Scrypt ASIC
Prototyping
Preliminary Design Document

Revision History

Version	Date	Author	Remarks	Approved by
v0.1				

Contents

List of Figures

List of Tables

No table of figures entries found.

1 Scrypt Algorithm

The following flow chart illustrates the Scrypt algorithm used in the Litecoin module. The input to the algorithm is a 84 byte block data. The algorithm generates a 128 bytes hash, of which MSB 4 bytes is compared with the input target. If the generated hash is less than the target, the module returns the nonce for which the successful hash was generated.

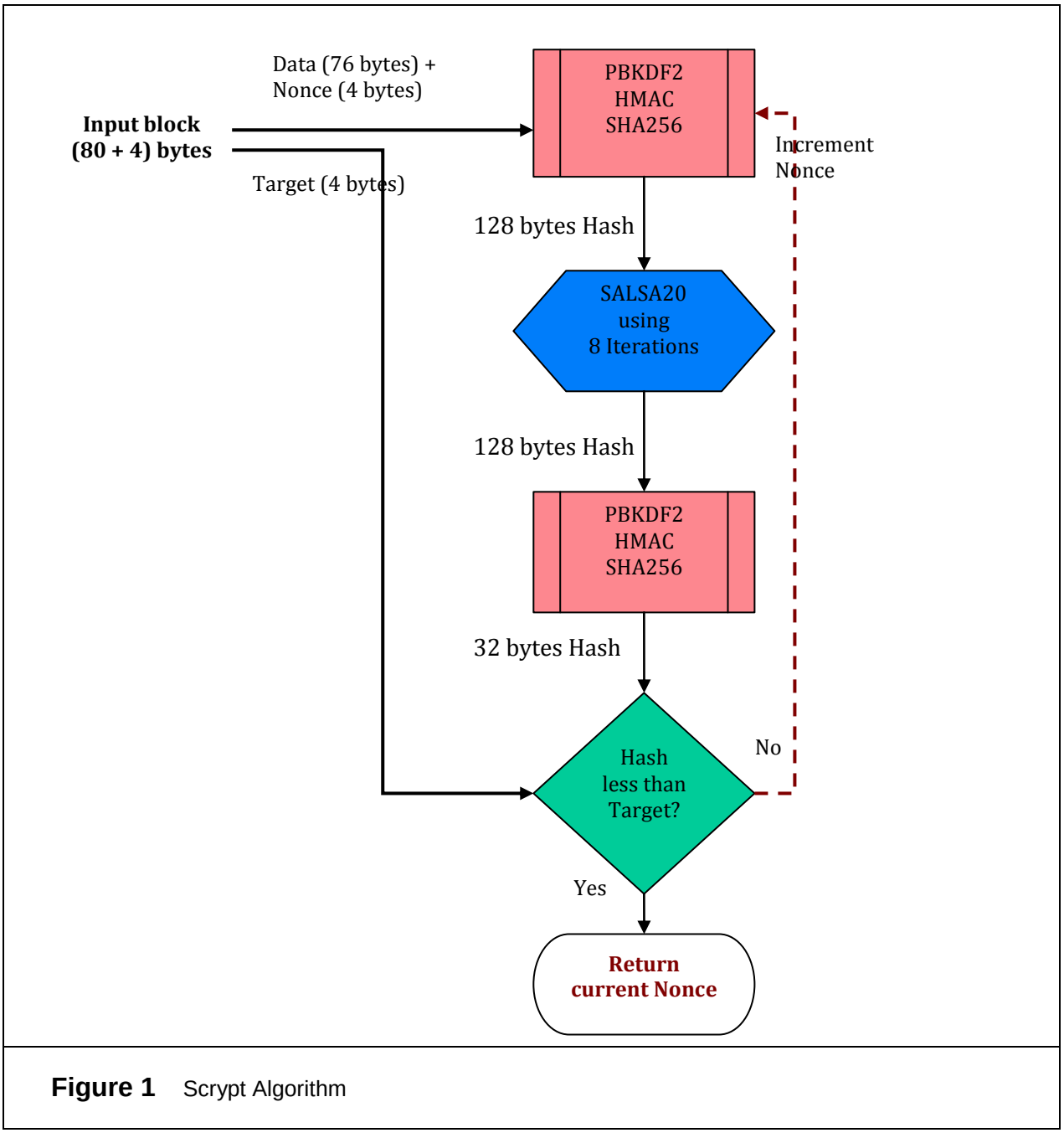

Figure 1 Scrypt Algorithm

2 Major blocks in a Scrypt core

The two major blocks in the Scrypt core is shown in the following block diagram. The blocks are similarly placed in the hardware architecture as well. The Scrypt cores require 84 bytes block as input and returns the matched nonce on successful computation of hash that is less than the target.

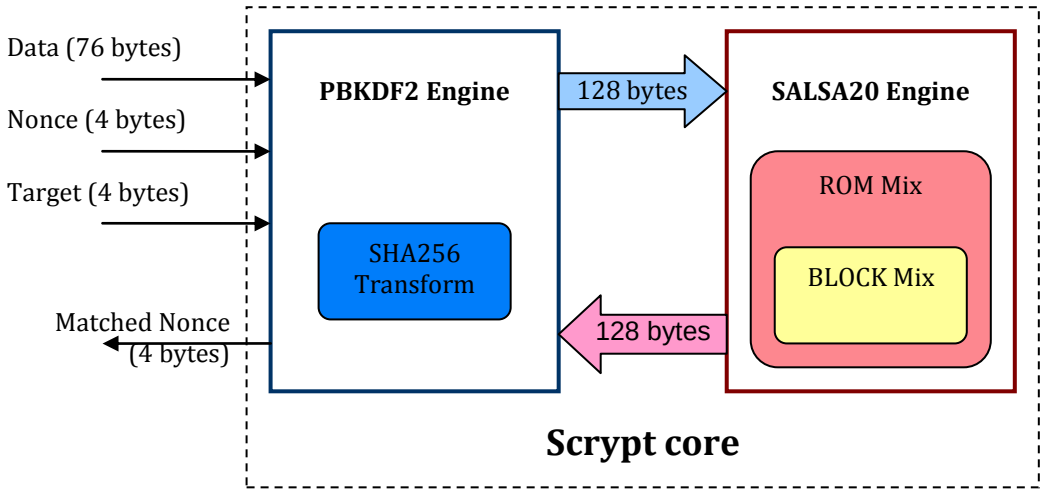

Figure 2 Scrypt Core Blocks

3 Internal architecture in an FPGA/ASIC

The basic ports in a FPGA/ASIC based Litecoin mining unit are clock, reset, serial data input/output and status LEDs. The input block data for mining is received by the FPGA/ASIC via serial communication (UART/SPI) from a microcontroller unit. A deserializer unit extracts the serial data into Blocks, Nonce and Target, and provides it to all the Scrypt cores. Each of the Scrypt core is given a core identification number to divide the nonce uniformly among the cores. After computation of one scrypt hash, each of the cores increments the nonce by itself and re-computes the hash using the new nonce. When the scrypt hash generated in any of the core is less than the target, the current nonce value from that particular core is sent to the microcontroller via serial communication.

The block diagram illustrating the internal/external communication of an FPGA/ASIC based Litecoin mining module as follows:

