SHIELD white paper V1.0.1

Pagpapatunay sa kinabukasan ng blockchain

Ang Samahan ng SHIELD

ShieldCoin@protonmail.com

https://ShieldCurrency.com

Patungkol

Ang SHIELD protocol ay papalit sa ECDS kasama ng Lamport, Winternitz or BLISS na akda, na mag papagana sa addresses para maging “katibayang-quantum”. Ang SHIELD ay makukuha ang sariling pag supportang pagbubuo, na magpapagana sa pagpapatuloy na pagbuo ng SHIELD protocol at iba pang proyekto na sasabihin dito sa artikulo. Ang SHIELD ay gagamit ng kakaibang PoS na pamamalakad (PoS Boo) kasama ang tulong ng Masternodes. Etong masternodes ay gagamitin din para mapagana ang iba pang nilalaman gaya ng Privatet Send at InstantSend.

Mga Kataga: SHIELD, katibayang-quantum, masternodes, cryptocurrency, blockchain, privacy

1 – Pauna

Ang SHIELD ay cryptocurrency na ibinase sa blockchain ng teknolohiya ng Satoshi Nakamoto (Kung saan siya ay naglabas ng white paper [1] noong 2009) Yuon ay nag simulang lumaki at gumanda simula noon. Sa kaunting panahon ngayon, ang teknolohiya ng blockchain ay naging mabilisang natanggap, ngunit may mga iba pang problema na pumipigal sa teknolohiyang ito para bumalik sa pagpunta sa pangunahing palatuntunin. Ang SHIELD ay naghahanap ng paraan para ma-solba ang maraming problema.

2 – Problemang i-solba

Ang Bitcoin ay talagang makabago ng ito ay inilatag, at ang mabuting bahagi ng nagawa ni Satoshi ay patuloy paring ginagamit ng karamihan sa mga pangunahing cryptocurrency ngayon. Isa sa mga nabahagi nito ay ang block mining, pero mas tinutukoy , block mining ng isang algoritmo. Ito ay naging daan para makabuo ng espesyal na kagamitan (ASICs) na kayang mag hash ng isang algoritmo sobrang epektibo na kayang alisin ang GPU mining. . Isang sa nakapag pababa ng desisyon na kanyang ginawa, na meron mga bagong cryptocurrencies na nakapag isip na hindi tama ang mga ngyari sa mining. Mababasa mo ang tungkol ditto sa seksyon 3, *Maraming Algoritmo mining sa PoW.*

Quantum kompyuter ay nagiging mas lalong sopistikadong at ito ay papalapit na ng papalapit na lumabasa na sa publiko. Sakaling ito man ay para sa tagapag-saliksik, gobyerno, negosyo okaya ay sa pangkalahatang publiko, di maglalaon ay makikita natin ang quantum kompyuting na maging pwede na sa mayayamang grupo at indibidual na may sariling interest. Kahit na ito ay napakatindi na bagong teknolohiya na pweding mas mapaganda an gating buhay, marami rin magagandang dahilan para magkaroon ng malasakit dito sa pagbubuo. Isa na dito ay ang makabagong cryptography na pwede magaling na mabuksan ng quantum computers. Para sa maraming cryptocurrencies, ito ay pwedeng magdulot ng sirang blockchain. Paano natin ma-resolba ang problemang ito ay nabangit sa seksyon 4, *Pagayaw sa Quantum.*

Ang malalaking korporasyon gaya ng Facebook o Google ay nagiging mahusay sa pag alam kung sino ka at ano ang iyong gusto. Kahit na ito ay di (kasalukuyan) masyadong kailangan, nangangahulogan ito na namumuhay tayo sa mundo kung saan ang negosyo ay manunuod sa atin;hindi man ito ganoon kasama, ngunit hindi ba iyon maganda tignan. Marami diyan na

currencies ang sinasabi papanatilihin nilang walang pag kakilanlan ang kanilang mga gumagamit. Na mag papanatili sa mga korporasyon at gobyerno na makayanan bantayan ang nakagawiang pag gastos. Ang problem sa ibang mga coin na ito ay hindi talaga gaano ka epektibo gaya ng kanilang sinasabi, Nangangahulugan ito na ang kanilang kakayahan at

katotohanan ay mababa na mag karoon ng kabuluhan. Marami pa tayong pag uusapan tungkol ditto, kung paano naming maitatago ang walang pag kilanlan ng mga gagamit nito sa seksyon 5, *Pribadong Nilalaman*

