BITCOIN CUSTODY STANDARD

BCRI Benchmark Report

Bitcoin Custody Resilience Index (BCRI)

Structural Resilience and Complexity in Custody Architecture

A structural benchmark for evaluating Bitcoin custody systems across resilience and complexity.

Bitcoin Custody Standard (BCS)
Public Normative Framework for Bitcoin Custody
bitcoincustodystandard.org

Publication: BCS-BR-1.0
Version: 1.0
Document Class: Normative Framework
Status: Public, Citable
Aligned Standard: BCS-NS-1.1 (Normative Standard)
Publication Date: March 2026
Next Scheduled Review: March 2027
Steward: Bitcoin Custody Standard Initiative

NON-ENDORSEMENT NOTICE This publication benchmarks custody architecture *design types* as assessed under the BCS methodology. It does not constitute certification, regulatory guidance, or endorsement of any specific product, implementation, or service provider. Where named examples appear, they are illustrative of the architecture class and do not represent endorsement or a complete enumeration. Sections 2 and 3 are normative. Annex A is informative.

1 Executive Summary

The BCRI benchmark demonstrates that prevailing assumptions about Bitcoin custody resilience are structurally incorrect.

First, the highest levels of structural resilience are not achieved through institutional custody. The three highest-scoring architectures fall within distributed self-custody and collaborative multisig design classes: Self-Managed Multisig — Hi Resilience (97.5, AAA), Collaborative Multisig — Advised (96.5, AA+), and Self-Managed Multisig — Advanced (89.6, A+). The highest institutional architecture, Qualified Custodian, scores 93.7, below the two leading self-custody designs. These scores measure structural resilience, not convenience, service quality, regulatory simplicity, or operational ease. Institutional custody delivers compliance and operational convenience, but it cannot eliminate the structural constraints of delegated control: regulatory intervention risk, charter-dependent operating limits, and concentration within institutional legal frameworks. By contrast, the highest-scoring self-custody and collaborative architectures achieve greater resilience through direct control, geographic distribution, and reduced dependence on regulated intermediaries. Structural resilience is a property of design, not delegation.

Second, resilience efficiency peaks at a moderate level of operational complexity and declines beyond that point. As shown in Exhibit 4.2, excess resilience efficiency (ERE) — defined as resilience gained above the structural baseline per unit of operational complexity — reaches a maximum near Complexity Score (CS) ≈ 4.5 and decreases as complexity increases beyond this range. Although some institutional architectures retain strong absolute resilience, the institutional category is concentrated on the high-complexity side of the frontier, where efficiency is materially lower than among the leading moderate-complexity designs. The Corporate Bitcoin Treasury — the most governance-intensive architecture in the dataset — records the lowest ERE of any scored architecture: 25.1 at CS 8.2. Governance cannot substitute for structural design.

Third, custody failure operates on two independent axes. The benchmark establishes two structurally distinct failure modes: insufficient structure (fragility) and misallocated complexity (inefficiency). Each requires a different corrective intervention. A single-axis evaluation framework cannot distinguish them.

Bitcoin custody is a design problem under constraints, not a product choice. The efficient frontier peaks below institutional-level complexity.

Primary implication: Evaluate the architecture before the product. Key distribution, quorum design, coordination model, and geographic separation determine the resilience ceiling. The provider determines the implementation.

Structural Model of Custody Resilience

The Bitcoin Custody Resilience Index (BCRI) is a composite structural model that evaluates custody systems across time, coordination, and adversarial conditions.

At the dimensional level, the model evaluates five orthogonal resilience pillars:

- **Cryptographic Integrity**
- **Physical Distribution**
- **Operational Dependency**

- **Cognitive Reliability**
- **Temporal Resilience**

These pillars are intentionally defined as analytically distinct domains. Strength in one dimension does not eliminate weakness in another.

The pillars are aggregated into four structural components that capture different aspects of custody resilience:

- **Architecture Resilience (ARS)**
- **Coordination Health (CHS)**
- **Entropy Resilience (ERS)**
- **Exposure Resilience (XRS)**

The BCRI is defined as:

$$BCRI = f(ARS, CHS, ERS, XRS)$$

This formulation reflects a core principle of the Bitcoin Custody Standard:

Custody resilience is not a single property.

It arises from interacting structural conditions across key management, coordination, entropy, and exposure.

This benchmark does not refine existing custody evaluation methods.
It replaces them.

2 Methodology and Scope

This benchmark applies the BCRI methodology to 14 Bitcoin custody architecture types, producing scored comparisons across structural resilience and operational complexity. This section provides the terms, scope boundaries, and model parameters necessary to interpret the benchmark results. The public normative basis of the framework is described in BCS-NS-1.1.

Scope. This publication benchmarks Bitcoin *custody architecture types* at the level of structural design patterns, not specific products, implementations, or service providers. The unit of analysis is the custody architecture itself, including key distribution, quorum requirements, hardware configuration, connectivity model, dependency structure, recovery design, and coordination architecture.

The assessment evaluates structural resilience and operational complexity at the architecture level, including long-horizon recoverability, documentation, succession, dependency exposure, and maintenance burden. The assessment boundary encompasses the custody architecture and its direct operational dependencies; it does not extend to unrelated external systems, broader enterprise functions, or investment activities.

This publication does not constitute a point-in-time security audit, penetration test, legal opinion, or implementation review of any specific deployment. It does not evaluate price risk, trading strategy, portfolio allocation, tax treatment, or investment suitability. Sections 2 and 3 are normative.

Key Terms

BCRI	Bitcoin Custody Resilience Index — composite score (0–100) measuring structural resilience across five dimensions.
CS	Complexity Score — operational burden placed on the custody operator by the architecture's design requirements.
RE	Resilience Efficiency — RE = BCRI ÷ √CS. Raw efficiency ratio shown in the benchmark dataset. RE measures total resilience per unit of complexity, while ERE isolates incremental resilience above the structural baseline.
ERE	Excess Resilience Efficiency — ERE = (BCRI − 25) ÷ √CS. Floor-adjusted metric used in frontier analysis; isolates earned resilience above the structural baseline. RE and ERE will diverge most at low CS values.

