate CBUAE approval required for stablecoin issuance and card programs.

UAE splits in two. Dubai (VARA): theoretically yes: VASP license obtainable, regulatory framework clarified. However, whether self-custody qualifies as "custody" under VARA's broad interpretation remains uncertain; VASP + CBUAE PTSR dual-license burden is significant. Abu

Dhabi (ADGM): innovation-focused approach, No-Action Letter possible, preferable for faster market entry.

7.4 Singapore

VASP license (PSA Part 9) mandatory under MAS Payment Services Act (PSA) since June 2025. MAS SCS framework finalized in August 2023; addition of "Stablecoin Issuance Service" to PSA and mid-2026 effective date target. Whether self-custody structure qualifies as "custody" not yet clarified; No-Action Letter application possible.

7.5 Hong Kong

Stablecoins Ordinance in force since August 2025. HKMA issued first stablecoin issuer licenses in March 2026; only a very small number of firms will make the list from 36 applications (including the Standard Chartered-led joint venture). HKMA Payment Service Provider license separately required for card programs; dual-license risk present.

7.6 United States of America

GENIUS Act enacted in July 2025. Federal or state license mandatory for stablecoin issuance. Full obligation effective: 18 months after enactment (January 2027) OR 120 days after OCC final rule: whichever comes first; OCC final rule targeting July 2026, ~November 2026 effective date expected. GENIUS Act does not directly bind a card issuer using an external stablecoin like USDC — the rule applies to the stablecoin issuer (e.g., Circle). However, using an unlicensed or MiCA-non-compliant stablecoin creates indirect risk; stablecoin selection in the contract should be evaluated against GENIUS Act scope. OCC final rules on card programs targeting July 2026. State-based MTL still applicable across 50 states. Bridge (Stripe) received conditional national bank charter approval from OCC in February 2026; this model may signal a new licensing pathway for self-custody card programs.

> *Precedent (March 4, 2026): Kraken Financial (Wyoming SPDI) set precedent as the first crypto firm in US history to receive a Federal Reserve master account (Kansas City Fed). The possibility of Wyoming SPDI-licensed institutions becoming BIN sponsors could open an alternative US licensing pathway for self-custody card programs; the sector is watching.*

- TCMB April 2021: Use of crypto as payment instrument prohibited; still in force

- SPK CASP Regulation (2024): Covers only buying and selling. BRSA payment institution license separately required for card programs.
- MASAK Article 24/A (February 25, 2025): Full identity information mandatory for crypto transfers of TRY 15,000 and above. Threshold approximately $425. Non-compliance penalty TRY 453,342 (2025, revalued annually).
- MASAK Regulation No. 29 (June 28, 2025): Daily $3,000 / monthly $50,000 stablecoin withdrawal limit. 48-hour waiting period (72 hours for first transaction). Board approval exemption possible for liquidity/market making.

> *As of 2026, Turkey faces the simultaneous barriers of payment prohibition + dual license + transaction limits. Priority market is EU or MENA.*

The current picture can be described as a high-risk grey area; saying "definitely no" is also not correct. The TCMB April 2021 circular prohibits providing services for "direct or indirect" use of crypto-assets in payments. In a self-custody card, the merchant sees fiat; the user technically pays fiat, not crypto. This reality generates a defensible counter-argument on whether it falls within the "indirect use" scope. However, since the card issuer's entire business model is crypto-based, the prohibition on "services that cannot be provided" may apply. TCMB has never clarified this interpretation in writing; where the line is drawn remains unclear. The legal path requires first revising TCMB's circular, then obtaining the SPK CASP + BRSA payment institution dual license. Development to watch: whether SPK CASP scope will include payment services: expected to be clarified by end of 2026.

