Braavos BTC Earn

Abstract

Braavos BTC Earn is a significant advancement within the Bitcoin ecosystem, offering users a way to earn yield in-kind on their Bitcoin while preserving self-custody and minimizing risk. Through a seamless, one-click experience, users can deposit BTC into audited yield strategies that prioritize security, transparency, and immediate liquidity.

Unlike traditional Bitcoin investment products, Braavos BTC Earn integrates Bitcoin directly into a self-custodial smart wallet environment, offering users a sovereign and frictionless path to unlock the earning potential of their BTC.

---

1. Introduction

Bitcoin remains the most trusted and valuable asset in the crypto ecosystem, yet the overwhelming majority of BTC sits idle, unproductive and underutilized. At Braavos, we believe the next chapter in Bitcoin's story is about activating this passive capital without compromising security, custody, or user experience.

Historically, Bitcoin holders faced a stark tradeoff: either hold BTC in cold storage earning nothing, or trust centralized intermediaries for yield, often at the cost of security and transparency.

Braavos BTC Earn changes this paradigm. It allows users to:

- **Maintain full self-custody** of their Bitcoin
- **Earn high yields** via integrated DeFi opportunities
- **Access yield with minimal friction** through an intuitive experience from any device
- **Minimize risks** with fully audited smart contracts, atomic swaps that eliminate bridge risk, and no credit risk

- **Withdraw anytime** with no lockups or holding periods

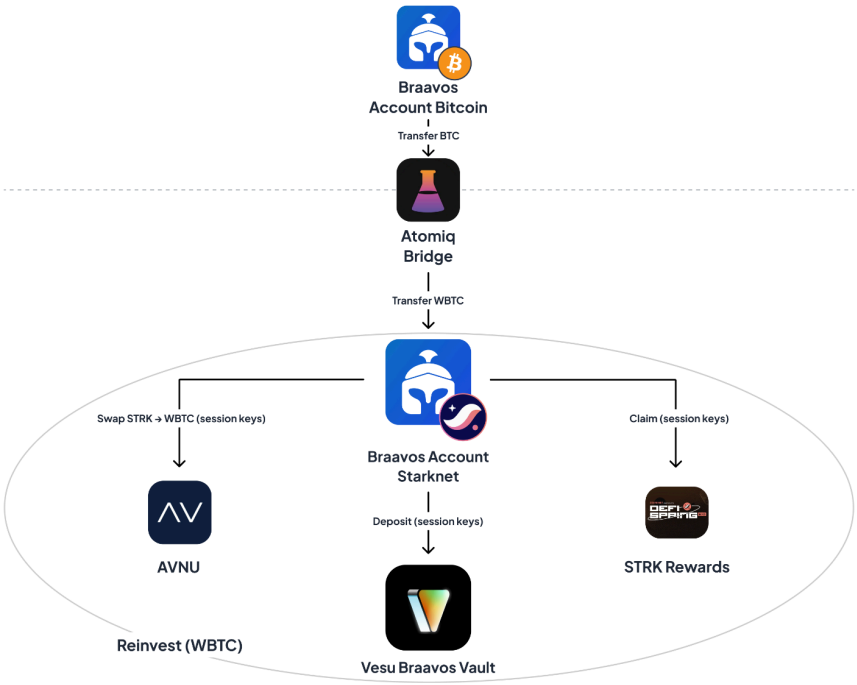
Braavos BTC Earn reflects a practical evolution in how Bitcoin holders can responsibly put their assets to work while retaining full control and security.

2. Product Architecture

Braavos BTC Earn is built upon a layered architecture that combines Bitcoin self-custody with decentralized yield generation mechanisms, ensuring user sovereignty and robust security at every step. The primary yield generation occurs on Starknet - a Layer 2 scalability solution for Ethereum and Bitcoin that pioneers the use of STARK validity proofs.

The core components include:

- **User BTC Account**: A native Bitcoin account (Native Segwit) within the Braavos Wallet where users maintain self-custody of their Bitcoin.
- **Atomic Swap**: Powered by Atomiq, this bridge facilitates atomic swaps, receiving BTC on the Bitcoin network and instantly exchanging it for WBTC on Starknet without introducing bridge risk.
- **User Starknet Smart Contract Accoun**t: A self-custodial smart contract account with the Braavos wallet that, using session keys, seamlessly interacts with the bridge, deposits funds into Braavos Vault on the Vesu protocol, collects rewards, and reinvests them to enable compounding yields.
- **Braavos Vault on Vesu**: A money market vault on the immutable Vesu protocol holding a WBTC-USDC liquidity pool designed to generate stable and sustainable yield.
- **STRK Rewards**: Weekly reward distributions from the Starknet Foundation, providing an additional layer of returns.
- **AVNU Trading Hub**: Integrated to swap STRK rewards back into WBTC at the best available rates, ensuring efficient compounding.



