DLResearch x hemi

Hemi: A Modular L2 Connecting the Bitcoin and Ethereum Ecosystems

www.dlnews.com/**research**

TABLE OF CONTENTS

Introduction

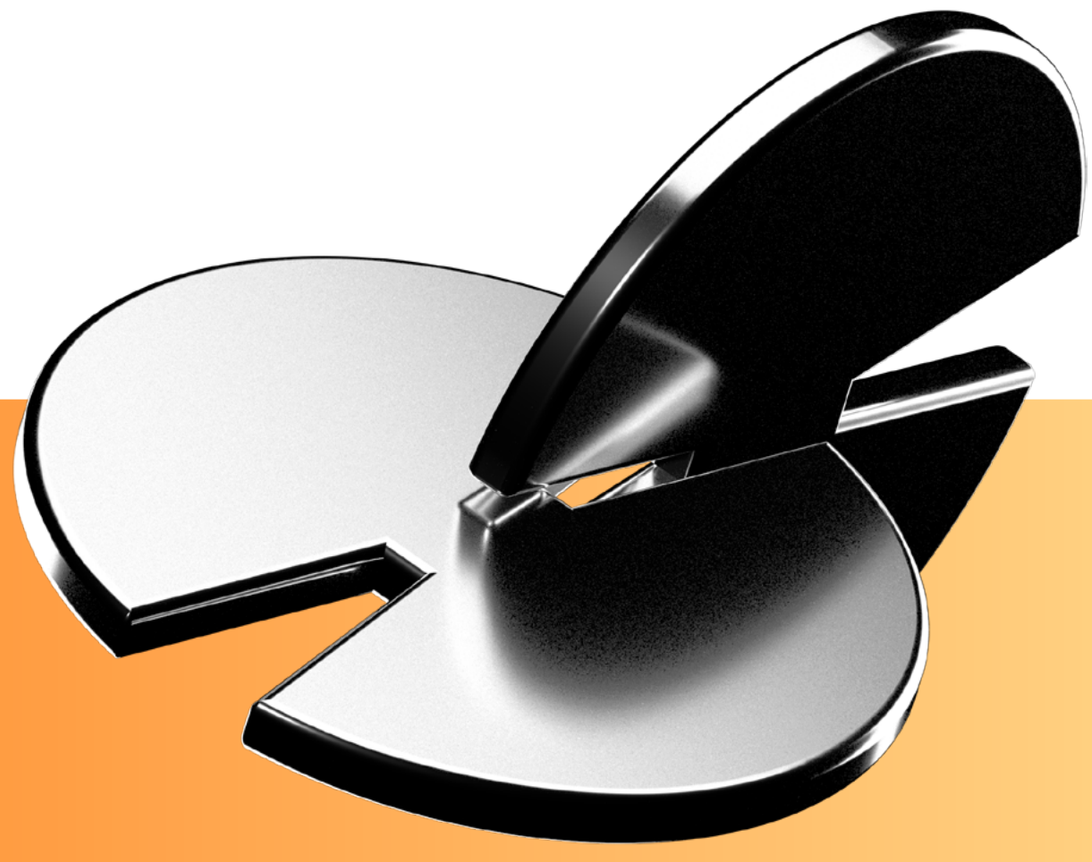
So far, interoperability between Bitcoin and Ethereum has been limited, preventing the seamless integration of Bitcoin's security and liquidity with Ethereum's flexibility and diverse ecosystem of protocols and assets. The Hemi Network addresses this gap by connecting the two ecosystems, enabling the development of cross-chain applications that approach Bitcoin and Ethereum as components of a single supernetwork. By merging Bitcoin's security with Ethereum's programmability, Hemi opens the door to a new era of decentralised applications (dApps) that operate across both chains without the need for intermediaries or centralised exchanges.

Currently, Hemi has announced a $15 million seed round led by Binance Labs, Breyer Capital, and Big Brain Holdings. Interest in the project has been high – since the launch of incentivised testnet in July, over 200,000 Proof-of-Proof ("PoP") miners testing Hemi's unique Bitcoin security inheritance mechanism have sent over 95 million PoP transactions on Bitcoin's testnet3 network. Additionally, community testing of Hemi's cross-chain asset transfer system ("Tunnels") at peak accounted for 88% of all traffic on Ethereum's Sepolia testnet and caused the base gas rate to spike above 10,000 Gwei - a value never before seen on the network.

The Team

Seasoned experts in blockchain development are spearheading the Hemi Network. Jeff Garzik, the CEO and Principal Engineer at Hemi, is a co-founder and CEO of Bloq with a rich history in Bitcoin development. As an early Bitcoin core developer, he worked alongside Satoshi Nakamoto in the early days of Bitcoin. His tenure at Red Hat involved significant contributions to the Linux kernel (work that underpins every Android device and Linux-based data centre today). Jeff's deep involvement in open-source software development uniquely positions him to lead Hemi's technical vision.

Max Sanchez, Hemi's Lead Architect, brings extensive experience in blockchain protocol design. Before joining Hemi, he co-invented the Proof-of-Proof (PoP) protocol for decentralised and permissionless Bitcoin security inheritance. A blockchain enthusiast since 2011, Max has been instrumental in launching innovative technologies like the first testnet utilising post-quantum cryptography. He has also contributed to the identification and disclosure of consensus vulnerabilities in multiple blockchain projects.



Key Features

Hemi is a modular multi-network L2 blockchain focused on securely connecting Bitcoin and Ethereum in a scalable manner. A key feature of Hemi is its robust interoperability layer, enabling seamless asset transfers and data sharing between Bitcoin and Ethereum. This feature creates an EVM-compatible environment for decentralised applications (dApps) that operate across both chains.

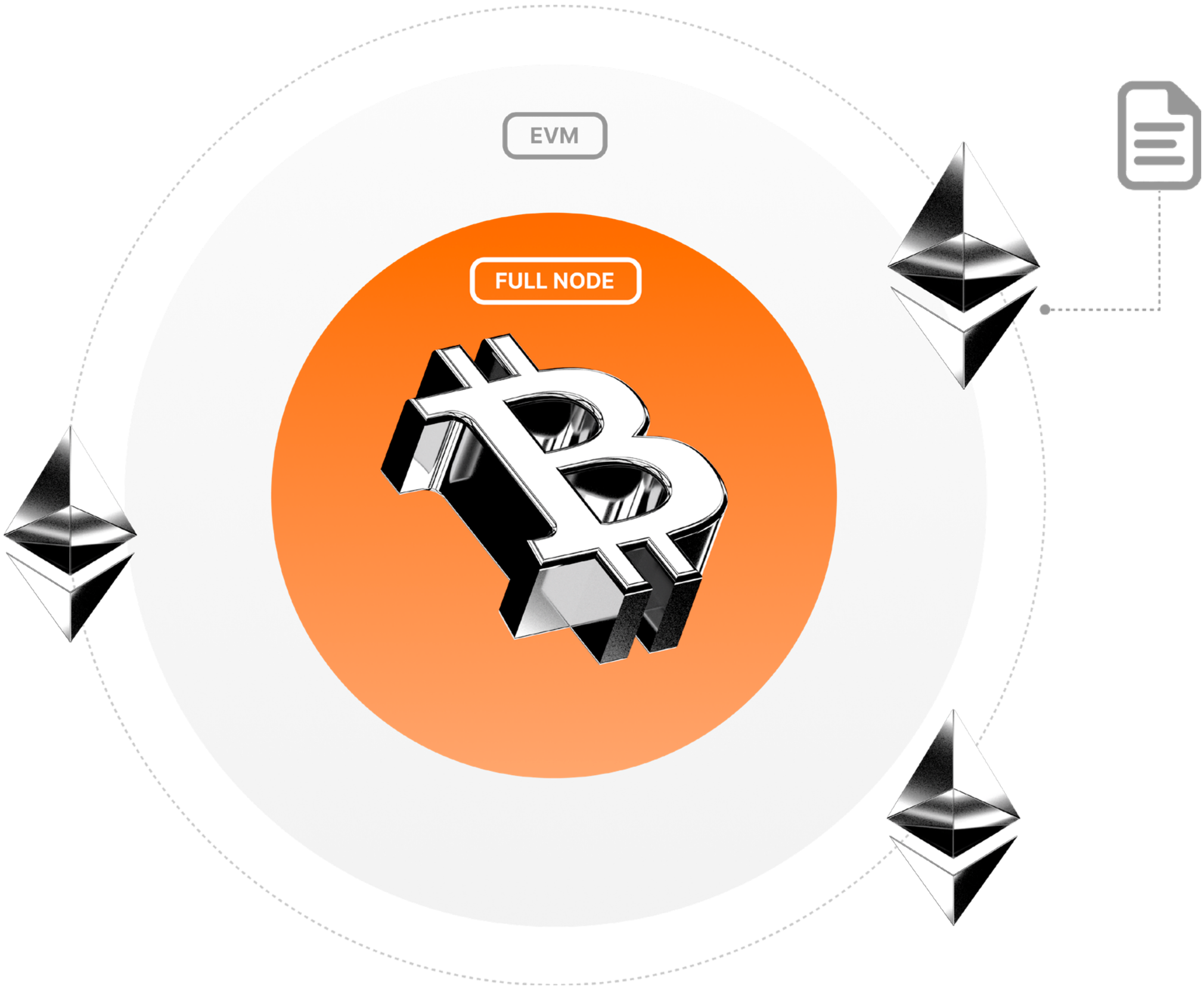
The Hemi Virtual Machine (hVM) introduces a novel way to build Bitcoin-aware smart contracts by embedding a full Bitcoin node inside the EVM. The flexibility provides applications with a complete view of Bitcoin's state without relying on third-party relayers or centralised oracles.

Hemi inherits Bitcoin's Proof-of-Work security in a fully decentralised and permissionless manner. The novel Proof-of-Proof protocol protects cross-chain transactions from reorg attacks and leverages both Bitcoin and Ethereum to protect users from censorship.

