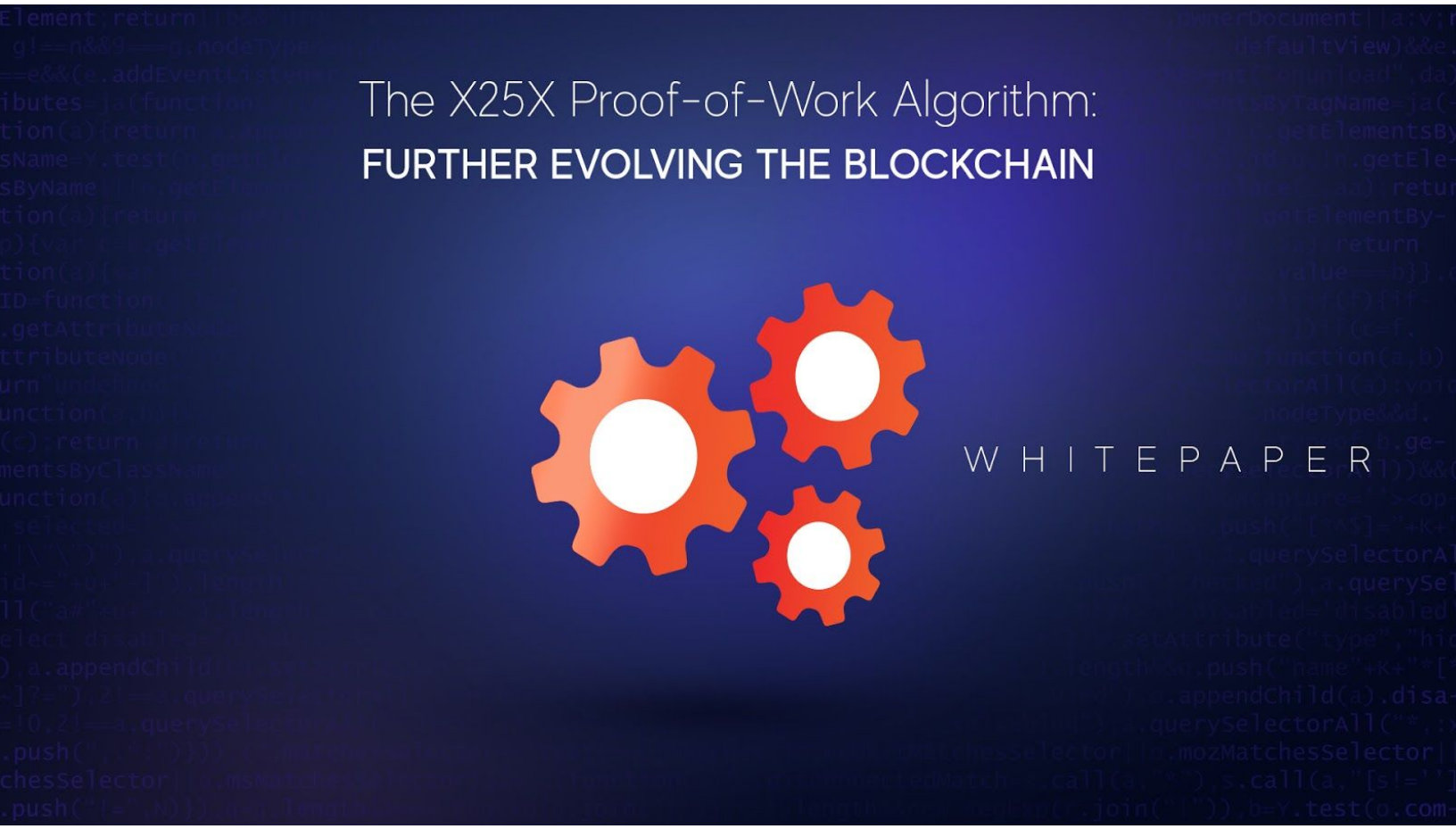
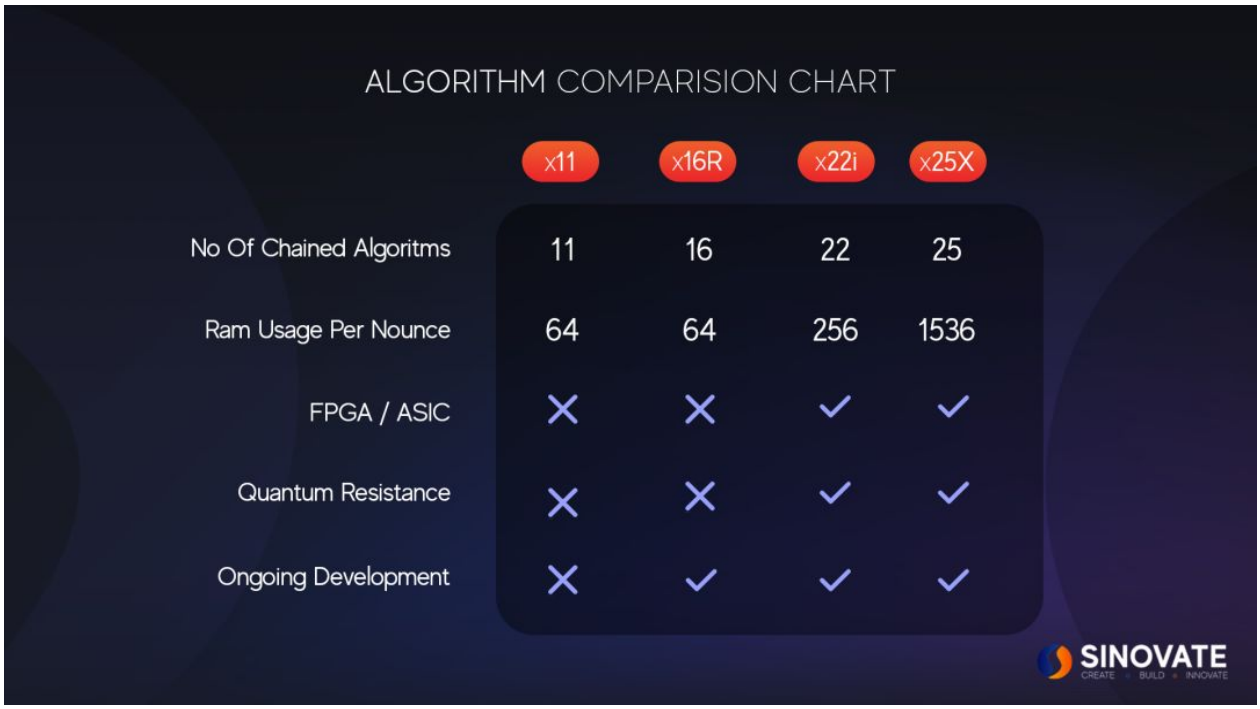


