Hemi Overview

Layer 1 blockchains have historically evolved as isolated networks, each with strengths and limitations, operating independently and unaware of any other chain. Bitcoin, over its 16-year history, has proven that it excels in security, decentralization, and as a store of value. However, the Bitcoin network has very limited native programmability, and its conservative development cycle has moved at a glacial pace compared to other blockchains. Ethereum, on the other hand, is the industry leader in smart contracts, programmability, and developers but has not attained the same level of security and asset value as Bitcoin. Despite nearly a decade of co-existing, Bitcoin and Ethereum still lack robust interoperability and thus are not able to mutually benefit from exploiting each other's value propositions.

Logically, the crypto ecosystem has long sought a solution combining the best of both blockchains: the security of Bitcoin and the programmability of Ethereum. There have been numerous attempts over the years to fuse the best qualities of existing blockchains into new models, but, generally speaking, these projects often rely on weak points like centralized bridges, compromise on finality and decentralization, or provide limited features that fail to serve many of the modern interoperability use cases seen between other chains.

Rather than follow the existing playbook, Hemi has created a new model. Hemi is a Layer-2 (L2) protocol that integrates both Bitcoin and Ethereum directly into a single supernetwork rather than treating them as individual silos. By deploying a modular approach and embedding a full Bitcoin node directly into an Ethereum-compatible Virtual Machine (the Hemi Virtual Machine, or hVM), Hemi offers developers an environment where Bitcoin and Ethereum states coexist natively. This innovation paves the way for secure, scalable, and truly interoperable decentralized applications (dApps), unlocking next-generation Bitcoin DeFi and delivering

superfinality secured by Bitcoin's proof-of-work (PoW).

What Are Bitcoin L2s?

Layer 2 (L2) solutions on the Bitcoin network represent a significant step forward in addressing the inherent limitations of the blockchain's original design. These solutions aim to enhance scalability, programmability, and functionality, leveraging the robust foundation provided by Bitcoin. Bitcoin L2 solutions are designed to operate atop the Bitcoin blockchain, utilizing it as a foundational asset and a settlement layer to enforce transactions. Through the use of execution layers capable of running Turing-complete virtual machines—including the Ethereum Virtual Machine (EVM)—Bitcoin L2 projects aspire to imbue the Bitcoin network with the capacity to support smart contracts and other advanced blockchain applications. This allows for the transfer of Bitcoin-based assets to L2, where they can be used in advanced DeFi protocols, with the capability to withdraw the underlying assets back to the primary layer, ensuring a functional dependence on the Bitcoin network.

While there are many different approaches, L2 technologies broadly in the crypto ecosystem can generally be grouped into two categories:

1. **State channels, which are short-lived isolated systems that are initialized on the L1 by users, are updated off-chain for a period of time and eventually settled back to the L1 and closed out.**
2. **L2 chains (including sidechains, rollups, and validiums) are long-lived blockchains with their own consensus that users can enter/leave at any time. Users can deposit assets from the L1 to the L2 and settle back to L1 as desired.**

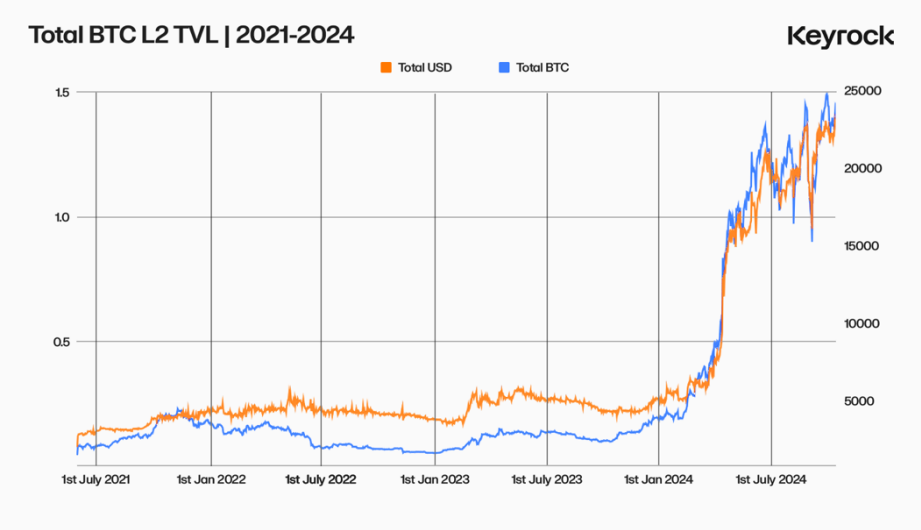
Both approaches serve different use cases. State channels are simpler and can provide extremely cheap and near-instant transactions between small groups of users but are generally extremely feature-limited and short-lived. L1-dependent chains are more complicated, more expensive, and slightly slower, but they can support any number of users with all the features of a complete blockchain and allow users to independently move assets to/from the L2 at any time. Over the last few years, the blockchain industry has primarily focused on L2 chains due to their ability to serve the evolving needs of increasingly complex blockchain use cases. In particular, rollups and validiums now comprise a significant portion of the Ethereum ecosystem's throughput due to their improved settlement security posture compared to the older side-chain

architecture.

