SIGNATUM

WHITEPAPER

REVISION 01/08/2017

Contents

Introduction

Signatum is a cryptocurrency aimed at offering seamless utility on both public and TOR markets. Signatum is designed to be easily integrated into several applications, including payment platforms, exchanges, and marketplaces. Signatum features the new SkunkHash Raptor algorithm that enables strong ASIC-resistance during the proof of work phase and encourages fairness for miners and investors alike by driving broad coin distribution and ownership while creating real-world application.

Executive Summary

The recent, and growing trend in new cryptocurrencies and tokens has been to fund development through Initial Coin Offerings (ICOs), pre-mining large quantities of coins (leading to a centralized distribution), or through alternative hybrid methods. Funding methods that allow developers to control large amounts of a coin's circulation may lead to coin devaluation (particularly in the case of developer "dumping") and forces investors to abide to a fixed team. In the event of an unsuccessful project, the investor has no voice to the outcome.

Signatum launched on July 18th, 2017, with no pre-mine, no initial offering, no developer fees and no bounties. Signatum launched with a focus on creating a highly responsive and secure network that provides a fair environment for all miners and investors. Aimed at decentralizing coin ownership as much as possible, it includes an aggressive mining algorithm that targets GPU miners and diminishes the opportunity for Application Specific Integrated Circuit (ASIC) development with an accelerated proof-of-work (PoW) phase. Signatum prides itself on being a 100% decentralized community with a driven concept, where anyone can contribute to the development and direction of the coin, just as Bitcoin was initially intended. The lack of ICO and development funds allows investors to also provide significant input and direction in a way that is non-existent in ICO based coins.

[1] *Initial Coin Offering - An established number of coins/tokens to be sold on a certain date for a certain rate. Similar to an IPO (Initial Public Offering) on the securities market.*

The launch of Signatum has challenged the current mining process, which formerly focused on established coins as centers for mining profit and until now failed to offer compelling new market entrants into the GPU mining space. Mining has never been more mainstream, and as a result, previous mineable coins are not able to adjust to the new environment. The number of miners has been growing rapidly, leading to massive increases in hashing power. With Signatum we shortened the proof-of-work period, to allow miners to switch to other coins faster than they would otherwise normally be able to. This thereby enables miners to accumulate the most profit out of their mining equipment as possible, without having to tie down their hardware for several years to the same coin and project. This in turn also creates a fair mining opportunity for everyone, as the mining period has been shortened from several years to approximately 100 days.

The accelerated mining period contributes to a fair wealth distribution, which is observable on the Signatum rich list (http://explorer.signatum.io/richlist).

The short PoW period safeguards against the development of market-disrupting ASIC hardware, which is specialized mining equipment optimized to perform specific functions with much lower energy cost and much higher hashing power than conventional video card mining systems. Access to ASIC hardware is usually limited due to the cost of creating the hardware and ASIC devices for mining and very often carry a very steep price because of the comparative advantages they provide. Hobbyist miners who attempt to mine against ASIC miners have a significant disadvantage in finding a block. As an example of the disparity between ASIC and GPU mining, a GPU system mining the X11 (DASH) algorithm would produce about 1/100th of the hash rate of the latest Dash ASIC (Bitmain’s D3). Signatum is also more environmentaly friendly than other PoW coins since the accelerated PoW phase requires less electricity to complete.

This coin has three phases:

- Pure Proof of Work
- Hybrid Proof of Work & Proof of Stake
- Pure Proof of Stake (5% APR)

Signatum introduces a brand-new GPU-optimized algorithm, further differentiating it from other mineable coins. Signatum's SkunkHash Raptor algorithm combines four different hashing functions and one balancer. The hashing functions combined to create this unique algorithm are Skein, CubeHash, Fugue, and GOST-Streebog. Raptor is the developer's fingerprint and is used to monitor proliferation of the SkunkHash algorithm. The mix of algorithms increases the security of Signatum's network significantly by increasing the complexity of the hashing function.

Signatum's broad-distribution approach begins with 2,500 SIGT rewards for the first 30,000 blocks, combined with a short block time, to ensure that as many miners as possible can earn a fair amount of coin. Even miners with low hashing power will have the opportunity to mine hundreds or thousands of coins in a much shorter period than usual. The total number of coins produced in PoW phase is approximately 137,500,500. After the PoW phase, Signatum enters a proof-of-stake phase and staked coins yield interest based on the number of coins staked in the coin-holder's local wallet.

Background on Algorithms

Skein

Introduced in 2008, Skein is a family cryptographic hashing function that is secure, fast, and flexible. Skein is an efficient GPU mining algorithm that is supported across multiple platforms and is also CPU mineable. Skein allows for multiple block-sizes, including 256, 512, and 1024 bits. Skein's primary innovation is the ability to build a hash function with an adjustable block cipher (called "Threefish"), which allows Skein to "hash configuration data along with the input text from every block, and make every instance of the compression function unique *(Ferguson, et al. 2010)*. The Threefish cipher employs many simple rounds of hashing to maximize security.

