March 2, 2020

Audit Report

PTOKEN BITCOIN BRIDGE

CRYTONICS CONSULTING

Cryptonics

Cryptonics Consulting S.L., Ramiro de Maetzu 7,
46022 Valencia, Spain

Table of Content

Disclaimer

Introduction

Purpose of this Report

Cryptonics Consulting has been engaged to perform an audit of the pToken Bitcoin to Ethereum 2-way asset transfer bridge, forming part of the pToken project (https://ptokens.io/).

The objectives of the audit are as follows:

1. Determine the correct functioning of the implementation in accordance with the project specification.
2. Determine possible vulnerabilities, which could be exploited by an attacker.
3. Determine contract bugs, which might lead to unexpected behavior.
4. Analyze whether best practices have been applied during development.
5. Make recommendations to improve code safety and readability.

This report represents the summary of the findings.

As with any code audit, there is a limit to which vulnerabilities can be found, and unexpected execution paths may still be possible. The authors of this report do not guarantee complete coverage (see disclaimer).

Codebase Submitted To The audit

The smart contract code has been provided by the developers in form of three compressed source code archive files with the following SHA-256 hash:

- pbtc-with-audit-fixes.zip:

  0x2a2b9a0571158c61667f609f7db7d2983e46fa462ea15c0880f605726956a29d

- pbtc-with-node-audit-fixes.zip:

  0xe625ced494a91ef8e90230ea8af8d7af8903604a64b01403605a2587556e00f6

- erc777-smart-contract-for-auditors.zip:

  0xe4f66783df8670a4cd37d3c950e5fe372e7f2a55cc5a78f0d5e664659ce8b234

Additional smart contract fixes have been provided separately in the form of a diff file.

Methodology

The audit has been performed in the following steps:

1. Gaining an understanding of the code base's intended purpose by reading the available documentation.
2. Automated source code and dependency analysis.
3. Manual line by line analysis of the source code for security vulnerabilities and use of best practice guidelines, including but not limited to:

- Race condition analysis
- Front-running issues and transaction order dependencies
- Under- / overflow issues
- Function visibility Issues
- Possible denial of service attacks
- Key management vulnerabilities

4. Report preparation

Project Overview

The submitted code provided in two separate repositories implements a cross blockchain bridge that allows assets to be moved from Bitcoin to Ethereum. Bitcoin is represented on the Ethereum blockchain in the form of an ERC20 token (pBTC).

The two-way peg works by depositing BTC (locking) on Bitcoin and minting pBTC on Ethereum and by burning pBTC on Ethereum and unlocking BTC on Bitcoin. Transactions are relayed across chains through light clients designed to operate in a secure enclave.

The enclave is designed to be executed in a protected enclave using a trusted execution environment, such as Intel SGX. Eventually, data can also be stored in an external encrypted database with HSM key storage. However, the current codebase includes an unprotected in-memory database and a rockDB-based unencrypted database for testing purposes.

Security Audit Findings

General

1. ⚠ [major] The output of the build process (including possible flattened files) should not be committed to the Git repository. Currently, `pbtc-address-generator-bin/pbtc-deposit-address-generator` is committed into multiple repositories. This might lead to outdated versions to be used.
   Status: ✔ [fixed]

pBTC-enclave

Rust-Specific Code Review

Given that the pBTC enclave is the key component written in the Rust language, a number of Rust-specific checks have been performed, according to the following checklist:

1. Development Environment
   a. Stable, nightly and beta toolchains
      i. 🚧 [minor] pBTC uses the nightly toolchain. Secure applications should be developed with the fully stable toolchain.
      Status: □ [acknowledged] Nightly tool-chain is currently used to use `?` operator on Options for succinct error handling.

b. Cargo
   i. ✔️ [no issues] Variables `debug-assertions` and `overflow-checks` are not overridden
   ii. ✔️ [no issues] Environment variables `RUSTC`, `RUSTC_WRAPPER` and `RUSTFLAGS` are not overriden
c. Linting
   i. ✔️ [no issues] Clippy (https://github.com/rust-lang/rust-clippy) does not reveal any issues.
d. Rustfmt
   i. 🚧 [minor] Rustfmt should be used to format the codebase correctly. Status: ☐ [acknowledged] "`rustfmt` insists on very long lines and [we] work on small screens with two files side by side. `rustfmt` renders this unreadable for [us]."

e. Rustfix
   i. ✔️ [no issues] Rustfix is not used

2. Libraries
   a. Cargo-outdated
      i. 🚧 [minor] Many libraries are outdated, see Appendix B. Status: ☐ [acknowledged] "Library dependencies were pinned to enable easier iteration with up-stream HSMs, many of whom (SGX, for example) have some very strict requirements (no-std etc)."

   b. Cargo-audit
      i. ✔️ [no issues] No issues found (only a warning that `term` is looking for a maintainer)
3. Language generalities
   a. Unsafe code
      i. ✔️ [no issues] No use of `unsafe`
   b. Integer overflows
      i. 🚧 [minor] `nonce` is using `usize`, which can be a 32-bit unsigned integer and could potentially overflow. Use `overflowing_add` and `overflowing_sub` instead and panic if overflows/underflows occur. (pbtc-enclave/src/btc/btc_database_utils.rs:70, pbtc-enclave/src/btc/get_btc_output_json.rs:92, pbtc-enclave/src/btc/sign_transactions.rs:46, pbtc-enclave/src/btc/utxo_manager/utxo_database_utils.rs:98, pbtc-enclave/src/btc/utxo_manager/utxo_database_utils.rs:330, pbtc-enclave/src/eth/eth_database_utils.rs:371, pbtc-enclave/src/eth/get_eth_output_json.rs:79, pbtc-enclave/src/btc/get_btc_output_json.rs:84, pbtc-enclave/src/eth/get_eth_output_json.rs:71) Status: ✔️ [fixed]

      ii. 🚧 [minor] some amounts/balances are using `usize`, which can be a 32-bit unsigned integer and could potentially overflow. More

specifically, Satoshi supply is bigger than `2^32-1`. Use `overflowing_add` and `overflowing_sub` instead and panic if overflows/underflows occur. (`pbtc-enclave/src/btc/utxo_manager/utxo_database_utils.rs:144`). Also change the arguments/return values in to `u64` in `pbtc-enclave/src/btc/utxo_manager/utxo_database_utils.rs:139`, `pbtc-enclave/src/btc/utxo_manager/utxo_database_utils.rs:149`, `pbtc-enclave/src/btc/utxo_manager/utxo_database_utils.rs:171` and `pbtc-enclave/src/btc/utxo_manager/utxo_database_utils.rs:179`.
Status: ✔️ [fixed]

c. Error handling
   i. 🚧 [minor] In some places, the code can panic. It is generally preferred to use Results instead.
      1. pbtc-enclave/src/btc/parse_minting_params_from_op_return_deposits.rs:73
      2. pbtc-enclave/src/eth/nibble_utils.rs:39
      3. pbtc-enclave/src/database_interface/mod.rs:70, 79 and 88

   Status: ✔️ [fixed]

4. Memory management
   a. Forget and memory leaks
      i. ✔️ [no issues] No use of forget and potential memory leaks found
   b. Uninitialized memory
      i. ✔️ [no issues] No uninitialized memory found
   c. Secure memory zeroing for sensitive information
      i. 🚧 [minor] memory is not zeroed currently, which means that sensitive information will stick in memory when the memory is freed. This is not a big issue since the enclave is running in a TEE, but might be added by implementing the Drop trait for the relevant memory (see https://anssi-fr.github.io/rust-guide/05_memory.html#secure-memory-zeroing-for-sensitive-information for details).
      Status: ✔️ [fixed]

5. Type system
   a. Drop trait, the destructor
      i. ✔️ [no issues] No implementation of the Drop trait
   b. Send and Sync traits
      i. ✔️ [no issues] No implementation of the Send or Sync traits
   c. Comparison traits (PartialEq, Eq, PartialOrd, Ord)
      i. ✔️ [no issues] Only PartialEq is implemented for one type: Nibbles. The implementation satisfies the invariants Rust assumes: Internal consistency, symmetry and transitivity
6. Foreign Function Interface (FFI)

a. ✅ [no issues] No use of the FFI

Security Audit

1. 🚨 [critical] Control flow: When a step fails in `submit_btc_block` or `submit_eth_block`, the script aborts, but the database might have been updated. That leads to inconsistent and irrecoverable state. I'd advice to do all parsing first and only work in memory, and only update the database in an atomic way in the end. An example would be a failure to parse burn amount or btc addresses from burn events (in `pbtc-enclave/src/eth/parse_burn_event_params.rs:117`), which aborts the whole block ingestion, but the block has already been written to the database (in `pbtc-enclave/src/eth/add_block_and_receipts_to_database.rs:13`. In that case, any valid burn transactions would have no effect, since the block can't be re-submitted to the enclave. Another example is any error returned from any of the db functions, e. g. a crash of the db.
   Status: ✅ [fixed]

2. 🚨 [critical] When in sudo mode, the CLI command `sudoGetKeyFromDb` allows retrieval of private keys (`pbtc-enclave/src/sudo_functions/mod.rs`). The danger here is that sudo mode might be used without being aware of that possibility. Either explain this explicitly in the docs/usage info or blacklist the keys for private keys given in `pbtc-enclave/src/btc/btc_constants.rs` and `pbtc-enclave/src/eth/eth_constants.rs`.
   Status: ✅ [fixed]: "All `sudo` occurrences have been renamed to `debug` for clarity, and the documentation has been updated to make it clear that they're only usable if the `DEBUG` flag is set to true when the core binary is built. The `debug` mode is now a Cargo feature, with the flag itself conditionally compiled. Both core and the app's READMEs have been updated to reflect this, along with a warning added to each about the security-bypassing nature of the debug mode. Finally, the state of the `DEBUG` flag has been added to the output of the getEnclaveState function"

3. ⚠ [major] Private keys are publicly accessible from other modules (`pbtc-enclave/src/btc/btc_crypto/btc_private_key.rs:27`), support printing (`pbtc-enclave/src/btc/btc_crypto/btc_private_key.rs:111`) and conversion to bytes (`pbtc-enclave/src/btc/btc_crypto/btc_private_key.rs:59`). Suggestion: make this safer by not allowing private keys to be exposed or read in any way. The best solution may be to actually invert the control flow here: instead of getting the bytes from private keys and passing these bytes to the database, pass the database into a write function on the private key struct.
   Status: ✅ [fixed]

4. ⚠ [major] The used library `rust-bitcoin` is used for validation of bitcoin blocks, but the library itself warns that it should not be used to fully validate blockchain data (https://github.com/rust-bitcoin/rust-bitcoin#consensus).
   Status: ✅ [no issue] The library is used to validate BTC blocks, not for consensus. Said validation includes the block-header hash, the block's proof-of-work and the merkle-root of the transactions. The rust-bitcoin library itself has a test covering the

first two (https://github.com/provable-things/rust-bitcoin/blob/cbc40408ffb6ef6efc0e6b859a0c84a66b56816a/src/blockdata/block.rs#L248), and the latter has a test in the pToken core in `src/btc/validate_btc_merkle_root.rs:38`.

5. ⚠ [major] In `get_first_deposit_value_from_tx`, only the deposit value of the first output to the Bitcoin deposit script is taken (`pbtc-enclave/src/btc/parse_minting_params_from_op_return_deposits.rs:120`). That implies that a tx with multiple outputs to the deposit address will not be captured. This is an edge case, but it should either be clearly documented and communicated or better the sum of all outputs should be used (Here is an example of a Bitcoin transaction with multiple outputs going to the same address: https://www.blockchain.com/btc/tx/4199f709bfab79f54938e80e11dc75c21a95e3183f8e8994306f5ff272fde42a).
   Status: ✔ [fixed]

6. ⚠ [major] Segwit is currently not supported, which is properly documented in code `pbtc-enclave/src/btc/btc_utils.rs:179` and `pbtc-enclave/src/btc/parse_minting_params_from_op_return_deposits.rs:165`. Ensure that it is also communicated in the README.md and any external facing documentation.
   Status: □ [acknowledged] Documentation has been improved.

7. ⚠ [major] 17 of 483 tests in pbtc-enclave fail, see Appendix A for details.
   Status: ✔ [fixed]

8. 🚧 [minor] The signature timestamp is verified to be after unix epoch begin. This check could fail and lead to a panic if the enclave's system time is wrong. Is this check needed (`pbtc-enclave/src/btc/get_btc_output_json.rs:66` and `pbtc-enclave/src/eth/get_eth_output_json.rs:53`)?
   Status: □ [acknowledged] This error will only occur if the time is before the unix epoch beginning, in which case it is fine to panic.

9. 🚧 [minor] `sig_script_contains_pub_key` does not check the logic of the sig script – it could be a standard p2pkh, but it could also be a p2sh. It would be better to match the exact sig script (`pbtc-enclave/src/btc/filter_op_return_deposit_txs.rs:28`).
   Status: ✔ [non issue] The core can only write `p2pkh` transactions, so a different check is not needed.

10. 🚧 [minor] Sending to the enclave only works with p2pkh and p2sh, not for p2pk (because of the filter in `pbtc-enclave/src/btc/filter_op_return_deposit_txs.rs:73`). Even if the usage with p2pk is not intended, it's easy to also allow these transactions.
    Status: □ [acknowledged] This is a design choice, documentation has been improved.

11. 🚧 [minor] The condition for updating the tail block hash in the enclave should check for smaller than or equal, not for equal. If any of the steps during block submission

after saving a new block to the db failed in a previous run, the tail block might be further back and might not be removed (`pbtc-enclave/src/btc/update_btc_tail_block_hash.rs:23` and `pbtc-enclave/src/eth/update_eth_tail_block_hash.rs:23`).
Status: ✔️ [fixed]

12. 🚧 [minor] The condition for updating the canon block hash in the enclave should check for smaller than or equal, not for equal. If any of the steps during block submission after saving a new block to the db failed in a previous run, the canon block might be further back and might not be removed (`pbtc-enclave/src/btc/update_btc_canon_block_hash.rs:79` and `pbtc-enclave/src/eth/update_eth_canon_block_hash.rs:22`).
Status: ✔️ [fixed]

13. 🚧 [minor] The function to remove parent blocks if they are not anchors should be called recursively. If any of the steps during block submission after saving a new block to the db failed in a previous run, blocks further behind the anchor might be in the db. If not removed, these would be orphan blocks in the db (`pbtc-enclave/src/btc/remove_old_btc_tail_block.rs:58` and `pbtc-enclave/src/eth/remove_old_eth_tail_block.rs:50`).
Status: ✔️ [fixed]

14. 🚧 [minor] Ethereum block import does not check whether the transactions correspond to the merkle root. Only a check on the block header and the receipts is done (`pbtc-enclave/src/eth/submit_eth_block.rs:40`).
Status: ✔️ [non issue] Only receipts are needed by light client, not the transaction hashes.

