SHIELD white paper V1.0.0

Blockchain zukunftssicher machen

Das SHIELD Team

ShieldCoin@protonmail.com

https://ShieldCurrency.com

Abstrakt

Das SHIELD Protokol wird ECDS durch Lamport-, Winternitz- oder BLISS-Signaturen ersetzen, wodurch Transaktionen gegen Quanten-Angriffe geschützt werden können. SHIELD wird einen selbsttragenden Entwicklungszyklus erhalten, der die Fortsetzung der Entwicklung des SHIELD-Protokolls und anderer in diesem Artikel beschriebener Projekte ermöglicht. SHIELD verwendet ein benutzerdefiniertes PoS-Schema (PoS Boo) mit Hilfe von Masternodes. Diese Masternodes ermöglichen auch Funktionen wie PrivateSend und InstantSend.

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

1 - Einleitung

SHIELD ist eine Kryptowährung, die auf der Blockchain-Technologie von Satoshi Nakamoto basiert (von der er 2009 ein Whitepaper [1] veröffentlicht hat), das seitdem stetig wächst und sich verbessert. Seit einigen Jahren wird die Blockchain-Technologie zunehmend in viele Projekte eingeglieder, aber es gibt immer noch viele Probleme, die es verhindern, dass die Blockchain Technologie für den Durchschnittsverbraucher interessant wird. SHIELD versucht, viele dieser Probleme zu lösen.

2 – Die zu lösenden Probleme

Bitcoin war wirklich innovativ, als es implementiert wurde, und ein guter Teil dessen, was Satoshi gemacht hat, wird immer noch im Kern vieler Kryptowährungen verwendet. Einer dieser Ideen ist das Block-Mining, genauer gesagt das Block-Mining mit einem einzigen Algorithmus. Dies hat zur Entwicklung von spezieller Hardware (ASICs) geführt, die einen Algorithmus so effektiv hashen können, dass GPU-Mining überflüssig wird. . Ein Nachteil der Entscheidung, die er getroffen hat, wie viele jüngere Kryptowährungen erkannt haben, ist die Tatsache, dass das Minen nicht wirklich fair ist. Sie können darüber in Abschnitt 3, Multi Algorithm Mining für PoW, lesen.

Quantencomputer werden immer ausgefeilter und stehen möglicherweise schon bald der Öffentlichkeit zur Verfügung. Quantencomputer warden ob für Forscher, Regierungen, Unternehmen oder die allgemeine Öffentlichkeit, mit der Zeit von Gruppen oder Einzelnen genutzt werden. Obwohl es sich um eine unglaubliche neue Technologie handelt, die unser Leben erheblich verbessern könnte, gibt es auch viele Gründe, sich über diese Entwicklung Gedanken zu machen. Eine davon ist, dass die moderne Kryptographie von zukünftigen Quantencomputern effizient geknackt werden kann. Für viele Kryptowährungen könnte das eine defekte Blockchain bedeuten. Wie wir dieses Problem lösen werden, erfahren Sie in Abschnitt 4, Quantenwiderstand.

Große Unternehmen wie Facebook oder Google werden immer besser, wenn Sie wissen, wer der Nutzer ist und was dieser möchte. Auch wenn dies (derzeit) vielleicht nicht zu sehr beunruhigend sein mag, bedeutet es doch, in einer Welt zu leben, in der Unternehmen uns beobachten werden. es ist vielleicht nicht so schlimm, aber es sieht nicht gut aus. Es gibt viele Währungen, die behaupten, ihre Benutzer anonym zu halten, was verhindern würde, dass diese großen Unternehmen und Regierungen Ihre Ausgabengewohnheiten verfolgen können. Das Problem mit einigen dieser Coins ist, dass sie nicht so effektiv sind, wie sie behaupten, was bedeutet, dass ihre Skalierbarkeit und Praktikabilität gering bis nicht existent ist. Wir werden in Abschnitt 5, Datenschutzfunktionen, mehr darüber sprechen, wie wir unsere Nutzer anonym halten.

