

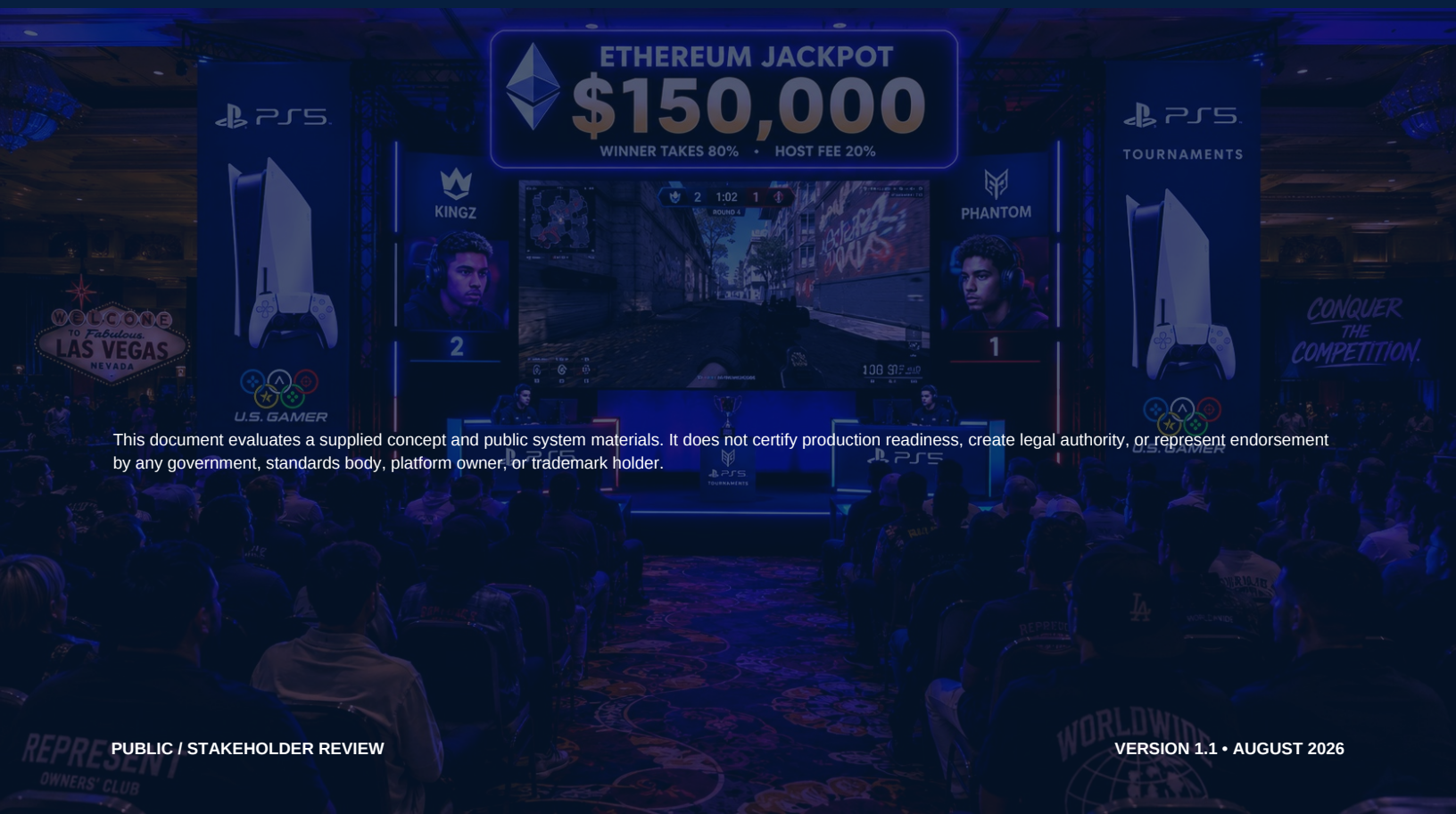


INSTITUTIONAL TECHNICAL WHITE PAPER

Pop-Up Community Wallet Technology

A governed reference architecture for temporary competitive events, self-custody digital assets, isolated offline game value, and a tamper-evident Records Vault

U.S. Gamer reference implementation • Policy, compliance, security, technology, and event-operations review



This document evaluates a supplied concept and public system materials. It does not certify production readiness, create legal authority, or represent endorsement by any government, standards body, platform owner, or trademark holder.

DOCUMENT CONTROL

Decision Brief

A concise statement of the decision, the evidence reviewed, and the conditions required before material deployment.

RECOMMENDED POSTURE Controlled pilot No material-value tournament until legal, security, and operations gates are closed.	REFERENCE BUILD v1.4.2 Public portal materials describe BTC, ETH, Postal Cash, NFC, biometric, recovery, and radio capabilities.
PRIMARY VALUE DOMAINS 3 silos Bitcoin mainnet, Ethereum mainnet, and isolated Postal Cash game value.	EVIDENCE PLANE Records Vault Signed wallet challenge, append-only event records, SHA-256 integrity envelopes, and public archive views.

Decision sought

Authorize a staged evaluation of the Pop-Up Community Wallet model as a **governed event settlement architecture**, not as a person-to-person betting product. Initial pilots should use Postal Cash or low-value test accounts while legal classification, money-transmission analysis, sanctions controls, software assurance, and event integrity controls are independently validated.

PROCEED Approve a bounded pilot with named owners, a written ruleset, explicit participant disclosures, a security test plan, and no unreviewed custody or commingling.	DO NOT INFER The CLARITY Act does not itself approve a tournament, waive state gaming law, remove BSA/AML obligations, or certify the U.S. Gamer implementation.
---	--

Evidence reviewed

SOURCE	USE IN THIS PAPER	LIMITATION
Sponsor-supplied concept brief	Problem framing and proposed Pop-Up Community Wallet model	Conceptual; not legal advice or implementation evidence
Live usgamer.org portal and Android imagery	Current public feature representation and user journey	Public presentation; not an independent functional certification
Live U.S. Gamer Records Vault	Record-only event lifecycle, signed wallet-control challenge, public archive, integrity operations, and SHA-256 envelopes	Observed public behavior; not a custody, legal-compliance, or cryptographic audit
U.S. Gamer Competition Rulebook v1.0	Integrity, safeguarding, anti-bullying, sanctions, and appeals model	Internal governance artifact; enforcement design remains to be tested
Congress.gov, CRS, FinCEN, OFAC, NIST, FTC	Primary-source legal, identity, sanctions, security, and privacy context	Authorities apply based on facts, roles, and jurisdiction

EXECUTIVE SUMMARY

A Community-Centric Settlement Model

The architectural shift is from merchant-centric payment acceptance to a temporary, rules-governed community with explicit value domains and independently reviewable receipts.

The Pop-Up Community Wallet model proposes that a physical competition venue temporarily become a managed digital community. Participants register a wallet, accept published event rules, authorize entry or game-value transfers, compete, and receive an outcome-based distribution under a disclosed settlement policy. The concept can reduce reliance on card terminals, chargeback workflows, and manual payout vendors while increasing settlement transparency.

The model is strongest when six conditions remain non-negotiable: **self-custody, published rules, separated value domains, participant intent, auditable evidence, and an independent record plane**. The U.S. Gamer Records Vault closes a critical evidence gap by preserving authenticated competition envelopes and integrity hashes without representing itself as a wallet custodian or automatic settlement engine. The model becomes materially riskier when an organizer takes discretionary custody, hides fees, blurs game value with real assets, permits underage or sanctioned participation, or represents competition entry as legally exempt without jurisdiction-specific analysis.

STRATEGIC VALUE

A common mobile chassis can support real-asset settlement and a no-real-value game mode while preserving a consistent event experience.

POLICY BOUNDARY

This paper treats competition administration as distinct from individualized wagers; legal classification still depends on event design and governing law.