15. 🚧 [minor] pbtc-enclave/README.md as well as pbtc-enclave/src/usage_info.rs describe an encrypted database, which is not currently used. pbtc-enclave/README.md also uses different method names (put, get, delete) from the implementation in `pbtc-enclave/src/database_interface/mod.rs` (`put_bytes_in_db`, `get_bytes_from_db`, `remove_bytes_from_db`). The documentation should be updated to describe the actual behaviour.
Status: ✔️ [fixed]

PBTC-BTC-SYNCER

1. ⚠️ [major] block data for a given height is queried three times directly in succession by block height in `pbtc-btc-syncer/lib/get-btc-block.js:27`, `pbtc-btc-syncer/lib/btc-endpoint-api.js` line 66 and 67. This is redundant. But more critically, due to soft forks, the returned block data could be for different blocks, and the database might be fed a block and txs from different block hashes. Query the block hash for a given height instead only once and re-use that hash for subsequent calls.
Status: ✔️ [fixed]

2. 🚧 [minor] `pollForBlock` is used recursively, which could potentially lead to a call stack overflow. Use a `setTimeout` with 0 ms to allow Node.js to clear the call stack `pbtc-btc-syncer/lib/errors.js:13`.
   Status: ✔️ [non issue] The trampoline already implements asynchronous recursion.

3. 🚧 [minor] Tests are failing, see Appendix C.
   Status: ✔️ [fixed] Failing test has been outdated and removed.

PBTC-ETH-SYNCER

1. ⚠ [major] block data for a given height is queried two times directly in succession by block height in `pbtc-eth-syncer/lib/get-block-and-receipts.js` line 26 and 32. This is redundant. But more critically, due to soft forks, the returned block data could be for different blocks, and the database might be fed a block and txs from different block hashes. Query the block hash for a given height instead only once and re-use that hash for subsequent calls.
   Status: ✔️ [fixed]

2. 🚧 [minor] `pollForBlock` is used recursively, which could potentially lead to a call stack overflow. Use a `setTimeout` with 0 ms to allow Node.js to clear the call stack `pbtc-eth-syncer/lib/errors.js:14`.
   Status: ✔️ [non issue] The trampoline already implements asynchronous recursion.

3. 🚧 [minor] Tests are failing: `npx mocha` > `rejectAPromise is not defined`
   Status: ✔️ [fixed] Failing test has been outdated and removed.

PBTC-ETH-AND-BTC-BLOCK-GETTER

1. ⚠ [major] block data for a given height is queried three times directly in succession by block height in both `pbtc-eth-and-btc-block-getter/lib/get-eth-block.js` line 56, 33 and 37 and in `pbtc-eth-and-btc-block-getter/lib/get-btc-block.js` line 88,70 and 71. This is redundant. But more critically, due to soft forks, the returned data could be for different blocks, leading to inconsistent data. Query the block hash for a given height instead only once and re-use that hash for subsequent calls.
   Status: ✔️ [fixed]

PBTC-DB-REPL

1. 🚧 [minor] repl allows deletion of reports, which is destructive. Consider using an `isDeleted` boolean flag and filtering by it instead, or remove the ability to delete reports (`pbtc-db-repl/pbtc-db-repl.js:57 and line 62`).
   Status: ✔️ [fixed]

PBTC-DEPOSIT-ADDRESS-GENERATOR

1. ✔️ [no issues] No security issues found.

PBTC-ENCLAVE-API

1. ✅ [no issues] No security issues found.

PBTC-TX-BROADCASTER

1. ✅ [no issues] No security issues found.

PBTC-ETH-SMART-CONTRACT

1. 🚧 [minor] The pBTC token contract does not implement any protection against the multiple withdrawal vulnerability (https://www.researchgate.net/publication/334161350_Resolving_the_Multiple_Withdrawal_Attack_on_ERC20_Tokens). Whilst protection against this vulnerability is not part of the ERC-20 standard, it has become common practise to enforce at least one protection mechanism. We recommend following Open Zeppelin's approach of including functionality for increasing and decreasing the allowance (https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/token/ERC20/ERC20.sol#L116).

   Status: ✅ [fixed]

2. 🚧 [minor] README is for pEOS smart contracts

   Status: ✅ [fixed]

3. [minor] The changePNetwork() function does not check for 0 address parameter.

   Status: ✅ [fixed]

Further Recommendations

PBTC-ENCLAVE

1. ⚠ [major] Error handling: When an error occurs, the whole block submission fails. E. g. if parsing one burn event amount in `pbtc-enclave/src/eth/parse_burn_event_params.rs:57`
   Status: ✅ [fixed]

2. ⚠ [major] A few TODOs with critical changes for mainnet are still open (`pbtc-enclave/README.md:261`):
   a. "Fee calculation to account for __`p2sh`__ transactions."
   b. "Decentralized methods for securely changing __`fee`__ , __`gas-price`__ & other CLI constants."

   Status: □ [acknowledged] Will be done in a future iteration

3. 🚧 [minor] The trace statement "✔ Putting BTC account nonce of 1 in db..." should read "✔ Putting BTC account nonce of 0 in db..." in `pbtc-enclave/src/btc/initialize_btc/btc_init_utils.rs:29`.
   Status: ✅ [fixed]

4. 🚧 [minor] The trace statement "✘ Too many bytes to convert to usize!" should read "✘ Too many bytes to convert to u64!" in `pbtc-enclave/src/eth/eth_database_utils.rs:349`.
   Status: ✅ [fixed]

5. 🚧 [minor] Use an enum for trie node types since the types are exclusive `pbtc-enclave/src/eth/trie_nodes.rs:225`.
   Status: □ [acknowledged] Deprioritized since it does not affect behaviour

6. 🚧 [minor] Linting/code format is not enforced everywhere, e. g. indentation in `pbtc-enclave/src/btc/get_deposit_info_hash_map.rs:20` and following.
   Status: □ [acknowledged] Deliberate choice not to use `rustfmt`.

PBTC-BTC-SYNCER

1. 🚧 [minor] Current design does not allow blocks to be fetched and prepared for submission in parallel. The limiting factor here potentially is network speed – the enclave is most likely faster with processing blocks than the syncer can fetch and submit them. This should be no issue under normal operation, but it might be if for some reason an enclave needs to re-run a big number of blocks, e. g. because of an error that led to an inconsistent database. It might make sense to work with a queue

here.
Status: □ [acknowledged] Deprioritized for now.

2. 🚧 [minor] A lot of code is duplicated between `pbtc-btc-syncer` and `pbtc-eth-syncer`. For better maintainability, consider moving shared functionality into a separate repository.
   Status: □ [acknowledged] Deprioritized for now.

3. 🚧 [minor] Querying the enclave does not have a timeout, meaning that it could hang forever. Use timeouts to allow retries (`pbtc-eth-syncer/lib/enclave-utils.js:14`).
   Status: ✔️ [fixed]

4. 🚧 [minor] Test coverage.
   Status: □ [acknowledged] Tests have been deprioritized on non-critical paths.

5. 🚧 [minor] ESLint reports warnings, see Appendix D.
   Status: ✔️ [fixed]

PBTC-ETH-SYNCER

1. 🚧 [minor] Current design does not allow blocks to be fetched and prepared for submission in parallel. The limiting factor here potentially is network speed – the enclave is most likely faster with processing blocks than the syncer can fetch and submit them. This should be no issue under normal operation, but it might be if for some reason an enclave needs to re-run a big number of blocks, e. g. because of an error that led to an inconsistent database. It might make sense to work with a queue here.
   Status: □ [acknowledged] Deprioritized for now.

2. 🚧 [minor] A lot of code is duplicated between `pbtc-btc-syncer` and `pbtc-eth-syncer`. For better maintainability, consider moving shared functionality into a separate repository.
   Status: □ [acknowledged] Deprioritized for now.

3. 🚧 [minor] npm reports 1 low severity vulnerability, which is irrelevant (web3 has an insecure credential storage – but since the pbtc-eth-syncer does not store any credentials, this is no issue).
   Status: ✔️ [non issue]

4. 🚧 [minor] Querying the enclave does not have a timeout, meaning that it could hang forever. Use timeouts to allow retries (`pbtc-eth-syncer/lib/enclave-utils.js:14`).
   Status: ✔️ [fixed]

5. 🚧 [minor] Test coverage.
   Status: □ [acknowledged] Tests have been deprioritized on non-critical paths.

6. 🚧 [minor] ESLint reports warnings, see Appendix H.
   Status: ✔️ [fixed]

PBTC-ETH-AND-BTC-BLOCK-GETTER

1. 🚧 [minor] getBlock is called three times, which is redundant, see `pbtc-eth-and-btc-block-getter/lib/get-eth-block.js` line 22, 56 and 33.
   Status: ✔️ [fixed]

2. 🚧 [minor] getBlockHashAtHeight is called twice, which is redundant, see `pbtc-eth-and-btc-block-getter/lib/get-btc-block.js` line 56, 61
   Status: ✔️ [fixed]

3. 🚧 [minor] Some code is duplicated between `pbtc-eth-and-btc-block-getter`, `pbtc-btc-syncer`, `pbtc-eth-syncer` and `pbtc-tx-broadcaster`. For better maintainability, consider moving shared functionality into a separate repository.
   Status: □ [acknowledged] Deprioritized for now.

4. 🚧 [minor] npm reports 1 low severity vulnerability, which is irrelevant (web3 has an insecure credential storage – but since the pbtc-eth-syncer does not store any credentials, this is no issue).
   Status: ✔️ [non issue]

5. 🚧 [minor] 0% test coverage.
   Status: □ [acknowledged] Tests have been deprioritized on non-critical paths.

6. 🚧 [minor] ESLint reports warnings, see Appendix G.
   Status: ✔️ [fixed]

PBTC-DB-REPL

1. 🚧 [minor] database ids/keys are reused across repositories – extract these constants into a separate repository for better maintainability. In some places, constants are used as strings, e. g. `pbtc-db-repl/pbtc-db-repl.js:65`.
   Status: ✔️ [fixed]

2. 🚧 [minor] Commented code should be removed (`pbtc-db-repl/lib/utils.js:60`).
   Status: ✔️ [fixed]

3. 🚧 [minor] Typo: `has` should be `hash` (`pbtc-db-repl/lib/constants.js:9`).
   Status: ✔️ [fixed]

4. 🚧 [minor] ESLint reports warnings, see Appendix E.
   Status: ✔️ [fixed]

PBTC-DEPOSIT-ADDRESS-GENERATOR

1. 🚧 [minor] Version information reported by cli is inconsistent with version in `pbtc-deposit-address-generator/Cargo.toml`. Use const VERSION: &'static str = env!("CARGO_PKG_VERSION“) in `pbtc-deposit-address-generator/src/get_version_info.rs:3`.
   Status: ✔️ [fixed]

2. 🚧 [minor] 0% test coverage.
   Status: ☐ [acknowledged] Tests have been deprioritized on non-critical paths.

PBTC-ENCLAVE-API

1. 🚧 [minor] database ids/keys are reused across repositories – extract these constants into a separate repository for better maintainability.
   Status: ✔️ [fixed]

2. 🚧 [minor] Do not return `200` if the functionality is not yet implemented. `501` might be appropriate here (`pbtc-enclave-api/lib/submit-eth-block-route.js`, `pbtc-enclave-api/lib/submit-btc-block-route.js`).
   Status: ✔️ [fixed]

3. 🚧 [minor] Parentheses are wrong in the limits for MongoDB queries, it should be: `.limit(isNaN(parseInt(_limit, 10)) ? 1 : parseInt(_limit, 10) > 100 ? 100 : parseInt(_limit, 10)))` or simpler: `.limit(isNaN(parseInt(_limit, 10)) ? 1 : Math.min(parseInt(_limit, 10), 100))` (`pbtc-enclave-api/lib/query-btc-address-route.js:5`, `pbtc-enclave-api/lib/query-btc-reports-route.js:5`, `pbtc-enclave-api/lib/query-eth-address-route.js:5`, `pbtc-enclave-api/lib/query-eth-reports-route.js:5`, `pbtc-enclave-api/lib/query-recipient-route.js:6`, `pbtc-enclave-api/lib/query-recipient-route.js:12`, `pbtc-enclave-api/lib/query-sender-route.js:5`).
   Status: ✔️ [fixed]

4. 🚧 [minor] npm reports 1 low severity vulnerability, which is irrelevant (web3 has an insecure credential storage – but since the pbtc-eth-syncer does not store any credentials, this is no issue).
   Status: ✔️ [non issue]

5. 🚧 [minor] ESLint reports warnings, see Appendix F.
   Status: ✔️ [fixed]

PBTC-TX-BROADCASTER

1. 🚧 [minor] Failing transactions do log an error, but they don’t save the error to the database yet. For better debugging, the error should also be written to the database. `pbtc-tx-broadcaster/lib/broadcast-transactions.js` lines 130 and 175

Status: ✔️ [fixed]

2. 🚧 [minor] After a failure of a Bitcoin transaction, there will be a 2 second wait before retrying the same transaction again. After a failure of an Ethereum transaction, the code will continue with the normal loop, interleaving the next Bitcoin transaction before trying the failed Ethereum transaction again. This second approach is preferable since it does not block transactions on the other chain.
`pbtc-tx-broadcaster/lib/broadcast-transactions.js` lines before 139 and 178
Status: ✔️ [fixed]

3. 🚧 [minor] `pbtc-tx-broadcaster/config.json` does not exist, but is imported in
`pbtc-tx-broadcaster/pbtc-tx-broadcaster.js:10`,
`pbtc-tx-broadcaster/lib/broadcast-transactions.js:19`,
`pbtc-tx-broadcaster/lib/get-config.js:1`,
`pbtc-tx-broadcaster/lib/set-last-seen-nonce.js:8`
Status: ✔️ [fixed]

4. 🚧 [minor] `REPORT_KEY` does not exist in `pbtc-tx-broadcaster/lib/constants.js`, which means that reports will fail. Used in
`pbtc-tx-broadcaster/lib/update-latest-nonce.js:2`,
`pbtc-tx-broadcaster/lib/get-signatures-from-database.js:7`,
`pbtc-tx-broadcaster/lib/broadcast-transactions.js:13`
Status: ✔️ [fixed]

5. 🚧 [minor] Some code is duplicated between `pbtc-eth-and-btc-block-getter`, `pbtc-btc-syncer`, `pbtc-eth-syncer` and `pbtc-tx-broadcaster`. For better maintainability, consider moving shared functionality into a separate repository.
Status: □ [acknowledged] Deprioritized for now.

