Phase I

zk-SNARK Privacy and a Holistic Approach to ASICs

Michael J. Toutonghi

June 13, 2018

Introduction

Since purpose built ASICs (application specific integrated circuits) started dominating Bitcoin mining, making electricity costs to mine bitcoin on a general purpose PC more than the Bitcoin mined, the cryptocurrency industry, in aggregate, has invested extraordinary amounts of research and development to create "ASIC resistant" hash algorithms. Although recently, a debate has raged as to the effectiveness or ultimate futility of developing ASIC resistant algorithms to ensure that public cryptocurrency mining remains the decentralized process originally envisioned in Satoshi Nakamoto's seminal Bitcoin Whitepaper [2].

On May 3rd, 2018, weeks after a Monero hard fork to enable a new ASIC resistant algorithm and eliminate ASIC mining of Monero, major ASIC manufacturer, Bitmain announced availability of an Equihash ASIC [4], shattering hopes that Zcash's Equihash, the last believed bulwark of ASIC resistance might last as a profitable, GPU mineable algorithm. Prior to this announcement, we on the Verus project had been hotly debating what solution might address the risk of centralization through ASICs facing cryptocurrencies today. We decided to consider solving, not just a problem of ASICs alone, but the holistic issue of centralization vs. decentralization.

If, as we and most computer scientists agree, any proof of work algorithm will eventually succumb to extreme hardware acceleration [3], given enough economic incentive, perhaps fighting against what is basically a consequence of thermodynamic law isn't the best or most efficient way to address the real issue that Satoshi Nakamoto cared to address, centralization. Furthermore, when an algorithm made intentionally difficult to implement in hardware that is slow on normal CPUs or even GPUs is finally converted to hardware, such an algorithm has the potential to be accelerated so significantly by an extremely small number of capable hardware designers that the centralizing effect of such a newly developed ASIC can counteract any previous decentralization gained from the initial ASIC resistance.

As past low level assembly language developers, we on the Verus project, sharing a strong commitment to fair distribution and decentralization, asked the question, "is there an ASIC equivalent in modern CPUs that will give them an advantage today over GPUs or today's ASIC designs?" Furthermore, we asked another question, "how can we preserve decentralization and value the work invested through decentralized, non-ASIC mining, even after value has grown so much that the eventual ASICs are made?"

We searched for suitable answers to these questions, and as a result of our research, discovery, and development, created VerusHash, an exceedingly CPU-friendly, quantum secure, long input hash function that uses the quantum secure, short input Haraka512 V2 as its core compression algorithm, resulting in the fastest known cryptocurrency hash algorithm available for todays CPUs. Better yet, it is fast, not due to the general purpose nature of the CPUs themselves, but due to heavy investment by Intel and AMD on the performance of specific, highly leveraged and complex cryptographic instructions from the AES-NI and AVX instruction sets, effectively an ASIC in the CPU. The development of VerusHash, a brand new, CPU-optimized cryptocurrency hash algorithm enables an infancy stage for Verus as a coin, similar to the stage that Bitcoin enjoyed, starting upon its release for CPUs and PCs worldwide to excel in mining and participate in bootstrapping the Verus network, while receiving outsized rewards for their early support.

To augment our new CPU-friendly proof of work algorithm with even more centralization resistance, we developed a unique proof of work / proof of stake hybrid algorithm for combined mining and staking that is immune to fluctuations in network hash rate. We did this to further harden the chain against future ASICs and proof of work only attacks that may ever be mounted by new ASIC systems. This approach will always enable the pre-ASIC participants to participate in rewards as long as they continue to use and save in the currency. To ensure independence from physical hash rate, Verus' proof of stake difficulty is managed completely relative to the proof of work progress, not as a separately managed difficulty. That means that mounting a 51% hash attack against such a hybrid algorithm operating at 50% proof of work and 50% proof of stake, even if there were such a thing as a Verus ASIC in the hands of a few, would effectively require much more than 51% of the network hash power and/or a great deal of the Verus coin supply as well.

With these new algorithms development underway, we further considered what we, as members of the Verus community should do if, once the economic incentive grew large enough, an ASIC was eventually developed for VerusHash. For many of us who believe in the original Bitcoin vision, the actual thing to be concerned about is centralization, not ASICs exactly, but ASICs in the hands of a few. So, in the event someone does develop a VerusHash ASIC, would it be possible to have a permanent solution to the problem of centralization, if not thermodynamics, that enables true decentralization in a fair and equitable manner, with an on-ramp if needed for Verus community members?