Executive findings

- **Architecture:** The three-silo model is conceptually sound only if Bitcoin, Ethereum, and Postal Cash state, identifiers, histories, and authorization paths remain isolated.
- **Security:** Strong local biometric intent is useful but insufficient by itself. Key storage, transaction construction, address verification, anti-replay, dependency governance, and recovery controls require independent assessment.
- **Compliance:** The organizer's actual role determines exposure. Accepting and transmitting value for others can trigger a different analysis from software that merely enables a user-controlled transfer.
- **Competition integrity:** Published rules, eligibility, anti-cheating, anti-bullying, anti-retaliation, dispute resolution, signed wallet-control challenges, and hashed event envelopes are foundational controls, not optional community features.
- **Agile settlement:** Participant-controlled BTC and ETH can serve as portable settlement or prize-funding assets for approved pop-up events, while the Records Vault preserves the rules-to-result evidence chain without taking custody.
- **Deployment:** Postal Cash offers the safest operational proving ground because it is represented as isolated game value with no blockchain or real-world monetary value.

Institutional recommendation

Proceed through gated pilots: first with no-real-value Postal Cash, then with test networks or low-value accounts, and only later with material mainnet value after independent legal opinions, threat modeling, code review, penetration testing, transaction-reconciliation testing, and operator training. Every pilot should produce a Records Vault envelope linking the approved rules, responsible officials, result evidence, settlement references, and any dispute or appeal. Treat every public claim as a control obligation that must be evidenced in operation.

OPERATING CONTEXT

Why Tournament Payments Fragment

Competitive events often assemble temporary operations on top of permanent financial infrastructure that was not designed for short-duration, community-governed settlement.

DIMENSION	CONVENTIONAL STACK	POP-UP COMMUNITY MODEL
Acceptance	Card terminal, payment gateway, merchant account	Participant-controlled wallet or isolated game-value account
Authorization	Issuer and processor approval	Device intent, event rule acceptance, and network validation
Settlement	Processor batches and bank payout	Blockchain confirmation or local offline transfer
Reversibility	Chargebacks and processor disputes	Blockchain finality; policy-based event correction must be separate
Payout	Manual award, ACH, check, or vendor disbursement	Published rule engine to winner wallet or game-value account
Evidence	Processor reports plus organizer spreadsheets	Signed transaction record, SHA-256 event envelope, public archive, and governance record
Geography	Processor and banking coverage	Network access plus jurisdiction, sanctions, and identity controls
Failure mode	Processor outage, frozen merchant account, reconciliation error	Key loss, wrong address, chain congestion, replay, device compromise

The architectural opportunity

A pop-up model does not eliminate intermediaries or law. It **reassigns responsibility**. The participant assumes more responsibility for keys and addresses; the organizer assumes more responsibility for rule clarity, eligibility, event integrity, fee disclosure, sanctions screening where applicable, dispute handling, and evidence retention; the software operator assumes more responsibility for secure transaction construction and truthful user interfaces.

POTENTIAL EFFICIENCIES

Fewer payment-vendor handoffs, direct receipts, common wallet UX, rapid deployment, and more transparent fee display.

TRANSFERRED RISKS

Irreversible loss, volatile network fees, chain congestion, compromised recovery material, sanctions exposure, and inconsistent state-law treatment.

CONCEPT OF OPERATIONS

From Venue to Governed Digital Community

The temporary community is created by rules, roles, identity, authorization, and evidence—not by the wallet alone.



Seven-stage operating cycle

STAG E	CONTROL POINT	MINIMUM EVIDENCE
1	Publish rules	Define eligibility, value domain, entry, prizes, organizer compensation, refunds, conduct, disputes, and shutdown conditions.
2	Register participants	Verify age and identity to the level required by jurisdiction and risk; bind a player identity to an approved device and wallet.
3	Authorize entry	Present destination, amount, asset, network charge, service fee, and event identifier before strong user confirmation.
4	Run competition	Monitor match integrity, conduct, device status, anti-cheating signals, and operational exceptions.
5	Verify result	Require dual control or independent validation before a payout instruction is released.
6	Settle outcome	Execute the published distribution, record transaction identifiers, and disclose pending/final status.
7	Seal vault record	Create the append-only competition envelope, bind its SHA-256 hash, publish the permitted record view, and preserve disputes, appeals, and incident evidence.

Role separation

PARTICIPANT Controls keys Verifies destination, amount, network, fee, and biometric intent.	ORGANIZER Controls event Publishes rules, verifies results, handles disputes, and preserves records.
SOFTWARE OPERATOR Controls code Builds, signs, distributes, monitors, patches, and truthfully describes the app.	INDEPENDENT REVIEWER Controls assurance Tests security, reconciles records, and validates governance claims.

REFERENCE ARCHITECTURE

Separated Value Domains, Shared Control Plane

A common mobile chassis can present a consistent event experience, but real-asset and no-real-value domains must remain technically and operationally isolated.

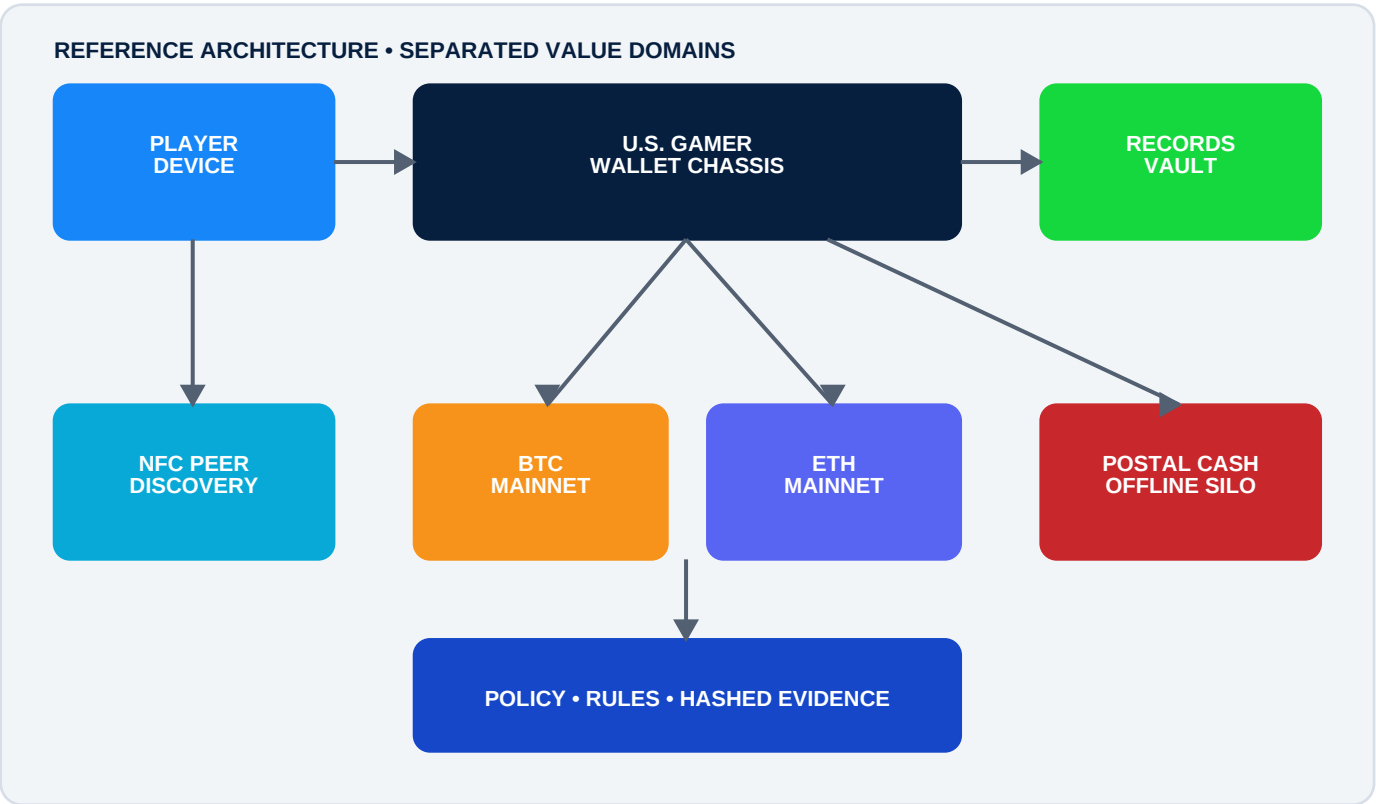


Figure 1. Target reference architecture. The Records Vault observes rules, outcomes, and receipts; it must remain separate from wallet custody and automatic settlement.

