

Evaluating Bitcoin-Anchored Treasury Infrastructure

A framework for institutions putting
Bitcoin to work without giving it up.

Prepared for treasury teams, allocators, and investment committees evaluating productive uses of balance-sheet Bitcoin.
This paper is research and education. It is not investment, legal, tax, or accounting advice.
Figures are current as of the dates cited. See important disclosures.

Executive summary

Most institutions that hold Bitcoin hold it idle. Under the prior accounting model, that was the rational default. Under the current one, it is a position that has to be defended. Since fair value accounting for crypto assets took effect, for fiscal years beginning after 15 December 2024, gains and losses on Bitcoin holdings flow through net income, and the return a treasury chooses not to earn on that capital is now legible to auditors, boards, and shareholders.¹ The question is no longer whether to have a view on productive Bitcoin. It is what that view should be.

The market has answered with a wide range of products that promise yield on Bitcoin. They vary widely in quality, and the differences are not apparent on a marketing page. Several of the structures sold as "Bitcoin yield" reproduce the precise counterparty and custody exposures that destroyed tens of billions of dollars of customer assets in 2022. Others are structurally different. Telling them apart is the work this paper is built to support.

We set out a neutral, fiduciary-grade framework organized around six pillars. A treasury can apply it to any provider, including the ones not named here. We then apply the same framework to a single reference architecture, Hemi, a modular Bitcoin-anchored Layer 2, named by BitcoinTreasuries.net as its Onchain Treasury and Finance Partner. Hemi appears in this paper because it scores well against criteria we defined independently. The criteria were not written around it.

Core finding

The decisive variable is not the headline yield. It is whether the asset remains native Bitcoin under the holder's control, and whether every movement is verifiable onchain. Architectures that keep BTC native and auditable occupy a different risk category from wrapped-token and custodial-lending models, irrespective of the rate on offer. A treasury that gets the structure right can treat yield as a second-order question. A treasury that gets it wrong has, in substance, made an unsecured loan to a counterparty and called it a return.

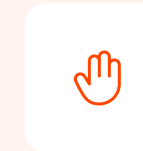
Reading the framework is the first step. Applying it is the second. The right configuration depends on a treasury's custody setup, its policy constraints, and the venues it is willing to use, and cannot be specified from a document. Section 8 sets out how that application works in practice.

REFERENCES:

¹ FASB, ASU 2023-08; effective for fiscal years beginning after 15 December 2024, with changes in fair value recognized in net income. Deloitte and KPMG summaries, 2023.



The six pillars in brief



Asset integrity

Does the Bitcoin remain Bitcoin, under control, with settlement assured back to the base chain.



Verifiability

Can reserves and yield source be proven onchain rather than taken on trust.



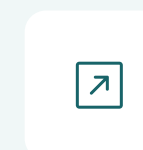
Security architecture

What the system does when something fails, not only when it works.



Control and reversibility

Whether the treasury can exit on its own terms and retains discretion throughout.



Yield quality

Where the return actually originates, and whether the source is durable.



Institutional fit

Whether the structure works inside a regulated entity, for its auditors and its board.

The allocation question

Bitcoin is on institutional balance sheets at scale. As of late May 2026, BitcoinTreasuries.net tracked 254 entities holding roughly 3.9 million BTC, close to 18.5 percent of the fixed 21 million supply.² Public companies account for approximately 5.7 to 5.9 percent of supply on their own, exchange-traded funds for a further 7 percent, and governments for around 2.5 percent.³ The single largest corporate holder, Strategy, reported 843,738 BTC; more than seventy public companies had adopted a Bitcoin treasury standard by early 2025, and the count has risen since.⁴ This is no longer a fringe allocation. It is a recognized treasury asset class with public comparables.

What the accounting change did

Before December 2023, US issuers accounted for Bitcoin as an indefinite-lived intangible asset under a cost-less-impairment model. Holdings could be written down when the price fell, but never written up when it recovered, until sale.⁵ The result was a balance sheet that understated the assets and an income statement that recognized only bad news. FASB's ASU 2023-08 replaced that treatment. Qualifying crypto assets are now measured at fair value, with changes recognized in net income each reporting period.

The change cuts both ways, and that is the point. Earnings now move with the Bitcoin price in both directions, which raises the salience of every position. An idle holding is no longer a quiet line item carried at cost. It is a marked asset earning nothing, sitting next to peers who have begun to put comparable holdings to work. Treasurers are being asked by boards and investors to show that the choice to do nothing is a choice, not an oversight.