Generally speaking, at the heart of these modern L2 chains is the bifurcation of the blockchain network into four synergistic layers: the data availability (DA) layer, the consensus layer, the settlement layer, and the execution layer. The DA layer ensures that the actual data that comprises the L2 chain is publicly available, which ensures that users of the network are able to see the current state and, where relevant, use this knowledge to challenge invalid L2 settlement operations. The consensus layer determines what transactions are considered part of the canonical L2 chain. The settlement layer enables withdrawals and other L2-to-L1 messages to be securely passed, ensuring bidirectionality of the flow of assets and information between the two networks. Finally, the execution layer processes L2 transactions and their corresponding updates to the L2 state machine.

However, Bitcoin's technical limitations have made the deployment of many L2 innovations from other ecosystems difficult. In particular, Bitcoin's lack of Turing-complete smart contracts and global state accessible and mutable during transaction execution has made it difficult to implement secure settlement solutions. Furthermore, cloning existing L2 architectures for use on Bitcoin has resulted in solutions that provide limited awareness of Bitcoin itself, requiring users to bridge funds to the L2 and be exposed to these less-than-ideal settlement solutions to engage with applications that could be better implemented by direct Bitcoin interoperability.

Despite these challenges, Bitcoin L2 solutions experienced unprecedented growth in 2024, with Total Value Locked (TVL) surging by over 700%, surpassing the combined growth of the previous three years. This exponential increase marked a significant inflection point, accelerating the ecosystem's expansion nearly fivefold within ten months.



Source: Keyrock

Types of L2s

Several paths have emerged for scaling Bitcoin Layer 2, each with its unique attributes and limitations:

- State channels (ex.g., Lightning Network): State channels represent the foundational layer of L2 solutions, offering a streamlined approach to transaction scalability. By establishing off-chain payment channels, state channels facilitate instantaneous and cost-efficient transactions between parties. The Lightning Network stands as the most notable implementation, enabling private transactions without necessitating broadcast on the Bitcoin mainnet. Considered an orthodox scaling approach due to its proximity to Bitcoin core developers, it has faced relatively niche adoption and increasing scrutiny over its ~6-year history.
- Sidechains (ex: Stacks): Diverging from the simplicity of state channels, sidechains are autonomous blockchains that operate with distinct consensus mechanisms and validator sets. These platforms conduct transactions independently of the Bitcoin network, settling and finalizing transactions within their own framework. Projects like Stacks illustrate the potential to inherit security aspects from Bitcoin through unique mechanisms such as proof-of-transfer, although such an approach tightly couples sequencing with Bitcoin security inheritance, posing transaction censorship risks.

Examples like Rootstock and Stacks V1 exemplify live implementations, showcasing the versatility and customization potential of sidechains.

- Client-side validation (e.g., RGB): Adhering to and building upon Bitcoin's UTXO model and state channel technology enables off-chain clients to handle complex transactions securely. However, programmability is still limited, both counterparties to a transaction must be online to transact, and the architectural differences mean the last decade of DeFi innovation can't be easily adapted to run on client-side validation systems.
- Rollups: Rollups execute transactions off the base layer and compress them for efficient on-chain storage. Rollups achieve significantly higher throughput and cost efficiency while remaining tightly coupled with their base chain by leveraging transaction batching and data availability from the parent blockchain. In the Ethereum world, Rollups are further divided into zk-Rollups, which use cryptographic proofs for immediate validation, and Optimistic Rollups, which assume validity but allow for dispute resolution within a predefined window. Due to Bitcoin's limitations, the only practical rollup with trust-minimized settlement combines these two technologies, using zero-knowledge proofs that are optimistically verified through a dispute system. This approach provides scalable, versatile frameworks for applications, from single-use cases to hosting multiple decentralized apps (dApps). Some developers have also built Sovereign Rollups, which only use the underlying blockchain as a data availability mechanism but do not facilitate the bridging of assets to/from the base layer or any other direct interoperability.

Type	Security Model		Trust Assumptions	Examples
	Consensus	**Fund Custodianship**		
State Channels	N/A	Bitcoin mainnet	Trustless, online channel participants	Lightning Network
Sidechains	Native	Federated Peg	Threshold of sequencers can censor and reorg, threshold of peg operators can steal funds	Liquid Network
	Native + Bitcoin Anchoring	Overcollateralized Decentralized Custodianship	Threshold of native sequencers can censor and reorg, collateral must exceed value of BTC deposits	Stacks v1
	Merged-mining	Federated Peg	Minority of Bitcoin miners can censor and reorg for “free,” threshold of peg operators can steal funds	Rootstock v1
	Merged-mining	BitVM Variant	All N-of-N bridge operators must collude to steal funds	Rootstock “v2” (Future)
	Merged-mining	BIP-300	Minority of Bitcoin miners can censor and reorg for “free,” majority of Bitcoin miners can steal funds	Drivechains

