SHIELD white paper V1.0.0

Geleceğe uyumlu Blockchain

SHIELD takımı

ShieldCoin@protonmail.com

https://ShieldCurrency.com

özet

SHIELD protokolü, adreslerin "kuantum uyumlu" olmasını sağlayan Lamport, Winternitz veya BLISS imzaları ile ECDS'nin yerini alacak. SHIELD protokolünün ve bu makalede açıklanan diğer projelerin geliştirilmesinin devam etmesini sağlayacak kendinden destekli bir geliştirme döngüsü alacaktır. SHIELD, Masternodes yardımıyla özel bir PoS şeması (PoS Boo) kullanacaktır. Bu masterodları ayrıca PrivateSend ve InstantSend gibi özellikleri de etkinleştirecek.

Anahtar Kelimeler: SHIELD, kuantum uyumlu, masternodlar, şifreleme(cryptocurrency), blockcain, gizlilik

1. Giriş

SHIELD, Satoshi Nakamoto'nun (2009'da bir [1] ‚withepaper' çıkardığı) blockchain teknolojisine dayanan bir şifreleme yöntemidir ve o zamandan beri gelişmekte ve gelişmektedir. Birkaç yıldır blockchain teknolojisi giderek daha çok benimseniyor ancak bu teknolojinin ana akım haline gelmesini engelleyen birçok sorun var. SHIELD bu sorunların çoğunu çözmek istiyor.

2 - Çözülmesi gereken sorunlar

Bitcoin, uygulandığında gerçekten yenilikçi ve Satoshi'nin yaptığı şeylerin bir kısmı günümüzde birçok şifreli para biriminin merkezinde hala kullanılmaktadır. Bu katkılardan biri blok madenciliğidir, ancak daha özel olarak, madenciliği tek bir algoritmayla engellemektedir. Bu, bir algoritmayı etkin bir şekilde karma yapabilen ve GPU madenciliğini eski haline getiren özel donanımın (ASIC'ler) geliştirilmesine yol açmıştır. . Yaptığı kararın bir dezavantajı, daha genç kripto para birimleri gerçekleştiği gibi, madenciliğin gerçekten adil olmadığı gerçeğidir. Daha fazla bilgi için Çoklu Algoritma madenciliği 3. bölümünde okuyabilirsiniz. (*Multi Algorithm mining for PoW*)

Kuantum bilgisayarlar gittikçe daha sofistike hale geliyor ve halka açık olma eşiğinde olabilir. İster araştırmacılar, hükümetler, işletmeler veya genel halk için olsun, sonunda kuantum bilgisinin varlıklı gruplar ve kendi çıkarları için bireyler tarafından kullanılabileceğini göreceğiz. Yaşamlarımızı büyük ölçüde artırabilecek inanılmaz yeni bir teknoloji olmasına rağmen, bu gelişme konusunda endişe edilecek nedenler de vardır. Bunlardan biri, günümüz kriptografisinin gelecek kuantum bilgisayarları tarafından bir şekilde kırılabilmesidir. Çoğu kripto para birimi için kırık bir blockchain anlamına gelebilir. Bu sorunu nasıl çözeceğimiz,4. Bölüm , Kuantum Direniş'te özetlenmiştir.

Facebook veya Google gibi büyük şirketler, kim olduğunuzu ve neyi istediğinizi bilmekte daha iyi hale geliyor. Bu, (şu anda) çok fazla ilgili olmasa da, işletmelerin bizi izleyeceği bir dünyada yaşamak anlamına gelecektir; bu o kadar da kötü olmayabilir, ama harika görünmüyor. Kullanıcılarını anonim tutmaya çalışan ve bu büyük şirketlerin ve hükümetlerin harcama alışkanlıklarınızı takip etmesini engelleyen para birimleri vardır. Bazı kripto paralar ile ilgili sorun, onların talep ettikleri kadar etkili olmaması, yani ölçeklenebilirliklerinin ve uygulanabilirliğinin düşük ve mevcut olmaması anlamına geliyor. Kullanıcılarımızı gizli tutmamızın yolları hakkında 5. bölümdeki Gizlilik özelliklerinde daha fazla bahsedeceğiz.
Bazı altcoinlar gerçekten umut verici bir yol haritasına sahiptir; Bazıları inanılmaz derecede yetenekli geliştiricilere sahipler. Fakat bir fon yardımı olmadan bir kripto paranın hayatta kalması yeterli olmayabilir. Geliştiriciler projeden bir miktar gelir bulamazlarsa, tam zamanlı çalışmak giderek daha zor hale gelecektir. Bunun olmasını istemiyoruz, SHIELD'e (ve SHIELD çevresindeki bazı platformlara) finansman konusunda yardımcı olabilecek bazı özellikleri uygulamayı planlıyoruz. Bu çözüm hakkında 6. bölümdeki kaynaklardan okuyabilirsiniz. (Funding)