The cost of idle Bitcoin

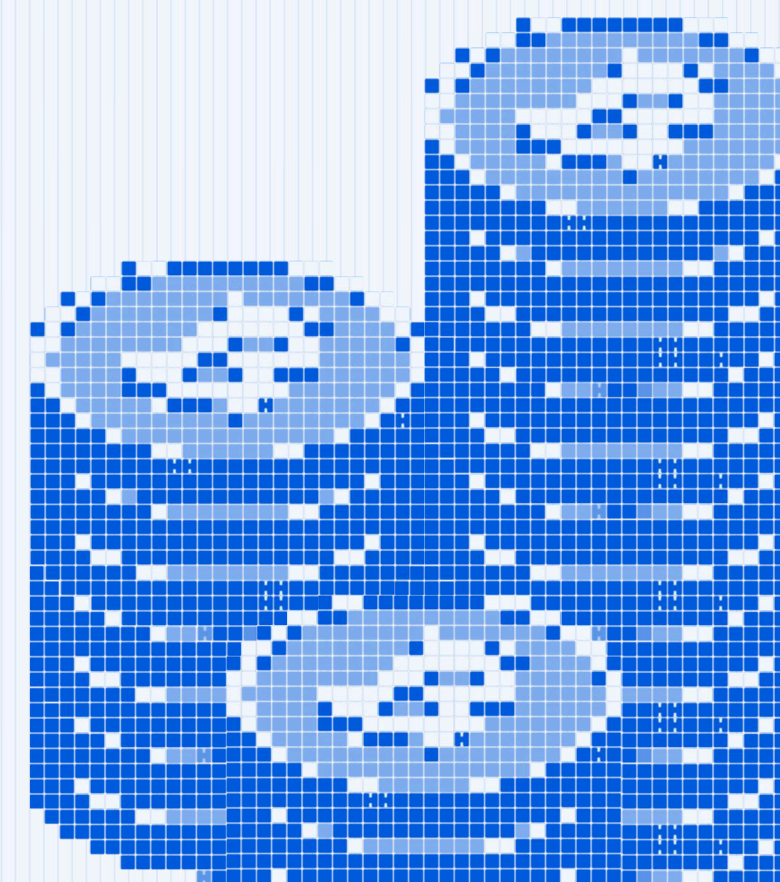
Bitcoin pays no native yield. A reserve that sits idle therefore carries an opportunity cost equal to whatever return the same capital could safely earn within a defined risk budget. For a small allocation, that cost is immaterial. For a holding measured in tens or hundreds of millions of dollars, the amount compounds into a figure a CFO must be prepared to discuss. The discipline this paper argues for is not to chase that return. It is to evaluate, on the merits, whether any available structure earns it without importing a risk the treasury would otherwise never accept.

REFERENCES:

- ² BitcoinTreasuries.net data via Cryptobriefing, late May 2026: 254 tracked entities, approximately 3.9 million BTC, about 18.5 percent of supply.
³ Category breakdown via Cryptobriefing and BitcoinTreasuries.net, 2026. Public-company share cited at approximately 5.7 to 5.9 percent.
⁴ Strategy holdings per BitcoinTreasuries.net, 2026; "more than seventy public companies" per Strategy Q1 2025 results, Form 8-K (May 2025)
⁵ Pre-ASU treatment: indefinite-lived intangible, cost less impairment. Deloitte application guidance, 2024.



Bitcoin
is no longer a
fringe allocation.



Why 2026

Three developments have converged. The holdings are large and public. The accounting now surfaces the cost of leaving them idle. And the infrastructure for productive Bitcoin has matured past its first, failure-prone generation. Together, they move the question from optional to fiduciary. A treasury holding a material Bitcoin position is now expected to hold a considered, documented answer to how that position is, or is not, being used. The remainder of this paper is the apparatus for forming one.

The solution spectrum

Approaches to making Bitcoin productive span a spectrum, from doing nothing to deploying native, programmable Bitcoin on a Bitcoin-anchored chain. Each approach imports a different primary risk. The single most useful question a treasury can ask of any option is whether, at the end of the process, it still holds native Bitcoin or a claim on someone else's.



