Project Proposal

Team:

Surya Vajjhala (vajjhala@bu.edu)

Description of Project

An implementation of an asymmetric proof of work algorithm that was demonstrated by Alex Biryukov, Dmitry Khovratovich [1]. Proof of work algorithms use “amount of work” as a proof of “honest” users. In asymmetric algorithms, proving is “hard” and verification is “easy”. Relying on computationally intensive algorithms has created a disparity between various CPU architectures, especially giving ASIC- CPU- users advantage over “normal” CPUs. To combat this the present paper provides an algorithm that relies on “memory-hardness” rather than “computational-hardness:”. This way even parallel computations can be contained by constraints on memory.

Plan:

1) Implementation of a Go Library of Equihash: An Asymmetric Proof-of-Work Based on the Generalized Birthday Problem.
2) Providing an interface so that any blockchain based application can deploy this as their “proof of work” algorithm for improved security.

Description of Demo:

The demo will talk about existing proof of work algorithms like Hashcah [2] (used by bitcoin).
Show the present implementation of the algorithm with other algorithms.
Briefly demonstrate the interface provided by the algorithm.

References:

[1] Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem
http://www.ledgerjournal.org/ojs/index.php/ledger/article/view/48
[2] Back, A. “Hashcash – A Denial of Service Counter-Measure.” (2002) (accessed 29 January 2017) http://www.hashcash.org/papers/hashcash.pdf