Bitcoin ve diğer pek çok para birimi ile ilgili bir diğer sorun, madencilerin işlem onayı vermesine izin vermek için çok enerji sarf eden bilgisayarlar ile madencilik yapmak zorunda kalmaları. Gerçekten yenilikçi ve hala iyi çalışıyor olur ancak blockchain devam ettirmenin ekonomik ve çevresel maliyeti (sadece ağ mutabakatı için İş Kanıtı'na sahip) çok yüksekselir. Bu konu,9ç bölümde okuyabileceğiniz Tahkim Kanıtı şema ile çözülmüştür.

3 PoW için çoklu algoritma madenciliği

Ödüllerin eşit dağılımını ve birden fazla PoW algoritması ile% 51'lik [atıf gerektiren] saldırılara karşı direnç üzerine geliştik. Çoklu algoritma madenciliği, birden fazla işleme ünitesinin bloklar için madencilik bağlanmasına izin veren bir yöntemdir; yaklaşımımız hem GPU'ları hem de ASIC'leri içeren çok sayıda farklı aygıtın SHIELD blockchainle birlikte kullanılmasını sağlar. Her algoritma için ödüllerin dağılımı hemen hemen her zaman toplam ödülün zaman içindeki oranı ile aynıdır. Örneğin, bir algoritma 300GH / s, diğeri 50MH / s olsa bile, bir saat içinde yine aynı miktarda kripto paraya sahip olmalı. Blokların dağıtılma biçimi nedeniyle% 51 saldırı önleme üzerinde geliştirir; her algoritma kendi "zamanlamasını" izler; bu, böyle bir saldırıyı gerçekleştirmek için her algoritmanın karma oranının% 51'e ihtiyaç duyduğunuz anlamına gelir. Bu sistemin önemli bir özelliği, her bir algoritmanın zorluğunun ayrı ayrı nasıl ayarlandığıyla ilgilidir.

Zorluk ayarı, Dash için geliştirilen, ancak çeşitli diğer kripto para birimlerinde kullanılan "Dark Gravity Wave v3" şemasına göre yönetilmektedir. Ağ karması ani ve ağ karması damlalarını geleneksel zorluk hesaplamasından çok daha iyi yönetir ve kötü niyetli madencilerin işlemleri harcamadan kripto paralara hızla çıkarması daha zor hale gelir.

4 Kuantum Direniş

SHIELD protokolü, belirli adreslerin kuantum uyumlu işlem / adresleme yöntemidir. Diğer kripto para birimleri, ECDS (kuantum bilgisayarları kullanarak etkinleştirilen Shor's Algorithm [9]'a karşı savunmasız olduğu için) nedeniyle kuantumlara dayanıklı değildir. Bunu değiştirmek için Lamport imzaları veya benzer düzenleri kullanmayı planlıyoruz. Lamport dijital imzalar karma işlevlerine dayanır ve karma işlevleri Shor'un Algoritması'na karşı savunmasız değildir. ECDS ile, bir işlem gönderdiğinizde, adresiniz savunmasız hale gelir, çünkü kırılabilir ECDS imzanız açıktır. Böyle bir imza çatlamak, o adresle ilişkili fonlara yetkisiz erişime izin verebilir. Yığınlar Shor'un Algoritması'na karşı savunmasız değildir, dolayısıyla karma tabanlı dijital imzalar etkilenen adreslerin bu belirsiz tehdide karşı geliştirilir.