Exhibit 1. (The solution spectrum)

Approach	Mechanism	Primary risk imported	Native BTC retained
Hold	BTC held in custody, unused.	No counterparty. Full opportunity cost.	Yes
Custodial lending / CeFi yield	BTC is transferred to a counterparty that lends or deploys it for a promised rate.	Counterparty and rehypothecation risk. The 2022 model.	No
Wrapped BTC on other chains	BTC is locked with a custodian; a synthetic token is minted elsewhere.	Custodial, smart-contract, and peg risk.	No
Synthetic / derivative exposure	Structured or derivative products referencing BTC.	Basis, counterparty, and complexity risk.	No
Native programmable (Bitcoin-anchored L2)	BTC moved via audited tunnels; deployed under policy; settled back to Bitcoin.	Smart-contract and venue risk. Counterparty transfer minimized.	Yes

Source: authors' classification. Risk labels describe the dominant exposure each approach introduces, not an exhaustive list.

The 2022 baseline

The cautionary cases are recent and well-documented. The collapse of the Terra and UST stablecoin in May 2022 triggered the failure of the hedge fund Three Arrows Capital, which in turn cascaded through the lenders and exchanges exposed to it: Voyager and Celsius in July, then BlockFi, Genesis, and FTX. ⁶ Celsius had marketed yields approaching 20 percent that were not supported by sustainable activity. ⁷ Voyager had lent Three Arrows a sum it could not recover; BlockFi carried direct exposure to the same fund and a credit line from FTX that vanished when FTX failed.⁸

The common thread was not the rate. It was the structure. In every case, customers had surrendered control of their assets to a counterparty, and the counterparty's solvency proved to be the real issue. The architectures examined later in this paper are an attempt to keep that surrender from happening in the first place.

REFERENCES:

⁶ Cleary Gottlieb, Novel Issues in the Crypto Bankruptcy Cluster; Federal Reserve Bank of Chicago, A Retrospective on the Crypto Runs of 2022.
⁷ CNBC, July 2022, on Celsius yields that were not supported by sustainable activity.
⁸ CryptocurrencyHelp and Milk Road on Voyager's loan to Three Arrows and BlockFi's exposure plus the FTX credit line, 2022.

The evaluation framework

The framework comprises six pillars. Each is stated as a question a fiduciary should be able to answer before any Bitcoin leaves the treasury, followed by what a strong design looks like and the red flags that should stop a process. The pillars are ordered by precedence. Asset integrity and verifiability are threshold tests; a structure that fails them does not warrant evaluation on yield. Exhibit 2 summarizes the framework as an at-a-glance matrix.



Asset integrity

Core question.

Does the Bitcoin remain Bitcoin, under the holder's control, with settlement assured back to the base chain?

Signs of a strong design

Native BTC throughout, with keys controlled by the treasury or held under transparent, verifiable custody. No rehypothecation or reuse of the underlying. A deterministic path that returns value to Bitcoin for final settlement, with the mechanics documented and audited.

Red flags

Bitcoin is transferred onto a counterparty's balance sheet in exchange for a claim. A synthetic token whose backing depends on an issuer's continued solvency. Any arrangement where redemption is a promise rather than an enforceable, onchain mechanism.



Verifiability

Core question.

Can reserves and the source of yield be proven onchain, rather than taken on trust?

Signs of a strong design

Positions and reserves are verifiable directly onchain. Current third-party smart-contract audits with high test coverage, refreshed on a stated cadence. A yield source that can be inspected and attributed, not merely asserted.

Red flags

Opaque or self-reported reserves. Audits that are stale, partial, or absent. Returns described in marketing terms with no traceable origin. The phrase that should end a conversation is any version of "trust us."



Security architecture

Core question.

What does the system do when something fails, not only when it works?

Signs of a strong design

Authorization through hardware-wallet multisignature with a meaningful quorum. Human approval is required for sensitive actions. Circuit breakers, supply caps, and time delays on administrative powers, so that a single error or compromise cannot instantly drain the system. An active, funded bug-bounty program. An incident record that is either clean or disclosed and remediated in the open.

Red flags

Single-key or hot-wallet control of material funds. No breakers, caps, or delays. Administrative keys that can move or freeze assets immediately and irreversibly. A history of incidents that surfaces only through third parties.




