中文版

神盾白皮书 V1.0.1

面向未来的区块链

神盾币团队

ShieldCoin@protonmail.com
https://ShieldCurrency.com

摘要

SHIELD 协议将使用 Lamport, Winternitz 或者 BLISS 代替 ECDS 对区块进行签名，以使钱包地址“抗量子攻击”。SHIELD 在开发周期内自给自足，以保证 SHIELD 协议和其他本文中描述的项目开发的延续性。SHIELD 将在主节点（Masternodes）的支持下使用自定义的 PoS 算法（PoS Boo），同时，这些主节点将会使能“私有发送（PrivateSend）”和“即时发送（InstantSend）”这样的特性。

关键词：神盾，抗量子，主节点，加密数字币，区块链，匿名

1．介绍

SHIELD 是一种基于中本聪(他在 2009 年发布了白皮书[1])提出的区块链技术的加密数字币，这种技术自从发布以后一直在不断的发展和改进。这几年里，区块链技术很快的获得了采用，但是仍然存在很多问题束缚着这种技术成为主流。SHIELD 将会解决这里边的很多问题。

2．解决的问题

比特币真是一个伟大的创新，现在很多的加密币依旧在使用中本聪提出的一些好的理念。其中一个贡献是区块挖矿，更具体的说，就是单一算法挖矿。这导致设计出了特殊的硬件来高效的计算一个算法对应的哈希值，以至于使 GPU 挖矿变得过时了。他做出的决定中有一个缺陷，也是许多新创建的加密币意识到的问题：这种挖矿方式非常的不公平。你可以在本文的*第三章：“多种 PoW 挖矿算法”*详细阅读。

量子计算机将会变得更加的复杂，而且很可能即将面世。不管是研究员、政府、商人，还是普通大众在研究它，我们终将会看到量子计算变成可能。虽然这是一个令人难以置信的新技术，它可以大大改善我们的生活。但是，对这种技术的发展存在很多值得我们关注的问题。其中一个问题是当代密码学可以被未来的量子计算机轻松的破解。对于许多的加密币来说，这意味着区块链被攻破了。我们的解决方案将在*第四章“抗量子”*进行介绍。

Facebook、Google 这样的大公司越来越清楚的知道你是谁，以及你想要什么。虽然这（在当前来看）还不需要太操心，但这也意味着我们生活在有企业监视的世界里。这点或许没有想象中的那么坏，但至少看起来不是很好。有很多的加密币声称它们可以保持用户匿名，即可以阻止大公司或者政府对他们的消费行为进行跟踪。问题是其中一些加密币的匿名性并没有达到他们声称的水平，这意味着在匿名扩展性和可用性上低到不存在。我们在*第 5 章“隐私性”*中讨论我们保持用户匿名的方法。

一些数字币有一个非常光明的路线图、一些甚至有非常有天赋的开发者。但如果没有资金支持，它的开发工作将很难持续下去。如果开发者不能够从项目中获取一些收入，他们将很难保持全职的开发工作。我们不希望这样的事情发生，所以我们计划通过实现 SHIELD（和 SHIELD 的周边平台）的一些特性来帮助我们获取资金。你可以在*第 6 章“资金”*中获取到我们的解决方案。

另一个比特币和其他许多数字币共同面对的问题是矿工不得不使用非常耗电的硬件设备来挖矿和确认交易。虽然这一点在当时非常的具有创新性，并且仍旧运转良好。但是继续运行区块链（只有网络共识的工作证明方式）的经济和环境成本是非常的高。这个问题已经通过我们的 PoS 方案解决了，你可以在*第 9 章“PoS Boo”*阅读它。

3．多种 PoW 挖矿算法

我们通过多种 PoW 算法来提升奖励平均分配性和抵抗 51%[需要引证]算力攻击能力。多算法挖矿是一种允许多种类型的处理单元在区块上挖掘的方法，我们的这种方法允许诸如 GPU、ASIC 等许多不同类型的设备在 SHIELD 区块链上共同挖掘。而且，每种算法挖矿奖励分配的比例几乎总是相同的。例如，一个算法的算力有 300GH/s，而另外一个只有 50MH/S，但这两个

