



Bitcoin Staking:

A complete guide for
institutions in 2025

Introduction

Bitcoin is the most established crypto asset in the world, yet much of the BTC supply remains idle, sitting in cold storage. Permissionless Bitcoin staking is a new primitive that has opened the door for institutional investors to earn a yield on their idle BTC.

The 2024 Staking Summit in Bangkok (Nov 8-9) united over 1,000 staking experts from across the globe to discuss the future of Bitcoin staking. This report distills the top Bitcoin staking opportunities for institutional investors, featuring insights from leading investors, protocols, and legal experts at this year's event.

About Staking Rewards

[Staking Rewards](#) is the leading crypto staking platform, empowering 3 million individuals and enterprises to stake since 2018. We offer unbiased real-time staking market data and tools for both private and institutional investors. Major companies like Coinbase, Kraken, Grayscale, and 21Shares utilize our Staking Data API to power their staking and investment products.

Chapter 1:

What is Bitcoin staking?



What is Bitcoin Staking?

Bitcoin staking represents a novel approach to utilizing Bitcoin within the Proof-of-Stake ecosystem, primarily facilitated by Babylon's innovative protocol. Their mechanism creates a two-sided marketplace where Bitcoin holders can securely lock their assets while earning yields by staking on various PoS chains. On one side of this marketplace are the PoS chains that require additional security and are willing to compensate Bitcoin holders for their contributions. On the other side are the Bitcoin holders, who seek to earn yields on their idle assets. The Babylon protocol ensures that both parties benefit.

The Babylon protocol uses advanced cryptography and smart contracts to lock Bitcoin securely in self-custodian vaults, eliminating the need to bridge to PoS chains and reducing risks. It also includes slashing mechanisms to penalize malicious activity. To learn more about Babylon, watch our [interview](#) with Fisher Yu, the Co-Founder of BabylonChain.

Babylon's implementation of Bitcoin timestamping further strengthens the staking process by synchronizing PoS chains with the Bitcoin blockchain, providing an additional layer of security and order. This synchronization allows for rapid unbonding processes and ensures that transactions are validated effectively.

- **Staking Contract Initiation:** A BTC holder begins by entering a staking contract and locking assets in a self-custodian vault through a transaction on the Bitcoin blockchain.
- **Locking Mechanism:** The locked Bitcoin can only be accessed using the staker's private key.
- **Validation Participation:** The staker chooses which PoS chains to stake to and starts validating by signing blocks using his key.
- **Reward Mechanism:** The staker earns rewards from the PoS chain while his BTC remains secured on the Bitcoin blockchain.
- **Unbonding Process:** The unbonding period takes roughly 7 days (or exactly 1008 Bitcoin blocks as defined by the unbonding script).
- **Slashing:** The delegated finality provider performs double-signing during staking or unbonding, then a proportional amount of the staking will be burned.
- **Phased Launch:** Babylon's staking protocol is being rolled out in phases, with initial capabilities focusing on locking Bitcoin and preparing for future integrations with PoS consensus mechanisms.

Chapter 2:

The growth of Bitcoin Staking



The Growth of Bitcoin Staking

Bitcoin staking via the Babylon protocol has seen tremendous growth in a record time. The Babylon protocol went live with a 1,000 BTC cap on Aug 22, reaching capacity in under an hour. Cap 2 was duration-based (10 BTC blocks) and saw an inflow of 24,308 BTC staked (valued at \$2.1B).

Babylon launched the third cap on Dec 10, with a raised deposit limit of 5000 BTC and a longer duration to stake. Cap 3 will last for 1,000 Bitcoin blocks. The latest phase almost doubled in value previously staked BTC with the TVL reaching \$3.8 Billion.

Bitcoin Staking Phases

Babylon Bitcoin Staking is rolling out in three main phases, each aimed at gradually connecting Bitcoin holders with the security requirements of Proof-of-Stake networks.

Phase 1: Bitcoin Locking

The first two caps were staked on a first-come, first-served basis, and both caps were filled in a matter of hours. Although no direct staking rewards are distributed during this phase, a point system tracks stakers' activities, allocating Babylon Points proportionally among active stakes.

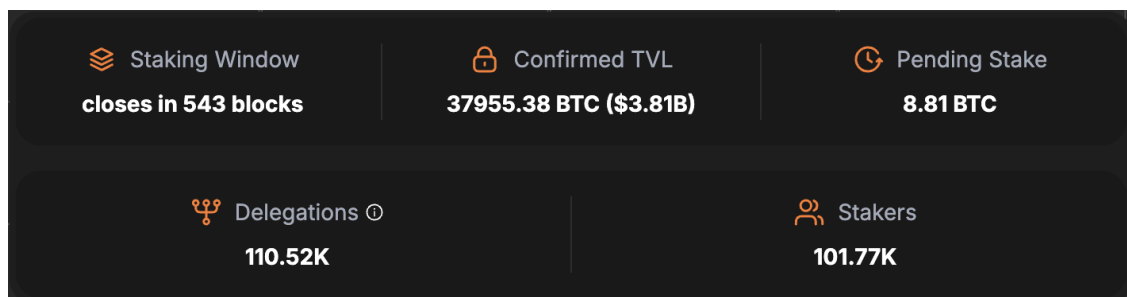
Phase 2: Bitcoin Staking Activation

TBD, this phase marks the launch of the Babylon chain, enabling delegated Bitcoin to contribute to the chain's consensus and security through finality providers.












Phase 3: Bitcoin Multi-Staking Activation

TBD, the final phase will facilitate the evolution of the protocol into a shared security marketplace, allowing Bitcoin holders to stake the same BTC across multiple PoS systems simultaneously.