Ang ibang altcoins ay meron talagang napakalupit na pagdadaanan; ang iba ay halos meron magagaling na talentadong taga-gawa. Ngunit pag walang pondo, ito ay maaring hindi sapat para matustusan ang coin. Kung ang taga-gawa ay hindi makakakita ng ilang maayos na kabuhayan galling sa proyekto, ito ay maaring maging mahirap na paraan para matrabaho ng buong oras. Hindi naming ito gustong mangyari kaya kami ay nag plano ng paglalatag ng ibang nilalaman sa SHIELD (at ibang platarporma na pumapaloob sa SHIELD) na makakatulong sa amin sa pag pondo. Maari mo itong mabasa pa tungkol sa solusyon in seksyon 6, *Pondohan.*

Isa pang problema sa Bitcoin at iba pang currencies ito ay dapat pang minahin ng mga minero gamit ang malalakas sa kuryenteng kagamitan upang magawa ang coin minting at kompirmasyon sa transakyson. Ito ay talagang makabago nung mga panahong iyon at gumagana ng maayos, ngunit ang pamilihan at kapaligirang gastusin sa pagpapatuloy ng blockchain (na meron lang Proof of Work para sa network consensus) ay talagang mataas. Ito ay na i-solba sa aming Proof of Stake na pamamalakad, na maarin mong mabasa ang tungkol ditto sa seksyon 9, *PoS Boo.*

3 – Ibat-ibang-Algoritmo ng mining para sa PoW

Aming pinagtibay ang pagbibigay na pantay pantay na pagbabahagi ng pabuya at sa pagiwas hanggang 51%[citation needed] atake sa ibat-ibang PoW algoritmo. Ibat-ibang-Algoritmo mining ay isang paraan para payagan ang ibat ibang klase ng unit ng proseso para maka mine para sa blocks; ang aming pag gawa ay pinapagamit ang ibat ibang kagamitan, kasama ang parehas na GPUs and ASICs, para maka mine ng sama-sama sa SHIELD blockchain. Ang pagbabahagi ng pabuya sa kada algoritmo ay halos lageng parehas at pantay-pantay sa kabuuan ng pabuya kada oras. Halimbawa, kahit may isang algoritmo na meron 300GH/s at ang isa naman ay 50MH/s, sila parin ay parehas makakakuha ng parehas na bilang ng coins s isang oras. Pagtitibayin nito ang 51% pag iwas sa pag atake dahil sa pamamagitan ng blocks ay binahagi; bawat algoritmo ay

sumusunod sa kani-kanilang sariling “iskedyul”, nangangahulugan ito na kailangan mo ng 51% ng hashing rate para sa bawat algoritmo para maayos ang pag gawa sa bawat atake. Ang importanteng nilalaman ng sistemang ito ay ang pag sunod kung paano nag adjust ang bawat algoritmo ng hiwa-hiwalay.

Ang pag adjust sa difficulty ay sinasaayos ng “Dark Gravity Wave v3”na pamamalakad, na ginawa para sa Dash ngunit ito ay ginagamit ng ilan din ibang cryptocurrencies. Sinasaayos nito ang pagtaas ng network-hash at pagbagsak ng network-hash ng mas maayos sa kinagawian na pag kalkula sa difficulty, at ginagawa nitong mahirap para sa nakakadudang minero na mabilisan nag mine ng coins ng hindi pino-proseso ang transakyson.