Optimistic +ZK Rollups	Native	BitVM Variant	Native sequencers can perform short reorgs, all N-of-N bridge operators must collude in order to steal funds. Full Bitcoin security for long reorgs.	Citrea
	Merged-Mining	BitVM Variant	Minority of Bitcoin miners can perform short reorgs, all N-of-N bridge operators must collude in order to steal funds. Full Bitcoin security for long reorgs.	BOB
Sovereign Rollups	Native	N/A	Native sequencers can perform short reorgs, full Bitcoin security for long reorgs. Note: No settlement to Bitcoin.	Rollkit Framework

Hemi: A New Approach to Bitcoin L2s

Though architected with different priorities and trade-offs, Hemi's design philosophy encompasses that Bitcoin and Ethereum are not mutually exclusive, nor should they remain perpetually siloed. Instead, their unique attributes (Bitcoin's robust security and immutable settlement assurances and Ethereum's versatile programmability and composability) can be woven into a unified platform. Hemi posits that these two leading blockchains are complementary components of a broader supernetwork, a next-generation paradigm where value, data, and logic flow freely without compromising trust or relying on brittle bridging structures.

The Supernetwork Vision

Traditionally, developers building cross-chain applications face persistent challenges: maintaining separate codebases, managing risks posed by different interoperability systems, and navigating the complexities of bridge risks such as censorship, hacks, or multisig key compromises. Within Hemi's supernetwork, however, these challenges are mitigated by instituting a single, cohesive environment where both Bitcoin and Ethereum states are first-class citizens.

By doing so, Hemi breaks down the walls between these ecosystems. This approach transforms Bitcoin from a passive reserve asset or settlement layer into a fully accessible data source and programmable foundation within Ethereum's established smart contract environment. At the same time, it enhances Ethereum's security posture and trust assumptions by embedding real-time connections to Bitcoin's PoW consensus.

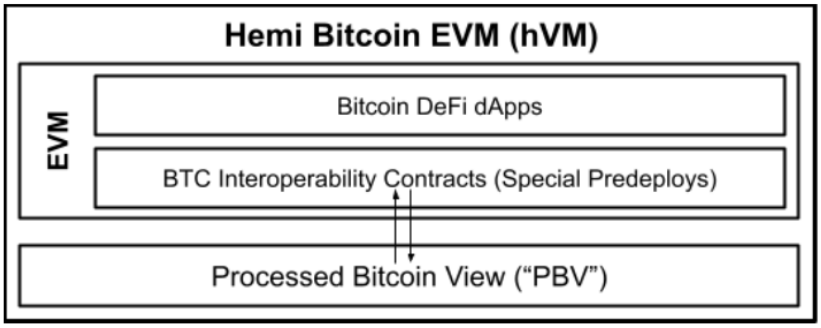
Hemi Virtual Machine (hVM)

At the heart of Hemi's architecture is the Hemi Virtual Machine (hVM), an execution environment that integrates a fully operational Bitcoin node directly within what otherwise functions like a standard EVM. Unlike approaches that rely on external oracles, off-chain relayers, or constrained bridging mechanisms, the hVM provides a single, unified framework where Ethereum-compatible smart contracts can interact with Bitcoin data and logic at a granular level.

With the hVM, developers gain real-time access to Bitcoin's state - things like confirmations, block headers, UTXOs, transaction indices, and fee rates - without leaving the Ethereum development paradigm. This native integration allows smart contracts to validate Bitcoin transactions, track Bitcoin balances, and enforce complex conditions based on the chain's history and consensus. By removing the need for external verification layers or trust in intermediaries, the hVM unlocks a new realm of cross-chain dApps, enabling sophisticated trustless or trust-minimized Bitcoin-based financial instruments, cross-chain liquidity protocols, and advanced DeFi primitives historically out of reach.

Because the hVM is fully backward-compatible with the Ethereum toolchain, developers can design applications that leverage this advanced Bitcoin introspection using familiar languages like Solidity. Existing Ethereum development tools like compilers, debugging tools, and libraries remain fully usable. This is a huge win as it means a lending protocol can, for instance, require proof that certain BTC is locked in a specific way before authorizing a loan disbursement on

Ethereum. This level of advanced coordination with Bitcoin no longer requires specialized languages, custom toolkits, or trusted oracle/relayer systems.



DeFi apps query new Bitcoin interoperability predeploys which communicate with the PBV.

Source

We can summarize hVM's key advantages as follows:

- **Native Bitcoin Integration:**
  By running a Bitcoin node internally, the hVM can directly validate Bitcoin transactions and observe the UTXO table. Developers can use hVM's deep Bitcoin state awareness to implement trustless non-custodial DEXes, lending markets, staking protocols, custom Bitcoin custodianship systems, cross-chain payment routing systems, and more - all with normal Solidity code.
- **Ethereum Compatibility:**
  The hVM does not force developers to reinvent their toolchains or learn new languages. Existing Ethereum infrastructures and skill sets apply directly. The only difference is that the contract environment is now Bitcoin-aware, allowing entirely new classes of dApps to be built.
- **Reduced External Dependencies:**
  By incorporating full Bitcoin capabilities on-chain, the hVM eliminates the reliance on off-chain verifiers, trusted intermediaries, and complex relay networks for observing the Bitcoin state. This reduces both the attack surface and the complexity of cross-chain integrations.

