DRAFT DO NOT PUBLISH

SHIELD,

solving problems of and improving on cryptocurrencies

The SHIELD team

ShieldCoin@protonmail.com

https://ShieldCurrency.com

Abstract

The SHIELD protocol will replace ECDS with Lamport, Winternitz or BLISS signatures, which will enable addresses to be "quantum-proof". SHIELD will get a self-supporting development cycle, which will enable the continuation of the development of the SHIELD protocol and other projects described in this article. SHIELD will use a custom PoS scheme (PoS Boo) with the help of Masternodes. These masternodes will also enable features like PrivateSend and InstantSend.

Keywords: SHIELD, quantum-proof, masternodes, cryptocurrency, blockchain, privacy

1 Introduction

SHIELD is a cryptocurrency based on the blockchain technology of Satoshi Nakamoto (which he released a white paper[1] of in 2009) that has been growing and improving ever since. For a few years now, blockchain technology has been increasingly adopted, but there are still many problems that hold this technology back from going mainstream. SHIELD is looking to solve many of these problems.

2 Problems to solve

Bitcoin was really innovative when it was implemented, and a good portion of what Satoshi made is still used in the core of many cryptocurrencies today. One of these contributions is block mining, but more specifically, block mining with a single algorithm. This has led to the development of specialised hardware (ASICs) that can hash one algorithm so effectively that they render GPU mining obsolete. . One downside of the decision he made, as many younger cryptocurrencies have come to realise, is the fact that mining isn't really fair. You can read about it in section 3: *Multi Algorithm mining for PoW*.

Quantum computers are getting ever more sophisticated and may be on the verge of being available to the public. Whether it be for researchers, governments, businesses or the general public, we will eventually see quantum computing become available for wealthy groups and individuals with self-interest. Although it is an incredible new technology which could greatly improve our lives, there are also a good amount of reasons to be concerned about this development. One of these is that modern-day cryptography can be efficiently cracked by future quantum computers. For many cryptocurrencies, it could mean a broken blockchain. How we are going to solve this problem is outlined in section 4, *Quantum Resistance*.

Big corporations like Facebook or Google are getting better at knowing who you are and what you want. Although this may not (currently) be too concerning, it will mean living in a world where businesses will be watching us; it may not be that bad, but it isn't looking great. There are a lot of currencies that claim to keep their users anonymous, which would prevent these big corporations and governments from being able to track your spending habits. The problem with some of these coins is that they are not as effective as they claim, meaning that their scalability and practicability is low to non-existent. We will talk more about the way we will be keeping our users anonymous in section 5, *Privacy features*.

Some altcoins have a really promising roadmap; some even have incredibly talented developers. But without funding, it may not be enough to keep a coin alive. If developers cannot find some kind of income from the project, it will become increasingly difficult to work on it full-time. We do not want this to happen so we plan on implementing some features to SHIELD (and some platforms around SHIELD) that can assist us with funding. You can read about this solution in section 6, *funding*.

Another problem with Bitcoin and many other currencies is that miners have to mine with power-hungry hardware to allow coin minting and transaction confirmation. It was really innovative at the time and it still works fine, but the economic and environmental cost of continuing the blockchain (that only has Proof of Work for network consensus) is really high. This has been solved with our Proof of Stake scheme, which you can read about in section 9, *PoS Boo*.

3 Multi-algorithm mining for PoW

We improved upon the equal distribution of rewards and upon resistance to 51%[citation needed] attacks with multiple PoW algorithms. Multi-algorithm mining is a way of allowing multiple types of processing units to mine for blocks; our approach enables many different devices, including both GPUs and ASICs, to mine together on the SHIELD blockchain. Distribution of rewards per algorithm is almost always the same proportion of the total reward over time. For example, even if one algorithm has 300GH/s and another has 50MH/s, they should still receive the same amount of coins in an hour. It improves on 51% attack prevention because of the way blocks are distributed; each algorithm follows their own “schedule”, which means you need 51% of the hashing rate for each algorithm to succeed in executing such an attack. An important aspect of this system is in how the difficulty for each algorithm is adjusted separately.