Regulatory Summary Table

Region	Primary Framework	Custody Interpretation	Travel Rule	Status (March 12, 2026)
AB	MiCA + TFR + PSD2	3 interpretations, ESMA clarification awaited	Threshold-free	Transition end: Jul 2026
UK	FSMA 2026	FCA sandbox active	FCA rules	Effective: Oct 2027
UAE	VARA + CBUAE PTSR	Broad interpretation	VARA rules	In force
Singapore	PSA + MAS	Not clarified	MAS rules	SCS draft law mid-2026

Hong Kong	Stablecoins Ordinance	Distributor guidance awaited	HKMA rules	Active since Aug 2025; first licenses Mar 2026
US	GENIUS Act + MTL	State-by-state variable	FinCEN rules	OCC rules Jul 2026
Turkey	TCMB + SPK + MASAK	Payment prohibition active	TRY 15,000 threshold	Restricted

8. Program Catalog

Leading self-custody card programs active in the market as of March 12, 2026. At least one example from each of the three technical architectures.

Program	Network	Architecture	BIN Sponsor	Market	Key Features
Gnosis Pay	Visa	Architecture C (Session Key)	Lithuanian EMI (own)	EEA	Safe AA wallet + Gnosis Chain L2; EURe native settlement; MiCA CASP application ongoing
Fiat24	Visa	Architecture C (Session Key)	SBA (Switzerland)	EEA + global	On-chain IBAN; USDC/EUROC direct settlement; Arbitrum-based
MetaMask Card	Mastercard	Architecture B (MPC)	Baanx	EEA	MetaMask wallet integration; USDC/DAI; Consensys infrastructure
Coin.me / CashCard	Visa	Architecture B (MPC)	Sutton Bank	US	ATM-focused; physical card; USDC spending
Kast (formerly Decaf)	Visa	Architecture C (Session Key)	Fonbnk / Visa	LatAm + global	Solana-based; USDC rewards; LatAm remittance-focused

> *The majority of self-custody card programs are in a hybrid position: self-custody for their own programs, offering white-label infrastructure for BIN sponsors or processors. The table covers only end-user-facing self-custody programs.*

9. Revenue Economics

Revenue distribution in the self-custody card model is more complex compared to other models. The card issuer must manage both FX conversion and interchange while providing the user with the self-custody advantage. This balance directly affects margin structure.

T + 0.3s

9.1 Interchange Revenue

The transaction fee collected from the merchant acquirer via the card network on each POS transaction. In the self-custody model, since the card issuer is both BIN sponsor and program manager, the entire interchange is collected by a single party; there is no sharing.

T + 0.6s

Item	Model 01 (Self-Custody)	T + 0.8s	Model 03 (Full-Stack)	Model 04 (White-Label)
T + 1.1s	$1.50	$1.50	$1.50	$1.50
→ Card network commission	-$0.05	-$0.05	-$0.05	-$0.05
→ BIN Sponsor share	Low (own issuer)	Low (own issuer)	—	-$0.30 ~ –$0.60
→ Processor share	Low / fixed	Low / fixed	Internal	Medium
FX Spread (~0.5–1.5%)	Medium	Exchange retains	PM retains (~$1.00)	Partial ($0.20 – $0.50)
Net to Issuer	Soft reserve liquidity	~$0.80–1.10	Soft reserve liquidity	~$0.60–0.90

Liquidity buffer

> *Figures are representative averages; actual margins vary by contract terms, country, and transaction type. Since the card issuer is also the BIN sponsor in the self-custody model, there is no PM layer cost; this structural difference is the primary source of net margin advantage.*

Liquidity buffer

9.2 FX Spread Revenue

The spread generated on each stablecoin-to-fiat conversion is set by the card issuer in the self-custody model. Typical spread is 0.5%–1.5%; disclosure to the user is mandatory under EU PSD2 Art. 45 and MiCA transparency obligations. Since FX conversion occurs simultaneously with the on-chain transaction in the self-custody model, rate risk exposure time is minimal.

9.3 Cashback and Reward Financing

Some self-custody card programs return a portion of interchange revenue to the user as stablecoin. This structure both increases user loyalty and keeps the user in the on-chain ecosystem. Tax classification of cashback varies by jurisdiction; some EU countries treat crypto cashback as taxable income while others do not.