Architectural requirements

CONTROL	TARGET REQUIREMENT
Value-domain isolation	Separate key material, state, histories, transaction builders, network identifiers, fee logic, and error handling for BTC, ETH, and Postal Cash.
Intent binding	Bind biometric authorization to a canonical transaction summary that includes asset, network, destination, amount, event identifier, and all fees.
Records Vault	Store the signed ruleset hash, participant acknowledgment, match identifier, result authority, settlement reference, status transitions, and integrity envelope without collecting private keys.
No hidden custody	Do not pool participant funds or permit discretionary operator transfers without a separately approved custody and compliance model.
Fail-closed behavior	Reject cross-silo, wrong-network, malformed, replayed, stale, and unverifiable requests before presenting an approval prompt.
Observability	Record security events and settlement state without collecting recovery phrases, private keys, raw biometrics, or unnecessary personal data.

SYSTEM EXPERIENCE

Public Portal and Mobile Wallet

The user experience joins deployment, governance, self-custody wallets, isolated game value, event records, and media in one branded operating surface.

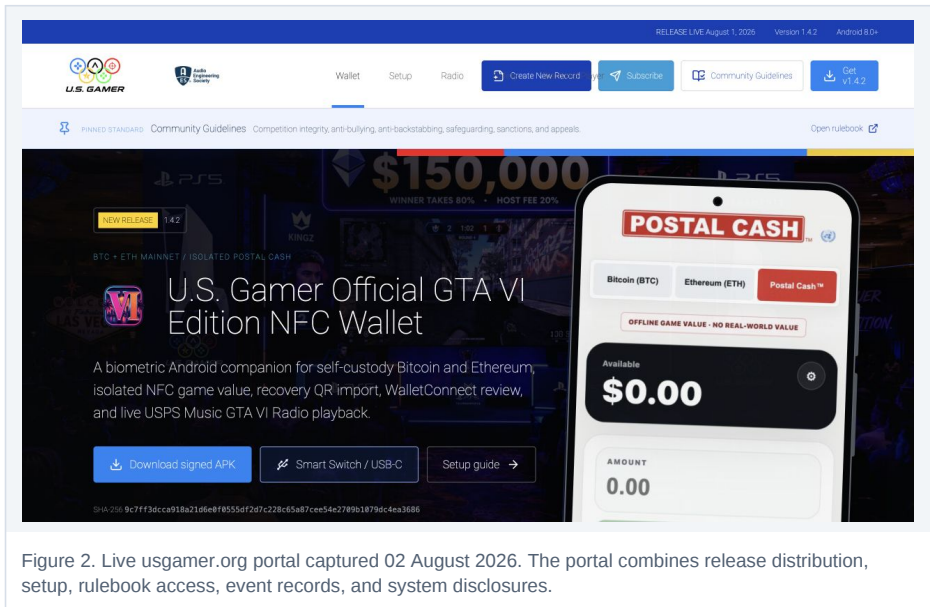


Figure 2. Live usgamer.org portal captured 02 August 2026. The portal combines release distribution, setup, rulebook access, event records, and system disclosures.

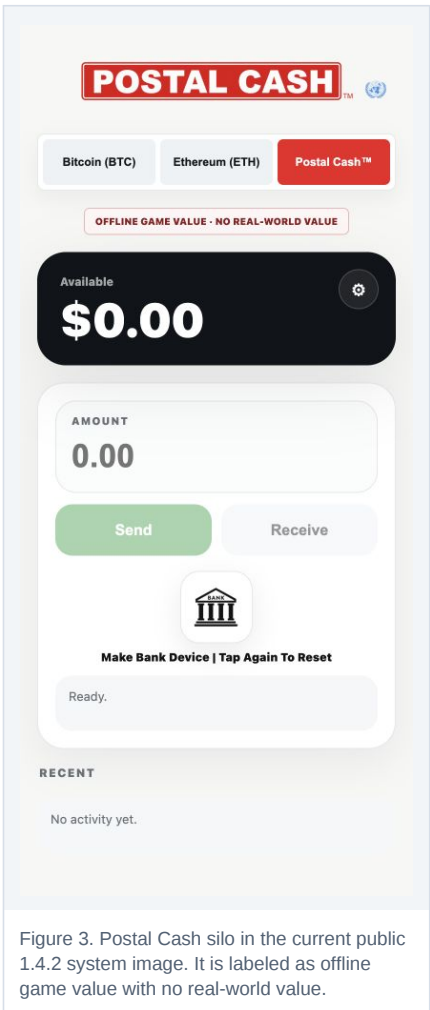


Figure 3. Postal Cash silo in the current public 1.4.2 system image. It is labeled as offline game value with no real-world value.

Experience principles

- State the active value domain before the amount.
- Keep the approval summary stationary and complete.
- Use plain-language pending, sent, settled, failed, and reversed-by-policy states.
- Show network charges separately from service fees.
- Distinguish external-wallet export from NFC event sends.
- Place rules, support, disputes, and record creation near the transaction journey.

The public portal is a distribution and education surface. It should not request wallet access unless a user deliberately enters a separate authenticated event flow. Download integrity, release identity, supported-device policy, and revocation instructions should remain visible and machine-verifiable.

RECORDS VAULT

The Trusted Record Layer

The Records Vault gives a temporary event a durable, independently inspectable evidence plane while expressly remaining outside wallet custody and automatic settlement.

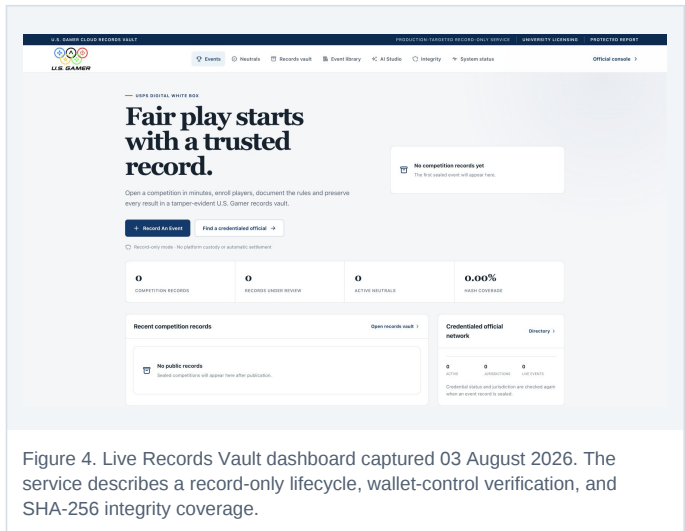


Figure 4. Live Records Vault dashboard captured 03 August 2026. The service describes a record-only lifecycle, wallet-control verification, and SHA-256 integrity coverage.

