

Bitlayer – First BitVM, Powering Bitcoin DeFi



Executive Summary

Bitlayer is a pioneering Layer-2 (L2) network built to scale Bitcoin and enable decentralized finance (DeFi) on the world's largest cryptocurrency. By leveraging the **BitVM** paradigm – an innovative mix of zero-knowledge and optimistic proofs – Bitlayer brings **Turing-complete smart contracts** and high-throughput execution to Bitcoin without compromising Bitcoin's security.

This report provides a comprehensive overview of Bitlayer's business strategy, ecosystem growth, and technical architecture for a dual audience of institutional and retail stakeholders interested in Bitcoin-based DeFi opportunities and infrastructure evolution.

Opportunity:

Bitcoin today holds immense untapped capital, yet its limited throughput and lack of programmability prevent this value from participating in DeFi. Bitlayer addresses this gap by introducing a Bitcoin “rollup” L2 that anchors security to Bitcoin's own blockchain, allowing BTC to *flow* into yield-generating DeFi ecosystems. The rationale is clear: expanding Bitcoin's utility beyond “digital gold” into an active financial asset can unlock new revenue streams (for users and miners alike) and cement Bitcoin's role in the multi-chain Web3 economy.

Solution:

Bitlayer's vision is to become the *computational layer for Bitcoin*, combining a fast Proof-of-Stake consensus chain with verifiable settlement on Bitcoin L1. The network achieves **sub-second transaction finality** on the L2 for a smooth user experience, while periodically settling batched state changes onto Bitcoin for ultimate security. Bitlayer's unique BitVM-based approach enables complex smart contracts to execute off-chain, with **fraud proofs** enforced on-chain if necessary, ensuring **Bitcoin-equivalent security** for L2 state transitions. A **trust-minimized Bitcoin bridge** (the BitVM Bridge) is deeply integrated, allowing BTC to be locked on L1 and “pegged” into Bitlayer (and other chains) as an L2 token (often called *Peg-BTC* or *Yield BTC*), and vice versa, with only *one* honest actor required to guarantee safety. This is a significant improvement over traditional federated bridges that require a majority of custodians to be honest.

Traction:

Strategically, Bitlayer has differentiated itself through key partnerships and rapid ecosystem growth. It has aligned with major Bitcoin mining pools – Antpool, F2Pool, and SpiderPool – which collectively control over one-third of Bitcoin's hashrate. This alliance not only legitimizes Bitlayer's BitVM implementation as the first of its kind on Bitcoin but also helps ensure BitVM transactions (which use *Non-Standard Transactions*, or NSTs) are mined and confirmed reliably. At the same time, Bitlayer has formed integrations with multiple Layer-1 and Layer-2 blockchain ecosystems (including Sui, Base, Arbitrum, StarkNet, Sonic, and Plume) to extend Bitcoin's liquidity into diverse DeFi networks. Since launching its V1 mainnet, Bitlayer reached an all-time high of **\$850 million TVL** with **200+ decentralized applications** deployed on the network – a testament to the demand for Bitcoin DeFi solutions. Prestigious investors such as **Franklin Templeton** and **Polychain Capital** have led funding rounds totaling \$25 million, underscoring strong institutional confidence in Bitlayer's approach.

Outlook:

Bitlayer is on track to launch its **Mainnet V2 (rollup architecture)** in Q2 2025, marking Bitcoin's first full-featured rollup L2 and a major milestone in Bitcoin's evolution. This upgrade will solidify Bitlayer's technical foundation (with EVM compatibility, advanced proving mechanisms, and flexible data availability options) and likely spur a new wave of Bitcoin-focused DApps and liquidity. Going forward, Bitlayer's strategy involves continued multi-chain integration, utilizing technologies like CCIP (Cross-Chain Interoperability Protocol), to connect Bitcoin with leading smart contract networks, with an initial focus on a trust-minimized bridge between Bitcoin and Ethereum. The ultimate vision is a thriving **Bitcoin DeFi (BTC-Fi)** ecosystem where Bitcoin's vast value can participate in lending, trading, yield farming, and more, all secured by Bitcoin's proof-of-work integrity. If successful, Bitlayer could become a cornerstone of Bitcoin's next chapter: a scalable financial platform that marries Bitcoin's security and liquidity with the programmability of modern DeFi.

Introduction: Why Bitcoin Needs a Layer-2 Like Bitlayer

Bitcoin remains the most secure and valuable blockchain, yet its base-layer design (limited to roughly seven transactions per second and a non-Turing-complete script) confines it to payments and value storage. Core DeFi functions such as lending, decentralized trading, or yield strategies simply cannot run on Layer 1. As Bitlayer co-founder Charlie Hu notes, Bitcoin “doesn’t have smart-contract capabilities; to do DeFi you must bridge to a programmable, trust-minimised Layer2.”

That gap leaves hundreds of billions in BTC sitting idle. While Ethereum and other smart contract chains channel their native assets into on-chain markets, Bitcoin holders can choose little beyond speculative holding or risky centralised lending desks. Unlocking this capital would generate new yield for users and fresh fee revenue for miners, turning static “digital gold” into an active part of Web3.

Bitlayer vs Ethereum

Source: docs.bitlayer.org

Feature	Bitlayer	Ethereum
Gas Price	Lower due to efficiency mechanisms.	Variable, dependent on network demand. High demand can lead to increased gas prices.
EVM Support	Supports EVM-compatible smart contracts.	Full EVM support as the native platform.
Solidity Support	Supports up to Solidity version v0.8.28. Future versions will be supported.	Supports the latest versions of Solidity, with ongoing updates.
Developer Implications	Offers a platform leveraging Bitcoin's security. Easier transition for those familiar with Ethereum's EVM.	Mature tooling and community support.
User Implications	Access to innovative dApps leveraging Bitcoin's security.	Vast ecosystem of dApps.