<p> Control and reversibility</p> <p>Core question.</p> <p>Can the treasury exit on its own terms, and what discretion does it retain?</p> <p>Signs of a strong design</p> <p>A defined, enforceable exit with predictable timing. The ability to size a position deliberately and to phase in and out. Discretion that stays with the treasury rather than the provider.</p> <p>Red flags</p> <p>Lockups without recourse. Withdrawal gates that the provider can impose at its discretion. All-or-nothing structures that cannot be unwound in part. Any design where leaving requires the counterparty's cooperation.</p>	<p> Yield quality</p> <p>Core question.</p> <p>Where does the return actually originate, and is the source durable?</p> <p>Signs of a strong design</p> <p>An identifiable, economically grounded source, such as borrowing demand, market-making, or protocol fees. Venues that have been vetted and are subject to concentration limits. A return assessed net of the risk taken to earn it, not gross.</p> <p>Red flags</p> <p>Yield is funded by token emissions and presented as organic. Undisclosed or unvetted venues. Rates so far above the market that they imply leverage, duration, or counterparty risk that the treasury has not been shown.</p>	<p> Institutional fit</p> <p>Core question.</p> <p>Does the structure work within a regulated entity for its auditors and board?</p> <p>Signs of a strong design</p> <p>Positions that map to a recognizable accounting and reporting treatment. A clear jurisdictional and regulatory posture. Counterparties and operators who are identifiable, accountable, and operationally mature.</p> <p>Red flags</p> <p>Structures that an auditor cannot classify. Anonymous operators or undisclosed control. Jurisdictional ambiguity that leaves the treasury unable to describe what it owns or to whom it has recourse.</p>
---	--	--

Exhibit 2. (The six-pillar framework)

Pillar	What good looks like	Red flags
1. Asset integrity	Native BTC throughout; controlled keys or transparent custody; no rehypothecation; settlement assured back to Bitcoin.	BTC on a counterparty balance sheet; synthetic claim; redemption dependent on issuer solvency.
2. Verifiability	Onchain reserves and positions; current audits, high coverage; traceable yield source.	Opaque reserves; stale or absent audits; asserted but unverifiable returns.
3. Security architecture	Hardware multisig with quorum; human authorization; breakers, caps, delays; active bounty.	Single-key control; no breakers or caps; instant irreversible admin powers; hidden incidents.
4. Control & reversibility	Defined, enforceable exit; predictable timing; treasury retains discretion and can phase.	Lockups without recourse; provider-controlled gates; all-or-nothing positions.
5. Yield quality	Identifiable, durable source; vetted venues; concentration limits; net-of-risk return.	Emissions dressed as organic yield; undisclosed venues; rates implying hidden leverage.
6. Institutional fit	Recognizable accounting treatment; clear jurisdiction; identifiable, mature operators.	Unclassifiable structures; anonymous operators; jurisdictional ambiguity.

Source: authors' framework. Pillars are ordered by precedence; the first two are threshold tests.

Risk framework

A framework that only describes what good looks like is a brochure. This section sets out the risks that remain even in a well-designed structure, and is the more important half of the analysis. A treasury should expect any credible provider to discuss these openly. Reluctance to do so is itself a finding.

Smart-contract risk

Any onchain system runs on code, and code is an attack surface. The mitigants are known: independent audits with high coverage, formal verification where feasible, a funded bug-bounty program, and time in production at scale without incident. None of these reduces the risk to zero. The right posture is to treat audit recency and coverage, bounty size, and production track record as measurable inputs, and to weight them accordingly.

Bridge and tunnel risk

Cross-chain infrastructure was the single largest source of crypto losses in 2022. By one widely cited estimate, roughly 2 billion dollars was stolen from bridges that year, around 69 percent of all funds lost to hacks.⁹ The largest individual events are instructive. The Ronin bridge lost about 625 million dollars in March 2022 after attackers obtained five of nine validator signing keys.¹⁰ The Wormhole bridge lost roughly 325 million dollars in February 2022 to a forged signature that authorized a mint with no backing.¹¹ Nomad lost about 190 million dollars in August, and Harmony's Horizon bridge about 100 million dollars in June, the latter again through a small validator set, two keys of five.¹² The pattern is consistent: a small, trusted set of signers and a mint that was not properly verified against locked collateral.

This is the failure mode a Bitcoin-settling tunnel is designed to avoid. The design intent is verifiable movement of value with settlement assurance back to Bitcoin, rather than the unbacked minting of a synthetic token governed by a multisignature. That is a meaningful structural difference, and it is the right thing to interrogate. It is not a claim of immunity. A tunnel is still software, still audited rather than proven, and still carries risk. The question to ask is how the movement is verified and how settlement to Bitcoin is enforced, not whether the provider asserts the bridge is safe.

REFERENCES:

- ⁹ CNBC citing Chainalysis: approximately 2 billion dollars stolen from bridges in 2022, about 69 percent of hack losses.
- ¹⁰ Cointelegraph: Ronin bridge, March 2022, approximately 625 million dollars; five of nine validator keys compromised.
- ¹¹ AMBCrypto and Cointelegraph: Wormhole, February 2022, approximately 325 million dollars via a forged signature.
- ¹² Fortune and CNBC: Nomad, August 2022, approximately 190 million dollars; Harmony Horizon, June 2022, approximately 100 million dollars, two of five keys.