4 – Pagayaw sa Quantum

Ang SHIELD protocol ay ang katibayang-quantum ng transaksyon/nagtuturo sa ibang addresses. Ibang cryptocurrencies ay kalimitang hindi katibayang-quantum dahil sa pag gamit nila ng ECDS (na mahina sa Shor's Algoritmo [9], gumagana sa pag gamit ng quantum kompyuter). Kami ay may nag plano na gagamit ng Akda Lamport, o iba pang kagaya na pamamaraan, para baguhin yun. Lamport digital na akda ay base sa ginagaawa ng hash, at ang ginagawa ng hash ay hindi mahina sa Shor's Algoritmo. Sa ECDS, kapag ikaw ay may binigay na transakyon, ang iyong address ay nagiging mahina dahil ang iyong ECDS na pwede pasukin ay makikita. Ang pagpasok sa akda ay pinapayagan ang hindi autorisadong pag gamit sa pondo na nakakabit sa address na iyon. Ang Hashes ay hindi mahina sa Shor's Algoritmo, bagkus hash-based digital akda ay pinapaganda ang seguridad ng apektadong addresses laban sa mga nakakatakot nakakatakot na banta.

5 – Pribadong Nilalaman

Ang SHIELD’s Project Perdu ay isa sa dumaan sa kamakailang pagbabago ng plano. Kami ay orihinal na nag plano na mag latag ng VergeCurrency's Wraith protocol[9] , ngunit sa relatibong mababa na espisipikasyon, sa halip nito kami ay nag desisyon na I-opt ang PrivateSend (ginawa ng Dash); ito ay gumagana ng mas mahusay para sa atin bilang kailangan maisakatuparan ang masternodes. Ang pag babagong ito ay opsyonal na mapabuti ang bilis sa pamamagitan ng InstantSend. Bagaman ang pag papabuti, PrivateSend hindi pa rin ginagawa ang mga transaksyon na ganap na pribado, kaya nga Zerocoin or zk-SNARKs / zk-STARKs ay isinasaalang alang.

Mag sasaliksik pa kami ng higit pang detalye ukol dito ng di mag tatagal ito ay maisakatuparan

Para sa pisikal na privacy, gagamit kami ng Tor/I2P wallets/nodes na nag tatago ng end-user’s IP address at lokasyon.

6 – Pag Pondo

Ang sariling pag-popondo ng SHIELD ay maaring gumana sa pamamagitan ng paggamit ng porsyento ng masternode at mining block. Ito ay pinakamaliit lamang na masternode dahil gusto lamang naming mapanatili ang koponan na naka ere, at ang iba ay para sa merkado.

Magkakaroon din kami ng panggagalingan ng suporta sa labas na magmumula sa pag-gawa at pagsali ng mga platforms na tutulungan ang parehong taga-gawa at gagamit. Meron kami, halimbawa, nakatanggap ng maraming donasyon mula sa komunidad na kung saan mapapasa ang ating proyekto, na kung saan sila rin ay nakakakuha ng suporta mula sa iba'I ibang mining pools. Umaasa kami na aasenso an gating proyekto ng walang hanggan. Wala kaming ICO o premine gaya ng madami sa aming ka kumpetensya sa kasalakuyan; naniniwala kami na ang may matibay na komunidad ay mas magandang daan upang lumago.

7 – Seguridad ng Aplikasyon

Ang shield ay patungkol lahat sa seguridad. Sinusubukan naming mapabuti sa ganito kasama ng nabanggit na na quantum proofing, ngunit nakakita kami ng takbo sa karamihan ng mahinang aplikasyon, na nakikipag-ugnayan sa blockchain, at napansin naming ang mga butas karamihan ay nasa gumagamit nito. Naiisip naming ito marahil kung bakit kailangan naming gumawa ng maraming orihinal na produktong subok, ito ay gagawin gamit ang open-soource community, kukuha ng pen testers upang subukin ito ng kada indibidwal at sa pamamagitan na din ng aming koponan ng tagagawa na suriin ang mga code kasama ang pag-kilala kada pagsagawa bago ituloy (hindi lang para sa opisyal na updates). Mula sa aming karanasan gamit ang aming Discord bot, naobserbahan naming-na kung may seguridad sa backend- ang link sa frontend ay isa sa mga pinaka-importanteng bagay sa ligtas na aplikasyon.

