Bitcoin Private

March 16, 2018

The Bitcoin Private foundation is awarding a series of grants of up to $150,000 for research in areas of cryptography and network security that further our goals of enhancing and democratizing personal privacy. We are accepting proposals for research projects that are anticipated to last from several months up to a full year. Grants will be awarded on a rolling basis.

Potential Research Directions

Proposals should include self-contained research that is accompanied by an implementation phase or expected to be implementable and relevant in the near-term future. At the moment - we are seeking to sponsor projects that will last from three months to a year. Some potential research directions we are interested in sponsoring include:

1. Enhancing lite (SPV) client privacy
    a. Private information retrieval protocols (e.g. on Electrum server)
    b. Server based generation of shielded transactions
2. Bridging the usability gap between bitcoin script and zk-SNARKS (shielded multi-sig, time locks, etc…)
3. Efficiency enhancements to zk-SNARK generation
4. Improving anonymity at the peer-to-peer network layer (mixnets, dandelion, tor, identifying spy nodes, etc.)

Who are we looking for?

Grantees should have or be working towards a Ph.D. in cryptography, computer security or a related field. Within your subject matter, both a theoretical understanding as well as strong ability to implement or audit implementations is desirable. As the lingua franca of our global team is English, you too must be fluent.

Some other desirable qualities:

1. Very strong level of comfort both writing and reading C++ bitcoin-based code.
2. Experience identifying potential vulnerabilities and attack vectors to cryptographic systems. Confident analyzing and fixing these vulnerabilities.
3. Ability to design and prove new cryptographic constructs

How to apply

To apply - please email a project proposal outlining the research you wish to engage in, including the funding and time necessary to accomplish your goals, along with a CV to research@btcprivate.org. You may also wish to include selected prior publications and code.

When is the application due?

Please have proposals submitted by May 1st. We'll announce a first batch of grant recipients no later than June 1st. After that grants will be awarded on a rolling basis.

Who are we?

We are the Bitcoin Private Contribution Team. Bitcoin Private is a first-of-its-kind fork-merge of Bitcoin and Zclassic. This resulting blockchain offers fast transactions, low fees, and shielded transactions via a bleeding-edge privacy technology, zk-SNARKs. Our goals are to introduce zk-SNARKs and anonymous ledgers to the broader crypto community, while also bringing cryptocurrency closer to mainstream adoption.