Trail of Bits BTC/ckBTC Review: Fix Notes

The issues in the report were addressed as follows.

Issue	Severity	Status
TOB-DFBTC-1	Low	Unresolved / Risk Accepted
TOB-DFBTC-2	Informational	Resolved
TOB-DFBTC-3	Informational	Resolved
TOB-DFBTC-4	Informational	Resolved
TOB-DFBTC-5	Low	Unresolved / Risk Accepted

TOB-DFBTC-1: KYT canister is centralized on third party provider

Status: Unresolved / Risk Accepted

Comment: We currently accept the risk because it is mainly a threat to availability in that converting between BTC and ckBTC won't be possible when the KYT provider is not reachable. All funds would be safe and ckBTC could still be transferred between accounts. If the KYT provider becomes inoperable, the KYT canister can be upgraded to use a different provider.
In the unlikely event that the KYT provider erroneously classifies all deposits as "tainted", a canister upgrade could be proposed to unlock the quarantined bitcoins.
Implementing a more decentralized approach that reduces these risks would require significant effort and is currently not planned.

TOB-DFBTC-2: Risk of amount underflow when retrieving BTC

Status: Resolved

Commit: https://github.com/dfinity/ic/commit/cf4e446d1997dd94c7fee21c6daffafded2857de

Comment: The changes ensure that the canister upgrade arguments are properly validated, addressing TOB-DFBTC-3 below as well. As a result, it is no longer possible to define a fee that is higher than the minimum retrieve amount, which could have potentially caused an underflow when retrieving BTC.

TOB-DFBTC-3: Minter's init and upgrade configs insufficiently validated

Status: Resolved

Commit: https://github.com/dfinity/ic/commit/cf4e446d1997dd94c7fee21c6daffafded2857de

Comment: The changes ensure that the canister upgrade arguments are properly validated.

TOB-DFBTC-4: Inconsistent error logging in minter

Status: Resolved

Commit: https://github.com/dfinity/ic/commit/6f546a0dc49f088294231add7a8194800aa05de1

Comment: The changes make the error logging more consistent.

TOB-DFBTC-5: KYT API keys are exposed

Status: Unresolved / Risk Accepted

Comment: We currently accept the risk because the risk is the same as for TOB-DFBTC-1 and fixing this issue would require a significant effort.

Quality Recommendations (Appendix C)

The recommended code quality recommendations have been applied. Specifically, the following changes have been made:

- Changed the `init_ecdsa_public_key` function to return the key.
- Updated the documentation comment for mode in the ckBTC minter's `InitArgs`.
- Updated the broken documentation.
- Removed the extra space between sentences.
- The redundant check in `submit_pending_requests` has been removed.
- The usage of `key_derivation` has been replaced with `public_key_derivation`.
- Documented all the data types and functions.
- Removed `unwrap` in the production code.

Commit: https://github.com/dfinity/ic/commit/b9d14e71b857ceca7087b31f5a32618d25555f29