6. 🚧 [minor] Duplicate constants `ETH_SIGNATURES_KEY` and `BTC_SIGNATURES_KEY` exist in `pbtc-tx-broadcaster/lib/constants.js:9` and line 10.
Status: ✔️ [fixed]

7. 🚧 [minor] Comments '✔ BTC report in state ∴ updating BTC nonce in db...' (`pbtc-tx-broadcaster/lib/update-latest-nonce.js:24`), '✔ No BTC report in state ∴ not updating BTC nonce in db' (`pbtc-tx-broadcaster/lib/update-latest-nonce.js:32`), '✔ ETH report in state ∴ updating ETH nonce in db...' (`pbtc-tx-broadcaster/lib/update-latest-nonce.js:37`) and '✔ No ETH report in state ∴ not updating ETH nonce in db' (`pbtc-tx-broadcaster/lib/update-latest-nonce.js:45`) are
wrong, the functions only update the nonces in state, not in the db.
Status: ✔️ [fixed]

8. 🚧 [minor] npm reports 1 low severity vulnerability, which is irrelevant (web3 has an insecure credential storage – but since the pbtc-eth-syncer does not store any credentials, this is no issue).

Status: ✔️ [non issue]

9. 🚧 [minor] 0% test coverage.
   Status: □ [acknowledged] Deprioritized for now.

10. 🚧 [minor] ESLint reports an error and warnings, see Appendix I.
    Status: ✔️ [fixed]

PBTC-ETH-SMART-CONTRACT

1. 🚧 [minor] Multiple calls fail implicitly through SafeMath without error messages, e. g. trying to transfer more than the current balance

   Status: ✔️ [fixed]

2. 🚧 [minor] npm reports 1 low severity vulnerability, which is irrelevant (web3 has an insecure credential storage – but since the pbtc-eth-syncer does not store any credentials, this is no issue).

   Status: ✔️ [non issue]