Model structure. The BCRI is a weighted composite of five dimensions: Cryptographic Integrity, Physical Distribution, Operational Dependency, Cognitive Reliability, and Temporal Resilience. Dimensional weights are internal BCS model parameters. The BCRI floor of 25 is the minimum score for architectures satisfying no scored resilience criteria — a classification baseline, not a resilience score. The Resilience Sufficiency Threshold at BCRI 75 is a classification boundary corresponding to the BBB+ rating and is used to distinguish structurally sufficient architectures in the benchmark analysis. The RE metric (BCRI ÷ √CS) is used in the dataset for straightforward efficiency comparison; the ERE metric ((BCRI − 25) ÷ √CS) is used in the frontier analysis to isolate resilience earned above the structural baseline. The two metrics diverge most at low CS values, where the floor adjustment has proportionally greater effect.

Model status and relationship to the Standard. This report is a benchmark publication of the Bitcoin Custody Standard. Its public normative basis is described in BCS-NS-1.1. BCRI scores reflect architecture characteristics and modeled resilience under the framework rather than empirical performance in documented custody failure events.

3 Benchmark Dataset

Fourteen Bitcoin custody architecture types representing the principal design patterns in the market as of March 2026 are benchmarked. Exchange Wallet (#1) and Hot Wallet (#2) receive BCRI Floor = 25 by definition — they satisfy no scored resilience criteria and serve as structural reference points. All three exhibits and the findings in Section 5 reference the 12 scored architectures.

Annex A provides detailed profiles for all 14 architectures, including reference configurations, score drivers, structural strengths, and structural limitations. Architecture numbers correspond to Table 3.1.

Table 3.1 BCRI Benchmark Dataset — All 14 Architectures — *RE = BCRI ÷ √CS (raw ratio). '—' indicates Floor architectures. Source: Bitcoin Custody Standard internal benchmark dataset, March 2026.*

#	Architecture	Zone	BCRI	CS	RE	Rating
1	*Exchange Wallet*	*No Sovereignty*	*25.0*	*1.0*	*—*	***Floor***
2	*Hot Wallet*	*Single-Key*	*25.0*	*1.4*	*—*	***Floor***
3	Single-Sig Cold Storage — Regular	Single-Key	**68.2**	2.6	42.3	**BBB-**
4	Single-Sig Cold Storage — Advanced	Single-Key	**84.1**	4.8	38.4	**A**
5	Self-Managed Multisig — Regular (2-of-3)	Distributed Self-Custody	**76.6**	4.4	36.5	**BBB+**
6	Self-Managed Multisig — Advanced (3-of-5)	Distributed Self-Custody	**89.6**	5.6	37.9	**A+**
7	Self-Managed Multisig — Hi Resilience (Geo)	Distributed Self-Custody	**97.5**	6.2	39.1	**AAA**
8	Collaborative Multisig — Assisted (2-of-3)	Collaborative	**79.2**	3.4	43.0	**BBB+**
9	Collaborative Multisig — Peer (2-of-3)	Collaborative	**82.0**	4.6	38.2	**A-**
10	Collaborative Multisig — Advised (3-of-5)	Collaborative	**96.5**	5.2	42.3	**AA+**
11	MPC Custody	Institutional	**89.6**	7.4	32.9	**A+**
12	Corporate Bitcoin Treasury	Institutional	**72.0**	8.2	25.1	**BBB**
13	Regulated Exchange Custody	Institutional	**75.5**	8.8	25.4	**BBB+**
14	Qualified Custodian	Institutional	**93.7**	9.4	30.6	**AA**

4 Results

The three benchmark exhibits are presented below with brief descriptive observations. Full analytical interpretation appears in Section 5.

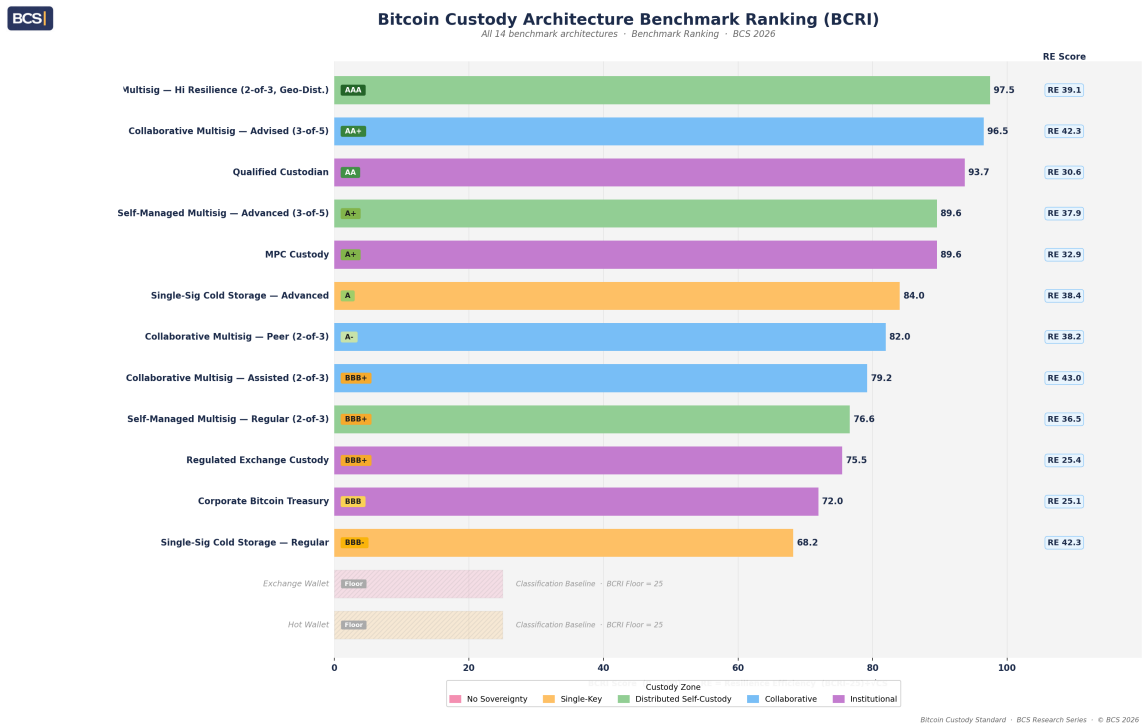

Exhibit 4.1 BCRI Benchmark Ranking — *BCRI scores and RE (= BCRI ÷ √CS) for 12 scored architectures, sorted by BCRI descending. Two Floor baselines shown separately. Rating classifications AAA through BBB- by badge color. RE Score column at right. Source: Bitcoin Custody Standard internal benchmark dataset, March 2026.*

The ranking orders 12 scored architectures by absolute BCRI. Distributed self-custody and collaborative multisig designs occupy the top positions; the highest institutional architecture falls below the top two self-custody configurations. The RE column establishes that BCRI rank order and efficiency rank order do not align: architectures with lower absolute BCRI scores achieve higher resilience efficiency than architectures ranked above them.

