CONSENSYS
Diligence

Summary - Thesis: tBTC and Keep Audit

Date	February 2020
Lead Auditor	Martin Ortner
Co-auditors	Alexander Wade

1 Executive Summary

In January 2020, Thesis asked us to conduct a security assessment of tBTC: a trust-minimized, redeemable, Bitcoin-backed ERC20 token. tBTC utilizes and builds on functionality provided by Summa and the Keep Network.

We performed this assessment from February 03 to March 27, 2020. The assessment primarily focused on tBTC alongside its associated components. The engagement was conducted by Martin Ortner and Alexander Wade over the course of twelve person-weeks. This document is a standalone summary. The full report can be found here.

In addition to the review of tBTC, a review was performed of the cryptographic constructions and algorithms used in the Keep Network. A complete report of this portion of the engagement can be found here.

1.1 Scope

We analyzed code located in the following repositories at the provided commits:

Repository	Audit Revision
keep-network/tbtc	#dcb1148025d6a1238b49a80fd56d8ca0beb93781

Repository	Audit Revision
summa-tx/bitcoin-spv	#f5e4da091a1c97e6432c2d70eba434edb189f919
keep-network/keep-tecdsa – keep-network/sortition-pools	#c69871d252378c63ab47ab3f652de0a63b09eea5 #32523a74bb5fa51345de05f756ca8a9ecf246282
keep-network/keep-core	#b76b418f04bc94030d10aff18220d8e560a2ab09

Third party dependencies not explicitly mentioned in the above list (e.g. `summa-tx/relay-sol`) were out of scope for the audit.

tBTC interacts with the Keep Network via customized interfaces from `keep-network/keep-tecdsa`, which itself uses `keep-network/sortition-pools`. The keep random beacon used for signer group election (`keep-network/keep-core`) builds on an implementation of BLS signatures on the altbn128 curve. The source code is located in five repositories with the following dependencies as seen from the tBTC solution:

- `keep-network/tbtc`
  - `summa-tx/bitcoin-spv`
  - `keep-network/keep-tecdsa`
    - `keep-network/sortition-pools`
  - `keep-network/keep-core`
- `keep-network/keep-core` (independent solution)

Together with the client, it was established that the main focus for the review would be the smart contracts in the listed repositories, with a secondary focus on reviewing the keep client (located in `keep-core`).

A complete list of files in scope can be found in the Appendix.

1.2 Objectives

Given the limited time available and ongoing development on some components in scope, we elected to begin with a top-down approach centered around tBTC as the focal point. We started by understanding the architecture and design of high-risk components first, before diving into various system components to verify security assumptions.

Our primary objectives were to:

1. Ensure that the system is implemented consistently with the intended functionality, and without unintended edge cases.
2. Identify known vulnerabilities particular to smart contract systems, as outlined in our Smart Contract Best Practices, and the Smart Contract Weakness Classification Registry.
3. Ensure that there is no way to break the TBTC-BTC peg and that it is as difficult as possible to abscond with deposited funds for the backing ECDSA keep.

We also sought opportunities to improve the quality of the code either by reducing the complexity, or improving clarity and readability.

1.3 Audit Log - Phase 1

The primary engagement (Feb 03 - Feb 28) was scheduled as follows:

Week 1	Week 2	Week 3	Week 4
- ramp up `tbtc` - review `bitcoin-spv`	- `bitcoin-spv` - tBTC Deposits	- tBTC Deposits - ramp up keep	- keep - `keep-tecdsa` - `sortition-pools`

Week 1

During the first week, our efforts were directed towards tBTC: understanding the intention of its design and how it uses `bitcoin-spv` to validate spv proofs and other Bitcoin transaction information. This involved defining key risk factors and potential vulnerabilities requiring further investigation. Key findings were shared with the client in an end-of-week sync meeting.

By the end of the first week, the tBTC codebase was modified from its initial audit commit to the revision v1-audit. The client also provided a frozen codebase for keep-network/keep-core. keep-network/keep-tecdsa was still undergoing changes.

Week 2

During the second week, we reviewed changes made to tBTC during the previous week. We also began a more detailed review of the tBTC codebase; in particular, tBTC Deposit flows and the investigation of potential vulnerabilities. Key findings were shared with the client in an end-of-week sync meeting and filed in the client repository where applicable. keep-network/keep-tecdsa was still undergoing changes by the end of week two.

The audit team informed the client that given the size and complexity of the audit there might not be enough time to cover all parts of the initial scope. Together with the client, it was determined that we would spend the next week finishing the review of tBTC Deposit flows before transitioning our review to `keep-core`.

Week 3

During the third week, we reviewed tBTC Deposit flows and started transitioning from tBTC to `keep-core`, maintaining a focus on the functionality of `keep-core` that was most relevant to tBTC.

