DUE DILIGENCE PROCESS
CHAIN-KEY BITCOIN (ckBTC)

Written by @manilpwn and @TrickyVik 06/2025

Team Background: Assess the founding team's transparency, credibility, experience, and any past contributions to the ICP ecosystem.

Chain-key Bitcoin (ckBTC) is developed and maintained by the DFINITY Foundation, the primary organization behind the Internet Computer Protocol (ICP). DFINITY is led by Dominic Williams, an experienced technologist and entrepreneur in blockchain, decentralized computing, and cryptography. The foundation employs a large team of expert developers, cryptographers, and researchers globally.

Token Utility: Examine the token's purpose and functionality within its ecosystem to ensure it provides tangible value and practical use cases.

Chain-key Bitcoin (ckBTC) serves as a multi-chain twin of Bitcoin, enabling BTC to be used seamlessly within the ICP ecosystem. It retains full 1:1 backing with native BTC, secured via cryptographic techniques and managed by the Network Nervous System (NNS).

Primary utilities include:

- Facilitation of DeFi applications
- Integration of Bitcoin into smart contracts and dApps
- Instant, low-cost transactions on ICP compared to native Bitcoin network fees and times.

Ecosystem Alignment: Evaluate the token's synergy with other ICP projects, including any existing collaborations and suitability for inclusion in the Salsa Season rewards program.

Programmable bitcoin is a unique value proposition. Integration of ckBTC can impact broader ICP adoption, facilitating enhanced liquidity and user engagement.

OpenChat uses ckBTC for tipping and Odin.Fun is a popular memecoin platform with ckBTC being the primary mode of payment.

Including ckBTC in the TACO DAO portfolio means that Salsa Season rewards program participants will gain exposure to BTC.

Technology: Review the project's technical foundation, focusing on code quality, scalability, and how effectively it leverages ICP's capabilities.

ICP's Chain-Key Technology allows smart contracts to securely sign Bitcoin transactions without any single node accessing private keys. This enables ckBTC to hold and manage Bitcoin addresses directly on-chain.

ICP's network security depends on validators who are paid in ICP tokens and the governance of ICP token holders.

ckBTC utilises the *ckBTC Minter,* a canister controlled by the NNS and operating on the 'pzp6e…' subnet (more information on this in *Security Risks).* Principal ID's inform the Minter about an increase in the

BTC balance as a result of their BTC address, and the Minter then mints ckBTC of identical value. Later, ckBTC can be burned in the Minter for an equivalent amount of BTC.

A minimum ckBTC burn (in other words BTC withdrawal) amount of 0.001 BTC, or 100,000 satoshi, and; a Know-Your-Transaction fee of 0.00002 BTC, or 2,000 satoshi

Liquidity:

As per SwapRunner on the 1st of June 2025, a single transaction of:

- 20000 ICP ($98739.32) will result in a trade to 0.75197956 ckBTC ($78761.20). 20.23% lost to price impact
- 10000 ICP ($49369.66) will result in a trade to 0.4307592 ckBTC ($45117.07). 8.614% lost to price impact
- 1000 ICP ($4936.97) will result in a trade to 0.04672558 ckBTC ($4893.97). 0.871% lost to price impact
- 250 ICP ($1234.24) will result in a trade to 0.01174256 ckBTC ($1229.90). 0.352% lost to price impact

As can be seen, liquidity for ckBTC remains limited. If liquidity is not recycled, and there are no 'sells' between the DAO's 'buys', the effective slippage rate will be identical regardless of whether multiple small transactions or one large one take place.

Competitors: Identify similar projects and assess the token's differentiators alongside the perceived competitive positioning within its niche.

- Wrapped Bitcoin is the Ethereum network's 1:1 tokenised version of Bitcoin. In the WBTC system, one party sends BTC to a custodian, who agrees to mint a token that is backed 1:1 by the held Bitcoin. This token, now holding an exact value pair with the BTC, can interface with the Ethereum network and all it has to offer.

  When BTC is deposited onto BTC addresses controlled by the ICP network, no one individual is now 'owning' the BTC and agreeing to mint a tokenised version of it in return. Instead, the ICP Network's various nodes split parts of the private key between themselves, cryptographically ensuring the existence of reserves and removing the necessity of human trust that a system such as WBTC employs. In WBTC, a custodian is simply holding the existing BTC and creating a token backed by it, creating a single point of failure: legitimacy of the custodian. WBTC can theoretically lose all value because its reserves can vanish or become compromised.

  Faster settlement times are seen on ICP, specifically:

  1. Ethereum's real-time TPS (transactions per second) is 1.75% that of ICP
  2. Ethereum's block time is 25x that of ICP

- Lighting Network represents a novel solution to the crypto ‘trilemma’ - the battle between security, scalability, and decentralisation. Lightning works by creating a *channel* between two individuals that essentially creates a locked figure of BTC belonging to both parties, in which infinite transactions of virtually any size can occur without causing an actual transaction on the BTC blockchain. Heavy fees are avoided, and extremely small payments can take place. Only two blockchain transactions occur: opening the channel with the initial figures, and closing it with the updated figures.

  ckBTC *also* uses two transactions, both ‘leaving’ and ‘entering’ the BTC blockchain. The main difference lies in utility. Lighting can *only* serve as a peer-to-peer transaction system. It cannot interface with any other system: there exists no DeFi, no smart contracts, no voting, and none of the other unique features available on other blockchains. ckBTC allows direct integration of BTC with ICP’s ecosystem.

Security Risks: Investigate perceived vulnerabilities, any audit reports, and adherence to security and regulatory standards.

Trail of Bits, an organization specializing in high-end security research, scanned the ckBTC codebase. The verdict was very positive and there were no medium or high-severity findings. The audit focused on preventing double-spending, denial-of-service attacks, and ensuring the ckBTC Minter could not be manipulated into signing invalid transactions or burning tokens improperly.

BitcoinLayers, a research initiative documenting Bitcoin scaling solutions, provided the following risk ratings:

- BTC Custody: High Risk
- Data Availability: High Risk
- Network Operators: Medium Risk
- Finality Guarantees: Medium Risk

While this may seem bad, it is worth noting that virtually all other layer-solutions score ‘very high’ or ‘critical’ on many of these tags, and that only Bitcoin native solutions (such as Lightning) score as ‘low risk’. When it comes to Bitcoin layers that allow interfacing with other systems, ICP is among the top in terms of safety.

The ‘pzp6e…’ subnet managing the ckBTC smart contract module has 34 node operators who have undergone a KYB process to ICP governance and are publicly known. If nodes for this subnet go offline, and a backup of the state is not regularly made, holders would lose access to their ckBTC. It would require 10 nodes to collude to take over the ckBTC subnet.

When a user deposits or withdraws bitcoin, the Bitcoin Checker Canister checks whether the bitcoin address is associated with any illicit activities on the SDN list of the OFAC. If it is, deposits are quarantined and withdrawals are rejected.