Finally, the network's architecture is built to extend access to Bitcoin and Ethereum assets, EVM-level Bitcoin awareness, Bitcoin security inheritance, and multi-network censorship protection to an ecosystem of interoperable L3 networks with the flexibility for developers to optimise for different use-cases like AI, gaming, and DeFi.

hVM

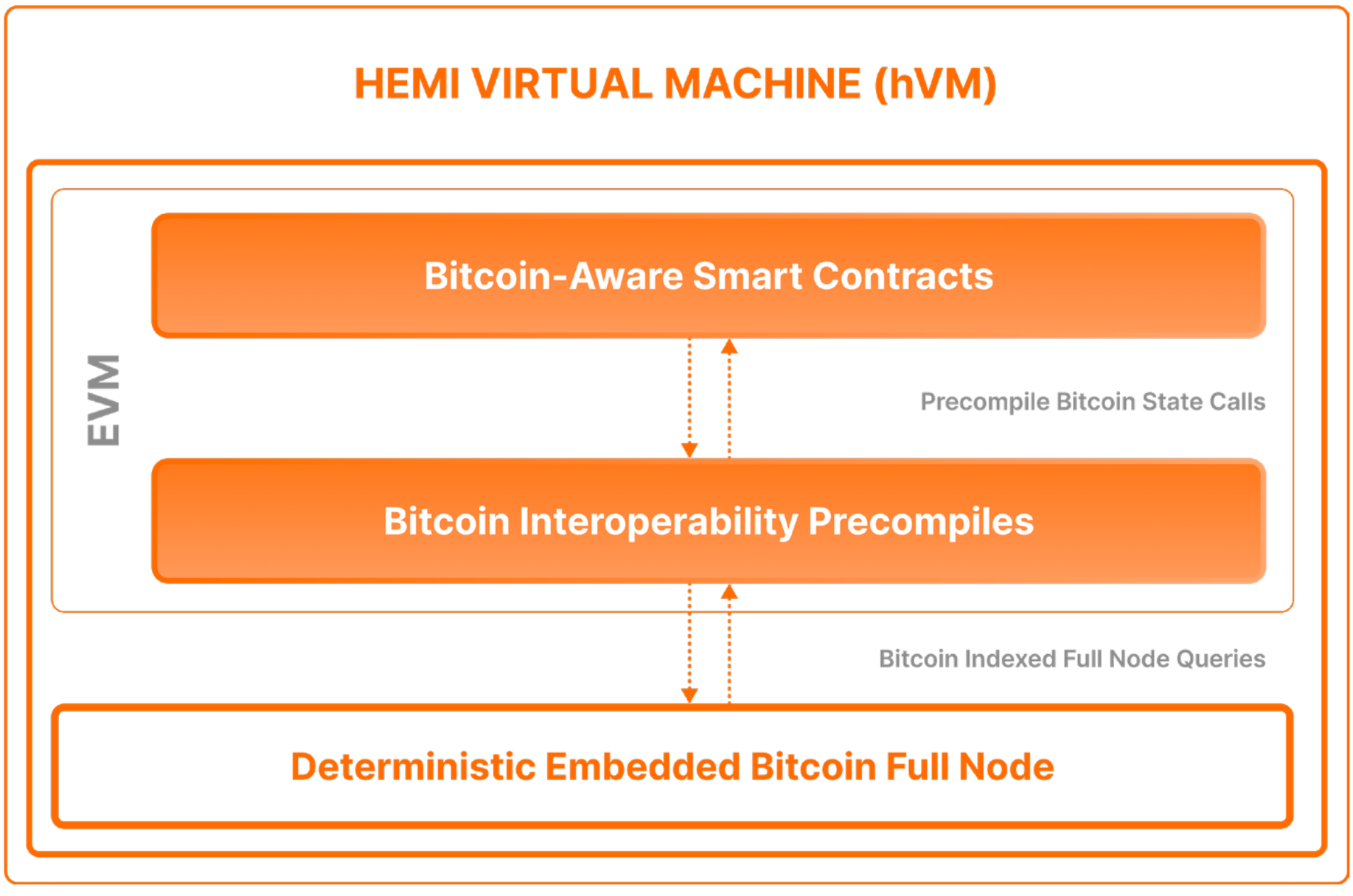
The hVM (Hemi Virtual Machine) enables Bitcoin interoperability and programmability by integrating a full Bitcoin node within a fully backwards-compatible Ethereum Virtual Machine (EVM) environment. This integration provides Ethereum-style smart contracts with direct access to Bitcoin's complete state, including states like the UTXO table, which previous Bitcoin interoperability technologies could not securely provide due to some limitations of Bitcoin's architecture.



Core Components of the hVM

The hVM consists of three major components – an EVM execution environment, a Bitcoin full node implementation designed to be driven deterministically as part of an L2's state transition function, and a set of precompile contract endpoints that facilitate communication between smart contracts executing inside the EVM and the Bitcoin full node.

GRAPH 1 **HEMI VIRTUAL MACHINE (hVM)**



The execution environment used for the hVM is a standard EVM which maintains full backwards compatibility with the Ethereum network, meaning any smart contract that runs on Ethereum can be deployed on Hemi without modification.

The Bitcoin node used for the hVM is a custom-built full node implementation that connects to the Bitcoin P2P network to synchronise Bitcoin blockchain data, but only indexes the chain to a tip specified by the Hemi protocol to ensure deterministic views of Bitcoin state from within the hVM. To drive this indexing, the Hemi protocol maintains its own lightweight consensus view of Bitcoin (using a dual-chain L2 block derivation process). This deterministic driving of the Bitcoin full node ensures that the Bitcoin state data available to smart contracts is universally consistent across all Hemi nodes when processing a particular Hemi block.

The hVM's precompile contracts connect the EVM execution environment with the Bitcoin node. Endpoints accessible from within the EVM perform queries on the Bitcoin node and return the results to the smart contract inside the EVM.

A fully indexed Bitcoin node within the EVM enables seamless smart contract interactions with the Bitcoin blockchain. By exposing comprehensive Bitcoin data — such as the UTXO set — directly into the EVM, the hVM provides smart contracts with a trustless and deterministic view of Bitcoin's state. This eliminates the need for external oracles or third-party relayers, enhancing security and decentralisation while enabling cross-chain functionality directly through Ethereum smart contracts.

In other words, Hemi allows smart contracts to access Bitcoin's state in much the same way they access the state of other contracts within the same EVM. For example, in Ethereum, a contract can interact with Uniswap to retrieve the current price of an asset without relying on external data sources; all necessary information is inherently available within the EVM.

This seamless access is possible because the EVM ensures the correctness of the data by default. Similarly, Hemi enables contracts to directly query Bitcoin's state — including specific transaction details — without the need for oracles or relayers. While the analogy isn't exact (since Hemi provides more extensive access to Bitcoin data than the EVM typically offers for its own chain) it illustrates how Hemi enhances cross-chain capabilities by making Bitcoin's state readily accessible within smart contracts.

Smart Contract Bitcoin Event Subscriptions

A slated feature of the hVM will further expand functionality by enabling real-time subscriptions to Bitcoin events. With the hVM event subscriptions, developers can program smart contracts to automatically execute specific actions based on Bitcoin events such as transaction confirmations, the mining of new blocks, or the spending of a particular transaction output. Event subscriptions also allow developers to build applications that respond dynamically to Bitcoin activity. This architecture supports highly customisable logic, enabling conditional workflows that don't require onchain initiation from an Externally Owned Account (EOA) on Hemi.

For example, escrowed funds in a non-custodial DEX could be released when a particular Bitcoin address receives the expected quantity of Bitcoin to complete a trade, or an operator could be deactivated from the active operator pool of a Bitcoin restaking protocol if they publish a transaction on Bitcoin that initiates a claim procedure to withdraw staked BTC collateral.

Enabling Cross-Chain Workflows

In addition to Bitcoin awareness, the hVM maintains awareness of Ethereum by processing Ethereum transactions that perform cross-network calls to Hemi during the L2 block derivation process. The hVM can also initiate outgoing calls to contracts on Ethereum.

As a result, smart contracts on Hemi can perform complex multi-chain workflows. For example, a smart contract could observe the confirmation of a specific transaction on Bitcoin and send a cross-chain call to a contract running on Ethereum. Or a smart contract on Ethereum could send a cross-chain message to trigger a smart contract on Hemi to perform a particular action based on Bitcoin state.

When designing cross-chain applications, the state challenge time for settlement of Hemi-to Ethereum cross-chain calls, along with the hVM's natural delay in processing Bitcoin blocks must be considered. However, Hemi's ability to observe and interact with both chains provides a powerful foundation for decentralised applications that demand secure and flexible cross-chain workflows.

Metaprotocol Support (Ordinals, BRC-20s, Runes, etc.)

As early as 2012, various developers have launched metaprotocols that live on top of the Bitcoin blockchain. These metaprotocols are unknown to the Bitcoin protocol itself, making them experimental for the protocol, but users can run additional metaprotocol-specific indexers that extract and process relevant information from Bitcoin transactions to track the metaprotocol's state machine.

The architecture of the hVM makes it possible to introduce future protocol upgrades that add additional indexers (along with their own precompile endpoints) to the embedded Bitcoin full node. These upgrades provide smart contracts with additional information about protocols running on top of Bitcoin. By adding metaprotocol-specific indexers to the hVM, the Hemi network can provide smart contracts with a complete Bitcoin metaprotocol state as well. Support for Ordinals, BRC-20s, and Runes are also possible additions to Hemi's roadmap for hVM functionality. When support for a specific metaprotocol is added to the hVM, a number of additional precompiles can be added that allow smart contracts to query the metaprotocol's state.