The audit revision for the `keep-tecdsa` codebase was provided in the second half of the week and tagged as keep-tecdsa#v0.8.0. Additionally, the sortition-pools#v0.1.1 repository referenced by `keep-tecdsa` was added to the audit's scope.

The cryptographic review that was planned to start this week had to be delayed due to availability problems with our cryptographer. The review of the keep client was temporarily set out of scope to ensure sufficient attention was given to the smart contracts. Key findings and questions were shared immediately via the client collaboration channel and discussed in an end-of-week sync meeting.

Week 4

During the fourth week, we focused on `keep-core` and the now frozen `keep-tecdsa` implementation. The week was kicked off by the client providing a walkthrough of the relevant code of `keep-tecdsa`. Key findings and questions were shared immediately via the client collaboration channel and discussed in an end-of-week sync meeting. The **preliminary report** outlining recommendations and findings was prepared towards the end of the week targeting delivery for the following Monday.

Two-week hiatus

A two-week hiatus allowing the client to address discussion points, recommendations, and issues found during the audit was planned from March 02 to March 13.

The engagement was scheduled to be continued for a final two-week review from March 16 to March 27.

1.4 Audit Log - Phase 2

The final phase of the engagement was scheduled as follows:

Week 1	Week 2
- review fixes made during hiatus - review `keep-core`	- surface-level review of `keep-core` client - finalize report

Week 1

During the first week after providing the initial report, we focused on continuing our efforts with `keep-core` and reviewing the feedback and fixes that were provided for the initial report. A secondary goal was to start reviewing the client implementations in `keep-core`. The client provided a high-level walkthrough of the keep client codebase and the audit team shared the sources for the tBTC state diagram (see Security - tBTC). The audit codebase was updated to the following revisions:

- `tbtc` : fbb2018c41456d19ec20eb28a17070ee2b10eb5d (noted above)
- `keep-tecdsa` : 2aab1f755e437d6e816c34a4fd354025cea5de3a (v0.10.0-rc)
- `keep-core` : 9f8b13fe54cc627548746d7e64b77d6aa50b94e1 (v0.11.0-rc] (provided on friday)
- `sortition-pools` : no update provided
- `bitcoin-spv` : no update provided

Week 2

During the second week, we continued with our focus on `keep-core` and started reviewing the client logic that is interacting with the smart contracts. The **final report** outlining recommendations and findings including client feedback and a review of provided fixes was prepared towards the end of the week targeting delivery for the following Monday. In addition to that the cryptographic review was finalized and prepared for the delivery on Monday.

Appendix 1 - Files in Scope

Our review covered the following files at the outset:

bitcoin-spv

File	SHA-1 hash

File	SHA-1 hash
bitcoin-spv/solidity/contracts/BTCUtils.sol	c35c9ea329cc87ff74f1c5ce0c300a0d7db3
bitcoin-spv/solidity/contracts/BytesLib.sol	2178fa49f897c2afe236478a9f4559408ac8
bitcoin-spv/solidity/contracts/SafeMath.sol	7462e2ec469c36913b6fc47bafef1749f29b
bitcoin-spv/solidity/contracts/BTCUtilsDelegate.sol	ea3bc8ef148ef4fb8daff8c4c260c24ff747e4
bitcoin-spv/solidity/contracts/CheckBitcoinSigs.sol	e9624d00af1fbd377229fe767032eceec856
bitcoin-spv/solidity/contracts/CheckBitcoinSigsDelegate.sol	53c0a185f9c778df4c184921a3bec6f0c6c5
bitcoin-spv/solidity/contracts/ValidateSPV.sol	1a5fcca4dfe7b2c6ec41603044522690563
bitcoin-spv/solidity/contracts/ValidateSPVDelegate.sol	1c0bfe67ec7d9c20192e1e940a8101c0ac7

tBTC

File	SHA-1
tbtc/implementation/contracts/DepositLog.sol	0b4097f3400f2b6bfd1783
tbtc/implementation/contracts/deposit/DepositFunding.sol	c77af1cd7eb7422bc1365e
tbtc/implementation/contracts/system/TBTCToken.sol	91a9c9663212800c7b1fb
tbtc/implementation/contracts/system/VendingMachineAuthority.sol	5e63aae00f82cd5c6c7823
tbtc/implementation/contracts/system/TBTCSystem.sol	2171736428af6abd9c31fc
tbtc/implementation/contracts/system/VendingMachine.sol	17f16b793f5c0378f88680
tbtc/implementation/contracts/system/TBTCDepositToken.sol	2e926a39620647d72dbfd
tbtc/implementation/contracts/system/DepositFactoryAuthority.sol	188311a48e8b7e4491d2b
tbtc/implementation/contracts/system/FeeRebateToken.sol	0e977f37fca62daeed737e
tbtc/implementation/contracts/deposit/TBTCConstants.sol	5b0fc693173bd612cba1cb
tbtc/implementation/contracts/deposit/DepositUtils.sol	7308079022c02b2e14646
tbtc/implementation/contracts/deposit/DepositStates.sol	5ebaa3a0c9f708a98f6536
tbtc/implementation/contracts/interfaces/ITBTCSystem.sol	97a6241eea43fd6f319def
tbtc/implementation/contracts/deposit/Deposit.sol	0449315750be89b5a74a0
tbtc/implementation/contracts/deposit/DepositLiquidation.sol	613be100e9f79a8964746