Appendix A: Test output of `pbtc-enclave > cargo +nightly test`

```
pbtc-enclave > cargo +nightly test

running 483 tests
test base58::tests::test_base58_decode ... ok
test base58::tests::test_base58_encode ... ok
test base58::tests::test_base58_roundtrip ... ok
test btc::btc_crypto::btc_private_key::tests::should_generate_key_from_slice ... ok
test btc::btc_crypto::btc_private_key::tests::should_get_private_key_bytes ... ok
test btc::btc_crypto::btc_private_key::tests::should_generate_random_private_key ...
ok
test btc::btc_crypto::btc_private_key::tests::should_get_private_key_from_wif ... ok
test
btc::btc_crypto::btc_private_key::tests::should_convert_private_key_to_p2pkh_address
... ok
test btc::btc_crypto::btc_private_key::tests::should_get_public_key_slice ... ok
test btc::btc_crypto::btc_private_key::tests::should_sign_hash ... ok
test btc::btc_crypto::btc_private_key::tests::should_get_public_key_from_private ...
ok
test btc::btc_crypto::btc_private_key::tests::should_sign_hash_and_append_hash_type
... ok
test btc::btc_database_utils::tests::existing_block_should_exist_in_db ... ok
test btc::btc_database_utils::tests::existing_key_should_exist_in_db ... ok
test btc::btc_database_utils::tests::non_existing_key_should_not_exist_in_db ... ok
test btc::btc_database_utils::tests::none_existent_block_should_not_exist_in_db ...
ok
test btc::btc_database_utils::tests::should_error_getting_non_existent_special_block
... ok
test
btc::btc_database_utils::tests::should_error_putting_non_existent_block_type_in_db
... ok
test btc::btc_database_utils::tests::should_get_and_put_anchor_block_hash_in_db ...
ok
test btc::btc_database_utils::tests::should_get_and_put_btc_address_in_database ...
ok
test btc::btc_database_utils::tests::should_get_and_put_btc_difficulty_in_db ... ok
test btc::btc_database_utils::tests::should_get_and_put_btc_canon_to_tip_length_in_db
... ok
test btc::btc_database_utils::tests::should_get_and_put_btc_fee_in_db ... ok
test btc::btc_database_utils::tests::should_get_and_put_btc_block_in_db ... ok
test btc::btc_database_utils::tests::should_get_and_put_btc_network_in_db ... ok
test btc::btc_database_utils::tests::should_get_and_put_canon_block_hash_in_db ... ok
test btc::btc_database_utils::tests::should_get_and_put_latest_block_hash_in_db ...
ok
test btc::btc_database_utils::tests::should_get_and_put_linker_hash_in_db ... ok
test btc::btc_database_utils::tests::should_get_and_save_btc_private_key_in_db ... ok
test btc::btc_database_utils::tests::should_get_btc_latest_block_number ... ok
test btc::btc_database_utils::tests::should_get_parent_block ... ok
test btc::btc_database_utils::tests::should_get_special_block_type ... ok
test btc::btc_database_utils::tests::should_maybe_get_btc_block_from_db_if_extant ...
ok
test
btc::btc_database_utils::tests::should_maybe_get_btc_block_from_db_if_none_extant ...
ok
test btc::btc_state::tests::should_add_config_in_state ... ok
test btc::btc_state::tests::should_fail_to_get_eth_block_and_receipts_in_state ... ok
```

```
test btc::btc_state::tests::should_fail_to_get_non_existent_config_in_state ... ok
test btc::btc_state::tests::should_not_be_able_to_overwrite_config_in_state ... ok
test btc::btc_test_utils::tests::should_get_sample_sequential_block_and_ids ... ok
test btc::btc_database_utils::tests::should_not_get_parent_block_if_non_existent ...
ok
test btc::btc_test_utils::tests::should_not_panic_getting_sample_btc_block_json ...
ok
test btc::btc_test_utils::tests::should_not_panic_getting_sample_btc_block_string ...
ok
test btc::btc_test_utils::tests::should_not_panic_getting_testnet_sample_block ... ok
test btc::btc_test_utils::tests::should_not_panic_getting_sample_btc_block ... ok
test btc::btc_transaction::tests::should_serialize_1_input_1_output_tx_correctly ...
ok
test btc::btc_transaction::tests::should_serialize_1_input_2_outputs_tx_correctly ...
ok
test btc::btc_utils::tests::should_calculate_btc_tx_size ... ok
test btc::btc_utils::tests::should_convert_btc_address_to_bytes ... ok
test btc::btc_utils::tests::should_convert_btc_address_to_pub_key_hash_bytes ... ok
test btc::btc_utils::tests::should_convert_bytes_to_btc_address ... ok
test btc::btc_utils::tests::should_create_new_pay_to_pub_key_hash_output ... ok
test btc::btc_utils::tests::should_create_new_tx_output ... ok
test btc::btc_transaction::tests::should_serialize_tx_with_n_inputs_and_n_outputs ...
ok
test btc::btc_database_utils::tests::should_put_hash_in_db ... ok
test btc::btc_utils::tests::should_deserialize_btc_utxo ... ok
test btc::btc_utils::tests::should_get_p2sh_redeem_script_sig ... ok
test btc::btc_utils::tests::should_get_p2sh_script_sig_from_redeem_script ... ok
test btc::btc_utils::tests::should_get_pay_to_pub_key_hash_script ... ok
test btc::btc_utils::tests::should_get_safe_eth_address ... ok
test btc::btc_utils::tests::should_get_script_sig ... ok
test btc::btc_utils::tests::should_get_total_value_of_utxos_and_values ... ok
test btc::btc_utils::tests::should_create_op_return_btc_utxo_and_value_from_tx_output
... ok
test btc::btc_utils::tests::should_create_unsigned_utxo_from_tx ... ok
test btc::btc_utils::tests::should_serde_btc_network_correctly ... ok
test btc::btc_utils::tests::should_serde_minting_params ... ok
test btc::btc_utils::tests::should_serialize_btc_utxo ... ok
test
btc::extract_utxos_from_op_return_txs::tests::should_create_unsigned_utxo_from_tx_out
put ... ok
test
btc::extract_utxos_from_op_return_txs::tests::should_extract_utxos_from_relevant_txs
... ok
test btc::extract_utxos_from_p2sh_txs::tests::should_extract_p2sh_utxos_from_txs ...
ok
test
btc::extract_utxos_from_p2sh_txs::tests::should_extract_p2sh_utxos_from_txs_with_gt_1
_p2sh_output_correctly ... ok
test btc::extract_utxos_from_p2sh_txs::tests::should_maybe_extract_p2sh_utxo ... ok
test
btc::filter_op_return_deposit_txs::tests::external_p2pkh_tx_should_have_output_with_t
arget_script ... ok
test
btc::filter_op_return_deposit_txs::tests::external_p2pkh_tx_should_not_have_input_loc
ked_to_pub_key ... ok
test
btc::filter_op_return_deposit_txs::tests::internal_p2pkh_tx_should_have_input_locked_
to_pub_key ... ok
test
btc::filter_op_return_deposit_txs::tests::internal_p2pkh_tx_should_have_output_with_t
arget_script ... ok
```

```
test btc::filter_op_return_deposit_txs::tests::script_sig_should_contain_pub_key ...
ok
test
btc::filter_op_return_deposit_txs::tests::should_filter_out_internal_p2pkh_deposits
... ok
test
btc::filter_op_return_deposit_txs::tests::should_not_filter_out_external_p2pkh_deposi
ts ... ok
test
btc::filter_p2sh_deposit_txs::tests::address_from_output_should_be_locked_to_pub_key
... ok
test
btc::filter_p2sh_deposit_txs::tests::address_from_wrong_output_should_not_be_locked_t
o_pub_key ... ok
test btc::filter_p2sh_deposit_txs::tests::address_should_be_locked_to_pub_key ... ok
test btc::filter_p2sh_deposit_txs::tests::outputs_address_should_be_in_hash_map ...
ok
test
btc::filter_p2sh_deposit_txs::tests::should_filter_txs_for_outputs_to_addresses_in_ha
sh_map ... ok
test
btc::filter_p2sh_deposit_txs::tests::wrong_address_should_not_be_locked_to_pub_key
... ok
test
btc::filter_p2sh_deposit_txs::tests::wrong_outputs_address_should_not_be_in_hash_map
... ok
test
btc::get_deposit_info_hash_map::tests::should_create_hash_map_from_deposit_info_list
... ok
test btc::btc_database_utils::tests::should_put_special_block_in_db ... ok
test
btc::initialize_btc::is_btc_initialized::tests::should_return_false_if_btc_enc_not_in
itialized ... ok
test
btc::initialize_btc::is_btc_initialized::tests::should_return_true_if_btc_enc_initial
ized ... ok
test btc::parse_btc_block::tests::should_not_panic_deserializing_tx ... ok
test btc::parse_btc_block::tests::should_parse_btc_block_json ... ok
test btc::parse_btc_block::tests::should_parse_deposit_list_json_to_deposit_info ...
ok
test
btc::parse_minting_params_from_op_return_deposits::tests::correct_output_should_be_de
sired_op_return_output ... ok
test btc::btc_utils::tests::should_serde_btc_block_in_db_format ... ok
test btc::btc_utils::tests::should_serde_btc_block_in_db_format_correctly ... ok
test
btc::parse_minting_params_from_op_return_deposits::tests::should_default_to_safe_addr
ess_if_no_op_return ... ok
test
btc::parse_minting_params_from_op_return_deposits::tests::incorrect_output_should_not
_be_desired_op_return ... ok
test
btc::parse_minting_params_from_op_return_deposits::tests::serialized_script_pubkey_sh
ould_be_desired_op_return ... ok
test
btc::parse_minting_params_from_op_return_deposits::tests::should_default_to_safe_addr
ess_if_no_op_return_present ... ok
test
btc::parse_minting_params_from_op_return_deposits::tests::should_get_eth_address_from
_op_return_in_tx_else_safe_address ... ok
```

```
test
btc::parse_minting_params_from_op_return_deposits::tests::should_extract_spender_addr
ess_from_p2pkh_input ... ok
test
btc::parse_minting_params_from_op_return_deposits::tests::should_get_first_deposit_va
lue_from_tx ... ok
test
btc::parse_minting_params_from_op_return_deposits::tests::should_parse_eth_address_fr
om_op_return_script ... ok
test
btc::parse_minting_params_from_p2sh_deposits::tests::should_parse_minting_params_stru
ct_from_p2sh_deposit_tx ... ok
test
btc::parse_minting_params_from_p2sh_deposits::tests::should_parse_minting_params_stru
ct_from_p2sh_deposit_txs ... ok
test
btc::parse_minting_params_from_p2sh_deposits::tests::should_parse_minting_params_stru
ct_from_two_p2sh_deposit_txs ... ok
test btc::sign_transactions::tests::should_get_eth_signatures ... ok
test btc::sign_transactions::tests::should_get_eth_signing_params ... ok
test
btc::utxo_manager::utxo_database_utils::tests::should_be_zero_utxo_balance_when_non_i
n_db ... ok
test
btc::utxo_manager::utxo_database_utils::tests::should_be_zero_utxos_when_non_in_db
... ok
test
btc::utxo_manager::utxo_database_utils::tests::should_decrement_total_utxo_balance_in
_db ... ok
test btc::utxo_manager::utxo_database_utils::tests::should_delete_balance_key ... ok
test btc::utxo_manager::utxo_database_utils::tests::should_delete_first_key ... ok
test btc::utxo_manager::utxo_database_utils::tests::should_delete_last_key ... ok
test
btc::utxo_manager::utxo_database_utils::tests::should_err_when_decrementing_with_unde
rflow ... ok
test
btc::utxo_manager::utxo_database_utils::tests::should_increment_num_of_utxos_in_db
... ok
test
btc::utxo_manager::utxo_database_utils::tests::should_increment_total_utxo_balance_in
_db ... ok
test btc::utxo_manager::utxo_database_utils::tests::should_put_and_get_utxo_in_db ...
ok
test btc::utxo_manager::utxo_database_utils::tests::should_put_num_of_utxos_in_db ...
ok
test
btc::utxo_manager::utxo_database_utils::tests::should_remove_1_utxo_correctly_when_gt
_1_exist ... ok
test btc::utxo_manager::utxo_database_utils::tests::should_remove_last_utxo_correctly
... ok
test btc::utxo_manager::utxo_database_utils::tests::should_save_gt_one_utxo ... ok
test
btc::utxo_manager::utxo_database_utils::tests::should_set_and_get_fist_utxo_pointer
... ok
test
btc::utxo_manager::utxo_database_utils::tests::should_set_and_get_last_utxo_pointer
... ok
test
btc::utxo_manager::utxo_database_utils::tests::should_set_and_get_total_utxo_balance_
from_db ... ok
```

```
test
btc::utxo_manager::utxo_database_utils::tests::should_update_pointer_in_utxo_in_db
... ok
test btc::utxo_manager::utxo_utils::tests::should_get_utxo_db_key ... ok
test btc::utxo_manager::utxo_utils::tests::should_serde_op_return_btc_utxo_and_value
... ok
test btc::utxo_manager::utxo_utils::tests::should_serde_p2sh_btc_utxo_and_value ...
ok
test
btc::utxo_manager::utxo_utils::tests::should_serde_utxo_and_value_with_something_in_t
he_maybe_pointer ... ok
test
btc::parse_minting_params_from_op_return_deposits::tests::should_parse_minting_params
_from_tx ... ok
test
btc::parse_minting_params_from_op_return_deposits::tests::should_parse_minting_params
_from_txs ... ok
test btc::parse_btc_block::tests::should_parse_block_and_tx_json_to_struct ... ok
test btc::validate_btc_block_header::tests::should_validate_btc_block_header ... ok
test btc::validate_btc_block_header::tests::should_error_on_invalid_block ... ok
test btc::validate_btc_difficulty::tests::should_err_if_difficulty_is_below_threshold
... ok
test
btc::validate_btc_difficulty::tests::should_not_err_if_difficulty_is_above_threshold
... ok
test
check_enclave_is_initialized::tests::should_check_enclave_initialized_and_return_arg
... ok
test check_enclave_is_initialized::tests::should_error_if_btc_enclave_not_initialized
... ok
test check_enclave_is_initialized::tests::should_error_if_eth_enclave_not_initialized
... ok
test
check_enclave_is_initialized::tests::should_return_false_if_enclave_not_initialized
... ok
test check_enclave_is_initialized::tests::should_return_true_if_enclave_initialized
... ok
test crypto_utils::test::should_generate_32_random_bytes ... ok
test crypto_utils::test::should_generate_random_private_key ... ok
test crypto_utils::test::should_generate_x_random_bytes ... ok
test crypto_utils::test::should_keccak_hash_bytes ... ok
test database_interface::tests::should_get_bytes_from_db ... ok
test database_interface::tests::should_put_in_db_via_path ... ok
test database_interface::tests::should_remove_bytes_from_db ... ok
test database_utils::tests::should_save_and_get_usize_from_db ... ok
test
eth::add_block_and_receipts_to_database::tests::should_error_if_block_already_in_db
... ok
test
eth::add_block_and_receipts_to_database::tests::should_maybe_add_block_and_receipts_t
o_db ... ok
test eth::calculate_linker_hash::tests::should_calculate_linker_hash_correctly ... ok
test
eth::check_parent_exists::tests::should_err_if_parent_not_in_database_and_anchor_hash
_is_set ... ok
test eth::check_parent_exists::tests::should_return_false_if_parent_not_in_db ... ok
test
eth::check_parent_exists::tests::should_return_state_if_block_parent_exists_in_db_and
_anchor_hash_set ... ok
```

```
test
eth::check_parent_exists::tests::should_return_state_if_parent_exists_in_db_and_ancho
r_hash_not_set ... ok
test eth::check_parent_exists::tests::should_return_true_if_parent_in_db ... ok
test
eth::eth_crypto::eth_private_key::tests::should_create_eth_private_key_from_slice ...
ok
test eth::eth_crypto::eth_private_key::tests::should_create_random_eth_private_key
... ok
test eth::eth_crypto::eth_private_key::tests::should_get_private_key_bytes ... ok
test eth::eth_crypto::eth_private_key::tests::should_sign_message_bytes ... ok
test eth::eth_crypto::eth_private_key::tests::should_sign_message_hash ... ok
test eth::eth_crypto::eth_public_key::tests::should_convert_public_key_to_bytes ...
ok
test eth::eth_crypto::eth_public_key::tests::should_convert_public_key_to_eth_address
... ok
test eth::eth_crypto::eth_public_key::tests::should_get_public_key_from_private ...
ok
test eth::eth_crypto::eth_transaction::tests::should_encode_minting_params ... ok
test eth::eth_crypto::eth_transaction::tests::should_get_signed_eth_smart_contract_tx
... ok
test eth::eth_crypto::eth_transaction::tests::should_get_signed_minting_tx ... ok
test
eth::eth_crypto::eth_transaction::tests::should_get_unsigned_eth_smart_contract_trans
action ... ok
test eth::eth_crypto::eth_transaction::tests::should_get_unsigned_minting_tx ... ok
test
eth::eth_crypto::eth_transaction::tests::should_read_smart_contract_bytecode_from_fil
e ... ok
test eth::eth_crypto::eth_transaction::tests::should_serialize_simple_eth_tx_to_bytes
... ok
test eth::eth_crypto::eth_transaction::tests::should_sign_simple_eth_tx ... ok
test eth::eth_database_utils::tests::existing_key_should_exist_in_db ... ok
test
eth::eth_database_utils::tests::maybe_get_block_should_be_none_if_block_not_extant
... FAILED
test eth::eth_database_utils::tests::non_existing_key_should_not_exist_in_db ... ok
test eth::eth_database_utils::tests::should_get_eth_block_from_db ... FAILED
test eth::eth_database_utils::tests::should_get_eth_pk_from_database ... ok
test eth::eth_database_utils::tests::should_get_eth_smart_contract_address_from_db
... ok
test eth::eth_database_utils::tests::should_get_no_nth_ancestor_if_not_extant ...
FAILED
test
btc::validate_btc_difficulty::tests::should_skip_difficulty_check_if_not_on_mainnet
... ok
test
btc::validate_btc_proof_of_work::tests::should_validate_proof_of_work_in_valid_block
... ok
test btc::validate_btc_merkle_root::tests::should_validate_sample_merkle_root ... ok
test eth::eth_database_utils::tests::should_get_nth_ancestor_if_extant ... test
eth::eth_database_utils::tests::should_get_nth_ancestor_if_extant has been running
for over 60 seconds
test eth::eth_database_utils::tests::should_increment_eth_account_nonce_in_db ...
test eth::eth_database_utils::tests::should_increment_eth_account_nonce_in_db has
been running for over 60 seconds
test eth::eth_database_utils::tests::should_maybe_get_parent_block_if_it_exists ...
test eth::eth_database_utils::tests::should_maybe_get_parent_block_if_it_exists has
been running for over 60 seconds
```

```
test eth::eth_database_utils::tests::should_maybe_get_some_block_if_exists ... test
eth::eth_database_utils::tests::should_maybe_get_some_block_if_exists has been
running for over 60 seconds
test eth::eth_database_utils::tests::should_get_nth_ancestor_if_extant ... ok
test eth::eth_database_utils::tests::should_increment_eth_account_nonce_in_db ... ok
test eth::eth_database_utils::tests::should_maybe_get_parent_block_if_it_exists ...
ok
test eth::eth_database_utils::tests::should_maybe_get_some_block_if_exists ... FAILED
test eth::eth_database_utils::tests::should_put_and_get_eth_address_in_db ... ok
test eth::eth_database_utils::tests::should_put_and_get_eth_hash_in_db ... FAILED
test eth::eth_database_utils::tests::should_put_and_get_public_eth_address_in_db ...
ok
test eth::eth_database_utils::tests::should_put_chain_id_in_db ... ok
test eth::eth_database_utils::tests::should_put_and_get_special_eth_block_in_db ...
FAILED
test eth::eth_database_utils::tests::should_put_and_get_special_eth_hash_in_db ...
FAILED
test eth::eth_database_utils::tests::should_put_eth_gas_price_in_db ... ok
test eth::eth_database_utils::tests::should_return_none_if_no_parent_block_exists ...
FAILED
test eth::eth_database_utils::tests::should_save_nonce_to_db_and_get_nonce_from_db
... ok
test eth::eth_json_codec::tests::should_encode_eth_block_as_json ... ok
test eth::eth_json_codec::tests::should_encode_eth_log_as_json ... ok
test eth::eth_json_codec::tests::should_encode_eth_block_and_receipts_as_json ... ok
test eth::eth_state::tests::should_add_config_in_state ... ok
test eth::eth_json_codec::tests::should_encode_eth_receipt_as_json ... ok
test
eth::eth_state::tests::should_err_when_overwriting_eth_block_and_receipts_in_state
... ok
test eth::eth_state::tests::should_add_eth_block_and_receipts_state ... ok
test eth::eth_state::tests::should_fail_to_get_eth_block_and_receipts_in_state ... ok
test eth::eth_state::tests::should_fail_to_get_non_existent_config_in_state ... ok
test eth::eth_state::tests::should_not_be_able_to_overwrite_config_in_state ... ok
test eth::eth_json_codec::tests::should_decode_block_and_recipts_json_correctly ...
ok
test eth::eth_json_codec::tests::should_encode_eth_block_and_receipts_as_json_bytes
... ok
test eth::eth_test_utils::tests::sample_log_with_desired_topic_should_contain_topic
... ok
test
eth::eth_test_utils::tests::sample_log_without_desired_topic_should_contain_topic ...
ok
test eth::eth_test_utils::tests::sample_logs_with_desired_topic_should_contain_topic
... ok
test
eth::eth_test_utils::tests::sample_logs_without_desired_topic_should_contain_topic
... ok
test
eth::eth_test_utils::tests::sample_receipts_with_desired_topic_should_contain_topic
... ok
test eth::eth_test_utils::tests::should_convert_hex_string_to_nibbles ... ok
test eth::eth_test_utils::tests::should_convert_offset_hex_string_to_nibbles ... ok
test eth::eth_test_utils::tests::should_get_expected_block_correctly ... ok
test eth::eth_test_utils::tests::should_get_expected_log_correctly ... ok
test eth::eth_test_utils::tests::should_get_expected_receipt_correctly ... ok
test eth::eth_test_utils::tests::should_get_sample_cli_args ... ok
test eth::eth_test_utils::tests::should_get_sample_config ... ok
test eth::eth_test_utils::tests::should_get_sample_config_string ... ok
test eth::eth_test_utils::tests::should_get_sample_eth_block_and_receipt_json ... ok
test eth::eth_test_utils::tests::should_get_sample_eth_block_and_receipts ... ok
```

```
test
eth::eth_test_utils::tests::sample_receipts_without_desired_topic_should_not_contain_
topic ... ok
test eth::eth_test_utils::tests::should_get_sample_eth_block_and_receipts_json ... ok
test eth::eth_state::tests::should_get_eth_parent_hash ... ok
test eth::eth_test_utils::tests::should_get_valid_initial_state ... ok
test eth::eth_test_utils::tests::should_get_sample_invalid_block ... ok
test eth::eth_test_utils::tests::should_get_valid_state_with_config ... ok
test eth::eth_state::tests::should_update_eth_block_and_receipts ... ok
test eth::eth_test_utils::tests::should_get_valid_state_with_blocks_and_receipts ...
ok
test
eth::eth_test_utils::tests::should_get_valid_state_with_invalid_block_and_receipts
... ok
test
eth::filter_receipts::tests::sample_log_receipt_with_desired_address_should_return_tr
ue ... ok
test
eth::filter_receipts::tests::sample_logs_without_desired_topic_should_contain_topic
... ok
test
eth::filter_receipts::tests::sample_log_without_desired_address_should_return_false
... ok
test eth::filter_receipts::tests::sample_logs_with_desired_topic_should_contain_topic
... ok
test eth::filter_receipts::tests::should_filter_eth_block_and_receipts ... ok
test
eth::filter_receipts::tests::sample_receipt_without_desired_address_should_return_fal
se ... ok
test eth::filter_receipts::tests::should_filter_receipts_for_topic ... ok
test
eth::filter_receipts::tests::sample_receipt_with_desired_address_should_return_true
... ok
test eth::get_eth_log::tests::should_get_log_from_log_json_correctly ... ok
test eth::get_eth_log::tests::should_get_logs_bloom_from_logs ... ok
test eth::get_eth_log::tests::should_get_logs_bloom_from_logs_correctly ... ok
test eth::get_eth_log::tests::should_get_logs_from_receipt_json ... ok
test
eth::get_linker_hash::tests::get_linker_or_genesis_should_get_genesis_hash_if_linker_
not_set ... ok
test
eth::filter_receipts::tests::should_return_false_if_log_does_not_contain_desired_topi
c ... ok
test eth::filter_receipts::tests::should_return_true_if_log_contains_desired_topic
... ok
test
eth::get_linker_hash::tests::get_linker_or_genesis_should_get_linker_hash_from_db_if_
extant ... ok
test eth::get_linker_hash::tests::should_get_linker_hash_from_db ... ok
test eth::get_linker_hash::tests::should_get_linker_hash_from_db_if_extant ... ok
test eth::get_trie_hash_map::tests::should_get_new_empty_trie_hash_map ... ok
test eth::get_trie_hash_map::tests::should_get_thing_from_trie_hash_map ... ok
test eth::get_trie_hash_map::tests::should_insert_thing_in_trie_hash_map ... ok
test eth::get_trie_hash_map::tests::should_remove_thing_from_trie_hash_map ... ok
test
eth::initialize_eth::generate_eth_contract_address::tests::should_calculate_contract_
address ... ok
test
eth::initialize_eth::is_eth_initialized::tests::should_return_false_if_eth_enc_not_in
itialized ... ok
```

```
test
eth::initialize_eth::is_eth_initialized::tests::should_return_true_if_eth_enc_initial
ized ... ok
test eth::nibble_utils::tests::empty_nibbles_should_have_nibble_length_of_zero ... ok
test eth::nibble_utils::tests::should_append_byte_to_empty_nibble_data_correctly ...
ok
test
eth::nibble_utils::tests::get_common_prefix_nibbles_should_work_if_first_nibbles_are_
shorter ... ok
test
eth::nibble_utils::tests::get_common_prefix_nibbles_should_work_if_second_nibbles_are
_shorter ... ok
test eth::nibble_utils::tests::should_append_byte_to_nibble_data_correctly ... ok
test eth::nibble_utils::tests::should_convert_nibble_i_to_byte_i_in_nibbles_correctly
... ok
test
eth::nibble_utils::tests::should_convert_nibble_i_to_byte_i_in_offset_nibbles_correct
ly ... ok
test eth::nibble_utils::tests::should_convert_nibble_to_usize ... ok
test eth::nibble_utils::tests::should_convert_nibbles_to_bytes_correctly ... ok
test eth::nibble_utils::tests::should_convert_offset_nibbles_to_bytes_correctly ...
ok
test
eth::nibble_utils::tests::should_convert_slice_with_nibble_at_index_one_correctly ...
ok
test
eth::nibble_utils::tests::should_convert_slice_with_nibble_at_index_zero_correctly
... ok
test eth::nibble_utils::tests::should_convert_zero_nibble_to_usize ... ok
test
eth::nibble_utils::tests::should_display_nibble_starting_at_index_one_string_correctl