9.4 Sustainability Analysis: Absence of Float and Compensation Mechanisms

"Float" income is among the most important revenue items in traditional banking: the bank earns interest by deploying customer deposits in loans or treasury instruments. In the self-custody card model, this income disappears entirely: customer funds are not in a bank but in the user's wallet. This structural shortfall raises a legitimate question about the model's sustainability.

Why is there no float?

- In Architecture A, the user holds USDC in their own wallet; it never enters the card issuer's balance sheet. In Architecture B, although technically residing in the user's wallet address, the company holds a shard under MPC, which raises the custody debate.
- In Architecture C, USDC pulled under session key authorization passes through the issuer's temporary account at authorization; settlement completes within minutes. Sustained float accumulation is not possible.
- Result: Even if 10,000 daily active users with an average $500 balance create a total of $5 million in "idle" capital, this money is not under the issuer's control.

Compensation mechanisms

Despite the absence of float, the self-custody model can be sustainable through the following revenue channels:

- Interchange + FX spread synergy: In the self-custody model, the card issuer is both BIN sponsor and FX converter. Two revenue streams combine in one hand; in other models these are shared. Net margin advantage is visible in the Section 9 table.
- Program fee: Monthly/annual card subscription fee. In the high-value user segment (crypto-native, on-chain active user), there is $5–15/month subscription tolerance.
- On-chain yield opportunity (indirect): The user can stake their own USDC in Aave or local vaults: the issuer does not earn this directly, but through "yield-bearing stablecoin" integration (e.g., sUSDe, USDY) a portion can be redirected to the issuer. This structure may be subject to the yield prohibition under GENIUS Act; careful evaluation required in the US market.

- Economies of scale: Each additional user amortizes fixed infrastructure cost. The on-chain settlement of self-custody architecture is cheaper than traditional banking infrastructure; cost structure is advantageous.

FX rate risk

> *Comparison: A traditional neobank (e.g., Revolut, N26) reaches profitability on a user making 200+ monthly transactions through interchange + premium subscription. For a self-custody card targeting the same user profile, interchange + FX spread may be sufficient. Profitability without float income is dependent on the combination of scale, FX margin, and subscription fee.*

---

10. Legal Implications of Payment Flows

The technical uniqueness of the self-custody card model complicates certain legal questions in unusual ways. Since the private key is with the user, the liability chain operates differently from the standard card model.

Liquidity buffer; on-chain TX delay scenario should be tested

> *Legal right nature: The self-custody model is the only structure among the four models in which the user holds a proprietary right over their assets. As long as the private key remains with the user, the stablecoin belongs directly to the user: it does not appear on the card issuer's balance sheet and cannot be included among creditors in an insolvency scenario. This distinction means the user holds a proprietary right, not a claim right, over the stablecoin, a distinction that is decisive in the event of company insolvency.*

Liquidity buffer; on-chain TX delay scenario should be tested

The card is issued in the name of the card issuer / BIN sponsor. The user's legal counterparty is the card issuer; however, in the self-custody model, the user is simultaneously the true legal owner of the asset. This dual identity: both customer and asset owner, which does not exist in the standard card model and must be explicitly addressed in the contract.

- Dispute right: The user exercises chargeback rights against the card issuer / BIN sponsor. On the on-chain side, the principle of transaction irreversibility applies; a signed TX cannot be cancelled.
- Account block: The card issuer can suspend the card program on AML grounds. However, it is not possible to freeze the user's on-chain assets: funds remain in the user's wallet.
- Insolvency: If the card issuer becomes insolvent, there is no pooled custody; the user's assets are in their own wallet and cannot be included among creditors.