8 – Pagsasama

Ang pag-sama ng teknolohiya sa bago o kasalukuyang platforms ay maaring maging maimpluwensya sa pagpapasya ng kanyang kagamitan at kaangkupan. Gagamit kami ng

maraming sikat at libreng platforms, gaya ng Discord at Twitter,gagamitin upang maging daan na pag-husayin ang karanasan ng gagamit. Gagawin namin ito sa pamamagitan ng pag-gawa ng

Plug-ins at bots para sa platfotms gaya ng Discord, Twitter, Facebook at madami pa. ang pagaanib na ito ay makakapag-bigay sayo ng abilidad na ipadala ang SHIELD sa isang tao nahindi na kailangan tanungin pa sa kanila ang kanilang wallet address. Ang pag-aanib na ito ay maaring isama ang wallet sa mga platforms.- sa pamamagitaan nito, hindi mo na kailangan ng dedikadong wallet sa iyong PC upang magamit ang SHIELD. Ang pag-sasama ay pagkuha din ng mas madaming kaso para sa pampublikong paggamit. Sa madaling sabi, ang kumbinasyon ng networking, ay importanteng parte ng pag-laki ng aming sakop na madla at pag-gamit. Kaya, kokontakin namin ang maraming negosyong kaugnay upang madagdagan ang mga nabanggit na kadahilanan. Magagawa ito upang magkaroon ng katatagan sa aming presyo at magkaroon din kami ng aplikasyon.

9 – PoS Boo

SHIELD Boo ay an gaming sariling Pos scheme base sa Pos Casper. Ang Casper Scheme ay pinabuti ng POSv3 na may intoduksyon ng mapanganib na kadahilanan para sa malisosyong mananaya. Ang sistema ay maunlad sa pamamagitan ng kahirapan sa pagsagawa ng mga atake gaya ng 51% atake: kinakailangan ng mas maraming minted coins at maari mo din harapin ang panganib ng pagkawala nila kapag naglunsad ng ganung atake. Ang kawakasan ay malalaman sa pagtataya at mga mapanganib na kadahilanan., kanya nga maaring mahirap na mag lunsad ng atakeng matagumpay, kahit may 51% sirkulasyon (Figure 2) ang sitwasyon kung saan maaring sobrang mapanganib para sa Coin gaya ng Bitcoin.

Sa iba pang problema, Pos Casper/Boo pag-resolba ay transaksyon na patago. Sa Pow, ang block miner ay maaring mamili na wag i-mine ang block na may tiyak na address, dahil doon itinatago ang address mula sa network. S a kadahilanang ang block creators ay pinipili at ang mga nagpapatunay ay mula sa iba't ibang bahagi ng mundo, magiging mahirap na maitago ang address sa network (na may karagdagang bonus na kapag sinubukan pwersahin ang network, mas malaki ang tsansa na mawawala sayo iyong taya.)

10 – Pag-aaral sa Hinaharap

Tulad ng iyong napansin sa-halimbawa-Seksiyon 5, tinatalakay namin ang ilang posibleng mga tampok / pagtutukoy na hindi tinatapos. Ang ilan sa mga tampok mula sa roadmap ay nawawala pati na rin, tulad ng "sharding" at "smart contracts". Ito ay dahil maraming SHIELD ang nasa ilalim pa rin mabigat na pag-unlad at maingat na konsiderasyon I-update namin ang whitepaper na ito o gumawa ng bago depende sa kung ano ang babaguhin namin sa hinaharap. Hindi ito ang kawakasan ng plano sa pagbuo pa ng SHIELD . Karagdagan pa, ang whitepaper na ito ay magkakaroon maramihang mga pagbabago na nagpapabuti sa approachability, pagiging madaling mabasa, at nag-aalok ng mas maraming detalye mga paksa na nangangailangan nito.