As the Bitcoin L2 ecosystem matures, innovations like the hVM will set a new standard for cross-chain programmability. Hemi's approach is no less than a breakthrough in cross-chain application design: a fully integrated, high-security structure where Ethereum-compatible contracts enjoy direct access to Bitcoin's ledger.

Hemi Bitcoin Kit (hBK)

The Hemi Bitcoin Kit is a dedicated toolkit designed to streamline the developer experience and accelerate time-to-market for new projects wanting to use hVM's advanced Bitcoin introspection. Developing cross-chain dApps often involves a steep learning curve: navigating Bitcoin's UTXO model, tracking Bitcoin consensus and validating Merkle proofs, or parsing raw Bitcoin transactions can be daunting even for seasoned Ethereum developers.

However, hBK is essentially a developer accelerator offering:

- **Developer-Friendly APIs and Libraries:**
  hBK provides high-level abstractions that encapsulate complex Bitcoin operations. Instead of processing raw Bitcoin transaction data, developers can call well-documented APIs that return interpreted transaction details, validated block headers, and information about the UTXO table.
- **Integration with hVM:**
  These libraries are tailored to the hVM environment, ensuring that Bitcoin state queries are performed efficiently and safely. For example, developers can query the Bitcoin state to trigger a smart contract function in response to a certain UTXO state change without writing custom indexing logic or dealing with the intricacies of Bitcoin data serialization.
- **Reduced Complexity and Development Overhead:**
  By handling the low-level details under the hood, hBK dramatically reduces development overhead. Projects can prototype Bitcoin-aware applications more rapidly and reliably.

Encapsulation

Hemi introduces encapsulation as a new approach to enhance the portability, security, and composability of digital assets. Encapsulation involves wrapping any digital asset - whether it's

a Bitcoin-based NFT, an ERC-20 token, or something else - into an NFT container that inherits advanced features by default.

With encapsulation, each wrapped asset can carry metadata, logic, and policy controls such as on-chain password protection, two-factor authorization (2FA), time-lock conditions, or gasless transfer capabilities. So, for example, consider a scenario where a cross-chain lending NFT holds Bitcoin collateral and Ethereum liquidity tokens.

Encapsulation allows the NFT to enforce withdrawal rules, slashing conditions, or provide other asset management functionality like transaction re-routing, gas subsidies, and more. Instead of relying on standalone contracts or complex bridging scripts, the encapsulated NFT itself enforces trust conditions at the protocol level, making it far less complicated to add sophisticated functionality. With encapsulation, managing Bitcoin and Ethereum assets together becomes easier and more secure.

What Can Be Built with Hemi?

Hemi is a platform that goes beyond interoperability. Thanks to the integration merging Bitcoin's security and Ethereum's programmability into a single entity, developers can build an entirely new class of dApps. This opens up development opportunities for countless ideas that would otherwise be impossible.

Some examples include the following:

- **Trustless Bitcoin (Re)Staking Protocols:** Hemi enables a model where native Bitcoin or Bitcoin-derived assets can secure other protocols.
- **Bitcoin-Authenticated AI Model Marketplaces:** Hemi's hVM can timestamp model weights on Bitcoin and integrate zero-knowledge proofs for verification of inference execution against open-source or proprietary models, an important feature for developing trustworthy AI applications.
- **Non-Custodial BTC Escrow and Lending:** Hemi's native Bitcoin awareness allows lending protocols to directly lend out native BTC against Ethereum-based collateral.
- **Bitcoin MEV Marketplaces / Transaction Accelerators:** A smart contract protocol can leverage Hemi's Bitcoin awareness to connect Bitcoin users and miners in a permissionless marketplace where users can pay Bitcoin transaction fees in any asset or predicate payout conditions based on the specific ordering of Bitcoin transactions in blocks.
- **Non-Custodial Exchanges:** Users can buy and sell Bitcoin-based assets (Bitcoin, BRC-20s, Runes, Ordinals NFTs, etc.) without ever having to transfer the asset off of Bitcoin.

The power of the hVM's Bitcoin programmability also enables developers to build bespoke Bitcoin interoperability infrastructure rather than enshrining rigid interoperability solutions directly into the protocol. For example, this allows the creation of custom bridge technologies optimized for specific use cases or Bitcoin smart wallets with configurable custodianship systems.

Technical Architecture and Components

Hemi's architecture can be viewed as a carefully orchestrated combination of subsystems, each addressing a critical challenge in blockchain interoperability and security. Collectively, these components redefine what developers and users can expect from an L2 protocol on Bitcoin, which increasingly demands trust-minimized, highly composable, and user-friendly environments alongside secure access to Ethereum's diverse asset ecosystem.