Cross-chain infrastructure was the single largest source of crypto losses in 2022

69%
of all funds lost to hacks.



Yield-source and venue risk

Yield inherits the risk of the venues that generate it. A return routed through lending markets, exchanges, or liquidity pools is exposed to the solvency and security of each. Diversification across vetted venues, explicit concentration limits, and the ability to inspect where capital is deployed are the controls that matter. A yield figure with no venue disclosure is not a yield figure. It is a marketing claim.

Liquidity and exit risk

The terms on which a treasury can leave are as important as the terms on which it enters. Withdrawal timing, market depth at the size held, and the existence of any discretionary gate all bear on whether a position can be unwound when needed rather than when permitted. These should be modelled before entry, not discovered during a drawdown.

Regulatory risk

The regulatory treatment of digital-asset instruments continues to evolve across jurisdictions, and classification can change. A treasury should understand how its position is characterized today, which authority has purview, and what a plausible change would mean for the holding. Jurisdictional clarity from the provider is part of the diligence, not an afterthought.

Risk budgeting for a treasury allocation

Productive Bitcoin should be sized to a defined loss tolerance and treated as a sleeve of the reserve, not the reserve itself. Phasing in allows a treasury to test operations, custody integration, and reporting at small scale before committing materially. The allocation that survives a bad year is the one that was sized to survive it.

What a Bitcoin-anchored model does not solve

Stated plainly, so there is no ambiguity. A Bitcoin-anchored, native-asset architecture changes the counterparty and custody profile of a position. It does not remove smart-contract risk. It does not eliminate venue or yield-source risk. It does not resolve regulatory uncertainty. And it is not a substitute for the holder's own custody discipline and policy controls. What it offers is a structurally better starting point, not a risk-free yield. Any provider claiming otherwise has told a treasury something useful about the provider.

A yield figure
with no venue
disclosure is not
a yield figure.

It is a marketing
claim.

Reference architecture

This section applies the framework to one worked example. Hemi is a modular Layer 2 anchored to Bitcoin and Ethereum. It is used here because it illustrates the native-asset approach that the framework rewards. The mapping below is held to what is publicly documented or reported by Hemi; specifics that require Hemi's own attestations are marked for completion.

How the workflow runs end-to-end

Native Bitcoin is held in institutional custody. An audited tunnel moves value to Hemi, where it is deployed across vetted venues in accordance with the treasury's policy. Returns and principal settle back to Bitcoin, with an audit trail at each step. The treasury's exposure is to the chain, the tunnel, and the venues it selects, not to a counterparty holding its Bitcoin.

The structural difference

Hemi's virtual machine embeds a full Bitcoin node within an Ethereum-compatible execution environment.¹³ Applications and treasury policies can therefore read native Bitcoin state directly, rather than operating against a synthetic representation of it. This is the mechanism behind the asset-integrity claim, and it is the line that separates a native-programmable design from a wrapped one. In a wrapped model, the asset a treasury holds is a token backed by Bitcoin held elsewhere, with the custodian's solvency as an embedded risk. In a native model, Bitcoin remains the asset.

Network context

Hemi launched its mainnet on 12 March 2025 with more than 440 million dollars in total value locked and over fifty ecosystem partners at launch.¹⁴ It was backed by a 15 million dollar seed round led by Binance Labs and Breyer Capital.¹⁵ Total value on the network reached roughly 800 million dollars within three weeks of launch¹⁶.

REFERENCES:

¹⁴ Coin Edition and TheStreet: Hemi mainnet, 12 March 2025, more than 440 million dollars TVL and over fifty ecosystem partners at launch.
¹⁵ Crypto Briefing: 15 million dollar seed round led by Binance Labs and Breyer Capital, September 2024.
¹⁶ Reflexivity Research: network value reached approximately 800 million dollars within three weeks of launch.
 Current figures of approximately 1.2 billion dollars and 90+ partners are as reported by Hemi.



In a native model, **Bitcoin** remains the asset.

