SHIELD

FUTURE-PROOFING THE BLOCKCHAIN

SHIELD WHITE PAPER

VERSION 1.0.2

THE SHIELD TEAM

ShieldCoin@protonmail.com

https://ShieldCurrency.com

ABSTRACT

In order to create “quantum-proof” peer to peer addresses, the SHIELD protocol will replace ECDS with Lamport, Winternitz or BLISS signatures. To facilitate the continual development of the SHIELD protocol, as well as other projects specified in this document, SHIELD will be subject to a self-supporting development cycle.

The SHIELD currency will further distinguish itself with the implementation of a custom PoS scheme (PoS Boo) operating on a network of Masternodes, the activation of these masternodes will also enable enhanced transaction capabilities such as PrivateSend and InstantSend.

Keywords:

SHIELD, quantum-proof, masternodes, cryptocurrency, blockchain, privacy SHIELD currency, Lamport signatures, Winternitz signatures, BLISS signatures.

1. INTRODUCTION

SHIELD is a cryptocurrency based on the blockchain technology developed by Satoshi Nakamoto in 2009.

Since the blockchain's genesis, blockchain technology has seen exponential growth and application across a variety of industries, however, the blockchain still faces many critical challenges that must be addressed and overcome before mainstream adoption can be achieved. SHIELD intends to solve these problems by creating the first truly secure, anonymous peer to peer cryptocurrency, resistant to both 51% attacks and the future threat posed by quantum computing, while maintaining unparalleled transaction times with minimal accompanying fees.

2. PROBLEMS TO SOLVE

When Bitcoin was first introduced, Bitcoin was regarded as an innovative technological breakthrough. This is exemplified in that much of the fundamentals of what Satoshi created can still be found at the core of many cryptocurrencies developed today. One such fundamental is block mining, or more specifically, block mining with one single algorithm. This aspect of blockchain technology has led to the development of specialised hardware (ASICs) that have the ability to hash one algorithm to an extreme level of effectiveness, rendering GPU mining obsolete. The drawback of development design decisions made by Satoshi, as many cryptocurrencies have since come to realize, is that mining is not always a "fair" process for all participants. Further information can be found in 'Section 3: Multi-Algorithm PoW Mining'.

Quantum computers have become increasingly sophisticated in recent years and will likely be made available to the public in the near future. Whether these quantum computers will be restricted to research groups, governments, industry or made accessible to the general public, quantum computing will eventually become available to individuals with nefarious self-interests. While this technology will undoubtedly greatly improve the lives of many, there are many legitimate reasons to be concerned with its increasing availability. One such reason is the vulnerability found in modern-day cryptography allowing them to be efficiently cracked by future quantum computers. For many cryptocurrencies, this advance in computing ability could create an effectively inoperative blockchain. *How the SHIELD currency will address this problem is outlined in 'Section 4: Quantum Resistance'.*

Industry dominant corporations such as Facebook and Google have become increasingly effective at knowing who their users are, and what their users want. While this may not currently be a major concern to the majority of the general public, this pervasive trend has created a world in which organisations can watch, evaluate and track both existing and potential consumers. Currently, there are multiple existing cryptocurrencies that claim to keep their users anonymous, such technology would prevent both corporations and governments from being able to track your spending habits. The problem with the vast majority of cryptocurrencies, is that they are not nearly as effective at maintaining user anonymity as they claim. This results in scalability and practicability which is low, or at times, non-existent. *We will talk more about maintaining user anonymity in 'Section 5: Privacy Features'.*

Many competing cryptocurrencies available today contain promising roadmaps, and some alternative cryptocurrencies even have incredibly talented, creative developers. Unfortunately, without funding, many of these coins will never see the completion of their projected goals and mission. Without a constant income stream produced by the project, maintaining a full-time development team can become increasingly difficult. This is the last thing we want at SHIELD, as we truly believe in our mission, our objectives, and our commitment to the SHIELD community. In order to counteract the funding problems commonly faced by many cryptocurrency projects, we intend to implement features to SHIELD (and platforms around SHIELD) that can assist us with funding. *You can read further about our innovative funding solution in 'Section 6: Funding'.*

Another problem we have identified is the increasingly high power consumption required by miners to allow coin minting and transaction confirmation through the 'Proof of Work' (PoW) protocols that Bitcoin and many other cryptocurrencies currently utilise. PoW was innovative in 2009 when Bitcoin was conceived, and still achieves the intended purpose for currencies today, unfortunately, the economic and environmental cost of the continued use of blockchains that rely on PoW protocols for network consensus is extremely high, and growing at an exponential rate. *This problem is efficiently solved with our Proof of Stake scheme, which you can read about in 'Section 9: PoS Boo'.*

3. MULTI-ALGORITHM PoW MINING

Through the use of multiple PoW algorithms, SHIELD has improved upon the blockchains equal distribution of rewards as well as the ability to resist a 51% attack. Multi-algorithm mining provides a method of allowing multiple and varied types of processing units to mine for blocks; our approach enables both GPUs and ASICs to mine together in harmony on the SHIELD blockchain. The distribution of rewards per algorithm is consistently proportionate to the total block reward over time.