Attempts to extend Bitcoin have been largely unsuccessful. Federated sidechains like Liquid and RSK compromise trustlessness; users rely on custodians to guard the bridge. Lightning excels at fast payments, but struggles with complex, composable contracts. Early “Bitcoin rollups” posted data on-chain but lacked any mechanism for Bitcoin nodes to verify state validity, leaving users unprotected if an operator cheated.

The 2023 Ordinals surge exposed these limits: a rush to embed NFT data flooded the mempool, fees spiked, and many transactions failed, wasting BTC without improving utility. Such episodes make clear that Bitcoin needs a scalable Layer-2 that preserves its security while adding real programmability.

Bitlayer sets out to fill that role. By anchoring an EVM-compatible roll-up to Bitcoin’s proof-of-work consensus, it promises smart-contract functionality and high throughput without altering the base chain or introducing new trusted intermediaries.

Bitlayer Vision and Strategy

Bitlayer's aim is simple yet ambitious: **turn Bitcoin from passive “digital gold” into the secure engine of a full DeFi economy**. It does this by becoming the “Computational Layer for Bitcoin”, pairing a high-speed proof-of-stake chain with Bitcoin's proof-of-work finality. Version 1, launched as a side-chain, proved market demand; the forthcoming **V2 roll-up** cements the model, posting every L2 state root to Bitcoin via **BitVM** fraud proofs so that Bitcoin itself enforces L2 integrity.

Core Pillars

1. Build on Bitcoin's security, add missing features

All execution happens on Bitlayer's fast EVM chain, yet periodic checkpoints land on Bitcoin, giving users both sub-second UX and Bitcoin-grade immutability.

2. Minimize trust everywhere

The **BitVM** Bridge needs only one honest signer to keep the BTC peg safe, and any watcher can challenge invalid roll-up states. No federations, no privileged operators, just open verification baked into game-theory incentives.

3. Offer Ethereum-class developer experience

Solidity contracts deploy largely unchanged, while dual finality supports everything from DeFi trading to real-time gaming, speed and certainty few other Bitcoin L2s can match.

4. Align with miners and the wider community

Bitlayer works hand-in-hand with pools like Antpool, F2Pool and SpiderPool (> 30 % hashrate) to mine BitVM transactions. Miners gain a fresh fee stream as block subsidies shrink; Bitlayer gains guaranteed inclusion of its on-chain proofs, a symbiosis that folds miners into Bitcoin's DeFi future.

5. Pair seasoned leadership with ecosystem growth

Founders Charlie Hu and Kevin He have scaled projects at Polygon, Polkadot and Huobi. In barely a year, they moved from BitVM research notes to a live network hosting hundreds of dApps and attracting capital from Franklin Templeton, Polychain and others. Beyond the core L2, they seed DEXes, lenders and oracles (what they call “BTC-Fi”) to ensure liquidity and utility arrive together.

The outcome

Bitlayer's roll-up architecture, trust-minimized bridge and miner partnerships create a pathway for trillions in dormant BTC to enter DeFi without leaving Bitcoin's security umbrella. By coupling technical innovation with stakeholder alignment, Bitlayer is positioned to lead Bitcoin's evolution from a savings asset to an active, yield-bearing cornerstone of Web3.

Business Differentiators & Competitive Positioning

Bitlayer Competitive Edge

Dimension	Bitlayer Advantage	Why It Matters
Security Anchor	Direct Bitcoin settlement every L2 state root is confirmed on-chain via BitVM fraud-proofs.	Removes federation risk seen in Liquid/RSK; users enjoy Bitcoin-equivalent security without trusting custodians.
Bridge Model	"One-honest-party" peg - BitVM Bridge needs only a single honest signer to keep funds safe.	Stronger than multisig bridges (require majority honesty); mitigates high-profile wrapped-BTC failures.
Developer On-Ramp	out-of-the-box. Full EVM compatibility deploy Solidity contracts	Re-uses Ethereum tooling; lowers costs and accelerates migration of DEXes, lenders, oracles, etc. Competing Bitcoin stacks require new languages.
Performance & Finality	Sub-second-level soft finality + Bitcoin hard finality (≈5-15 blocks).	Users get instant UX; institutions get irreversible settlement within ~1 hour - a unique dual-finality spectrum versus Lightning-only speed or sidechain-only security.
Flexibility	Configurable data availability (on-chain or external DA) + high-throughput PoS execution.	Serves both security maximalists and cost-sensitive apps; supports real-time trading & gaming that Bitcoin L1 cannot.
First-Mover on BitVM	First live BitVM rollup backed by >30% Bitcoin hashrate.	Early standard-setter; real-world usage and miner buy-in create a lead that latecomers must overcome.

Bottom line

Bitlayer fuses Bitcoin's unmatched security and liquidity with Ethereum-class smart-contract capability, yet strips out federation risk. It offers a fast, developer-friendly, trust-minimized L2 that already runs on real Bitcoin hash power, positioning it as Bitcoin's answer to Ethereum roll-ups rather than just another sidechain.

Strategic Partnerships & Ecosystem Traction




A growing network of **strategic partnerships** and tangible ecosystem traction bolsters Bitlayer's rapid progress. These partnerships span Bitcoin infrastructure, other blockchain networks, and financial institutions, all converging to support Bitlayer's vision. Below, we outline key partners and integrations, followed by an overview of Bitlayer's ecosystem growth:

Key Partners and Integrations

To illustrate Bitlayer's collaborative strategy, the section summarizes major partners, their domain, and their role in Bitlayer's ecosystem

Mining Pool Alliances:







Bitlayer Mining Pool Partners

Partner	Integration Type	Role
 Antpool (Bitmain)	Bitcoin Mining Pool	Bridge Operator & BitVM Mining Partner: Collaborating to mine BitVM transactions and ensure on-chain inclusion of Bitlayer's Non-Standard TXs. Antpool's support helps secure the BitVM Bridge and is aimed at driving more transaction fees to miners. Antpool's CEO endorsed Bitlayer as strengthening Bitcoin's infrastructure and long-term miner revenues.
 F2Pool	Bitcoin Mining Pool	BitVM Mining Partner: Providing hashrate and mempool support for BitVM transactions. F2Pool's leadership emphasized balancing Bitcoin network security with innovation, supporting high-quality BitVM projects like Bitlayer. Together with Antpool and SpiderPool, F2Pool helps Bitlayer achieve ~36% of network hashrate coverage for BitVM transaction confirmation.
 SpiderPool	Bitcoin Mining Pool	BitVM Mining Partner: Contributing mining power and technical integration for BitVM. SpiderPool's CTO highlighted that Bitlayer's scaling solutions (BitVM-based) enable faster, low-cost Bitcoin transactions and align with SpiderPool's vision of empowering Bitcoin DeFi while preserving security. Provides additional decentralization to BitVM transaction processing.