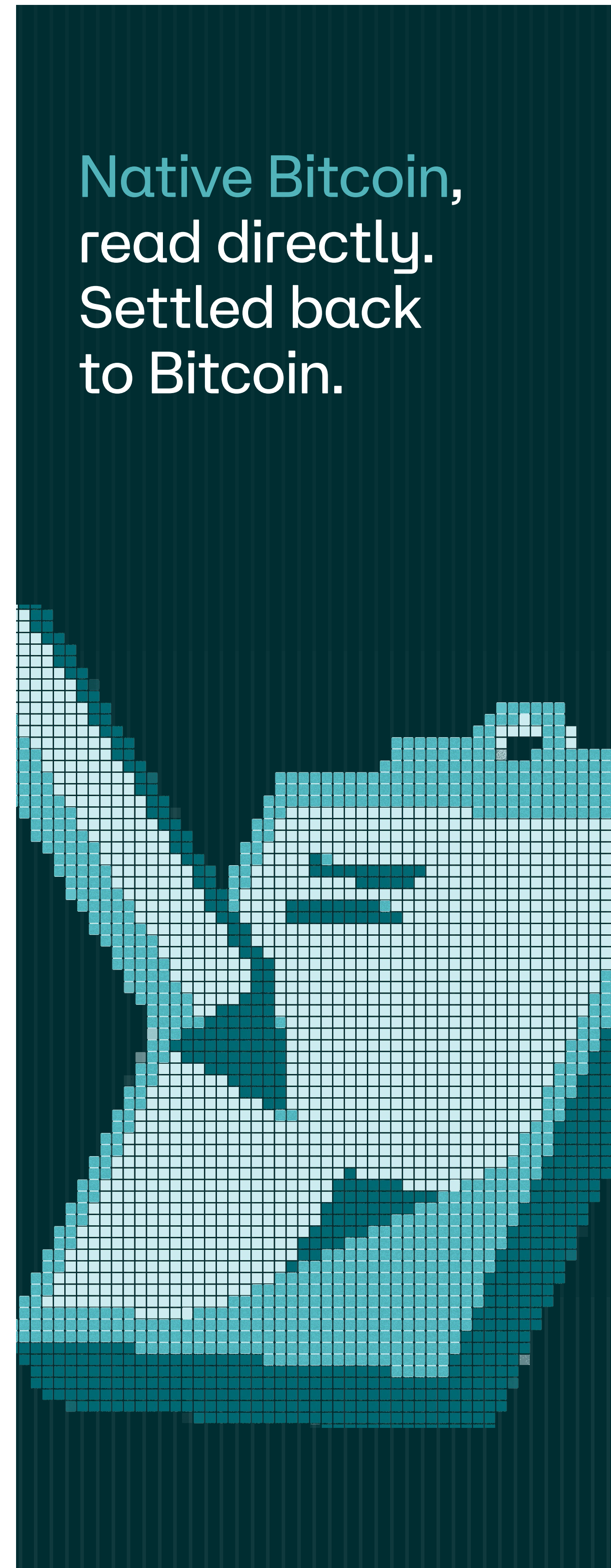
\$800m

Total value on the network reached within three weeks of launch.



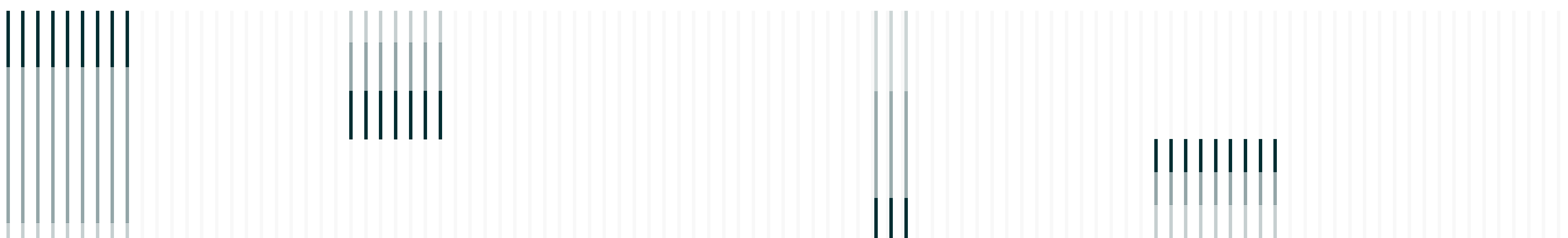
Exhibit 3. (Hemi mapped to the six pillars)

Pillar	How the reference architecture addresses it
1. Asset integrity	Native BTC throughout, read directly via the hVM; value settles back to Bitcoin.
2. Verifiability	Onchain positions; audited tunnels with a documented audit trail.
3. Security architecture	Bitcoin-settling tunnel design that avoids reliance on a small trusted signer set, with movement audited and settlement enforced back to Bitcoin.
4. Control & reversibility	Tunnels move value to and from Bitcoin on defined mechanics.
5. Yield quality	Deployment across an ecosystem of vetted venues.
6. Institutional fit	Identifiable team and partners; established network with public metrics.