The ranking presents two simultaneous views: bar length measures absolute structural resilience; the RE column measures resilience output per unit of operational complexity. The benchmark is not one-dimensional — the strongest architectures by BCRI are not the most efficient by RE. This distinction is the basis for the frontier analysis that follows.

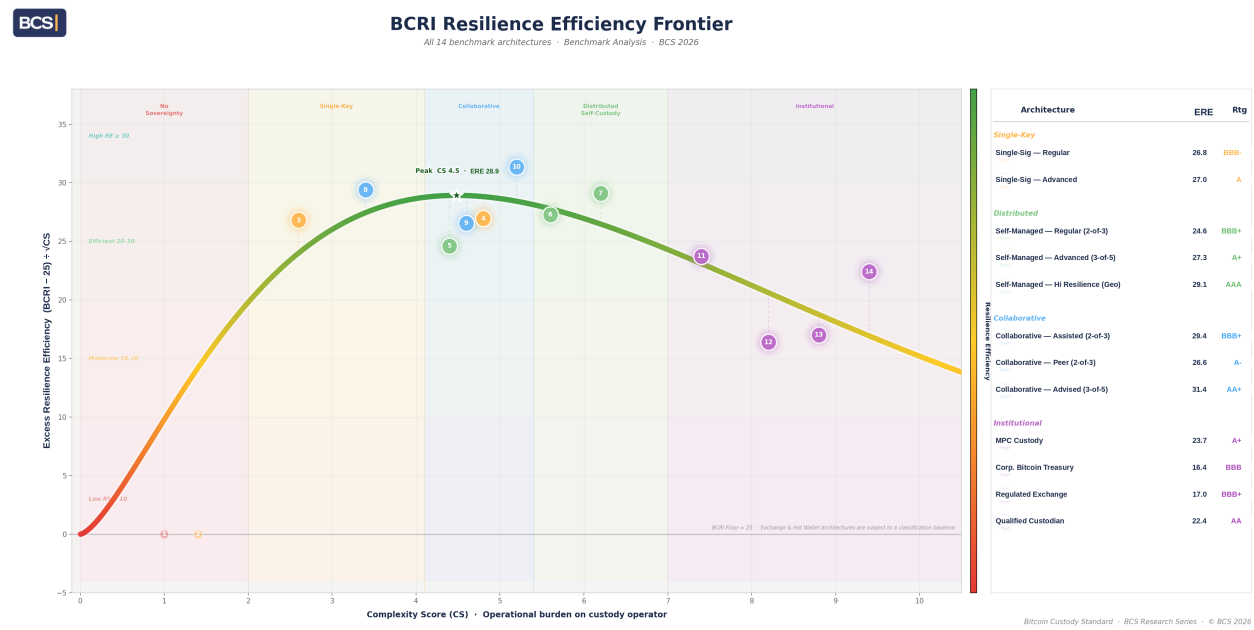

Exhibit 4.2 BCRI Resilience Efficiency Frontier — *ERE = (BCRI − 25) ÷ √CS plotted against CS for all 14 architectures. Floor-adjusted metric isolates earned resilience above the structural baseline. Fitted frontier curve shown; peak annotated at CS ≈ 4.5. Zone shading by background region. Source: Bitcoin Custody Standard internal benchmark dataset, March 2026.*

The frontier plot maps floor-adjusted resilience efficiency (ERE) against Complexity Score (CS) across all 14 architectures. ERE rises through the low- and moderate-complexity range, peaks near CS ≈ 4.5, then declines as complexity increases. The highest ERE values are concentrated in the moderate-complexity range — not at the high-complexity end where institutional architectures are located.

Institutional architectures cluster to the right of the frontier peak. Their absolute BCRI scores can remain strong, but ERE is generally lower, indicating that added complexity does not produce proportional resilience gains. Beyond the peak, the benchmark shows a pattern of diminishing marginal resilience efficiency: a limited number of architectures remain strong, but most additional complexity yields lower resilience efficiency rather than better structural performance.

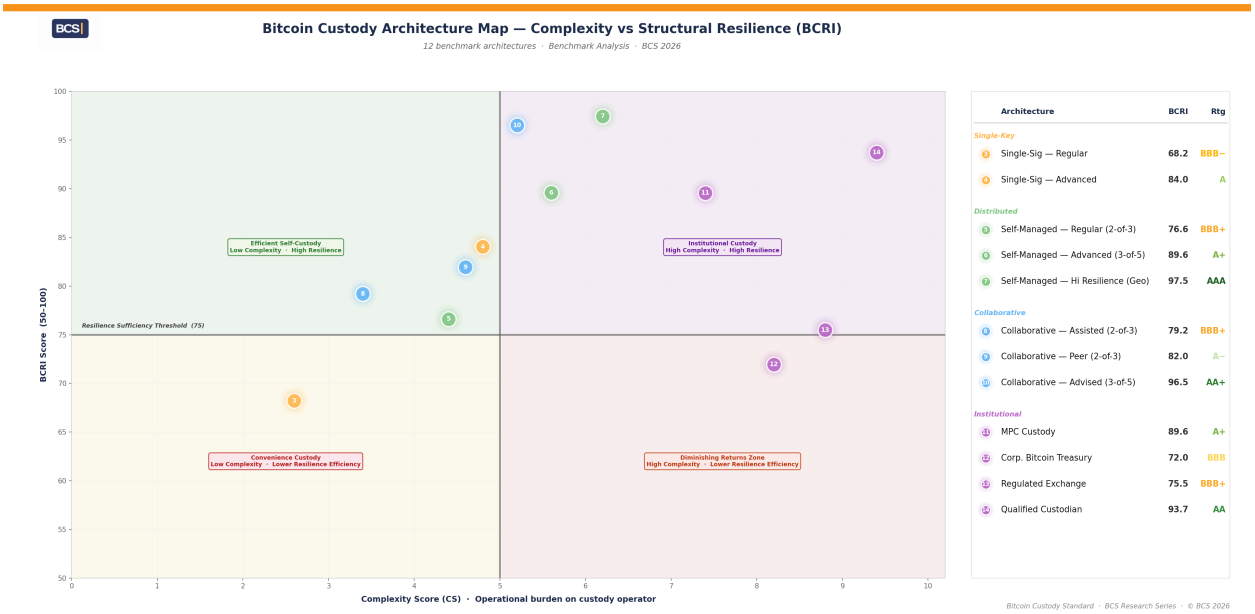

Exhibit 4.3 Bitcoin Custody Architecture Map — Complexity vs Structural Resilience — *12 scored architectures plotted on CS (horizontal) vs BCRI (vertical) axes. Resilience Sufficiency Threshold at BCRI 75. Four labelled quadrant regions. Source: Bitcoin Custody Standard internal benchmark dataset, March 2026.*

The architecture map plots 12 scored architectures on CS (horizontal) against BCRI (vertical). The BCRI 75 Resilience Sufficiency Threshold divides the design space into architectures above and below the threshold. Two scored architectures fall below this line at markedly different complexity levels — confirming that sub-threshold outcomes arise from distinct structural causes.