Bitcoin Staking Metrics



(Source: [Babylon](#))

1	 Lombard	Copy address  609b...9806	Staked Tokens 14.95k BTC 108.65%	Fee 3%	Points per 1BTC per day ☹️ 76.9123
2	 Solv Protocol	Copy address  fa74...8bfb	Staked Tokens 6.68k BTC 11.18%	Fee 5%	Points per 1BTC per day ☹️ 75.3265
3	 RockX	Copy address  bb0b...fdd1	Staked Tokens 1.22k BTC 20.04%	Fee 3%	Points per 1BTC per day ☹️ 76.9123
4	 PumpBTC	Copy address  0f5c...85e4	Staked Tokens 3.59k BTC 72.7%	Fee 5%	Points per 1BTC per day ☹️ 75.3265
 5	 HashKey Cloud	Copy address  3a39...9ad4	Staked Tokens 172.33 BTC 48.84%	Fee 3%	Points per 1BTC per day ☹️ 76.9123

(Source: [Staking Rewards](#))

Chapter 3:

Different ways to stake Bitcoin via Babylon



Different Ways to Stake Bitcoin via Babylon

Bitcoin staking represents an innovative advancement in cryptocurrency, currently undergoing testing and refinement. This emerging concept has delineated two primary staking types: custodial and non-custodial.

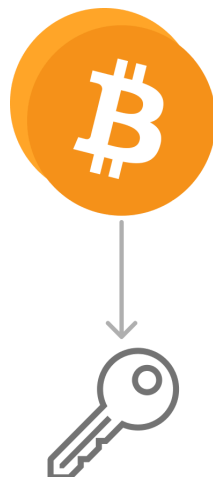
Non-Custodial Staking

Non-custodial staking empowers Bitcoin holders to retain full control over their assets. By utilizing self-custodial solutions, participants can stake their Bitcoin without relinquishing ownership or access to their private keys.

Non-custodial BTC staking is accomplished directly through Babylon by depositing assets into a self-custodian vault. Bitcoin holders can also utilize third-party applications, including the Staking Rewards Stake App, without transferring ownership of their assets. Users can stake with various wallets and choose the most suitable option. Babylon will support Ledger to answer the community's demands for cold wallet staking.

- **Full Control Over Assets:** Users retain complete ownership of their private keys and funds, reducing the risk of loss due to hacks or mismanagement (when maintaining appropriate precautions).
- **Transparency and Trustlessness:** Non-custodial staking operates on decentralized protocols governed by mostly open-source code. This transparency allows users to verify and audit the mechanisms behind staking processes.
- **Flexibility and Liquidity:** Users can withdraw or transfer their staked assets at any time, subject to protocol conditions.
- **Encouragement of Innovation:** The decentralized nature of non-custodial staking promotes the development of new financial products and services within the DeFi ecosystem.

Non-custodial staking involves technical complexity, requiring users to understand wallet management and blockchain protocols. Security is the user's responsibility, risking permanent asset loss if private keys are lost. Support is often limited compared to custodial services, and liquidity may be constrained due to locked assets.



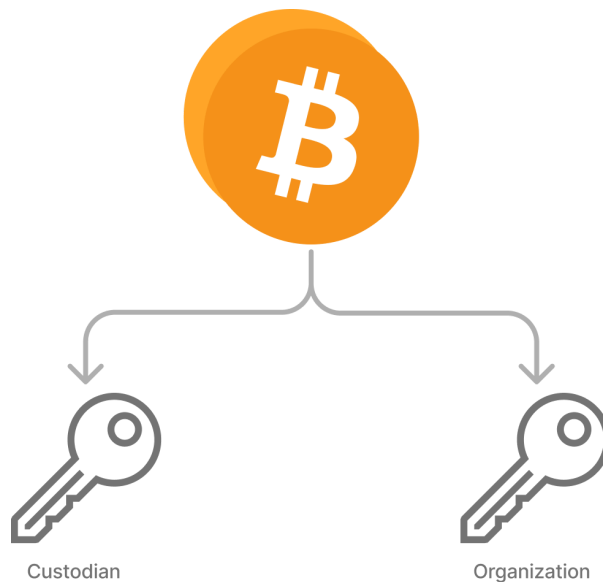
Single Private Key

Organization-Managed Custody

As Bitcoin evolves, staking strategies are emerging as a way for organizations to improve security, increase transparency, and maximize yield potential from their BTC holdings. In collaboration with custodians, institutions can maintain control over their funds or assets on behalf of users, with secure access facilitated through Multi-Party Computation (MPC) wallets. In this model:

- Key Distribution: The organization holds one key share and a trusted custodial partner holds the second one.
- Enhanced Security: No single party has access to the full private key.
- Redundancy: Even if one party's key share is compromised, the funds remain secure.
- Flexibility: Configurations can be customized to suit organizational requirements.

An Organization-Managed Custody enables institutions to securely manage and transact Bitcoin through a decentralized security model, like a 2-2 signature scheme. Transactions can only be authorized when both parties cooperate, enhancing security against internal or external threats.