Einige Altcoins haben eine wirklich vielversprechende Roadmap; Einige haben sogar unglaublich talentierte Entwickler. Aber ohne Finanzierung reicht es möglicherweise nicht aus, einen Coin am Leben zu erhalten. Wenn Entwickler aus dem Projekt keine Einnahmen erzielen können, wird es immer schwieriger werden, Vollzeit daran zu arbeiten. Wir möchten nicht, dass dies geschieht, daher planen wir, einige Funktionen für SHIELD (und einige Plattformen rund um SHIELD) zu implementieren, die uns bei der Finanzierung unterstützen können. Sie können über diese Lösung in Abschnitt 6, Finanzierung, nachlesen.

Ein weiteres Problem mit Bitcoin und vielen anderen Währungen ist, dass Miner mit leistungshungriger Hardware minen müssen, um Coins herzustellen und Transaktionen zu bestätigen. Es war damals wirklich innovativ und es funktioniert immer noch gut, aber die wirtschaftlichen und ökologischen Kosten der Fortsetzung der Blockchain (die nur einen Arbeitsnachweis für den Netzwerkkonsens hat) sind wirklich hoch. Dies wurde mit unserem Proof of Stake-Schema gelöst, über das Sie in Abschnitt 9, PoS Boo, nachlesen können.

3 Multi-algorithm mining für PoW

Wir verbesserten die Verteilung von Belohnungen und die Resistenz gegen 51% Angriffen durch Nutzung von mehreren PoW-Algorithmen. Multialgorithmus-Mining ist eine Möglichkeit, mehreren Algorithmen die Möglichkeit zu geben, nach Blöcken zu suchen. Unser Ansatz ermöglicht es, viele verschiedene Geräte, einschließlich GPUs und ASICs, es zu ermöglichen, gemeinsam auf der SHIELD Blockchain zu minen. Die Verteilung der Belohnungen pro Algorithmus ist fast immer der gleiche Anteil der gesamten Belohnung. Zum Beispiel, selbst wenn ein Algorithmus 300GH / s und ein anderer 50MH / s hat, sollten sie immer noch die gleiche Menge an Coins in einer Stunde erhalten. Es verbessert den Schutz vor einem 51% Angriff, da die Blöcke verteilt sind. Jeder Algorithmus folgt seinem eigenen "Zeitplan", was bedeutet, dass Sie 51% der Hashing-Rate für jeden Algorithmus benötigt werden, um einen solchen Angriff auszuführen. Ein wichtiger Aspekt dieses Systems besteht darin, wie die Mining Schwierigkeit für jeden Algorithmus separat eingestellt wird.

Die Schwierigkeitseinstellung wird durch das "Dark Gravity Wave v3" -Schema verwaltet, das für Dash entwickelt wurde, aber in verschiedenen anderen Kryptowährungen Verwendung findet. Es verwaltet Netzwerk-Hash-Spikes und der Netzwerk-Hash fällt deutlich besser aus als die herkömmliche Schwierigkeitsberechnung und erschwert es böswilligen Minern, Coins schnell zu minen, ohne Transaktionen zu verarbeiten.

4 Schutz vor Quantenangriffen

Das SHIELD-Protokoll ist eine quantensichere Transaktion bzw. Adressierung für bestimmte Adressen.
Andere Kryptowährungen sind oft nicht quantensicher, da sie ECDS verwenden (das anfällig für Shors Algorithmus ist [9], der durch die Verwendung von Quantencomputern ermöglicht wird). Wir planen, Lamport-Signaturen oder ähnliche Schemata zu verwenden, um dies zu

ändern. Lamports digitale Signaturen basieren auf Hash-Funktionen, und Hash-Funktionen sind nicht anfällig für eine Shors Algorithmus-Attacke. Mit ECDS wird Ihre Adresse immer dann angreifbar, wenn Sie eine Transaktion senden, da Ihre crackbare ECDS-Signatur verfügbar ist. Wenn eine solche Signatur geknackt wird, wird ein unbefugter Zugriff auf die mit dieser Adresse verbundenen Geldmittel ermöglicht. Hashes sind nicht anfällig für den Algorithmus von Shor, so dass Hash-basierte digitale Signaturen die Sicherheit betroffener Adressen gegen diese drohende Bedrohung verbessern.