Source

Nodes and Participants in PoP Mining

PoP consensus relies on a set of specialized nodes and participants, each playing a distinct role in ensuring accurate state publication and timely finalization. To perform PoP publications of Hemi state to Bitcoin and inherit Bitcoin security:

1. **A Bitcoin-Secure Sequencer (BSS) node produces a new block on the Hemi L2, which is broadcast to all other BSS nodes on the Hemi network over P2P, and this new header is also communicated to all BFG nodes.**
2. **Proof-of-Proof (PoP) Miners acquire the new Hemi L2 block header from BFG nodes.**
3. **PoP Miners encode this new Hemi block header in a Bitcoin transaction, paying BTC transaction fees to publish Hemi chain state information to the Bitcoin network. They send these signed Bitcoin transactions to BFG nodes for propagation.**
4. **Bitcoin Finality Governor (BFG) nodes propagate these Bitcoin transactions over Bitcoin's P2P network for inclusion in Bitcoin blocks.**
5. **BFG nodes monitor the Bitcoin network for inclusion of these Bitcoin transactions and use these publications of the Hemi chain state to determine Bitcoin finality for the Hemi network. The publication status of the Hemi chain in Bitcoin is communicated to BSS nodes, who use this information for determining Hemi consensus.**
6. **A BSS node produces a new Hemi L2 block which contains updated Bitcoin consensus information, which communicates the latest Bitcoin block containing these PoP publications to the deterministic Bitcoin node embedded in the Hemi Virtual Machine (hVM) nodes.**
7. **After a period of time, hVM nodes use their embedded Bitcoin node to calculate and execute the payouts that PoP miners receive for securing the Hemi network to Bitcoin.**

Proof-of-Proof (PoP) Consensus

Traditional Proof-of-Stake (PoS) and PoW systems have well-known limitations. Pure PoS systems, while efficient, can suffer from weak subjectivity and are vulnerable if a malicious party accrues a majority stake. Mature pure PoW systems like Bitcoin, on the other hand, offer strong

subjectivity but are expensive and difficult to bootstrap. Hemi's Proof-of-Proof (PoP) consensus addresses these challenges by linking the Hemi network's state to the Bitcoin blockchain, effectively combining PoS-like efficiency with the ironclad security of Bitcoin's PoW. This hybrid approach creates a robust security model that gets the best of both worlds.

Source

How PoP Works

At the heart of Proof-of-Proof (PoP) is a mechanism that anchors the state of the Hemi blockchain to the Bitcoin network in an entirely decentralized and permissionless manner. This is achieved through the periodic inclusion of Hemi's state proofs—cryptographic commitments that represent recent segments of the Hemi chain—into the Bitcoin blockchain by PoP miners. Any user with BTC to pay fees can participate in PoP mining. These state proofs serve as a verifiable snapshot of the Hemi network's state at a particular point in time, which the Hemi protocol uses for fork resolution.

This anchoring process is not continuous; it occurs at carefully calibrated intervals. The frequency of these publications is designed to strike a balance that maximizes security while minimizing the load on the Bitcoin network and security costs to the Hemi protocol. By choosing a measured cadence, Hemi ensures the integrity of its chain without overburdening Bitcoin's decentralized infrastructure.

The end result of this process is that blocks on the Hemi network achieve superfinality after approximately 90 minutes, and transactions within these blocks are as secure as transactions on Bitcoin itself.

The inclusion of these state proofs in Bitcoin brings a unique advantage. Bitcoin's global network of miners and its immense hash power provide unparalleled security. By leveraging this security, any attempt to alter or rewrite Hemi's chain history would require an adversary to successfully 51% attack Bitcoin itself. This would involve not only overpowering Bitcoin's miners but also maintaining dominance long enough to manipulate both networks—a feat that is prohibitively expensive and logistically infeasible, even for state-level adversaries.

Unlike other approaches to Bitcoin security inheritance, like Merged-Mining, Proof-of-Proof inherits Bitcoin's full native security without requiring the participation or permission of any Bitcoin miner. Additionally, PoP decouples block creation from long-term block finality, enabling PoP-secured networks to leverage any consensus protocol for decentralized network sequencing.

Furthermore, PoP's architecture allows it to be efficiently extended to secure an unlimited quantity of additional chains through the Hemi network as a security aggregation layer without increasing the transaction costs or Bitcoin footprint of the protocol. This functionality enables Hemi to offer a secure ecosystem for the deployment of L3 networks that all share mutual Bitcoin finality for secure cross-chain settlement while providing these chains with the flexibility to customize their block production protocol to suit their decentralization and throughput needs.