算法在 1 个小时内获取到的币数量是相同的。SHIELD 通过控制出块方式来提升其抵抗 51% 算力攻击的能力：每种算法有它们独自的“进度”，也就是说你需要控制每种算法都达到 51% 的哈希算力才能成功的实施这种攻击。另外一个重要的方面是，系统中每种算法难度的调整是单独的。

挖掘难度调整是通过专门为 Dash 设计的“暗黑重力波 V3”方案来控制的，这种算法已经被很多的加密币广泛使用。它比以往的难度计算方案在控制网络哈希峰值和低谷上好得多，这就会让不处理交易而快速挖掘币的恶意矿工实施起来变得更难。

4．抗量子

SHIELD 协议对特定地址的交易和寻址是抗量子攻击的，而其他很多加密币通常因为使用 ECDS 算法（这种算法通过在量子计算机中使用 Shor 算法[9]很容易攻破）而不是抗量子的。我们计划使用 Lamport 签名或者其他类似的方案来解决量子攻击问题：因为哈希算法是不会被 Shor 算法攻破的，而 Lamport 数字签名正是基于哈希算法的，所以 Lamport 签名是不会被量子计算机攻破的。如果使用 ECDS，任何时候你发起一笔交易，你的地址将可能会被攻击，因为你泄露了可以被攻破的 ECSD 签名信息。一旦签名信息被攻破，攻击者就可以在未经授权的情况下访问该地址上的资金。哈希算法不会被 Shor 算法攻破，因此使用基于哈希数字签名的方案能够改善受影响地址的安全性，以此来抵御这种迫在眉睫的威胁。

5．隐私性

最近，SHIELD 的 Perdu 项目在原来的计划上发生一些改变：原先我们计划实现 Verge 币的 Wraith 协议[6]，但是由于它的规格相对较低，我们最终决定采用 PrivateSend（Dash 开发的），这将与我们已经在实现的主节点更好的配合工作。这个改变可能会提升 InstantSend 的交易速度。虽然这是一个很大的提升，但是 PrivateSend 仍然不能完全保护交易的隐私信息，这也是 Zerocoin 或 zk-SNARKs[4]/zk-STARKs 在考虑的问题。我们将在本季度实现了之后更加深入的讨论这些内容。

至于物理的隐私信息，我们会使用 Tor[8]/I2P[7]来隐藏最终用户的钱包/节点 IP 地址和地理位置。

6．资金

SHIELD 通过部署一部分主节点和挖矿的回馈实现资金自筹。对于我们团队自身来说只需要使用其中很小的一部分，大部分将用在市场方面。另外，我们也会加入或开发一些对开发者和用户都有益的平台来获取外部的资助。例如，我们从社区收到了大量的支持我们项目开发的捐助，也获得很多矿池的帮助。我们希望这可以让我们持续的推进项目的开展。我们不像其他很多竞争对手一样进行 ICO 或预挖，我们相信拥有一个强大的社区是一个更好的扩张方式。

7．应用安全

SHIELD 特别注重安全！我们尝试在很多方面进行大幅安全提升，比如前面提到的抗量子攻击。但是，我们在很多受攻击的区块链应用中看到了一个趋势：漏洞往往发生在用户与区块链交互的接口上。我想这是为什么我们需要在原型产品上进行大量测试的原因。一方面，测试工作可以通过收集开源社区、个人渗透爱好者的测试结果来开展；另一方面，我们要求所有的开发团队在提交代码（不仅仅是官方更新）时尽可能详细的进行代码检查。根据我们使用 Discord 机器人的经验，我们意识到，有一个安全的后端--以此链接到前端是安全应用程序中最重要的事情之一。

8．融合

将一种新技术融合到一个新的或已有的平台可能会影响产品最终的可用性和适用性。我们会使用诸如 Discord、Twitter、Facebook 等免费而流行的平台，并在其上开发插件、“机器人”，以此来提升用户体验。这个整合将使你在无需询问对方钱包地址的情况将神盾币发送给对方；同时，这个整合可能会最终为这些平台开发出相应的钱包，那样的话你就不会只能在电脑上使用神盾币了。