The X25X Proof-of-Work Algorithm: Further Evolving The Blockchain



1) The Problem

Centralisation remains of high concern to many within the Cryptocurrency Community, as well as an increasing number of the wider general public. Bitcoin was founded with the intention of creating **financial freedom** for all, away from the **controlling factors** inherent within the culture of banks and financial institutions globally. As a result, the concept of decentralisation has become a hot topic which continues to grow in prominence, for reasons to be discussed in this article.

Specifically, if we consider the issue of centralisation in relation to cryptocurrency mining, repelling the creation of **ASIC and FPGA devices** is of **utmost importance**, in order to promote **fairness** and maintain a **long term egalitarian approach**. In theory, this is possible via modest and easily obtainable GPU and CPU mining equipment.

However, many Cryptocurrency Developers thus far have been unsuccessful in implementing sustainable equality measures within their respective projects. Predominantly, crypto coins with large trading volumes are mined by efficiency enhanced devices, with GPU and CPU miners only able to profit for a few short months or even weeks.

FPGAs and ASICs require expensive machines and cannot be utilised for additional tasks - unlike GPUs and CPUs. Furthermore, FPGA programming is extremely complex and resource intensive. As a result, these technological mechanisms directly result in mining centralisation, significantly reducing rewards previously enjoyed by many. SINOVATE (SIN) has and continues to **reinvigorate Proof-of-Work (PoW) mining**, reinforcing and enhancing Bitcoin's original vision of "One CPU One Vote".

2) The Original X22i Proposition

The purpose of the original X22i Whitepaper was to design a **highly efficient** PoW algorithm, which provides a **multitude of distinct advantages** to GPU miners over commercial mining farms:

1. Make **ASIC and FPGA design much more difficult and expensive**
2. Allow GPU optimised miners to be developed quickly
3. Allow **GPU miners to obtain maximum efficiency**
4. Add **Quantum Resistance**
5. Use proven, **industry standard** components such as sha-2 and sha-3 to enable **optimal security**

3) The Solution - X25X: The Evolution of Proof-of-Work Mining

X22i was successful in implementing all of the above, but in order for miners to continue receiving long term rewards, evolving and adapting to increasing demands in computing power and efficiency required by modern hardware systems was necessary. This has been carried out via SINOVATE's **brand new custom X25X algorithm**.