1. **Bitcoin-Secure Sequencers (BSS):**
   BSS nodes manage to produce and sign new Hemi blocks and track Hemi's consensus based on its native sequencing protocol and publications of the Hemi chain state to Bitcoin, communicating the current state of the Hemi chain to hVM nodes for state transition processing. BSS nodes also direct hVM to calculate the payout of rewards to PoP miners who successfully publish Hemi consensus data to Bitcoin to provide the network with Bitcoin security and ensure the execution of these payouts in the Hemi chain.
2. **Bitcoin Finality Governor (BFG) Nodes:**
   BFG nodes orchestrate the relationship between Hemi and Bitcoin. Upon receiving new Hemi block headers from BSS nodes, BFG nodes forward these headers to PoP Miners. Later, once PoP Miners return signed Bitcoin transactions embedding these headers, BFG nodes propagate them into the Bitcoin network. BFG nodes also track the publication state of Hemi on Bitcoin and provide Bitcoin Finality information for Hemi chain segments.
3. **PoP Miners:**
   PoP Miners are decentralized participants who take Hemi's block headers (provided by BFG nodes) and encode them into signed Bitcoin transactions. They return these transactions to BFG nodes, which then broadcast them to the Bitcoin network. By doing so, PoP Miners effectively publish Hemi's state proofs on Bitcoin.

PoP Miners pay Bitcoin transaction fees to ensure their PoP transactions are mined into Bitcoin blocks. In return for their service, they receive rewards from the Hemi protocol once the PoP publication is confirmed. Their incentives encourage fast publication and honest participation, as timely inclusion in Bitcoin blocks leads to higher relative rewards.

4. **Hemi Virtual Machine (hVM) Nodes:**
   hVM nodes process all of the transactions on the Hemi network and consist of an EVM environment augmented with an embedded deterministic Bitcoin full node peered with the Bitcoin P2P network which is directly accessible through precompile contracts available to hVM smart contracts. After the PoP mining window closes for a given segment, hVM nodes use their indexed Bitcoin data to calculate PoP payouts owed by the protocol to PoP Miners. Finally, hVM nodes also monitor for new Bitcoin blocks over Bitcoin P2P and generate new Bitcoin Attributes Deposited transactions, which communicate this updated Bitcoin information to the Hemi protocol when generating block bodies for a BSS node running in sequencer mode.

Source

Tunneling System

The movement of assets across chains has been a persistent headache in the blockchain industry, often requiring trust in third-party custodians, complex cryptographic schemes, or extended finalization periods that diminish user experience. Hemi's Tunneling System addresses these pain points with a trust-minimized, protocol-level approach that stands apart from the conventional bridges model.

Tunnels rely on the hVM's intrinsic capacity to read and interpret both Bitcoin and Ethereum states without recourse to off-chain relays or oracles. This greatly reduces the need for trust. Users know that cross-chain asset movements are validated and enforced at the protocol level rather than by a handful of off-chain actors.

So, when a user moves BTC into Hemi, the Bitcoin Tunnel locks the BTC on the Bitcoin chain in a secure, decentralized custodianship system and mints a corresponding representation on Hemi. When Bitcoin assets are withdrawn, the Hemi protocol instructs the custodianship system to securely transfer the assets, and leverages its Bitcoin awareness to ensure appropriate behavior and enforce penalties for misbehaving or offline participants. Similarly, Ethereum assets are locked in secure smart contracts on the Ethereum chain, and can be withdrawn by users with a

valid cryptographic withdrawal proof. This creates a fluid continuum where assets can circulate freely between the chains, benefitting from Bitcoin's liquidity and Ethereum's programmability simultaneously.

Hemi's unique position with native connectivity to both Bitcoin and Ethereum also makes it possible for assets to flow *between* these ecosystems through Hemi – for example, securely tunneling Bitcoin assets *through* Hemi into the broader Ethereum ecosystem.

Hemi will launch with an economically secure over-collateralized BTC custodianship system and will transition to a variant of BitVM2, which replaces superblock light-client emulation with a more secure and robust system that leverages hVM as a censorship-resistant external observer of Bitcoin consensus to reflect correct Bitcoin state back to on-Bitcoin contracts for cross-chain state validation.

Security and Finality

Security and finality are foundational to blockchain infrastructure, directly shaping trust for users and developers alike. Hemi's architecture is designed to exceed the security standards of traditional Layer 2 (L2) solutions by delivering robust resistance to censorship and strong settlement assurances. Proof-of-Proof provides the Hemi network with the full security assurances of Bitcoin, providing network participants with iron-clad finality assurances.

Proof-of-Proof's design also enables Hemi to decentralize the network's sequencer using a liveness-preserving and decentralization-optimizing sequencing protocol based on Ethereum-style PoS, which the team expects to activate in 2025. By integrating this native PoS validator framework with Bitcoin's PoW security through the Proof-of-Proof (PoP) mechanism, Hemi introduces a level of decentralized security that sets it apart from other L2 environments.

Security in Hemi is a multi-layered approach. It combines stake-based sequencing, Bitcoin-anchored proofs of chain state, and incentive-aligned actor behavior. The PoP mechanism functions as a checkpoint system, leveraging Bitcoin's global hash power to secure the Hemi chain, rendering rollback attempts economically unviable and logistically impractical.