For example, should the x17 algorithm accumulate 300GH/s of network hash, while the blake2s algorithm accumulates only 50MH/s, both algorithms will receive the same number of coins per hour. This system improves 51% attack prevention due to the fair and equal nature of block distribution; each algorithm follows its own "schedule", meaning 51% of the hashing rate is needed for each algorithm to succeed in executing such an attack.

An integral element of this multi-algorithm system is the way in which each algorithms difficulty is individually adjusted. Difficulty adjustment is managed by the "Dark Gravity Wave v3" scheme (DGW), although originally developed for the Dash currency, DGW has since been successfully implemented in other cryptocurrencies. DGW manages network-hash spikes and network-hash drops more efficiently than the conventional difficulty calculation, making it more difficult for malicious miners to quickly mine coins without first processing transactions.

4. QUANTUM RESISTANCE

Current cryptocurrencies are generally not quantum-proof due to their use of ECDS (which is vulnerable to Shor's Algorithm). Current transactions which use ECDS reveal the users address in the process, exposing the crackable ECDS signature. Cracking such a signature would allow unauthorized access to any and all funds associated with that address, creating a potential threat every time a transaction is made.

The SHIELD protocol will introduce Lamport signatures, or similar schemes to enable the quantum-proofing of transactions and addresses on the SHIELD network. Lamport digital signatures are based on hash functions which are not vulnerable to Shor's Algorithm, creating an additional layer of security for SHIELD users.

5. PRIVACY

SHIELD’s Project Perdu has recently been re-evaluated to ensure the correct path forward is maintained. Early plans called for the implementation of the Wraith Protocol devised by Verge Currency. However, due to Wraith Protocols relatively low specifications, we have decided to instead use PrivateSend (developed by Dash). The decision to utilize PrivateSend is advantageous as development plans to implement masternodes will be more easily aligned. This change in direction will optionally improve the transaction speed via InstantSend.

Although PrivateSend is an improvement, implementing the PrivateSend feature alone will not make transactions entirely private, to address this, Zerocoin or zk-SNARKs/zk-STARKs implementation is under consideration. Further details regarding this aspect of SHIELD will be announced in Q2 2018.

To ensure location privacy is achieved in addition to the blockchain transaction privacy, SHIELD will use Tor/I2P wallets/nodes that obfuscate the end-user’s IP address and location.

6. FUNDING

SHIELD’s self-funding mechanism may involve using a percentage of the masternode and mining block rewards. If this path is chosen, the percentage will be very small, as we only need to keep the team afloat, and the remaining funding will be used for marketing. We will also have some external sources of support which will be made by creating and joining platforms that help both developers and users. For example, SHIELD has received many donations from our supportive community which has enabled the development progress to date, furthermore, SHIELD is currently receiving support from various mining pools.

This community support will help progress the SHIELD project forward indefinitely throughout the roadmap. SHIELD did not have an ICO or a premine, unlike many of our competitors who have chosen this path; at SHIELD, we believe a strong, active community will allow SHIELD to grow and expand more organically and adaptively.

7. APPLICATION SECURITY

Security is, and always has been, a core fundamental of the SHIELD currency. We always strive to improve the security functionality of SHIELD, demonstrated in the aforementioned quantum proofing protocols.

Throughout the development of the SHIELD currency, we have identified multiple security flaws, predominantly in user interfaces, in many applications that interact with the blockchain. For this reason, we aim to have all of our original products tested on multiple levels. Using the open-source community, gathering pen testers to test applications individually, and having all members of the development team check the code, ideally acknowledging each commit before being pushed (not just for official updates). From our experience using the SHIELD Discord bot, we have observed that - with a secure backend - the link to the frontend is one of the most important aspects of a secure application.

8. INTEGRATION

The integration of a new technology with existing or purpose built platforms can be integral in determining SHIELD's ultimate usability and applicability. We will be using many popular, free platforms, such as Discord, Twitter, Facebook and more, in order to improve the SHIELD user experience. Integration on these platforms will be achieved through the development of plugins and 'bots', providing users with the ability to send SHIELD to friends, followers or influencers without the need to request a wallet address. Deeper integration may include the development of platform specific wallets - negating the need for users to have dedicated PC wallets in order to access their SHIELD currency.

