X25X:A Proof-of-Work GPU Mining Algorithm

The SINOVATE Developers
https://sinovate.io/

Abstract

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing
the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest
proof-of-work chain as proof of what happened while they were gone.

Satoshi Nakamoto

1. Custom X25X Algorithm

To protect and enhance the decentralization of the SINOVATE blockchain, a leading-edge custom proof-of-work hashing algorithm was innovatively developed and implemented. The X25X algorithm is a brand new algorithm best suited for GPU mining. It is also ASIC, FPGA, and Quantum resistant with the addition of SWIFFTX to the algorithm chain. Ultimately, the X25X hashing algorithm prevents large mining operations or farms from dominating the SINOVATE blockchain. It is praised for being a very secure, fair, decentralized, and highly accessible method by which to mine SIN coins. The X25X is an excellent example of how SINOVATE is evolving blockchain technology.

2. The Problem

FPGAs and ASICs are expensive machines that cannot be used for other tasks (unlike GPUs and CPUs). Furthermore, FPGA programming is much more complex and resource-heavy for an ordinary user. This leads to centralization and risk of control by single entities. Instead, everyone should be able to mine their coins. This is the original Bitcoin idea, a truly decentralized cryptocurrency must be open to all who want to join and contribute.

The current efforts by the developers of cryptocurrencies have not been overly successful: most of the coins released with this aim are thwarted in their claims of being ASIC/FPGA resistant. Many fall prey, just several months after they are released, even sometimes weeks.
The purpose of the original X22i whitepaper was to design a proof of work algorithm that could provide the best possible combination of the following points:

- Make ASIC and FPGA design much more difficult and expensive
- Allow GPU optimised miners to be developed quickly
- Allow GPU miners to have maximum efficiency
- Add quantum resistance
- Use components which are proven, industry standard algorithms, like sha-2 and sha-3, for best security

So far, X22i has proven to be successful, but for its effort to last, it needs to evolve and adapt to the increasing computing power and efficiency that current hardware does have. It was also necessary to make FPGA design (and thus ASIC chip design as a consequence) much less profitable, because of the short timeframe for using the product.
Additionally, X25X aims for lower power consumption of GPUs.

3. FPGA and ASIC Resistance

X25X pursues the goal of ASIC and FPGA resistance by implementing multiple additional features over the standard proof-of-work algorithm chains like X11. One of these features is increasing the memory requirements by a factor of 24 (our previous algorithm X22i was by a factor of 4 over x11), which is not a problem for CPU and GPU but much harder to deal with for FPGA and ASIC; the reason for this is they need to either use commodity RAM (giving them no advantage over CPU and GPU) or implement more internal ram, increasing the chip space needed.
Additionally, X25X has a new shuffle stage, working on the 1536 bytes buffer (for every nonce) with random access. It prevents a wide swade of optimizations that defeat the purpose of the bigger buffer, and also deters private miners coming out with secret tricks involving, for example, combining multiple algorithms into one (because the output of every stage is needed for the final result). This also indirectly promotes the writing of clean code for the algorithm, so that the open-source code is more valuable both in terms of quality and hash rate. This is important in the long term.

Another advantage of this stage is lower power consumption for GPUs, as the stage is dependent on random RAM access, which puts wait cycles in the process.

Compared to other PoW algorithms, ours is a much longer algorithm chain: 25 algorithms create the need for a lot of chip space to implement the whole chain, which is not very cost-effective for FPGA and ASIC.

Finally, the bigger plan evolving around X22i and continuing with X25X is to increase the chain size with further hashing stages, to be released periodically. This approach forces the chip designers to revise the design often, meaning more costs and less time for actually using the chips for mining. Moreover, making the chain progressively longer addresses the concern of future FPGA chips bigger in size, and being possibly able to fit the whole X25X chain in a single chip (leading to much higher efficiency).

4. GPU Miner Software Development

Being X25X, a chain of well-known hashing functions, coding a GPU miner is mostly a work of assembling open-source code. X22i currently has many implementations, both private and open source, and the missing stages to reach the full X25X chain are all available as open source as well (except the shuffle stage, which is new, but is simple to implement on GPU code).

Many overly-optimized sources will not work or need to be heavily modified, as they do not provide full output for all the algorithms in the chain. This is good because it should decrease the hash rate difference between private and open source miners.

5. Quantum resistance

A big concern in the crypto community, linked to centralization, but with even worse consequences, if ever exploited, is the possibility of “breaking” the hashing algorithms used in the current coins with a quantum computer. A particular entity with access to this kind of hardware could be able to achieve a considerable efficiency advantage over the rest of the miners, or even being able to make an “extreme 51% attack”, reverting a big chunk of the chain and introducing the possibility of double-spending, and total control of the blockchain.

To address this issue, X22i introduces a post-quantum element in the chain, SWIFFTX, with lattice-based cryptography. Of course, this component is also present in X25X.