After approximately nine Bitcoin blocks (around 90 minutes), it is impossible to revert a Hemi block without attempting a reorganization of Bitcoin itself. Shortly thereafter, it achieves superfinality, or the point at which Hemi starts to become incrementally more secure than Bitcoin. At this stage, the cost and complexity of reversing Hemi's chain state are prohibitively

high, requiring an attacker to simultaneously compromise Bitcoin and Hemi's native block production consensus protocol. Unlike pure PoS systems that are susceptible to long-range attacks or weak subjectivity and optimistic rollups that rely on extended dispute windows, Hemi uses Bitcoin's immutable ledger as a real-time security anchor. This approach eliminates these vulnerabilities, providing unparalleled finality. Superfinality ensures that once Hemi blocks are confirmed, they are irreversibly final, enabling high-value applications requiring the highest security and permanence levels.

Source

Validator and Miner Behavior

Hemi's hybrid model relies on carefully structured incentives for validators, sequencers, and PoP miners. Sequencers, once the decentralized sequencing system is activated, stake their economic interest in the Hemi network to propose and confirm blocks, earning rewards for honest participation and being slashed if they misbehave. Sequencers must align with protocol rules, providing strong censorship resistance. Because the chain state is periodically anchored in Bitcoin, any attempt to subvert the network and perform a long reorg would be countered by the difficulty of altering Bitcoin's chain—censorship and fraudulent reorganizations are economically self-defeating.

Additionally, Hemi includes additional anti-censorship systems through transaction offloading that leverage Bitcoin and Ethereum's native censorship resistance.

PoP miners, who embed Hemi's state commitments into Bitcoin, earn rewards proportional to their prompt and accurate publications. With multiple PoP miners vying to produce truthful proofs, there is no single point of failure or easy avenue for collusion. Trust is replaced by cryptographic proofs and economic incentives, making honest behavior consistently the most profitable and secure route. As a permissionless protocol, if the current PoP miners active on the network fail to publish specific Hemi chain data to Bitcoin, they create a profit opportunity for other users to participate and perform the required publications.

Many projects claim decentralization, but Hemi operationalizes it. By efficiently leveraging the security provided by Bitcoin's immense network of miners, Ethereum's varied validator sets, and a dynamic group of PoP miners, Hemi provides robust protection from any attacker to censor transactions or reorganize the chain's history without incurring astronomical costs.

Incentives and Ecosystem Integration

While architectural innovation is critical, it must be paired with a healthy ecosystem and strong economic incentives to attract builders, users, and long-term stakeholders. Hemi's approach to ecosystem growth involves technical accessibility and a structured incentive model that evolves as the network matures. Hemi's incentive model is organized into Seasons, each reflecting a phase in the network's maturity and targeting distinct growth objectives:

- **Season 1 (Testnet):**
  The first phase focuses on establishing a foundation of users and protocols. Early participants earn points for on-chain test activities, community engagement, and developer advocacy. The emphasis is on learning, experimentation, and seeding initial liquidity. Builders benefit from a testnet points program, grants, and ecosystem support, refining their dApps in a safe, incentivized environment.
- **Season 2 (Mainnet Launch):**
  Following the Mainnet launch, incentives pivot to economically impactful actions. Rewards focus on boosting TVL, transaction volume, and liquidity for lending protocols and DEXes. Developer bounties, hackathons, and grants encourage builders to produce high-value tooling and educational materials leveraging Hemi's dual-chain asset ecosystem and Bitcoin awareness. Early Season 1 participants leverage their prior contributions for greater rewards, while targeted investments and partnerships shape the network's immediate growth trajectory.
- **Seasons 3-N (Governance Transition):**
  As the network matures, Hemi transitions toward more decentralized decision-making. Liquidity mining incentives encourage deep liquidity pools, while retroactive funding rewards developers who have consistently delivered value over time. Governance-based incentives shift power and resource allocation into the hands of the community, creating a sustainable ecosystem driven by user priorities and long-term commitments rather than top-down directives.

Grant Programs and Strategic Projects

Hemi supports a variety of developer initiatives through grants and strategic investments. Early on, broad calls for proposals invite innovation from all corners, fostering experimentation in areas like non-custodial BTC DEXs and lending protocols, auditable AI marketplaces, Ordinal/BRC-20/Rune exchanges, and protocols that generate yield for ETH and BTC assets. Over time, grant programs become more focused, channeling resources into specific, high-impact projects aligned with Hemi's evolving roadmap. This strategic alignment ensures that incentives and capital deployment remain coherent with the network's broader vision of secure, trust-minimized cross-chain operations.

Hemi's Position in the Competitive Landscape

Since 2018, Bitcoin's Lightning Network has successfully facilitated fast and inexpensive transactions for a small subset of users but has failed to garner mass adoption or create popular, easy-to-use, yield-generating solutions for BTC. This limitation is largely due to Bitcoin's lack of support for general-purpose smart contracts, with no foreseeable upgrades to enable such functionality. In response, many BTC holders have opted to bridge their assets to blockchains like Ethereum (and others), which offer Turing-complete environments. Wrapped BTC (e.g., WBTC, cbBTC, tBTC, and more) has become a dominant force in Ethereum's DeFi ecosystem, accounting for over $13 billion in value and comprising ~65% of all BTC in wrapped formats. This trend underscores a growing demand for ways to make BTC more productive.