5 Datenschutzfunktionen

Das Projekt Perdu von SHIELD hat kürzlich eine Planänderung erfahren.
Wir hatten ursprünglich vor, das Wraith-Protokoll von Verge [6] zu implementieren, aber aufgrund seiner relativ niedrigen Spezifikationen haben wir uns stattdessen für PrivateSend (von Dash entwickelt) entschieden; Das funktioniert besser für uns, da wir bereits Masternodes implementieren müssen. Diese Änderung verbessert optional die Transaktionsgeschwindigkeit über InstantSend. Obwohl es eine Verbesserung ist, macht PrivateSend die Transaktionen immer noch nicht vollständig privat, weshalb Zerocoin [5] oder zk-SNARKs [4] / zk-STARKs in Betracht gezogen werden
Wir werden im kommenden Quartal näher darauf eingehen, ob und wie dies umgesetzt wird.

Für physische Privatsphäre werden wir Tor [8] / I2P [7] Wallets / Nodes verwenden, die die IP-Adresse und den Standort des Endnutzers verbergen.

6 Finanzierung

SHIELD-Eigenfinanzierung kann unter Umständen dadurch funktionieren, dass ein Prozentsatz der Masternode- und Mining-Block-Belohnungen verwendet werden. Dies wird ein sehr kleiner Prozentsatz sein, da wir nur das Team über Wasser halten müssen, und der Rest ist für das Marketing. Wir werden auch einige externe Quellen der Unterstützung haben, die durch das Herstellen und Verbinden von Plattformen begründet warden und sowohl Entwicklern als auch Benutzern helfen. Wir haben zum Beispiel viele Spenden von der Gemeinde erhalten, mit denen wir das Projekt vorwärts bringen können, und bekommen auch Unterstützung von verschiedenen Mining-Pools. Wir hoffen, dass dies dazu beiträgt, unser Projekt auf unbestimmte Zeit voranzubringen. Wir hatten zu dieser Zeit kein ICO oder eine Pre-mine wie viele unserer Konkurrenten; Wir glauben, dass es eine bessere Art ist, eine starke Gemeinschaft zu haben um zu Wachsen.

7 Anwendungssicherheit

Bei SHIELD dreht sich alles um Sicherheit. Wir versuchen, in dieser Hinsicht mit dem oben erwähnten Quantum-Proofing eine Menge zu verbessern, aber wir haben einen Trend in vielen anfälligen Anwendungen gesehen, die mit der Blockchain interagieren, und festgestellt, dass sich diese Sicherheitslücken fast immer in den Benutzerschnittstellen befinden. Wir denken, das ist der Grund, warum wir viele unserer Originalprodukte testen lassen müssen. Dies wird unter Verwendung der Open-Source-Community geschehen, indem Sicherheitstester und unser Entwicklerteam den Code auf mögliche Schwachstellen hin möglichst penibel überprüft.

Aus unserer Erfahrung mit unserem Discord-Bot haben wir festgestellt, dass - mit einem sicheren Back-end - die Verbindung zum Front-end eines der wichtigsten Dinge in einer sicheren Anwendung ist.

8 Integration

Die Integration einer neuen Technologie in neue oder bestehende Plattformen kann Einfluss auf die endgültige Verwendbarkeit und Anwendbarkeit haben. Wir werden viele beliebte und kostenlose Plattformen wie Discord und Twitter nutzen, um die Benutzererfahrung zu verbessern. Wir werden dies tun, indem wir Plugins und Bots für Plattformen wie Discord, Twitter, Facebook (und mehr) entwickeln. Diese Integration gibt Ihnen die Möglichkeit, SHIELD an jemanden zu senden, ohne sie nach ihrer Wallet-Adresse fragen zu müssen. Diese Integration könnte auch eine Wallet für diese Plattformen beinhalten - auf diese Weise brauchen Sie nicht einmal einen speziellen Wallet auf Ihrem PC zu haben, um SHIELD zu verwenden.