Bitlayer's integration with **three of the top Bitcoin mining pools** is a landmark achievement. Collectively, these pools represent over **one-third of Bitcoin's hashrate**, meaning more than one-third of Bitcoin's mining power is actively supporting Bitlayer's BitVM transactions. This collaboration is unprecedented for a Bitcoin L2 project. By working with pools to accept Non-Standard Transactions (needed for BitVM's on-chain steps), Bitlayer essentially extends Bitcoin's protocol in a *backwards-compatible* way – without requiring a soft fork, they created a **parallel “bridge mining network”** that relays and mines BitVM transactions reliably. The mining partners have publicly praised this effort: F2Pool and SpiderPool echoed support for innovation that doesn't compromise security. This alignment of incentives means Bitlayer is not working against Bitcoin's entrenched interests, but with them - a critical factor for sustainable growth in the Bitcoin ecosystem.

Layer-1 and Layer-2 Integrations:

Bitlayer Blockchain Partners

Partner	Type	Role
 Sui Network (Mysten Labs)	Layer-1 Blockchain (Move VM)	Launched Peg-BTC via BitVM Bridge, importing > 587 BTC into Sui DeFi and giving holders on-chain yield.
 Base (Coinbase's L2)	Ethereum L2 (OP Stack)	Adds BitVM Bridge so BTC can flow into Coinbase's OP-stack L2 and its DeFi apps.
 Arbitrum	Ethereum L2 (Optimistic)	Destination for Peg-BTC, opening Arbitrum's large DeFi market to Bitcoin liquidity.
 StarkNet (StarkWare)	Ethereum L2 (ZK-Rollup)	Extends BTC into StarkNet's ZK-rollup dApp ecosystem through BitVM Bridge.
 Sonic (Sonic SVM)	Layer-1 (Solana VM-based)	Connects BTC to a Solana-VM chain, proving Bitlayer's non-EVM versatility for high-speed use-cases.
 Plume Network	Layer-1 Blockchain	Brings Bitcoin liquidity to a newer L1, highlighting Bitlayer's chain-agnostic expansion.

On the multi-chain front, Bitlayer has shown impressive agility. In a short time, it formed integration partnerships with several prominent blockchain networks. The **Sui integration** is especially notable because it's already live (YBTC on Sui) and provides a real use-case of Bitcoin DeFi: BTC holders can deposit into Sui's BitVM bridge contract and receive YBTC (Pegged BTC) to deploy in Sui's DeFi protocols. In doing so, they earn yields such as staking rewards or lending interest on Sui, all while effectively still being "long BTC". This is a paradigm shift for BTCfi as Bitcoin's value is actively utilized to generate on-chain yield instead of sitting idle.

Similarly, partnerships with **Base, Arbitrum, StarkNet, Sonic, and Plume** extend Bitlayer's reach. These networks span both optimistic and zero-knowledge rollups (Arbitrum, StarkNet) and even non-EVM environments (Sonic's Solana VM). Bitlayer's bridge being flexible enough to support both EVM and non-EVM chains is a key advantage. It positions Bitlayer as potentially the *de facto* gateway for moving Bitcoin into various DeFi worlds. If Bitlayer becomes a hub where BTC can be ported anywhere (akin to how Ethereum's USDC or USDT moves cross-chain), that's a powerful network effect. Each new integration adds more utility for Bitlayer's YBTC, potentially increasing fees and attracting more users to funnel back to Bitlayer. For instance, an Arbitrum user could use BTC in Arbitrum's DeFi via Bitlayer, and when done, withdraw back to Bitcoin L1 through Bitlayer's bridge – all without trusting a centralized exchange or custodian.

This interoperability focus is a strong differentiator as well: Bitlayer is not trying to isolate Bitcoin in its own ecosystem, but rather to make Bitcoin a *liquid asset across ecosystems*, with Bitlayer as the facilitator.

Institutional and VC Backing:

The investments led by Franklin Templeton and Polychain, alongside many more prestigious participants, not only provided capital but also validation. Franklin Templeton's involvement is particularly significant: it's a very traditional finance player deeply vetting a crypto project. Their presence suggests Bitlayer's narrative of unlocking Bitcoin's value resonated with institutions looking at long-term crypto opportunities. In fact, Franklin Templeton publicly championed the concept of Bitcoin earning yield (seeing it as a way to enhance Bitcoin's appeal beyond just being held). Such endorsements can attract other institutional participants (e.g., pension funds or crypto yield funds) to explore Bitcoin DeFi via Bitlayer, knowing a reputable firm is already engaged. Polychain's investment, on the other hand, signals to the crypto-native community that Bitlayer's tech is promising (Polychain has a track record of backing successful protocols early). These backers may also assist Bitlayer in governance, market-making, and ecosystem growth initiatives, further solidifying Bitlayer's position.