y ... ok
test
eth::nibble_utils::tests::should_display_nibble_starting_at_index_zero_string_correct
ly ... ok
test eth::nibble_utils::tests::should_err_if_attempting_to_get_out_of_bounds_nibble
... ok
test
eth::nibble_utils::tests::should_get_all_nibbles_with_first_nibble_at_index_one_corre
ctly ... ok
test
eth::nibble_utils::tests::should_get_all_nibbles_with_first_nibble_at_index_zero_corr
ectly ... ok
test eth::nibble_utils::tests::should_get_appending_byte_from_nibble_correctly ... ok
test eth::nibble_utils::tests::should_get_byte_containing_nibble_at_i_correctly ...
ok
test
eth::nibble_utils::tests::should_get_common_prefix_nibbles_recursively_correctly_when
_one_offset ... ok
test
eth::nibble_utils::tests::should_get_common_prefix_correctly_when_one_is_substring_of
_other ... ok
test
eth::nibble_utils::tests::should_get_common_prefix_nibbles_recursively_when_both_not_
offset ... ok
test
eth::nibble_utils::tests::should_get_common_prefix_nibbles_recursively_when_both_offs
et ... ok
test
eth::nibble_utils::tests::should_get_common_prefix_nibbles_recursively_when_same_and_
offset ... ok
```

```
test
eth::nibble_utils::tests::should_get_common_prefix_nibbles_recursively_when_same_and_
not_offset ... ok
test
eth::nibble_utils::tests::should_get_common_prefix_when_no_common_prefix_and_both_off
set ... ok
test
eth::nibble_utils::tests::should_get_common_prefix_when_no_common_prefix_and_neither_
offset ... ok
test
eth::nibble_utils::tests::should_get_common_prefix_when_no_common_prefix_and_one_offs
et ... ok
test eth::nibble_utils::tests::should_get_high_nibble_from_byte_correctly ... ok
test eth::nibble_utils::tests::should_get_low_nibble_from_byte_correctly ... ok
test
eth::nibble_utils::tests::should_get_common_prefixy_when_one_is_substring_of_other_an
d_offset ... ok
test eth::nibble_utils::tests::should_get_zero_nibble ... ok
test eth::nibble_utils::tests::should_mask_higher_nibble_correctly ... ok
test eth::nibble_utils::tests::should_merge_nibbles_from_bytes_correctly ... ok
test eth::nibble_utils::tests::should_prefix_nibble_with_byte_correctly ... ok
test eth::nibble_utils::tests::should_prefix_offset_nibble_with_byte_correctly ... ok
test eth::nibble_utils::tests::should_push_nibble_into_empty_nibbles_correctly ... ok
test eth::nibble_utils::tests::should_push_nibble_into_nibbles_correctly ... ok
test
eth::nibble_utils::tests::should_push_nibble_into_nibbles_of_length_one_correctly ...
ok
test eth::nibble_utils::tests::should_remove_first_byte_from_nibbles ... ok
test eth::nibble_utils::tests::should_push_nibble_into_offset_nibbles_correctly ...
ok
test eth::nibble_utils::tests::should_remove_first_byte_of_single_nibble_correctly
... ok
test eth::nibble_utils::tests::should_remove_first_byte_from_offest_nibbles ... ok
test eth::nibble_utils::tests::should_remove_first_nibble_from_offset_nibbles ... ok
test eth::nibble_utils::tests::should_remove_first_nibble_from_nibbles ... ok
test eth::nibble_utils::tests::should_remove_first_nibble_if_only_one_nibble ... ok
test eth::nibble_utils::tests::should_remove_last_byte_from_empty_nibble_correctly
... ok
test eth::nibble_utils::tests::should_remove_last_byte_from_nibbles_correctly ... ok
test eth::nibble_utils::tests::should_remove_last_byte_from_offset_nibbles_correctly
... ok
test eth::nibble_utils::tests::should_remove_last_byte_from_single_nibble_correctly
... ok
test eth::nibble_utils::tests::should_replace_byte_in_nibbles_correctly ... ok
test eth::nibble_utils::tests::should_replace_byte_in_offset_nibbles_correctly ... ok
test eth::nibble_utils::tests::should_replace_high_nibble_in_byte_correctly ... ok
test eth::nibble_utils::tests::should_replace_high_offset_nibble_in_byte_correctly
... ok
test eth::nibble_utils::tests::should_replace_low_nibble_in_byte_correctly ... ok
test eth::nibble_utils::tests::should_replace_low_offset_nibble_in_byte_correctly ...
ok
test
eth::nibble_utils::tests::should_replace_nibble_at_nibble_index_in_nibbles_correctly
... ok
test
eth::nibble_utils::tests::should_replace_nibble_at_nibble_index_in_offset_nibbles_cor
rectly ... ok
test
eth::nibble_utils::tests::should_replace_offset_nibble_at_nibble_index_in_nibbles_cor
rectly ... ok
```

```
test
eth::nibble_utils::tests::should_return_empty_nibbles_when_slicing_with_i_greater_tha
n_length ... ok
test
eth::nibble_utils::tests::should_replace_offset_nibble_at_nibble_index_in_offset_nibb
les ... ok
test
eth::nibble_utils::tests::should_set_first_nibble_flag_in_nibbles_to_one_correctly
... ok
test
eth::nibble_utils::tests::should_set_first_nibble_flag_in_nibbles_to_zero_correctly
... ok
test eth::nibble_utils::tests::should_shift_bytes_in_vec_left_one_nibble ... ok
test eth::nibble_utils::tests::should_shift_bytes_in_vec_right_one_nibble ... ok
test eth::nibble_utils::tests::should_shift_nibble_left_correctly ... ok
test eth::nibble_utils::tests::should_shift_no_bytes_in_vec_left_one_nibble ... ok
test eth::nibble_utils::tests::should_shift_nibble_right_correctly ... ok
test eth::nibble_utils::tests::should_shift_no_bytes_in_vec_right_one_nibble ... ok
test eth::nibble_utils::tests::should_shift_one_byte_in_vec_left_one_nibble ... ok
test eth::nibble_utils::tests::should_shift_one_byte_in_vec_right_one_nibble ... ok
test eth::nibble_utils::tests::should_slice_nibbles_at_byte_index_correctly ... ok
test eth::nibble_utils::tests::should_slice_nibbles_at_even_nibble_index_correctly
... ok
test eth::nibble_utils::tests::should_slice_nibbles_at_nibble_index_of_one_correctly
... ok
test eth::nibble_utils::tests::should_slice_nibbles_at_odd_nibble_index_correctly ...
ok
test eth::nibble_utils::tests::should_slice_nibbles_at_zero_nibble_index_correctly
... ok
test eth::nibble_utils::tests::should_slice_offset_nibbles_at_byte_index_correctly
... ok
test
eth::nibble_utils::tests::should_slice_offset_nibbles_at_even_nibble_index_correctly
... ok
test
eth::nibble_utils::tests::should_slice_offset_nibbles_at_nibble_index_of_one_correctl
y ... ok
test
eth::nibble_utils::tests::should_slice_offset_nibbles_at_zero_nibble_index_correctly
... ok
test
eth::nibble_utils::tests::should_slice_ofset_nibbles_at_odd_nibble_index_correctly
... ok
test eth::nibble_utils::tests::should_split_at_first_nibble_correctly ... ok
test
eth::nibble_utils::tests::should_split_at_first_nibble_from_empty_nibbles_correctly
... ok
test
eth::nibble_utils::tests::should_split_at_first_nibble_from_single_nibbles_correctly
... ok
test eth::parse_burn_event_params::tests::burn_event_log_should_be_burn_event ...
FAILED
test eth::parse_burn_event_params::tests::non_burn_event_log_should_not_be_burn_event
... FAILED
test
eth::parse_burn_event_params::tests::should_parse_amount_and_address_tuples_from_rece
ipt ... FAILED
test eth::parse_burn_event_params::tests::should_parse_burn_event_params_from_block
... FAILED
test eth::parse_burn_event_params::tests::should_parse_btc_address_from_log ...
FAILED
```

```
test eth::parse_burn_event_params::tests::should_parse_burn_amount_from_log ...
FAILED
test eth::parse_eth_block::tests::should_parse_eth_block_json_to_eth_block ... ok
test
eth::parse_burn_event_params::tests::should_parse_burn_event_params_from_log_and_rece
ipt ... FAILED
test eth::parse_burn_event_params::tests::should_parse_p2sh_btc_address_from_log ...
FAILED
test eth::parse_eth_block_and_receipts::tests::should_parse_eth_block_and_receipts
... ok
test
eth::parse_eth_block_and_receipts::tests::should_parse_eth_block_and_receipts_json_st
ring ... ok
test eth::parse_eth_receipt::tests::should_parse_eth_receipt_json ... ok
test
eth::parse_eth_block_and_receipts::tests::should_parse_eth_block_and_receipts_json
... ok
test
eth::path_codec::tests::should_decode_even_path_to_nibbles_and_extension_node_type_co
rrectly ... ok
test
eth::parse_eth_block_and_receipts::tests::should_parse_eth_block_and_receipts_and_put
_in_state ... ok
test
eth::path_codec::tests::should_decode_even_path_to_nibbles_and_leaf_node_type_correct
ly ... ok
test
eth::path_codec::tests::should_decode_odd_length_extension_path_to_nibbles_correctly
... ok
test eth::path_codec::tests::should_decode_odd_length_leaf_path_to_nibbles_correctly
... ok
test
eth::path_codec::tests::should_decode_odd_path_to_nibbles_and_extension_node_type_cor
rectly ... ok
test
eth::path_codec::tests::should_decode_odd_path_to_nibbles_and_leaf_node_type_correctl
y ... ok
test eth::path_codec::tests::should_encode_even_length_extension_path_correctly ...
ok
test eth::path_codec::tests::should_encode_even_length_leaf_path_correctly ... ok
test eth::path_codec::tests::should_encode_extension_path_from_nibbles_correctly ...
ok
test eth::parse_eth_receipt::tests::should_parse_eth_receipt_jsons ... ok
test
eth::path_codec::tests::should_encode_extension_path_from_offset_nibbles_correctly
... ok
test eth::path_codec::tests::should_encode_leaf_path_from_nibbles_correctly ... ok
test eth::path_codec::tests::should_encode_leaf_path_from_offset_nibbles_correctly
... ok
test eth::path_codec::tests::should_encode_odd_length_extension_path_correctly ... ok
test eth::path_codec::tests::should_encode_odd_length_leaf_path_correctly ... ok
test eth::path_codec::tests::should_error_when_decoding_a_wrongly_encoded_path ... ok
test
eth::remove_receipts_from_canon_block::tests::should_remove_receipts_from_block_and_r
eceipts ... ok
test eth::rlp_codec::tests::should_encode_tx_receipt ... ok
test eth::rlp_codec::tests::should_encode_tx_receipt_of_0 ... ok
test eth::rlp_codec::tests::should_get_encoded_receipt_and_hash_tuple ... ok
test eth::rlp_codec::tests::should_get_encoded_receipts_and_hash_tuples ... ok
```

```
test
eth::remove_receipts_from_canon_block::tests::should_not_err_if_canon_has_no_receipts
... ok
test eth::rlp_codec::tests::should_rlp_encode_receipt ... ok
test eth::trie::tests::should_get_empty_trie ... ok
test eth::rlp_codec::tests::should_rlp_encode_block ... ok
test eth::trie::tests::should_put_node_in_trie_hash_map_in_trie ... ok
test eth::trie::tests::should_put_thing_in_empty_trie ... ok
test eth::trie::tests::should_put_invalid_sample_receipts_in_trie_correctly ... ok
test eth::trie::tests::should_remove_node_from_trie_hash_map ... ok
test eth::trie::tests::should_sum_length_of_key_so_far_in_found_stack ... ok
test eth::trie::tests::should_update_root_hash ... ok
test eth::trie::tests::should_validate_root_hash_correctly ... FAILED
test eth::trie_nodes::tests::should_fail_to_get_non_existing_node_from_db ... ok
test
eth::trie_nodes::tests::should_fail_to_update_branch_of_non_branch_node_correctly ...
ok
test eth::trie_nodes::tests::should_get_branch_node_from_trie_hash_map ... ok
test eth::trie_nodes::tests::should_get_branch_node_hash_correctly ... ok
test eth::trie_nodes::tests::should_get_extension_node_correctly ... ok
test eth::trie_nodes::tests::should_get_extension_node_from_trie_hash_map ... ok
test eth::trie_nodes::tests::should_get_extension_node_hash_correctly ... ok
test eth::trie::tests::should_put_valid_sample_receipts_in_trie_correctly ... ok
test eth::trie_nodes::tests::should_get_key_from_extension_node ... ok
test eth::trie_nodes::tests::should_get_key_from_leaf_node ... ok
test eth::trie_nodes::tests::should_get_key_length_of_branch_node ... ok
test eth::trie_nodes::tests::should_get_key_length_of_extension_node ... ok
test eth::trie_nodes::tests::should_get_key_length_of_leaf_node ... ok
test eth::trie_nodes::tests::should_get_leaf_node_hash_correctly ... ok
test eth::trie_nodes::tests::should_get_leaf_node_from_trie_hash_map ... ok
test eth::trie_nodes::tests::should_get_new_branch_with_no_value_correctly ... ok
test eth::trie_nodes::tests::should_get_new_branch_with_value_correctly ... ok
test eth::trie_nodes::tests::should_get_new_leaf_node_correctly ... ok
test eth::trie_nodes::tests::should_get_no_key_from_branch_node ... ok
test eth::trie_nodes::tests::should_get_value_from_branch_node ... ok
test eth::trie_nodes::tests::should_get_value_from_extension_node ... ok
test eth::trie_nodes::tests::should_get_value_from_leaf_node ... ok
test eth::trie_nodes::tests::should_rlp_decode_branch_node ... ok
test eth::trie_nodes::tests::should_rlp_decode_extension_node ... ok
test eth::trie_nodes::tests::should_rlp_decode_leaf_node ... ok
test eth::trie_nodes::tests::should_rlp_encode_branch_node_correctly ... ok
test eth::trie_nodes::tests::should_rlp_encode_extension_node_correctly ... ok
test eth::trie_nodes::tests::should_rlp_encode_leaf_node_correctly ... ok
test eth::trie_nodes::tests::should_update_branch_at_index_correctly ... ok
test
eth::remove_receipts_from_canon_block::tests::should_remove_receipts_from_canon_block
... ok
test eth::eth_test_utils::tests::should_get_sequential_block_and_receipts ... ok
test eth::update_eth_canon_block_hash::tests::should_maybe_update_canon_block_hash
... ok
test
eth::update_eth_canon_block_hash::tests::should_not_maybe_update_canon_block_hash ...
ok
test
eth::update_eth_canon_block_hash::tests::should_return_block_if_nth_ancestor_of_lates
t_block_exists ... ok
test
eth::update_eth_canon_block_hash::tests::should_return_false_if_canon_block_does_not_
require_updating ... ok
```

```
test
eth::update_eth_canon_block_hash::tests::should_return_none_if_nth_ancestor_of_latest
_block_does_not_exist ... ok
test
eth::update_eth_canon_block_hash::tests::should_return_true_if_canon_block_requires_u
pdating ... ok
test eth::update_eth_linker_hash::tests::should_get_new_linker_hash ... ok
test eth::update_eth_linker_hash::tests::should_get_parent_of_canon_if_extant ... ok
test
eth::update_eth_linker_hash::tests::should_maybe_update_linker_hash_if_canon_parent_e
xtant ... ok
test
eth::update_latest_block_hash::tests::should_return_false_if_block_is_not_subsequent
... ok
test eth::update_eth_linker_hash::tests::should_not_get_parent_of_canon_if_extant ...
ok
test eth::update_latest_block_hash::tests::should_return_true_if_block_is_subsequent
... ok
test eth::validate_block::tests::invalid_block_header_should_return_true ... ok
test eth::validate_block::tests::should_fail_to_validate_invalid_block_in_state ...
ok
test eth::validate_block::tests::should_hash_block ... ok
test eth::validate_block::tests::should_validate_block_in_state ... ok
test eth::validate_block::tests::valid_block_header_should_return_true ... ok
test eth::validate_receipts::tests::should_get_receipts_root_from_receipts ... ok
test eth::validate_receipts::tests::should_not_validate_invalid_receipts_in_state ...
ok
test
eth::validate_receipts::tests::should_return_false_if_receipts_root_is_not_correct
... ok
test eth::validate_receipts::tests::should_return_true_if_receipts_root_is_correct
... ok
test eth::validate_receipts::tests::should_validate_receipts_in_state ... ok
test get_cli_args::tests::should_read_from_file_and_update_cli_args_block_if_flag_set
... ok
test get_cli_args::tests::should_update_block_in_cli_args ... ok
test
eth::update_eth_linker_hash::tests::should_not_update_linker_hash_if_canon_parent_not
_extant ... ok
test
eth::update_latest_block_hash::tests::should_not_update_latest_block_hash_if_not_subs
equent ... ok
test
eth::update_latest_block_hash::tests::should_update_latest_block_hash_if_subsequent
... ok
test get_config::tests::should_parse_config_file_to_config_json ... ok
test get_config::tests::should_parse_config_json_to_config ... ok
test initialize_logger::tests::should_get_log_path ... ok
test utils::tests::invalid_eth_addresses_should_be_invalid ... ok
test utils::tests::should_convert_bytes_to_u64 ... ok
test utils::tests::should_convert_bytes_to_h256 ... ok
test utils::tests::should_convert_bytes_to_usize ... ok
test utils::tests::should_convert_decimal_string_to_u256 ... ok
test utils::tests::should_convert_eth_address_to_padded_hex ... ok
test get_config::tests::should_read_config_from_file ... ok
test utils::tests::should_convert_h256_to_prefixed_hex_correctly ... ok
test utils::tests::should_convert_h256_to_bytes ... ok
test utils::tests::should_convert_hex_strings_to_h256s ... ok
test utils::tests::should_convert_hex_to_address_correcty ... ok
test utils::tests::should_convert_hex_to_h256_correctly ... ok
test utils::tests::should_convert_hex_to_u256_correctly ... ok
```

```
test utils::tests::should_convert_u256_to_padded_hex ... ok
test utils::tests::should_convert_u64_to_bytes ... ok
test utils::tests::should_convert_prefixed_hex_to_bytes_correctly ... ok
test utils::tests::should_convert_unprefixed_hex_to_bytes_correctly ... ok
test utils::tests::should_convert_usize_to_bytes ... ok
test utils::tests::should_decode_none_prefixed_hex_correctly ... ok
test utils::tests::should_decode_prefixed_hex_correctly ... ok
test utils::tests::should_error_converting_too_few_bytes_to_u64 ... ok
test utils::tests::should_error_converting_too_many_bytes_to_u64 ... ok
test utils::tests::should_fail_to_convert_invalid_hex_to_h256_correctly ... ok
test utils::tests::should_fail_to_convert_long_hex_to_h256_correctly ... ok
test utils::tests::should_fail_to_convert_non_decimal_string_to_u256 ... ok
test utils::tests::should_get_no_overwrite_err_string ... ok
test utils::tests::should_fail_to_convert_short_hex_to_h256_correctly ... ok
test utils::tests::should_get_no_state_err_string ... ok
test utils::tests::should_left_pad_string_with_zero_correctly ... ok
test utils::tests::should_not_strip_missing_hex_prefix_correctly ... ok
test utils::tests::should_strip_hex_prefix_correctly ... ok
test utils::tests::should_strip_newline_chars ... ok
test utils::tests::valid_eth_address_should_be_valid ... ok

failures:

----
eth::eth_database_utils::tests::maybe_get_block_should_be_none_if_block_not_extant
stdout ----
thread
'eth::eth_database_utils::tests::maybe_get_block_should_be_none_if_block_not_extant'
panicked at 'called `Result::unwrap()` on an `Err` value: Custom("✘ Cannot find
sample-eth-block-and-receipts-json file!")', src/libcore/result.rs:1187:5
note: run with `RUST_BACKTRACE=1` environment variable to display a backtrace.

---- eth::eth_database_utils::tests::should_get_eth_block_from_db stdout ----
thread 'eth::eth_database_utils::tests::should_get_eth_block_from_db' panicked at
'called `Result::unwrap()` on an `Err` value: Custom("✘ Cannot find
sample-eth-block-and-receipts-json file!")', src/libcore/result.rs:1187:5

---- eth::eth_database_utils::tests::should_get_no_nth_ancestor_if_not_extant stdout
----
thread 'eth::eth_database_utils::tests::should_get_no_nth_ancestor_if_not_extant'
panicked at 'called `Result::unwrap()` on an `Err` value: Custom("✘ Cannot find
sample-eth-block-and-receipts-json file!")', src/libcore/result.rs:1187:5

---- eth::eth_database_utils::tests::should_maybe_get_some_block_if_exists stdout
----
thread 'eth::eth_database_utils::tests::should_maybe_get_some_block_if_exists'
panicked at 'called `Result::unwrap()` on an `Err` value: Custom("✘ Cannot find
sample-eth-block-and-receipts-json file!")', src/libcore/result.rs:1187:5

---- eth::eth_database_utils::tests::should_put_and_get_eth_hash_in_db stdout ----
thread 'eth::eth_database_utils::tests::should_put_and_get_eth_hash_in_db' panicked
at 'called `Result::unwrap()` on an `Err` value: Custom("✘ Cannot find
sample-eth-block-and-receipts-json file!")', src/libcore/result.rs:1187:5

---- eth::eth_database_utils::tests::should_put_and_get_special_eth_block_in_db
stdout ----
thread 'eth::eth_database_utils::tests::should_put_and_get_special_eth_block_in_db'
panicked at 'called `Result::unwrap()` on an `Err` value: Custom("✘ Cannot find
sample-eth-block-and-receipts-json file!")', src/libcore/result.rs:1187:5
```

```
---- eth::eth_database_utils::tests::should_put_and_get_special_eth_hash_in_db stdout
----
thread 'eth::eth_database_utils::tests::should_put_and_get_special_eth_hash_in_db'
panicked at 'called `Result::unwrap()` on an `Err` value: Custom("✘ Cannot find
sample-eth-block-and-receipts-json file!")', src/libcore/result.rs:1187:5

---- eth::eth_database_utils::tests::should_return_none_if_no_parent_block_exists
stdout ----
thread 'eth::eth_database_utils::tests::should_return_none_if_no_parent_block_exists'
panicked at 'called `Result::unwrap()` on an `Err` value: Custom("✘ Cannot find
sample-eth-block-and-receipts-json file!")', src/libcore/result.rs:1187:5

---- eth::parse_burn_event_params::tests::burn_event_log_should_be_burn_event stdout
----
thread 'eth::parse_burn_event_params::tests::burn_event_log_should_be_burn_event'
panicked at 'called `Result::unwrap()` on an `Err` value: Custom("✘ Cannot find
sample-eth-block-and-receipts-json file!")', src/libcore/result.rs:1187:5

---- eth::parse_burn_event_params::tests::non_burn_event_log_should_not_be_burn_event
stdout ----
thread
'eth::parse_burn_event_params::tests::non_burn_event_log_should_not_be_burn_event'
panicked at 'called `Result::unwrap()` on an `Err` value: Custom("✘ Cannot find
sample-eth-block-and-receipts-json file!")', src/libcore/result.rs:1187:5

----
eth::parse_burn_event_params::tests::should_parse_amount_and_address_tuples_from_rece
ipt stdout ----
thread
'eth::parse_burn_event_params::tests::should_parse_amount_and_address_tuples_from_rec
eipt' panicked at 'called `Result::unwrap()` on an `Err` value: Custom("✘ Cannot find
sample-eth-block-and-receipts-json file!")', src/libcore/result.rs:1187:5

---- eth::parse_burn_event_params::tests::should_parse_burn_event_params_from_block
stdout ----
thread
'eth::parse_burn_event_params::tests::should_parse_burn_event_params_from_block'
panicked at 'called `Result::unwrap()` on an `Err` value: Custom("✘ Cannot find
sample-eth-block-and-receipts-json file!")', src/libcore/result.rs:1187:5

---- eth::parse_burn_event_params::tests::should_parse_btc_address_from_log stdout
----
thread 'eth::parse_burn_event_params::tests::should_parse_btc_address_from_log'
panicked at 'called `Result::unwrap()` on an `Err` value: Custom("✘ Cannot find
sample-eth-block-and-receipts-json file!")', src/libcore/result.rs:1187:5

---- eth::parse_burn_event_params::tests::should_parse_burn_amount_from_log stdout
----
thread 'eth::parse_burn_event_params::tests::should_parse_burn_amount_from_log'
panicked at 'called `Result::unwrap()` on an `Err` value: Custom("✘ Cannot find
sample-eth-block-and-receipts-json file!")', src/libcore/result.rs:1187:5

----
eth::parse_burn_event_params::tests::should_parse_burn_event_params_from_log_and_rece
ipt stdout ----
thread
'eth::parse_burn_event_params::tests::should_parse_burn_event_params_from_log_and_rec
eipt' panicked at 'called `Result::unwrap()` on an `Err` value: Custom("✘ Cannot find
sample-eth-block-and-receipts-json file!")', src/libcore/result.rs:1187:5
```

```
---- eth::parse_burn_event_params::tests::should_parse_p2sh_btc_address_from_log
stdout ----
thread 'eth::parse_burn_event_params::tests::should_parse_p2sh_btc_address_from_log'
panicked at 'called `Result::unwrap()` on an `Err` value: Custom("✘ Cannot find
sample-eth-block-and-receipts-json file!")', src/libcore/result.rs:1187:5

---- eth::trie::tests::should_validate_root_hash_correctly stdout ----
thread 'eth::trie::tests::should_validate_root_hash_correctly' panicked at 'called
`Result::unwrap()` on an `Err` value: Custom("✘ Cannot find
sample-eth-block-and-receipts-json file!")', src/libcore/result.rs:1187:5


failures:

eth::eth_database_utils::tests::maybe_get_block_should_be_none_if_block_not_extant
    eth::eth_database_utils::tests::should_get_eth_block_from_db
    eth::eth_database_utils::tests::should_get_no_nth_ancestor_if_not_extant
    eth::eth_database_utils::tests::should_maybe_get_some_block_if_exists
    eth::eth_database_utils::tests::should_put_and_get_eth_hash_in_db
    eth::eth_database_utils::tests::should_put_and_get_special_eth_block_in_db
    eth::eth_database_utils::tests::should_put_and_get_special_eth_hash_in_db
    eth::eth_database_utils::tests::should_return_none_if_no_parent_block_exists
    eth::parse_burn_event_params::tests::burn_event_log_should_be_burn_event
    eth::parse_burn_event_params::tests::non_burn_event_log_should_not_be_burn_event

eth::parse_burn_event_params::tests::should_parse_amount_and_address_tuples_from_rece
ipt
    eth::parse_burn_event_params::tests::should_parse_btc_address_from_log
    eth::parse_burn_event_params::tests::should_parse_burn_amount_from_log
    eth::parse_burn_event_params::tests::should_parse_burn_event_params_from_block

eth::parse_burn_event_params::tests::should_parse_burn_event_params_from_log_and_rece
ipt
    eth::parse_burn_event_params::tests::should_parse_p2sh_btc_address_from_log
    eth::trie::tests::should_validate_root_hash_correctly

test result: FAILED. 466 passed; 17 failed; 0 ignored; 0 measured; 0 filtered out

error: test failed, to rerun pass '--lib'
```