5 Gizlilik özellikleri

SHIELD Perdu Projesi, son zamanlarda bir plan değişikliği geçirmiş olan bir projedir. Başlangıçta VergeCurrency'ın Wraith protokolünü [6] uygulamayı planladık, ancak nispeten düşük özellikleri nedeniyle, bunun yerine PrivateSend'i (Dash tarafından geliştirilen) seçmeye karar verdik; zaten masternodları uygulamamız gerektiğinden bu bizim için daha iyi sonuç veriyor. Bu değişiklik isteğe bağlı olarak InstantSend aracılığıyla işlem hızını artıracaktır. Özel bir gelişmeyle birlikte, PrivateSend hâlâ

işlemleri tamamen özel yapmaz, bu nedenle Zerocoin [5] veya zk-SNARK [4] / zk-STARK'lar inceleniyor
Bunun uygulanacağı çeyrekte bu konuyla ilgili daha detaylı bilgi alacağız.
Fiziksel gizlilik için son kullanıcının IP adresini ve konumunu gizleyen Tor [8] / I2P [7] cüzdanlarını / düğümlerini kullanacağız.

6 Finansman

SHIELD öz finansmanı, masternod ve madencilik blok ödüllerinin bir yüzdesini kullanarak çalışabilir. Bu, yalnızca ekibi ayakta tutmamız gerektiğinden çok az bir yüzdelik olacak ve gerisi pazarlama içindir. Hem geliştiricilere hem de kullanıcılara yardımcı olan platformlar kurarak ve katılarak yapacak bazı dış destek kaynakları edineceğiz. Örneğin, projeyi yönlendirebildiğimiz topluluktan birçok bağış aldık ve çeşitli madencilik havuzlarından da destek aldık. Umarız bunun projemizi süresiz ilerletmesine yardımcı oluruz. Şu anda pek çok rakibimiz gibi bir ICO veya bir öncülümüz yoktu; güçlü bir topluluğa sahip olmamız genişlememiz için daha iyi bir yol olduğuna inanıyoruz.

7 Uygulama güvenliği

SHIELD, güvenlikle ilgili. Yukarıda bahsedilen kuantum uyumlu koruma ile bu konuda çok şey geliştirmek için çalışıyoruz, ancak blockchain etkileşime giren çok sayıda savunmasız uygulamada bir eğilim gördük ve deliklerin neredeyse daima kullanıcı arabirimlerinde olduğunu fark ettik. Bunun için orijinal ürünlerimizi test ettirmek zorunda kalmamızın nedeni budur, bu açık kaynak topluluğunu kullanarak yapılmalı, bireysel olarak test etmek için kalem testçileri bir araya getirilmelidir ve tüm geliştirme ekibimiz kodu belki de her ikisini de onaylamış olarak kontrol ettirmelidir (ve sadece resmi güncellemeler için değil).
Discord bot'u kullanan deneyimlerimizden, güvenli bir arka uçla ön uç bağlantısının güvenli bir uygulamadaki en önemli şeylerden biri olduğunu gözlemledik.

8 Entegrasyon

Yeni bir teknolojinin yeni veya mevcut platformlara entegrasyonu, nihai kullanılabilirliğini ve uygulanabilirliğinin belirlenmesinde etkili olabilir. Discord ve Twitter gibi birçok popüler ve ücretsiz platformu kullanıcı deneyimini iyileştirmenin bir yolu olarak kullanacağız. Bunu Discord, Twitter, Facebook (ve daha pek çok) gibi platformlar için eklentiler ve 'botlar' geliştirerek yapacağız. Bu entegrasyon SHIELD'i cüzdan adresinden istemek zorunda kalmadan bir başkasına gönderebilme olanağı sağlar. Bu entegrasyon, bu platformlar için bir cüzdan da içerebilir. Bu şekilde, SHIELD'i kullanmak için bilgisayarınıza özel cüzdan almanız gerekmez.

Entegrasyon, kamu tüketiminde daha fazla kullanım örneği alıyor. Yani, ağ oluşturma ile birlikte, kitlenizi genişletmek ve vakaları kullanmanın çok önemli bir parçasıdır. Bu nedenle, bu faktörleri artırmak için birçok ilgili işletmeye başvuracağız. Bu, fiyatlarımızda daha istikrarlı olmamızı sağlayacak ve daha fazla uygulanabilirlik kazanacağız.