Integration initiatives intended to achieve a more wide-spread level of public consumption will also be pursued through a combination of networking, and reaching out to organisations to develop additional use cases for SHIELD. This increased applicability will be vital in ensuring a stable coin price is maintained in the future.

9. PoS BOO

Project Boo is SHIELD’s own PoS scheme, modeled after Ethereum’s PoS Casper. With the introduction of a risk factor for malicious stakers, the Casper scheme improves significantly on “POSv3”. The progressive nature of the protocol makes execution of attacks exceptionally difficult, such as the 51% attack. A malicious attacker would need to hold the majority of all minted coins, while running the risk of potentially losing them all when launching such an attack.

The finality is mainly determined by stake and risk factors, which is why, theoretically, it would be difficult to execute a attack successfully even with 51% of circulation (Figure 2). A similar attack situation would be dire for a cryptocurrency like Bitcoin.

Project Boo will also solve the problem of transaction censoring. With PoW, a block miner can “choose” not to mine a block containing certain addresses, thereby censoring that address from the network. Since block creators are chosen at random, and validators are global with this PoS scheme, censoring addresses from the network becomes exceptionally difficult (with the added bonus that if you try to force the network, you will likely lose your stake).

10. FUTURE STUDY

Throughout this white paper, we have discussed some possible features and specifications that are not yet finalized. While some features such as “sharding”, and “RSK Smart Contracts” are slated on our roadmap, but are not mentioned in this document. This is due to the current state of the SHIELD currency project, which has gone through a period of heavy development and careful consideration.

This white paper is not the representative of the finality of the SHIELD development plan. The SHIELD team will release multiple white paper revisions aiming to improve approachability and readability, while also providing updated details on aspects of the project as the developers see necessary.

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*: 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 signatures**
Minting	PoW using x17, blake2s, lyra2rev2, myriad-groestl, and scrypt. PoS Boo using Quark*** hash and Slasher scheme
Transaction Min. Fee	0.05 XSH per kB
Privacy Features	Tor/I2P nodes, PrivateSend, Zerocoin****

* Best/Worst case determined by the amount of inputs/outputs in a block because inputs are 'heavier' than outputs.
** To be determined.
***Not conclusive
****Not conclusive

FIGURES:

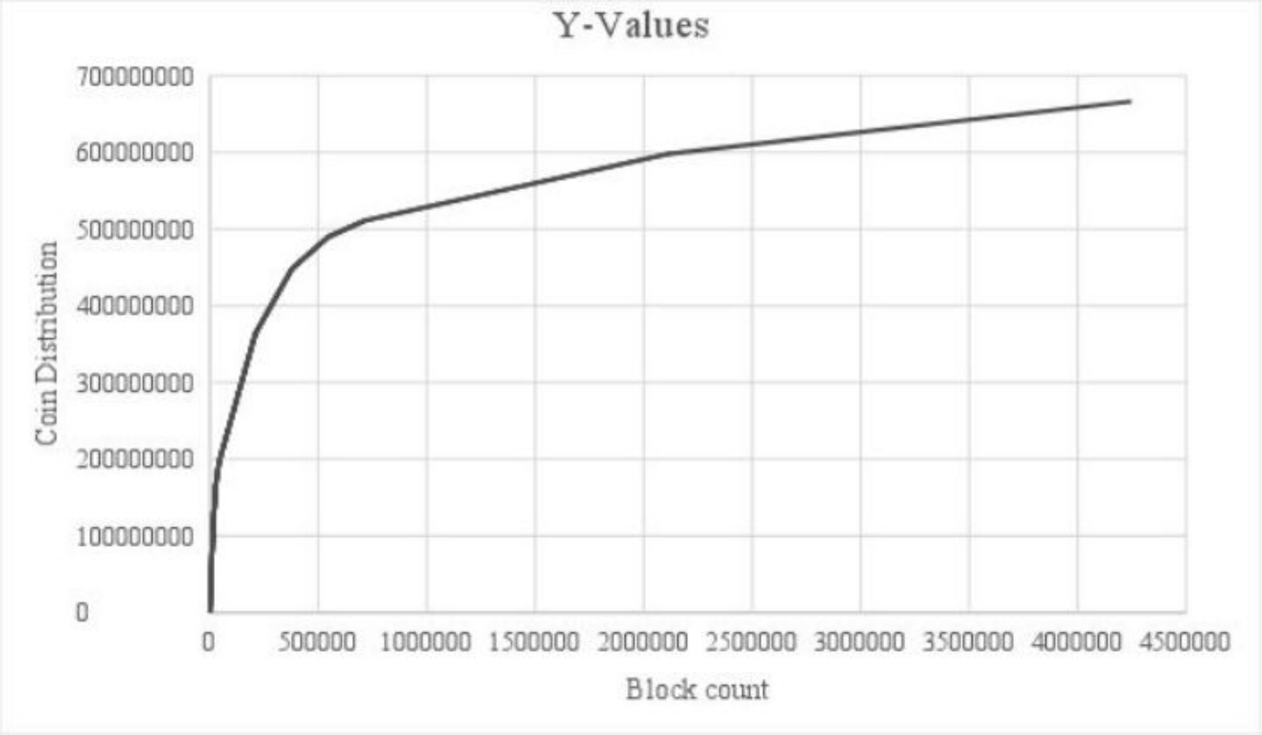

Figure 1. Graph of coin distribution (y) over blocks (x).

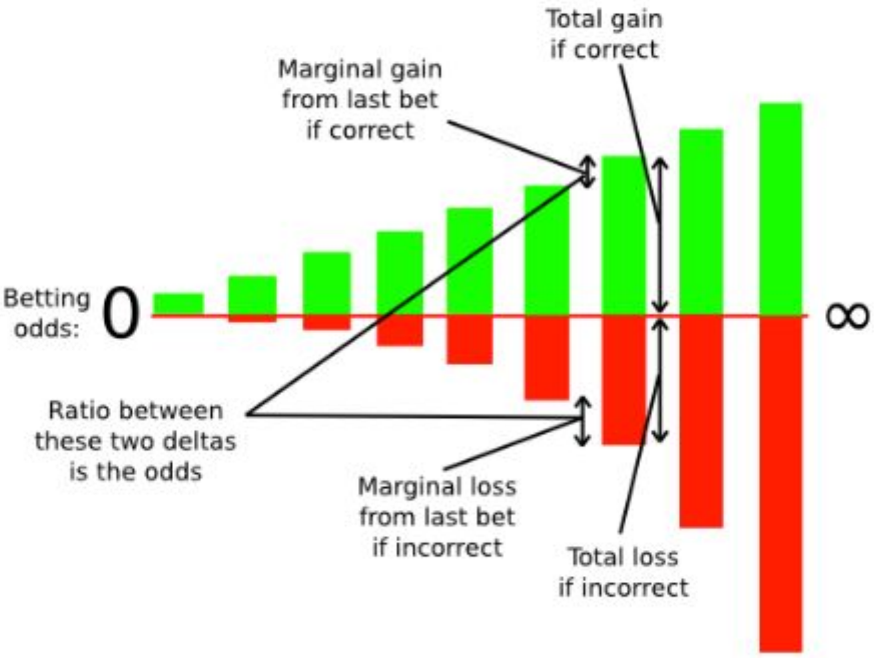

Figure 2. Graph for loss or gain for the betting system of PoS Casper.

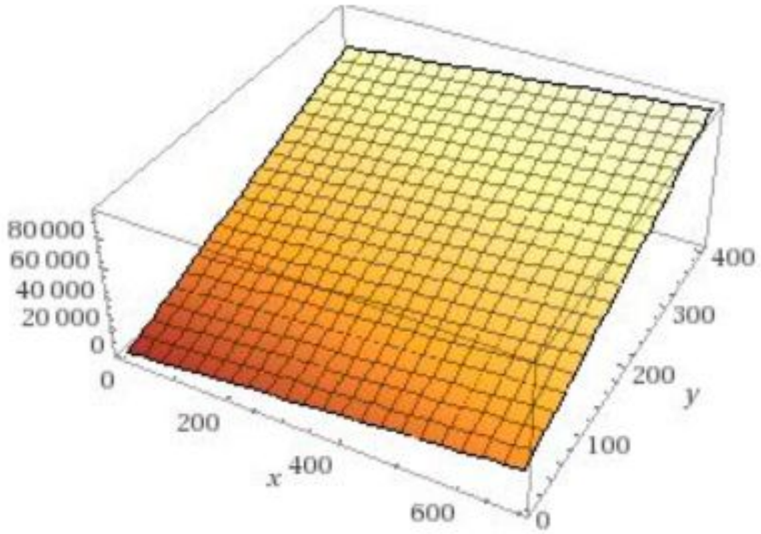

Figure 3. 3D plot of inputs(y) and output(x) where z is the size in kB The worst and best case are always around Z=500000. This assumes a bitcoin type of scenario where blocks need to be filled to process as many transactions as possible.