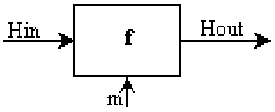
CubeHash

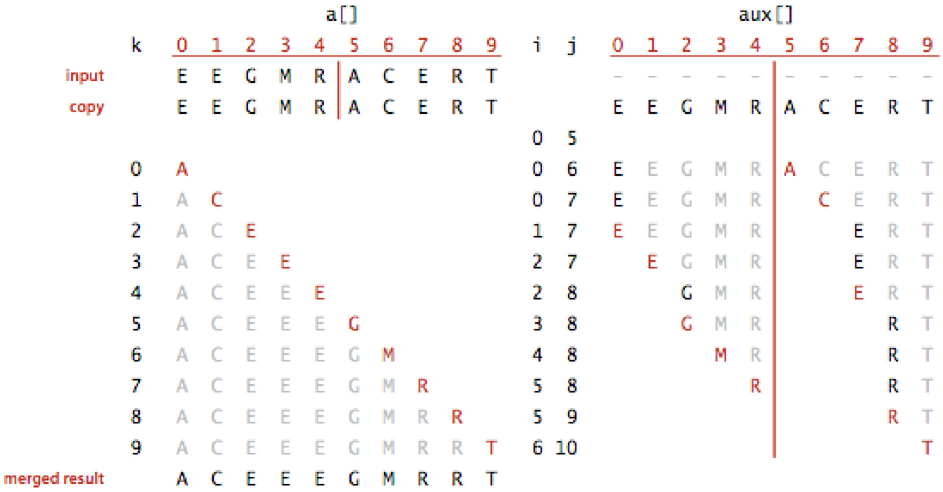
Originally submitted to the NIST competition by Daniel Bernstein, CubeHash is a cryptographic hash function that, "is parametrized by a pair of positive integers (r, b) with b ≤ 128. CubeHashr/b applies an r-round transformation after each b-byte message block." *(Bernstein, 2009)*. CubeHash allows for significant parametric adjustment and is extremely flexible, which allows for the function to operate across a range of computer systems, making it a good choice for GPU-optimized mining.

GOST-Streebog

Streebog is a cryptographic hash function that is part of the Russian Federal Standard and it employs a multiple-round cipher. Similar to Skein, Streebog will present a significantly altered hash function if the input is only slightly modified due to the avalanche effect.

The step hash function maps two 256-bit blocks into one, It consists of three parts:





		a[]												aux[]									
	k	0	1	2	3	4	5	6	7	8	9	i	j	0	1	2	3	4	5	6	7	8	9
input		E	E	G	M	R	A	C	E	R	T			-	-	-	-	-	-	-	-	-	-
copy		E	E	G	M	R	A	C	E	R	T			E	E	G	M	R	A	C	E	R	T
												0	5										
	0	A										0	6	E	E	G	M	R	A	C	E	R	T
	1	A	C									0	7	E	E	G	M	R		C	E	R	T
	2	A	C	E								1	7	E	E	G	M	R			E	R	T
	3	A	C	E	E							2	7		E	G	M	R			E	R	T
	4	A	C	E	E	E						2	8			G	M	R			E	R	T
	5	A	C	E	E	E	G					3	8			G	M	R				R	T
	6	A	C	E	E	E	G	M				4	8				M	R				R	T
	7	A	C	E	E	E	G	M	R			5	8					R				R	T
	8	A	C	E	E	E	G	M	R	R		5	9									R	T
	9	A	C	E	E	E	G	M	R	R	T	6	10										T
merged result		A	C	E	E	E	G	M	R	R	T												

Merge v/s Split

```
procedure MERGE SPLIT(S)
    Step 1:    for i = 1 to N do in parallel
                   QUICKSORT ($S_i$)
               end for.

    Step 2:    for j = 1 to [N/2] do

    (2.1)          for i = 1,3,...,2[N/2] - 1 do in parallel
                   (i) SEQUENTIAL MERGE ($S_i$, $S_{i+1}$, $S_i'$)
                   (ii) $S_i \leftarrow \{s'_i, s'_2,...,s'_{2n/N}\}$
                   (iii) $S_{i+1} \leftarrow \{s'_{(n/N)+1}, s'_{(n/N)+2,...,}s'_{2n/N}\}$
               end for
    (2.2)      for l = 2, 4,...,2[(N - 1] do in parallel
                   (i) SEQUENTIAL MERGE ($S_i$, $S_{i+1}$, $S'_i$)
                   (ii) $S_i \leftarrow \{s'_i, s'_2,...,s'_{n/N}\}$
                   (iii) $S_{i+1} \leftarrow \{s'_{(n/N)+1}, s'_{(n/N)+2,...,}s'_{2n/N}\}$
               end for
           end for.
```