Metaprotocol support will make it possible to develop smart contracts that interact with Bitcoin metaprotocols, including expanding the Hemi Bitcoin Tunnel system to support the tunnelling of metaprotocol assets.

Advantages of hVM for Bitcoin Interoperability and Programmability

Over the past decade, developers have introduced a variety of different mechanisms to introspect Bitcoin in a smart contract environment. The architecture of Bitcoin makes this particularly complex because Bitcoin maintains (the UTXO table) an actual state machine that isn't cryptographically committed to in the Bitcoin blockchain. Therefore, proving/validating statements like "X output has not been spent" or "the balance of X address is Y" is impossible or extremely impractical with traditional approaches.

These approaches fall into three broad categories:

Bitcoin Header Relay: A smart contract tracks lightweight Bitcoin consensus using Bitcoin headers, which relayers communicate to the consensus-tracking smart contract. Other smart contracts that want to introspect Bitcoin have their users submit relevant Bitcoin transactions with Merkle proofs. These prove transactions are contained within a particular Bitcoin block by authenticating them, which is validated against the Merkle root contained in a Bitcoin block.

Bitcoin State Oracles: A trusted oracle system is used which tracks Bitcoin state and responds to queries by signing or otherwise endorsing the response as valid.

Succinct Arguments of Knowledge (SNARG): Users or specialised parties with access to extensive computing power construct SNARG (in practice, generally zk-SNARK) proofs of processing large amounts of data from Bitcoin to validate onchain a certain statement about Bitcoin is correct.

Each approach has significant limitations.

The header relay model can only prove that a particular transaction exists on Bitcoin, but cannot prove anything about the UTXO table. It also requires validating Merkle proofs onchain and doesn't allow the smart contract to dynamically request additional Bitcoin data.

The Oracle model introduces a significant trust assumption. Depending on the implementation, it generally does not allow the smart contract to dynamically request data unless the oracle is built into the virtual machine protocol itself.

The SNARG approach can prove anything about Bitcoin's state. However, it is extremely computationally expensive for end users to compute the original proofs and for a smart contract to validate the proof onchain. Additionally, since the SNARG must be computed for each specific statement about Bitcoin state, the contract cannot dynamically request additional Bitcoin data.

By making a fully indexed Bitcoin node available within the EVM, the hVM:

- Does not rely on any relayers to keep Bitcoin's state up-to-date
- Does not rely on oracles to report information about Bitcoin that must be trusted
- Always provides correct and complete Bitcoin information, in the same way data in the EVM itself is available to smart contracts
- Can answer queries about Bitcoin state that isn't cryptographically authenticated to Bitcoin block headers
- Allows a smart contract to dynamically query for any Bitcoin data needed
- Does not require any expensive proof computation/verification to demonstrate the authenticity of claims about Bitcoin's state

hBK

The Hemi Bitcoin Kit (hBK) is a developer-friendly toolkit designed to abstract the complexities of interacting with the hVM precompiles. With the hBK, developers can call simple high-level Solidity functions and receive back Bitcoin data in the form of convenient structures rather than needing to implement custom serialisation and deserialisation logic. The hBK also includes integrations with libraries like Viem to make the development of off-chain portions of Bitcoin-aware decentralised applications (like UIs) easier.

By making the hVM's Bitcoin state awareness accessible through familiar smart contract calls, the hBK enables developers to create Bitcoin-aware decentralised applications without requiring deep expertise in the specifics of the hVM's implementation.

GRAPH 2 **HEMI BITCOIN KIT (HBK):** MAKING THE hVM's ADVANCED BITCOIN INTROSPECTION ACCESSIBLE

BALANCE

UTXOs

TX INPUT

TX OUTPUT

TX EXISTS

HEADER

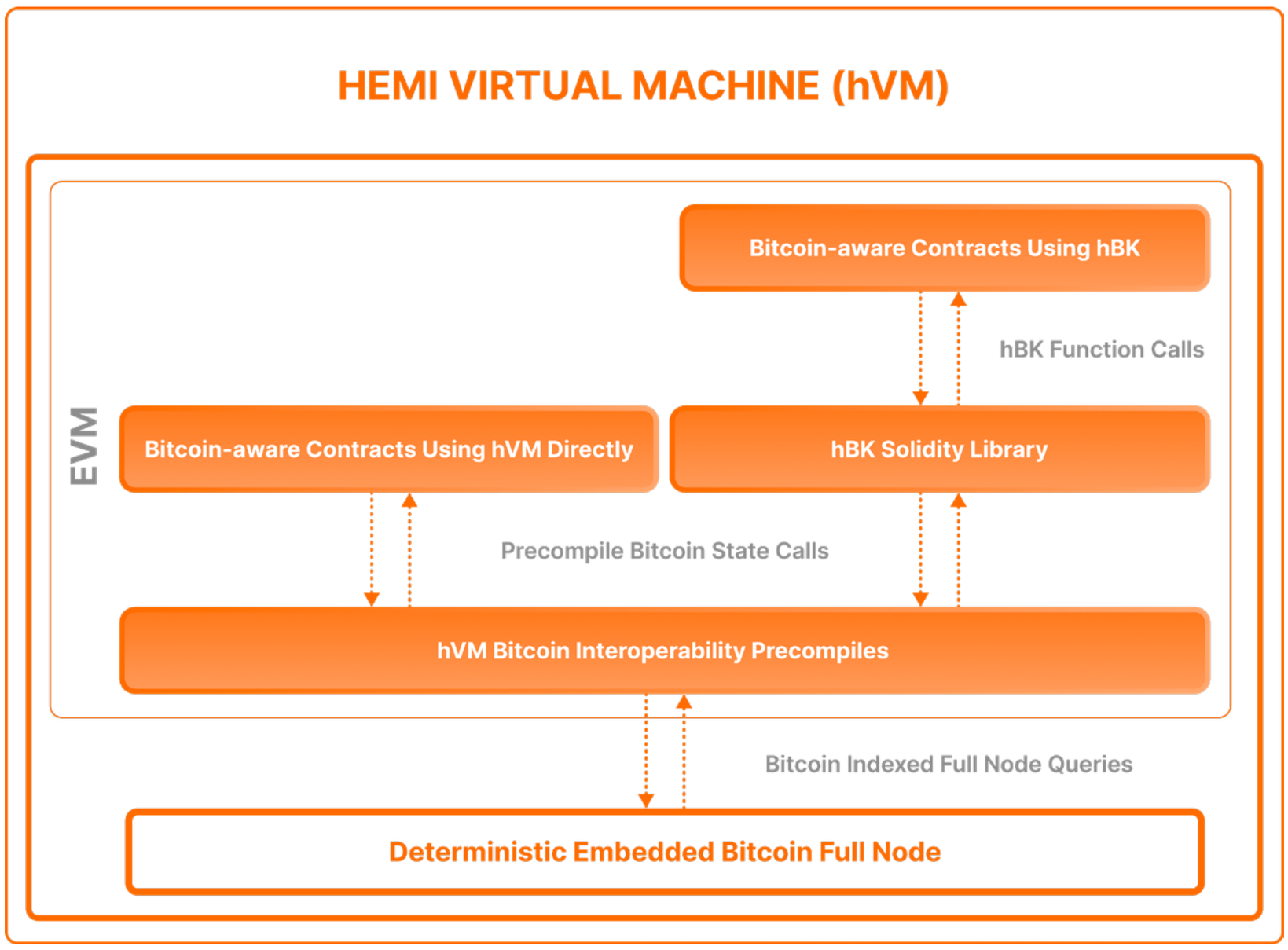
OUTPUT SPENT

```
function checkLatestUtxo(string address) public returns (bool) {
        UTXO[] memory utxos = hBK.getUTXOsForBTCAddr(btcAddress, 0, 1);
        if   (utxos.lenght >= 1) {
              UTXO utxo = utxos[0]
               /**
                * UTXO contains:
                *    bytes32 txId
                *    uint256 index
                *    uint256 value
                *    bytes scriptPubKey
                */
               // Your code here
        }
}
```

Core Components of hBK

A primary component of the hBK is its Solidity library. This collection of smart contracts manages data serialisation/deserialisation and the calls to the underlying hVM precompiles. The latest version of the hBK's Solidity contracts will always be deployed and usable on the network. Further, developers can also expand the hBK's features and deploy custom versions for themselves or others to use.

GRAPH 3 **HEMI VIRTUAL MACHINE (hVM)**



The initial version of the hBK's Solidity library enables smart contracts to:

- Know the balance (in satoshis) of a Bitcoin address
- Obtain the UTXOs of a Bitcoin address, with control over pagination
- Determine whether a specific output of a transaction has been spent
- Obtain the full data (or specific pieces of data, like a single input or output) of a Bitcoin transaction by TxID
- Determine whether a specific transaction exists in the canonical Bitcoin chain, and if so the number of confirmations
- Convert a Bitcoin address to its corresponding spend script
- Get the latest Bitcoin header, or the header at a specific height on the canonical chain

Future versions of the hBK Solidity library will add support for upcoming hVM features like Bitcoin event subscriptions and metaprotocol state awareness.

The hBK is also integrating with third-party libraries that interface with EVM chains and are used to build supporting software like dApp frontends. This major component includes an initial version of the hBK and a Viem extension, but future hBK versions will provide integrations with other libraries like Ethers.js.

Developer Tools and Integrations

The hBK Solidity library is compatible with popular Ethereum development tools like Truffle, Hardhat, and Remix. This compatibility allows developers to build Bitcoin-aware applications using familiar workflows and toolchains. This reduces the learning curve associated with adopting new technologies. Developers can utilise their existing Ethereum development environments while leveraging the hBK Solidity library to write cross-chain smart contracts able to view and react to events on Bitcoin.

Beyond just developing Bitcoin-aware smart contracts themselves, developers often need to build frontends and other off-chain software that interact with the smart contracts they develop. To facilitate this, the hBK Viem extension makes it easy to call the hBK Solidity library endpoints from Javascript applications. The extension can also retrieve Bitcoin finality statistics for blocks on the Hemi network.