> *The strongest legal advantage of the self-custody model is the insolvency protection argument. Since user funds do not appear on the card issuer's balance sheet, customer assets are not at risk in the event of company insolvency. This aligns with the asset protection obligation under MiCA Art. 70.*

10.2 Chargeback: The On-Chain Irreversibility Problem

In the standard card system, chargeback means the financial reversal of a transaction. In the self-custody model, fiat reimbursement is possible on the POS side; however, an on-chain TX that has already occurred cannot be reversed. This gap creates a practical problem:

- If chargeback is accepted: The card issuer refunds the user in fiat. But the on-chain stablecoin has already been spent/converted. There is no double-spend risk; however, the card issuer incurs a loss.
- If chargeback is rejected: The user has lost both fiat and spent stablecoin. This scenario must be explicitly addressed in the card agreement.

> *If Visa's 0.9% and Mastercard's 1% chargeback thresholds are exceeded, the card issuer faces program termination risk. The on-chain irreversibility of transactions makes chargeback management more critical in the self-custody model.*

10.3 Tax and Reporting Obligations

Each stablecoin → fiat conversion may be a taxable event. By jurisdiction:

- EU: Under DAC8 (January 1, 2026), the card issuer must report user transactions to national tax authorities. Since each transaction is a separate TX in the self-custody model, reporting is clearer.
- US: Every crypto → fiat conversion is subject to capital gains tax. IRS Form 1099-DA is mandatory for crypto brokers from 2025. Card issuer is the reporting obligor.
- Turkey: Taxation of crypto-asset gains has not yet been clarified; under consideration within the Income Tax Code framework.

User Experience Dilemma: The Disposal Burden

Even if the legal framework is correctly constructed technically, the self-custody card can result in an unexpected tax burden for the user. Scenario: user makes an average of 5 card transactions per day. Approximately 1,800 transactions per year, each a separate crypto-asset disposal. For each disposal, cost basis and proceeds must be calculated separately; profit or loss must be reported.

> *A user facing 1,800 rows of tax reporting per year is the biggest behavioral barrier to mass adoption of the self-custody card. The perception of "filing a tax return when buying coffee" pushes crypto-non-native users toward the custodial model.*

Automated Tax Reporting Integration

Two approaches exist in the industry to solve this problem:

- Issuer-side reporting: The card issuer automatically converts each transaction into a tax record and provides the user with an annual tax summary. IRS 1099-DA obligation already requires this; DAC8 produces the same result in the EU. Problem: the issuer cannot always know cost basis: where and at what price did the user buy the USDC?
- Third-party tool integration: Crypto tax software such as Koinly, CoinTracker, Coinpanda, and Blockpit automatically pulls the entire on-chain transaction history by reading the wallet address and calculates cost basis. Integration of these tools with the wallet address is technically feasible for the self-custody card architecture; however, it has not become standard. The "set up card and connect Koinly" flow is offered optionally by a few programs as of 2026.

> *Practical recommendation: Self-custody card programs should provide users with a tax obligation disclosure during the setup flow and list supported tax integrations. This step both satisfies the regulatory transparency obligation and reduces user churn. Disclosure obligation already exists under MiCA Art. 68 and PSD2; expanded disclosure including the tax dimension is becoming best practice.*

10.4 Types of Rights: Property, Claim and Custody

The fundamental element legally distinguishing the self-custody card model from other models is the nature of the right the user holds over their assets. This nature must be analyzed through three frameworks: property right, claim right, and custody. Each model corresponds to a different right category; this difference is decisive across areas from insolvency scenarios to tax classification, from contract liability to MiCA compliance.

Three Types of Rights

Property right (in rem / proprietary right): The asset belongs directly to its owner. The right operates "against the thing" (in rem): enforceable against third parties. In company insolvency,

creditors cannot seize these assets. Equivalent to "legal title" in common law and "ayni hak" (real right) in civil law.

Claim right (in personam / claim right): The user holds the right to demand the equivalent, not the asset itself. The right operates only against the obligor. In company insolvency, the user becomes an ordinary creditor. Traditional bank deposits fall in this category.

Custody: The asset is held by a third party. Legally, title may remain with the custodian (legal title) or beneficial ownership may rest with the user. MiCA Art. 3(1)(16) and FATF place this distinction at the center of the custody definition.

Which Right Applies in a Self-Custody Card?