File	SHA-1
tbtc/implementation/contracts/deposit/OutsourceDepositLogging.sol	790c605150564a8963be5
tbtc/implementation/contracts/deposit/DepositRedemption.sol	7ee02dd144011e257f246
tbtc/implementation/contracts/system/TBTCSystemAuthority.sol	7924969f054ee6740de37
tbtc/implementation/contracts/proxy/DepositFactory.sol	26a280871b518490022b5
tbtc/implementation/contracts/proxy/CloneFactory.sol	9044bc020f1d0132f5d408
tbtc/implementation/contracts/interfaces/IBTCETHPriceFeed.sol	d9d24818569427dbc4d64
tbtc/implementation/contracts/external/IMedianizer.sol	957d66ee5fc768bf9ff7c47
tbtc/implementation/contracts/price-feed/BTCETHPriceFeed.sol	3658670d0d66b155cdf56

keep-tecdsa

File Name	SHA-1 Hash
contracts/BondedECDSAKeep.sol	bc89cc51280d6c424fa76ac70afaca59794bf8ce
contracts/BondedECDSAKeepFactory.sol	23d428253b1f70f12e98e791ff39547edac898ad
contracts/BondedECDSAKeepVendor.sol	6397c7bac818add006ec5add72f72f8ca77dee0
contracts/BondedECDSAKeepVendorImplV1.sol	4314a3c1f5aff333db73426d35da9b545e46834
contracts/CloneFactory.sol	7408e755f2f9eb6699c04b45a8c28446041a3f73
contracts/KeepBonding.sol	a3b01f99c4fde8652f050a45fe2b4a30c6fa4b9e
contracts/api/IBondedECDSAKeep.sol	02624cb967aade2c5290cb13c9740825e905b4
contracts/api/IBondedECDSAKeepFactory.sol	30d55d502d4ef0f5aadb812ab553c6221cc1d63
contracts/api/IBondedECDSAKeepVendor.sol	764019742ba132a75ddf1272cdeb0e8a7ccb7f1

sortition-pools

File Name	SHA-1 Hash
contracts/AbstractSortitionPool.sol	7a4b163dcf5fd3ea8a9c74c5c219aadfc6c007b9
contracts/BondedSortitionPool.sol	3cde74fa4b63e4e9979dafc6418aa57ac90ec798
contracts/BondedSortitionPoolFactory.sol	49706b318ace886b3b8bd0725d546ece329958b9
contracts/Branch.sol	2571e8c19fe3f4764aa9feac8b37808f595bb407

File Name	SHA-1 Hash
contracts/DynamicArray.sol	ab6b782ce938cf958cc56e2c6b2a0f2334715d18
contracts/GasStation.sol	790159120d85a0dbdbfe57f729b5ada572ebbaef
contracts/Interval.sol	1fab3c416d8261f42d35d53d37c77b644fa1e3c0
contracts/Leaf.sol	22b7bee520b77214b1f81b75e352f44ad059ffc8
contracts/Position.sol	36cf18478fae2c9e22124d3ac52b5a050c7fe78b
contracts/RNG.sol	dc7862e02c56b9b033cc1db67fe19153a1e38ba7
contracts/SortitionPool.sol	e889623764112859984 2d0951f8721632cfd061e
contracts/SortitionPoolFactory.sol	56bcc990f6a8cbfbd877b06ca0df43a7da21dd38
contracts/SortitionTree.sol	7d4d0fac5e8d8d1bea709280c442576751f18b33
contracts/StackLib.sol	e91cfb78f3b90ca8b3a18f701356c565a933e52e
contracts/api/IBondedSortitionPool.sol	d9fd422dc4a6ca6323a0ba536cb65f33e44c3e1b
contracts/api/IBonding.sol	71b96ff01a2efdb09e6d24b7432484b9a15a4a00
contracts/api/ISortitionPool.sol	709d56b46065c160042dcac8c2cb9a42a1ea201c
contracts/api/IStaking.sol	9412ade9ccf9f0672875d1c94b49d230dbbe4be1