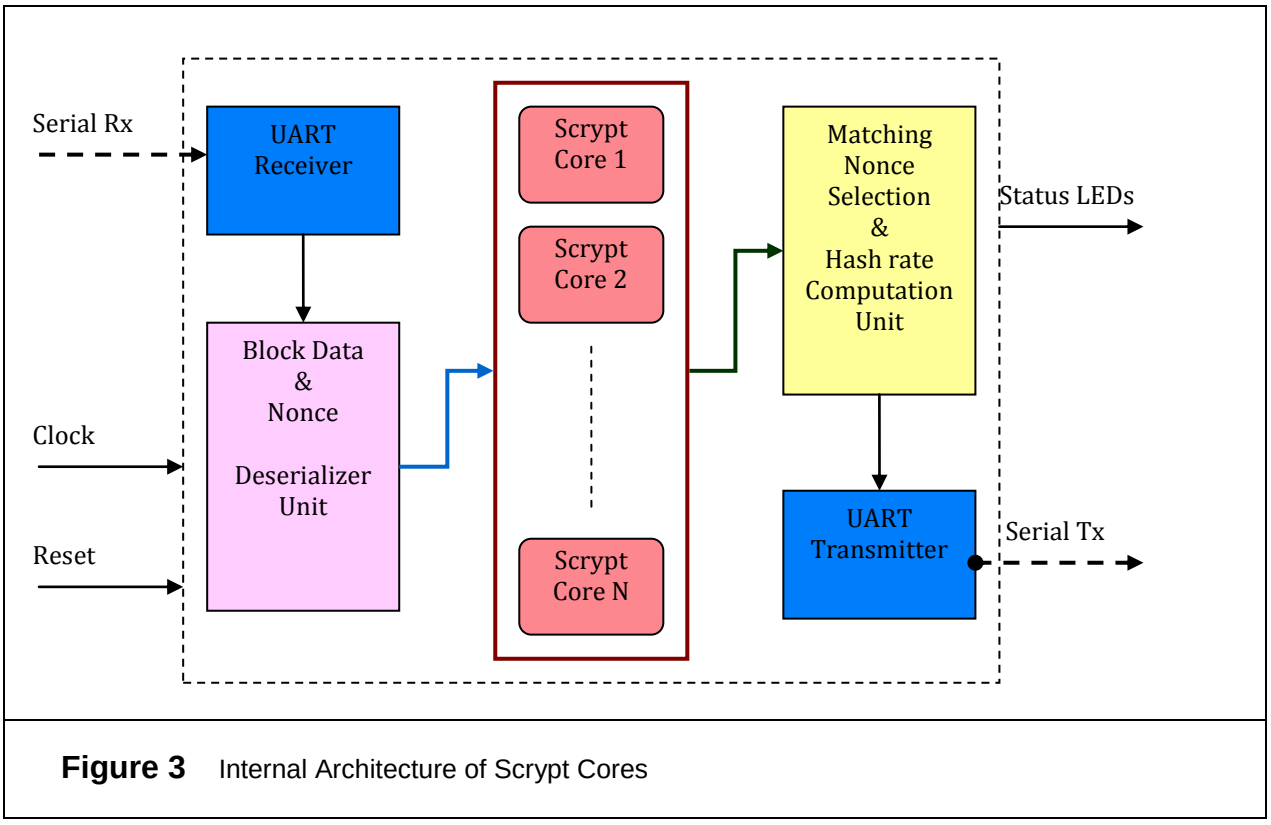

Figure 3 Internal Architecture of Scrypt Cores

4 External communication with multiple FPGA/ASIC

An FPGA/ASIC may consist of several Scrypt cores. Each of the FPGA/ASIC can be connected to an 8/16/32 bit MCU for distribution of header block to mine on single or multiple cores.

A simple block diagram using such an interface is shown in the following figure.