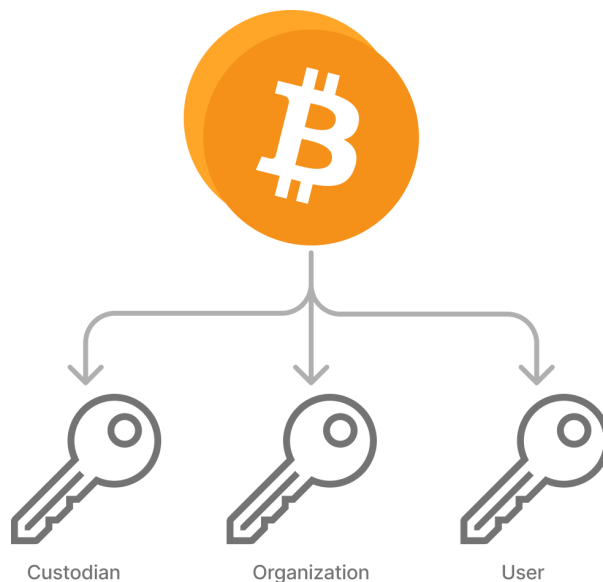


Co-managed Custody

Co-managed custody combines the security of organization-controlled wallets with the autonomy of user-controlled wallets, making it a robust solution for Bitcoin staking. This model leverages MPC wallets with customizable threshold signature schemes to distribute key shares among the organization, end users, and a trusted custodial partner. Configurations like 3-3, 2-3, or 2-2 enable tailored control, ranging from maximum security (all parties must sign) to greater flexibility (only some parties need to sign).

- **MPC Wallet Security:** Uses distributed key shares to enhance security and mitigate risks, with no single entity holding full control of the private key.
- **Threshold Signature Configurations:** Depending on the scheme the security is distributed among several parties, requiring signatures from the organization, end user, and custodial partner.
- **User Autonomy with Organizational Oversight:** Empowers end users to control their assets while allowing the organization to intervene in emergencies or disputes.
- **Customizable and Compliant:** Tailored custody setups meet both user needs and regulatory requirements, making it scalable for institutional and individual use cases.

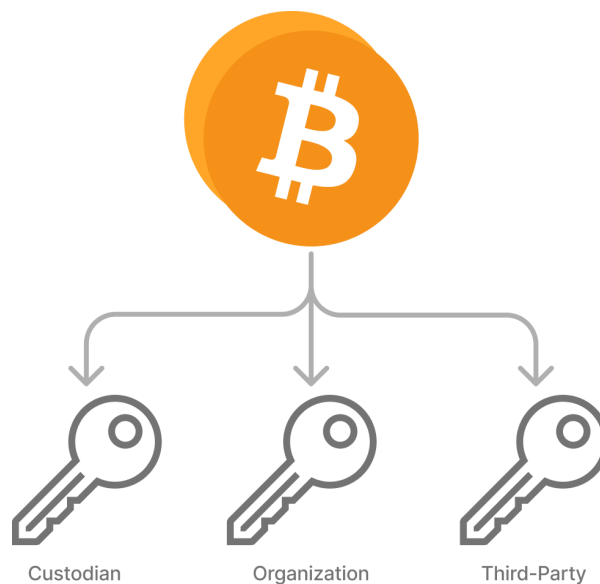
This approach balances user empowerment with organizational oversight, providing resilience against risks like key compromise or insider threats. By integrating co-managed custody and non-custodial MPC wallets into applications, organizations can offer secure, customizable, and compliant staking solutions that cater to both institutional needs and user preferences.



Third-party Custodial Staking

Custodial Staking offers a convenient approach, allowing participants to delegate their Bitcoin holdings to third-party services that manage the staking process on their behalf. This method often utilizes Multi-Party Computation (MPC) wallets. Custodial staking solutions include enhanced safety measures, dashboards for reporting and monitoring, custom support, compliance with regulatory standards, insurance coverage, and user permissions management, thereby minimizing human error and facilitating instant settlement and rebalancing. [Anchorage](#), [ChainUp Custody](#), [Fordefi](#), [Cobo](#), and [Hex Trust](#) have integrated the Babylon protocol to enable secure custodial Bitcoin staking for individuals and institutions.

- **MPC Wallets:** Fordefi, ChainUp, and Cobo leverage MPC wallet technology, enhancing security for custodial Bitcoin staking by distributing signing authority across multiple parties.
- **Policy-Driven Transaction Security:** Fordefi's policy engine allows institutional clients to customize transaction rules and workflows, providing compliance and risk management for staking operations like deposits, withdrawals, and early unbonding.
- **User-Friendly Integration:** Cobo's Babylon staking API allows asset managers and providers to integrate BTC staking into their services. ChainUp Custody offers an API for institutional clients and professional investors, enabling automated staking.
- **Institutional-Grade Custody:** Anchorage, ChainUp, and Hex Trust integrate Babylon's staking into its custody services, enabling regulated, air-gapped, and insured staking solutions.
- **High Demand and Adoption:** The launch of Babylon's mainnet attracted substantial interest, with around \$4 billion in BTC staked, highlighting strong demand for secure and regulated BTC staking solutions.



Chapter 4:

Bitcoin staking market outlook



Bitcoin Staking Market Outlook

Supply

Bitcoin staking affects supply dynamics by removing coins from circulation within its 21 million cap. About 0.12% of Bitcoin is staked, with various liquid staking protocols available, showing a growing interest in yield opportunities. As staking expands, Bitcoin may increasingly serve as a security asset across blockchains and possibly in traditional finance through Asset-Backed Securities (ABS), broadening its role beyond a store of value.