Developer and Community Growth:

Partnerships are not only external; Bitlayer is also cultivating an internal community of validators, node operators, and developers. The press mentions that Bitlayer is “*actively onboarding more validators and early adopters to help secure and expand the BitVM Bridge*”. This likely refers to testnet participants, BitVM challenge game testers, and new projects deploying on Bitlayer. An ecosystem thrives when many independent actors are involved. Having many validators (even though it's PoS, broad participation increases decentralization) and third-party dev teams launching DApps indicates a healthy network. Bitlayer already boasts **200+ DApps launched** on L2 since its initial launch, covering use cases from BTC DEXes and staking platforms to oracles and even NFT-related (rune & ordinal) apps. This breadth shows that Bitlayer is attracting a *diverse array of projects*. It's not just one or two flagship apps – it's an ecosystem forming. Such traction can create a virtuous cycle: more DApps attract more users and liquidity, which in turn attracts more DApps, and so on.

Total Value Locked and Usage Metrics:

Bitlayer Transaction History Last 14 Days



Achieving an **all-time high TVL of \$850 million** on Bitlayer L2 is a standout milestone. For context, this approaches the scale of mid-sized Ethereum L2s or alt-L1s – an impressive feat for a Bitcoin L2 that has not yet deployed the full rollup. It demonstrates substantial user trust in depositing assets into Bitlayer's ecosystem. Additionally, it implies there are yield opportunities or applications on Bitlayer attractive enough to draw nearly a billion dollars in assets. The *growth rate* is noteworthy: in under a year from its Series A funding, Bitlayer went from concept to hundreds of millions in TVL and live partnerships. This rapid execution sets Bitlayer apart from many blockchain projects that spend longer in R&D. It also provides a “**proof of concept**” – Bitlayer doesn't just promise capabilities, it's already showcasing them.

Overall, Bitlayer's strategic partnerships and ecosystem metrics paint the picture of a project with strong momentum and network alignment. By engaging miners, Bitlayer secured the base layer support needed for its BitVM tech. By integrating with other chains, it extended its reach and demonstrated the value of its bridge. By fostering its own DeFi apps and securing funding, it built confidence in its viability. This multi-pronged traction significantly de-risks the project for potential users and partners: one can see that Bitlayer is not operating in isolation but is at the center of a growing web of Bitcoin and crypto stakeholders coalescing around the idea of Bitcoin DeFi.

Bitcoin DeFi and Yield Generation Opportunities

A primary promise of Bitlayer is to unlock **yield generation opportunities for Bitcoin**, turning BTC from a passive asset into an active participant in DeFi. This section explores how Bitlayer enables Bitcoin holders to earn on-chain yields, the types of DeFi activities now possible with BTC, and the broader implications for the Bitcoin ecosystem and investors.

From “HODL” to “Deploy”:

Traditionally, Bitcoin’s value proposition for holders has been price appreciation (i.e., “**HODL and hope**”) or at best, lending out BTC on centralized platforms for interest – a practice not without risks, as seen in various CeFi lender failures. Bitlayer changes this by allowing BTC to be *trust-minimized, lent, staked, or otherwise utilized on-chain* to earn rewards. Through Bitlayer’s BitVM bridge and YBTC mechanism, a Bitcoin holder can lock BTC on Layer-1 and obtain an equivalent token (e.g., Yield BTC or YBTC) on Bitlayer or a connected chain. This YBTC can then flow into smart contracts just like any ERC-20 token on Ethereum or any native asset on other chains, meaning BTC holders can now become liquidity providers, yield farmers, borrowers, or any role available in DeFi.

Concrete Yield Use-Cases Enabled

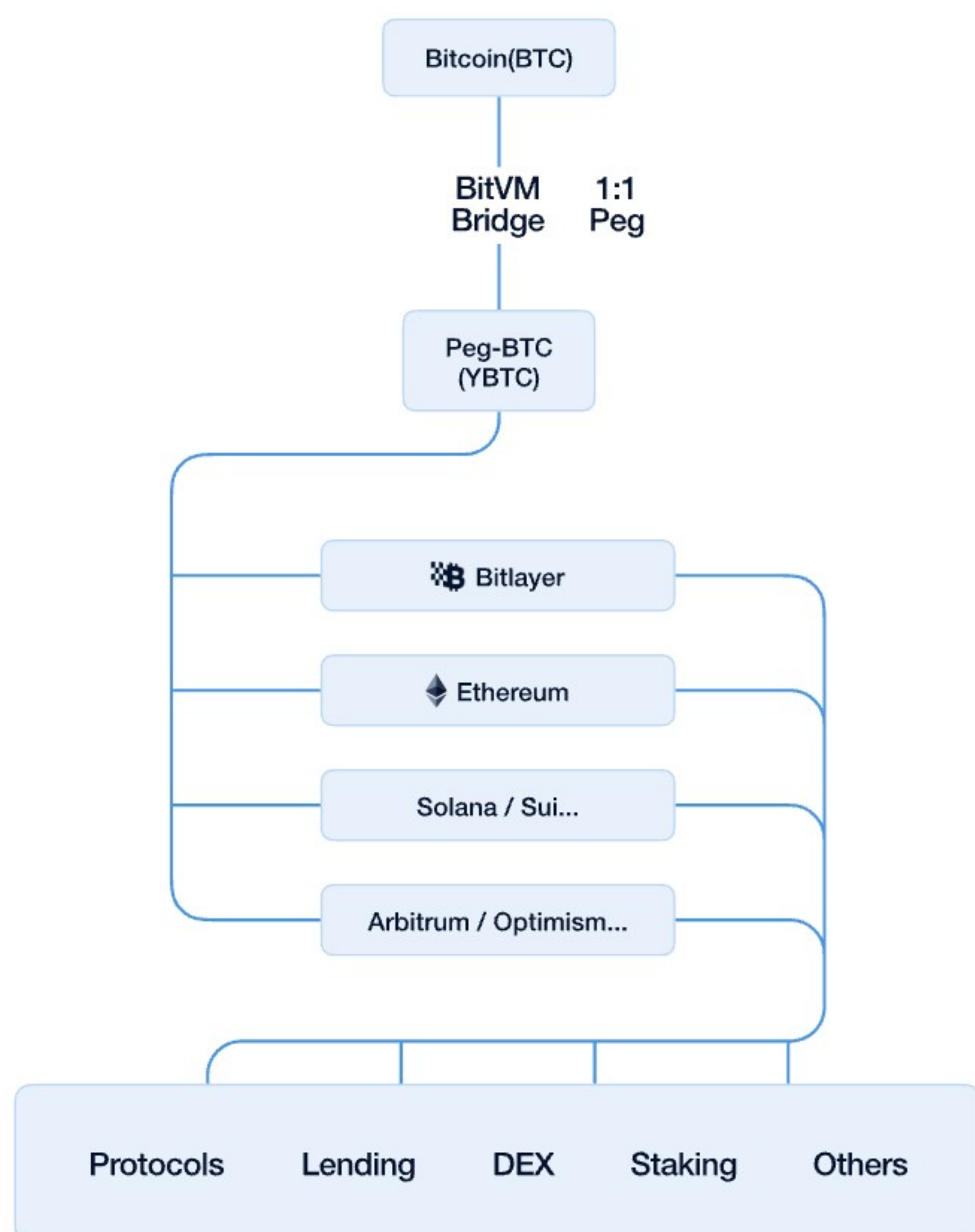
Yield Use-Case	What it Enables	Typical Platforms / Examples
Yield-farming & Liquidity provision	Supply Peg-BTC (YBTC) to AMMs/liquidity pools and earn swap fees + incentives.	YBTC/SUI pool on Sui; YBTC/ETH or YBTC/USDC pools on Arbitrum or Base.
Lending & Borrowing	Lend YBTC to earn interest, or post it as collateral to borrow stablecoins without selling BTC.	Compound-style money markets on Bitlayer L2 or integrated chains.
Staking & Restaking	Stake or liquid-stake BTC to secure protocols and receive yield-bearing derivative tokens.	Liquid-staking modules on Sui (YBTC-staking pilot) and forthcoming Bitlayer services.
On-chain derivatives / structured products	Lend YBTC to earn interest, or post it as collateral to borrow stablecoins without selling BTC.	Maker-like vaults, options AMMs and structured-yield protocols launching on Bitlayer EVM.