9 PoS Boo

SHIELD Boo, PoS Casper'a dayanan kendi PoS şemamızdır [2]. Casper planı, kötü amaçlı saldırılar için bir risk faktörü getirilerek "POSv3" [3] 'ü en iyi düzeye getirir.

Sistem,% 51 saldırı gibi saldırıları gerçekleştirmek oldukça zor hale getiren ilerici bir program. tüm kripto paraların çoğunluğuna ihtiyaç duyarsınız ve böyle bir saldırıyı başlattığınızda hepsini kaybetme potansiyeline de sahip olacaksınız [2]. Sonuç çoğunlukla bahis ve risk faktörleri tarafından belirlenir, bu nedenle dolaşımın% 51'inde bile başarıyla bir saldırı yürütmek zor olabilir (Şekil 2), bu durum Bitcoin gibi bir kripto para için çok korkunç olur.

PoS Casper / Boo'nun çözdüğü bir diğer problem, işlem sansürlenmesidir. PoW ile, bir blok madencisi belirli adresleri içeren bir bloğu almama "seçebilir" ve böylece o adresin şebekeden sansürlenmesini seçebilir. Blok yaratıcıları rasgele seçildiğinden ve doğrulayıcılar bu PoS şemasında küresel olduğunda, ağları adresleri sansürlemek gerçekten zor (şebekeyi zorlamaya çalışırsanız, muhtemelen bahis miktarınızı kaybedersiniz).

10 Gelecekteki çalışma

Örneğin-Bölüm 5'te fark ettiğiniz gibi, kesinleşmemiş bazı olası özellikler / özellikler tartışılmaktadır. Yol haritasındaki bazı özellikler de "gelişmekte" ve "akıllı sözleşmeler"de eksikikler vardır. Bunun nedeni, çok sayıda KORUNMA ağır gelişim ve dikkatli düşünülme halindedir.

11 Temel Özellikler

Not: Bu spesifikasyonlar gelecek planları içermektedir
SHIELD'in çekirdeği için aşağıdaki özellikleri kullanacağız:

konu	tanımlama
Blok zamanı	45 saniye ; 240 onay ; SwiftTx/InstantSend
Blok	500kB/blok
Blok ödülü	Şema 1e bakınız
işlemler/blok	En kötü[1]: 2777 tx/blok en iyi: 14701 tx/blok
işlemler/saniye	En kötü: 61 tx/s en iyi: 327 tx/s Grafikler için şema 3 bakınız
imzalar	ECDSA Lamport/Winternitz/BLISS[2] seçenekli imzalar

madencilik	PoW kullanımı x17, blake2s, lyra2rev2, myriad-groestl, and scrypt. PoS Boo using Quark[3] hash and Slasher scheme
Işlem ücreti	0.05 XSH bir kB
Gizlilik özellikleri	Tor/I2P nodes, PrivateSend, Zerocoin[4]

[1] Bir blokta girdi / çıktı miktarı tarafından belirlenen en iyi / en kötü durum, girdiler çıktılardan 'daha ağır' olduğu için Belirlenecek