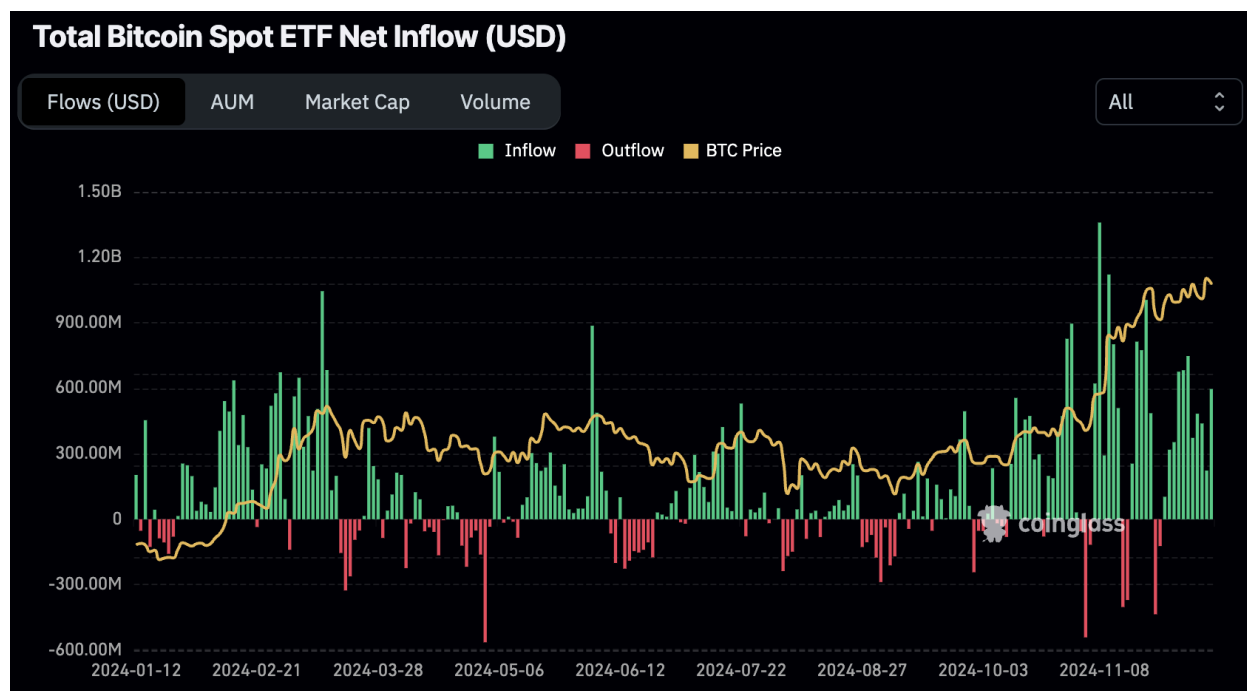
ETFs

Bitcoin exchange-traded funds (ETFs) have gained significant traction in the financial markets, particularly following the launch of the first U.S. Bitcoin-linked futures ETF, the ProShares Bitcoin Strategy ETF, on October 19, 2021. The wave of spot Bitcoin ETFs debuted in January 2024, including products from major firms such as BlackRock, Fidelity, and ARK Invest, quickly attracting substantial investments.

The current outlook for Bitcoin ETFs remains optimistic, as they are expected to facilitate greater institutional and retail participation, potentially driving significant inflows and further legitimizing Bitcoin as an asset class. In the future, we expect ETFs that provide yield similar to funds that include dividends. BTC and ETH accumulated in ETFs could be used in native staking or yield-generating protocols.

ETPs

Several ETPs currently offer staked products, although these are not yet available in the United States. These products have gained regulatory approval from European authorities, paving the way for BTC staking in traditional markets. Among the largest issuers is Coinshares, whose ETHW product boasts a market capitalization exceeding \$300 million and is actively traded on the SIXT exchange in Switzerland.



(Source: [Coinglass](#))

Pro-crypto Narrative

The pro-crypto narrative in the United States and globally has gained significant momentum, particularly following the recent US elections. Bitcoin's November performance has been an indicator of that. It is not a mystery that Trump is pro-crypto, positioning himself as a strong advocate for cryptocurrencies, and has pledged to establish the U.S. as the "crypto capital of the world." In addition, most of the House of Representatives and Senate are crypto-friendly, according to [Stand with Crypto](#), which can reduce regulatory burdens and foster innovation in the crypto space.

Globally, this pro-crypto sentiment is mirrored in various jurisdictions adopting more favorable regulatory frameworks to attract blockchain and cryptocurrency businesses. Countries like Switzerland and Singapore have long been recognized for their supportive environments, driven by increasing institutional interest, substantial political backing, and a growing recognition of cryptocurrencies as a viable asset class.

The United States is poised for significant legislative and regulatory changes concerning the blockchain and cryptocurrency sectors. In the upcoming year, we anticipate that staking and DeFi initiatives will be introduced, which will likely attract a substantial influx of new users and investors. Presently, many leading staking and DeFi platforms, including Babylon, restrict participation from U.S. jurisdictions. However, once these constraints are lifted, we can expect unprecedented levels of interest, trading volumes, and wallet creation within the market.

Chapter 5:

Bitcoin Staking Regulation



Bitcoin Staking Regulation

Now is the optimal time to engage with staking. With new regulations taking shape, staking associations worldwide are being actively included in key discussions. Compliance frameworks are evolving within the blockchain industry, reflecting a significant shift in market dynamics.

Non-Custodial vs. Custodial Staking

Non-custodial staking remains largely unregulated in most jurisdictions since it doesn't involve third-party control over assets. For example, Switzerland initially considered regulating non-custodial staking under banking rules, which "would've impacted us significantly," noted Brian Fabian Crain - Co-Founder & CEO of Chorus One, but the decision was later reversed based on industry feedback.

Staking services offered by regulated exchanges, such as Coinbase, have attracted regulatory scrutiny, especially from the U.S. SEC. Lewis Han from Coinbase explained, "While non-custodial staking isn't a focus for regulators, staking through exchanges, like Coinbase, has drawn attention." Coinbase has faced challenges over allegations of unregistered securities dealings, highlighting the need for regulatory clarity to guide custodial staking operations.

Tax, KYC, and AML

Regulations are extending beyond securities to include tax compliance, KYC, and AML requirements. Eric Hill from Lido emphasized, "These decisions are being made now, so stakeholders must get involved." Tal Zakon, CEO of Tres Finance, elaborated on how these rules can complicate tax obligations, stating, "In some jurisdictions, claimable rewards must be declared as income, which can complicate tax reporting."