The architectures distribute across four structurally distinct regions — not a single linear spectrum from weak to strong. Architecture families cluster by design type: low-complexity high-resilience configurations occupy the upper-left; high-complexity institutional configurations occupy the upper-right; sub-threshold architectures divide into the two failure zones below the threshold line. This spatial structure is the basis for the two-dimensional failure framework in Section 5.

5 Analysis and Key Findings

Finding 1 ***Maximum resilience is achieved through architecture design, not delegation.***

Exhibit 4.1: three of the four highest-scoring architectures are distributed or collaborative designs. Self-Managed Multisig — Hi Resilience (97.5, AAA) achieves the benchmark maximum through three geographically separated, air-gapped hardware signing devices operating across distinct regulatory jurisdictions, combined with a personal Bitcoin node — eliminating every significant structural attack vector (see Annex A, #7). Collaborative Multisig — Advised (96.5, AA+) reaches the second score through professional HSM (hardware security module) co-signing, multi-continental key distribution, and estate-grade succession without surrendering client sovereignty (Annex A, #10). The highest institutional score, Qualified Custodian (93.7, AA), is the only institutional architecture above ERE 30, achieved through individual on-chain addressing and statutory trust law. Within the BCRI model, AAA is unattainable for any OCC- or NYDFS-chartered intermediary because chartered custody structures remain subject to irreducible regulatory intervention risk: assets or transactions may be frozen, delayed, restricted, or compelled under applicable legal authority, and no configuration choice can eliminate that exposure. Resilience cannot be purchased. It is built into the structure at design time.

Finding 2 ***Resilience efficiency peaks at moderate complexity and declines steeply beyond it.***

Exhibit 4.2: ERE rises steeply from CS 1.0 to the frontier peak near CS 4.5, then declines. The three most ERE-efficient architectures — Collaborative Multisig Assisted (ERE 43.0, CS 3.4), Collaborative Multisig Advised (ERE 42.3, CS 5.2), and Single-Sig Cold Storage Regular (ERE 42.3, CS 2.6) — all operate between CS 2.6 and 5.2. Every institutional architecture with CS above 7.0 produces ERE between 25.1 and 32.9. The Corporate Bitcoin Treasury (Annex A, #12) is the benchmark's clearest case of misallocated complexity: CS 8.2, ERE 25.1, BCRI 72.0. Its board governance is the strongest in the dataset, but that strength sits on top of a structurally constrained custody model: delegated control without direct signing authority, disclosure-driven exposure, coordination latency, institution-mediated recovery paths, multi-entity dependency, and limited jurisdictional dispersion. The decisive limiting factor is jurisdictional concentration: treasury custody arrangements typically remain concentrated within a single legal and regulatory jurisdiction, even when multiple custodians or governance layers are involved. The score therefore reflects the combined effect of constrained control, high coordination overhead, institutional dependency, and limited jurisdictional dispersion — not governance weakness alone. Governance increases oversight, but it does not increase structural control. As a result, complexity rises without a corresponding increase in resilience.

Finding 3 ***Custody failure is two-dimensional: under-engineering and over-engineering are structurally distinct failure modes.***

Exhibit 4.3: two scored architectures sit below the Resilience Sufficiency Threshold at BCRI 75. Single-Sig Cold Storage Regular (68.2) sits in the Convenience Custody zone — constrained by its inherent single-point-of-failure design (Annex A, #3). Corporate Bitcoin Treasury (72.0) sits in the Diminishing Returns Zone — achieving sub-threshold BCRI at CS 8.2 despite the strongest governance controls in the benchmark (Annex A, #12). These represent structurally different failure modes requiring different interventions: the bottom-left architecture needs greater structural redundancy; the bottom-right architecture needs reduced dependency concentration and broader jurisdictional dispersion, which governance alone cannot provide. A practitioner who treats custody risk as a single axis will misdiagnose the bottom-right failure mode every time.

The benchmark establishes that custody risk has a measurable efficient range — and that both failure modes are structurally avoidable through design.

6 Limitations

The following limitations apply to all findings in this publication.

– Architecture-type scoring, not deployment-specific assessment. BCRI scores in this report reflect benchmarked architecture classes and reference configurations chosen to represent implementation ranges within each design type. They are not individualized reviews of specific products, custodians, or user deployments. Actual scores may vary materially depending on implementation quality, operational discipline, jurisdictional distribution, documentation quality, succession design, and maintenance practices.

– Expert-assigned dimensional weights. Dimensional weights reflect the considered judgement of the Bitcoin Custody Standard and were assigned as part of the internal model design. Future revisions to these weights may alter relative scores.

– Model parameters subject to revision. The ERE formula, BCRI floor (25), Resilience Sufficiency Threshold (75), and CS scoring basis are internal BCS model parameters and may be revised in future versions. The √CS scaling is a modelling choice, not an empirically derived relationship.

– Not empirically validated against failure-event datasets. The BCRI is a structural assessment model. It has not yet been validated against a comprehensive dataset of documented custody failures or security incidents. Scores reflect modeled resilience properties of architecture design, not realized historical outcomes.

– Dataset scope. The 14 architectures represent principal custody design types as of March 2026 and are not intended as a statistically representative sample of all possible custody implementations. Emerging architecture types, hybrid variants, and non-standard deployments may not be captured.

– No external comparative baseline. BCRI scores are internally consistent within the BCS framework and this benchmark dataset. Cross-framework comparisons with SOC 2, ISO 27001, or other security or control frameworks are outside scope.

7 Practitioner Implications

The benchmark findings translate into three direct implications for custody design and evaluation.

