Quarkslab
SECURING EVERY BIT OF YOUR DATA

Quote EH/2018/02/13

Quote date : 13-févr-18

Quarkslab 13 rue St Ambroise, 75011 Paris, France Tél. : +33 6 33 28 11 77 Email :ehoudet@quarkslab.com	The Monero LAB

Reference	Description	Days	Price per day	Cost
18-02-398-PRO	**Bulletproofs review**			
	Step 1: Understanding the protocols and isolating the main points	8	$ 1 650,00	$ 13 200,00
	Step 2: Crypto design Assessing the conformity of the C++ code	8	$ 1 650,00	$ 13 200,00
	Step 3: Looking for vulnerabilities and assessing their severity	9	$ 1 650,00	$ 14 850,00
	50% at the launch of the mission 50% upon completion of the mission			
			Total $ excl VAT	$ 41 250,00

Online payment max 30 days after bill
Late payment penalties : BCE rate + 10 points

Quarkslab, SAS au capital de 113 390 €
RCS : : Paris 538 485 897
SIRET : 538 485 897 00036
APE : 7490B
TVA FR : FR 12 538 485 897 00036

Payment to :
Banque : Banque Palatine
RIB :40978 00022 1384828V800 25
IBAN : FR74 4097 8000 2213 8482 8V80 025
BIC :BSPFFRPPXXX

STATEMENT OF WORK

Description of the request
==========

The Monero project (https://getmonero.org) is implementing a new cryptographic proof for Monero (XMR), an open-source cryptocurrency.

The Monero project currently uses Borromean-style range proofs in their confidential transactions, and plan to replace them with bulletproofs (https://crypto.stanford.edu/bulletproofs/). Moving from Borromean range proofs to Bulletproofs would significantly reduce the size of the blockchain, as well as bring down transaction fees on the platform by an estimated 70-80%.

The Monero Research Lab is interested in a limited-scope analysis of the bulletproof prove/verify algorithms, hitting as many of the following questions as possible:
1. Does their code (https://github.com/moneromooo-monero/bitmonero/tree/bp-multi/src/ringct) accurately represent the prove/verify algorithms from the bulletproof whitepaper (http://web.stanford.edu/~buenz/pubs/bulletproofs.pdf)?
2. Does their implementation allow an attacker to generate a false proof that an honest verifier judges as correct?
3. Does their implementation allow an attacker to examine an honest prover's proof and gain information about the hidden amount or other masks?

In order to test correctness, the original whitepaper's prove/verify routines has been translated into Java code (https://github.com/b-g-goodell/research-lab/tree/master/source-code/BulletProofs). The code could be used as extra material to help bridge the gap between the paper and the final code.

Quarkslab's work description
==========

The evaluation work that Quarkslab will undertake includes the three following steps:
* Understanding the protocols and isolating the main points of attention regarding implementation. (Note: The bulletproofs research results are very new. They are to be published at IEEE S&P 2018 and the researchpaper is available at https://eprint.iacr.org/2017/1066.pdf).
* Assessing the conformity of the C++ code (ringct amounts to around 3000 lines) to the specifications (and the reference source code) both from a logical and an implementation point of view, including the underlying elliptic curve arithmetic used.
* Looking for vulnerabilities and assessing their severity.

At the end of the evaluation, Quarkslab will produce a report detailing the evaluation activities undertaken and results achieved.

Considering the novelty and difficulty of the task, we are proposing a team of 2 senior evaluators in cryptography, implementation of cryptography and vulnerability research. The review would take place between end of April and end of June.

We plan to devote an amount of 25 man.days to the work proposed. The applicable rate is $1650 per man.day.