KYC / AML Considerations for Bitcoin Staking

Native staking is the most secure approach, allowing users to retain full control over their Bitcoin in a self-custodial vault. Although, during withdrawals or slashing events, stakers won't receive the assets exactly from the UTXO they deposited with, they will receive the same amount of Unspent Transaction Output they originally deposited minus transaction fees paid to miners during withdrawal or unbonding.

Lombard offers an asset separation solution for institutions needing specific flow-of-fund arrangements to meet compliance requirements.

In contrast, purchasing Bitcoin Liquid Staking Tokens on the open market introduces risks associated with mingling funds, complicating compliance with KYC and AML regulations. To mitigate these risks, it is advisable to engage only in the direct minting of LBTC rather than acquiring it from third-party sources. Institutions involved in Bitcoin staking should implement robust KYC/AML compliance frameworks, including customer due diligence, ongoing transaction monitoring, staff training, and thorough documentation.

Regulatory Challenges

The Markets in Crypto Assets (MiCA) regulation in Europe and the Virtual Asset Regulatory (VAR) frameworks are setting global standards. Tal Zakon highlighted Tres Finance's API, which provides accurate staking data to help institutional clients meet compliance needs. Europe leads the U.S. in adopting frameworks for products like staking-enabled ETPs, which remain unavailable in the U.S. due to regulatory uncertainty. Lewis Han stressed the need for clear U.S. rules on staking rewards and taxes, while Eric noted the influence of global organizations like the OECD and FATF in shaping national crypto policies.

ESMA recently proposed extending regulatory oversight to validators, a departure from MiCA's original scope. Daniel Schrader of Finoa expressed concerns, noting that validators operate differently from brokers or investment firms. In Switzerland, advocacy by industry leaders like Bitcoin Suisse led FINMA to revise its stance on staking. Initially requiring a banking license for custodial staking, FINMA's updated December guidelines now allow it without such restrictions, preserving the business case for staking.

Compliance Standards

For non-regulated entities working with regulated clients, compliance often depends more on customer requirements than direct regulation. Anticipating future regulations, Brian Fabian Crain noted that, although his company is not directly regulated, they pursue certifications like ISO 27001, while Tal Zakon added that Tres Finance has built solutions specifically for staking providers, "to support institutional clients with accurate data."

Active Engagement with Regulators

Eric Hill noted that the next two years are critical for engaging with regulators, as rules are being formulated. Coinbase has taken a proactive approach to working with U.S. regulators, aiming to clarify guidelines for crypto operations and resist the SEC's broad interpretation of securities law. "We're actively engaging with policymakers, such as through initiatives like Stand with Crypto, to push for clearer rules," Lewis Han shared.

Potential Shifts in U.S. Regulatory Landscape

An impending shift in U.S. administration could foster a more crypto-friendly regulatory environment. If a pro-crypto cabinet takes office, the SEC may see leadership changes that encourage clearer boundaries between its role and that of the CFTC. Lewis Han stated, "Historically, the SEC chair steps down before the inauguration, so we might see Gensler leave." While a more crypto-welcoming administration could reduce hostility, Eric Hill cautioned that it won't be a quick fix. Changing leadership affects enforcement style but doesn't alter existing laws.

Jurisdiction Summary

US

- U.S. regulators, especially the SEC, enforce staking rules mainly through action rather than clear guidelines.
- The latest U.S. election may bring a crypto-friendly administration, possibly leading to a more supportive SEC stance and promoting U.S. leadership in crypto standards.
- Institutions are proactively adopting compliance measures, using certifications and innovative tech to navigate regulatory uncertainty and meet client needs.

EU

- The MiCA framework will unify EU rules for custodians, token issuers, and exchanges, with potential expansion to include validators, impacting institutional staking.
- ESMA views MEV as a possible market abuse risk, but solutions like PBS may reduce validators' liability, addressing concerns for institutional clients.
- Industry leaders urge institutions to engage with EU regulators to clarify validators' roles, supporting balanced, sustainable growth in crypto services.

CH

- FINMA requires custodial staking providers to implement robust risk mitigation measures, including clear client risk disclosures and pre-signed exit transactions, ensuring greater security and transparency.
- Bitcoin Suisse, SEBA, and others, supported by the Swiss Blockchain Federation, pushed back through legal analysis and public engagement to clarify staking's regulatory status.
- In December, FINMA allowed custodial staking without a banking license if providers meet risk, authorization, and continuity requirements, making Switzerland a favorable jurisdiction for institutional staking.

Chapter 6:

Taxation



Taxation

The taxation policy for cryptocurrency staking varies widely depending on the country you reside in, as different jurisdictions have distinct tax laws regarding digital assets. Generally, staking rewards are considered taxable income at the time they are received, but the specifics can differ based on several factors.

For Bitcoin, native Babylon BTC staking does not trigger a taxable event. In contrast, utilizing LSTs or other wrapped BTC solutions can be classified as a taxable event due to the underlying sale of BTC involved. Similarly, unwrapping WBTC is treated as a BTC purchase, which carries tax implications. As a result, native staking provides a more tax-efficient alternative.

Income Classification

- **Ordinary Income:** In many countries, staking rewards are treated as ordinary income and taxed according to your income tax bracket.
- **Capital Gains:** Some jurisdictions may consider the appreciation of staked assets as capital gains, taxable upon disposal of the assets.
- **Business Income:** If staking is part of a business operation, the rewards might be taxed differently, possibly allowing for expense deductions.

Taxation Timing

- **Upon Receipt:** Tax authorities may require you to report staking rewards as income when you gain control over them.
- **Upon Disposal:** In some cases, taxes are due only when you sell or exchange the staking rewards for fiat currency or other assets.