Appendix B: Output of `pbtc-enclave > cargo outdated`

```
pbtc-enclave > cargo outdated

Name                                Project  Compat                      Latest
Kind         Platform

----                                -------  ------                      ------
----         --------

aho-corasick->memchr                2.2.1    2.3.2                       2.3.2
Normal       ---

arrayvec->nodrop                    0.1.13   Removed                     Removed
Normal       ---

atty->libc                          0.2.62   0.2.66                      0.2.66
Normal       cfg(unix)

backtrace->backtrace-sys            0.1.31   0.1.32                      0.1.32
Normal       ---

backtrace->backtrace-sys            0.1.31   Removed                     Removed
Normal       ---

backtrace->cfg-if                   0.1.10   Removed                     Removed
Normal       ---

backtrace->libc                     0.2.62   0.2.66                      0.2.66
Normal       ---

backtrace->libc                     0.2.62   Removed                     Removed
Normal       ---

backtrace->rustc-demangle           0.1.16   Removed                     Removed
Normal       ---

backtrace-sys->cc                   1.0.41   1.0.50                      ---
Build        ---

backtrace-sys->cc                   1.0.41   Removed                     Removed
Build        ---

backtrace-sys->libc                 0.2.62   0.2.66                      0.2.66
Normal       ---

backtrace-sys->libc                 0.2.62   Removed                     Removed
Normal       ---

base64->byteorder                   1.3.2    1.3.4                       1.3.4
Normal       ---

base64->byteorder                   1.3.2    Removed                     Removed
Normal       ---

base64->safemem                     0.3.2    0.3.3                       0.3.3
Normal       ---

bindgen->bitflags                   1.2.0    1.2.1                       1.2.1
Normal       ---
```

```
bindgen->cexpr                      0.3.5    0.3.6                      0.3.6
Normal       ---

bindgen->regex                      1.3.1    1.3.4                      1.3.4
Normal       ---

bitcoin->bech32                     0.7.1    0.7.2                      0.7.2
Normal       ---

bitcoin->bitcoin_hashes             0.7.1    0.7.4                      0.7.4
Normal       ---

bitcoin->byteorder                  1.3.2    1.3.4                      1.3.4
Normal       ---

bitcoin->secp256k1                  0.15.0   ---                        0.15.5
Normal       ---

bitcoin_hashes                      0.7.1    0.7.4                      0.7.4
Normal       ---

bitcoin_hashes->byteorder           1.3.2    Removed                    Removed
Normal       ---

bitcoin_hashes->serde               1.0.101  Removed                    Removed
Normal       ---

blake2b_simd->arrayref              0.3.5    0.3.6                      0.3.6
Normal       ---

blake2b_simd->arrayvec              0.4.11   0.5.1                      0.5.1
Normal       ---

blake2b_simd->constant_time_eq      0.1.4    0.1.5                      0.1.5
Normal       ---

block-buffer->arrayref              0.3.5    0.3.6                      0.3.6
Normal       ---

byteorder                           1.3.2    1.3.4                      1.3.4
Normal       ---

c2-chacha->lazy_static              1.4.0    Removed                    Removed
Normal       ---

c2-chacha->ppv-lite86               0.2.5    0.2.6                      0.2.6
Normal       ---

cc->rayon                           1.2.1    Removed                    1.3.0
Normal       ---

cc->rayon                           1.2.1    Removed                    Removed
Normal       ---

chrono                              0.4.9    0.4.10                     0.4.10
Normal       ---

chrono->libc                        0.2.62   Removed                    Removed
Normal       ---

chrono->num-integer                 0.1.41   0.1.42                     0.1.42
Normal       ---
```

```
chrono->num-traits                    0.2.8    0.2.11                        0.2.11
Normal       ---

clang-sys->libc                       0.2.62   0.2.66                        0.2.66
Normal       ---

clap->atty                            0.2.13   0.2.14                        0.2.14
Normal       ---

clap->bitflags                        1.2.0    1.2.1                         1.2.1
Normal       ---

clap->unicode-width                   0.1.6    0.1.7                         0.1.7
Normal       ---

cloudabi->bitflags                    1.2.0    1.2.1                         Removed
Normal       ---

cloudabi->bitflags                    1.2.0    Removed                       Removed
Normal       ---

crossbeam-deque->crossbeam-epoch      0.8.0    Removed                       ---
Normal       ---

crossbeam-deque->crossbeam-epoch      0.8.0    Removed                       Removed
Normal       ---

crossbeam-deque->crossbeam-utils      0.7.0    Removed                       ---
Normal       ---

crossbeam-deque->crossbeam-utils      0.7.0    Removed                       Removed
Normal       ---

crossbeam-epoch->autocfg              0.1.6    Removed                       0.1.7
Build        ---

crossbeam-epoch->autocfg              0.1.6    Removed                       Removed
Build        ---

crossbeam-epoch->cfg-if               0.1.10   Removed                       ---
Normal       ---

crossbeam-epoch->cfg-if               0.1.10   Removed                       Removed
Normal       ---

crossbeam-epoch->crossbeam-utils      0.7.0    Removed                       ---
Normal       ---

crossbeam-epoch->crossbeam-utils      0.7.0    Removed                       Removed
Normal       ---

crossbeam-epoch->lazy_static          1.4.0    Removed                       ---
Normal       ---

crossbeam-epoch->lazy_static          1.4.0    Removed                       Removed
Normal       ---

crossbeam-epoch->memoffset            0.5.3    Removed                       ---
Normal       ---

crossbeam-epoch->memoffset            0.5.3    Removed                       Removed
Normal       ---
```

```
crossbeam-epoch->scopeguard          1.0.0    Removed                        ---
Normal       ---

crossbeam-epoch->scopeguard          1.0.0    Removed                        Removed
Normal       ---

crossbeam-queue->crossbeam-utils     0.7.0    Removed                        ---
Normal       ---

crossbeam-queue->crossbeam-utils     0.7.0    Removed                        Removed
Normal       ---

crossbeam-utils->autocfg             0.1.6    Removed                        0.1.7
Build        ---

crossbeam-utils->autocfg             0.1.6    Removed                        Removed
Build        ---

crossbeam-utils->cfg-if              0.1.10   Removed                        ---
Normal       ---

crossbeam-utils->cfg-if              0.1.10   Removed                        Removed
Normal       ---

crossbeam-utils->lazy_static         1.4.0    Removed                        ---
Normal       ---

crossbeam-utils->lazy_static         1.4.0    Removed                        Removed
Normal       ---

crypto-mac->constant_time_eq         0.1.4    0.1.5                          0.1.5
Normal       ---

dirs-sys->libc                       0.2.62   0.2.66                         0.2.66
Normal       cfg(unix)

dirs-sys->redox_users                0.3.1    0.3.4                          0.3.4
Normal       cfg(target_os = "redox")

docopt->regex                        1.3.1    1.3.4                          1.3.4
Normal       ---

docopt->serde                        1.0.101  1.0.104                        1.0.104
Normal       ---

docopt->strsim                       0.9.2    0.9.3                          0.9.3
Normal       ---

env_logger->atty                     0.2.13   0.2.14                         0.2.14
Normal       ---

env_logger->regex                    1.3.1    1.3.4                          1.3.4
Normal       ---

env_logger->termcolor                1.0.5    1.1.0                          1.1.0
Normal       ---

ethbloom->fixed-hash                 0.4.0    ---                            0.5.2
Normal       ---

ethbloom->impl-rlp                   0.2.0    0.2.1                          0.2.1
Normal       ---
```

```
ethbloom->impl-serde                    0.2.1    0.2.3                          0.2.3
Normal        ---

ethereum-types                          0.7.0    ---                            0.8.0
Normal        ---

ethereum-types->ethbloom                0.7.0    ---                            0.8.1
Normal        ---

ethereum-types->fixed-hash              0.4.0    ---                            0.5.2
Normal        ---

ethereum-types->impl-rlp                0.2.0    0.2.1                          0.2.1
Normal        ---

ethereum-types->impl-serde              0.2.1    0.2.3                          0.2.3
Normal        ---

ethereum-types->primitive-types         0.5.1    ---                            0.6.2
Normal        ---

ethereum-types->uint                    0.8.1    0.8.2                          0.8.2
Normal        ---

failure->backtrace                      0.3.38   0.3.44                         0.3.44
Normal        ---

failure->backtrace                      0.3.38   Removed                        Removed
Normal        ---

failure->failure_derive                 0.1.5    Removed                        Removed
Normal        ---

failure_derive->proc-macro2             0.4.30   Removed                        Removed
Normal        ---

failure_derive->quote                   0.6.13   Removed                        Removed
Normal        ---

failure_derive->syn                     0.15.44  Removed                        Removed
Normal        ---

failure_derive->synstructure            0.10.2   Removed                        Removed
Normal        ---

fixed-hash->byteorder                   1.3.2    1.3.4                          1.3.4
Normal        ---

fixed-hash->rand                        0.5.6    ---                            0.7.3
Normal        ---

fixed-hash->rustc-hex                   2.0.1    2.1.0                          2.1.0
Normal        ---

fixed-hash->static_assertions           0.2.5    ---                            1.1.0
Normal        ---

fxhash->byteorder                       1.3.2    1.3.4                          1.3.4
Normal        ---

getrandom->libc                         0.2.62   0.2.66                         0.2.66
Normal        cfg(any(unix, target_os = "redox"))
```

```
getrandom->wasi                        0.7.0    0.9.0+wasi-snapshot-preview1
0.9.0+wasi-snapshot-preview1  Normal       cfg(target_os = "wasi")

hermit-abi->libc                       0.2.62   Removed                       0.2.66
Normal       ---

hermit-abi->libc                       0.2.62   Removed                       Removed
Normal       ---

hex                                    0.4.0    0.4.1                         0.4.1
Normal       ---

humantime->quick-error                 1.2.2    1.2.3                         1.2.3
Normal       ---

impl-codec->parity-scale-codec         1.0.6    1.1.2                         1.1.2
Normal       ---

impl-rlp->rlp                          0.4.2    0.4.4                         0.4.4
Normal       ---

impl-serde->serde                      1.0.101  1.0.104                       1.0.104
Normal       ---

libloading->cc                         1.0.41   1.0.50                        ---
Build        ---

librocksdb-sys->bindgen                0.49.2   0.49.4                        0.49.4
Build        ---

librocksdb-sys->cc                     1.0.41   1.0.50                        ---
Build        ---

librocksdb-sys->libc                   0.2.62   0.2.66                        0.2.66
Normal       ---

memoffset->rustc_version               0.2.3    Removed                       ---
Build        ---

memoffset->rustc_version               0.2.3    Removed                       Removed
Build        ---

nom->memchr                            2.2.1    2.3.2                         2.3.2
Normal       ---

num-integer->autocfg                   0.1.6    1.0.0                         1.0.0
Build        ---

num-integer->num-traits                0.2.8    0.2.11                        0.2.11
Normal       ---

num-traits->autocfg                    0.1.6    1.0.0                         1.0.0
Build        ---

num_cpus->hermit-abi                   0.1.3    Removed                       0.1.6
Normal       cfg(all(any(target_arch = "x86_64", target_arch = "aarch64"), target_os
= "hermit"))

num_cpus->hermit-abi                   0.1.3    Removed                       Removed
Normal       cfg(all(any(target_arch = "x86_64", target_arch = "aarch64"), target_os
= "hermit"))
```

```
num_cpus->libc                        0.2.62   Removed                        0.2.66
Normal       ---

num_cpus->libc                        0.2.62   Removed                        Removed
Normal       ---

parity-scale-codec->arrayvec          0.4.11   0.5.1                          0.5.1
Normal       ---

parity-scale-codec->bitvec            0.14.0   0.15.2                         0.15.2
Normal       ---

parity-scale-codec->byte-slice-cast   0.3.2    0.3.5                          0.3.5
Normal       ---

parity-scale-codec->serde             1.0.101  1.0.104                        1.0.104
Normal       ---

primitive-types->fixed-hash           0.4.0    ---                            0.5.2
Normal       ---

primitive-types->impl-codec           0.4.1    0.4.2                          0.4.2
Normal       ---

primitive-types->impl-rlp             0.2.0    0.2.1                          0.2.1
Normal       ---

primitive-types->impl-serde           0.2.1    0.2.3                          0.3.0
Normal       ---

primitive-types->uint                 0.8.1    0.8.2                          0.8.2
Normal       ---

proc-macro2->unicode-xid              0.1.0    ---                            0.2.0
Normal       ---

proc-macro2->unicode-xid              0.1.0    Removed                        Removed
Normal       ---

proc-macro2->unicode-xid              0.2.0    Removed                        Removed
Normal       ---

quote->proc-macro2                    0.4.30   ---                            1.0.8
Normal       ---

quote->proc-macro2                    0.4.30   Removed                        Removed
Normal       ---

quote->proc-macro2                    1.0.4    1.0.8                          1.0.8
Normal       ---

quote->proc-macro2                    1.0.4    Removed                        Removed
Normal       ---

rand                                  0.7.2    0.7.3                          0.7.3
Normal       ---

rand->cloudabi                        0.0.3    ---                            Removed
Normal       cfg(target_os = "cloudabi")

rand->fuchsia-cprng                   0.1.1    ---                            Removed
Normal       cfg(target_os = "fuchsia")
```

```
rand->getrandom                      0.1.12   0.1.14                        0.1.14
Normal       ---

rand->libc                           0.2.62   0.2.66                        0.2.66
Normal       cfg(unix)

rand->rand_core                      0.3.1    ---                           0.5.1
Normal       ---

rand->winapi                         0.3.8    ---                           Removed
Normal       cfg(windows)

rand_chacha->c2-chacha               0.2.2    0.2.3                         0.2.3
Normal       ---

rand_core->getrandom                 0.1.12   0.1.14                        0.1.14
Normal       ---

rand_core->rand_core                 0.4.2    ---                           Removed
Normal       ---

rand_core->rand_core                 0.4.2    Removed                       Removed
Normal       ---

rand_os->cloudabi                    0.0.3    Removed                       Removed
Normal       cfg(target_os = "cloudabi")

rand_os->fuchsia-cprng               0.1.1    Removed                       Removed
Normal       cfg(target_os = "fuchsia")

rand_os->libc                        0.2.62   Removed                       Removed
Normal       cfg(unix)

rand_os->rand_core                   0.4.2    Removed                       Removed
Normal       ---

rand_os->rdrand                      0.4.0    Removed                       Removed
Normal       cfg(target_env = "sgx")

rand_os->winapi                      0.3.8    Removed                       Removed
Normal       cfg(windows)

rayon->crossbeam-deque               0.7.2    Removed                       ---
Normal       ---

rayon->crossbeam-deque               0.7.2    Removed                       Removed
Normal       ---

rayon->either                        1.5.3    Removed                       ---
Normal       ---

rayon->either                        1.5.3    Removed                       Removed
Normal       ---

rayon->rayon-core                    1.6.1    Removed                       1.7.0
Normal       ---

rayon->rayon-core                    1.6.1    Removed                       Removed
Normal       ---

rayon-core->crossbeam-deque          0.7.2    Removed                       ---
Normal       ---
```

```
rayon-core->crossbeam-deque          0.7.2    Removed                        Removed
Normal       ---

rayon-core->crossbeam-queue          0.2.0    Removed                        0.2.1
Normal       ---

rayon-core->crossbeam-queue          0.2.0    Removed                        Removed
Normal       ---

rayon-core->crossbeam-utils          0.7.0    Removed                        ---
Normal       ---

rayon-core->crossbeam-utils          0.7.0    Removed                        Removed
Normal       ---

rayon-core->lazy_static              1.4.0    Removed                        ---
Normal       ---

rayon-core->lazy_static              1.4.0    Removed                        Removed
Normal       ---

rayon-core->num_cpus                 1.11.0   Removed                        1.12.0
Normal       ---

rayon-core->num_cpus                 1.11.0   Removed                        Removed
Normal       ---

rdrand->rand_core                    0.3.1    Removed                        Removed
Normal       ---

redox_users->failure                 0.1.5    Removed                        Removed
Normal       ---

redox_users->rand_os                 0.1.3    Removed                        Removed
Normal       ---

redox_users->rust-argon2             0.5.1    0.7.0                          0.7.0
Normal       ---

regex->aho-corasick                  0.7.6    0.7.8                          0.7.8
Normal       ---

regex->memchr                        2.2.1    2.3.2                          2.3.2
Normal       ---

regex->regex-syntax                  0.6.12   0.6.14                         0.6.14
Normal       ---

regex->thread_local                  0.3.6    1.0.1                          1.0.1
Normal       ---

rlp                                  0.4.2    0.4.4                          0.4.4
Normal       ---

rlp->rustc-hex                       2.0.1    2.1.0                          2.1.0
Normal       ---

rocksdb->libc                        0.2.62   0.2.66                         0.2.66
Normal       ---

rust-argon2->base64                  0.10.1   0.11.0                         0.11.0
Normal       ---
```

```
rust-argon2->blake2b_simd          0.5.8    0.5.10                    0.5.10
Normal       ---

rust-argon2->crossbeam-utils       0.6.6    0.7.0                     0.7.0
Normal       ---

rustc-hex                          2.0.1    2.1.0                     2.1.0
Normal       ---

rustc_version->semver              0.9.0    Removed                   ---
Normal       ---

rustc_version->semver              0.9.0    Removed                   Removed
Normal       ---

secp256k1                          0.15.0   ---                       0.17.2
Normal       ---

secp256k1->cc                      1.0.41   1.0.50                    ---
Build        ---

secp256k1->cc                      1.0.41   1.0.50                    Removed
Build        ---

semver->semver-parser              0.7.0    Removed                   ---
Normal       ---

semver->semver-parser              0.7.0    Removed                   Removed
Normal       ---

serde                              1.0.101  1.0.104                   1.0.104
Normal       ---

serde->serde_derive                1.0.101  1.0.104                   1.0.104
Normal       ---

serde->serde_derive                1.0.101  Removed                   Removed
Normal       ---

serde_derive                       1.0.101  1.0.104                   1.0.104
Normal       ---

serde_derive->proc-macro2          1.0.4    1.0.8                     1.0.8
Normal       ---

serde_derive->proc-macro2          1.0.4    Removed                   Removed
Normal       ---

serde_derive->quote                1.0.2    Removed                   Removed
Normal       ---

serde_derive->syn                  1.0.5    1.0.14                    1.0.14
Normal       ---

serde_derive->syn                  1.0.5    Removed                   Removed
Normal       ---

serde_json                         1.0.40   1.0.48                    1.0.48
Normal       ---

serde_json->itoa                   0.4.4    0.4.5                     0.4.5
Normal       ---
```

```
serde_json->ryu                    1.0.0    1.0.2                    1.0.2
Normal       ---

serde_json->serde                  1.0.101  1.0.104                  1.0.104
Normal       ---

serial_test                        0.1.0    ---                      0.3.2
Development  ---

serial_test_derive                 0.2.0    ---                      0.3.2
Normal       ---

serial_test_derive->quote          0.6.13   ---                      1.0.2
Normal       ---

serial_test_derive->syn            0.15.44  ---                      1.0.14
Normal       ---

simplelog                          0.7.3    0.7.4                    0.7.4
Normal       ---

simplelog->chrono                  0.4.9    0.4.10                   0.4.10
Normal       ---

syn->proc-macro2                   0.4.30   ---                      1.0.8
Normal       ---

syn->proc-macro2                   0.4.30   Removed                  Removed
Normal       ---

syn->proc-macro2                   1.0.4    1.0.8                    1.0.8
Normal       ---

syn->proc-macro2                   1.0.4    Removed                  Removed
Normal       ---

syn->quote                         0.6.13   ---                      1.0.2
Normal       ---

syn->quote                         0.6.13   Removed                  Removed
Normal       ---

syn->quote                         1.0.2    Removed                  Removed
Normal       ---

syn->unicode-xid                   0.1.0    ---                      0.2.0
Normal       ---

syn->unicode-xid                   0.1.0    Removed                  Removed
Normal       ---

syn->unicode-xid                   0.2.0    Removed                  Removed
Normal       ---

synstructure->proc-macro2          0.4.30   Removed                  Removed
Normal       ---

synstructure->quote                0.6.13   Removed                  Removed
Normal       ---

synstructure->syn                  0.15.44  Removed                  Removed
Normal       ---
```

```
synstructure->unicode-xid              0.1.0    Removed                        Removed
Normal       ---

termcolor->wincolor                    1.0.2    Removed                        Removed
Normal       cfg(windows)

textwrap->unicode-width                0.1.6    0.1.7                          0.1.7
Normal       ---

time->libc                             0.2.62   0.2.66                         0.2.66
Normal       ---

tiny-keccak                            1.5.0    ---                            2.0.1
Normal       ---

uint->byteorder                        1.3.2    1.3.4                          1.3.4
Normal       ---

uint->rustc-hex                        2.0.1    2.1.0                          2.1.0
Normal       ---

which->failure                         0.1.5    0.1.6                          0.1.6
Normal       ---

which->libc                            0.2.62   0.2.66                         0.2.66
Normal       ---

winapi->winapi-i686-pc-windows-gnu     0.4.0    ---                            Removed
Normal       i686-pc-windows-gnu

winapi->winapi-i686-pc-windows-gnu     0.4.0    Removed                        Removed
Normal       i686-pc-windows-gnu

winapi->winapi-x86_64-pc-windows-gnu   0.4.0    ---                            Removed
Normal       x86_64-pc-windows-gnu

winapi->winapi-x86_64-pc-windows-gnu   0.4.0    Removed                        Removed
Normal       x86_64-pc-windows-gnu

winapi-util->winapi                    0.3.8    Removed                        Removed
Normal       cfg(windows)

wincolor->winapi                       0.3.8    Removed                        Removed
Normal       ---

wincolor->winapi-util                  0.1.2    Removed                        Removed
Normal       ---
```