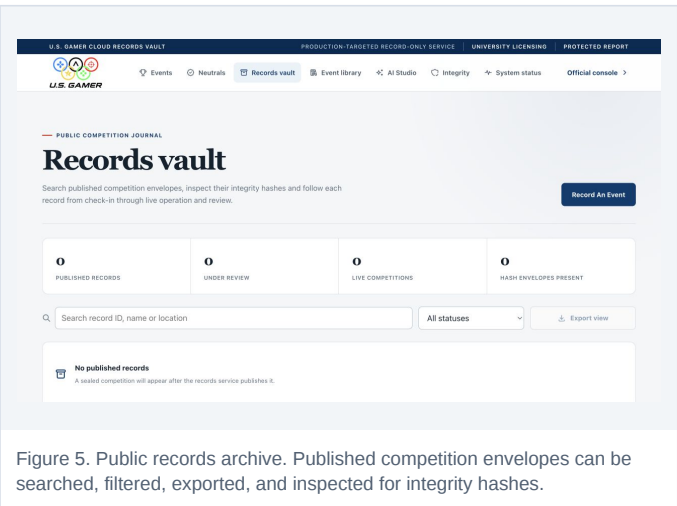


Figure 5. Public records archive. Published competition envelopes can be searched, filtered, exported, and inspected for integrity hashes.

The live service states that event creation is authenticated and append-only, wallet ownership is demonstrated through a signed challenge, amounts are stored in integer base units, and accepted records receive a SHA-256 integrity hash.[13][14] This creates a verifiable chain from rules and officials to result, settlement reference, review, and archive without requiring the vault to possess participant recovery material or sign asset transfers.

BOUNDARY Record-only No platform custody and no automatic settlement are claimed by the live service.	WALLET PROOF Signed challenge The official proves control of a public wallet without a transaction or gas fee.
INTEGRITY SHA-256 envelope Accepted records receive a content-integrity anchor for later comparison.	PUBLIC UTILITY Searchable archive Permitted event envelopes expose lifecycle state and hashes without exposing private keys.

INSTITUTIONAL ADVANTAGE

The vault separates the evidence function from the asset function. That division reduces pressure to centralize participant funds merely to obtain a common event ledger and gives reviewers a consistent record even when settlement occurs on different networks or in isolated Postal Cash.

AGILE MOBILE BACKING

BTC and ETH for Rules-Governed Pop-Up Play

Participant-controlled Bitcoin and Ethereum can fund or settle authorized competition outcomes at temporary venues while the Records Vault preserves the evidence chain required by U.S. Gamer rules.

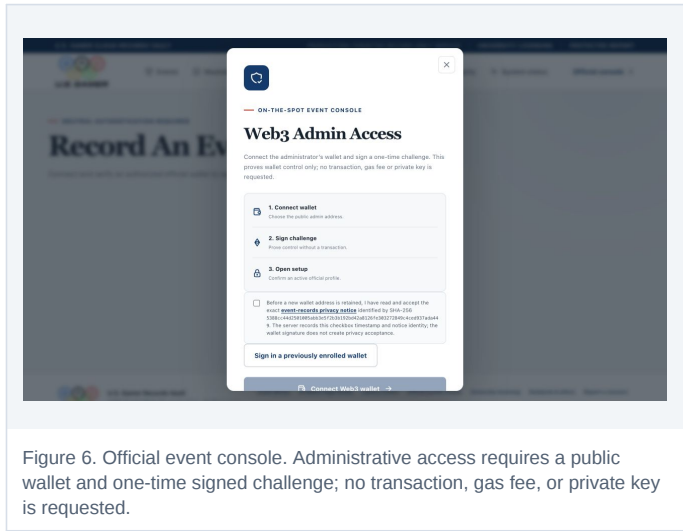


Figure 6. Official event console. Administrative access requires a public wallet and one-time signed challenge; no transaction, gas fee, or private key is requested.

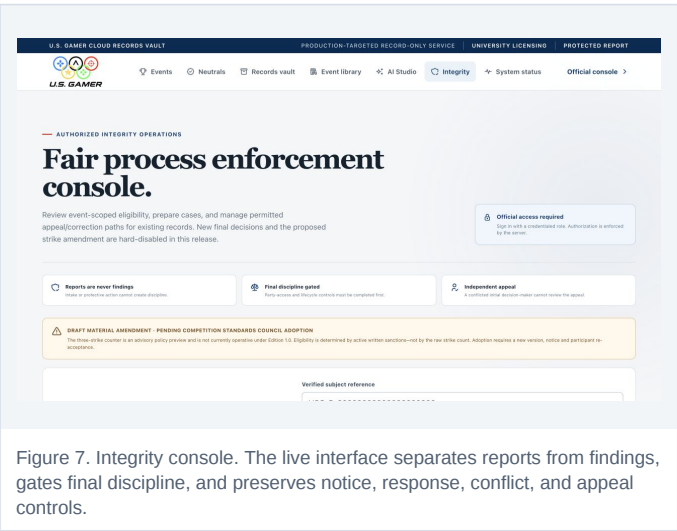


Figure 7. Integrity console. The live interface separates reports from findings, gates final discipline, and preserves notice, response, conflict, and appeal controls.

MEANING OF BACKING

In this paper, BTC or ETH ‘backing’ means that participant-owned digital assets are the disclosed settlement asset or prize-funding source under an approved event ruleset. It does not mean a peg, platform guarantee, insured deposit, redemption promise, escrow service, or custody claim.

MOBILE ADVANTAGE	CONTROL THAT MAKES IT DEFENSIBLE
Rapid venue deployment	A supported Android device can join a short-duration event without installing a merchant terminal stack; the event still requires named officials and a published ruleset.
Portable self-custody	Participants keep their own BTC or ETH keys; the event and vault receive only the minimum public identifiers and evidence references they require.
Chain-native receipts	Transaction IDs and confirmation state can be referenced in the competition envelope without rewriting blockchain history or treating a network receipt as proof of a match result.
Rules-to-record traceability	Ruleset hash, event ID, officials, participant acknowledgments, result authority, settlement reference, disputes, and appeals can be preserved as one evidence journey.
Jurisdictional modularity	Event configuration can cap value, restrict eligibility, choose Postal Cash, test networks, or mainnet, and stop deployment where law or operating controls are unresolved.
No hidden custody	The Records Vault authenticates officials and preserves records; it does not request recovery phrases, sign transfers, pool assets, or automatically distribute prizes.

This architecture does not legalize wagering, waive state gaming law, eliminate sanctions or consumer-protection duties, or establish that any event is permissible. Mainnet use remains contingent on the event design, participant roles, jurisdiction, custody facts, tax treatment, and independent legal and security review. The Records Vault supplies evidence; it does not supply legal authority.[15][16]

VALUE ARCHITECTURE

Three Wallet Silos, Three Risk Profiles

A single interface does not make the underlying assets equivalent. Controls must follow the value domain.

BITCOIN	ETHEREUM	POSTAL CASH
Public description Self-custody BTC mainnet wallet with UTXO settlement, address recovery, history, and NFC discovery.	Public description Self-custody ETH mainnet wallet with gas visibility, address recovery, history, and NFC discovery.	Public description Isolated offline competitive value, no blockchain, and no represented real-world monetary value.
Primary risks UTXO selection, fee estimation, change address handling, address substitution, irreversible broadcast.	Primary risks Gas estimation, chain ID, nonce management, address substitution, smart-contract and RPC dependencies.	Primary risks Replay, stale balance, double-spend across devices, reset abuse, counterfeit event state, player confusion.
Required evidence Test vectors, signed transaction decoding, watch-only reconciliation, recovery and export tests.	Required evidence Chain-ID enforcement, nonce tests, RPC-failure behavior, signed transaction decoding, reconciliation.	Required evidence Offline protocol specification, monotonic transaction IDs, duplicate rejection, multi-device consistency tests.

Non-negotiable isolation controls

- No request may cross from one value domain into another through a shared identifier, cached amount, stale NFC payload, deep link, or UI state.
- The active domain must be explicit in the approval screen and cryptographically bound to the transaction or offline transfer record.
- Postal Cash must never display exchange rates, withdrawal paths, or language implying redeemability for fiat or digital assets.
- A recovery or export action in one domain must not reveal, modify, or reset key material or history in another domain.