Valuation Methods

- Accurate record-keeping of the fair market value of staking rewards at the time of receipt is crucial for tax calculations.
- The method used to determine the value (e.g., specific exchange rates) can affect the taxable amount.

Staking Method

- **Direct Staking vs. Staking Pools:** Participating in staking pools or using third-party services might have different tax implications compared to staking directly.

Taxation Examples in Different Countries

US

- The IRS treats staking rewards as taxable income upon receipt, valued at fair market value.
- Selling or exchanging staking rewards incurs capital gains tax based on the difference between the sale price and initial value at receipt.

EU

- Since the EU does not have a unified tax policy, the treatment of staking rewards varies by member state.
- Income Tax or Capital Gains Tax: In some EU countries, staking rewards may be subject to income tax, while in others they might be treated as capital gains. For example:
 - Germany: Staking rewards are generally treated as income, subject to income tax rates.
 - France: Rewards can be subject to both income tax and capital gains tax, depending on the holding period and the nature of the activity.

CH

- Staking rewards are considered taxable income if the staking activity is part of a business or self-employment. For private investors, rewards are not subject to income tax but are included in wealth tax calculations.
- Cryptocurrencies, including staking rewards, are subject to wealth tax. The value of the crypto assets is declared in the annual tax return, and wealth tax is levied based on the total value of the assets.

Taxation Summary

- Jurisdictional tax laws and local regulations define how staking is classified (income vs. capital gains) and taxed.
- Individual vs. business activity determines whether you stake as a personal investment or as part of a business can influence tax treatment.
- The nature of the asset and the staking method may have varied tax implications based on their characteristics and use cases.
- Accurate record-keeping of staking activities, including dates, values, and amounts, is important for compliance. Given the complex and evolving regulations, consulting a tax professional is highly recommended.

Given the complexity and evolving nature of cryptocurrency tax laws, institutional clients are advised to consult a tax professional well-versed in digital assets, stay updated on regulatory changes, and maintain thorough records of all transactions. This information is general guidance and not a substitute for tailored tax or legal advice. The presence or absence of clear guidelines from tax authorities in your country can impact how staking is taxed and reported.

Chapter 7:

Bitcoin Liquid Staking Opportunities



Bitcoin Liquid Staking Opportunities

The concept of tokenized Bitcoin, such as LBTC, represents a significant development in making Bitcoin more versatile and usable within DeFi and application layers. The idea was quickly implemented on a big scale after Babylon introduced native staking, which locks BTC in a self-custodian vault.

Luke Xie of SatLayer highlighted how integrating Bitcoin with staking and restaking functions can connect it to the broader crypto ecosystem, adding practical utility. The focus on LSTs reflects the industry's movement to bridge Bitcoin with decentralized applications, enhancing Bitcoin's role beyond a store of value.

Lombard

Lombard is a liquid staking protocol built on the Babylon platform, offering LBTC as its primary liquid staking token. LBTC represents a user's staked BTC with Babylon, enabling participation in DeFi activities while preserving Bitcoin's fundamental characteristics, such as value and security—similar to how Lido's stETH functions on Ethereum. For more insights into Lombard, explore our [research article](#).

Lombard's Security Consortium is designed to be a decentralized framework for enabling Bitcoin staking and liquid staking operations in conjunction with the underlying Lombard protocol. At its core, the Consortium is a dispersed, multi-signature system that oversees staking, unstaking, and asset bridging on the Lombard protocol through a state machine governed by a consensus mechanism. The Consortium operates as a proof-of-authority network, with each member maintaining its own infrastructure, ensuring decentralization and independence.

How the Lombard Consortium Works

- When a deposit is initiated, the Consortium validates a deterministic BTC address managed securely by CubeSigner, a trusted cryptographic tool.
- The Consortium verifies deposit transactions on the Bitcoin blockchain, including transaction existence, BTC amount, confirmations, and address accuracy.
- Members select and stake BTC to designated finality providers, with the Consortium overseeing logic for rewards collection and distribution.
- The Consortium operates by standard consensus rules, requiring $\frac{2}{3}$ of members to sign off on operations, distributing keys to eliminate single points of failure and ensure secure data notarization.
- New Consortium members must receive approval, deploy the necessary infrastructure, exchange public keys with current members, and be registered within CubeSigner for notarizations.

Lombard Benefits and Returns

- Identical Babylon points to direct staking.
- Yield from Babylon secured networks in native tokens - expected from Babylon Staking Phase 2.
- Lombard LUX through the [Luminary Program](#).
- Opportunity to earn yield from DeFi protocols, like Pendle, Morpho, Gearbox, Veda, etc.

Lombard's Security Consortium - Potential Risks and Concerns

- **Coordination and Consensus Risk:** While the Consortium's reliance on consensus among independent members could pose risks if coordination fails, Lombard's system mitigates these risks through automation and cryptographic guarantees. The consensus process, managed by software, ensures that multiple independent parties validate critical operations.
- **Centralization Risk:** Lombard is designed with a decentralized consortium of multiple independent and reputable parties; however, the Lombard team retains some influence during the early stages of the network. This temporary centralization could raise concerns about decision-making, but practical safeguards limit the potential for misuse. The consortium's structure prevents any single entity, including the Lombard team, from acting unilaterally, as actions require consensus among independent members.
- **Security Vulnerabilities:** The diversity of infrastructure introduced by new Consortium members enhances the system's resilience against disruptions but also increases the protocol's complexity. This higher complexity expands the surface area for potential bugs or security vulnerabilities, particularly as the system scales and incorporates new members. However, the decentralized nature of the consortium means that the failure of a single node or member does not jeopardize the entire system.
- **Technical Dependencies:** The Consortium's reliance on CubeSigner introduces dependencies on these technologies. Any vulnerabilities in these systems could impact the overall security and reliability of the Consortium.