The threat of quantum computers while present is not yet something active though continually evolving, as seen with Google's recent advancements.
The consequences of a quantum computer being able to break Sha-256 (the algorithm used by Bitcoin) would be far-reaching beyond cryptocurrency with most websites and other internet traffic using the same or similar encryption methods. SINOVATE will continue to monitor this situation and add further protection if necessary, with our ever-evolving algorithms.

"Its main attractive features, among others (including no known quantum attack at the time this paper is written), are probably rigorous asymptotic security analyses and asymptotic efficiency."
(https://eprint.iacr.org/2012/343.pdf)

An active ASIC, FPGA, and the Quantum resistant algorithm is essential for the mining community. It defends the blockchain against attacks as described earlier.

Mining hardware for SINOVATE is readily available and offers a range of entry levels for participants that are as inexpensive as the vast array of GPUs available. This means the hardware used to mine the coins is readily available and guards against the centralization threat from specialized ASIC and FPGA manufacturers.

X25X is the natural evolution of X22i, the previous algorithm used for SUQA cryptocurrency before rebranding to SINOVATE with further improvements on ASIC and FPGA resistance. It aims to help rejuvenate and sustain the GPU mining community and enhances the decentralization of the network.

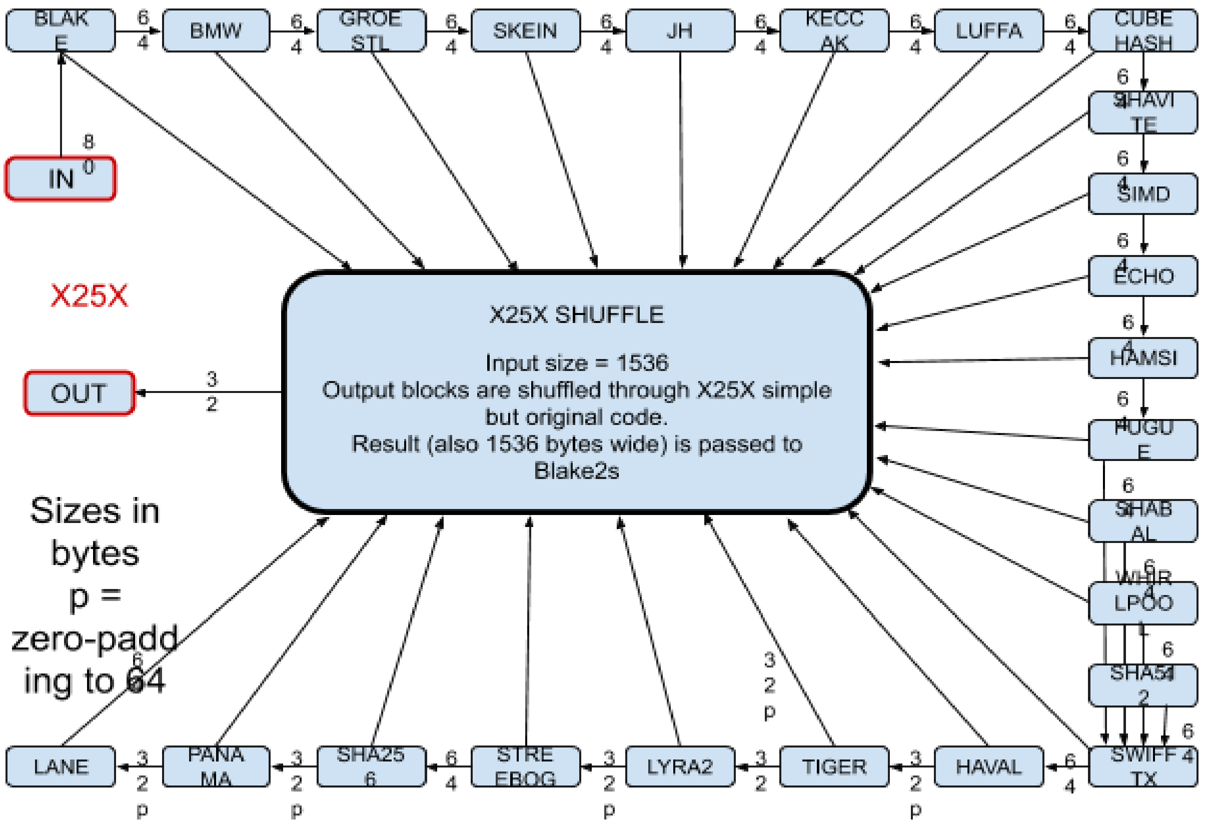
X25X follows the goal of ASIC and FPGA resistance by implementing multiple additional features over the outdated proof-of-work algorithm chains like X11 that are now dominated by ASIC miners.

X25X raises the memory requirements of X22i by a factor of five. This is not a problem for CPU and GPU mining but much harder for FPGA and ASIC. They need to either use commodity RAM (giving them no advantage over CPU and GPU) or implement more embedded internal RAM, increasing the chip space needed.

Another advantage over the classic proof-of-work algorithms is in having a much longer algorithm chain. Twenty-five algorithms make up the full chain, which again creates the need for more chip space to implement. This is hugely cost-prohibitive for FPGA and ASIC manufacturers.