PILOT RECOMMENDATION

Use Postal Cash to validate tournament rules, role separation, NFC reliability, dispute handling, accessibility, and event records before introducing any material-value asset.

SETTLEMENT MODEL

Disclosure Before Authorization

Every value movement should be explainable as a rule-based instruction, not a hidden processor decision or an individualized wager.

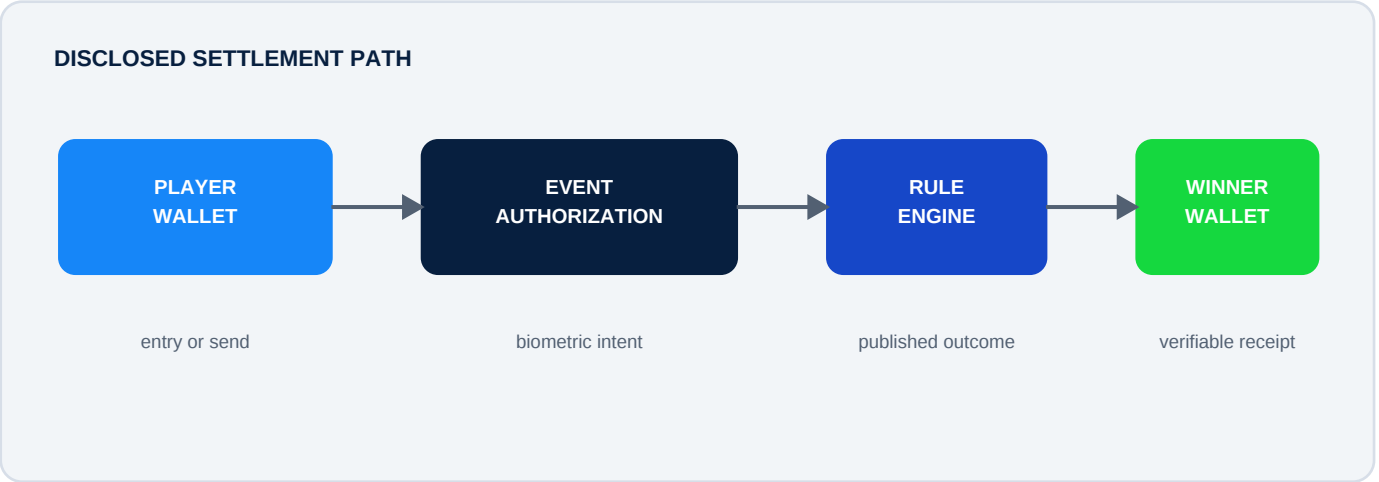


Figure 8. Target settlement path. The event authorization layer verifies intent and policy; the rule engine verifies the published outcome; the network or offline protocol produces the receipt.

Fee and accounting policy

ACTION	USER DISCLOSURE	ACCOUNTING TREATMENT
BTC or ETH NFC send	Recipient, asset, network, amount, blockchain charge, U.S. Gamer service fee, total debit	Separate organizer/service revenue from pass-through network charges; preserve transaction ID and event ID
BTC or ETH external export	Destination, asset, network, amount, network charge; public materials state no U.S. Gamer export fee	No service-fee revenue; reconcile only user-authorized asset movement and network charge
Postal Cash transfer	Player, amount, event, no-real-value notice; public materials state no service or network fee	Event ledger only; prohibit conversion, redemption, or treatment as cash equivalent
Event correction	Reason, authority, affected record, correction mechanism, and appeal path	Never rewrite blockchain history; issue a new corrective event record and, if applicable, a separate authorized transfer

Reconciliation minimum

AUTHORIZATION Intent record Canonical summary acknowledged by the participant.	EXECUTION Network receipt Transaction ID, confirmations, status, and error state.
COMPETITION Outcome record Ruleset hash, result authority, and payout allocation.	FINANCE Daily control Opening state + authorized changes = closing state, by value domain.

Any organizer-controlled service fee must be displayed before approval, legally reviewed, and tied to a disclosed service. A blockchain network charge is not organizer revenue. A flat service fee can become disproportionate on small transfers; product governance should set minimum and maximum transaction policies and monitor effective fee rates.

IDENTITY AND KEY MANAGEMENT

Strong Intent Without Centralizing Secrets

Local biometrics can activate a protected device credential, but the design must not treat a biometric match as a complete security architecture.

PREFERRED MODEL

User keys remain in platform-protected storage; biometrics activate a device-bound cryptographic operation; the app never receives raw biometric templates.

PROHIBITED MODEL

Recovery phrases, private keys, or biometric artifacts must not be sent to event servers, analytics systems, support channels, or public records.

Target authorization controls

CONTROL	TARGET IMPLEMENTATION
Device binding	Bind a cryptographic key to a supported Android device and secure hardware where available; record attestation posture without overstating assurance.
Biometric intent	Require strong local biometric confirmation for wallet opening, sends, exports, recovery import, key reveal, connection approvals, and security-setting changes.
Trusted display	Show the exact asset, chain, destination, amount, all fees, event ID, and request origin in a native confirmation surface.
Recovery	Accept only validated BIP-39 material through a private, explicit flow; warn that any observer of a phrase or QR can control the wallet.
Export	Require fresh intent, full destination review, and a clear statement that export is irreversible; do not impose a hidden service fee.
Session	Reauthenticate after risk events, inactivity, background return, device-state change, or security-sensitive navigation.

NIST alignment

NIST SP 800-63B-4 states that a biometric is not an authenticator by itself; it is used with a physical authenticator, and local biometric verification is preferred to central biometric comparison. The same publication emphasizes authenticated protected channels, replay resistance, phishing resistance at higher assurance levels, and explicit authentication intent.[6] These principles support a device-bound, local-confirmation design but do not certify any specific wallet implementation.

LOCAL COMMUNICATIONS

NFC Is a Discovery Channel, Not a Trust Decision

Proximity reduces friction; it does not prove recipient identity, transaction freshness, asset compatibility, or event authority.

A production NFC protocol should exchange the minimum information required to propose a transaction. The sender independently constructs and signs the final transfer after validating the peer payload, active value domain, network, event, and freshness. No peer should be able to cause an automatic debit, bypass the native confirmation screen, or replay a previously approved request.

Required message fields

FIELD	PURPOSE	VALIDATION
Protocol version	Prevent silent incompatibility	Reject unsupported versions; no permissive fallback
Value-domain ID	Bind BTC, ETH, or Postal Cash	Exact match to active silo; reject cross-domain messages
Network / chain ID	Prevent wrong-network transfers	Exact allowlist; include in signed or authenticated transcript
Recipient identifier	Specify destination	Canonical decode, checksum, type, and full user review
Event ID and role	Associate the request with an approved competition	Known active event; role authorization; ruleset hash
Nonce and expiry	Prevent replay and stale requests	Single-use nonce, short validity, monotonic local record
Amount proposal	Reduce typing without forcing payment	Never auto-approve; display full amount and fee summary
Authentication tag	Protect integrity where the offline protocol supports it	Verify before presentation; fail closed on mismatch

Offline Postal Cash consistency

- Use a monotonic transaction sequence or cryptographically unique transfer identifier and reject duplicates on every device.
- Always read the peer's current authoritative state before crediting or debiting; never rely on a cached card or device panel amount.
- Define interruption-safe commit semantics so moving devices apart cannot credit both parties or strand one side in an ambiguous state.
- Provide a visible reconciliation and reset procedure for event operators without granting them silent access to player balances.

CONTROL OBJECTIVE

The same event and value-domain rules must govern device-to-device, NFC, recovery, history, and export paths. A feature-specific exception is a new attack surface.

COMPETITION GOVERNANCE

Integrity Is Part of the Payment System

A wallet can settle an outcome, but only a governed competition can establish which outcome is legitimate.