11 – Pangunahing Espesipikasyon

Note: Kasama na sa mga espesipikasyon na ito ang mga Paplanuhin pa
Aming gagamitin ang mga sumusunod na espesipikasyon para sa pangunahin ng SHIELD:

Paksa	Espesipikasyon
Oras ng Block	45 segundo; 240 kumpirmasyon para mag mature; SwiftTX/InstantSend
Block	500k/block
Pabuya sa block	Tignan ang Figure 1

Transaksyon/block	Pinaka-masamang lagay[1]:2777 tx/block Mabuting lagay:14701 tx/block
Transaksyon/segundo	Pinaka-masamang lagay:61 tx/block Mabuting lagay:327 tx/block
Akda	ECDSA na meron optional Lamport/Winternitz/BLISS[2] akda
Minting	PoW gamit ang x17, blake2s, lyra2rev2, myriad-groestl, and scrypt. PoS Boo using Quark[3] hash and Slasher scheme
Pinaka-mababang bayad sa Transaksyon	0.05 XSH kada kB
Pribadong nilalaman	Tor/I2P nodes, PrivateSend, Zerocoin[4]

Batayan

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

---

[1] ang Mabuti/Masamang lagay ay makikita sa dami ng inputs/outputs sa block dahil ang inputs ay "heavier' kay sa outputs

[2] Malalaman pa

[3] Hindi kapani-paniwala

[4] Hindi kapani-paniwala

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

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

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

[5] cs.jhu.edu, (n.d.) *Zerocoin* Kinuha sa

http://spar.isi.jhu.edu/~mgreen/ZerocoinOakland.pdf

[6] “CryptoRekt”, (2017) *Verge Blackpaper* Kinuha sa

https://github.com/vergecurrency/Verge-Blackpaper/blob/master/Verge-Anonymity-Centric-CryptoCurrency.pdf

[7] I2P, (n.d.) *I2P tech intro* Kinuha sa

https://geti2p.net/en/docs/how/tech-intro

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

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

Figures

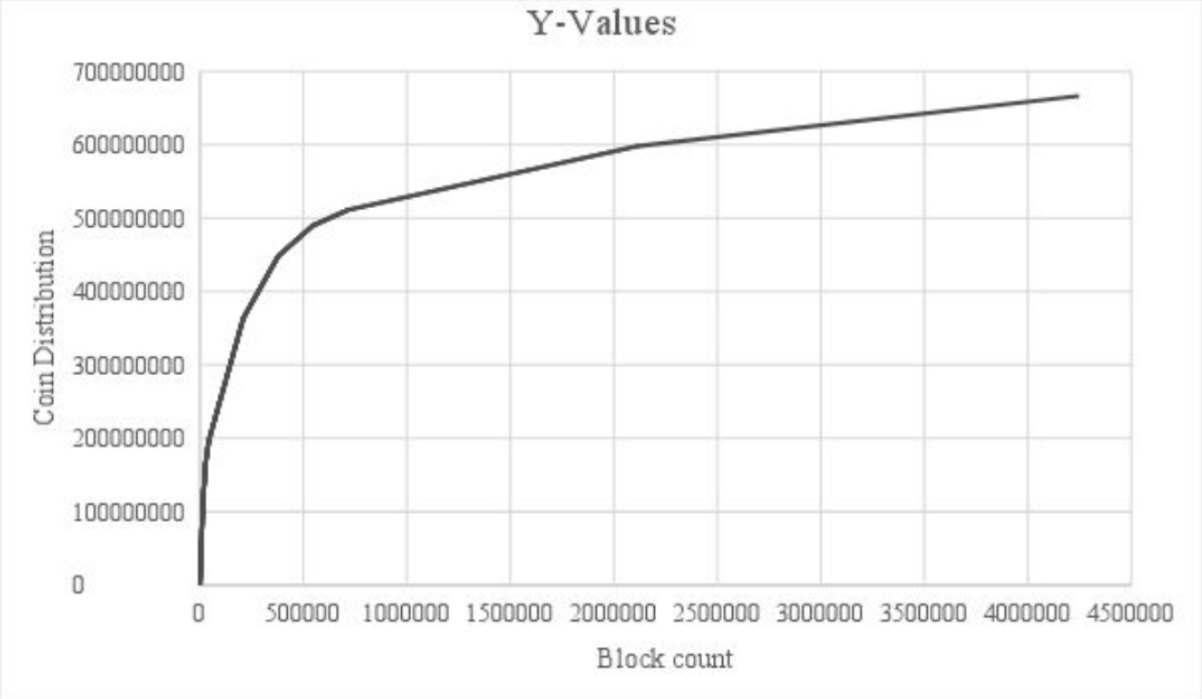

Figure 1 . Graph ng pagbabahagi ng coin (y) over blocks (x)

