# Bulletproofs review

Vendor overview

Prepared by Sarang Noether, Monero Research Lab

## Introduction

The Monero Research Lab has proposed replacing Borromean-style range proofs in its confidential transaction model with Bulletproofs, a new technique described in a paper by Benedikt Bünz and collaborators[1]. Lab researchers have reviewed the paper and determined that a change to Bulletproofs will dramatically reduce the size of future transactions (on average by over 90%, based on earlier transaction distributions) and the time to verify such a proof (on average by over 50%).

Lab researchers and developers translated the algorithms in the paper to Java prototype code, using a test library that is not compatible with the Monero codebase. This code was used for correctness testing, as well as to examine the effects of possible optimizations to the prove and verify algorithms. Once complete, the Java code was used for the development of C++ code compatible with the Monero codebase and containing additional optimizations for speed. After ongoing informal consultation with the paper's authors, several iterations of the Java code were made to introduce new optimizations, and these changes were subsequently updated in the C++ code.

The Bulletproofs work is relatively new and (to the best of our knowledge) has not yet been deployed in a major cryptocurrency project. Range proofs are critical for ensuring the balance of transaction inputs and outputs, and it is essential that the final Monero implementation be correct and secure. For this reason, the Monero Research Lab and Monero Project wish to secure the services of independent third-party reviewers to determine the correctness of the implementation and the level to which it is secure against attacks and flaws in design or coding. Once such a review is complete and any necessary changes are made, the Bulletproofs code will be deployed in a hard fork, and will be the only type of range proof accepted for new transactions by consensus.

The Monero Research Lab solicited proposals for such a review, and also reached out to targeted individuals with advanced knowledge of the Bulletproofs mathematics. We have received statements of work from several groups and must choose which groups to hire for the review. Once the decision is made, the Lab will make a community funding request via the Forum Funding System to secure donations. After all funding is committed, the Monero Project will formally contract the chosen groups to begin the review process. All results and reports from the audit will be made publicly available when completed.

[1] https://crypto.stanford.edu/bulletproofs/

This document provides an overview of the groups that provided statements of work to the Monero Research Lab, and contains the Lab's initial recommendations for group selection. The Lab encourages community members, researchers, and developers to provide feedback on these statements of work and the review process, either on the Lab's #monero-research-lab freenode IRC channel, or to sarang.noether@protonmail.com by email. All email correspondence on this matter may be made public in the interest of transparency.

Reviewers are listed in no particular order.

Reviewer: Benedikt Bünz

The Lab reached out directly to Benedikt Bünz, the lead author of the Bulletproofs paper. Bünz is a doctoral student at Stanford University in applied cryptography. Previous published research focuses on randomness beacons, proofs of solvency, zero-knowledge proofs, confidential transactions, and other topics related to cryptocurrencies.

Bünz has agreed to perform a review of the Lab's Java prototype code. If selected for the review, his work will determine the extent to which the Java code faithfully represents the prove and verify algorithms in the Bulletproofs paper, taking into account the specific optimizations made to the code. He would be compensated 6 XMR per work day, with a maximum compensation of 36.4 XMR allocated.

Bünz has indicated he would be available to begin the review presently, and requested that the Lab prepare a statement of work for his review. This document, which he has approved, is attached for public comment.

Reviewer: QuarksLab

QuarksLab was brought to the Lab's attention by the Open Source Technology Improvement Fund (OSTIF) as a potential reviewer. OSTIF has worked with QuarksLab on many previous occasions. Their audits include the disk encryption utility VeraCrypt and the OpenVPN project. The lead reviewer, Prof. Marion Videau, has an extensive record in academia, government, and industry as a consultant and researcher.

If selected for this audit, QuarksLab will review the Monero Project's C++ implementation of Bulletproofs. They will assess the extent to which the C++ code matches the paper's specifications and the Lab's prototype Java code, and identify vulnerabilities in implementation. Specifically, they will determine if it is possible for an attacker to generate a false proof that an honest verifier judges to be correct, and if it is possible for an attacker to examine an honest proof and gain information about its input values.

If selected, QuarksLab would be compensated $1650 USD per person-day of work, with a cap of $41250 USD. However, OSTIF indicates that previous collaborations have completed under budget. Payment would be made in XMR to OSTIF, who would complete the exchange to

QuarksLab at no additional fee or cost. They would be available to begin the review at the end of April. A statement of work from QuarksLab is attached for public comment.

Reviewer: X41 D-sec

X41 D-sec (X41) was brought to the Lab's attention by OSTIF as a potential reviewer. OSTIF has not collaborated with X41 previously on any projects, but X41 has examined security in the Signal messaging protocol, popular web browsers, the Linux kernel, and other projects and platforms. The reviewers for this audit have experience in penetration testing, protocol design and review, and source auditing.

If selected for this audit, X41 will review the C++ implementation of Bulletproofs. They will perform a cryptographic review of the design and code, and perform an audit of the code for implementation errors and language-specific flaws. Specifically, they will determine if it is possible for an attacker to generate a false proof that an honest verifier judges to be correct, and if it is possible for an attacker to examine an honest proof and gain information about its input values.

If selected, X41 would be compensated $31350 USD. Payment would be made in XMR to OSTIF, who would complete the exchange to X41 at no additional fee or cost. X41 states that the latest end-of-project date is June 1, 2018. A statement of work from X41 is attached for public comment.

Reviewer: Kudelski Security

Kudelski Security contacted the Lab in response to a call for proposals. Researchers at Kudelski have broad experience in cryptographic design and analysis, including the design and analysis of cryptographic systems, as well as proprietary designs for smart cards and other applications. The lead reviewer, Dr. Jean-Phillipe Aumasson, has extensive experience in the cryptographic community and was the designer of the BLAKE and BLAKE2 hash functions, as well as SipHash and NIST-submitted quantum-resistant signature schemes.

If selected for this audit, Kudelski will review the C++ implementation of Bulletproofs. They will perform a review of the code for correctness, as well as identify implementation-specific flaws in the implementation. They will generate proof-of-concept code for any flaws identified, and determine steps for remediation.

If selected, Kudelski would be compensated $2500 USD per person-day of work, with an estimate of 10-12 person-days required; this yields an estimated total of $30000 USD. Payment would need to be made in USD after an exchange from XMR. Kudelski states that they are able to begin work with a month of hiring. A statement of work from Kudelski is attached for public comment.

Reviewer: name withheld

The Monero Research Lab contacted an additional security firm as a potential reviewer. However, the firm's legal team took issue with the Lab's request to have the group identified with a public statement of work prior to hiring, as well as possible issues with the public release of final reports.

The Lab is in further communication with this firm to determine if it is possible to perform a public release of their information. Until and unless such terms are met, the group is not under further consideration for funding. The Lab believes that an open and transparent audit is essential to a proper review and is in line with the Monero Project's community philosophy.

## Recommendation

The Lab recommends that the community fund reviews by Benedikt Bünz and one of QuarksLab or Kudelski, due to the unique and different expertise that each brings to the table and the excellent record of quality work from each. Bünz's review will help to assure that the underlying mathematics is faithfully interpreted into prototyping code, and the additional review will analyze the ported C++ code for implementation and cryptographic correctness. As funding is raised, Bünz should be prioritized, followed by the choice of Kudelski or QuarksLab, in case sufficient funding for both groups is not forthcoming.