[2] Belirlenecek

[3] Not conclusive

Kaynaklar

[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

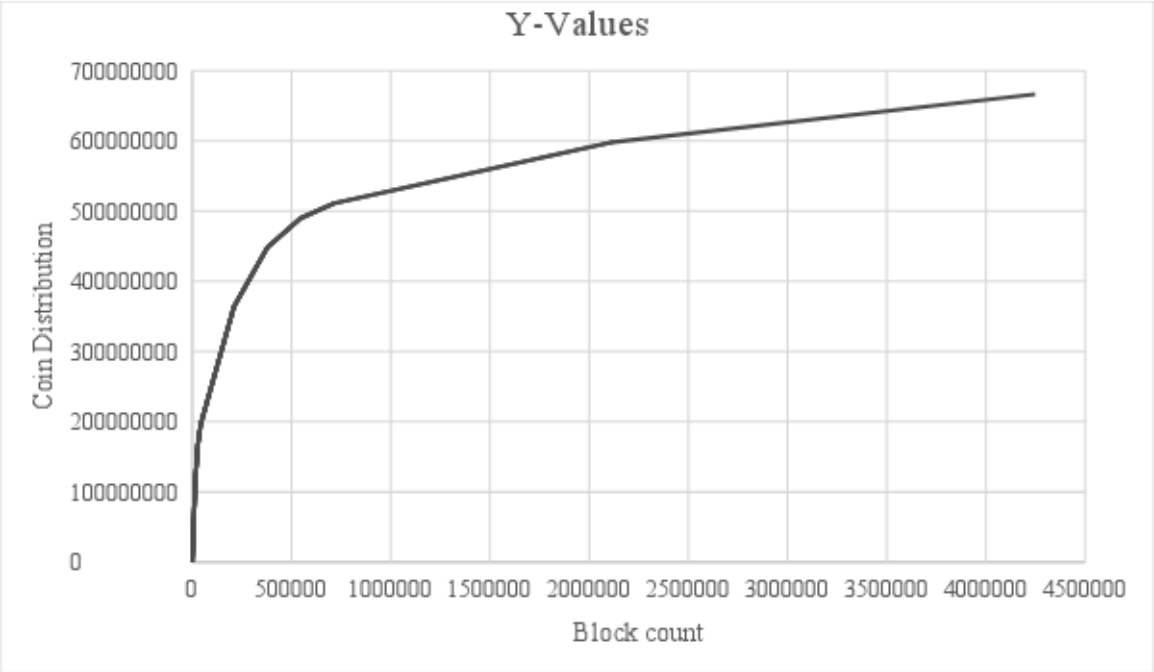
[6] "CryptoRekt", (2017) *Verge Blackpaper* Retrieved from https://github.com/vergecurrency/Verge-Blackpaper/blob/master/Verge-Anonymity-Centric-CryptoCurrency.pdf

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

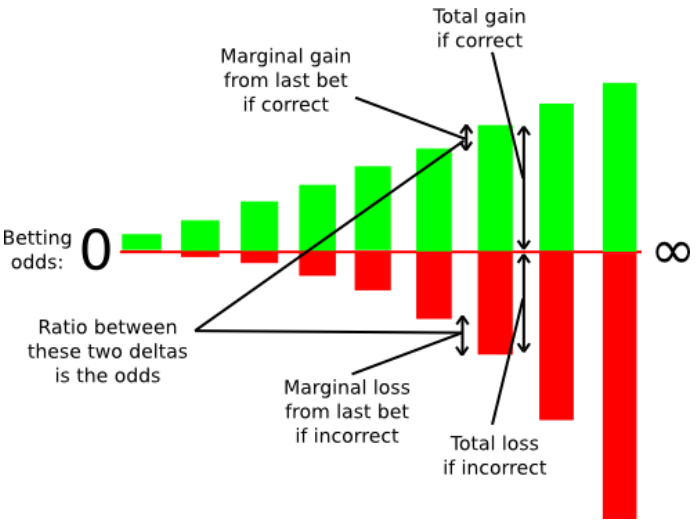
[8] Tor, (n.d.) *Tor: The Second-Generation Onion Router Retrieved* from https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf

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

Figures



Şekil 1. Bloklar üzerindeki madeni para dağılımının grafiği (x)



Şekil 2. PoS Casper için kayıp veya kazanç grafiği

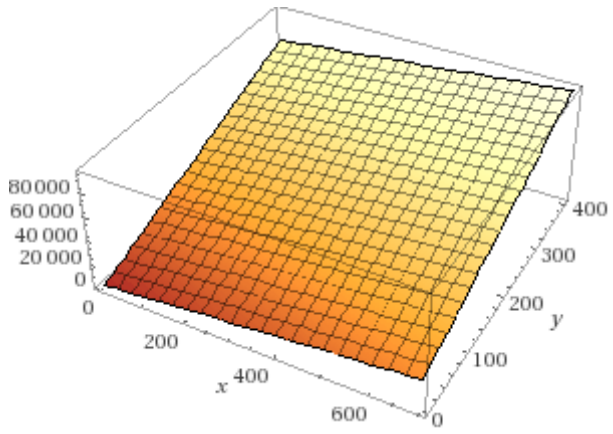


Figure 3. 3D plot of inputs(y) and output(x) where z is the size in kBThe worst and best case are always around Z=500000. This assumes a bitcoin type of scenario where blocks need to be filled to process as many transactions as possible.