Fugue

Fugue is a hashing function that supports “variable length inputs” *(Halevi et al, 2009)* that was originally submitted by IBM to the NIST competition. Fugue can be implemented in many environments and is resistant to multiple current attack techniques *(Halevi et al, 2009)*. Fugue’s flexibility and attack resistance made it a strong choice for inclusion into the SkunkHash Raptor algorithm

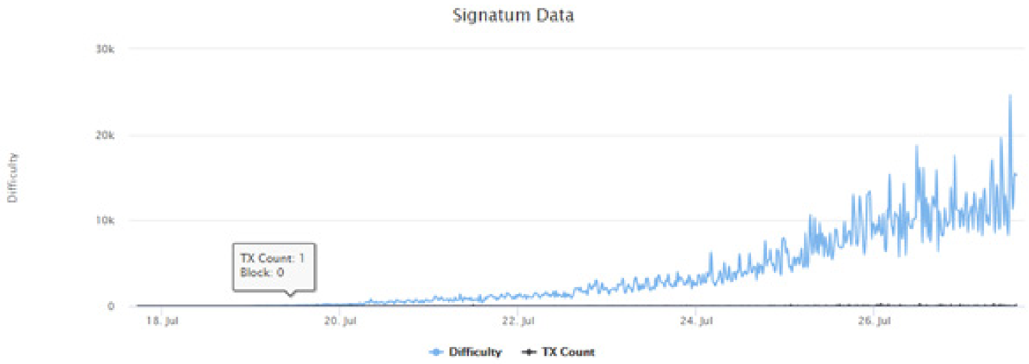
Three Phases of Signatum Expanded

Pure Proof of Work Phase

The first phase of Signatum is the proof-of-work phase. The proof of work phase will last for the first 100,000 blocks, or approximately 100 days. Figure (1) details the distribution of block rewards through the first 100,000 blocks. At the end of the PoW phase, the PoS phase begins.

The SkunkHash Raptor algorithm supports both SGminer (AMD) and CCminer (Nvidia) mining software.

The PoW difficulty adjustment is dynamic and executed with Dark Gravity Wave v3 (DGW3), which was originally created for Dash. DGW3 allows for continual difficulty re-targeting by pulling statistical data from the last block found and modifying the difficulty for the next block accordingly. This allows for the algorithm to be responsive to network hashing power dynamically, rather than at a fixed interval which leads to a less linear progression. DGW3 also encourages fixed block times, regardless of the hashing power applied through mining. Ultimately, DGW3 results in a more agile difficulty which is best viewed by exploring the Signatum coin difficulty charts:



Below is a chart describing the amount of coins produced at each block.

Figure (1). Block Bracket Coin Distribution

Blocks	Rewards	Coins Generated
0 - 30,000	2,500 SIGT	75,000,000 SIGT
30,001 - 60,000	1,250 SIGT	37,498,750 SIGT
60,001 - 100,000	625 SIGT	24,999,375 SIGT

The total coins generated during the PoW phase is: 137,498,125.

Coins mined in PoW are fully mature and ready to be transferred after 60 confirmations.

Hybrid Proof of Work & Proof of Stake Phase

The hybrid PoS and PoW phase will last for 1,500 blocks. This phase will begin once PoW reaches block 98,500 and will end once miners find and complete block 100,000. The hybrid phase is estimated to last for approximately 1.5 days.

Pure Proof of Stake Phase

Once the available 100,000 PoW blocks have been mined, Signatum will transition into a full PoS coin. Users staking coins through their local wallet will receive a fixed 5% APR with payouts based on the number of coins staked in the wallet. As an example, if a user stakes 1,000 coins through the wallet, they would receive 50 extra coins in a year ((1,000 x 1.05) - 1,000). The staking APR is paid out every 5 minutes and coins generated during the PoS phase will be fully mature after 50 confirmations - after which the coins are fully transferrable.

Skunkhash Raptor Algorithm

The algorithm is comprised of four intensive algorithms and includes one balancer. The algorithms included are:

- Skein
- CubeHash
- Fugue
- GOST-Streebog

This combination increases the overall security of the Signatum network by requiring any potential attackers to overcome an extremely complex cryptographic hashing function.

Increased Anonymity through Tor Nodes

Official Tor nodes have been added to increase the anonymity of the end-users, making their transactions more secure. Connecting Signatum through a network of relays rather than making direct connections, increases the overall anonymity of the network and its transactions. To secure the network even further, more Tor nodes are planned to be added, forming part of the already published roadmap. To help secure the network even more, the community is also encouraged to run nodes on their own. There are currently (26th July 2017) 261 nodes active for Signatum. For comparison, there are more nodes active currently than Ethereum had at this point in its launch cycle.