Appendix C: Test output of `pbtc-btc-syncer > pnpx mocha`

```
pbtc-btc-syncer > pnpx mocha

  ❍ Testing the sleep module
    ✓ Should sleep for x milliseconds (1003ms)
✔ Sleeping for 1000 milliseconds...

    ✓ Should sleep for amount of time in state (1002ms)

  ❍ Testing the trampoline module
    1) Should trampoline a fxn


  2 passing (2s)
  1 failing

  1) ❍ Testing the trampoline module
       Should trampoline a fxn:
     TypeError: trampolineAndRecurseWith is not a function
      at Context.<anonymous> (test/trampoline-test.js:12:11)
      at processImmediate (internal/timers.js:439:21)
```

Appendix D: Output of `pbtc-btc-syncer > pnpx eslint .`

```
pbtc-btc-syncer > pnpx eslint .

pbtc-btc-syncer/lib/btc-endpoint-api.js

   9:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors

  18:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors

  21:13  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors



pbtc-btc-syncer/lib/check-api-endpoint.js

  8:7  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors



pbtc-btc-syncer/lib/enclave-utils.js

  21:18  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors

  28:18  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors



pbtc-btc-syncer/lib/errors.js

  13:58  warning  Unexpected 'note' comment              no-warning-comments

  32:38  warning  Arrow function has a complexity of 12  complexity



pbtc-btc-syncer/lib/format-enclave-output.js

  41:7  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors



pbtc-btc-syncer/lib/get-btc-block.js

  33:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors

  34:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors
```

```
pbtc-btc-syncer/lib/get-deposit-address-list.js

  32:7  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors


pbtc-btc-syncer/lib/get-mongo-db.js

  29:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors


pbtc-btc-syncer/lib/save-enclave-output-in-db.js

  32:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors


pbtc-btc-syncer/lib/trampoline.js

  4:3  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors


pbtc-btc-syncer/lib/utils.js

  35:7   warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors

  63:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors


pbtc-btc-syncer/test/trampoline-test.js

  9:27  warning  Expected an assignment or function call and instead saw an
expression  no-unused-expressions

  9:44  warning  Unexpected use of comma operator
no-sequences


✖ 19 problems (0 errors, 19 warnings)
```