This is when we evaluated VerusHash from another perspective, which is whether or not we believe our development team would be capable of leading development of an open source ASIC and making it available to the broader Verus community if anyone else is suspected to have developed an ASIC. We believe that such an effort is within our capability, and should it become an actual goal of our community, we are confident that other capable engineers would likely join and accelerate such an effort for the benefit of the community itself. We have no plans at this time to realize such an ASIC, but given our goals and belief

in decentralization, if we do undertake such an effort in the future either in response to an outside development effort or the wishes of our community, we fully intend to make such hardware available to everyone who wants it, open source and at the lowest possible cost.

VerusHash

VerusHash is a long-input hash function based on a Haraka512 V2 [1] core. Haraka512 V2 is designed as a short input hash to exclusively consume one chunk of 512 bits and produce 256 bits of a hash result, with 256 bits of cryptographic security against classical attacks and 128 bits of cryptographic security against quantum attacks, VerusHash is a specific digest that uses the Haraka512 V2 short input hash algorithm as a core compression function, takes any length of input, and produces a 256 bit hash result unique to VerusHash that also provides the same security guarantees as Haraka512 V2, making it both 256 bit secure for classical computing attacks and 128 bit secure against quantum computers [1].

While VerusHash has not yet been implemented for GPUs, which may turn out to be slower at VerusHash than CPUs, let alone FPGA or ASIC hardware, it's Haraka V2 core is based on the AES encryption standard and leverages modern CPUs internal AES instructions and the massive investment of Intel and AMD that is behind them. This makes VerusHash extremely fast on modern CPUs, and since it is based on standard AES operations, can offer both strong security guarantees and freely licensable building blocks that will enable the Verus community, not just ASIC manufacturers with the biggest pockets, to have competitive ability to develop and make available open source hardware solutions to Verus miners when such economics make sense.

We have a lot to do on the Verus project that is not that, and we will put our efforts towards such an effort only if it becomes clearly necessary to defend the broader community decentralization or if the Verus community collectively decides that it is time to make an ASIC for the algorithm. Until then, to help answer the question of potential GPU performance at least, jl777, lead developer of the Komodo platform, Verus community member, and adviser to the Verus project is offering a 1 Bitcoin bounty for any developer who can make a GPU miner for VerusHash that runs on commodity GPUs (gaming or mining GPUs under $1000) and is able to beat a similarly priced CPU by delivering more than 5x the hashrate. To implement such an algorithm, a GPU developer will need to implement both VerusHash and Haraka512 V2 as accelerated GPU code. We will describe the basic operation of VerusHash here, enabling those skilled in the art to attempt such development if they so choose.

To understand the VerusHash algorithm, it helps to separate the digest from the core, and consider the Haraka512 V2 core as an abstract compression function that takes 512 bits (64 bytes) of input and produces 256 bits (32 bytes) of output. Given such a compression function, pseudocode for the VerusHash hash digest is as follows:

```
parameters:
source_pointer (unlimited number of bytes)
dest_pointer (256 bits)
source_length

code:
last_hash (256 bits) = 0
input_pointer = &source_pointer
digest_buffer (512 bits)
digest_buffer_lo (alias of low 256 digest_buffer) = undefined
digest_buffer_hi (alias of high 256 digest_buffer) = undefined

while source_length > 0
  digest_buffer_lo = last_hash
  digest_buffer_hi = zero padded input_pointer data up to min(source_length,32)
  input_pointer = input_pointer + min(source_length,32)
  source_length = source_length - min(source_length,32)
  last_hash = haraka512v2(digest_buffer)
end while

return last_hash
```

Verus Proof of Stake

In addition to a state of the art, highly optimized cryptographic hash algorithm, the Verus blockchain also combines that proof of work with a consensus method known as proof of stake. Combining both approaches as security solutions in one blockchain, enable Verus to provide increased decentralization by leveraging two different, but intersecting populations of interested network parties, those who mine and stake, and more broadly, those who only stake. This enhanced decentralization contributes to security, by requiring a combination of attack vectors to be successful in order to mount a 51% attack on the network.

To ensure a fair, statistical method to determine the validity of a proof of stake claim to the right to process a block of transactions and receive its block reward, Verus combines a specific combination of data into a hash, adjusts that hash mathematically based on the amount of Verus Coin in the staking operation, and then compares the result to a difficulty target, much like the process of comparing hash to a target difficulty in POW.

For simplicity, this operation is done by a staking party on each of their unspent transaction outputs, or UTXOs, that are not coinbase transactions. Since Verus Coin follows the Zcash rule that coinbase transactions must first be shielded to a private address before being used, staking works on any transparent, non-coinbase UTXOs. When a staker performs the test for eligibility and discovers a winning UTXO for a block, they can add that UTXO as a no-fee spend to themselves to the end of that block, validate the block in all other respects, and submit that block to the Verus network, along with the coinbase transaction, which pays new coins to the same address of the staking transaction at the end of the block.