与大众消费的融合有更多其他的场景。也就是说，神盾与网络相融合是一种非常重要的拓展使用场景和用户的方式。因此，我们会与很多相关联的商业机构合作来增强这些方面。如此这样，神盾币的价格会更加的稳定，并且将拥有更广阔的应用市场。

9．PoS Boo

SHIELD Boo 是我们基于 PoS Casper 独创的 PoS 方案。我们知道 Casper 方案对“PoSv3”改进最成功的点是引入了风险因子，以此来对付恶意矿工。这个系统在对付类似 51%算力攻击方面取得了长足的进步：你需要拥有已挖出的大部分币，而且你在攻击时将面临失去它们全部的风险。而且攻击成功与否主要取决于你的股份和风险因子，这就是为什么即使拥有 51%算力（*图 2*），成功的实施攻击也是很困难的。而这样的机制正是比特币所迫切需要的。

另外一个 PoS Casper/Boo 解决的问题是交易审查。对于 PoW 机制，区块矿工可以“选择”不去挖掘包含某些特定地址的块，然后在网络上审查这些地址。由于区块的创造者是随机选择的，而在 PoS 方案里验证者是全局的，这样就很难从网络中对地址进行审查（通过增加额外股息，如果你想在网络上欺骗，你将会失去你的股份）。

10．未来的研究

你可能已经注意到了在第 5 章我们讨论了并没有最终确定的一些特性/规格。另外，有一些在路线图中的特性（比如“分片”和“智能合约”）同样没有出现。这是因为当前很多 SHIELD 相关的工作正在集中开发和仔细考虑。

我们会不断的更新白皮书，或者干脆基于未来的改变重写一份。这不是 SHIELD 最终的开发计划书。另外，这份白皮书将会在可实现性、易用性、信息详细性方面进行多次修订。

11．关键规格

注：这些规格包括未来的一些计划内容

SHIELD 的核心规格参数如下表所示：

类别	规格参数
出块时间	45 秒; 240 个确认才成熟; SwiftTx/InstanSend
块大小	500kB/块
块回馈	见图 1
交易量/块	最坏情况：2777 笔/块　最好情况：14701 笔/块
交易量/秒	最坏情况：61 笔/秒　最好情况：327 笔/秒 见图 3 的图像所示
签名	ECDSA（带有可选 Lamport/Winternitz/BLISS 算法）签名
挖矿	PoW：x17, blake2s, lyra2rev2, myriad-groestl, scrypt PoS Boo：使用 Quark 哈希 和 Slasher 方案
最小交易费用	0.05 XSH/kB
隐私特性	Tor/I2P 节点，PrivateSend，零币