How the use cases line up

Four uses recur in member questions, and each maps to the framework. Yield on idle treasury Bitcoin sits against Pillar 5. Liquidity without selling, retaining the position while accessing working capital, sits against Pillars 1 and 4. Programmatic policy enforcement within risk limits sits against Pillar 3. Auditable reporting for fiduciaries sits against Pillars 2 and 6.



Implementation considerations

Moving from evaluation to a live position involves work across custody, policy, accounting, and governance. The notes below are practical starting points, not a substitute for a treasury's own controls and advisors.

Custody integration

Determine how native Bitcoin is held and how it enters and exits the tunnel. The objective is to retain control and a clear chain of custody throughout, with no point at which the asset becomes a counterparty's liability. Test the full round trip at a small scale before committing materially.

Policy and signing

Encode the treasury's existing investment policy into the signing and authorization model, rather than relaxing the policy to fit the product. Quorum requirements, human authorization for sensitive actions, and limits on size and venue should mirror what the treasury already enforces elsewhere.

Sizing and phasing

Begin with a sleeve sized to a loss the treasury can absorb without consequence, and expand only after operations, custody, and reporting have been validated in production. Phasing is risk management, not timidity.

Accounting and reporting

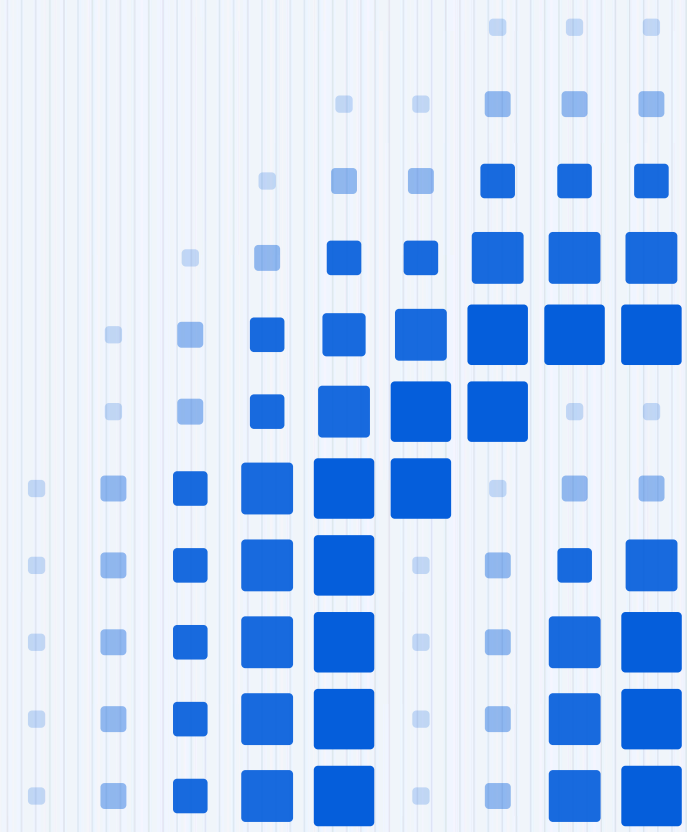
Confirm how each position is classified for financial reporting and how it interacts with fair value treatment of the underlying Bitcoin. Engage the external auditor early. A structure that cannot be cleanly reported will create friction at every quarter close, regardless of its returns.

Internal approval and the board

Package the decision as the framework applied to the specific balance sheet, with the risk section addressed explicitly. Boards and investment committees approve documented reasoning, not vendor enthusiasm. The output of the working session described in Section 8 is designed to be exactly that package.



Test the full round trip at a small scale before committing materially.



The path forward

The framework gives a treasury the criteria to evaluate any provider of productive Bitcoin infrastructure on its merits.

It is deliberately neutral, and it applies equally to options not named in this paper.

Applying it is the step that cannot be done on one's own. The right configuration depends on a treasury's custody setup, its policy constraints, and the venues it is willing to use. For members who want to move from reading the framework to scoping it against a specific balance sheet, Hemi's team offers a working session. The treasury brings its constraints. Hemi maps where native Bitcoin remains native, how value moves and returns to Bitcoin for settlement, and which vetted venues align with the treasury's risk posture. The output is a board-ready view, structured around the six pillars, not a sales pitch.