To prevent any ability of the staking party to influence their chances of successfully

staking a block by generating numbers that could influence their outcome, Verus proof of stake requires that the source transaction for a minted, or staked, block has had at least 150 confirmations before it can be used to mint a block and receive the block reward. This prevents even a blockchain chain reorganization from changing the eligibility of a staking transaction.

In addition, the Verus proof of stake calculation hashes past data from the blockchain, specifically, the block hash of the block 100 less than the block being minted, along with the transaction ID of the staking source, the output number of the staking source, a seed from the Verus blockchain, and the block height of the block to be minted, then it divides the hash result by the number of satoshis in the source UTXO and compares that value to the current proof of stake difficulty as determined by the difficulty algorithm. If the number is less than or equal to the target, the staker submits the block to the network, and the block is either orphaned behind another winning block or added to the Verus blockchain.

The end result is an algorithm that provides a statistical probability of winning the proof of stake competition that is proportional to the total amount being staked in UTXOs by any participant. In addition, the Verus network adjusts the difficult of the proof of stake target based on an exponentially adjusted, linear weighted moving average of the ratio of proof of work blocks to proof of stake blocks, without regard to actual block time. Proof of work difficulty is adjusted based on the total block solve times, including both proof of work and proof of stake. This approach makes the proof of stake difficulty independent of hash rate and immune to disruption by hash attacks, further ensuring the integrity of the entire Verus system.

Emission Schedule and Time Locked Rewards

We had a few requirements that we planned to adhere to when deciding the block reward schedule that we believed would provide the best motivation, not just for us, but for anyone in the community that wanted to contribute to the project, both now and in the future. Our goal was to create a fairly launched coin that we would mine and earn like everyone else, but since we know that we want to use it as a platform for realizing a longer term vision, would commit to donate back the majority of our earnings to help create a project more valuable for the world in the process. While we hope that others who believe in the Verus project donate to the development fund through the development donation address, the Verus Core developer's donation is not conditional on any other party.

We all know there are challenges in funding the continued development of a project that is fairly launched, as quite often, people who participate early in accelerated rewards are thinking very short term and supplemental donations aren't always forward looking enough to support a broad and strong development effort. At the same time, our goal was to create a fairly launched cryptocurrency that through our early participation, could enable funding of long term development as members of a community with a longer term outlook, many who may also enjoy contributing to the success of the project in other ways than mining or staking. We also wanted to reward those who supported the project in the early days, weeks, and months after launch, with rewards weighted by their early support of the Verus vision.

We considered what issues could arise with any fair emission schedule that released significantly more coins in the early months than later in the project, and one concern that immediately came to mind after seeing other projects, was the potential for anyone to heavily dump supply on an early project due to a short term self interest to quickly capture, rather than allow growth, or help create value. We decided to avoid that concern for everyone, ourselves included, by making the largest emitted blocks in the early months of mining randomly time locked to open in a manner that provided uniformly random supply at a rate lower than the first unlocked month of supply. We also decided to make the time locks start to open a few weeks after mining started on the first major release of still accelerated supply so that a new phase of miners could earn rewards before the early, more advantaged miners rewards began to open, our own included.

We believed that this would help enable those who had a real interest in the project to openly and fairly earn more coins than those with a shorter term outlook in spite of the longer wait for rewards. We knew that our own perspectives were not short term, and that we would be interested in mining time locked coins, so in the spirit of a fair launch, we designed that into the emission schedule and mine and stake for time locked coins, for ourselves and in larger amounts, to donate to the Verus project.

Summary

By adding proof of stake as a security and reward component of the Verus blockchain, developing VerusHash to close the performance gap between regular CPUs, GPUs, and ASICs, and ensuring a long term option for community open source hardware should the need arise, we believe that Verus Coin provides, once and for all, a fair start, decentralized cryptocurrency with a long term, permanent solution to the centralizing force of today's ASIC challenges, enabling decentralized CPU mining for the indefinite future, and a plan for decentralized and easy ASIC availability for the community when and if we all decide it is an appropriate time. Happy mining!

References

[1] Klbl, Stefan, et al. "Haraka v2 – Efficient Short-Input Hashing for Post-Quantum Applications." International Association for Cryptologic Research, 24 Dec. 2016.

[2] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin.org, http://bitcoin.org/bitcoin.pdf

[3] Vorick, David. "The State of Cryptocurrency Mining." Sia.https://blog.sia.tech/the-state-of-cryptocurrency-mining-538004a37f9b. Accessed 12 Jun. 2018.

[4] @BITMAINtech. "Pleased to announce the Antminer Z9 mini, an ASIC miner to mine #Equihash-based cryptocurrencies. To prevent hoarding and to let more individuals worldwide get one, we've set a limit of one miner per user. Order here (https://goo.gl/fqzDLV) now while stock lasts! #AntminerZ9." *Twitter*, 3 May 2018, 6:34 AM, https://twitter.com/BITMAINtech/status/992034662875779072