2.1 Self-Custody Model

Braavos BTC Earn operates under a self-custodial model. Users retain ownership of their assets at all times, both on Bitcoin and Starknet. Deposits into the vault are protected by permissioned Session Keys, which are strictly limited to the following actions: depositing or withdrawing to/from the user's own account, claiming rewards into the user account, and swapping rewards to WBTC into the same account. The smart contract that manages user funds and session keys, along with the Vesu vault protocol, are audited by independent third-party security firms.

2.1.1 Session Keys

Session keys are a core capability of account abstraction, allowing users to authorize limited operations on their smart contract account without having to sign synchronously for each such operation. In Braavos BTC Earn, session keys are programmed and enforced by the account smart contract and used to sign a narrowly scoped set of permissions.

Each session key is:

- **Protocol restricted**, granting permission only for specific contracts (e.g., Vesu vault, AVNU STRK swap)

- **Functionally restricted**, granting permission only for specific contract calls (e.g., deposit to a particular vault, claim rewards, swap tokens).
- **Parameter constrained**, meaning the key is only valid if the function parameters match exact criteria. For example, the destination address must be the user's account, or the maximum swap amount must not exceed a set threshold.

This restricted design ensures that even if a session key is compromised, it cannot be used to perform arbitrary actions or transfer funds to unauthorized parties. Instead, it enables secure, automated interactions (like compounding rewards) while preserving user control and minimizing trust assumptions.

2.1.2 Atomic Swaps

Atomiq Exchange enables secure, trustless atomic swaps between Bitcoin and Starknet by combining an on-chain Bitcoin light client with Proof-Time Locked Contracts (PTLCs). The Bitcoin light client verifies Bitcoin transactions by storing block headers and validating Merkle proofs, allowing smart contracts to independently confirm Bitcoin events without relying on external oracles. PTLCs govern the swap: funds are released when a valid Bitcoin transaction proof is submitted, or refunded to the sender if the proof is not provided within a preset timelock.

The swap process involves a user locking assets into a PTLC, a corresponding Bitcoin transaction being made, and the Bitcoin light client verifying its inclusion on-chain. Relayers update the light client with new Bitcoin headers, while optional watchtowers automate the claiming process for users. This design removes the need for trusted third parties, creating a decentralized and secure way to exchange Bitcoin with assets on Starknet.

2.2 Yield Generation

2.2.1 The Braavos Vault on Vesu

The Braavos pool on the Vesu protocol is an isolated lending market with its own minimal risk parameters and supported assets - WBTC and USDC. It is configured such that WBTC can only be supplied (not borrowed), meaning it is always available for withdrawal. This design ensures

that depositors earning yield on their WBTC take on no credit risk. Price oracles are used solely to track the WBTC and USDC price, with a time-weighted average of 4 hours gathering data from 3 different sources to guard against manipulation or price attacks. It should be emphasized that WBTC is not employed as collateral, nor is it accessible for loaning.

Vesu is a fully permissionless, governance-free, immutable lending protocol on Starknet, designed to maximize decentralization and composability in DeFi lending.

2.2.2 STRK Rewards

The yield originates primarily from the Starknet DeFi Spring Rewards program, designed to incentivize total value locked (TVL) growth and on-chain activity on Starknet.

Yields are not derived from rehypothecation, opaque lending, or leverage. Moreover, user assets are never borrowed, eliminating credit risk and ensuring that funds remain fully available for withdrawal at all times with no lockups.

Rewards are distributed weekly, typically every Friday, enabling yields to compound on a weekly basis.

2.3 Protocol Fees

Fees are composed of two primary elements:

- **Bitcoin Network Fee**: Applicable to deposits from Native Segwit accounts, paid by the user.
- **Protocol Fee**: A 15% fee on the yield generated (APR), automatically retrieved by the protocol during each reward claim cycle.

Additional fees are fully subsidized and not borne by the user:

- **Bridging Fee**: Covered by Braavos on all deposits to incentivize participation.
- **Starknet Gas Fees**: Fully subsidized for all DeFi operations, ensuring a seamless user experience.

2.4 Tracking and Insights

The Braavos Wallet provides users with comprehensive visibility into their BTC Earn position, allowing them to monitor and understand the performance of their investment in real time. Key metrics include:

- **Current Balance**: The total amount currently held in the vault, including the original deposit and all accumulated yield.
- **Invested Amount**: The cumulative BTC amount deposited into the vault across all user transactions.
- **Value at Time of Deposit (USD)**: The equivalent USD value of the BTC when initially deposited, serving as a cost basis reference.
- **BTC Gains**: The total amount of BTC earned via yield, net of fees.
- **USD Gains**: The net USD gains, which reflect both the BTC yield and any BTC/USD exchange rate appreciation since the initial deposit.

All figures are updated regularly and accessible from both mobile and browser versions of the Braavos Wallet, offering users full clarity and control over their investment performance.