Native, On-Chain Yield, Not CeFi IOUs:

A crucial point is that the yields enabled via Bitlayer are “**native, on-chain yields**”. This means the yield comes from actual protocol revenue (trading fees, interest paid by borrowers, staking rewards from protocol inflation, etc.) within decentralized protocols, *not* from off-chain lending desks or unsustainable incentive schemes. “*This yield is real yield, generated within DeFi, without relying on incentivized tokens or other artificial mechanisms,*” Charlie explains. In other words, Bitcoin can now generate an **organic yield** similar to how ETH holders earn fees in DeFi or staking rewards – a fundamental shift from the past, where any yield on Bitcoin typically meant entrusting a third party to lend it out behind the scenes. By keeping the yield generation on-chain and transparent, Bitlayer allows BTC holders to gauge and manage their risk better, and avoid opaque arrangements that have led to losses in the past (for example, Bybit’s wrapped BTC issues were alluded to, where trust in multisig signers caused vulnerability).

Paradigm Shift Illustrated – Sui Integration:

The partnership with Sui offers a concrete illustration of Bitcoin DeFi in action:



- Bitcoin holders used Bitlayer’s bridge to mint **YBTC** on Sui.
- Once on Sui, **users could stake YBTC to earn interest, lend it out for yield, use it as collateral for loans, or trade it on Sui’s DEXes for fees.** All these activities generate some form of return, either in the form of more YBTC, additional tokens, or fees.
- Crucially, throughout, the user retains exposure to Bitcoin’s price (their YBTC is 1:1 backed by BTC), so they are *earning yield while maintaining direct exposure to BTC’s value*. This is a big selling point: *Earn yield without selling your Bitcoin*. It marries the store of value appeal (don’t lose your upside) with “yield-bearing asset” appeal (make your asset work for you). Franklin Templeton has pointed out that this capability could “**boost BTC’s appeal beyond the long-prevalent store of value story**” by giving investors a way to get income from BTC holdings.

The success so far on Sui is telling and if similar outcomes occur on Base, Arbitrum, and others via Bitlayer, we could see thousands of BTC flowing into DeFi protocols across networks, significantly growing the overall DeFi TVL and usage.

Bitcoin represents the largest single source of liquidity in crypto that has been largely untapped by DeFi. Bitlayer’s role is to **inject this liquidity into DeFi** in a trust-minimized way. As the BitVM bridge brings more BTC into various protocols, the total liquidity (and hence Total Value Locked) across DeFi can increase substantially. A higher TVL generally leads to a more robust and attractive DeFi ecosystem, benefiting everyone, from small users (who enjoy better liquidity, lower slippage, and more opportunities) to large institutions (which can deploy large amounts without moving markets).

Yield Bitcoin (Yield BTC) – a New Asset Class?

Bitlayer’s concept of Yield BTC (which is essentially the bridged Bitcoin that can earn yield) could be seen as carving out a new subclass of BTC. There may emerge a distinction between *inactive BTC* (cold storage) and *active BTC* (Yield BTC in DeFi). Over time, if a meaningful percentage of Bitcoin’s supply becomes Yield BTC, it could even influence Bitcoin’s economy – e.g., if many BTC are locked earning interest, the circulating supply on exchanges might drop, potentially affecting price dynamics (a scenario similar to ETH’s staking reducing float).

It also introduces *Bitcoin yield curves* – for example, one could imagine interest rate markets for borrowing BTC on various terms, all facilitated by the liquidity that Bitlayer brings on-chain. This is speculative, but it shows the far-reaching implications: **Bitcoin could develop a DeFi-driven financial layer with interest rates and credit markets**, which would be a radical extension of its current purely monetary role.