Also, an algorithmic change was required in order to make ASIC chip production as well as FPGA design far less profitable, due to the short timeframe permitted for using the product. Additionally, X25X enables **lower power consumption** for GPUs, as this enhancement is dependent on random RAM access which integrates wait cycles into the mining process.

3.1 FPGA and ASIC Resistance

X25X pursues the goal of ASIC and FPGA resistance, by implementing multiple additional features over standard PoW algorithm chains such as X11. Features include increasing memory requirements by **24 times**, with X22i standing at **4 times**. This is not a problem for CPUs and GPUs, but is significantly more difficult for FPGA and ASIC devices to maintain. The reason for this is because they either require **commodity RAM usage**, which provides **no advantages over CPUs and GPUs**, or these appliances must apply 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. This is to prevent multiple optimisations overriding the purpose of the bigger buffer, and also to **circumvent malicious activities** from private miners seeking to gain unfair advantages over honest workers (for instance, combining multiple algorithms into one, as the output of every stage is required to reach the final result). Also, this indirectly promotes the writing of **clean code** for algorithms, so that the opensource code is more

valuable both in terms of quality and hash rate. This is important for the **long term continuity and viability** of Proof-of-Work mining.

Another advantage over traditional PoW algorithms is a much longer algorithm chain: **25 algorithms** require vastly increased chip space to implement the entire chain, which is extremely costly for both FPGA and ASIC appliances.

The wider plan for X25X is to increase the chain size with further hashing stages, to be released periodically. This approach forces chip designers to **constantly revise** their designs, further increasing costs and reducing the time required to utilise chips for mining purposes. Moreover, making the chain progressively longer addresses concerns surrounding future FPGA chips with increased capacity. Any efficiency gains, as well as capability of these devices fitting the entire X25X chain into a single chip will be **nullified**.

3.2 GPU Miner Software Development

As X25X is a chain of well-known hashing functions, coding a GPU Miner for this algorithm mostly entails assembling opensource code. As previously discussed, X22i came equipped with many implementations, both private and opensource, with the missing stages to reach the full X25X chain all being made available as opensource. The new shuffle stage, which can also be implemented on GPU code, will be opensourced shortly.

Many overly-optimised sources **will not function** or will need to be **heavily modified**, as they do not provide full output for all of the algorithms within the chain. This helps to increase the decentralised consensus mechanism provided by the SINOVATE Blockchain, as hash rate disparity between private and opensource miners will decrease.

3.3 Quantum Resistance

A growing concern within the crypto sphere also relating to centralisation, which potentially presents an even greater threat than ASIC and FPGA devices is the possibility of **“breaking”** hashing algorithms, which are utilised within existing cryptocurrency coins via a **Quantum Computer**. Access to this hardware could permit huge efficiency advantages over the mining majority, manifesting the likelihood of an **extreme 51% attack** being carried out on the network. This would result in a significant chunk of the chain reverting and increase the possibility of double spending, with a single entity well positioned to assume **total Blockchain control**.