2.5 Categorized Product Architecture Summary

Component	Description	Category
User BTC Account	Native Segwit BTC account in Braavos Wallet; full self-custody of Bitcoin.	Self-Custody
Atomic Swap (Atomiq)	Trustless bridge via Atomiq enables atomic swaps BTC ↔ WBTC on Starknet without bridge risk.	Architecture / Security
User Starknet Smart Contract Account	Smart contract wallet on Starknet using session keys to automate yield flow and maintain self-custody.	Architecture / UX
Braavos Vault on Vesu	WBTC-USDC vault on Vesu; isolated lending pool that offers stable yield with no credit risk.	Yield Generation
STRK Rewards	Weekly yield from Starknet's DeFi Spring rewards program; compounds automatically.	Yield Generation
AVNU Trading Hub	Swaps STRK back into WBTC using best rates for reinvestment and compounding.	Yield Optimization
Session Keys	Limits fund management permissions to specific contracts, actions (like deposit, claim, swap) and recipients to protect from misuse.	Security
Yield Source	Yield from STRK incentives on Starknet; no borrowing, leverage, or rehypothecation involved.	Yield Source
Protocol Fees	15% fee on yield; Bitcoin network fee applies, but bridging and Starknet gas fees are subsidized.	Fees
Tracking & Insights	Real-time metrics including current balance, invested BTC, USD value at deposit, BTC and USD gains.	User Insights

3. Risk Management

3.1 Audited Smart Contracts

All contracts are tested and audited by third-party security auditors. Audit reports are publicly available:

- Braavos audit
- Vesu vault audit
- Atomiq exchange audit

3.2 Yield Source Transparency

For Braavos BTC Earn, the primary yield is derived from the Starknet DeFi Spring Rewards program, with no reliance on borrowing or leverage. Deposited WBTC is never lent out, ensuring no credit risk. Weekly STRK rewards, typically distributed on Fridays, enable compounding yield. In addition, a portion of the yield is generated from lending activity within the pool, specifically from borrowers of USDC, and at no time interacts with or puts the WBTC at additional risk. Historical reward rates, risk classification, and audited contract details are accessible in-app and via linked documentation.

The yield on the BTC investment is paid in-kind. For example, if a user deposits 1 BTC and earns a 10% APR, their balance will grow to 1.1 BTC, which they can withdraw in full without lockups or redemption delays.

3.3 Withdrawal Liquidity

The BTC Earn product is designed to ensure user withdrawals are honored promptly, with no lockups. Typically as fast as the confirmation time of one Bitcoin block plus a minimal delay for Starknet processing.

4. Security Architecture

- **Account Ownership**: Users' private keys remain securely stored on their personal devices at all times, never exposed to Braavos or any third party.
- **Biometric 2FA/3FA**: Transactions on Starknet are protected with biometric authentication (e.g., Face ID, fingerprint), in combination with passkeys bound to the device. This provides strong 2FA and optional 3FA authentication, ensuring only the device owner can approve sensitive operations.
- **Atomic Swaps**: By leveraging Atomiq's trustless swap mechanism, users avoid bridge risk entirely. Funds can never be stolen or lost due to intermediary failure.

- **Secure Key Management**: The wallet relies on secure enclaves or trusted execution environments and encrypted local storage to keep cryptographic material isolated from the app layer.
- **Open Source Smart Contracts**: All smart contracts, including account and session key management, vault logic, and reward operations, are fully open-source and publicly auditable.
- **Immutable Vault Protections**: The Vesu vault is immutable and features protocol-level safeguards such as stop-loss protections and recovery logic, ensuring reliable access to user funds even under volatile conditions.

5. About Braavos

Braavos is a self-custodial smart contract wallet purpose-built for Starknet and Bitcoin. It pioneers advanced account abstraction features such as biometric 2FA/3FA signing, session keys for seamless automation, multi-owner accounts, and secure key storage utilizing the device's secure enclave.

Braavos is trusted by over 1 million users and continues to lead the way in secure and intuitive wallet design. With the introduction of BTC Earn, Braavos offers Bitcoin holders a sovereign and transparent way to generate yield, without sacrificing control or custody.

6. Conclusion

Braavos BTC Earn offers a new paradigm for Bitcoin holders, combining the trustless architecture of atomic swaps, the programmability of account abstraction, the transparency of audited DeFi vault and the risk free of the STRK incentives rewards mechanism. With a fully self-custodial design, automated compounding via session keys, and subsidized access to Starknet DeFi rewards, users can earn meaningful yield on their BTC without compromising on security or control.

From seamless onboarding to real-time rewards and permissioned automation, Braavos BTC Earn empowers Bitcoin holders with a sovereign, intuitive, and secure path to put their assets to work.

Braavos BTC Earn: **Secure**. **Transparent**. **Self-Custodial**.

7. References

- **Website:** https://braavos.app/
- **App:** https://braavos.app/download-braavos-wallet/
- **Blog:** https://braavos.app/blog/
- **Community:** Telegram | Discord
- **Social:** X (Twitter) | LinkedIn