The supplied U.S. Gamer rulebook establishes a foundation for competitive integrity, safeguarding, anti-bullying, anti-backstabbing, sanctions, and appeals. A production program should turn those principles into enforceable roles, evidence standards, response times, and transparent consequences.

DOMAIN	MINIMUM STANDARD	EVIDENCE
Eligibility	Age, jurisdiction, identity, device, wallet, and sanctions eligibility before entry	Participant record and screening disposition
Published rules	Versioned rules, prize structure, fees, refunds, game settings, disconnections, ties, and appeals	Signed ruleset hash and acknowledgment
Anti-cheating	Approved software, device policy, telemetry boundaries, observer roles, and evidence chain	Match evidence package and reviewer decision
Anti-bullying	No harassment, threats, humiliation, stalking, discrimination, or coordinated exclusion	Moderation record, safeguarding action, and appeal
Anti-backstabbing / retaliation	No sabotage, bad-faith reporting, retaliatory exclusion, doxxing, or abuse of private information	Incident chronology, evidence, proportional sanction
Dispute resolution	Independent reviewer, defined filing window, conflict disclosure, written outcome	Case file and final disposition
Payout control	Result validation separated from transfer approval; dual control for material value	Outcome certificate and settlement receipt
Exclusion / blacklist	Criteria, duration, notice, data minimization, review, and appeal; avoid unbounded or secret lists	Decision authority, reason code, expiry, appeal status

COMMUNITY PROTECTION

Safety rules should protect participants without becoming a tool for retaliation. Confidential reports need trained review, limited access, and a non-retaliation rule.

DUE PROCESS

Any ban or blacklist affecting participation should have documented criteria, notice, proportionality, retention limits, correction, and an appeal path.

REGULATORY POSTURE

A Framework Context, Not a Blanket Exemption

Legal treatment follows the facts: who accepts value, who controls it, who transmits it, how prizes are funded, and where participants and operators are located.

Congress.gov records that H.R. 3633, the Digital Asset Market Clarity Act of 2025, passed the House on 17 July 2025 and was received in the Senate and referred to the Committee on Banking, Housing, and Urban Affairs on 18 September 2025.[1] The Congressional Research Service describes a proposed allocation of digital-commodity oversight between the CFTC and SEC.[2] This paper does not assume enactment, implementing rules, or that the bill resolves event, gaming, money-transmission, consumer-protection, tax, or sanctions questions.

Regulatory decision matrix

QUESTION	WHY IT MATTERS	PRE-LAUNCH EVIDENCE
Is the operator accepting and transmitting value for others?	FinCEN analysis distinguishes users from certain administrators, exchangers, and money transmitters based on activity.[3][4]	Written BSA/MSB analysis of each role and flow
Is the contest a game of skill, gambling, a sweepstakes, or another regulated activity?	Classification varies by jurisdiction, game mechanics, entry, prize, chance, and operator conduct.	State-by-state and venue-specific gaming counsel memorandum
Are participants or transactions sanctions-restricted?	OFAC states that sanctions obligations apply to virtual-currency activity and recommends a risk-based compliance program.[5]	Sanctions policy, screening design, escalation, recordkeeping
Are fees and claims clear?	Consumer-protection risk rises when disclosures are hidden, claims overstate security, or app behavior conflicts with promises.[8][9]	Approved disclosures, fee tests, marketing substantiation
Are minors involved?	Age, privacy, contracting capacity, prizes, and safeguarding may change the control model.	Age gate, parental-consent analysis, youth-safety controls
Are tax and reporting obligations triggered?	Entry fees, prizes, service fees, and digital-asset dispositions can have distinct reporting consequences.	Tax counsel memorandum and operational reporting plan

REQUIRED DISCLAIMER

Do not market the CLARITY Act, self-custody, blockchain settlement, or a competition ruleset as an exemption, approval, license, or government endorsement. Obtain counsel for every jurisdiction and operating role.

SECURITY AND PRIVACY

Target Control Framework

The program should govern risk through the NIST CSF 2.0 functions and apply identity controls consistent with NIST SP 800-63B-4 where appropriate.

CSF FUNCTION	U.S. GAMER TARGET OUTCOME	PRIORITY EVIDENCE
GOVERN	Named risk owner; legal and security gates; supplier policy; vulnerability disclosure; truthful claims	Risk register, RACI, approval minutes, supplier inventory
IDENTIFY	Asset, data, key, network, dependency, device, venue, and event inventories	System/data-flow diagrams, SBOM, threat model
PROTECT	Secure key storage, least privilege, signed builds, strong intent, code review, secrets management	Build provenance, secure-storage tests, access review
DETECT	Tamper, replay, double-spend, wrong-chain, RPC anomaly, failed auth, and reconciliation detection	Alert catalog, test results, monitoring coverage
RESPOND	Containment, user notice, transaction hold policy where possible, venue escalation, evidence preservation	Incident plan, contact tree, tabletop record
RECOVER	Known-good release, key and wallet recovery guidance, record restoration, participant remediation	Recovery runbook, backup test, release rollback test

Privacy-by-design minimum

COLLECT LESS
Do not collect recovery phrases, private keys, raw biometric data, full device contents, or unrelated contacts and location.

EXPLAIN USE
Provide concise, just-in-time notices for identity, event records, sanctions screening, telemetry, and support.

SEPARATE RECORDS
Keep public competition results separate from identity, security events, and dispute evidence.

LIMIT RETENTION
Use purpose-based retention schedules and delete or de-identify data when no longer required.

PROTECT ACCESS
Apply least privilege, hardware-backed administrator MFA, immutable audit logs, and periodic access reviews.

HONOR PROMISES
FTC guidance emphasizes privacy by design, data minimization, transparency, consent for sensitive data, and reasonable security.[8][9]

Assurance work products

Before material use: independent architecture review; mobile application security test; dependency and SBOM review; cryptographic test vectors; transaction-construction review; NFC protocol test; replay/double-spend test; privacy impact assessment; incident tabletop; and documented remediation closure.

OPERATIONAL RESILIENCE

Design for Interrupted Events and Irreversible Transfers

A temporary event needs a permanent plan for outages, mistakes, disputes, and recovery.

The operating model should distinguish four states: **event unavailable**, **wallet unavailable**, **network unavailable**, and **settlement uncertain**. Each state requires a predetermined action that preserves participant rights and prevents duplicate or ambiguous transfers.

SCENARIO	DEFAULT RESPONSE	RESTART / CLOSURE CRITERIA
NFC interruption	Stop the transfer; show an unambiguous incomplete state; query both peers before retry	No debit or credit unless both sides agree on one transfer ID
RPC or chain outage	Disable new mainnet sends; preserve locally signed but unbroadcast state separately	Independent network health plus reconciliation of pending transactions
Wrong destination detected before signature	Cancel without side effect and clear the request	Fresh discovery and full re-authorization
Wrong destination after broadcast	Escalate as irreversible loss; do not mislabel as reversible or settled to the intended party	Incident record, participant notice, legal and support review
Device loss	Revoke event registration for the lost device; do not claim to revoke blockchain keys	Secure wallet recovery on a trusted device and new event binding
Result dispute	Pause organizer-initiated payout if policy permits and no transaction has been broadcast	Independent decision within published time; written outcome
Compromised release	Block download, publish advisory, revoke event eligibility, preserve evidence	Signed clean build, independent validation, participant remediation
Venue connectivity loss	Switch to approved offline mode only if the event rules and value domain permit it	Complete reconciliation before any mainnet settlement

Target service objectives for a pilot

CRITICAL INCIDENT 15 min Target acknowledgement by the named incident lead.	PARTICIPANT NOTICE 60 min Target initial notice for a confirmed material incident.
EVENT RECORD 0 loss No accepted competition or settlement record may be silently discarded.	RECOVERY TEST Quarterly Run build rollback, record restore, and operator tabletop.

These are proposed pilot objectives, not measured current-state service levels. Formal service levels should be approved only after load, failure, and recovery testing.