For members who are at the reading stage, that is the right place to be. The framework is the foundation.

Apply it when the question is live on the balance sheet.

Appendix

Methodology

The six pillars are derived from three inputs: the questions institutional Bitcoin holders raise most often about productive Bitcoin; the post-mortems of the 2022 lending and bridge failures, which isolate the structural causes of loss; and established institutional practice in custody, audit, and treasury risk. The framework is intended to be provider-neutral and to remain stable as specific products change.

Glossary

- **Native BTC** Bitcoin held as the base-chain asset itself, rather than a token representing it on another chain.
- **Wrapped BTC** A token on another chain backed by Bitcoin held with a custodian; a claim, not the asset.
- **Tunnel / bridge** Infrastructure that moves value between chains. Designs differ widely in how movement is verified and secured.
- **Rehypothecation** Reuse of a customer's pledged assets by the party holding them, a central cause of the 2022 failures.
- **Proof of reserves** Verifiable, typically onchain, evidence that reserves backing a claim actually exist.
- **hVM** Hemi's virtual machine, which embeds a full Bitcoin node within an Ethereum-compatible execution environment.
- **Circuit breaker** A control that halts or limits activity automatically when defined thresholds are breached.
- **Fair value (ASU 2023-08)** The accounting standard requiring qualifying crypto assets to be measured at fair value, with changes in net income.

About and disclosures

Hemi is a modular Layer 2 anchored to Bitcoin and Ethereum.

Important disclosures. This paper is provided for research and educational purposes. It is not investment, legal, tax, or accounting advice, and it is not an offer or solicitation to buy or sell any asset or to use any service. Digital assets carry significant risk, including the risk of total loss. Past performance does not indicate future results. Network and holdings figures are current as of the dates cited and will change. Statements about future plans are forward-looking and not guarantees. Readers should consult their own advisors before making any decision.

References

1. FASB, ASU 2023-08, Accounting for and Disclosure of Crypto Assets (Subtopic 350-60), effective for fiscal years beginning after 15 December 2024. Deloitte, Heads Up (2023). [dart.deloitte.com](https://www.deloitte.com)
2. Cryptobriefing, Institutions now hold 18.5% of all Bitcoin (2026). cryptobriefing.com
3. BitcoinTreasuries.net, public-companies and category data (2026). bitcointreasuries.net
4. MicroStrategy / Strategy, Q1 2025 results, Form 8-K (May 2025); Strategy holdings, BitcoinTreasuries.net. [sec.gov](https://www.sec.gov)
5. Deloitte, application guidance on the pre-ASU cost-less-impairment model for crypto assets (2024). [deloitte.com](https://www.deloitte.com)
6. Cleary Gottlieb, Novel Issues in the Crypto Bankruptcy Cluster; Federal Reserve Bank of Chicago, A Retrospective on the Crypto Runs of 2022. [clearygottlieb.com](https://www.clearygottlieb.com)
7. CNBC, How the fall of Celsius dragged down crypto investors (2022). [cnbc.com](https://www.cnbc.com)
8. CryptocurrencyHelp, What happened to Celsius, BlockFi and Voyager; Milk Road, BlockFi bankruptcy overview. cryptocurrencyhelp.com
9. CNBC, Hackers have stolen \$1.4 billion this year using crypto bridges (2022); Chainalysis estimates via The Block. [cnbc.com](https://www.cnbc.com)
10. Cointelegraph, The 10 largest crypto hacks and exploits in 2022 (Ronin). cointelegraph.com
11. AMBCrypto / Cointelegraph, Wormhole bridge exploit, February 2022. ambcrypto.com
12. Fortune, 5 biggest crypto hacks of 2022 (Nomad, Harmony). [fortune.com](https://www.fortune.com)
13. TheStreet, With \$440M in TVL, Hemi Labs launches its mainnet (hVM). [thestreet.com](https://www.thestreet.com)
14. Coin Edition, Hemi Mainnet Launches with Over \$440M TVL, 50+ Ecosystem Partners (March 2025). coinedition.com
15. Crypto Briefing, Hemi launching mainnet on March 12 (\$15M seed, Binance Labs and Breyer Capital). cryptobriefing.com
16. Reflexivity Research, Hemi Q1 2025 Overview (TVL reached approximately \$800M within three weeks). x.com/reflexivityres
17. Coin Bureau, What Is Wrapped Bitcoin (WBTC): custody and counterparty risk (2026). coinbureau.com
18. Hemi, network figures as reported by Hemi (2026).