CryptoHash

C4: William Zhao, David Cheung, Lulu Shyr
18-500 Capstone Design, Spring 2022
Electrical and Computer Engineering Department
Carnegie Mellon University

Product Pitch

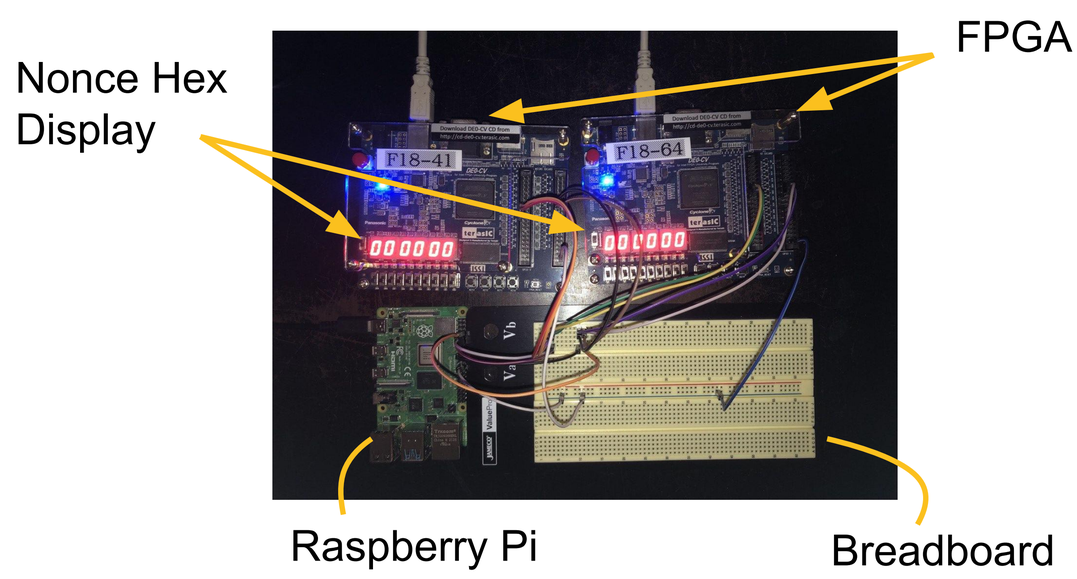
CryptoHash is a system capable of algorithmically choosing the optimal cryptocurrency for miners to maximize their revenue. It offers the flexibility of being able to mine different coins at the same time while still maintaining a competitive hashrate to a GPU. We were able to achieve a **6.38 second configuration switching time**, well below our requirement of 10 seconds. In addition, we were able to verify the functionality of the system once we scaled it to **10 FPGAs** while still meeting the requirements for each board. However, after factoring in our hashrate with local energy costs, each board on our system **loses approximately $6.57 * 10^{-9} per second**.

System Description

We are using a Pi Wedge with one end inserted into the 40 GPIO pins found on the Raspberry Pi and the other end into a breadboard. The FPGAs will receive their inputs by connecting jumper wires from their GPIO pins into the breadboard.

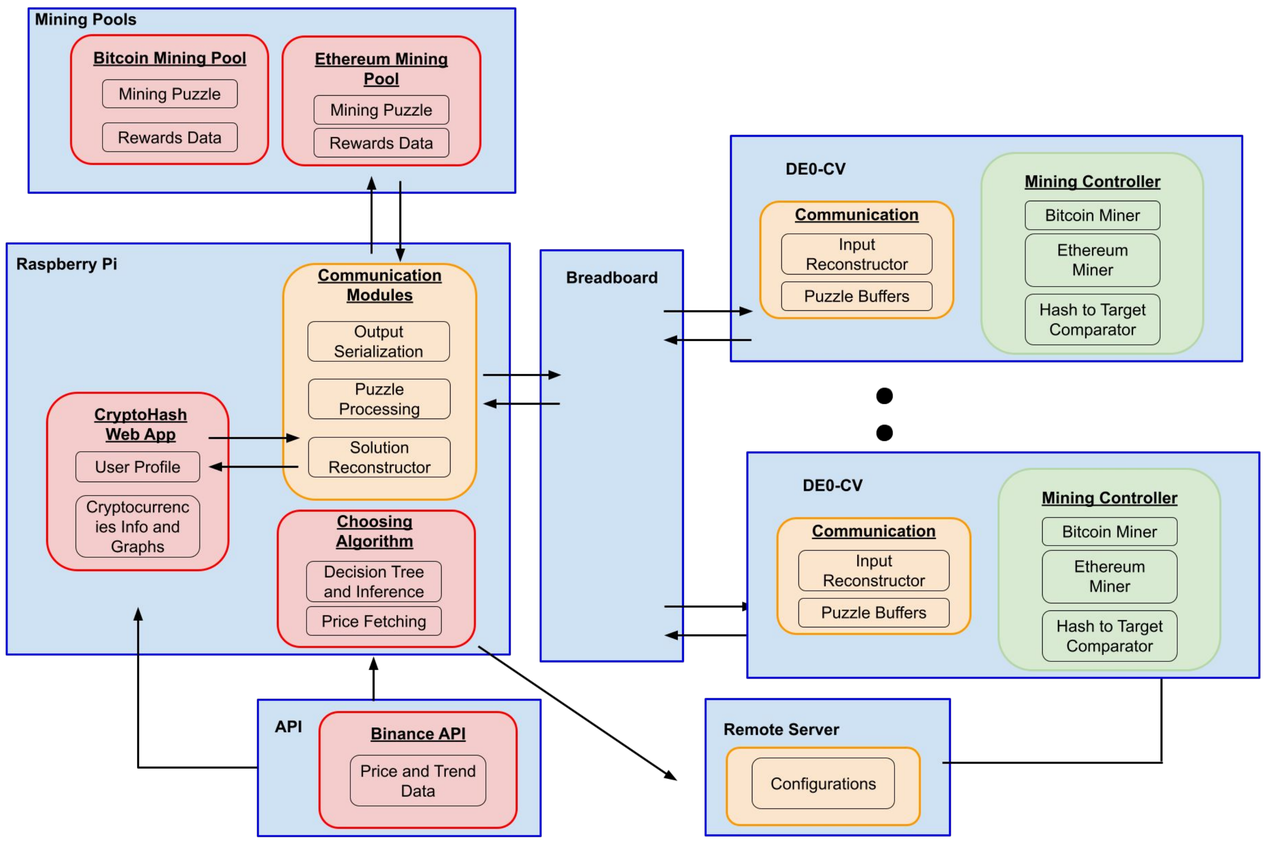
After the decision tree determines that it would be more profitable to switch to a particular cryptocurrency, it sends data to a remote server which details which board to switch and to which coin. The computer in charge of programming the boards then uses Quartus to load a new configuration onto the targeted board. The same computer will house the choosing algorithm and communicate with the mining pools for all of the coins as well.