Signatum & Anonymity

The internet is a huge community and is continuously going through an evolution over and over again. What is today’s evolution will be a thing of the past tomorrow. The right to anonymous internet access is becoming a major challenge for organizations that are fighting to protect this right for their users. The signatum project offers full anonymity to users as a free selected service by offering them completely anonymous nodes that do not track or forward origin IP addresses and even use Tor exit nodes to protect themselves. The web sites and block chain explorers do not keep track of access logs as they have been disabled. Each service that is part of the Signatum project has internet access from the deep web (Tor).

(Anonymous User) → Signatum Anonymous Node → Exit Node → Global Node Cluster

Confirmations

With an average 2-minute block time and 6 confirmations required for full maturity for peer-2-peer transfers, SIGT can be transferred after 720 seconds or just 12 minutes. In contrast to Bitcoin, it typically requires 3 confirmations with a block time of 10 minutes, meaning full maturity is usually achieved after a lengthy 30 minute transaction delay. Bitcoin’s transaction times make it less ideal for merchants unless a third party intermediary is employed to guarantee transactions before they are fully confirmed by the network. With Signatum’s accelerated maturity and transaction speeds, it is more than ideal for merchants to utilize for customer payments. To enable merchants to easily use Signatum as a currency for payments, a universal SIGT wallet is planned for development and will be connected to a payment gateway. This will also enable the possibility to connect debit and credit card transactions directly with the Signatum network at a future date.

The Long-Term Plan (Roadmap)

We aim to enable the wide real-world application of Signatum in the long-term. To achieve this objective, specific development items that would enable SIGT to be utilized more practically in the future are planned. These development items include:

- Signatum Marketplace: A marketplace that will enable people and companies to sell products and services around the world, using Signatum as a currency.

- Signatum Web Wallet: This makes SIGT easily accessible for transactions from anywhere in the world.

- SignatumPay: Creating a SignatumPay feature enables merchants to connect directly to the Signatum network and utilize it as a payment option. Combining this feature with SIGTs fast transaction speeds will make the currency more than ideal for merchants to utilize it as a payment option.

- A dedicated Signatum exchange site: We aim to create a dedicated Signatum exchange site, where end-users can buy and sell Signatum using fiat through bank transfers, debit and credit card transfers where and as allowed by local regulations and oversight.

- Signatum crowdfunding platform: Crowdfunding through cryptocurrency is becoming more popular and as a result, Signatum aims to create a fair and balanced crowdfunding platform, where investors and entrepreneurs can raise funds for their projects, communicate business objectives and provide updates on project status.

The Long-Term Plan (Roadmap) Cont.

Other items planned for developments or already delivered include:

- A Dedicated official Signatum explorer with difficulty graph. (Delivered 24th July 2017).

- Launching more Tor nodes in order to increase the healthiness of the network and to increase anonymity even further. As of today, (26th July 2017) 261 nodes are already up and running.

- Plan & Build Signatum Foundation: more details will be revealed at a later stage.

- Add Signatum to more exchange sites: applications filed for Poloniex and Bittrex (25th July 2017) More exchange sites will increase the adaptability of Signatum due to its greater accessibility. This is key to making the coin more usable and increasing the consumer awareness.

DEVELOPERS

Doctor	http://www.signatum.io
Gabriel	http://www.signatum.io

COMMUNITY CONTRIBUTORS

Cryptovore	http://cryptovore.com/
Padraiq	BMTHkXVbT7JRyYtXSftHV8niVVgdp2hgyi

Official Telegram & Discord Members

REFERENCES

http://csrc.nist.gov/archive/aes/round2/conf3/papers/06-iharvey.pdf
Ferguson, et al (2010) http://www.skein-hash.info/sites/default/files/skein1.3.pdf
Bernstein (2009) http://cubehash.cr.yp.to/submission/tweak.pdf
Halevi (2009) http://researcher.watson.ibm.com/researcher/files/us-csjutla/fugue_Oct09.pdf
https://en.wikipedia.org/wiki/CubeHash
https://en.wikipedia.org/wiki/GOST_(hash_function)
https://en.wikipedia.org/wiki/Skein_(hash_function)
https://en.wikipedia.org/wiki/Fugue_(hash_function)
http://algs4.cs.princeton.edu/22mergesort
https://www.dash.org/dark-gravity-wave
https://en.wikipedia.org/wiki/Bitcoin
https://en.wikipedia.org/wiki/Proof-of-work_system
https://en.wikipedia.org/wiki/Proof-of-stake