Bitcoin Script Validation Accelerator

Team: James Lovejoy, Jonathan Harvey-Buschel

Bitcoin uses the secp256k1 Koblitz elliptic curve for cryptographic operations like signature validation, and Bitcoin transactions are scripts are written in a custom bytecode language that runs in a simple virtual machine. A majority of the machine time spent when synchronizing to the Bitcoin network is used for signature checking and script validation; our goal is to accelerate one, and ideally both, of these processes by developing dedicated cores for ECDSA signature validation and script evaluation. The accelerator will communicate with a host machine and offload the signature validation operations to the FPGA; we plan to use the DSP blocks to handle the 256-bit integers involved in ECDSA operations. If we reach this goal early, we plan to implement the full script evaluation virtual machine alongside the cryptographic accelerator. Currently end-to-end synchronizing a new Bitcoin node requires 1+ GB of RAM & 4+ GBs of storage at a minimum which would be limited to expensive FPGA models. New research at MIT allows this validation to take place using only a few KBs of storage with no loss of security; we will try to implement this scheme on the FPGA if we successfully complete the first two accelerators.