Die Integration erhält auch mehr Anwendungsfälle für den öffentlichen Konsum. In Verbindung mit der Vernetzung ist dies ein sehr wichtiger Teil der Erweiterung unserer Zielgruppe und der Anwendungsfälle. Daher werden wir viele verbundene Unternehmen kontaktieren, um diese Faktoren zu erhöhen. Dies ermöglicht es uns mehr Stabilität in unseren Preisen zu haben und wir mehr Anwendungsmöglichkeiten haben werden.

9 PoS Boo

SHIELD Boo ist unser eigenes PoS-Schema basierend auf PoS Casper [2]. Das Casper-Schema, PoSv3, verbessert sich am meisten [3] mit der Einführung eines Risikofaktors für böswillige Stakers (Staken ist das Halten der Coins und das Erhalten einer Belohnung vom System hierfür). Das System ist so progressiv, dass Angriffe wie der 51% -Angriff erheblich erschwert werden. Sie würden die Mehrheit aller existierenden Coins benötigen, und Sie werden auch das Potenzial haben, alle Coins, wenn Sie einen solchen Angriff starten [2]. Die Endgültigkeit wird hauptsächlich durch Einsatz- und Risikofaktoren bestimmt, weshalb es schwierig sein kann, einen Angriff selbst mit 51% der Zirkulation

erfolgreich durchzuführen (Abbildung 2), eine Situation, die sonst für eine Münze wie Bitcoin sehr schlimm wäre.

Ein weiteres Problem, das PoS Casper / Boo löst, ist die Transaktionzensur. Mit PoW kann ein Block Miner "auswählen", einen Block nicht zu minen, der bestimmte Adressen enthält, und diese Adresse aus dem Netzwerk zensieren. Da Block-Ersteller zufällig ausgewählt werden und Validierer mit diesem PoS-Schema global sind, ist es wirklich schwierig, Adressen aus dem Netzwerk zu zensieren (mit dem zusätzlichen Bonus, dass Sie höchstwahrscheinlich Ihre Stakes verlieren werden, wenn Sie versuchen, das Netzwerk zu erzwingen).

10 Zukünftige Studien

Wie Sie vielleicht zum Beispiel in Abschnitt 5 bemerkt haben, diskutierten wir einige mögliche Merkmale / Spezifikationen, die nicht abgeschlossen sind. Einige der Funktionen aus der Roadmap fehlen ebenfalls, wie "Sharding" und "Smart Contracts". Dies liegt daran, SHIELD sich noch immer in der Entwicklungsphase befindet und jeder Schritt sorgfältig geprüft wird.

Wir werden dieses Whitepaper aktualisieren oder ein Neues erstellen, je nachdem, was wir in Zukunft ändern. Dies ist nicht der Endgültige SHIELD-Entwicklungsplan. Darüber hinaus wird dieses Dokument mehrere Revisionen enthalten, die die Zugänglichkeit, Lesbarkeit und Details zu Themen, die es erfordern, verbessern.