Difficulty adjustment is managed by the “Dark Gravity Wave v3” scheme, which was developed for Dash but has been used in various other cryptocurrencies. It manages network-hash spikes and network-hash drops a lot better than the conventional difficulty calculation, and makes it harder for malicious miners to quickly mine coins without processing transactions.

4 Quantum Resistance

The SHIELD protocol is the quantum-proof transactions/addressing for certain addresses. Other cryptocurrencies are often not quantum-proof due to their use of ECDS (which is vulnerable to Shor's Algorithm[9], enabled by using quantum computers). We are planning on using Lamport signatures, or similar schemes, to change that. Lamport digital signatures are based on hash functions, and hash functions are not vulnerable to Shor's Algorithm. With ECDS, whenever you send a transaction, your address becomes vulnerable because your crackable ECDS signature is exposed. Cracking such a signature would allow unauthorised access to the funds associated with that address. Hashes aren't vulnerable to Shor's Algorithm, thus hash-based digital signatures improve upon the security of affected addresses against this looming threat.

5 Privacy features

SHIELD's Project Perdu is one that has recently undergone a change of plan.
We were originally planning to implement VergeCurrency's Wraith protocol[6], but due to its relatively low specifications, we have decided to opt for PrivateSend (developed by Dash) instead; this works better for us as we already need to implement masternodes. This change will optionally improve the transaction speed via InstantSend. Although it is an improvement, PrivateSend still does not make the transactions fully private, which is why Zerocoin[5] or zk-SNARKs[4]/zk-STARKs is under consideration
We'll go more into detail about this in the quarter that this will be implemented.

For physical privacy, we will use Tor[8]/I2P[7] wallets/nodes that hide the end-user's IP address and location.

6 Funding

SHIELD self-funding may work by using a percentage of the masternode and mining block rewards. This will be a very small percentage as we only need to keep the team afloat, and the rest is for marketing. We will also have some external sources of support which will be made by making and joining platforms that help both developers and users. We have, for example, received many donations from the community by which we can forward the project, and are also getting support from various mining pools. We hope that this will help forward our project indefinitely. We didn't have an ICO or a premine like many of our competitors at this time; we believe that having a strong community is a better way to expand.

7 Application security

SHIELD is all about security; we try to improve a lot on our security with the aforementioned quantum proofing, but we have seen a trend in a lot of the applications, interacting with the blockchain, that are vulnerable and noticed that the holes are almost always to do with the interfaces. We think this is why we need to have a lot of our original products tested, this will be done using the open-source community, gathering pen testers to do test it individually, and having all of our development team check the code possibly even acknowledging each commit before pushed not just an official update.

From our experience using our Discord bot, we can conclude that with a secure backend the link to the frontend one of the most important things is in a secure application.

8 Integration

A lot about the usability and applicability of a new technology is due to the it's integration into existing or other new platforms. We will be using many popular and free to use as a way to improve the user experiences. We will do this by making plugins and ‘bots’ for platforms such as Discord, Twitter, Facebook, and more. This integration will give you the ability to send XSH to someone without the need to ask them. This integration might also include a wallet for this platform, this way you don’t even need to get dedicated wallet on your pc to use SHIELD.

Integration is also getting more use cases for public consumption. That is, in combination with networking, a very important part of expanding our audience and use cases. Therefore, we will be contacting many related businesses to increase those factors. This will make it so that we have more stability in our prices and we’ll have more applicability.

9 PoS Boo

SHIELD Boo is our own PoS scheme based on the PoS Casper[2] scheme. The Casper scheme improves the most on the “POSv3”[3] with a risk factor for malicious stakers. The system is progressive in the way that it's really hard to do attacks like the 51% attack, you would need a majority of all the coins, with a potential to lose them all when launching an attack[2]. The finality is mainly determined by stake and risk factors, that’s why even with 51% of the circulation it may be hard to execute a attack successfully. See ‘Figure 2’.

