Scholarship for Research on Zero-Knowledge Proofs #31

Benedikt Bünz benedikt@cs.stanford.edu

1 Motivation and Overview

I am applying for a scholarship to support my PhD research on Zero-Knowledge Proofs and other cryptographic systems motivated by cryptocurrencies.

Zero-Knowledge proofs are at the core of privacy preserving cryptocurrencies like ZeroCash. The success of these cryptocurrencies would not have been possible without recent advances in the practicality of zero-knowledge proofs. However, there are still many open questions that remain. For example, is it possible to instantiate the ZeroCash protocol using a ZKP that does not rely on trusted setup in a practical manner? Can we have privacy preserving transactions in connection with (privacy-preserving) smart contracts? What zero-knowledge proof systems are most useful in these situations and is it possible to improve on them? The ZeroCash foundation lists in its mission statement that it "will encourage this scientific research and educate the public regarding the substance and benefits of these scientific developments". In my PhD studies I have and will continue to attempt to answer such scientific question, as they relate specifically to zero-knowledge proofs and in general to the cryptography of cryptocurrencies. This has yielded significant results such as the development of Bulletproofs a new zero-knowledge proof system with short proofs that doesn't require a trusted setup. To continue such research and to be able to purely focus on the research topics outlined in this proposal I am asking for a scholarship from the ZCash Foundation. The scholarship will go towards both my tuition and my stipend.

2 Research Goals

One of the most immediate and tangible research goals which would be of value to the ZCash community is exploring the feasibility of implementing the ZeroCash protocol[6] using Bulletproofs[3] . Bulletproofs is a new zero-knowledge proof system that I co-authored. Bulletproofs are both asymptotically and practically very short. Unlike preprocessing SNARKs[5] Bulletproofs do not require a trusted setup, however they asymptotically take longer to verify. Given that the proofs are practically very efficient it is an interesting question whether the ZeroCash protocol can be practically instantiated using Bulletproofs. This requires optimizing the Sapling[1] circuit for the Bulletproof proving system and doing benchmark measurements. Accurate and optimized benchmark will make it easier to way off the benefits of not having a trusted setup vs. the larger transaction size and transaction verification time. As for future research research direction my main focus will be on improving zero-knowledge proofs and their applicability to cryptocurrencies. Roughly this can be divided into three areas:

2.1 Improving Zero-Knowledge proof systems:

In recent years a variety of Zero-knowledge proof systems have been developed each one with a different set of tradeoffs. A majority of my research will focus on improving these proof systems. For example I have ideas for and will work on improving the verification time of Bulletproofs and reducing the proof size for STARK and making the trusted setup for SNARKs more universal. Many of these objectives can be achieved by cleverly combining proof systems in such a way that the benefits of each proof system remain. Another concrete idea is relying on different cryptographic assumptions to achieve better properties. I will explore building a Bulletproofs-like construction from lattices to attain short quantum-secure profs. I believe that exploring and expanding the tradeoff space of zero-knowledge proof system will enable exciting new applications as well as improve existing ones.

2.2 Finding new applications for Zero-Knowledge proofs in crypto currencies:

With the ZeroCash protocol the problem of private crypto currency transactions is largely solved from an academic point of view. However, there remain many open challenges. ZeroCash only supports simple transfers of

[1] `https://z.cash/technology/jubjub.html`

money. Even a limited SCRIPT support like in Bitcoin seems non-trivial. In particular, how can we enable private SCRIPTs for private cryptographic transactions such that neither sender, receiver, amount or the SCRIPT get's leaked. A current technological hurdle is that SNARKs require a circuit-specific trusted setup that is not flexible to handle a variety of SCRIPTs. An interesting research question is how other proof techniques like Bulletproofs or even new and advanced proof systems can handle such situations. Another interesting research challenge is how to design confidential smart contracts such that multiple parties can interact with the smart contract without leaking their inputs to the contract or the output of the contract. This will likely require other cryptographic techniques such as secure multi-party computation. One important aspect when designing such systems is understanding the specific requirements of each application. Having a ceremony backed setup for a global transfer of money system may be acceptable but such a setup for each different kind of smart contract seems unreasonable. On the other hand, it is important to realize that every user in the system cares that a transaction does not inflate the total money supply but most users do not care whether the sender was authorized to spend the money. Some applications require global consensus and some require only local agreement. Carefully analyzing which properties of proof systems are optimal for which applications is an important task which requires a deep understanding of both the cryptographic tools as well as the cryptocurrency applications.

