The Design of a Bitcoin Hash Processor

ECE 111 Final Project

Fall Quarter 2020

(If you are in a team of two, only one report needs to be submitted)

Date:

Team Members: (or just Name: if you did the project on your own.)

**Introduction**

* Briefly say that Bitcoin is a cryptocurrency that enables users to exchange this form of electronic cash with each other without the need for banks. (See e.g. the wikipedia page on “Bitcoin” for more info.)
* Briefly say that in order to keep track of all transactions, a “blockchain” is used to maintain a growing list of records. This “blockchain” acts as a global ledger for all transactions, where new transactions are added as new blocks to the blockchain. (See e.g. the “Blockchain” section of the Bitcoin wikipedia page for more info.)
* Briefly say that a blockchain is secure because new blocks can only be added to the blockchain by someone (a bitcoin miner) finding a cryptographic hash for the new block that satisfies some computationally difficult condition. This “proof-of-work” (which is referred to as “Bitcoin mining”) is what makes blockchains secure and unalterable. (See e.g. the “Mining” section of the Bitcoin wikipedia page for more info.)
* Briefly say that at the core of the “proof-of-work” computation is the SHA256 algorithm.
* Briefly say that the final project is a “Bitcoin-Hash Processor” that will compute different cryptographic hashes for different values of “nonces,” which will be further explained later in the report.

**Description of the SHA-256 Algorithm**

* You can describe the algorithm using a combination of the description/figures shown in the PowerPoint presentation “Lecture11.pptx,” pseudo code, etc, to adequately describe how the SHA-256 algorithm works.
* You are free to borrow “figures” from “Lecture11.pptx.”
* You can also use the “bullet points” from “Lecture11.pptx” (or any other class material), but put them in your own words.
* You can also use other references like wikipedia pages, other papers on SHA-256, but use your own words when writing the description. You can use figures from other sources (incl. pseudo-code) as long as you cite the source.

**Description of the Bitcoin-Hash Processor Final Project**

* You can describe the final project using the description/figures shown in the PowerPoint presentation “Lecture13.pptx” (or any other class material).
* You are free to borrow “figures” or use any “bullet points” from “Lecture13.pptx” (or any other class material), but put them in your own words.
* You can also use the “bullet points” from “Lecture13.pptx”, but put them in your own words.
* You can also use other references like wikipedia pages or other Bitcoin references, but use your own words when writing the description. You can use figures from other as long as you cite the source.

**Design Details**

* Briefly describe the approach/strategy that you took for the design.
* If you did two different designs, one “Area\*Delay-optimized,” and another “Delay-optimized,” briefly describe the approach/strategy that you took for the two designs.
* If you adopted strategies explained in the lecture slides (e.g., in “Lecture11.pptx,” “Lecture12.pptx,” “Lecture13.pptx,” or any other class material), feel free to use the “figures” or “bullet points” from these class materials, but write the explanations in your own words.

**Summary of Results**

* If you are just turning in one design, summarize the results for this design in terms of #ALUTs, #Registers, Area = #ALUTs + #Registers, Clock period = 1/Fmax, #cycles from the testbench, Delay = Clock period x #cycles, Area\*Delay = Area x Delay.
* If you are turning in two designs, then say explicitly that you are turning in two designs and provide the same summary of results for:
  + Best Area x Delay Design: …
  + Delay Design: … (optional) (for extra grade)
* Essentially, put your “finalsummary.xlsx” results into a table form in this report.