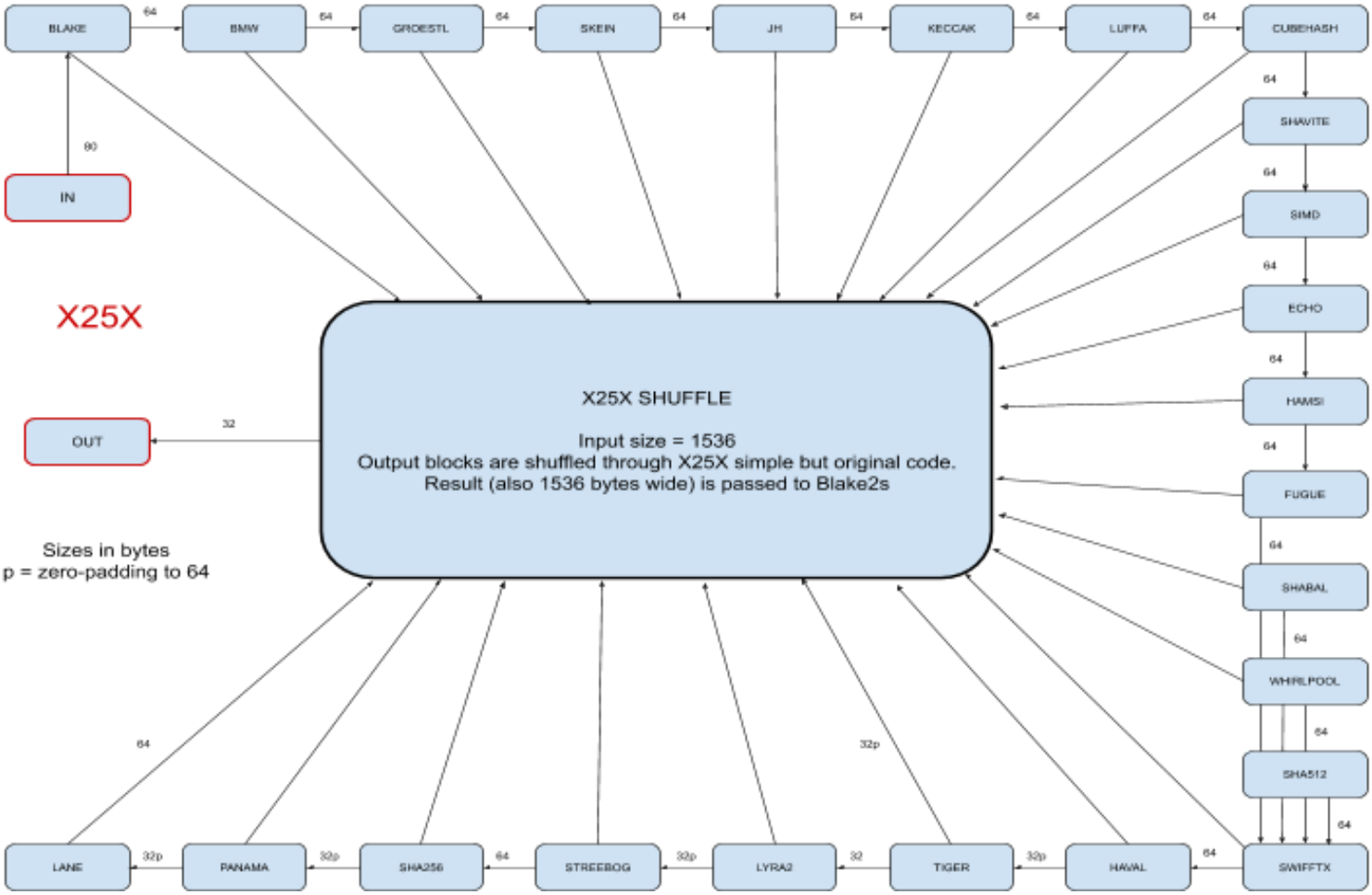
In order to address this issue, X22i introduced a **post-quantum element** in the chain called SWIFFTX, with lattice-based cryptography. This component has also been implemented into X25X:

“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)

3.4 Algorithm Chain

Below is the full list of standard hashing algorithms integrated by the X25X Chain including the unique shuffle stage, corresponding input and output sizes as well as eventual **zero-padding**. SWIFFTX implements a much greater input size, which spans across the outputs of 4 preceding algorithms. The shuffle stage accepts all preceding algorithm outputs as input:

1. Blake (in: 80b, out: 64b)
2. BMW (in: 64b, out: 64b)
3. Groestl (in: 64b, out: 64b)
4. Skein (in: 64b, out: 64b)
5. JH (in: 64b, out: 64b)
6. Keccak (in: 64b, out: 64b)
7. Luffa (in: 64b, out: 64b)
8. Cubehash (in: 64b, out: 64b)
9. Shavite (in: 64b, out: 64b)
10. SIMD (in: 64b, out: 64b)
11. Echo (in: 64b, out: 64b)
12. Hamsi (in: 64b, out: 64b)
13. Fugue (in: 64b, out: 64b)
14. Shabal (in: 64b, out: 64b)
15. Whirlpool (in: 64b, out: 64b)
16. SHA512 (in: 64b, out: 64b)
17. SWIFFTX (in: 256b, out: 64b)
18. Haval (in: 64b, out: 32b + 32b zero-padding)
19. Tiger (in: 64b, out: 32b, + 32b zero-padding only for the shuffle stage)
20. Lyra2 (in: 32b, out: 32b + 32b zero-padding)
21. Streebog (in: 64b, out: 64b)
22. SHA256 (in: 64b, out: 32b + 32b zero-padding)
23. Panama (in: 64b, out: 32b + 32b zero-padding)
24. Lane (in: 64b, out: 64b)
25. X25X Shuffle (in: 1536b, out: 1536b)
26. Blake2s (in: 1536b, out: 32b)



X25X PROOF OF WORK ALGORITHM CHAIN

Join us and stay tuned for all forthcoming updates via our website and social media platforms:

Website Discord . Telegram . Bitcointalk . Twitter . Facebook .Linkedin. Team.YouTube. Reddit.

Telegram Rus - Telegram Chinese - Telegram Africa - Telegram Espanol - Telegram French - Telegram Indonesia - Telegram Italian - Telegram Turkish - Telegram Vietnamese

Author: ***Pallas Amit Kaushal***