It is worth acknowledging that Lombard plans to launch a public blockchain for the decentralized bookkeeping of the Consortium. The public ledger would reduce anxieties regarding centralization risks.

Lombard's BTC LST approach prioritizes decentralization, robustness, and transparency by leveraging a consortium of geographically distributed, independent parties with strong reputations. It supports scaling key holders to over 20 entities, eliminating single points of failure. Withdrawals and third-party proof-of-reserve verification have been enabled from day one, ensuring user confidence and operational resilience. Lombard's multi-layered framework aims to provide a reliable and scalable BTC LST solution, though its complexity introduces operational challenges that require ongoing management.

Solv Protocol

Solv Protocol is a platform designed to integrate Bitcoin into the DeFi ecosystem, leveraging several innovative approaches to unlock the potential of idle Bitcoin assets. The platform utilizes its unique Staking Abstraction Layer (SAL) to maximize Bitcoin's potential.

SolvBTC.BBN is a liquid staking token for Bitcoin, representing staked BTC in the Babylon protocol. It enables Bitcoin holders to earn staking rewards while contributing to Bitcoin's economic security on PoS chains while retaining the flexibility to engage in DeFi. Designed in anticipation of Babylon's staking rewards launch, SolvBTC.BBN positions itself as one of the tokens to offer Bitcoin-staking yields once Babylon rewards go live. To acquire SolvBTC.BBN users need to deposit SolvBTC.

How Solv Bitcoin Staking Works

- Users can deposit BTC or wrapped Bitcoin into Solv Protocol, with all transactions immutably recorded on-chain to ensure full transparency and traceability. Solv partners with custodians like Ceffu and Cobo to ensure secure asset storage.
- Self-custody is not permitted. For certain larger users and institutions, assets can be held by custodians of their choice. However, access and withdrawal rights remain strictly controlled by Solv, ensuring that assets cannot be withdrawn without Solv's explicit authorization.
- Depositors receive SolvBTC at a 1:1 ratio with their staked BTC, providing access to DeFi opportunities and SolvBTC.BBN.
- SolvBTC.BBN enables institutions and individuals to earn returns by leveraging integrated yield strategies, including Babylon staking and other yield-optimizing mechanisms tailored for sustainable growth.




Solv Benefits and Returns

- Earn additional rewards by restaking Bitcoin into integrated DeFi ecosystems and Proof-of-Stake networks via SolvBTC.BBN.
- Benefit from advanced trading mechanisms, including basis-trading and arbitrage strategies.
- Yield in native tokens from Babylon-secured networks - anticipated in Babylon Staking Phase 2.
- Earn Solv points reward for depositing assets into the protocol and utilizing DeFi options.

Solv Protocol - Potential Risks and Concerns

- **Custodial Risks:** Solv Protocol ensures that solvBTC is consistently backed 1:1 by Bitcoin, with no exceptions for institutions or individuals. While institutional clients may choose third-party custodians for BTC storage, Solv retains strict control over access and withdrawal rights. However, reliance on third-party custodians introduces an additional layer of operational dependency, which could present risks in cases of custodian failure or mismanagement. Although these risks are managed, they are inherent to any third-party custody model and warrant ongoing oversight.
- **Key Management:** The keys to BTC are jointly managed by Solv, trusted custodians, and in some cases, independent third parties. While this diversified approach reduces the risk of a single point of failure, it introduces dependencies on the security and reliability of multiple custodians. Additionally, accommodating specific client preferences could add complexity to the overall custody structure.
- **SolvBTC.BBN Redemptions:** Solv currently has redemptions for solvBTC.BBN paused. The interim solution involves swapping assets on decentralized exchanges.
- **Wrapped BTC Stability:** SolvBTC's value is linked to the stability of wrapped BTC assets (e.g., WBTC, FBTC). Market volatility or depegging events could pose risks to its value. To mitigate this, Solv implements a tiered reserve strategy, diversifying across multiple trusted wrapped BTC issuers to reduce concentration risk and enhance stability.
- **Smart Contract Risks:** As a decentralized protocol, Solv operates through smart contracts, which inherently carry potential risks of vulnerabilities or exploits. To address these concerns, Solv employs rigorous security measures, including regular audits, incentivized bug bounty programs, and a modular architecture designed to enhance resilience and adaptability.

Bitcoin Derivatives Comparison

	 WBTC BTC Pegged	 FBTC BTC Pegged	 LBTC BTC LST's	 solvBTC.BBN BTC LST's
Custody/Risk	Multi-Jurisdictional Custody	MPC Custody	Lombard Consortium	MPC Custody
Yield	No Native Yield	No Native Yield	Native Babylon Yield + Lux	Native Babylon Yield + XP
DeFi Options	Multiple	Multiple	Multiple	Multiple

The table below highlights the differences between native staking on Babylon and yield-generating liquid staking solutions.

	Native Staking (Babylon)	Liquid Staking (LSTs)
Fees	None	Fees apply on Babylon staking yield
Liquidity	None	Fully liquid
Caps	Capped phases	Unlimited
Risk	Self-Custodial Vault	Custody Challenges
Complexity	Medium (Limited Ledger Support so far)	Easy (Hot and Cold Wallets Support)
Rewards	BTC staking rewards + Babylon points	Babylon staking rewards + Babylon points + LST protocol points + additional DeFi yield
Target User	BTC holders looking to participate in Babylon BTC Staking	BTC holders looking to participate in Babylon BTC Staking, whilst keeping their position liquid, enabling participation in DeFi
Capital requirements	0.005 BTC in a hot wallet	Lower capital requirements with no caps

Non-Yield Bearing BTC Tokens

Non-yield-bearing BTC tokens, are tokenized representations of Bitcoin that allow BTC holders to engage in DeFi. These tokens are pegged to the value of Bitcoin, allowing holders to unlock liquidity and use their assets on DeFi platforms on different networks.