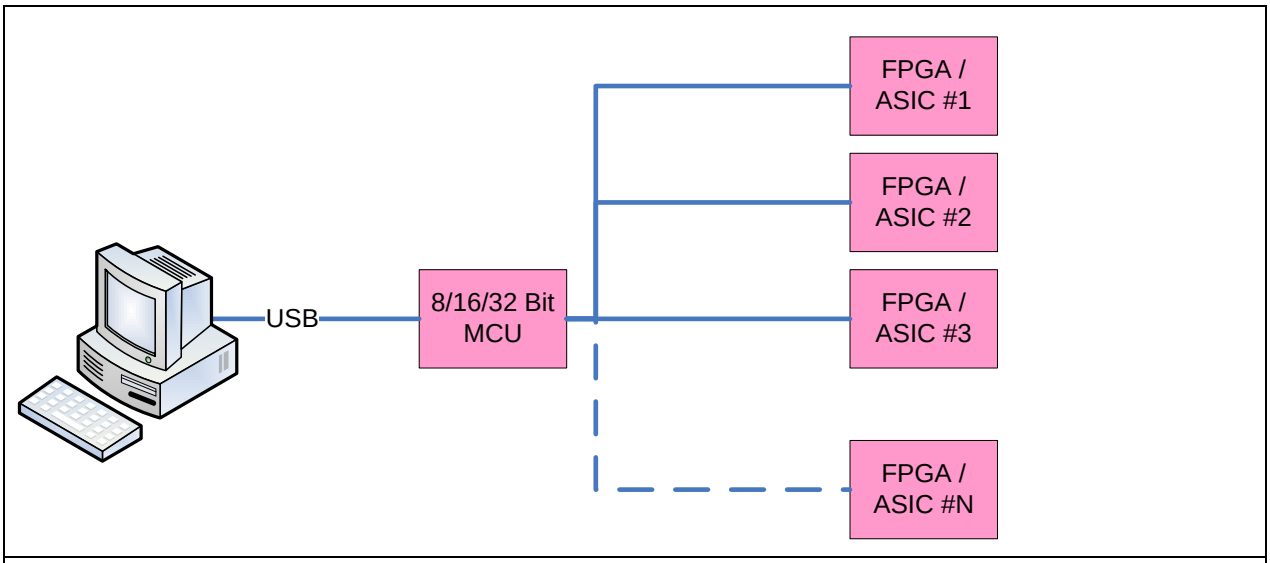

Figure 4 External Communication with multiple FPGA/ASIC

5 Proposed internal architecture for ASIC

In the ASIC implementation of Litecoin module, a total of 128 cores are available for mining. 8 groups are created with 16 cores in each group. The architecture will have the flexibility in communicating each of the cores individually or group wise. This feature will be made available by using an Address decoder/Command Parser unit. A Status Register will be used to keep track of the Nonce match/distribution status of the cores. The mining module will communicate with the external devices (computer or microcontroller) via serial communication engine (UART/SPI). A block diagram of the proposed architecture is shown in the following figure.