Constructed System with 2 FPGA boards



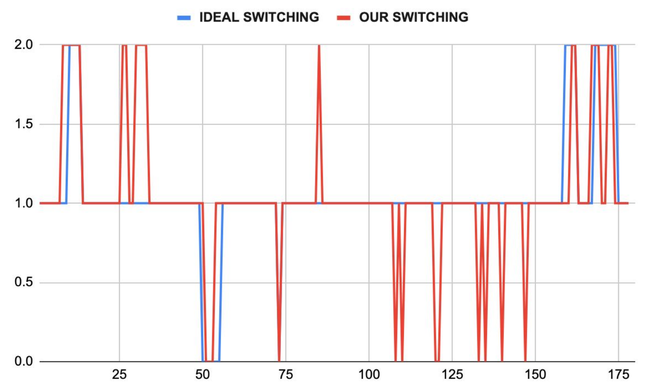
System Architecture

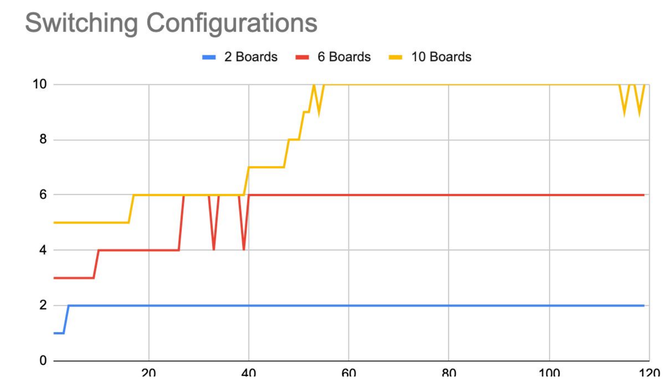
The choosing algorithm is pre-trained and uses current data on the coins to create a spread of the mining modules. The spread of the mining modules is then processed by a remote server that houses the mining configurations. The decision inference is dependent on obtaining current data about the coins from the Binance API and the cryptocurrency proof of work puzzles from the respective coins' F2Pool mining pool. All of this pre-processed on the Raspberry Pi before being sent to the FPGAs. The FPGAs perform the actual mining and send all of the correct nonces they find back to the Raspberry Pi. Finally, the Raspberry Pi sends all of the nonces to the mining pools and receives the mining reward.

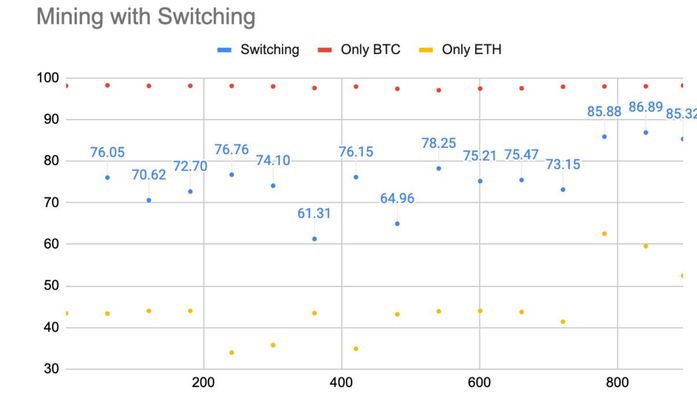


System Evaluation

For accuracy testing, we define an ideal switching that takes into account the built in robustness of the system against volatility. The accuracy measure here is 85%. The main tradeoffs for the system lie with the number of times the configurations are switched and the weights on which we predict on. Different events such as transaction volumes for coins and the changes in difficulty affect which coin to mine. Switching configurations also pose a time overhead when we have to load in a new configuration so that we can contribute as much processing power as the FPGA has for mining. Switching a configuration causes the board to also reset, invoking more overhead if we keep switching the same board. There also comes a tradeoff of robustness and profitability as we scale up the system in terms of the number of boards, where more boards invokes less robustness for higher attainable hashrates and thus more revenue from the mining pools.







Conclusions & Additional Information

http://course.ece.cmu.edu/~ece500/projects/s22-teamc4/

Overall, we were able to achieve the general concept of the system we set out to build. To expand this project, future work could examine the possibility of mining more than two coins. The decision process is also another area that could be improved upon and perhaps utilize a recurrent neural network that not only use historical data but also use inference data to continue training the model as the model performs inference. The mining modules can also be improved for each coin and optimized to improve the efficiency to achieve higher hash rates.

Electrical & Computer ENGINEERING
Carnegie Mellon