Blockchain Security and Financial Cryptography
Student Thesis/Paper Competition 2016

Call for participation: We encourage submissions of student research thesis and research papers in areas of blockchain, bitcoin or other financial cryptography research. Language should be English. We seek [primarily] submissions from students which have already been graded by a university. Independent researchers and participants from start-ups are allowed, however blockchain professionals and well-funded professional researchers will not qualify for cash research prizes unless we decided otherwise.

Ethics: This is a grass-roots independent academic effort to crowd-source security research for the benefit of a broader community which intends to protect their financial assets stored in blockchains. This is primarily a game which is declared of public interest. We provide research prizes of moderate size in order to demonstrate the honest effort of researchers in order to discover security vulnerabilities in bitcoin and blockchain systems and in order to increase the awareness about potential and real attacks on these systems.

Prize Jury:

- Prof. Jan Aldert Bergstra, Institute of Informatics, University of Amsterdam
- Prof. Alex Biryukov, University of Luxembourg
- Dr. Nicolas T. Courtois, Senior Lecturer, University College London
- Ass. Prof. Stefan Dziembowski, University of Warsaw, Poland
- Prof. Jean-Paul Delahaye, Lille University of Science and Technology, France
- Dr. Aggelos Kiayias, University of Edinburgh, UK
- Prof. David Naccache, Ecole Normale Supérieure and Ingenico Labs, France
- Dr. Vassilis Zikas, Rensselaer Polytechnic Institute, US
- Dr. Paolo Tasca, Deutschebank, Frankfurt, Germany

Deadline: End of Sept. 2016. Info: http://blog.bettercrypto.com/?p=2711

Submissions: https://easychair.org/conferences/?conf=studblocseccomp16
Several prizes will be awarded in October 2016 for master thesis and other research work. E.g.

- 5 BTC for a contribution to security of bitcoin/blockchain in a Master thesis/student work.
- 5 BTC for discovery of attacks bugs or flaws in ZK proofs, ring signatures, ECCs, key management and other advanced cryptographic techniques relevant to blockchain tech.