Advantages of the hVM/hBK

By using the hVM/hBK, developers can build sophisticated Bitcoin-aware dApps in a secure, gas-efficient, and straight-forward way. Further, Hemi's connectivity to Ethereum enables these Bitcoin-aware dApps to also securely leverage Ethereum-based assets and send/receive cross-chain contract calls to the Ethereum network. Together, these features unlock new applications that were impossible or impractical with other interoperability solutions.

Use Cases Enabled by the hVM/hBK

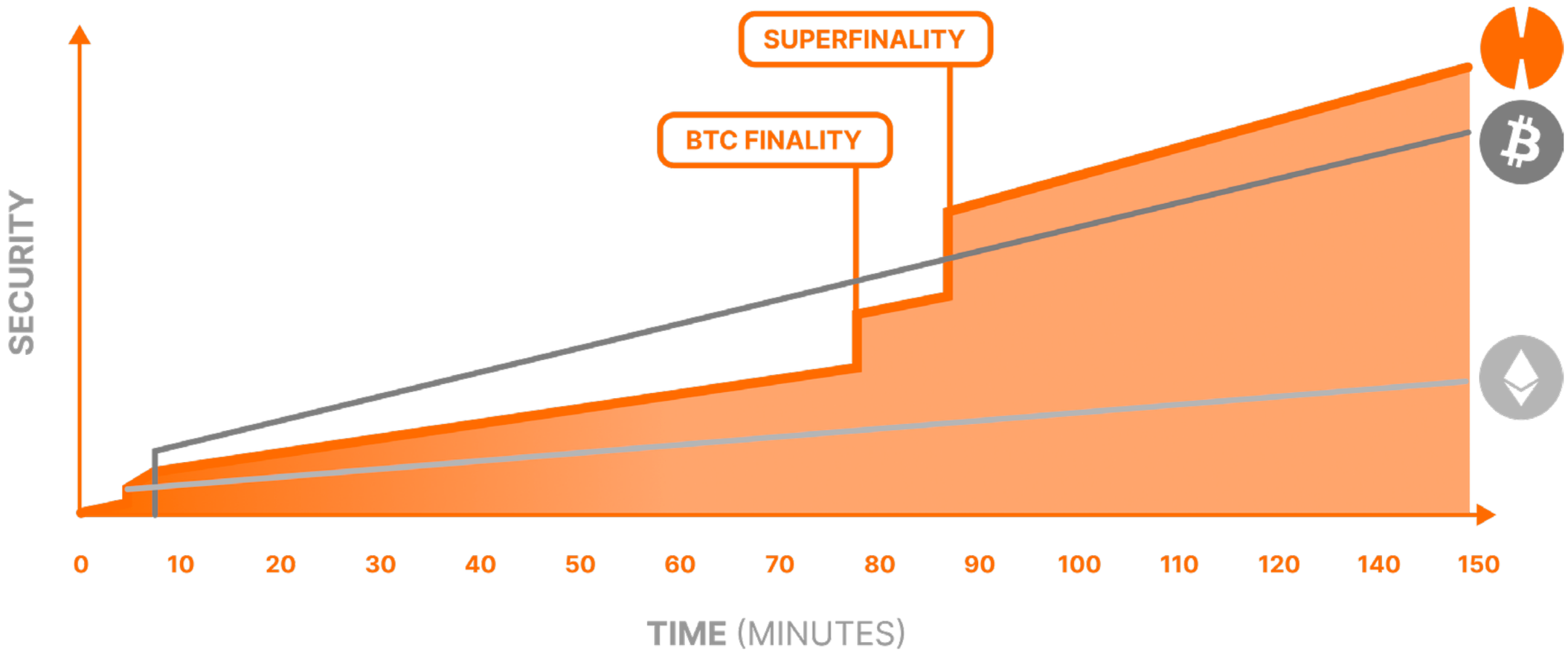
Using the hVM/hBK, developers can build sophisticated Bitcoin interoperability infrastructure and applications that leverage assets from or interact directly with the Ethereum ecosystem. Some of these use cases include:

- **Non-Custodial Bitcoin and Ethereum DEXes**
- **Non-Custodial Bitcoin Lending Markets**
- **Programmable Bitcoin Smart Wallets**
- **Dynamic Bitcoin Fee Marketplaces**
- **Custom Bitcoin Asset Tunnelling Protocols**
- **Non-Custodial Bitcoin Staking**

Bitcoin Security Inheritance and Superfinality

Unlike standard block confirmations — vulnerable to forks or miner attacks — Superfinality in the Hemi Network offers an extra layer of security. Once a block (and the transactions it contains) achieves Superfinality, it becomes fully irreversible and protected against any form of reorganisation or alteration with the combined force of Bitcoin's PoW and Hemi's native block production consensus. This is especially important for cross-chain transactions, where guaranteed immutability is essential for maintaining trust and reliability.

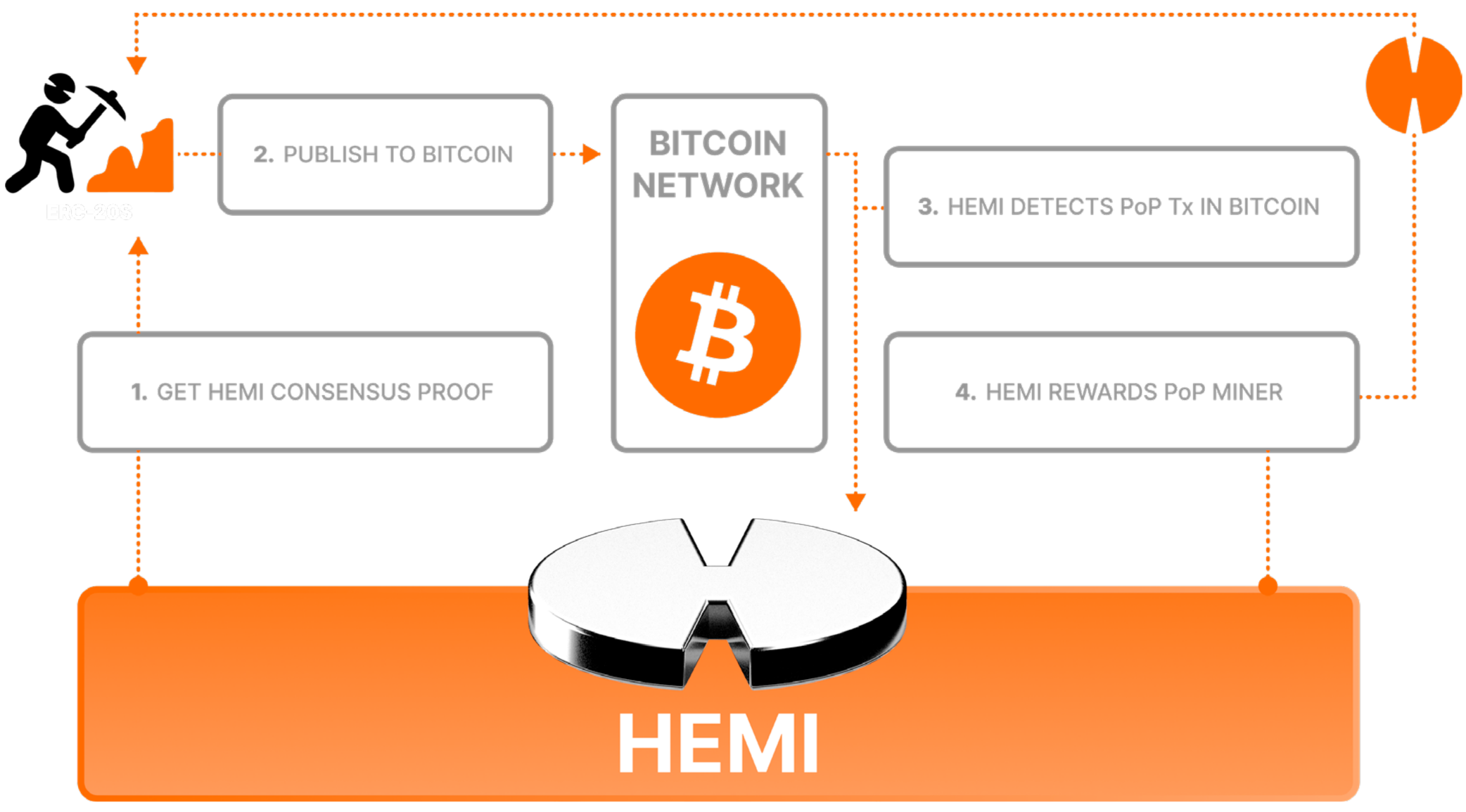
GRAPH 4 **SUPERFINALITY**



How Superfinality Works

The Hemi Network's concept of **Superfinality** relies on Bitcoin's Proof-of-Work (PoW) security. Using its Proof-of-Proof (PoP) consensus, Hemi inherits Bitcoin's security in a fully permissionless and decentralised manner. During normal operation, Hemi blocks achieve Bitcoin Finality after nine Bitcoin block confirmations and Superfinality after ten confirmations. This process provides high security assurance, making Hemi highly resistant to chain reorganisations. Once Hemi blocks achieve Superfinality, reversing them would require a concurrent 51% attacking Bitcoin and Hemi's native block-producing consensus.

GRAPH 5 **PROOF-OF-PROOF (PoP)** PERMISSIONLESS BITCOIN SECURITY INHERITANCE



The PoP mechanism introduces a new class of lightweight miners who periodically record Hemi consensus data on the Bitcoin blockchain in exchange for a protocol-provided reward.