11 Kern Spezifikationen

Hinweis: Diese Spezifikationen enthalten Zukunftspläne

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

Quellen

[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

[4] Not conclusive

[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

Figures

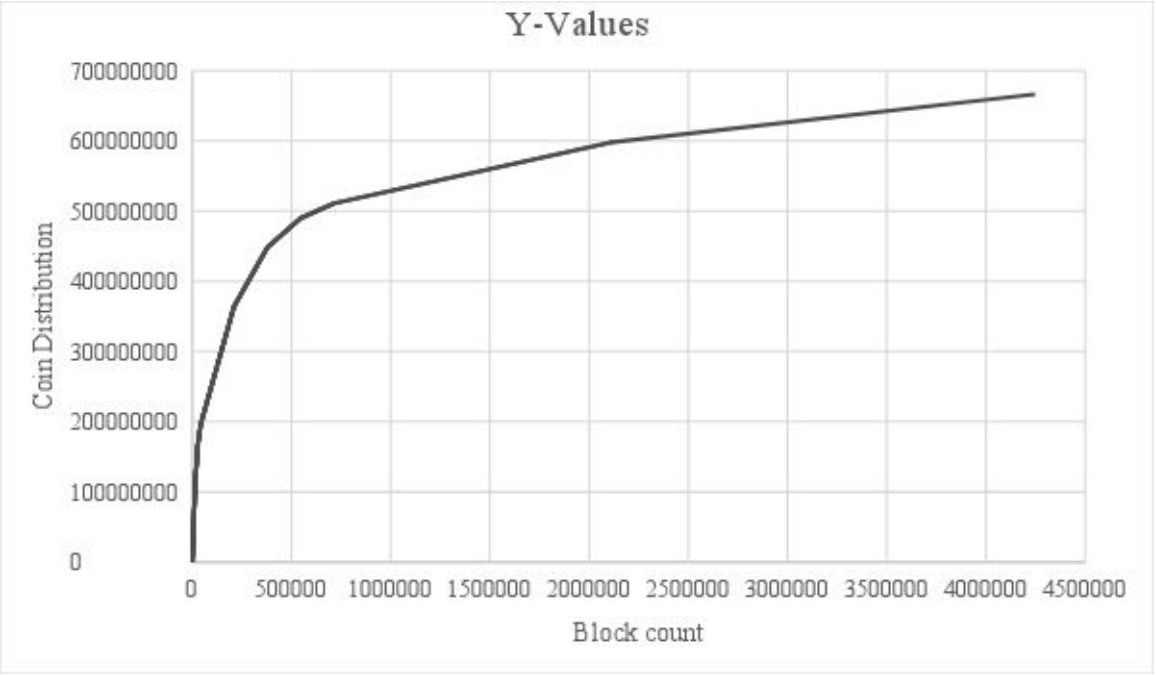

Abbildung 1. Graph der Münzverteilung (y) über Blöcke (x)

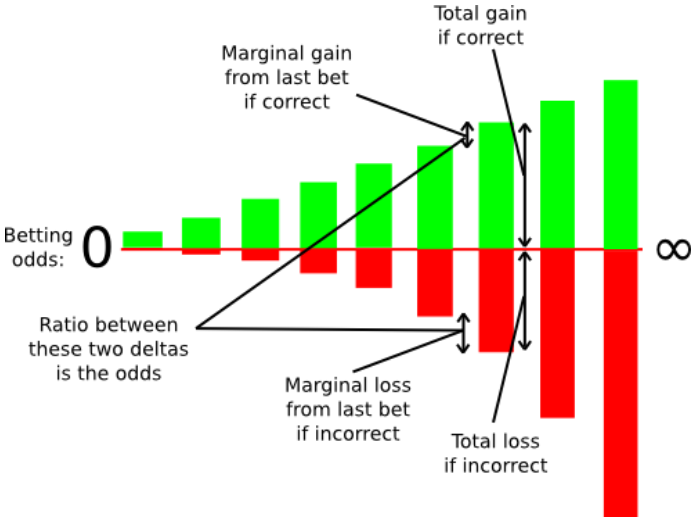

Abbildung 2. Graph for loss or gain for the betting system of PoS Casper

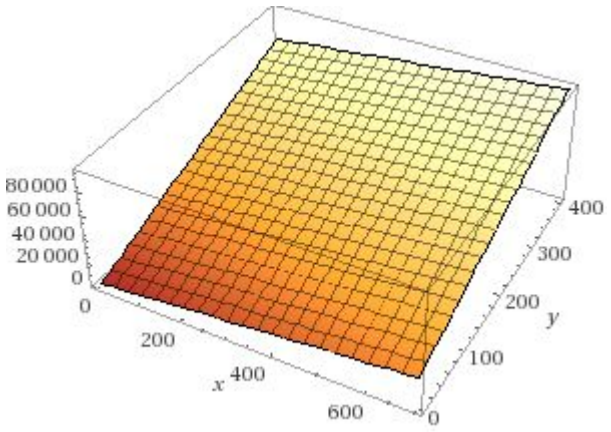

Abbildung 3. 3D-Darstellung von Eingaben (y) und Ausgabe (x) wobei z die Größe in kB ist. Der schlechteste und der beste Fall sind immer in der Nähe von Z = 500000. Dies setzt ein Bitcoin-Szenario voraus, in dem Blöcke gefüllt werden müssen, um so viele Transaktionen wie möglich zu verarbeiten.