Another thing PoS Casper/Boo solves is censoring. With PoW a block miner can ‘choose’ not to mine a block containing certain addresses, censoring that address from the network. Since block creators are chosen at random and validators are global, it’s really hard to censor addresses from the network,with that added bonus that if you try to force the network you will most probably lose your stake.

10 Future study

As you may have noticed in, for example, Section 5, we discussed some possible features/specifications that aren't decided yet. Some of the features from the roadmap are missing as well, like “Sharding” and “Smart Contracts”. This is because a lot of SHIELD is still under heavy development and careful consideration. We will update this whitepaper or make a new one depending on what we change in the future. This isn't the finality of the SHIELD development plan.

Additionally, this paper will have multiple revisions, which will improve upon being user-friendly and will give more substance to details and subjects.

11 Core Specifications

Note: these specifications include future plans

We will use the following specifications for the core of SHIELD:

Subject	Specification
Blocktime	45 seconds; 240 confirmations to mature; SwiftTx/InstantSend
Block	500kB/block
Block reward	See Figure 1
Transactions/block	Worst case[1]: 2777 tx/block Best case: 14701 tx/block
Transactions/seconds	Worst case: 61 tx/s Best case: 327 tx/s See Figure 3 for graphs
Signatures	ECDSA with optional Lamport/Winternitz/BLISS[2] signatures
Minting	PoW using x17, blake2s, lyra2rev2, myriad-groestl, and scrypt. PoS Boo using Quark[3] hash and Slasher scheme
Transaction Min Fee	0.05 XSH per kB

[1] Best/Worst case determined by the amount of inputs/outputs in a block because inputs are 'heavier' than outputs

[2] To be determined

[3] Not conclusive

Privacy features	Tor/I2P nodes, PrivateSend, Zerocoin[4]

References

[1] Nakamoto, S. (n.d.). *Bitcoin*. Retrieved from https://bitcoin.org/bitcoin.pdf

[2] Buterin, V. (2015). *Understanding Serenity...* Retrieved from https://blog.ethereum.org/2015/12/28/understanding-serenity-part-2-casper/

[3] Vasin, P. (n.d.) *PoSv2* Retrieved from https://bravenewcoin.com/assets/Whitepapers/blackcoin-pos-protocol-v2-whitepaper.pdf

[4] Ben-Sasson, E(2014) *zk-SNARKs* Retrieved from http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf

[5] cs.jhu.edu, (n.d.) *Zerocoin* Retrieved from http://spar.isi.jhu.edu/~mgreen/ZerocoinOakland.pdf

[6] "CryptoRekt", (2017) *Verge Blackpaper* Retrieved from https://github.com/vergecurrency/Verge-Blackpaper/blob/master/Verge-Anonymity-Centric-CryptoCurrency.pdf

[7] I2P, (n.d.) *I2P tech intro* Retrieved from https://geti2p.net/en/docs/how/tech-intro

[8] Tor, (n.d.) *Tor: The Second-Generation Onion Router Retrieved* from https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf

[9] McAdam, S (n.d.) Shor's Algorithm Retrieved from https://www.ma.utexas.edu/users/mcadam/monographs/Shor's_algorithms.pdf