If a reorganisation of Hemi is proposed, the protocol uses this consensus information embedded in Bitcoin to perform fork resolution and determine the canonical chain based on the relative publication state of both chains to Bitcoin. Once a consensus proof of a Hemi chain segment has been published on Bitcoin without the publication of a competing chain segment for nine blocks, the fork resolution algorithm will never accept an alternative chain segment as canonical. As a result, the only way for an attacker to cause a competing Hemi chain to become canonical is to rewrite Bitcoin's chain to retroactively insert proofs, which requires 51% attacking Bitcoin's own PoW.

If an attacker does publish a consensus proof of a valid Hemi chain segment within the nine Bitcoin block period, this publication is visible to all external observers. Bitcoin Finality statistics will not consider this segment of Hemi's chain to have Bitcoin Finality until the potential fork is resolved. Only a subsequent, uncontested Hemi chain segment (consisting of nine Bitcoin blocks) can resolve the fork.

After a Hemi chain segment reaches ten Bitcoin confirmations, it achieves Superfinality. At this point, once again, multiple Bitcoin blocks would have to be 51% attacked for an attacker to produce a valid reorganisation.

Implications for Developers

Superfinality is particularly significant for cross-chain applications dealing with high-value transfers and real-world service providers like exchanges and payment processors. Once a transaction on Hemi achieves Superfinality, protocols and service providers can accept the transaction with the same security assurances as transactions on Bitcoin itself. This provides the reliability necessary for large-scale financial operations.

For example, a non-custodial Bitcoin lending protocol could wait until the transaction depositing collateral assets on Hemi has achieved Superfinality before sending Bitcoin to the borrower. This would ensure that a Hemi reorganisation that removes the loan's collateral could not be performed. Superfinality is also used for settlement to Ethereum. In addition to the normal fault dispute process for challenging invalid L2 state, cross-chain transactions from Hemi to Ethereum must achieve Superfinality before being processed.

Outside of cross-chain applications, Superfinality also protects users and third-party services that accept transactions on Hemi. For example, an exchange or payment processor could wait for a deposit or payment to achieve Superfinality. Then, it could allow the user to trade and withdraw funds or complete a purchase to ensure the transaction cannot be clawed back by a network reorganisation.

Additionally, Superfinality also provides value to non-financial applications. Multi-chain decentralised autonomous organisations (DAOs) can use Superfinality to ensure that votes, transactions, and decisions are final and can be used on other chains without the risk of being modified. This adds a critical layer of trust and security to cross-chain governance mechanisms.

Superfinality provides the ultimate guarantee of security and immutability. Developers can confidently build applications that require strong security assurances. This paves the way for more complex and high-stakes applications to run on the Hemi Network.

Superfinality's Role in Sequencer Decentralisation

One of the primary limitations of L2 networks across the Bitcoin and Ethereum ecosystems is using a centralised sequencer. These are responsible for ordering and confirming transactions to create L2 blocks.

When decentralising the sequencer, networks must weigh the tradeoffs between different consensus protocols. Today, most projects opt for Proof-of-Stake (PoS). Different flavours of PoS-style consensus mechanisms make different tradeoffs between liveness (the ability of the protocol to continue operating when a large quantity of consensus power is offline or misbehaving) and safety (the assurance that agreed-upon state updates will not be reverted).

Protocols like Ethereum-style PoS that optimise for liveness must allow for reorganisations to occur. These protocols are unable to provide finality whenever the protocol is progressing despite a large portion of the network's stake being offline or acting maliciously. Alternately, protocols like CometBFT that optimise for safety will never experience reorganisations but will permanently halt in the event of a consensus fault.

Additionally, today's liveness-preserving protocols are capable of handling orders of magnitude more validators compared to their safety-preserving counterparts. This scalability enables greater decentralisation and provides more users with the opportunity to directly participate in the block production process.

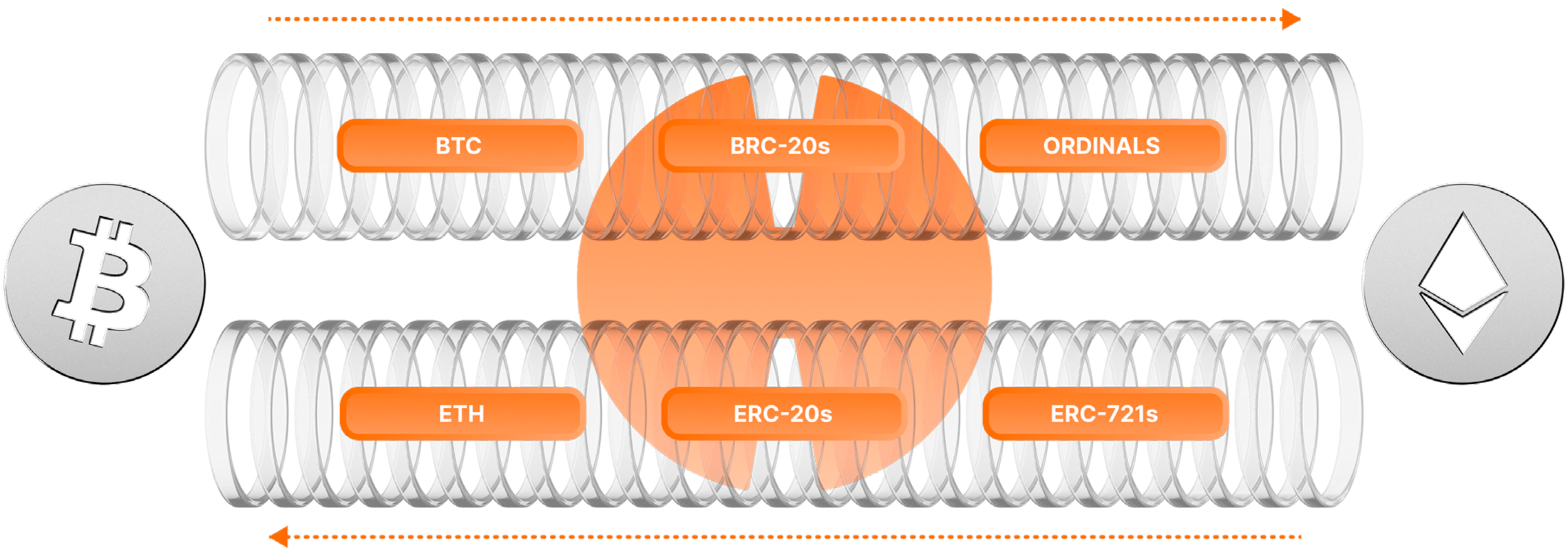
By reinforcing the network with Bitcoin's finality guarantees, Proof-of-Proof enables Hemi to securely implement a liveness-saving PoS consensus protocol and enjoy the associated robustness and improved decentralisation while still providing strong finality guarantees after a short period of time.

Tunnels

Architectural differences have historically hindered the integration of Bitcoin and Ethereum. The primary differences include distinct consensus mechanisms, limitations in Bitcoin's scripting language, and the absence of robust cross-chain awareness and communication.

Early solutions like token wrappers and centralised bridges facilitated asset movement between the two blockchains. However, these early solutions were often vulnerable to attacks and exploits. The hVM offers a superior solution by maintaining protocol-level awareness of both Bitcoin and Ethereum states, enabling secure and scalable cross-chain asset transfers through a feature known as Tunnels.

GRAPH 6 **TUNNELS:** A BETTER WAY TO GO CROSS-CHAIN



Tunnels in the Hemi Network facilitate secure asset transfers between Bitcoin, Ethereum, and Hemi without relying on centralised custodians. Architectural differences dictate that the Bitcoin and Ethereum components of Hemi's tunnel system operate differently.

Bitcoin Tunnels

Traditional methods of bringing Bitcoin onto EVM-compatible chains often rely on trusted centralised entities holding the actual BTC, backing synthetic assets, thus introducing custodial risks. While Bitcoin's architecture prevents the implementation of completely trustless settlement mechanisms available on Ethereum, Hemi's Bitcoin tunnels address these vulnerabilities through a trust-minimised and incentive-aligned dual-custodianship system:

Overcollateralised Low-Value Vaults are employed to secure small deposits of Bitcoin-based fungible assets and non-fungible tokens. The operators of these vaults post collateral in Hemi or Ethereum-based tokens. Operators then hold deposits smaller than the value of their collateral on behalf of the Hemi protocol. In the event of operator misbehaviour, the operator's collateral is slashed and used to make harmed users whole.

BitVM2-Based High-Value Vaults will be employed in the future to secure large deposits of BTC and other fungible Bitcoin-based assets in BitVM2-based vaults. A vault's security is contingent on two factors. Vaults will remain secure as long as one out of hundreds of operators is honest, and at least one rational actor is monitoring the vault custodianship system and challenging invalid withdrawal attempts on Bitcoin in exchange for a reward.

The Bitcoin tunnel system is implemented as smart contracts that run on Hemi and leverage the hVM/hBK for Bitcoin awareness. When Bitcoin-based assets are deposited in a vault, the tunnel protocol detects the deposit and mints corresponding representative tokens on Hemi. These behave identically to their Ethereum counterparts throughout the Hemi ecosystem. When users want to withdraw the underlying Bitcoin-based asset, they redeem their representative tokens with the tunnel protocol, which ensures operators fulfil the withdrawal request from one of the system's vaults.

The hVM enables the BitVM2 collateral system to utilise a modified version of the BitVM2-based BitVM Bridge protocol with various economic and security improvements made. Specifically, the hVM enables Hemi to act as a censorship-resistant external observer of the canonical Bitcoin consensus. This will be used to replace superblock-based light client emulation to provide enhanced protection against chain faking and operator ransom attacks. Portions of the incentive system that are normally performed on Bitcoin will run on Hemi to improve capital efficiency and resiliency against Bitcoin fee market spikes.

Hemi's Bitcoin tunnel system will initially use Overcollateralised Vaults for all BTC deposits. Once the new custodianship system is launched, the underlying custodianship mechanism will be migrated to the BitVM2-Based Vaults.