DEPLOYMENT MODEL

From No-Value Pilot to Managed Mainnet Event

Deployment gates should increase assurance faster than they increase value at risk.

TIER	PERMITTED USE	MANDATORY GATES
0 • Lab	Emulator, unit tests, protocol simulation, no participant data	Threat model; test vectors; reproducible build; automated tests
1 • Postal Cash pilot	Invited participants; no real-world value; limited venue	Ruleset; NFC consistency test; safeguarding; disputes; record reconciliation
2 • Test-network / low-value	Approved test networks or controlled low-value accounts	Independent security review; key-recovery test; transaction decoding; incident tabletop
3 • Managed mainnet pilot	Named jurisdiction, adult participants, capped value, named operators	Legal opinions; sanctions design; penetration test; insurance/risk acceptance; dual control
4 • Scaled event	Multiple venues or larger value under a formally governed program	Production SLOs; continuous monitoring; external audit; vendor management; regulator engagement as applicable

Distribution and device posture



Figure 9. Managed-device concept image supplied with the public portal.

Signed release controls

- Publish APK/AAB hash, signer identity, version, support window, and revocation status.
- Use a documented, access-controlled signing process with offline recovery and key rotation.
- Treat Smart Switch or USB-C restore media as a software-supply-chain channel requiring manifest, signature, provenance, and malware scanning.
- Re-enroll device biometrics after restore and independently verify wallet addresses and recovery material.
- Do not represent consumer sideloading warnings as proof of malware or proof of safety.

MANAGED-DEVICE PRINCIPLE

A restored image can accelerate deployment, but it also magnifies a compromised build. No event should trust an image merely because it came from branded media.

ANCILLARY SUBSYSTEM

Audiophile Media Without Expanding Wallet Trust

The Diamond Player and USPS Music presentation can enrich the event experience, but media processing should not share secrets, authorization state, or privileged wallet permissions.

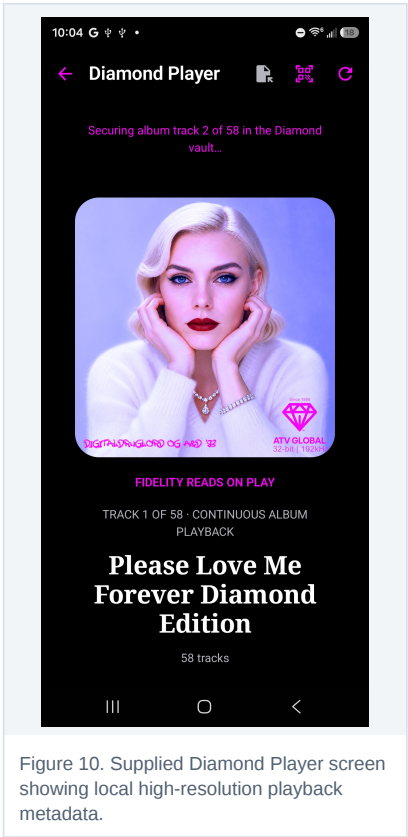


Figure 10. Supplied Diamond Player screen showing local high-resolution playback metadata.

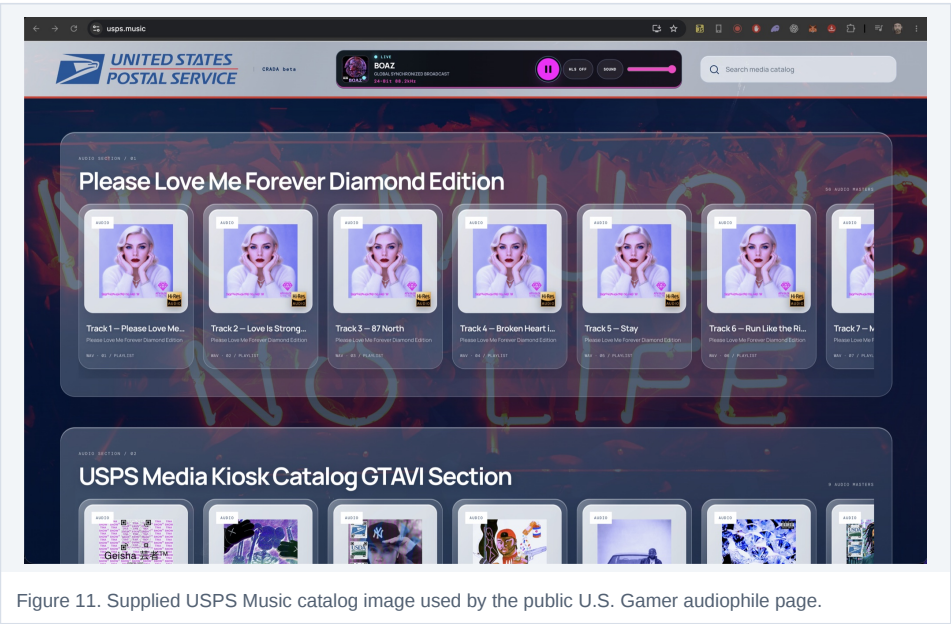


Figure 11. Supplied USPS Music catalog image used by the public U.S. Gamer audiophile page.

Separation requirements

MEDIA CAPABILITY	WALLET BOUNDARY
HLS and WAV-direct playback	No access to private keys, recovery material, wallet database, transaction builder, or NFC payment payloads
QR / media handoff	Strict content-type and size validation; never interpret media QR data as a wallet command
Background playback	No relaxation of biometric timeout, foreground confirmation, or protected-screen policy
DAC / headset metadata	Informational only; no effect on transaction authorization or event eligibility
Catalog and artwork	Content provenance, licensing, privacy, and telemetry reviewed independently from wallet security

Public portal materials state that the wallet includes radio controls while the standalone Diamond Player app is available through the supplied Smart Switch image. That packaging choice should not create hidden permissions or an undocumented dependency between media and financial functions.

MEASUREMENT AND EVIDENCE

Operate What Can Be Proved

A credible program reports control performance and failure rates, not just downloads, balances, or tournament volume.

Pilot scorecard

MEASURE	DEFINITION	PILOT TARGET / GATE
Authorization integrity	Approved transactions whose decoded payload exactly matches the displayed summary	100%; any mismatch halts the pilot
NFC duplicate rate	Duplicate credit or debit after retry, interruption, or replay testing	0 in test corpus and live pilot
Reconciliation variance	Difference between authorized event records and domain-specific ledger/network state	0 unexplained variance
Vault hash coverage	Accepted competition envelopes with a retrievable SHA-256 integrity hash and lifecycle state	100% of accepted records
Recovery success	Successful restore from valid recovery material on a clean supported device	100% of approved test cases
Cross-silo rejection	Wrong-domain or wrong-network requests rejected before approval	100% of negative tests
Biometric enforcement	Sensitive flows completed without required strong confirmation	0; fail closed
Dispute timeliness	Cases acknowledged and resolved within published service targets	>=95% within target
Safety response	Substantiated bullying, retaliation, or safeguarding reports with documented action	100% documented; trend reviewed
Security remediation	Critical/high findings closed before the next deployment tier	100% critical; risk acceptance for any high
Disclosure comprehension	Participants correctly identify asset, fees, irreversibility, and support path	>=90% in pre-pilot usability test

Minimum evidence package

BUILD Provenance Commit, dependencies, SBOM, signer, hash, test report.	EVENT Vault envelope Ruleset hash, acknowledgments, roles, result, settlement reference, integrity hash.
SETTLEMENT Receipts Authorization summary, transaction ID, confirmations, reconciliation.	GOVERNANCE Cases Incidents, disputes, moderation, sanctions, appeals, outcomes.

Evidence should be tamper-evident, access-controlled, purpose-limited, and retained only as long as required. Public competition records should contain the minimum necessary information and should not expose personal identity, private wallet recovery data, or security telemetry.