In conclusion, Bitlayer significantly expands the capabilities of Bitcoin holders with their assets. **DeFi on Bitcoin** is no longer an oxymoron – it is here in early form and growing. The ability to earn real yield on BTC without forsaking Bitcoin’s security or upside is a powerful offering that could attract both crypto-native users and traditional investors into the space. As more users realize they can have their Bitcoin and earn on it too, the adoption of Bitcoin in DeFi (or **BTC-Fi**) is likely to accelerate, with Bitlayer at the center, enabling these flows. This not only benefits individual investors seeking returns but also fortifies the entire Bitcoin network with increased activity and utility.

Technical Section: Architecture, BitVM, Bridge Design, and Security Assumptions

While the business implications of Bitlayer are vast, its foundation is a sophisticated technical architecture that marries cutting-edge cryptography with pragmatic design. In this section, we delve into Bitlayer's technical architecture, explain the BitVM-based rollup mechanism, outline the BitVM Bridge design for BTC transfer, and discuss the security assumptions and guarantees of the system.

Layer-2 Architecture Overview

Dual-Level Architecture:

Bitlayer operates on a dual-layer model comprising a Layer-2 blockchain (the Bitlayer network itself) and Bitcoin's Layer-1 as the settlement layer. The L2 is an EVM-compatible blockchain using a Proof-of-Stake (PoS) consensus for fast block production and high throughput. This means that within Bitlayer, validators stake a native token (BTR) to secure the network and reach consensus on L2 transactions, similar to how validators work on networks like Polygon or BNB Chain. The L2 block time and finality are on the order of a second or less, providing a responsive environment for users.

On top of this PoS chain, Bitlayer implements a rollup protocol. At regular intervals, the L2 state is summarized (in the form of a state root hash and accompanying cryptographic proofs) and committed to the Bitcoin blockchain (L1). In essence, Bitlayer is a rollup on Bitcoin: it batches many L2 transactions and posts a succinct proof on L1 to prove those transactions were valid. If we analogize to Ethereum's ecosystem, Bitlayer is to Bitcoin what Optimistic or ZK-Rollups are to Ethereum, except that Bitcoin's scripting constraints require a novel approach (BitVM) to accomplish this.

Network Participants:

Bitlayer's L2 network has distinct roles:

Bitlayer L2-Network Roles & Incentives

Participant	Core Duties	Key Incentive / Safeguard
Validators (PoS stakers)	Stake BTR, produce L2 blocks, keep the chain live. One validator at a time is promoted to Roll-up Operator.	Earn block fees & staking rewards; stake can be slashed for mis-behavior.
Roll-up Operator (rotates among validators)	Sequencer-order & execute txsProver-generate zk/optimistic proofs Controller-post state roots to Bitcoin and handle dispute windows.	Must lock BTC collateral on L1; bond is lost if fraud is proven.

Full Nodes / Watchers	Keep a full copy of Bitlayer, verify every state change, and challenge invalid roots on Bitcoin. Act as decentralised "police".	Claim a share of the operator's slashed collateral when a successful fraud challenge is filed.
Attesters (Bridge committee)	Co-sign peg-in/peg-out transactions for the BitVM Bridge; maintain the two-way BTC peg.	Trust-minimised: safety needs only one honest signer, may receive bridge fees for their service.

Dual Finality Model:

As introduced, Bitlayer offers transactions two levels of finality:

Bitlayer L2-Dual Finality Model

Finality Layer	How It's Achieved	Typical Time	Practical Meaning
Soft Finality (L2)	Tx included in a Bitlayer PoS block and not reverted.	Sub-second	"Instant confirmation" suitable for DeFi trades, UX feedback; By using a deterministic consensus protocol, there is no risk of L2 re-orgs or transaction rollbacks.
Bitcoin Finality (L1)	Every state change is verifiably settled on Bitcoin through BitVM-based fraud proofs.	Approximately 6 hours (state committed); Approximately 7 days (pass the challenge window)	Bitcoin/Hard Finality is achieved when the L2 state is settled and finalized on the Bitcoin blockchain. At this point, the transaction becomes as immutable as native BTC

BitVM and Optimistic Rollup Mechanism

At the heart of Bitlayer's technical breakthrough is **BitVM**, a concept originally proposed by Robin Linus, which Bitlayer has extended. BitVM provides a way to execute arbitrary computations off-chain and verify them on-chain using Bitcoin's limited scripting. It's akin to an optimistic rollup, where the chain *optimistically accepts* a proposed new state, and only if someone finds a fault do they resort to an on-chain dispute resolution.

How BitVM Secures Bitlayer — concise version

1. Execute off-chain, prove off-chain.

The roll-up operator processes all L2 transactions inside Bitlayer's PoS chain and produces a ZK proof of the new state. Because Bitcoin cannot verify that proof directly, it is posted only as a commitment.

2. Post state to Bitcoin "optimistically."

The operator commits the new state root to Bitcoin via a standard Taproot output that contains only the root itself and a commitment of transaction data; no proof hash is embedded, and the transaction uses ordinary policy rules, so miners relay and confirm it like any other transfer.

3. Challenge & Dispute (BitVM 2)

After the root is posted, any watcher can challenge it. First, the operator is forced to reveal intermediate data of the ZKP verifier. BitVM 2 lets parties compare the output of locally executed sub-programs with the data revealed by the operator, pinpointing the exact segment that was executed incorrectly; no step-by-step bisection is needed. If no one challenges, the root finalises; if fraud is proven, the root is discarded and the operator's BTC collateral is slashed. The process is permissionless, low-cost, and secure with only one honest watcher.

