Anti-parallel Cryptocurrency

John Lore (jlore) and Richard Zhu (rzhu1) - November 1st, 2017

As the basis for a new crytocurrency, we are creating a proof of work algorthm with specifically poor parallelization on hardware such as GPUs and high transaction scalability. We aim to better democratize mining our coin by optimizing for modern day CPUs, such that anyone with a modern computer can profitably mine. Further, we plan to develop a new crytocurrency that employs this algorithm and scales transactions effectively.

Project Website

Background

Cryptocurrency is a quickly expanding subsection of computer science, first emerging onto the scene with Bitcoin in Satoshi Nakamoto's white paper. The key idea behind bitcoin is the proof of work algorithm, a.k.a. blockchain technology. This uses computation power to find a random number, or "nonce", which once summed with a block, will hash to a number with n trailing zeroes. The user who manages to first discover this nonce will be awarded the block, a certain amount of coin, and will continue the blockchain. The blockchain - history of hashes serves as a public proof of work for every transaction.

Scalability Problem

There are many problems with the current implementation of bitcoin. This has spawned many alternative currencies and forks of the bitcoin blockchain, each of which attempts to ameliorate one or more of these aspects. Take for example IOTA, a cryptocurrency which is designed for microtransactions. The current implementation of bitcoin is not conducive to microtransactions, due to the fact that the entire system can only process 3-4 transactions per second. Thus, it cannot handle a high volume of transactions, and so IOTA uses a giant graph called "The Tangle", which makes it easy to perform microtransactions. Ethereum, the second largest cryptocurrency by market capitalization, attempts to improve scalability, and has a limit of about 20 transactions per second. For comparison, Paypal currently processes about an average of 200 transactions per second, with peaks on Cyber Monday of 500 transactions per second. VISA is able to handle almost 2000 transactions per second. Clearly, scalability issues need to be addressed if cryptocurrencies are ever meant to be used for meaningful real world transactions rather than just speculation and investment. Current work is in progress to increase this maximum limit to 1 million transactions per second.

Mining Integrity Problem

Another problem with mined cryptocurrencies has to do with its integrity. One of the major innovations introduced in the whitepaper by Satoshi Nakamoto was blockchain technology. This technology makes it so the currency is not regulated by a central authority, but rather is decentralized and validated by its users. However, with this, there arises a problem know as mining

consolidation. If a single entity is able to comprise over 50% of all the mining power, then this entity would theoretically be able to out-mine everyone else, and thus eventually mine farther on the blockchain than everyone else combined. This undermines the integrity of the currency, because everyone else's hard work on their fork of the blockchain would be completely invalidated, and their currency lost and worthless. Originally, bitcoin could be mined by CPUs for profit. Today, however, it is not worth the cost in energy to mine bitcoin on a CPU, and thus miners must use specialized hardware such as high end GPUs and custom ASICs for mining to be profitable.

Summary

All these factors -- transaction latency, transaction fees, mining consolidation, and scalability -- limit the potential of crytocurrencies and their widespread adoption by businesses for everyday transactions. Targeting CPUs for parallelism of proof-of-work is interesting as GPUs are notoriously more efficent than CPUs for mining. Furthermore, the scalabilty of transactions lends itself well to being parallelized.

The Challenge

The challenge therefore is to develop a cryptocurrency which has huge scalability potential, but is balanced such that it is extremely difficult for one body to be able to amass a majority of mining power. Our coin aims to be profitably mined by any person owning a modern CPU. We aim to learn deeply about crytocurrency and blockchain technology, and seek to understand what proof of work algorithms are very efficiently made parallel on modern CPUs while running inefficiently on GPUs. We also look to understand why transaction throughput for existing coins is so low and how to make transactions scalable to be competitive with more classic currencies.

Democratized Mining

The difficulty does not lie in making our proof of work algorithm parallel, as this is conceptually easy, but in making it very parallel on CPUs specifically. We will seek to design our algorithm such that it benefits from modern CPU hardware, while exploiting issues with GPU hardware. Some examples include performing irregular memory accesses, having low arithmetic intenstity, and employing a significant amount of branching.

Transaction Scaling

Due to the low number of transactions per second possible with bitcoin, the latency of verifying a transaction is very high. At the moment, it takes over an hour for a transaction to be verified. It is our goal to be able to create an algorithm for a cryptocurrency which not only has a high throughput, but also a low latency, and a latency which does not scale as the number of users and transactions increases.

Resources

We will most likely be starting from an existing alternative coin implementation. We will be using the bitcoin whitepaper written by Satoshi Nakamoto as a reference for how bitcoin works and its

capability. We will be using whitepapers for other cryptocurrencies as well, to determine strengths and weaknesses already present in existing coins. All the code for popular alternative currencies are open-sourced, and they all have whitepapers published. We will run our algorithm on our personal computers, and will verify that NVIDIA GPUs are unable to mine more effectively than CPUs for specific CUDA implementations.

Goals

We plan to achieve a working cryptocurrency which is demonstrably parallel on moderns CPUs and is resistant to GPU parallelization. If we are unable to accomplish everything we wish, a reasonable fall-back goal is to design and implement simply the proof of work algorithm behind the cryptocurrency and demonstrate that this algorithm is difficult to parallelize among GPUs, but parallelizes well among CPUs. This would eliminate all the overhead and increased difficulty of actually implementing the cryptocurrency in totatality.

Stretch Goals

In regard to what we hope to achieve, we would like to actually refine this into a usable and minable currency and publish it for use by the general public. Ideally, we'd like to extend our algorithm to run poorly on custom ASICs and FPGAs in addition to GPUs. Furthermore, we'd like to make our coin pooling-resistant, such that a miner controlling a botnet would have little to no advantage. If we somehow accomplish even these goals, we would like to focus on our coin supporting high latency interplanetary transactions with integrity. Martians will need to be able to exchange goods and services with Earthlings, too. This resultant crytpocurrency would have high viablity and potential.

Demo & Presentation

For our presentation and demo, ideally, if we are able to accomplish our reach goal and deliver a true minable cryptocurrency, we would be able to complete transactions from one user to another, and so we would hopefully be able to demonstrate that, along with a demonstration of a miner validating the transaction. Minimally, we will show live demonstrations of mining on CPUs and GPUs alongside graphs depicting the speed comparisons.

Platform

We plan on using C++ as our language of choice. This is because bitcoin and most subsequent cryptocurrencies are written in C++. The reasoning for this is that these cryptocurrencies must be extremely consistent across all platforms, or a fork will happen in the blockchain. Additionally, C++ has great performance, which is preferred in order to maximize the number of transactions per second. Our cryptocurrency will be platform agnostic. It should not matter which system one is using, given they have a modern CPU.

Schedule

Week of 10/30/2017: Finalize project idea and plan, begin research.

Week of 11/06/2017: Finish research and complete initial design of proof of work algorithm.

Week of 11/13/2017: Create sequential version of algorithm and coin.

Week of 11/20/2017: Parallelize mining for the CPU and transactions for scalability.

Week of 11/27/2017: Attempt parallelization on GPUs, showing that CPUs are more efficient.

Week of 12/04/2017: Work on stretch goals and wrap up project, including presentation and writeup.

Week of 12/11/2017: Put finishing touches on the presentation & writeup and present our project.