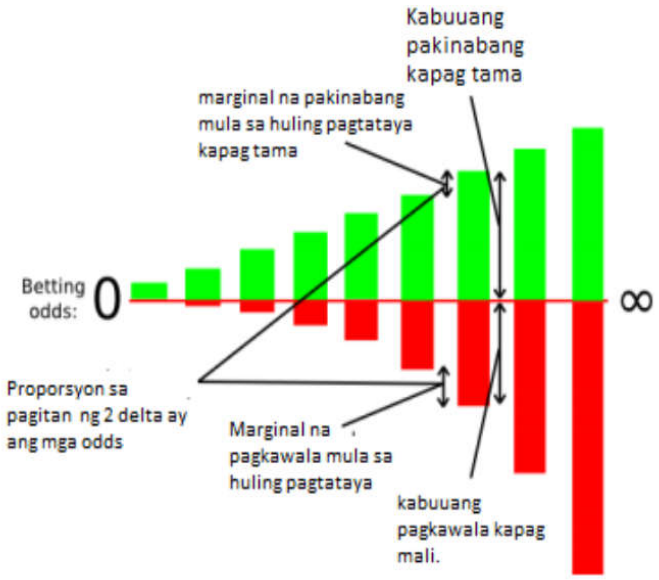

Figure 2. Talangaguhit ng pagkawala o pakinabang para sa sistema ng pagtataya ng PoS Casper

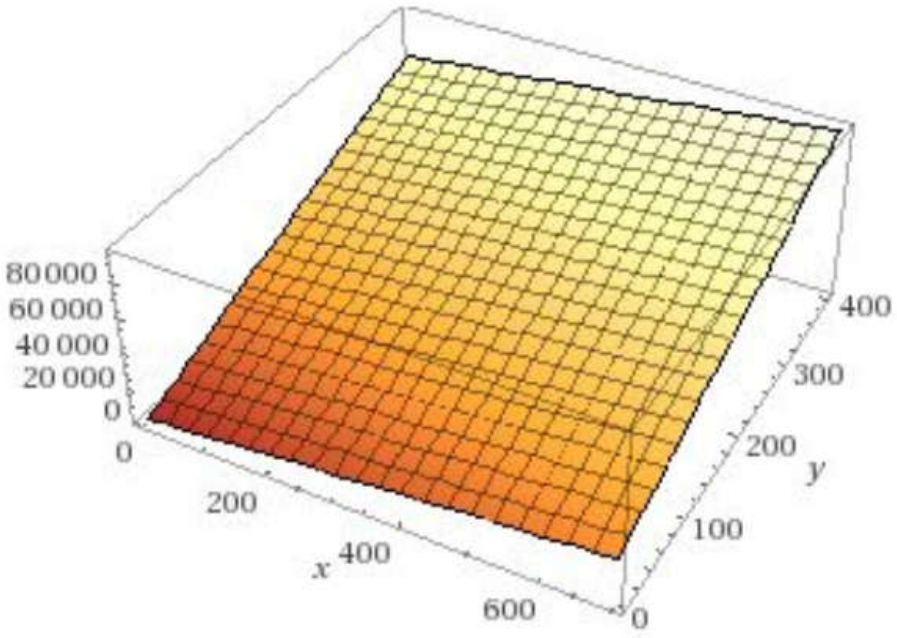

Figure 3. 3D plot of inputs(y) and output(x) Na kung saan ang Z ay kasukat ng kb. Ang pinakamasama at pinakamaganda naman ay nasa Z=50000. Ipagpalagay na ang tipo ng bitcoin na sitwasyon ay kung saan ang blocks na kailangan ma punan para ma-proseso ang kahit na anong dami ng transakyon hangga't maari.