Bulletproofs: Short Proofs for Confidential Transactions and More

Benedikt Bünz[*1], Jonathan Bootle[†2], Dan Boneh[‡1],
Andrew Poelstra[§3], Pieter Wuille[¶3], and Greg Maxwell[‖]

[1]Stanford University
[2]University College London
[3]Blockstream

Full Version[**]

Abstract

We propose Bulletproofs, a new non-interactive zero-knowledge proof protocol with very short proofs and without a trusted setup; the proof size is only logarithmic in the witness size. Bulletproofs are especially well suited for efficient range proofs on committed values: they enable proving that a committed value is in a range using only $2\log_2(n)+9$ group and field elements, where n is the bit length of the range. Proof generation and verification times are linear in n.

Bulletproofs greatly improve on the linear (in n) sized range proofs in existing proposals for confidential transactions in Bitcoin and other cryptocurrencies. Moreover, Bulletproofs supports aggregation of range proofs, so that a party can prove that m commitments lie in a given range by providing only an additive $O(\log(m))$ group elements over the length of a *single* proof. To aggregate proofs from multiple parties, we enable the parties to generate a single proof without revealing their inputs to each other via a simple multi-party computation (MPC) protocol for constructing Bulletproofs. This MPC protocol uses either a constant number of rounds and linear communication, or a logarithmic number of rounds and logarithmic communication. We show that verification time, while asymptotically linear, is very efficient in practice. Moreover, the verification of multiple Bulletproofs can be batched for further speed-up. Concretely, the marginal time to verify an aggregation of 16 range proofs is about the same as the time to verify 16 ECDSA signatures.

Bulletproofs build on the techniques of Bootle et al. (EUROCRYPT 2016). Beyond range proofs, Bulletproofs provide short zero-knowledge proofs for general arithmetic circuits while only relying on the discrete logarithm assumption and without requiring a trusted setup. We discuss many applications that would benefit from Bulletproofs, primarily in the area of cryptocurrencies. The efficiency of Bulletproofs is particularly well suited for the distributed and trustless nature of blockchains.

[*]benedikt@cs.stanford.edu
[†]jonathan.bootle.14@ucl.ac.uk
[‡]dabo@cs.stanford.edu
[§]apoelstra@blockstream.io
[¶]pieter@blockstream.com
[‖]greg@xiph.org

[**]An extended abstract of this work appeared at IEEE S&P 2018 [BBB+18]