While Bitcoin has evolved into a store of value, its use for everyday payments has diminished over time. Additionally, holders of Bitcoin have largely been unable to participate in DeFi unless they accept the security tradeoffs of wrapped Bitcoin solutions. As a result, many users have shifted to Ethereum or other networks for transactions. By incorporating Bitcoin into Hemi's Ethereum-style chain, Bitcoin regains its original utility as a medium of exchange and can be used alongside Ethereum-based assets in DeFi protocols.

Ethereum Tunnels

Hemi's Ethereum tunnels enable secure asset transfers between Ethereum and Hemi by locking assets on Ethereum and minting representative tokens on Hemi. Similar to other optimistic rollups, this system relies on fraud-proof mechanisms to ensure the integrity of L2 state transitions. An added requirement is that Hemi blocks achieve Superfinality before being accepted to protect against 51% attacks.

To decentralise the publication and verification of state roots published to Ethereum for settlement, Hemi plans to introduce a system of collateralised publishers. They will perform state root publications (in addition to publishing DA blobs) and permit anyone to act as a challenger who will receive a portion of a publisher's slashed collateral. That is, if they correctly prove the misbehaviour of a publisher through the fault dispute process.

To transfer assets from Ethereum to Hemi, users initiate a deposit on Ethereum, locking their assets within Hemi's tunnel contracts. Upon confirmation, representative tokens are minted on Hemi, completing the tunnel deposit process.

To return assets from Hemi to Ethereum, users burn their representative tokens on Hemi to initiate a withdrawal of the underlying asset on Ethereum. After the withdrawal initialisation transaction achieves Superfinality and a state root authenticating the withdrawal is published on Ethereum and is not challenged during the fault dispute process, users can claim their original assets on Ethereum from the Hemi tunnel contracts. This system ensures secure, reliable cross-chain transfers by combining Bitcoin's robust security with Ethereum's flexibility.

Asset Portability Between Bitcoin and Ethereum

Hemi's connection to the Bitcoin and Ethereum networks enables Hemi to act as an intermediary that securely moves assets between both networks. Hemi does more than just provide a common blockchain where Bitcoin and Ethereum assets can come together for use in Hemi-based protocols. In the future, this functionality will enable users to transfer Bitcoin assets through Hemi into the broader Ethereum ecosystem, and vice versa.

For example, users could tunnel BTC through Hemi to Ethereum. This option provides a form of ERC-20-compliant tokenised BTC for use in DeFi on Ethereum and other Ethereum L2s that inherits the custodial security guarantees of Hemi's Bitcoin tunnel system. Combined with BitVM-based Vaults, this will provide economically efficient BTC secured with a 1-of-N trust model across the entire Ethereum ecosystem.

Hemi will also be able to tokenise Ethereum-based assets like ETH, ERC20s, and even Ethereum-based NFTs. This tokenisation will occur in a trustless manner on Bitcoin as BRC-20s, Runes, or Ordinals using Hemi's future support for Bitcoin metaprotocol awareness. For example, a new BRC 20 token could be minted that is redeemable 1:1 for native ETH, or an Ordinal could be minted that is redeemable for an Ethereum-based NFT. This mechanism for tunnelling assets out to both networks also enables tokens launched natively on Hemi to be trustlessly transferred to Bitcoin and Ethereum and later redeemed for the original underlying Hemi-native token.

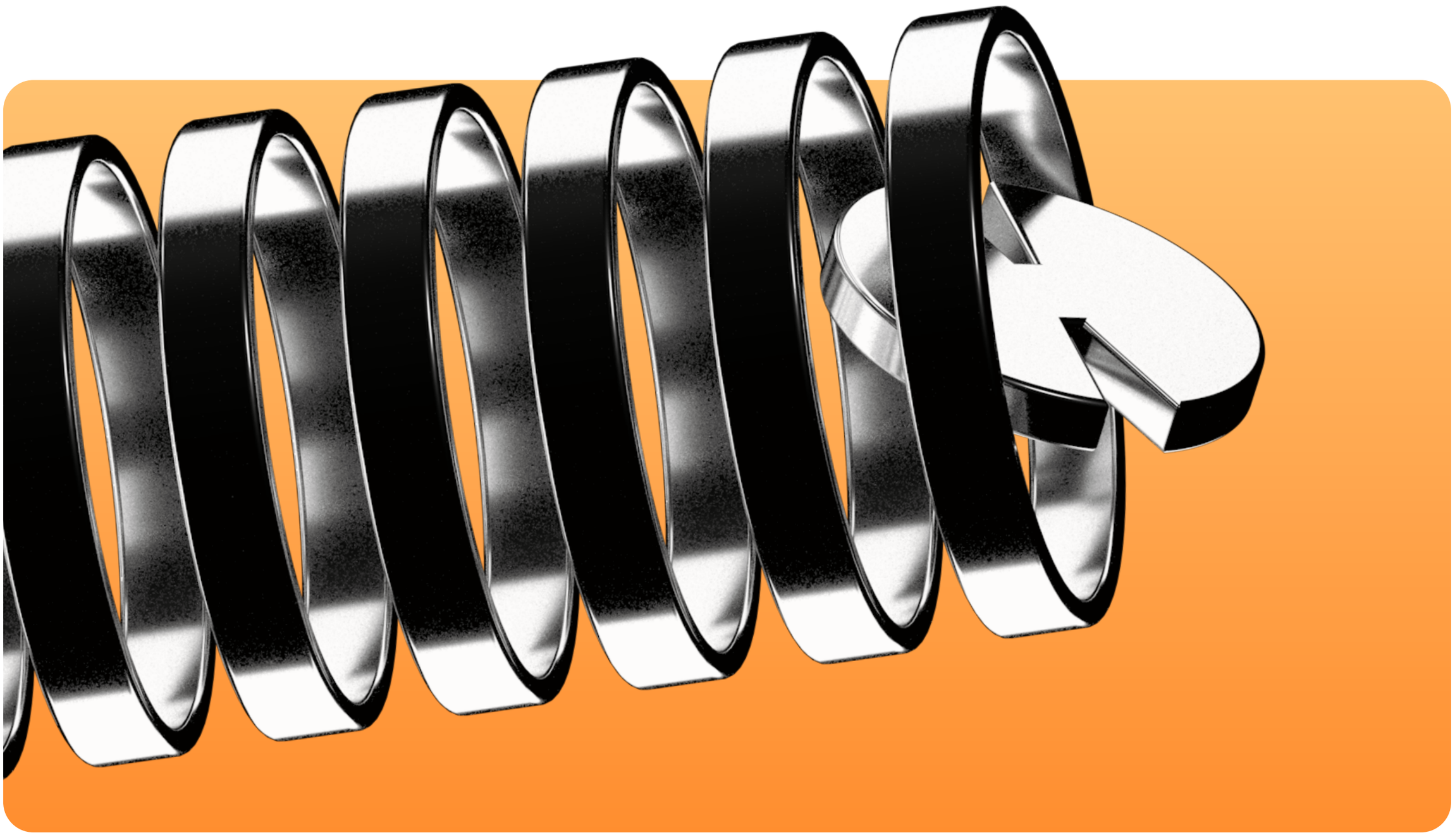
Security and Trust Considerations

Tunnels provide robust cross-chain asset portability with minimal trust assumptions to reduce risks associated with custodial failures and consensus attacks. They operate using robust multi-chain state-awareness, cryptographic proofs, and incentive-aligned operators.

Tunnels utilise Bitcoin's Proof-of-Work to ensure settlement finality to safeguard against chain reorganisations and the associated de-pegging risks. Finality is guaranteed after nine Bitcoin confirmations, ensuring that a completed transfer cannot be reversed or manipulated once it is complete.

Enhancing this security framework, Tunnels employ custodianship models tailored to the value of the assets being transferred and the capabilities of the source network. For Bitcoin-based assets where custodianship and settlement has historically relied on trusted custodians, Hemi employs a dual vault system to securely support deposits of fungible and non-fungible assets regardless of the size. These features bolster Hemi's security framework.

High-value vaults use BitVM2-based custodianship with collateralised validators to secure large deposits with a trust-minimised 1-of-N trust assumption. For smaller deposits, low-value vaults utilise over-collateralised validators. Both vault systems leverage the robust Bitcoin awareness provided by the hVM to ensure the protocol can securely and efficiently monitor for misbehaviour. This approach ensures all transfers are backed by adequate collateral and stringent security measures. Notably, system integrity is maintained across varying transaction sizes.



Encapsulation

The Hemi Network uses encapsulation to bundle, secure, and manage multiple digital assets — including Bitcoin and Ethereum-based tokens and NFTs — within a single package. This feature simplifies complex cross-chain transactions by allowing multiple assets to be handled simultaneously. Ultimately, encapsulation fosters the Hemi Network's ability to enhance efficiency and reduce transaction costs.

Encapsulation ensures that only authorised parties can access or move the bundled assets through security features such as password protection and time locks. For instance, a user could package BTC, an Ethereum-based stablecoin, and an NFT into a single capsule that can only be opened after specific conditions are met.

Encapsulation also supports gasless transfers and smart routing. Users are able to move assets without needing to hold gas tokens to pay transaction fees. Smart routing ensures assets are transferred securely and can be re-routed by the sender if required. These features provide a user-friendly and low-friction experience for casual users.

Implications for Developers and Users

For developers and users, encapsulation simplifies asset management and allows users to create platforms to easily manage portfolios containing assets from multiple blockchains. Developers can build sophisticated financial products that combine assets across different blockchains, such as packaged investment products that include a mix of Bitcoin, Ethereum assets, and tokenised derivatives. This offers investors a diversified exposure within a single tokenised product.

Chainbuilder

Hemi's modular architecture is designed to support a robust ecosystem of L3+ networks that inherit and extend Hemi's security and multi-network interoperability features. They retain the flexibility to optimise for specific use-cases by customising the data availability (DA), execution, and consensus layers. Hemi's upcoming Chainbuilder system will provide developers with the ability to easily spin up and maintain these L3+ networks.