First, architecture selection dominates provider selection. The benchmark demonstrates that the structural ceiling of a custody arrangement is set by key distribution, quorum design, geographic dispersion, and control structure — the properties measured by the BCRI. Provider quality affects implementation quality within an architecture class, but it does not alter the upper bound of resilience achievable within that class. Selecting a stronger provider within a weaker architecture does not raise the architecture's resilience ceiling. In delegated custody models, that ceiling is further constrained by intermediary dependence, regulatory intervention risk, and the possibility that access to funds may be delayed, conditioned, or frozen under institutional legal frameworks.

Second, resilience must be evaluated jointly with operational complexity. The benchmark does not show that more complexity produces more resilience in a linear way. Rather, resilience efficiency peaks in the moderate-complexity range and generally declines as complexity rises beyond that point. Within the benchmark, systems with CS above 7.0 consistently produce lower ERE than systems in the CS 3.0–5.5 range. This indicates that additional operational burden often yields diminishing resilience benefit rather than proportional structural improvement. Complex custody arrangements may still achieve strong absolute resilience, but they do so at materially lower efficiency and with greater coordination burden over time.

Third, custody risk must be assessed across two independent dimensions. Under-engineered systems fail through lack of structural redundancy; over-engineered systems fail through misallocated complexity and concentration risk. The benchmark quantifies both failure modes separately. They require different corrective actions: adding redundancy resolves the first; reducing concentration or simplifying coordination resolves the second. A single-axis evaluation framework — more security equals better — will systematically misdiagnose the second failure mode.

For practitioners, the implication is direct: custody design should begin with structural architecture selection, validated against the benchmark frontier, before any specific product, provider, or jurisdiction is chosen. The architecture determines the resilience ceiling. Everything else determines how close to that ceiling the implementation operates.

In practical terms, custody architecture is the primary determinant of long-term survivability. All other variables — provider quality, operational execution, and regulatory environment — operate within the constraints imposed by that architecture.

8 Conclusion

The BCRI benchmark establishes a new baseline for evaluating Bitcoin custody architecture.

This publication provides a structured, scored, and reproducible framework for comparing custody systems on the basis of structural resilience and operational complexity.

Its central finding is clear: custody resilience is determined by architecture, not assumed from brand, convenience, or institutional form.

The benchmark establishes three core findings.

First, structural resilience follows a defined efficiency range rather than a linear relationship between complexity and strength. The highest-performing architectures are concentrated in distributed self-custody and collaborative multisig design classes, while most institutional architectures operate at materially higher complexity and lower resilience efficiency.

Second, custody failure is not one-dimensional. It arises either from insufficient structure or from misallocated complexity. These are distinct failure modes with different causes and different remedies.

Third, provider selection is secondary to architecture selection. The relevant determinant of long-term resilience is the structure itself: key distribution, quorum design, dependency profile, recovery design, and geographic dispersion.

These findings redefine the basis on which Bitcoin custody should be evaluated. Any assessment that does not account for architecture design, complexity constraints, and frontier positioning is incomplete.

The relevant question is no longer:

Which provider?

The question is:

What is the architecture, and where does it sit on the benchmark?

This report provides a measurable answer to that question.

The BCRI framework is intended to serve as a reference baseline for custody evaluation across research, institutional use, and long-term Bitcoin stewardship.

Within this framework, custody is not a matter of preference. **It is a matter of design.**

9 References

BCS Standard Documents

[1] Bitcoin Custody Standard. BCS Normative Standard BCS-NS-1.1. Bitcoin Custody Standard, March 2026.

Standards and Regulatory Framework

[2] National Institute of Standards and Technology. Cybersecurity Framework v2.0. NIST, 2024. https://doi.org/10.6028/NIST.CSWP.29

[3] National Institute of Standards and Technology. FIPS PUB 140-2: Security Requirements for Cryptographic Modules. NIST, 2001. Relevant to HSM security level claims in Architecture #14. https://csrc.nist.gov/publications/detail/fips/140/2/final

[4] Office of the Comptroller of the Currency. OCC Interpretive Letter 1174 — National Banks and Federal Savings Associations as Cryptocurrency Custodians. OCC, January 2021. https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2021/int1174.pdf

Qualified Custodian and Exchange Custody Sources

[5] Coinbase Global Inc. Annual Report on Form 10-K (fiscal years 2022, 2023, 2024). SEC EDGAR. Primary source for Architecture #13 and CCTC data in Architecture #14. https://www.sec.gov/cgi-bin/browse-edgar?action=getcompany&CIK=COIN&type=10-K

[6] Anchorage Digital Bank, National Association. OCC Conditional Approval No. 1317, January 13, 2021. OCC charter source for Architecture #14. https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2021/pub-conditional-approval-1317.pdf

[7] Fidelity Digital Assets Services, LLC. NYDFS License and Custody Service Overview. Source for Fidelity reference in Architecture #14. https://www.fidelitydigitalassets.com/overview

[8] NYDIG LLC. NYDFS New York Trust Company Charter and custody operations. Source for NYDIG reference in Architecture #14. https://nydig.com

[9] U.S. Securities and Exchange Commission. Spot Bitcoin ETP S-1 and 8-A Registration Statements. SEC EDGAR, January–March 2024. Source for ETF custody characterization in Architecture #14. https://www.sec.gov/cgi-bin/browse-edgar?action=getcompany&company=bitcoin+trust&CIK=&type=S-1

Exchange Insolvency and Legal Framework

[10] United States Bankruptcy Court, SDNY. In re: FTX Trading Ltd. et al., Case No. 22-11068. Filed November 11, 2022. https://www.courtlistener.com/docket/66201306/ftx-trading-ltd/

[11] Ernst & Young LLP (Monitor). Report to the Court on the Affairs of Quadriga Fintech Solutions Corp. Ontario Superior Court of Justice, 2019. https://www.ic.gc.ca/app/scr/bsf-osb/ins/login.html

[12] Uniform Law Commission. UCC Article 8 — Digital Asset Amendments. ALI and ULC, 2022–2023. https://www.uniformlaws.org/committees/community-home?CommunityKey=0b7e07ec-15ae-4e5d-9e20-bd5a4d6e9cc5

MPC Custody Sources

[13] Boneh, D.; Franklin, M. Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman Group Signature Scheme. PKC 2003, Springer, 2003. https://link.springer.com/chapter/10.1007/3-540-36288-6_3

[14] Fireblocks Inc. Platform Security Architecture and SOC 2 Type II Attestation Report (executive summary). 2023. https://www.fireblocks.com/blog/fireblocks-security

[15] BitGo Inc. Institutional Custody Security Overview and SOC 2 Type II Attestation. 2023. https://www.bitgo.com/security