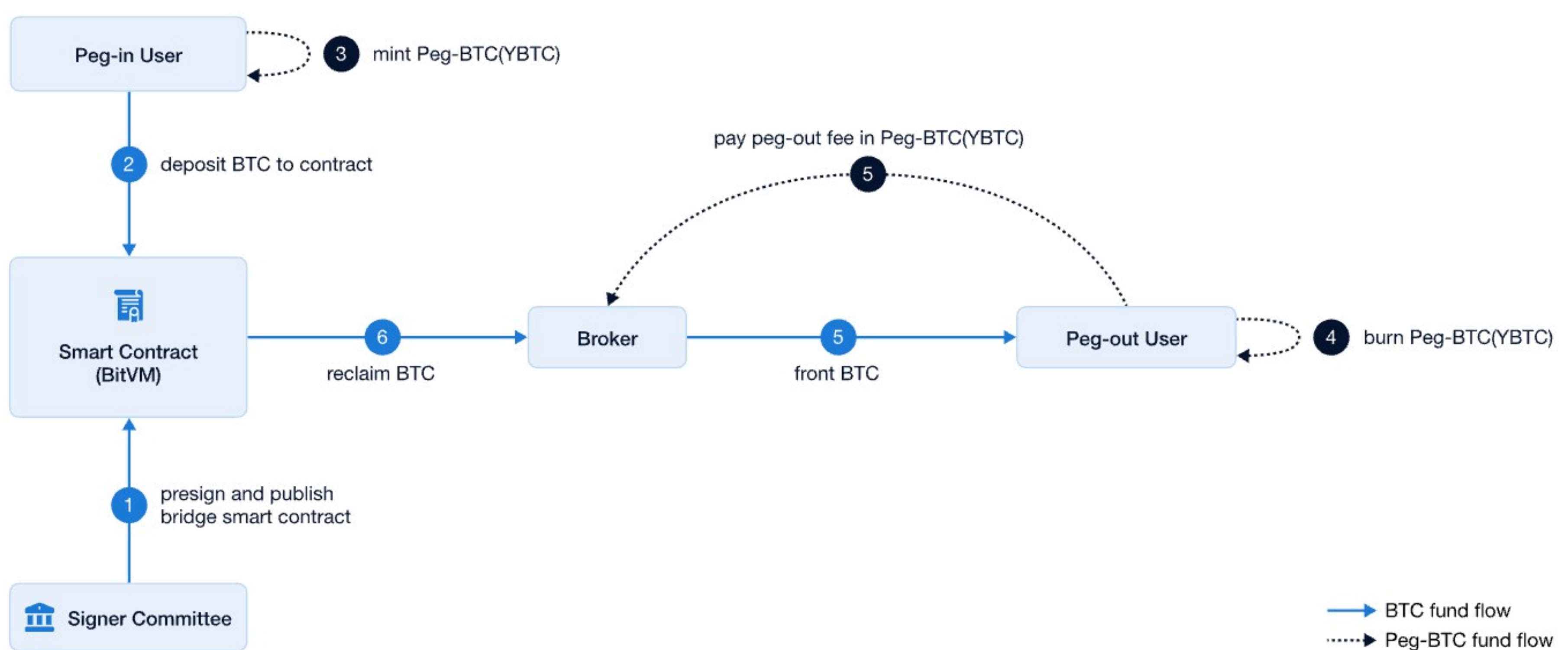
Key Security Assumptions

Requirement	Rationale
≥1 honest watcher	Any node can earn the slashed bond by proving fraud, so at least one will monitor.
Sufficient BTC collateral	Cheating costs the operator more than any potential gain.
Guaranteed data availability	Operators must publish all L2 data (on-chain or to an external DA layer); without it, watchers can force inclusion.
Miner inclusion of NSTS	Pool deals (>30% hashrate) ensure BitVM transactions propagate; more pools can be added if policy toughens.

With these safeguards, an attacker cannot alter state or steal funds without being caught. Watchers can always submit a forced transaction or use the bridge's escape-hatch path if an operator withholds data, while honest batches settle in a single step, keeping costs low and enabling truly scalable, trust-minimised smart contracts on Bitcoin.

BitVM Bridge Design (Peg-In/Peg-Out)

BitVM Bridge: Workflow



How the BitVM Bridge Works - High-Level Overview

Two-way peg in a nutshell

The BitVM Bridge locks BTC on Bitcoin L1 and mints a 1:1 YBTC token on Bitlayer L2; the process reverses when users burn YBTC to reclaim native BTC. BitVM fraud-proofs enforce all mint/burn events on Bitcoin, so bridge safety depends on code and one honest watcher, not on a trusted federation.

Peg-in (BTC → L2)

1. User signals a deposit and receives a pre-signed transaction bundle from the Bridge Committee.
2. After verifying the bundle, the user sends BTC to the bridge multisig.
3. Once the deposit appears on-chain, Bitlayer mints the same amount of YBTC to the user.
4. YBTC can be minted on rollup if the deposit is confirmed on Bitcoin. The mint itself, as part of the rollup STF, is confirmed along with the STF via the optimistic mechanism.

Peg-out (L2 → BTC)

1. User burns YBTC on L2.
2. A broker immediately pays the user the equivalent BTC from its own reserves on L1.
3. The broker broadcasts a **kick-off transaction** that carries only the public inputs for the zkVM program; the actual ZK proof is supplied in the subsequent BitVM dispute window, after which the broker can reclaim the locked BTC from the vault.
4. If the proof is invalid, any watcher can challenge via BitVM, slashing the broker's bond and protecting the funds.

Why it's safe and fast

One-honest-actor security – only a single truthful signer or watcher is required to foil theft, stronger than the majority-honest multisig bridges.

Unified roll-up + bridge proofs – the same BitVM mechanism guards both state roots and peg transactions, eliminating extra trust layers.

Instant user exits – brokers front liquidity, so users avoid long dispute windows. Brokers are repaid only after an on-chain proof succeeds, preventing fraud.

Native Bitcoin enforcement – Bitcoin Script ensures BTC leaves the vault only against a valid burn proof; miners already include the necessary non-standard TXs thanks to Bitlayer's pool partnerships.