2.3 Other cryptographic tools for and from cryptocurrencies:

I will also focus on additional cryptographic tools that can increase the usability of cryptocurrencies or interact with cryptocurrencies. Specifically building randomness beacons from and for blockchains is an exciting research area. I will also work on improving mobile light clients for more scalable blockchains.

3 Evaluation

I plan to work on the topics that I outlined in Section 2 and will continuously update the foundation and the community about the state of my research projects. However, please note that my plans may evolve based on new insights and research published by others. If this is the case, I will of course communicate this openly. All of the research will be submitted

to and hopefully published in peer-reviewed academic conferences. In these publications, I will acknowledge the ZCash foundation as my funding source.

4 Qualifications

I am currently finishing the 2nd year of my PhD at Stanford. I am advised by Dan Boneh(`https://crypto.stanford.edu/~dabo`) and a member of the Applied Cryptography Group (`https://crypto.stanford.edu`) and the Crypto Currency Research Group (`https://crypto.stanford.edu/c2rg`) at Stanford. My research on cryptocurrencies includes proofs of solvency for cryptocurrency exchanges[4], randomness beacons[2, 1], and super light clients. Most recently I worked on a new zero-knowledge proof system called Bulletproofs[3] that does not require a trusted setup but still has short proofs. I attached my CV and you can find my website at `https://crypto.stanford.edu/~buenz`

5 Security considerations

My work is focussed on analyzing and improving the security of the underlying cryptography of ZCash and other cryptocurrencies.

6 Schedule

The goal of the scholarship is that I can focus on the ideas that I have laid out in the next two years of my PhD.

7 Budget and justification

A scholarship to support a PhD student for one year comes to about $80,000. It covers both the cost of tuition[2] and a salary stipend[3]. Until now I have received funding through teaching and research assistantships. Both of which are 20h of work per week during the school year. Teaching assistants help with grading homework, teaching sections, holding office hours and other organizational tasks for a class. Research assistants work on research with the professor that provides them the funding. The funding comes from the professor's research grants. If I received the scholarship I would not have

[2] `https://registrar.stanford.edu/students/tuition-and-fees`
[3] `https://gfs.stanford.edu/salary/salary19/salary_tables.pdf`

to work as an assistant. I would be extremely grateful for any support, but supporting my work for two years would enable me to purely focus on the research topics outlined above.

References

[1] Dan Boneh, Joseph Bonneau, Benedikt Bünz, and Benjamin Fisch. Verifiable delay functions. In *38th International Cryptology Conference*, 2018. URL: `https://eprint.iacr.org/2018/601.pdf`.

[2] Benedikt Bünz, Joseph Bonneau, and Steven Goldfeder. Proofs-of-delay and randomness beacons in ethereum. In *IEEE SECURITY & PRIVACY ON THE BLOCKCHAIN (IEEE S&B)*, January 2017. URL: `http://www.jbonneau.com/doc/BGB17-IEEESB-proof_of_delay_ethereum.pdf`.

[3] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In *39th IEEE Symposium on Security and Privacy (SP)*, May 2018. URL: `https://eprint.iacr.org/2017/1066.pdf`.

[4] Gaby G Dagher, Benedikt Bünz, Joseph Bonneau, Jeremy Clark, and Dan Boneh. Provisions: Privacy-preserving proofs of solvency for bitcoin exchanges. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 720–731. ACM, October 2015. URL: `https://eprint.iacr.org/2015/1008.pdf`.

[5] Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova. Quadratic span programs and succinct nizks without pcps. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 626–645. Springer, 2013.

[6] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza. Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy*, pages 459–474, May 2014. `doi:10.1109/SP.2014.36`.