IMPLEMENTATION ROADMAP

Gated Delivery, Not Feature Accumulation

The shortest credible route to scale is a sequence of narrow pilots with explicit stop conditions.

WINDOW	PHASE	DELIVERABLES	EXIT GATE
0–30 days	Baseline	Freeze architecture; inventory code, dependencies, keys, domains, data, claims, and operator roles; establish risk owner and legal workstream.	Approved scope and threat model
31–90 days	Postal Cash pilot	Specify offline protocol; complete replay/interruption tests; finalize rules, safety, disputes, record model, and operator training.	No-value pilot with zero unexplained variance
3–6 months	Assurance	Independent mobile review, penetration test, cryptographic review, privacy assessment, incident tabletop, build provenance, and remediation.	Critical findings closed; high findings accepted or closed
6–9 months	Low-value test	Use controlled wallets/test networks; verify history, recovery, fee disclosure, reconciliation, and participant comprehension.	Legal and security gate for selected jurisdiction
9–12 months	Managed mainnet pilot	Capped value, adult participants, named venue, dual control, sanctions process, support and insurance posture.	Independent go/no-go review

Top program risks

ID	RISK	INHERENT	PRIMARY TREATMENT
R1	Regulatory misclassification	High	Jurisdiction-specific legal opinions; role and flow mapping; no exemption claims
R2	Key or recovery compromise	Critical	Hardware-backed storage, secure display, recovery isolation, independent crypto review
R3	Wrong-chain / wrong-address transfer	Critical	Canonical transaction review, chain binding, address validation, test vectors
R4	Offline duplicate or stale balance	High	Protocol specification, nonce/sequence, interruption-safe commit, reconciliation
R5	Software supply-chain compromise	Critical	Reproducible build, SBOM, signed provenance, protected signer, revocation
R6	Bullying, retaliation, or blacklist abuse	High	Confidential reporting, independent review, proportionality, appeal, retention limits
R7	Misleading affiliation or security claims	High	Claim substantiation, trademark review, clear independent-status disclosure
R8	Participant fee misunderstanding	Medium	Pre-approval total, service/network fee separation, comprehension testing

CONCLUSION

Proceed Only Through Evidence-Based Gates

The Pop-Up Community Wallet model is a credible architecture hypothesis. Its legitimacy will be earned through transparent rules, technical assurance, participant protection, and jurisdiction-specific compliance.

The model's central contribution is not simply a new payment interface. It is the idea that a temporary physical event can become a **governed digital community** with explicit membership, separated value domains, published competition rules, secure participant intent, verifiable settlement, and a durable Records Vault envelope.

That architecture can reduce operational fragmentation and increase transparency. It can also concentrate new risks: irreversible loss, key compromise, wrong-network transactions, offline replay, sanctions exposure, legal misclassification, privacy overcollection, and misuse of community sanctions. A responsible program therefore scales controls before it scales value.

The Records Vault materially improves the concept by separating authenticated event evidence from self-custody asset execution. It allows agile Android deployments to reference BTC or ETH settlement without turning the record service into a custodian, and it gives Postal Cash pilots the same rules-to-result evidence discipline. This is an architectural advantage, not a substitute for legal authority, operational competence, or independent assurance.

Go / no-go preconditions

GATE	REQUIRED CONDITION
Legal	Written analysis for event classification, money transmission, sanctions, consumer protection, tax, age, privacy, and the selected jurisdiction.
Security	Independent architecture, cryptography, mobile, NFC, supply-chain, and penetration testing with remediation closure.
Operations	Named owners, training, rules, disputes, incident response, reconciliation, participant support, and release revocation.
Evidence	Authenticated Records Vault envelope covering rules, officials, authorization, result, settlement reference, moderation, appeal, and incident evidence with privacy controls.
Pilot	Postal Cash no-value pilot completed without unexplained variance, duplicate transfer, cross-silo acceptance, or unresolved critical incident.

Recommended institutional position

CONDITIONAL PROCEED

Authorize a bounded no-real-value pilot and independent assurance program. Do not authorize material-value public competition until every precondition above is closed by an accountable owner and independently reviewed.

The public U.S. Gamer materials, live Records Vault, and supplied concept brief provide a coherent starting point. This white paper converts that starting point into a testable governance and control agenda. It should be maintained as a living artifact: each version must identify which statements describe current implementation, which are target requirements, and which remain unverified assumptions.

REFERENCES

Primary Sources and Project Materials

Sources were selected for authority and direct relevance. Access date: 03 August 2026.

[1] **U.S. Congress.** H.R. 3633 — Digital Asset Market Clarity Act of 2025, official status and actions.
<https://www.congress.gov/bill/119th-congress/house-bill/3633/all-info>

[2] **Congressional Research Service.** Crypto Legislation: An Overview of H.R. 3633, the CLARITY Act, IN12583, updated 30 September 2025.
<https://www.congress.gov/crs-product/IN12583>

[3] **Financial Crimes Enforcement Network.** Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001, 09 May 2019.
<https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models>

[4] **Financial Crimes Enforcement Network.** Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, 18 March 2013.
<https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>

[5] **U.S. Department of the Treasury / OFAC.** Sanctions Compliance Guidance for the Virtual Currency Industry, October 2021.
https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf

[6] **National Institute of Standards and Technology.** Digital Identity Guidelines: Authentication and Authenticator Management, NIST SP 800-63B-4, July 2025.
<https://doi.org/10.6028/NIST.SP.800-63B-4>

[7] **National Institute of Standards and Technology.** The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, 26 February 2024.
<https://doi.org/10.6028/NIST.CSWP.29>

[8] **Federal Trade Commission.** Marketing Your Mobile App: Get It Right from the Start.
<https://www.ftc.gov/business-guidance/resources/marketing-your-mobile-app-get-it-right-start>

[9] **Federal Trade Commission.** App Developers: Start with Security.
<https://www.ftc.gov/business-guidance/resources/app-developers-start-security>

[10] **U.S. Gamer.** Public portal and system materials, version 1.4.2.
<https://www.usgamer.org/>

[11] **U.S. Gamer Competition Standards Council.** U.S. Gamer Official Competition Rulebook, version 1.0, 2026.
<https://www.usgamer.org/downloads/US-Gamer-Official-Competition-Rulebook-v1.0-2026.pdf>

[12] **Sponsor-supplied concept brief.** Esports payment comparison and Pop-Up Community Wallet white-paper framing.
https://chatgpt.com/s/t_6a6fd2eb391081918186370e48fe8017

[13] **U.S. Gamer.** Records Vault dashboard and record-only competition lifecycle.
<https://events.usgamer.org/>

[14] **U.S. Gamer.** Public Records Vault archive and published competition envelopes.
<https://events.usgamer.org/records>

[15] **U.S. Gamer.** Official event console and wallet-control challenge.
<https://events.usgamer.org/record>

[16] **U.S. Gamer.** Integrity operations console, evidence standards, and appeal controls.
<https://events.usgamer.org/integrity>

[17] **U.S. Gamer.** Records Vault privacy notice, version 1.0.
<https://events.usgamer.org/privacy-notice-v1.0.html>

Legal and status notice

This is an independent technical and policy analysis prepared from sponsor-supplied and public materials. It is not legal, tax, investment, accounting, cybersecurity-certification, or regulatory advice. It is not an official publication of the White House, U.S. Department of the Treasury, U.S. Postal Service, United Nations, Audio Engineering Society, Sony, PlayStation, Rockstar Games, Take-Two Interactive, or any other referenced entity. Inclusion of names, marks, screenshots, or links does not imply endorsement, sponsorship, authorization, or affiliation. All trademarks and copyrighted materials remain the property of their respective owners.

Image notice

Figures reproduce or derive from assets supplied with the U.S. Gamer project and from the live public portal. Competition and venue imagery is illustrative. Product screens evidence presentation, not independently verified functionality. No representation is made that a depicted event, device, partner, agency, or platform has approved or deployed the system.