To effectively compete with Wrapped Bitcoin (WBTC) in decentralized finance (DeFi), Bitcoin L2 lending protocols must enhance BTC utilization by offering secure and capital-efficient custodianship systems, higher yields, adequate stablecoin liquidity, and reliable/stable infrastructure for borrowing. Notably, about 70% of WBTC in DeFi is allocated to lending platforms, insinuating that these BTC holders primarily engage with lending services.

Source: Keyrock

Bitcoin L2 solutions are emerging to recapture this user base by providing native BTC yield opportunities. Since 2021, Bitcoin L2 projects have grown from just a handful to 80+, driven by the appeal of enabling BTC use within DeFi without leaving its ecosystem and becoming exposed to centralized custodianship risks. By reducing bridging friction and enhancing security, Bitcoin L2s address key pain points of existing solutions. These projects leverage Bitcoin's unmatched security, liquidity, and brand with diverse approaches like the payment-focused Lightning protocol, flexible sidechains such as RSK and Stacks, and various bridging methods. However, many face trade-offs in trust, complexity, or programmability. A standout advantage of Bitcoin L2 DeFi is that BTC functions as both the native gas asset and the core of

development, aligning with the historical trend of native assets being most effective on their origin networks.

Hemi takes a different path. Treating Bitcoin and Ethereum as components of one supernetwork achieves direct Bitcoin state integration, true cross-chain synergy, and a unique superfinality model that elevates the security baseline. While other Bitcoin L2s struggle to provide strong finality or remain limited to niche use cases, Hemi offers a general-purpose platform that natively incorporates Bitcoin's ledger into an EVM-compatible environment. Developers gain access to Ethereum's rich DeFi ecosystem and tooling alongside Bitcoin's immense security, all within a consistent and incentive-rich framework.

One of Hemi's most direct competitors is BOB. BOB, or "Build on Bitcoin," is an EVM-compatible Layer 2 (L2) solution designed to function as a co-processor for Bitcoin. Developed by the Interlay ecosystem, which originates from Polkadot and Cosmos, BOB aims to bridge the gap between Bitcoin and Ethereum while leveraging Bitcoin's robust Layer 1 (L1) capabilities for settlement, custody, and storage.

Key features of BOB include plans to inherit Bitcoin security with a variant of merged-mining, which initially adopts an Ethereum-based optimistic rollup model and leverages Ethereum-ecosystem Bitcoin-backed tokens but plans to transition to a trust-minimized BitVM2-based system for native Bitcoin settlement. Support for the Bitcoin Stack ensures compatibility with existing Bitcoin technologies like Ordinals, Lightning, and Nostr, alongside tools such as a Bitcoin smart contract SDK based on a Bitcoin header relay system, Rust zkVM, and a trustless Ethereum bridge for secure transfer of Ethereum-based assets. Its EVM compatibility allows integration with Ethereum's tooling and infrastructure, while its ETH Rollup Support enables Bitcoin-based applications to access Ethereum's DeFi liquidity and efficient on/off-ramps, enhancing utility for web3 power users.

As the industry demands scalable, trust-minimized solutions that can host complex financial operations and next-generation dApps, Hemi stands out as a pioneer. Rather than extending Bitcoin with a few conveniences, it refashions the concept of an L2 entirely, delivering a supernetwork where Bitcoin and Ethereum seamlessly reinforce one another, setting the stage for large-scale adoption and institutional confidence.

Conclusion

The Hemi Layer-2 Supernetwork represents a paradigm shift in blockchain interoperability and Bitcoin scalability. By seamlessly integrating Bitcoin's industry-leading security and Ethereum's programmability into a unified supernetwork, Hemi unifies the long-standing divide between these two foundational blockchains. Its innovative approach, anchored by the Hemi Virtual Machine (hVM), encapsulation, and Proof-of-Proof (PoP) consensus, set a new standard for cross-chain programmability, security, and developer usability. Additionally, the design choice to embed a full Bitcoin node within an Ethereum-compatible environment eliminates the need for insecure crypto bridges and external verifiers, enabling developers to build sophisticated decentralized applications (dApps) and native Bitcoin interoperability infrastructure that was previously unattainable.

As the demand for scalable, secure, and composable blockchain solutions grows, Hemi's superfinality model and its ecosystem-wide incentive structure position it as a leader in the evolving Bitcoin Layer 2 landscape. Unlike other L2 solutions that often compromise on trust or functionality, Hemi redefines the possibilities of decentralized finance (DeFi), non-custodial asset management, and programmable interoperability. By treating Bitcoin and Ethereum as complementary components of a single system, Hemi resolves existing limitations and lays the groundwork for the next generation of multi-chain innovation, fostering institutional confidence and mainstream adoption.