Three architectures carry the same "property right" claim, but the underlying legal reality differs:

- Architecture A — Strongest property right: The user controls the private key independently. The co-signer imposes a restriction through smart contract policy, but this restriction does not change who the asset legally belongs to. Even if the issuer's systems go down, the user can access the wallet through another interface. The purest "in rem" position.
- Architecture B — Weak property claim: In MPC architecture, the company holds a shard; the user never has the complete private key. If the company loses its shard, the user's access can be permanently blocked. The legal reality is closer to a claim right.
- Architecture C — Bare ownership problem: Property right is with the user; the private key belongs to the user. However, the session key grants the card issuer limited spending authorization. This creates the "bare ownership vs beneficial use" tension: legal ownership is with the user but day-to-day economic use depends on issuer authorization.

Bare Ownership vs Beneficial Use

The tension that Architecture C reveals is discussed in legal literature as the distinction between "bare ownership" and "beneficial use." The practical test: if the issuer's systems completely fail, can the user access their assets?

- Architecture A: Yes, access is possible as long as the smart contract exists on-chain. Genuine property.
- Architecture B: No, signature cannot be completed without the company shard. The property claim is effectively hollow.
- Architecture C: Partially; when the session key is revoked, the user regains full control. While the key is active, daily use is subject to issuer conditions. Can be described as "revocable economic dependency."

Comparison with Other Models: Brief Note

This distinction emerges more sharply in the series' other models. In M02 and M03, the user typically holds a claim right: the asset is on the exchange's balance sheet. In M04, the liability chain becomes even more complex. Detailed rights analysis for each model is covered in its own section.

⚖️ **Legal Obligations**

▸ MiCA Art. 3(1)(16): Custody is defined as "holding or controlling crypto-assets or means of access on behalf of clients." ESMA has not yet clarified whether session key and co-signer structures fall within this definition. Even if the property right argument is valid, the presence of "control" may trigger the custody interpretation.

▸ MiCA Art. 70 (asset protection): In the self-custody model, customer assets do not enter the issuer's balance sheet, so this obligation is naturally met. If Architecture B's MPC shard is classified as custody, MiCA Art. 70 comes into force and asset segregation becomes mandatory.

▸ Insolvency law: Assets of a user holding a property right cannot be included in the insolvency estate. A user holding a claim right enters the pool of general creditors. In a self-custody card, this difference represents the gap between zero and full protection in an insolvency scenario.

▸ Contract obligation: The card agreement must explicitly address (1) the type of right the user holds, (2) how the session key/co-signer restricts this right, and (3) what the user can do if the issuer's systems fail. MiCA Art. 68 transparency requirements cover this scope.

11. Case Study: The Anatomy of a Single Transaction

A realistic scenario to concretize the theoretical flow: Alex makes an 18 Euro purchase at a cafe in Amsterdam. They hold their self-custody card to the POS terminal. What happens in 11 seconds behind the scenes?

Scenario Parameters

User	Alex: EEA resident, self-custody card user with a Dutch IBAN
Card model	Architecture C (Session Key) — Gnosis Pay-like structure
Transaction	18 Euro POS transaction in Amsterdam
Wallet balance	250 EURe (EUR-pegged stablecoin, Gnosis Chain)
Session key scope	EURe only, daily 500 Euro limit, valid 90 days