Appendix E: Output of `pbtc-db-repl > pnpx eslint .`

```
pbtc-db-repl > pnpx eslint .


pbtc-db-repl/lib/get-btc-deposit-address-obj.js

  33:13  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors



pbtc-db-repl/lib/utils.js

   7:7   warning  'getUnixTimestampInSeconds' is assigned a value but never used
no-unused-vars

  15:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors



pbtc-db-repl/pbtc-db-repl.js

  168:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors


✖ 4 problems (0 errors, 4 warnings)
```

Appendix F: Output of `pbtc-enclave-api > pnpx eslint .`

```
pbtc-enclave-api > pnpx eslint .

pbtc-enclave-api/lib/get-btc-deposit-address-obj.js

  33:13  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors



pbtc-enclave-api/lib/get-btc-deposit-address-route.js

    6:3   warning  'checkEthAddressAndGetDbObject' is assigned a value but never used
no-unused-vars

    7:3   warning  'getEthAddressFromMaybeEthAddress' is assigned a value but never
used  no-unused-vars

   36:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors

  120:13  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors



pbtc-enclave-api/lib/get-info-route.js

  13:9   warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors

  15:55  warning  Arrow function has a complexity of 6                  complexity

  23:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors

  24:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors

  34:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors

  38:13  warning  Unnecessary parentheses around expression
no-extra-parens



pbtc-enclave-api/lib/get-mongo-db.js

  22:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors



pbtc-enclave-api/lib/query-recipient-route.js

  1:24  warning  Arrow function has a complexity of 7  complexity
```

```
pbtc-enclave-api/lib/routes.js

  1:1  warning  Unexpected 'todo' comment  no-warning-comments


pbtc-enclave-api/lib/submit-eth-block-route.js

  15:7  warning  'blockIsReadyForSubmission' is assigned a value but never used
no-unused-vars

  21:7  warning  'createSubmissionObject' is assigned a value but never used
no-unused-vars

  25:1  warning  Unexpected 'todo' comment
no-warning-comments


pbtc-enclave-api/lib/utils.js

  15:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors


✖ 18 problems (0 errors, 18 warnings)

  0 errors and 1 warning potentially fixable with the `--fix` option.
```

Appendix G: Output of `pbtc-eth-and-btc-block-getter > pnpx eslint .`

```
pbtc-eth-and-btc-block-getter > pnpx eslint .

pbtc-eth-and-btc-block-getter/get-latest-blocks.js

  12:9  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors



pbtc-eth-and-btc-block-getter/lib/get-eth-block.js

  13:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors



✖ 2 problems (0 errors, 2 warnings)
```

Appendix H: Output of `pbtc-eth-syncer > pnpx eslint .`

```
pbtc-eth-syncer > pnpx eslint .

pbtc-eth-syncer/lib/enclave-utils.js

  21:18  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors

  28:18  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors



pbtc-eth-syncer/lib/errors.js

  14:58  warning  Unexpected 'note' comment             no-warning-comments

  33:38  warning  Arrow function has a complexity of 9  complexity



pbtc-eth-syncer/lib/format-enclave-output.js

  41:7  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors



pbtc-eth-syncer/lib/get-block-and-receipts.js

  26:57  warning  Unexpected 'todo' comment
no-warning-comments

  34:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors

  49:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors



pbtc-eth-syncer/lib/get-mongo-db.js

  27:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors



pbtc-eth-syncer/lib/save-report-in-db.js

  32:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors



pbtc-eth-syncer/lib/submit-block.js

  58:12  warning  Arrow function has a complexity of 6  complexity
```

```
pbtc-eth-syncer/lib/trampoline.js

  4:3  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors


pbtc-eth-syncer/lib/utils.js

  34:7  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors


pbtc-eth-syncer/test/trampoline-test.js

  21:27  warning  Expected an assignment or function call and instead saw an
expression  no-unused-expressions

  21:44  warning  Unexpected use of comma operator
no-sequences


✖ 15 problems (0 errors, 15 warnings)
```

Appendix I: Output of `pbtc-tx-broadcaster > pnpx eslint .`

```
pbtc-tx-broadcaster > pnpx eslint .

pbtc-tx-broadcaster/lib/broadcast-transactions.js

   21:53  warning  Unexpected 'todo' comment
no-warning-comments

  111:34  warning  Arrow function has a complexity of 6                 complexity

  153:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors

  158:34  warning  Arrow function has a complexity of 6                 complexity

  169:13  warning  Unexpected 'todo' comment
no-warning-comments

  177:51  warning  Unexpected 'todo' comment
no-warning-comments


pbtc-tx-broadcaster/lib/get-last-seen-nonce.js

  11:1  warning  Unexpected 'todo' comment  no-warning-comments


pbtc-tx-broadcaster/lib/get-mongo-db.js

  24:24  warning  Unexpected 'todo' comment
no-warning-comments

  31:11  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors


pbtc-tx-broadcaster/lib/get-signatures-from-database.js

  17:1   warning  Unexpected 'todo' comment             no-warning-comments

  25:11  warning  Arrow function has a complexity of 6  complexity

  26:51  warning  Unexpected mix of '||' and '&&'       no-mixed-operators

  27:24  warning  Unexpected mix of '||' and '&&'       no-mixed-operators

  40:11  warning  Arrow function has a complexity of 6  complexity

  41:51  warning  Unexpected mix of '||' and '&&'       no-mixed-operators

  42:24  warning  Unexpected mix of '||' and '&&'       no-mixed-operators


pbtc-tx-broadcaster/lib/set-last-seen-nonce.js
```

```
  15:1   warning  Unexpected 'todo' comment             no-warning-comments

  49:44  warning  Unexpected 'todo' comment             no-warning-comments

  53:11  warning  Arrow function has a complexity of 6  complexity

  66:11  warning  Arrow function has a complexity of 6  complexity

  78:31  warning  Unexpected 'todo' comment             no-warning-comments


pbtc-tx-broadcaster/lib/trampoline.js

  9:3  warning  Expected the Promise rejection reason to be an Error
prefer-promise-reject-errors


pbtc-tx-broadcaster/lib/update-latest-nonce.js

   7:31  warning  Unexpected 'todo' comment  no-warning-comments

  16:1   warning  Unexpected 'todo' comment  no-warning-comments


pbtc-tx-broadcaster/pbtc-tx-broadcaster.js

  26:36  error  'mainEthLoop' was used before it was defined  no-use-before-define


✖ 25 problems (1 error, 24 warnings)
```