WBTC

- Definition: WBTC is an ERC-20 token that represents Bitcoin on the Ethereum blockchain, allowing Bitcoin to be used in Ethereum's DeFi ecosystem.
- Yield Generation: WBTC can be used in various DeFi protocols to earn yields. However, the yields on WBTC are generally low, ranging from 0.01% to 0.08% APY on platforms like Compound and AAVE.
- Usage in DeFi: WBTC can be lent, borrowed, or used in liquidity pools to generate income. For example, users can supply WBTC on Aave, borrow stablecoins like USDT, and then use these stablecoins in other high-yield DeFi protocols to maximize returns.

FBTC

- Definition: FBTC is a type of synthetic asset that is 1:1 pegged to Bitcoin, allowing users to participate in various DeFi scenarios across different chains. It is generated when BTC is deposited into a specific address controlled by multi-party computation (MPC) nodes.
- Yield Generation: FBTC can be used to earn yields in multiple DeFi scenarios. Unlike WBTC, FBTC is designed to support Bitcoin yield scenarios in ecosystems like Babylon and other CeDeFi products. Users can deposit BTC, receive FBTC, and then use it to earn yields in various DeFi protocols.
- Usage in DeFi: FBTC is integrated across decentralized finance. FBTC can be utilized for staking and lending on several platforms.

Chapter 8:

Outlook



Outlook

BTC Staking Growth

The future of Bitcoin staking is poised for significant growth as more investors recognize the potential benefits of staking their assets. Currently, only a small portion of Bitcoin is staked, but this is expected to grow enormously as the cap limits on the Babylon protocol are lifted. The anticipated emergence of competitors to Babylon will further drive innovation and adoption in Bitcoin staking. The evolution will attract a broader audience, including institutional investors, who are increasingly seeking yield-generating opportunities within the Bitcoin ecosystem.

Lombard Decentralization

Lombard aims to reduce reliance on centralized custodians and intermediaries, thereby enhancing transparency and trust among users. This shift towards a more decentralized model will empower participants by giving them greater control over their staked assets while ensuring that the integrity of the network is maintained. Building a public ledger to track the consortium is a first step towards greater transparency.

Reduced Babylon Unbonding Times

Babylon is set to enhance its withdrawal capabilities through the Bitcoin Timestamping protocol implementation. This innovative protocol facilitates synchronization between PoS blockchains and Bitcoin, significantly reducing unbonding periods to just a few hours. Importantly, enabling withdrawals does not necessarily imply that Bitcoin will be withdrawn from the staking contract. A pertinent example is Ethereum 2.0, which experienced an increase in staked amounts following the introduction of withdrawal capabilities. This phenomenon occurs as more holders are encouraged to stake their assets, knowing they retain the flexibility to withdraw at any time.

DeFi Enters US

The US is heading for the inevitable legislation and regulation changes regarding the blockchain and cryptocurrency market. Next year, staking and DeFi will open up, flooding the market with new users. Currently, most of the top staking and DeFi protocols are excluding the US jurisdiction from participation, including Babylon. Once the constraints targeting the US users are lifted, we can expect record-high interest.

Wallets and Custodians Support

As Bitcoin staking gains traction, an increasing number of wallets and custodians are expected to incorporate support for staking functionalities. This expansion will provide users with more options for managing their assets while participating in staking activities. This trend will not only enhance accessibility for retail investors but also attract institutional clients seeking reliable and secure platforms for managing their Bitcoin holdings.

Crypto Stack Integration

Bitcoin staking is gradually becoming a native component of the broader cryptocurrency stack, akin to Ethereum's established staking ecosystem. As protocols like Babylon and Lombard continue to develop robust staking solutions, Bitcoin holders will increasingly view staking as an integral part of their investment strategy. This integration will facilitate cross-chain interactions and enhance capital efficiency, allowing users to leverage their staked Bitcoin across various DeFi platforms.

Regulatory Outlook

The panelists from the Staking Summit foresee a promising future if the U.S. assumes a leading role in crypto regulation, potentially driving global standards. Tal Zakon noted, "A regulatory reset in the U.S. could be a turning point, encouraging a global environment where crypto companies can thrive." Nonetheless, Eric Hill tempered expectations, explaining that even with leadership changes, "Crypto is a broad category with varying priorities... the change could be gradual rather than sweeping." Eric suggested that, where regulations are unclear, there's room for innovation.

Chapter 9:

Conclusion



Conclusion

Bitcoin staking, spearheaded by Babylon's protocol, is redefining BTC's utility from a passive asset to an active, yield-generating one. This innovative staking approach offers both non-custodial options for asset control and custodial solutions that streamline processes for institutions, supported by regulatory developments in key jurisdictions. With expanding tokenized BTC options and liquid staking, Bitcoin is being integrated into broader financial ecosystems, fostering liquidity, security, and flexibility. As regulations evolve and institutional interest grows, Bitcoin staking presents a compelling new landscape for financial and crypto markets alike, paving the way for BTC's role as both a security asset and a diversified financial instrument.

Acknowledgments

Special thanks to Jacob Phillips, Matt Donovan and the team from Lombard, Trudy Liu, Boris Alergant and the team from Babylon Labs, and Jing Xiong and Nic from Solv for their contributions to the report.

Looking to stake your BTC?

Get in touch with the Staking Rewards team. You may be eligible for a personalized staking offer. Earn more rewards, pay less fees and get 1-1 support.

[Book a call](#)