Step-by-Step Flow

#	Time	What Happens

1	T = 0	Alex holds their card to the POS. The terminal generates an ISO 8583 auth message for 18 Euro and sends it to the Visa network. No crypto in this message; fiat only.
2	T + 0.3s	Visa routes the auth request to the card issuer's (Gnosis Pay infrastructure) endpoint.
3	T + 0.6s	Card issuer calculates the instant rate: 18 EUR ≈ 18.04 EURe (FX spread included). Session key scope is checked: daily limit 500 Euro, 0 used today: approved.
4	T + 0.8s	18.04 EURe is placed in soft reserve: no on-chain movement, account-internal lock. Card issuer sends "Approved" to Visa.
5	T + 1.1s	POS terminal receives approval signal. Alex's screen shows "Approved 18.00 EUR." Merchant receipt shows fiat; crypto is not visible.
6	T + 2–4s	Using session key authorization, the card issuer pulls 18.04 EURe from Alex's wallet. The on-chain TX is broadcast to Gnosis Chain. TX hash recorded on-chain; Alex can verify via explorer.
7	T+0 / T+1	Clearing message transmitted via Visa network to acquirer bank. TFR obligation: originator (Alex, wallet address, identity), beneficiary (card issuer settlement address) information recorded.
8	T+1 / T+2	Card issuer transfers fiat to acquirer. Acquirer pays merchant 17.55 Euro (18 EUR minus ~2.5% total card acceptance cost). Process complete for merchant; crypto never appeared.
9	T+1 / T+2	Under DAC8, the on-chain TX is added to the list of transactions the card issuer will report to the Dutch tax authority (Belastingdienst). For Alex, this transaction will appear in the 2026 crypto transaction record.

> *This scenario is built on Architecture C. In Architecture A, Steps 4 and 6 swap: direct on-chain TX instead of soft reserve, separate signature per transaction. In Architecture B, Step 6 is deferred to end-of-day batch; no separate on-chain TX for Alex's transaction.*

---

12. Risk Matrix

Risk	Architecture A	Architecture B	Architecture C	Mitigation
Smart contract vulnerability	High	Low	Medium	Regular audit

Session key security	N/A	N/A	High	Device security
Soft reserve liquidity	Low	Management required	Low	Liquidity buffer
Co-signer censorship	Present	Present	Revocable	Guardian mechanism
Travel Rule compliance	Low	Attribution problem	Additional design	Compliance infrastructure
MiCA custody interpretation	Contested	Contested	Contested	Legal opinion
Card network rule change	Present	Present	Present	Multiple BIN sponsors
FX rate risk	Low (instant)	Medium (deferred)	Low	Hedge mechanism
Systemic crypto crash (ESMA TRV No.1/2026: October 2025 crypto market sudden value loss)	High	High	High	Liquidity buffer; on-chain TX delay scenario should be tested

> *Operational Note: The concepts of chargeback and cashback are frequently confused by users. Chargeback is a dispute resolution mechanism operating under card network rules and may give rise to a reimbursement obligation. Cashback is the card issuer's spending reward program; it operates as a completely separate process. It is recommended that the card agreement define both under separate headings.*

---

13. Summary

The self-custody card model cannot be reduced to a single technical architecture. Three different architectures, three different balances. Common point: private key is with the user. Divergence point: approval mechanism, on-chain timing, and the company's level of access.

- Architecture A: Every transaction on-chain. Most transparent, most independent. Travel Rule attribution is clear. Smart contract risk and auth latency management required.
- Architecture B: Fast auth, low gas, scalable. However, MPC holds a company shard and batch attribution complicates Travel Rule compliance.

References

Model 01: Self-Custody Card — Primary and Secondary Sources

I. Regulatory Documents — European Union

European Parliament and Council. Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA). Full force: December 30, 2024.

European Parliament and Council. Regulation (EU) 2023/1113 on Transfer of Funds (TFR). Effective December 30, 2024. Threshold-free.

European Banking Authority (EBA). No-Action Letter EBA/Op/2025/08. June 10, 2025. MiCA-PSD2 dual-license framework for EMT.

European Banking Authority (EBA). Opinion EBA/OP/2026/01. February 12, 2026. CASP classification under PSD2. Effective March 2, 2026.

European Commission. MiCA Implementing Regulations and ESMA CASP Transition Period Guidance. Q4 2024.

Council Directive 2023/2226 (DAC8). Effective January 1, 2026. Crypto-asset tax reporting by CASPs.

ESMA CASP License Tracker. March 12, 2026. 40+ licenses issued.

ECB Working Paper. Stablecoin Growth and EU Bank Deposits. March 3, 2026.

II. Regulatory Documents — United Kingdom

Financial Services and Markets Act 2026 (FSMA 2026). Enacted February 2026; effective October 2027.