In short, the BitVM Bridge offers a near-instant, trust-minimised path for BTC to enter and exit Bitlayer, combining optimistic roll-up security with a two-way peg – an architecture long thought impossible on Bitcoin without sacrificing trustlessness.

Roadmap & Future Outlook

Having established Bitlayer's current state, it's important to look ahead at how the project plans to evolve. The roadmap gives insight into upcoming technical milestones, partnership goals, and Bitlayer's vision for the future of Bitcoin-centric DeFi. The broader outlook considers how Bitlayer might shape the Bitcoin ecosystem in the years to come.

Roadmap Highlights

Bitlayer's Mainnet-V1, a Bitcoin Layer 2 built on the BitVM paradigm, went live in April 2024 following an extensive testnet and multiple security audits. By mid-2025, it had surpassed one year of operation and outpaced many peers in adoption and usage. As of June 2025, Bitlayer recorded over \$650 million in total value locked, peaking at \$850 million and ranking among the top three in the Bitcoin ecosystem. It also reported more than 3 million unique wallet addresses, over 65 million total transactions, and 60,000 to 80,000 daily active addresses. Annualized protocol revenue reached \$15 million in bitcoin, the highest in the BTC Layer 2 segment.

Mainnet V2 Launch (Q3 2025):

Bitlayer is gearing up for the release of **Bitlayer V2**, which transitions the network from its current sidechain architecture to the full BitVM-powered rollup model described in this report. According to the team, Mainnet V2 is slated for launch in **Q3 2025**. This will mark the official deployment of the recursive settlement protocol on Bitcoin and the enhanced BitVM Bridge on mainnet. The launch of V2 effectively realizes the "Bitcoin rollup" vision and could be heralded as a **major milestone in Bitcoin's evolution**, bringing it closer to the multi-chain world without a hard fork. A final V3 is set to be released sometime in 2026.

Bitlayer Timeline



Expanded Mining Support:

While Bitlayer already counts three major pools as partners (covering over one-third of hashrate), the team is not stopping there. Their contingency planning implies continuous efforts to **onboard more mining pools** to support BitVM transactions. The goal would be to reach a critical mass of hashrate (e.g., >50% or even > majority) such that BitVM transactions are reliably mined even if some pools or default nodes don't propagate them. This could involve more partnerships or possibly incentives for miners (like sharing some bridge fees or token incentives for miners who support the network). In the long run, if Bitlayer's transaction volume grows, the natural fee market could entice more miners without direct deals. But in the interim, proactive collaboration is likely.

Cross-Chain Interoperability (CCIP & More Integrations):

Bitlayer is positioning itself as a hub for Bitcoin liquidity across chains. The roadmap includes integrating more networks using the **Cross-Chain Interoperability Protocol (CCIP)**. CCIP (a standard spearheaded by Chainlink) would allow Bitlayer to connect to various blockchains in a standardized way, potentially automating YBTC movement or enabling generalized messaging. For example, CCIP could let smart contracts on Ethereum request BTC from Bitlayer or trigger peg-out in a secure manner. This suggests Bitlayer foresees a more *automated and seamless bridging experience* in the future, possibly abstracting away Bitlayer's presence so that users on other chains can use BTC without manual steps.

Scaling Enhancements:

Bitlayer's whitepaper hints at advanced cryptographic upgrades, like exploring **next-generation STARKs (BF-STARK)** contingent on future Bitcoin upgrades. While speculative, if Bitcoin were to implement certain opcodes or covenants that make verification easier, Bitlayer could upgrade its proof system to be faster or more efficient (e.g., moving from Groth16 proofs to STARK proofs, if the verification becomes feasible on-chain). The team is likely keeping an eye on Bitcoin protocol developments that could either aid or compete with them. The roadmap might not list these as concrete items since they depend on external factors, but Bitlayer is architected to adapt to a changing Bitcoin.

Conclusion

Bitlayer has advanced from concept to a live, revenue-backed Layer-2 that combines Bitcoin-equivalent security with EVM-level programmability, something no earlier side-chain or payment-channel solution has achieved. With a **\$25million funding base** and a consortium of blue-chip investors already published on the Series A cap-table slide, the project has both capital longevity and market validation.

Technically, Bitlayer's roadmap now hinges on three pillars:

1. BitVM-secured roll-up – Soft finality in sub-second and hard finality after the **seven-day optimistic** window keeps the user experience fast while mapping every state root back to Bitcoin's PoW consensus.

2. Trust-minimized BTC bridge – The 1-of-n fraud-proof model eliminates multisig custodial risk and is already forging integrations with Base, Arbitrum, Starknet and other high-liquidity chains.

3. Performance uplift – The V2/V3 roadmap targets sub-second soft confirmations and **20k TPS**, a throughput class that will make BTC-denominated DeFi economically viable for market-making, derivatives and high-frequency use-cases.

In parallel, community traction is accelerating: TVL has already broken industry benchmarks, ecosystem partnerships span centralized and decentralized liquidity venues, and the BitVM Alliance is driving open-source contributions upstream. These external network effects amplify the purely technical moat of Bitlayer's dual-finality roll-up.

If the team continues executing, Bitlayer will not merely scale Bitcoin; it will re-position BTC as the base collateral for a cross-chain, yield-driven financial system. That would close the current gap between Bitcoin's approximately \$2.3 trillion of dormant capital and the programmable liquidity that Ethereum enjoys, delivering precisely the upside outlined at the start of this report.

Disclaimer:

This report was commissioned by Bitlayer. This research report is exactly that — a research report. It is not intended to serve as financial advice, nor should you blindly assume that any of the information is accurate without confirming through your own research. Bitcoin, cryptocurrencies, and other digital assets are incredibly risky and nothing in this report should be considered an endorsement to buy or sell any asset. Never invest more than you are willing to lose and understand the risk that you are taking. Do your own research. All information in this report is for educational purposes only and should not be the basis for any investment decisions that you make.

“

Our mission is to bridge traditional finance into digital assets through our crypto native research.