参考文献

[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

图表

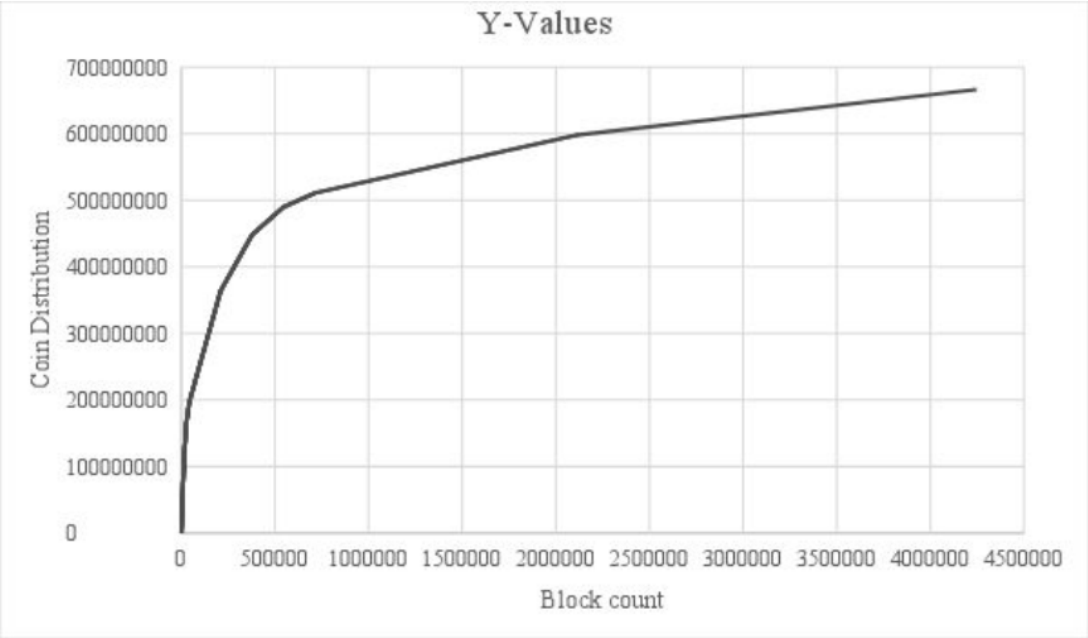

图 1. 区块与币分发量关系图

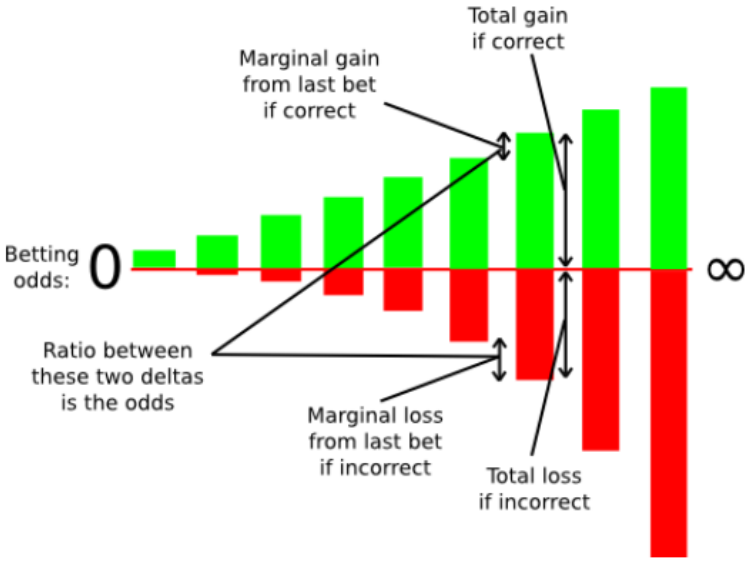

图 2. PoS Capser 赌注系统的得与失关系图

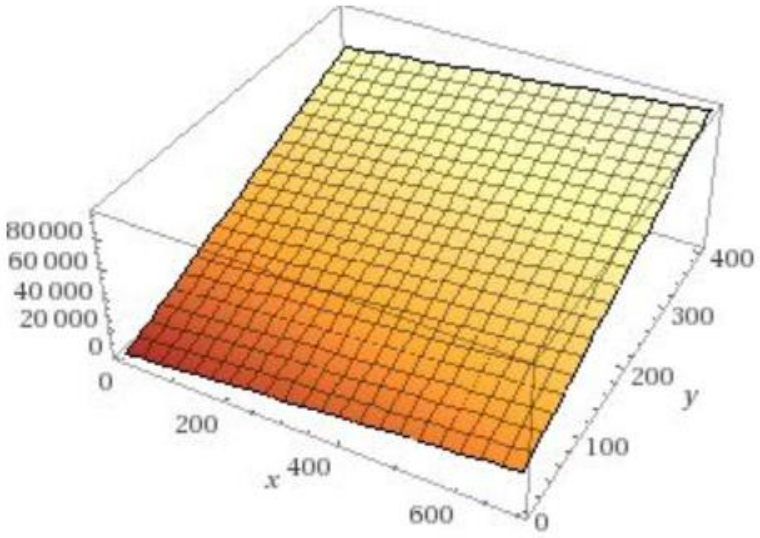

图 3. 输入（y）和输出（x）的三维关系图，其中 z 是以 kB 为单位。最好和最坏的情况总是出现在 Z=500,000 左右。这个关系图建立在类似比特币的场景之上：区块总是被装满以处理尽可能多的交易。