Financial Conduct Authority (FCA). CP26/4 Cryptoassets Consultation Paper. Closed March 12, 2026.

FCA License Application Window: September 30, 2026 to February 28, 2027.

III. Regulatory Documents — United States

Guiding and Establishing National Innovation for US Stablecoins Act (GENIUS Act). Enacted July 2025.

Office of the Comptroller of the Currency (OCC). Card Program Final Rules. Target: July 2026.

FinCEN. Customer Identification Program (CIP) Requirements. 31 CFR § 1020.220.

Internal Revenue Service (IRS). Form 1099-DA. Mandatory for crypto brokers from 2025.

Bridge (Stripe). OCC Conditional National Bank Charter Approval. February 2026.

Kraken Financial (Wyoming SPDI). Federal Reserve Master Account (Kansas City Fed). March 4, 2026.

IV. Regulatory Documents — UAE, Singapore, Hong Kong

UAE Central Bank (CBUAE). Payment Token Services Regulation (PTSR). August 2025.

VARA Rulebook v2.0. June 2025. VASP license mandatory; broad custody interpretation.

Monetary Authority of Singapore (MAS). Payment Services Act (PSA). Part 9 VASP license mandatory since June 2025.

Hong Kong Monetary Authority (HKMA). Stablecoins Ordinance (Cap. 656). In force August 2025; first licenses March 2026.

V. Regulatory Documents — Turkey

Republic of Turkey. Law No. 7518 on Crypto-Asset Service Providers.

Capital Markets Board of Turkey (SPK). Communiqués III-35/B.1 and III-35/B.2. March 2025.

MASAK Regulation No. 29. June 28, 2025. Daily $3,000 / monthly $50,000 stablecoin withdrawal limit.

Central Bank of the Republic of Turkey (TCMB). Prohibition on Use of Crypto-Assets in Payments. April 2021.

MASAK Article 24/A. February 25, 2025. Full identity required for transfers of TRY 15,000+.

VI. International Standard Bodies

FATF. Targeted Report on Stablecoins and Unhosted Wallets. March 3, 2026. Stablecoins: 84% of illicit virtual asset transactions in 2025.

FATF. Updated Guidance for a Risk-Based Approach to Virtual Assets. 2023.

ISO 8583. Financial Transaction Card-Originated Messages. Card transaction messaging standard.

VII. Card Network Rules and Announcements

Visa / Cuy Sheffield. Stablecoin Settlement Run-Rate Statement. December 2025. Annualized ~$4.5B.

Visa / Stripe Bridge. Expansion to 100+ Countries. March 3, 2026. Four blockchains, four stablecoins.

Visa Core Rules and Visa Product and Service Rules. Chargeback thresholds: Visa 0.9%, Mastercard 1%.

Gnosis Pay. Safe AA Wallet on Gnosis Chain L2. EURe native settlement; MiCA CASP application ongoing.

VIII. Company Announcements and Public Sources

Artemis Analytics. Stablecoin Card Volume Report. January 2026. Volume: $100M/month (Jan 2023) to $1.5B/month (Dec 2025).

insights4vc. State of Stablecoin Cards Report. January 22, 2026.

Stablecoin Insider. Stablecoin Market Data. February 2026.

Elliptic. Blockchain Analytics and Compliance Platform. AML risk scoring and on-chain monitoring.

Chainalysis. Blockchain Analytics Platform. $200,000–$500,000/year; mixer/tumbler detection.

Fiat24 (SBA, Switzerland). On-chain IBAN; USDC/EUROC settlement; Arbitrum-based.

Kast (formerly Decaf). Solana-based; USDC rewards; LatAm remittance-focused.

MetaMask Card / Baanx. MetaMask wallet integration; USDC/DAI; Consensys infrastructure.

FCA. Wirecard Card Solutions Ltd: Immediate Suspension. June 26, 2020. Operational risk reference.

Lietuvos Bankas. Revolut Bank UAB AML Non-Compliance Penalty. €3.5 million. November 2023.