keep-core

File Name	
keep-core/contracts/solidity/contracts/cryptography/AltBn128.sol	0af848f5bdf3bc54
keep-core/contracts/solidity/contracts/cryptography/BLS.sol	95f316615a6177e
keep-core/contracts/solidity/contracts/DelayedWithdrawal.sol	ad8109961339eaf
keep-core/contracts/solidity/contracts/KeepRandomBeaconOperator.sol	206cb9399c1d4c7
keep-core/contracts/solidity/contracts/KeepRandomBeaconService.sol	280a810f174100a
keep-core/contracts/solidity/contracts/KeepRandomBeaconServiceImplV1.sol	8d23f4ef32aea55e
keep-core/contracts/solidity/contracts/KeepToken.sol	91f2bb61583f741
keep-core/contracts/solidity/contracts/Registry.sol	e1b58dd981a5baa
keep-core/contracts/solidity/contracts/StakeDelegatable.sol	0e469a07df4bb72

File Name	
keep-core/contracts/solidity/contracts/TokenGrant.sol	cf6b6befe786cfc1
keep-core/contracts/solidity/contracts/TokenStaking.sol	02c0446475d84a
keep-core/contracts/solidity/contracts/libraries/operator/DKGResultVerification.sol	132d1a7aa9c6d6
keep-core/contracts/solidity/contracts/libraries/operator/GroupSelection.sol	8812a2027044f6a
keep-core/contracts/solidity/contracts/libraries/operator/Groups.sol	ba8c30b6340966
keep-core/contracts/solidity/contracts/libraries/operator/Reimbursements.sol	285de769e1f56d8
keep-core/contracts/solidity/contracts/utils/AddressArrayUtils.sol	85d9bf08c8628ec
keep-core/contracts/solidity/contracts/utils/ModUtils.sol	ebf6ebc9647c6b6
keep-core/contracts/solidity/contracts/utils/ThrowProxy.sol	fa012ba7589dc8b
keep-core/contracts/solidity/contracts/utils/UintArrayUtils.sol	5d1210befba8fc72

Appendix 2 - Disclosure

ConsenSys Diligence (“CD”) typically receives compensation from one or more clients (the “Clients”) for performing the analysis contained in these reports (the “Reports”). The Reports may be distributed through other means, including via ConsenSys publications and other distributions.

The Reports are not an endorsement or indictment of any particular project or team, and the Reports do not guarantee the security of any particular project. This Report does not consider, and should not be interpreted as considering or having any bearing on, the potential economics of a token, token sale or any other product, service or other asset. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. No Report provides any warranty or representation to any Third-Party in any respect, including regarding the bugfree nature of code, the business model or proprietors of any such business model, and the legal compliance of any such business. No third party should rely on the Reports in any way, including for the purpose of making any decisions to buy or sell any token, product, service or other asset. Specifically, for the avoidance of doubt, this Report does not constitute investment advice, is not intended to be relied upon as investment advice, is not an endorsement of this project or

team, and it is not a guarantee as to the absolute security of the project. CD owes no duty to any Third-Party by virtue of publishing these Reports.

PURPOSE OF REPORTS The Reports and the analysis described therein are created solely for Clients and published with their consent. The scope of our review is limited to a review of Solidity code and only the Solidity code we note as being within the scope of our review within this report. The Solidity language itself remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond Solidity that could present security risks. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty.

CD makes the Reports available to parties other than the Clients (i.e., "third parties") – on its website. CD hopes that by making these analyses publicly available, it can help the blockchain ecosystem develop technical best practices in this rapidly evolving area of innovation.

LINKS TO OTHER WEB SITES FROM THIS WEB SITE You may, through hypertext or other computer links, gain access to web sites operated by persons other than ConsenSys and CD. Such hyperlinks are provided for your reference and convenience only, and are the exclusive responsibility of such web sites' owners. You agree that ConsenSys and CD are not responsible for the content or operation of such Web sites, and that ConsenSys and CD shall have no liability to you or any other person or entity for the use of third party Web sites. Except as described below, a hyperlink from this web Site to another web site does not imply or mean that ConsenSys and CD endorses the content on that Web site or the operator or operations of that site. You are solely responsible for determining the extent to which you may use any content at any other web sites to which you link from the Reports. ConsenSys and CD assumes no responsibility for the use of third party software on the Web Site and shall have no liability whatsoever to any person or entity for the accuracy or completeness of any outcome generated by such software.

TIMELINESS OF CONTENT The content contained in the Reports is current as of the date appearing on the Report and is subject to change without notice. Unless indicated otherwise, by ConsenSys and CD.