Corporate Bitcoin Treasury Sources

[16] Strategy Inc. (formerly MicroStrategy Incorporated). Annual Reports on Form 10-K (FY2022–2024). SEC EDGAR. CIK 1050446. https://www.sec.gov/cgi-bin/browse-edgar?action=getcompany&CIK=1050446&type=10-K

[17] Marathon Digital Holdings, Inc. Annual Report on Form 10-K, 2023. SEC EDGAR. CIK 1507605. https://www.sec.gov/cgi-bin/browse-edgar?action=getcompany&CIK=1507605&type=10-K

Collaborative Multisig Provider Sources

[18] Unchained Capital, Inc. Multi-Institutional Bitcoin Custody: Collaborative Custody Architecture Overview. https://unchained.com/collaborative-custody

[19] Keys.casa Inc. (Casa). Multi-Key Security Platform Architecture. https://keys.casa/how-it-works

Bitcoin Protocol and Signing Workflow Sources

[20] Chow, A. BIP-174: Partially Signed Bitcoin Transactions (PSBT). Bitcoin Improvement Proposal, 2017. https://github.com/bitcoin/bips/blob/master/bip-0174.mediawiki

[21] Bitcoin Core Contributors. Bitcoin Core Reference Implementation. Open source. https://bitcoin.org/en/bitcoin-core

[22] Coldcard Wallet (Coinkite Inc.). PSBT Signing Workflow and Air-Gap QR Implementation Documentation. https://coldcard.com/docs

Hardware Device and Foundational Bitcoin References

[23] Ledger SAS. Ledger Security Model. 2023. https://www.ledger.com/academy/security

[24] SatoshiLabs. Trezor Security and Open Source Model. 2023. https://trezor.io/learn

[25] Antonopoulos, A. M. Mastering Bitcoin, 2nd Edition. O'Reilly Media, 2017.

[26] Unchained Capital. Multisig Security Tradeoffs. 2022. https://unchained.com/blog

[27] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. https://bitcoin.org/bitcoin.pdf

Annex A Benchmark Architecture Profiles (Informative)

This annex documents the reference configuration, score driver, primary structural strength, and primary structural limitation for each of the 14 benchmark architectures. These profiles provide the architectural grounding for the scores and findings presented in the main report. They are informative — they support but do not form part of the normative methodology of the Bitcoin Custody Standard. Where named products, providers, or institutions appear, they are cited as representative examples of the relevant architecture class, not as a complete enumeration or endorsement. Architecture numbers correspond to Table 3.1.

Zone 1 — No Sovereignty

#1 Floor **BCRI 25 | CS 1**	**Exchange Wallet** *No Sovereignty*
Config	Client account on a centralized exchange. The exchange holds all keys in omnibus pools; the client owns a ledger balance, not on-chain Bitcoin. No personal hardware or node required.
Driver	Mandatory BCRI floor of 25. Client holds no keys and cannot independently verify holdings. Insolvency or regulatory freeze terminates access entirely.
Strength	Zero operational burden. Instant liquidity and integrated fiat rails.
Limit	No Bitcoin ownership — client is an unsecured creditor in the event of exchange insolvency. Documented exchange insolvencies — including FTX Trading Ltd. (2022, [10]) and Quadriga Fintech Solutions Corp. (2019, [11]) — resulted in partial or total client loss under omnibus custody arrangements.

Zone 2 — Single-Key

#2 Floor **BCRI 25 | CS 1.4**	**Hot Wallet** *Single-Key*
Config	Software wallet on a smartphone or desktop device. Single private key held in device memory or cloud backup service. Internet-connected at all times; relies on a third-party node or provider API for chain data.
Driver	Mandatory BCRI floor of 25. Internet-connected key storage satisfies no scored resilience criteria. Device compromise produces immediate, unrecoverable total loss.
Strength	Frictionless on-chain access. No specialist hardware. Compatible with all protocols and DeFi interfaces.
Limit	Maximum attack surface — key lives on an internet-connected device. Device loss or cloud backup compromise equals total loss.

#3 BBB- **BCRI 68.2 | CS 2.6**	**Single-Sig Cold Storage — Regular** *Single-Key* · RE 42.3
Config	Single air-gapped hardware signing device (e.g., Coldcard, Ledger, Trezor, or equivalent). Seed phrase backed up on stamped metal plate. Third-party node for transaction broadcast. No multisig. Single geographic location.
Driver	Air-gapped hardware eliminates internet-connected key exposure, pushing Key Security near single-key maximum. BCRI 68.2 reflects the irreducible single-point-of-failure: one device loss or seed compromise is unrecoverable.
Strength	True key sovereignty at minimal operational complexity. RE 42.3 is the third-highest in the benchmark — strong resilience per unit of operational effort.

Limit	Structurally non-redundant. Physical coercion, device failure, or seed compromise produces immediate total loss. No geographic distribution or succession mechanism.

#4 A	**Single-Sig Cold Storage — Advanced**
BCRI 84.0 | CS 4.8	*Single-Key* · RE 38.4
Config	Air-gapped hardware signing device with passphrase-hardened key. PSBT signing via microSD transfer — zero USB connections during signing [20]. Personal Bitcoin node on dedicated hardware [21] (e.g., Bitcoin Core, Umbrel, Start9, RaspiBlitz, or equivalent). Seed backed up on stamped metal with passphrase stored separately. Transaction construction via a PSBT-capable wallet coordinator connected to own node.
Driver	Personal node closes third-party chain data dependency. Passphrase hardening means seed theft alone is insufficient. Air-gapped microSD workflow removes USB attack surface. Combined, these push BCRI to near the single-key ceiling at 84.1.
Strength	Complete operational sovereignty — own node, no USB signing exposure, passphrase separation from seed. No third-party data dependency at any layer.
Limit	Still a single key — physical coercion or seed-plus-passphrase compromise is unrecoverable. Personal node requires ongoing maintenance and technical competency.

Zone 3 — Distributed Self-Custody

#5 BBB+	**Self-Managed Multisig — Regular (2-of-3)**
BCRI 76.6 | CS 4.4	*Distributed Self-Custody* · RE 36.5
Config	2-of-3 multisig with three hardware signing devices (e.g., Coldcard, Trezor, Foundation Passport, or equivalent), all operator-held at a single primary location. Sequential PSBT signing [20] via a multisig-capable wallet coordinator. Multisig descriptor backed up on encrypted storage. Third-party node for broadcast.
Driver	2-of-3 quorum eliminates single-device failure as a loss event. BCRI 76.6 reflects single-geography exposure — all three keys co-located and susceptible to simultaneous seizure or loss.
Strength	Full key sovereignty with fault tolerance. One device loss is operationally recoverable. No third-party key dependency.
Limit	Single-geography key storage — fire, physical seizure, or coercion can compromise all three keys simultaneously. Multisig descriptor backup is critical and frequently neglected.