[4] Not conclusive

Figures

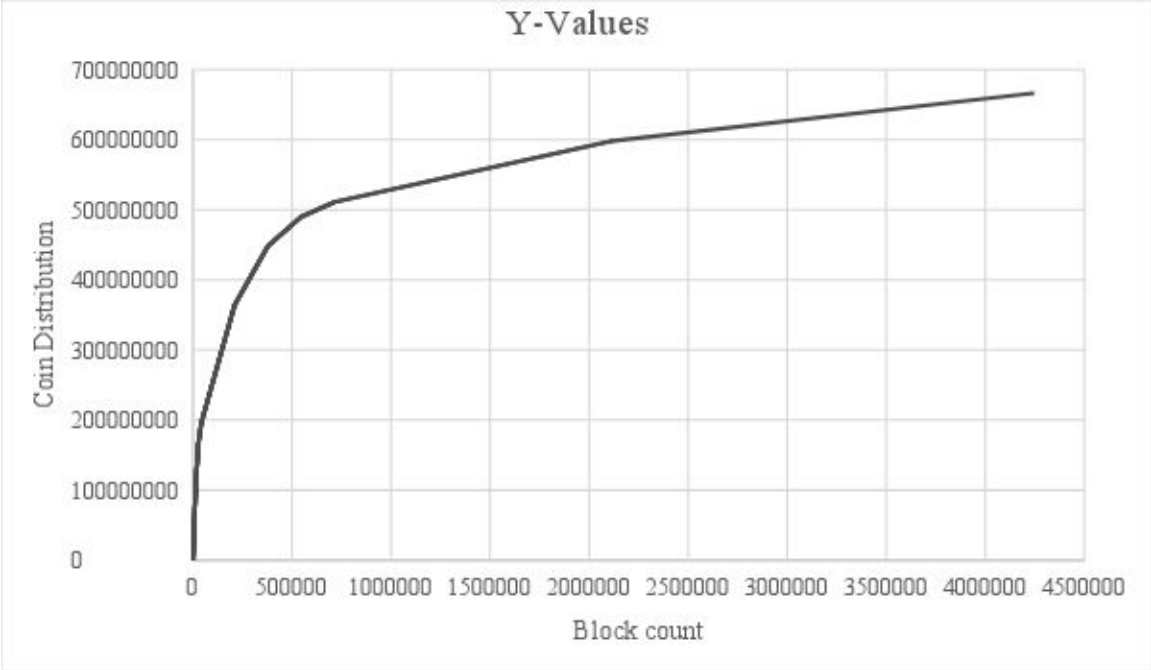

Figure 1. Graph of coin distribution (y) over blocks (x)

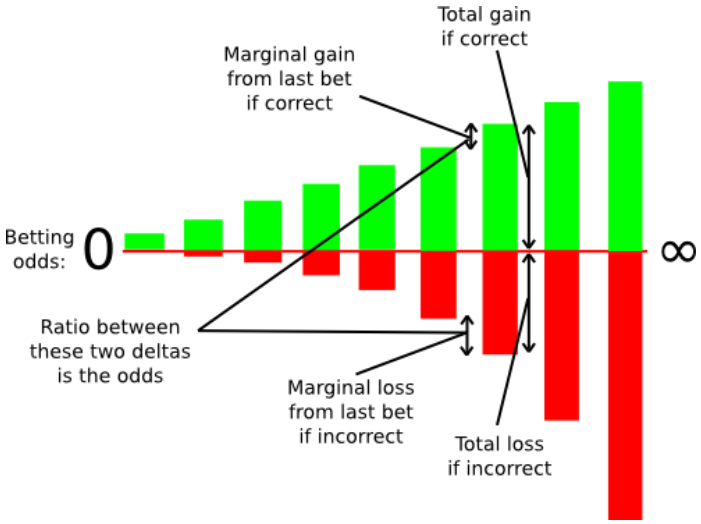

Figure 2. Graph for loss or gain for the betting system of PoS Casper

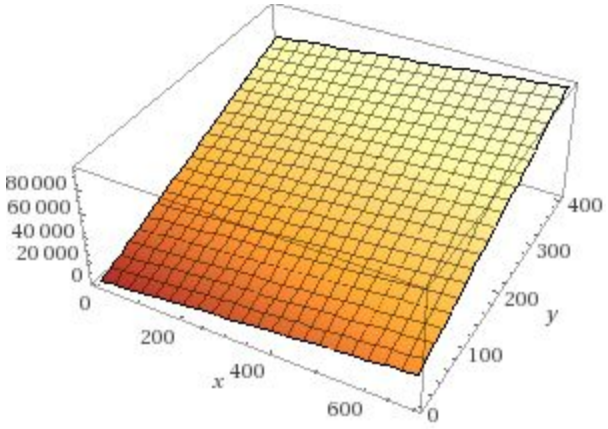

Figure 3. 3D plot of inputs(y) and output(x) where z is the size in kBThe worst and best case are always around Z=500000. This assumes a bitcoin type of scenario where blocks need to be filled to process as many transactions as possible.