Superfinality

Hemi's Proof-of-Proof consensus protocol provides scalable, efficient Bitcoin security inheritance capabilities by leveraging Hemi as a security aggregation layer.

In this context, a handful of Bitcoin PoP transactions securing Hemi's L2 also secure Hemi's entire L3+ chain ecosystem. They do this without increasing Bitcoin's block space utilisation. Due to PoP's flexibility, these L3+ chains can use whatever native block production consensus protocol best suits their speed, decentralisation, throughput, and decentralisation needs.

Additionally, other L2 networks and independent L1s can leverage Hemi as only a PoP aggregation layer to inherit Bitcoin security without participating in Hemi's L3+ ecosystem.

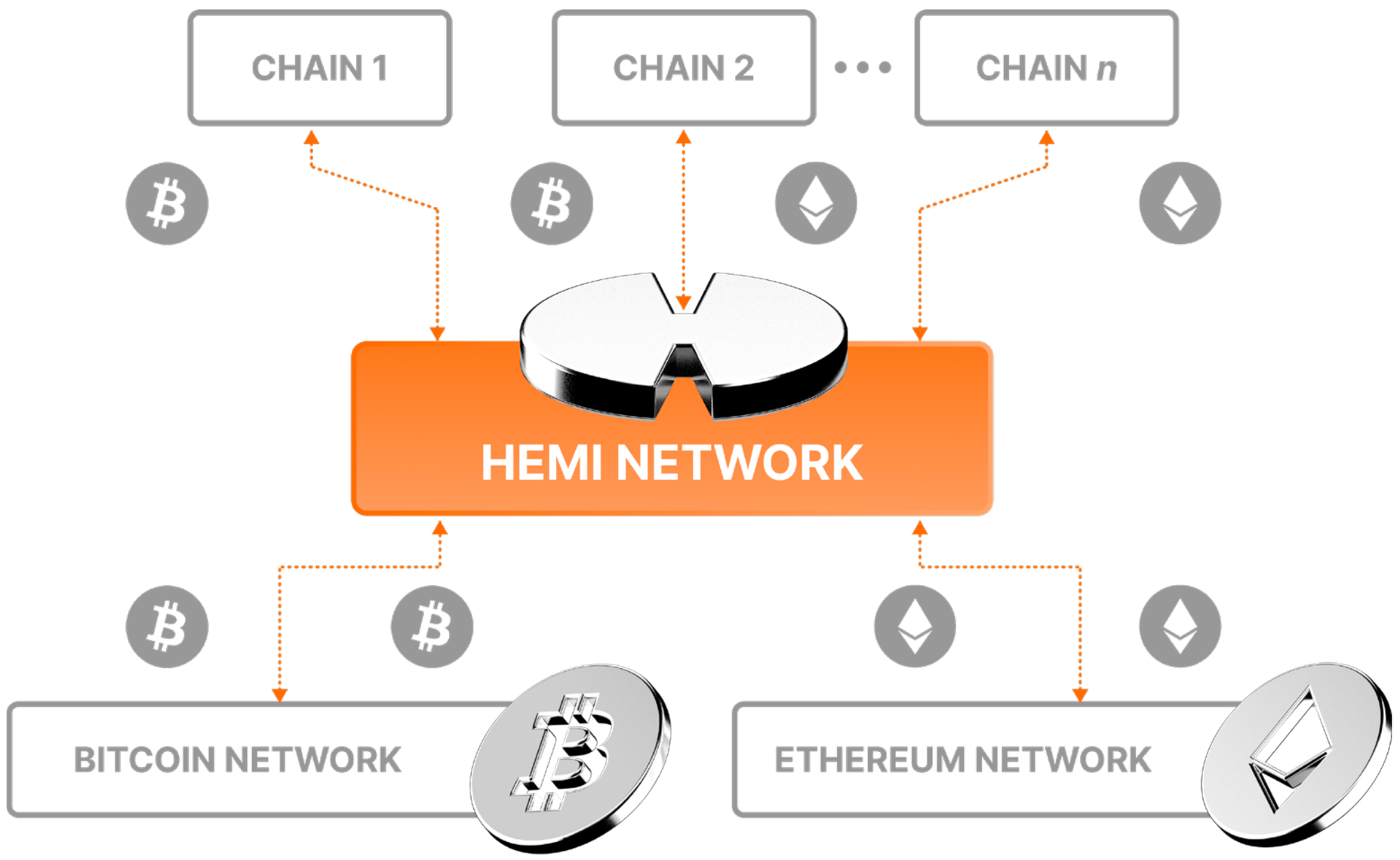
Bitcoin and Ethereum Interoperability

Networks built on top of Hemi can take advantage of some or all of Hemi's multi-network interoperability features. Hemi's tunnel system allows any network that connects to Hemi as an L3+ to gain access to Bitcoin and Ethereum assets.

Any such chain that uses an EVM-based execution environment can also leverage the hVM (and the hBK) directly. This provides smart contracts on their network with direct access to the same Bitcoin awareness available on Hemi's L2. Bitcoin awareness for hVM-supporting chains across the entire Hemi ecosystem will be synchronised through the block derivation process. This synchronisation makes Bitcoin-aware dApps that operate across Hemi's entire chain ecosystem easier and more secure to build.

Additionally, hVM support can be added for other execution environments, enabling developers to build secure Bitcoin-aware dApps using non-EVM environments.

GRAPH 7 **INTEROPERABILITY AND SCALABILITY**



What Applications Does Hemi Unlock?

New applications and improved functionality of existing ones are unlocked by a combination of Hemi's value propositions:

- Secure, capital-efficient BTC and ETH assets programmable in a single EVM environment using industry standards like ERC-20/ERC-721/etc.
- Transfer of Bitcoin-based assets through Hemi out into the broader Ethereum ecosystem and transfer of Ethereum-based assets onto Bitcoin metaprotocols
- Advanced direct Bitcoin introspection for smart contracts without oracles or relayers
- Bidirectional cross-network smart contract calls with Ethereum
- Bitcoin security, inheritance and Superfinality
- Anchoring/auditability of all onchain activity to Bitcoin and Ethereum
- Sophisticated asset management using encapsulation
- Flexible L3+ launchpad, extending all of these features to customisable chains

Use Case: Bitcoin + Ethereum DeFi

The secure availability of Bitcoin and Ethereum assets on a single chain through Hemi's tunnel system allows any EVM-based DeFi protocol to deploy seamlessly on Hemi, supporting assets from both networks without modification.

This setup enables a range of DeFi applications, including decentralised exchanges (DEXes), derivatives, lending markets, synthetic assets, liquid staking, restaking, algorithmic stablecoins, prediction markets, payment systems, treasury management, and yield aggregation.

Use Case: Advanced Bitcoin Awareness and Programmability

The hVM and the hBK enable developers to create once impossibly sophisticated infrastructure and applications that interact directly with Bitcoin. This opens the door to dApps, financial products, and DAOs built natively on Bitcoin — overcoming the historical limitations of Bitcoin's design.

Non-Custodial Bitcoin<>Ethereum DEXes

A non-custodial DEX allows users to securely trade assets natively on Bitcoin for Ethereum-based assets. Assets are delivered either through Hemi or directly on Ethereum. Users agree to the terms of a trade in a smart contract. Then, Ethereum-based assets being traded are held in escrow and are released to the counterparty after they deliver the expected native assets on Bitcoin.

Non-Custodial Bitcoin Lending Markets

A non-custodial Bitcoin lending market allows a borrower to post collateral in the form of Ethereum-based assets and borrow native Bitcoin – directly delivered to their Bitcoin address. The borrower can later repay the loan with interest by sending native Bitcoin back to the specified Bitcoin address. Once repayment of the loan on Bitcoin is detected by the protocol, the borrower's Ethereum-based collateral would be released.

Bitcoin Smart Wallets

Bitcoin smart wallet protocols enable users and smart contracts to programmatically manage a Bitcoin wallet. The protocol coordinates the collateralisation and incentive enforcement of operators who manage keys for the Bitcoin smart wallet. This builds on Bitcoin's tunnelling custodianship systems. Different versions of such a protocol could use different custodianship and collateral mechanisms with different fund security assurances.

Dynamic Bitcoin Fee Marketplaces

A Bitcoin fee marketplace/Bitcoin transaction accelerator protocol enables users to directly interact with Bitcoin miners in a dynamic marketplace to pay for Bitcoin transactions to be processed. Users can attach and modify extra fees paid in Ethereum-based assets to the Bitcoin miner who includes their transaction in a block. More advanced versions of such a protocol could predicate payouts on more sophisticated logic. For example, the fee could only be paid if the transaction is included quickly enough to be able to access a BRC-20 mint.

Custom Bitcoin Asset Tunnelling Protocols

Hemi's own native Bitcoin asset tunnelling system is implemented as smart contracts that leverage Hemi's Bitcoin awareness features. Anyone could launch a modified version that handles collateralization differently or uses a different custodianship system (like a new variant of BitVM or a new custodianship mechanism made possible by future opcodes) to optimise for a specific use case.

Non-Custodial Bitcoin (Re)Staking

A non-custodial Bitcoin staking/restaking protocol allows users to retain custody of their native Bitcoin while earning yield. Staking native Bitcoin to participate in protocols seeking Bitcoin-based economic security generates the yield. Advancements in technologies like BitVM can be used for self-custody of native Bitcoin while providing strong slashability guarantees to participating protocols in the event of misbehaviour while supporting complex fault detection logic.

Native Bitcoin Payment Rails

A native Bitcoin payment rail protocol provides users with the ability to send payments that originate on Hemi but send native Bitcoin to the recipient directly by using liquidity providers who fulfil the native Bitcoin payment for a fee. Different types of protocols could allow users to send tunnelled Bitcoin, or automatically convert other assets like ETH or stablecoins to native Bitcoin sent to the recipient's Bitcoin wallet. Such a protocol could also integrate with payment networks like Lightning.