#6 A+	**Self-Managed Multisig — Advanced (3-of-5)**
BCRI 89.6 | CS 5.6	*Distributed Self-Custody* · RE 37.9
Config	2-of-3 multisig across three independent operators, each holding one hardware signing device at their own location in geographically separate cities. Any two participants must coordinate to produce a valid signature. Each operator maintains independent copies of the multisig descriptor and encrypted seed backup.
Driver	Three-operator geographic distribution eliminates single-location seizure risk and requires simultaneous compromise of two independent individuals. BCRI 89.6 reflects strong multi-party resilience; the limiting factor is succession planning.
Strength	No single point of failure across devices, operators, or locations. No third-party service dependency. Peer accountability prevents unilateral action.
Limit	Succession failure is the primary structural gap — one participant's incapacity without documented key recovery creates complex recovery from the remaining two signers. All participants must maintain hardware wallet competency.

#7 AAA **BCRI 97.5 | CS 6.2**	**Self-Managed Multisig — Hi Resilience (Geo)** *Distributed Self-Custody* · RE 39.1
Config	2-of-3 multisig with hardware signing devices (e.g., Coldcard Mk4 or equivalent air-gapped device) at three geographically separate locations in distinct regulatory jurisdictions. Personal Bitcoin node on dedicated hardened hardware [21] running a Bitcoin-only operating system. Fully air-gapped PSBT signing [20] via QR code only — zero USB connections [22]. Stamped-metal seed backups at each location. Unique passphrases per device, stored separately from seeds. Transaction construction via PSBT-capable wallet coordinator on a dedicated, hardened device.
Driver	Geographic separation across distinct jurisdictions eliminates single-jurisdiction seizure across all three keys. Personal node provides complete chain sovereignty. QR-only signing eliminates the USB attack surface. Combined, these close every major structural attack vector. BCRI 97.5 is the benchmark maximum.
Strength	No single jurisdiction can capture more than one key. No third party holds signing authority. Complete chain sovereignty. Physical seed theft is insufficient without the separately-stored passphrases.
Limit	Travel between jurisdictions may be required for some operations. Extreme documentation discipline required — a configuration error under time pressure is potentially catastrophic. Not appropriate without sustained operational commitment and rehearsed recovery procedures.

Zone 4 — Collaborative

#8 BBB+ **BCRI 79.2 | CS 3.4**	**Collaborative Multisig — Assisted (2-of-3)** *Collaborative* · RE 43.0
Config	2-of-3 multisig: client holds one hardware signing device; a collaborative co-signing provider (e.g., Casa [19], Unchained Capital [18], or similar provider model) holds one key in HSM-secured infrastructure; a third path uses the client's own seed backup. Day-to-day spending requires client hardware plus provider co-signature via provider application. Recovery is possible with the client's own seed alone, without provider involvement.
Driver	Provider co-signing eliminates single-device failure without requiring the client to manage multiple hardware devices. Highest RE in the benchmark at 43.0, reflecting exceptional efficiency at CS 3.4. Provider HSM security and client-independent recovery are the key score drivers.
Strength	Lowest operator complexity of any multisig design. Recovery is provider-independent by design. Best-in-class RE at this complexity level.
Limit	Provider holds one key — custody is not fully sovereign. Day-to-day transactions require provider platform availability. Provider insolvency or policy change requires migration to a new configuration.

#9 A- **BCRI 82.0 | CS 4.6**	**Collaborative Multisig — Peer (2-of-3)** *Collaborative* · RE 38.2
Config	2-of-3 multisig across two equal co-signing peers, each holding one hardware signing device at their own location in geographically separate cities. An optional third recovery key is held in a secure facility. Signature coordination via encrypted channel or in-person PSBT exchange. Each peer maintains an independent copy of the multisig descriptor.
Driver	Two-party structure distributes physical key custody with no third-party service dependency. BCRI 82.0 reflects strong peer resilience — neither party can spend unilaterally, and geographic separation addresses primary single-key failure modes.
Strength	No company dependency at any layer. Two independent physical locations. Neither party can act unilaterally. Strong mutual accountability.

Limit	Succession is the primary structural gap — if one peer becomes unavailable without a documented recovery path, access depends on the third recovery key. Both peers must maintain hardware wallet competency.

#10 AA+	**Collaborative Multisig — Advised (3-of-5)**
BCRI 96.5 | CS 5.2	*Collaborative* · RE 42.3
Config	3-of-5 multisig: client holds two hardware signing devices at separate locations; a professional co-signing custodian (e.g., Unchained Capital [18], Casa Covenant [19], or similar provider) holds one key in HSM-secured infrastructure; an independent key agent holds one key in geographically separate secure storage; a fifth sealed recovery package provides an additional path. Three of five keys required to spend. Multi-continental key distribution. Formal succession and estate documentation tied to key access procedures.
Driver	Maximum key redundancy — two simultaneous key losses still leave the wallet fully accessible. Professional HSM co-signing adds institutional-grade key security without removing client sovereignty. BCRI 96.5 is the second-highest score in the benchmark.
Strength	Two keys can be lost or compromised simultaneously with no risk to funds. Estate-grade succession planning built into the architecture. Professional key oversight without surrendering client control.
Limit	Three-institution coordination increases operational latency for routine transactions. Ongoing service relationships with multiple parties required. The complexity overhead is only justified for large, permanent holdings.

Zone 5 — Institutional

#11 A+	**MPC Custody**
BCRI 89.6 | CS 7.4	*Institutional* · RE 32.9
Config	Multi-party computation custody: no complete private key exists at any point [13]. Cryptographic key shares are distributed across geographically separate HSM nodes operated by the custodian. Representative providers operating MPC custody infrastructure include Fireblocks, Copper, Zodia Custody, BitGo, and others (illustrative, not exhaustive). Client initiates transactions via API or platform dashboard. Multi-jurisdictional cold storage. Independent third-party audit attestation (SOC 2 Type II or equivalent) is publicly disclosed by certain providers in this class — including those cited at [14][15]; practices vary by provider and should be verified independently. Multi-party approval workflow enforced at the HSM layer.
Driver	MPC architecture prevents any single operator or machine from possessing a complete key, removing insider theft as a single-event failure mode. BCRI 89.6 reflects excellent Key Security and Physical Distribution scores. The structural ceiling is omnibus pooling: no individual on-chain addresses, and clients cannot independently verify their holdings.
Strength	Highest ERE in the institutional zone (32.9). No client hardware burden. Multi-jurisdictional cold storage. Certain providers in this class — including those cited at [14][15] — publicly disclose independent third-party audit attestation (SOC 2 Type II or equivalent).
Limit	Omnibus architecture — clients cannot verify their holdings independently on-chain. Bankruptcy protection is contractual, not statutory. CS 7.4 reflects high coordination complexity.