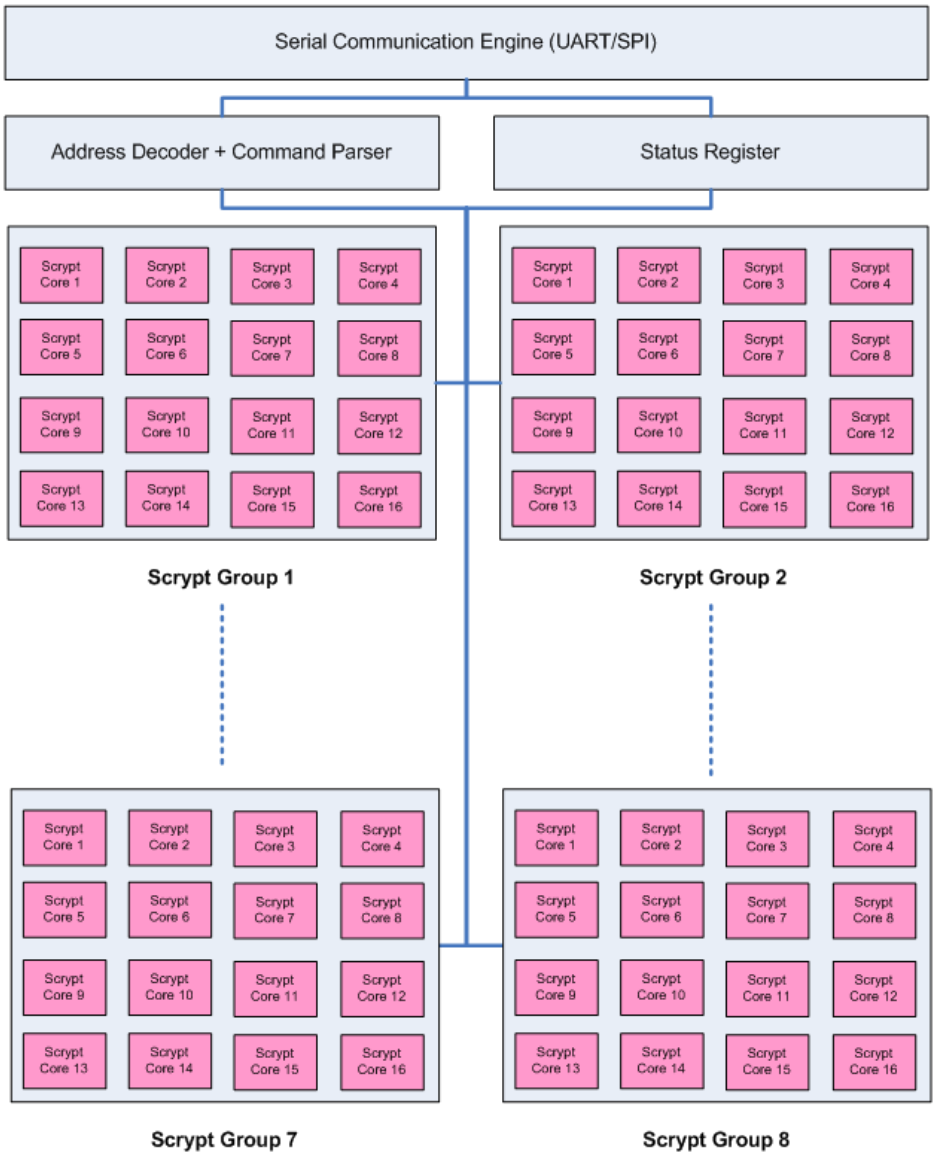

Figure 5 Proposed Internal Architecture for ASIC

The proposed packet format for communicating the mining module is shown below. This packet will be passed through the Address Decoder/Command Parser unit for configuring the Scrypt cores for mining.

Figure 6 Proposed Packet Format

Group Addr: For group wise addressing of Scrypt cores
Eg: 0x00 to 0x07 for unicast and 0xFF for broadcast

Core Addr: For addressing individual Scrypt cores
Eg: 0x00 to 0x0F for unicast and 0xFF for broadcast

Command: A command for execution in the module
Eg: Reset, Disable, Start mining, Update with new data/nonce, Read matched nonce, Specify nonce range, etc.

Data: Applicable data depending on the command used

6 Scrypt Hash Computation Complexity

Scrypt blocks	Clock cycles per block	Total Cycles
PBKDF2		
(A) SHA256 Transform	258	
(B) Serial data In and Out	32	
Total = (A + B) ×18	(258 + 32) ×18	5,220
SALSA20/8		
(C) BLOCK Mix (Mem. WR)	2 × (32+2) = 68	
(D) ROM Mix (Mem. WR)	1024 × C = 69,632	
(E) BLOCK Mix (Mem. RD)	(2 × (32+2))+4 = 72	
(F) BLOCK Mix (Mem. RD)	1024 × E = 73,728	
(G) Serial data In and Out	32 × 2 = 64	
Total = D + F + G	69632 + 73728 + 64	143,424
Serial data pre/post processing	678× 2	1,356
Per Scrypt hash computation		150,000

7 Hash rate experimented using Xilinx Virtex 6 FPGA

Device: Xilinx Virtex 6 LX240T (ML605)

FPGA resources	Available	1 core	4 cores
Slice LUTs	150,720	13,268	55,123
Slice Registers	301,440	10,955	45,179
Slices	37,680	(12%) 4,670	(49%) 18,628
BRAM (18 Kbit)	832	57	228
Total Memory (M bits) - Full RAM	14.6	1	4
Total I/O (using UART)	600	8	8
Max. clock frequency (MHz):	-	200	200
Hash Rate (KH/s)	-	1.33	5.33

Note : There are more cores possible in LX240T, however idea is to show case linearity achieved in actual as in theory

8 Target Hash rate in ASIC

Technology: 28nm/45 nm

	8 cores	64 cores	128 cores	512 cores
Virtex 6 LX240T	single	8	16	64
ASIC gates (Million)	1.7	14	28	112
Total memory (Mbits)	8	64	128	512
Hash rate at 200 MHz	11 KH/s	85 KH/s	170 KH/s	680 KH/s
Hash rate at 400 MHz	22 KH/s	170 KH/s	340 KH/s	1.36 MH/s
Hash rate at 600 MHz	33 KH/s	255 KH/s	510 KH/s	2 MH/s

Note : Above figures are estimated based on our experiments done on LX240T present on ML605