Use Case: Enhanced Asset Management

Hemi allows users to bundle, secure, and automate the management of digital assets from multiple blockchains through encapsulation. Users can protect their assets with password protection, time locks, and routing automation. These security mechanisms provide unprecedented flexibility of enhanced asset management capabilities.

Reroutable/Recallable Transactions

By encapsulating assets in a reroutable package, the sender can send assets to a user and later reroute or recall the assets if unclaimed. This could be used by service providers like exchanges to send assets to users and be able to re-route the transaction if the user entered the wrong address or lost access to their private key, or to send assets to users which must be claimed within a certain amount of time before the assets are pulled back.

Gasless Transfers

Gasless transfers provide the sender with the ability to send assets that can be redeemed without the user having to hold native gas tokens to pay network fees for low-friction user onboarding.

Portfolio Management

Encapsulation allows a user to package many different assets of various types into a single token. As a result, the entire portfolio is easily transferred in a single low-cost transaction. The portfolio can hold yield-bearing tokens like LSTs/LRTs or LP positions.

Use Case: Bitcoin and Ethereum Anchoring/Auditability

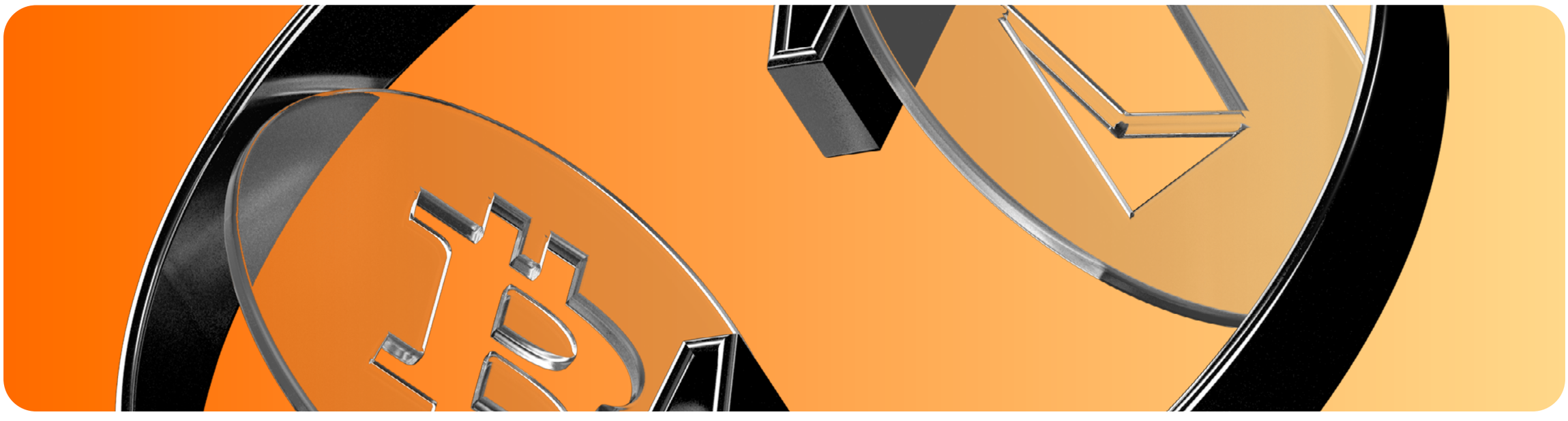
All activities and data published to Hemi is anchored to Bitcoin through Hemi's PoP mining process, and anchored to Ethereum through the publication of state roots for settlement. This feature allows anyone to produce cryptographic audit trails of activity or use Hemi as a multi-network timestamping solution.

Provable AI Model Training and Inference

Recent advancements in cryptography have made zero-knowledge proofs of AI model inference practical. Owners of proprietary models could timestamp their model weights to Hemi and provide zero-knowledge proofs proving that a particular inference result came from a specific input into a particular model. Additionally, as algorithms continue to improve and available computing power grows, producing zero-knowledge proof that a particular model was trained using specific data will become increasingly practical. These technologies, coupled with Hemi, can provide full Bitcoin-authenticated supply chain auditability for AI applications.

Intellectual Property Rights Management

With the advent of widespread AI use, systems for easily licensing IP and proving licensing compliance are becoming increasingly necessary. Hemi's Bitcoin and Ethereum data anchoring enables IP systems that allow easy bulk licensing of various data sources for different use cases with the ability to produce cryptographic proofs of licensing compliance. This solution can enable IP holders the ability to more effectively monetise their property while lowering compliance costs and democratising access to compliant training data for startups.



Document/File Timestamping

Hemi's ability to efficiently timestamp data to Bitcoin and Ethereum can serve needs in verifying the authenticity of data. Real-world examples include proving the state of a legal contract at a specific point in time, preventing stealth edits to news articles, and protecting user-generated content from manipulation.

Decentralised Identity and Verifiable Credentials

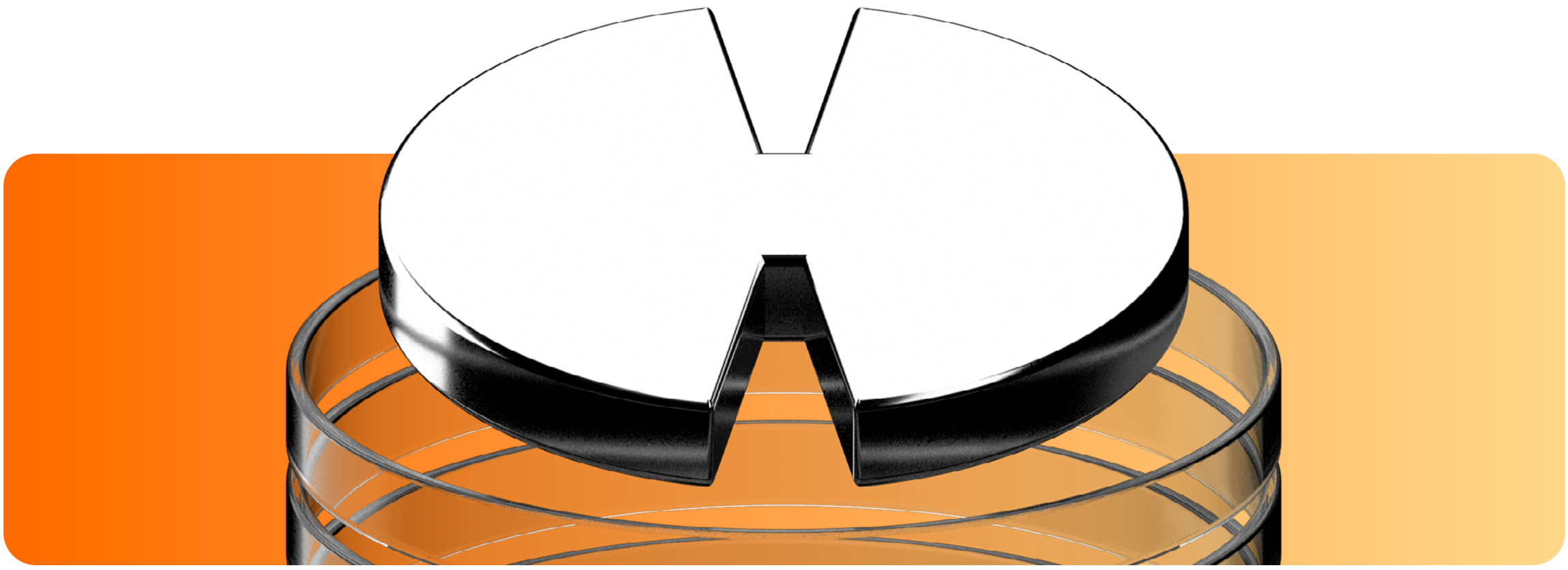
Hemi facilitates decentralised identity solutions through Bitcoin's immutability to anchor verifiable credentials onchain and facilitates robust identity management and rights assignment using Ethereum's programmability. This enables users and organisations to create secure, tamper-proof identity systems able to be used across different platforms and services. It unlocks new possibilities for decentralised authentication, digital certifications, and secure identity verification. Without reliance on centralised authorities, Hemi's decentralised identity solutions and verifiable credentials benefit applications in financial services, healthcare, voting systems, and more.

Final Thoughts

The Hemi Network addresses the gap between Bitcoin and Ethereum. It combines Bitcoin's industry-leading security and liquidity with Ethereum's powerful programmability and diverse ecosystem of assets and protocols. Hemi's core components — such as the hVM, the hBK, superfinality, tunnels, and encapsulation — provide developers with the tools to build decentralised applications that operate seamlessly across Bitcoin and Ethereum without relying on intermediaries or centralised exchanges. Hemi unlocks many novel use cases and additional utility for participants in both ecosystems.

As more complex, high-value applications emerge — especially in decentralised finance and cross-chain transactions — the need for secure and tamper-proof finality increases. Leveraging the real-time synchronisation provided by the hVM and facilitated by the hBK, the concept of superfinality ensures that once transactions are confirmed, they are immutable and secure against chain reorganisations. This added layer of security enhances developers' confidence to build high-stakes applications, further advancing cross-chain interoperability within the Hemi Network.

This integration of Bitcoin and Ethereum goes beyond improving existing applications; it also creates new opportunities for cross-chain DeFi platforms, programmable Bitcoin assets, secure asset management, and innovative value creation methods. Hemi's technology expands the possibilities for blockchain, encouraging new ideas and use cases that go beyond current limits. By providing the necessary infrastructure, Hemi enables developers and enterprises to tackle today's challenges and push the boundaries of decentralised applications.



DLResearch x hemi

Hemi: A Modular L2 Connecting the Bitcoin and Ethereum Ecosystems

www.dlnews.com/**research**