#12 BBB	**Corporate Bitcoin Treasury**
BCRI 72.0 | CS 8.2	*Institutional* · RE 25.1
Config	Bitcoin held as a treasury reserve asset through multiple regulated custodians under board committee governance. Board approval required for all withdrawals. Direct primary custodian relationships with no sub-custodians. Multi-custodian model provides redundancy against single-custodian failure. Scored using publicly disclosed custody arrangements of listed corporate Bitcoin treasury holders; primary source data drawn from SEC 10-K filings [16][17].

Driver	Within the benchmark, this architecture achieves the strongest governance and withdrawal-control profile in the dataset. BCRI 72.0 is constrained by a structural characteristic of the reference filings: the custodians disclosed in the 10-K filings used for this architecture [16][17] are all US-based. This observation is specific to the benchmarked reference set; corporate Bitcoin treasury arrangements at other entities may differ. Single-jurisdiction concentration means a coordinated domestic regulatory action can simultaneously freeze all holdings — a risk made more acute by mandatory public disclosure of holding size and custodian identity per SEC reporting obligations.
Strength	Strongest board-level governance in the benchmark. Direct primary custodian relationships with no sub-custodian exposure. Multi-custodian redundancy against single-provider failure.
Limit	Jurisdictional concentration is a structural constraint that governance quality cannot compensate for. RE 25.1 is the lowest of any scored architecture. Public SEC disclosure makes precise holdings and custodian identity visible to all regulators simultaneously.

#13 BBB+	**Regulated Exchange Custody**
BCRI 75.5 | CS 8.8	*Institutional* · RE 25.4
Config	Industrial-scale MPC custody at the exchange layer. Approximately 98% of assets in cold storage, with a small hot wallet allocation for operational liquidity. Omnibus client pooling — no individual on-chain addresses. Geographically distributed cold storage vaults. Based on Coinbase Global, Inc. 10-K filings (2022–2024) as the best-case reference point for this architecture class [5]; the following characteristics are sourced from those filings: SOC 2 Type II and PCAOB audit engagement annually; OFAC compliance screening applied to all transactions; 98% cold storage verified by third-party attestation. Other regulated exchanges in this class may differ materially in operational controls.
Driver	Strong operational controls are offset by the structural characteristics of the exchange model: omnibus pooling means no client can independently verify on-chain holdings, and client assets in exchange accounts are generally held under arrangements that rely on UCC Article 8 or equivalent contractual frameworks; as of the publication date, the application of these protections in a major digital asset exchange insolvency has not been adjudicated, creating a structural uncertainty that is not resolved by the reference filing [12]. RE 25.4 at CS 8.8 is the second-lowest efficiency in the benchmark.
Strength	Cold storage percentage independently attested per Coinbase 10-K filings [5]. MPC layer prevents single-employee unilateral access. Annual SOC 2 Type II and PCAOB audit engagements disclosed in filings [5].
Limit	No on-chain client verification possible by design. UCC Article 8 structural uncertainty as of publication date. Government freeze and OFAC authority applies. The FTX insolvency (2022, [10]) illustrates the failure mode inherent to omnibus exchange custody, regardless of operational control quality.

#14 AA	**Qualified Custodian**
BCRI 93.7 | CS 9.4	*Institutional* · RE 30.6
Config	OCC national bank charter or NYDFS limited purpose trust company charter. Individual segregated on-chain addresses per client — independently verifiable at any time. Hardware security modules meeting or exceeding FIPS 140-2 Level 3 [3] (FIPS 140-2 Level 3 compliance for custody HSMs is referenced in OCC and NYDFS supervisory frameworks and publicly disclosed by certain institutions in this charter class). Multi-continental cold storage vaults. Hardware-enforced client quorum approval policies. OCC and NYDFS chartering frameworks establish trust law structures that are generally understood to provide bankruptcy remoteness for client assets, in contrast to the purely contractual protection available under non-chartered custody models [4][6]. This characterization describes the legal structure of the charter; it is not a legal opinion on the treatment of client assets in any specific insolvency proceeding. Illustrative examples of institutions operating under this charter model include Coinbase Custody Trust Company (CCTC, NYDFS) [5], Anchorage Digital Bank (OCC) [6], Fidelity Digital Assets (NYDFS) [7], and NYDIG [8]; this list is illustrative, not exhaustive. Spot Bitcoin ETF registration statements filed with the SEC in January–March 2024 [9] disclose CCTC as custodian for multiple US-listed products, including the iShares Bitcoin Trust (BlackRock), Fidelity Wise Origin Bitcoin Fund, ARK 21Shares Bitcoin ETF,

	and others; the count and composition of ETF custody arrangements changes as products launch or migrate and should be verified against current filings.
Driver	Individual addressing and statutory trust protection are the decisive resilience drivers — materially strengthening the architecture's control, recoverability, and continuity profile. BCRI 93.7 is the third-highest in the benchmark. Within the BCRI model, the structural ceiling for any banking-chartered intermediary is set by irreducible regulatory intervention risk under chartered custody structures — a consequence of chartering law that no configuration choice can reduce. Within the BCRI model, AAA is therefore unattainable for any OCC- or NYDFS-chartered intermediary.
Strength	The only institutional architecture in which clients can independently verify their holdings on-chain at any time. Under applicable OCC or NYDFS chartering law, the trust structure provides bankruptcy remoteness — in contrast to the purely contractual protection available under exchange or MPC custody models. The only institutional architecture above ERE 30.
Limit	Highest CS in the benchmark (9.4) — maximum coordination complexity and cost. Regulatory freeze authority under banking law is a permanent structural characteristic of any chartered intermediary. Within the BCRI model, AAA is unattainable for any OCC- or NYDFS-chartered intermediary because regulatory intervention risk under applicable chartering law imposes a structural ceiling that no implementation choice can raise.