Finally, the more excellent plan evolving around X25X is to increase the chain size with further hashing stages (X27mh, X3XX,) to be released periodically. This approach forces the chip designers to revise the design often, meaning more cost and less time for using the chip for mining.

Moreover, making the algorithm chain progressively longer addresses the concern of future FPGA chips growing to accommodate the whole X25X chain on a single chip.



6. Linearly Weighted Moving Average (LWMA) Difficulty Adjustment

“To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.” - Satoshi Nakamoto.

To ensure that blocks timestamp at more or less regular time intervals, the difficulty associated with successfully mining blocks has to fluctuate to take into account the overall hash power committed to the network. When there is an increase in network hash power, the difficulty has to rise to prevent miners from mining too many blocks within a specific time frame. Difficulty adjustment algorithms have been designed, tested and implemented to improve the way in which the mining difficulty responds to fluctuating network hash power, however small or large.

Since the innovative Dark Gravity Wave v3 algorithm was implemented into DASH in May 2014, developers have been testing better methods by which to improve difficulty adjustment with smoother transitions. There have been countless examples of blockchains that were subjected to massive boosts of hash power, over short periods of time, by malicious third parties. This practice resulted in that particular miner gaining large amounts of coins by mining a significant number of successive blocks while exploiting the lag in difficulty adjustment. It has particularly affected blockchains with small overall hash power networks. This has become less prevalent over time as better difficulty adjustment algorithms have been released and then implemented.

More recently, more advanced difficulty adjustment algorithms have been released and adopted after meticulously testing phases. SINOVATE has been at the forefront by integrating the latest difficulty algorithms into their code protocol. In particular, the LWMA Difficulty Adjustment Algorithm is being used to solve 51% attacks and functions as follows:

It estimates current hashrate in order to set difficulty to get the correct solvetimes by dividing the harmonic mean of the difficulties by the Linearly Weighted Moving Average (LWMA) of the solvetimes. It gives more weight to the most recent solvetimes. It is designed for small coin protection against timestamp manipulation and hash attacks. The basic equation is:

next_difficulty = harmonic_mean(Difficulties) * target_solvetime / LWMA(solvetimes)

As succinctly put forward by its name, the LWMA algorithm (by zawy12) more heavily weighs recently solved block times. It ensures that the SINOVATE blockchain is less susceptible to 51% attacks from large hash power operations or centralized mining farms. As a result, issues such as long block times experienced due to lagging high mining difficulty are becoming a thing of the past.

The Bitcoin network protocol adjusts the difficulty of successfully mining its blocks every 2016 blocks. It can lead to what is known as “multipool mining” during which time miners can opt to direct hash power to other blockchain networks once difficulty gets too high. As a result, other blockchains are subject to large fluctuations in hash power and an increased likelihood of a 51% attack.

7. SINOVATE Solution

As described above, SINOVATE is constantly seeking to improve the way in which mining difficulty adjusts as hash power is increased or decreased during the SIN mining process. It is a vital aspect of the main SINOVATE blockchain which will make it more secure and reliable, and even more so, highly decentralized. Large hash power miners will be deterred from exploiting (51% attack) the main SINOVATE blockchain that can adjust its difficulty more smoothly over every single block thanks to the Linearly Weighted Moving Average (LWMA) Adjustment Algorithm. It also fixed some key architectural issues. The SINOVATE network is more immune to hash power fluctuations as evidently witnessed, or can be potentially the case, with other blockchain projects. Block times will be more consistent and less susceptible to spikes in hash power.

8. Specifications

Name: SINOVATE

Ticker: SIN

Algorithm: X25X

Block Rewards: PoW-25 SIN & Infinity Nodes-3150 SIN

Block Time: 2 minutes

Current Blockchain Size: 1.9 gb

Difficulty Retargeting Algo: LWMA

Infinity Nodes Collateral: 100K-500K-1000K (three-tiers)

Max Supply: Always less than 800 million infinitely

Pre-Mine: No

P2P Port: 20970

RPC Port: 20971

Treasury: 10%

9.Conclusion

There is a necessity for an agile, secure, ASIC and FPGA resistant, memory optimized algorithm that is prepared for constant dynamic decentralization alignment against ever changing advances in computing technology.

An evolving world requires adaptable algorithms and that is why SINOVATE will keep adding innovations and new algorithms to stay away from the threat from the large ASIC and FPGA hardware companies and, if it emerges on a practical scale, the threat of Quantum Computing.

The cross-functional algorithm team work using Agile project practices and are in constant communication, despite being all over the globe. This allows a nimble software development cycle with adaptive planning to allow the team to keep ahead of any challenges and can react quickly to change.

The efficiency and reduced heat profile of the X25X hashing algorithm aids miners and proves that mining operations do not have to maximize power consumption and heat output to compete and to be ASIC/FPGA/Quantum resistant. For larger miners this can mean easier scalability with less cooling and ventilation requirements.