Abstraksi

Shield protocol akan menggantikan ECDS dengan Lamport, Winternitz atau BLISS signatures, yang mana akan memungkinkan address menjadi “quantum-proof”. SHIELD dapat mendukung pengembangan siklusnya secara mandiri., yang mana pada akhirnya dapat terus menjaga keberlangsungan pengembangan protocol SHIELD dan projek-projek lainnya yang akan digambarkan dalam tulisan ini. SHIELD nantinya akan menggunakan skema PoS custom (PoS Boo) melalui bantuan Masternode. Masternode ini tentunya akan memungkinkan fitur PrivateSend dan InstanSend.

Kata kunci: SHIELD, quantum-proof, masternodes, cryptocurrency, blockchain, privacy

1.–Perkenalan

SHIELD adalah cryptocurrency yang berbasiskan pada teknologi blockchain oleh Satoshi Nakamoto (yang ia release dalam whitepaper pada 2009 lalu) yang terus tumbuh dan berkembang sejak pertama kali. Dalam beberapa tahun belakangan ini, teknologi blockchain secara pesat terus diadaptasi/digunakan, namun tentunya masih banyak persoalan yang menyebabkan teknologi ini pada akhirnya akan kembali pada hal mainstream. SHIELD hadir berupaya untuk menjawab banyak persoalan ini.

2. –Persoalan yang harus di atasi

Bitcoin sangatlah inovatif saat kemudian diterapkan, dan hal terbaik yang dibuat oleh satoshi ketika itu masih digunakan sebagai Core/inti dari banyak Cryptocurrencies saat ini. Salah satu kontribusinya adalah Block Mining, namun secara khususnya adalah block mining dengan algoritma tunggal. Ini mendorong pada pengembangan hardware khusus (ASICs) yang hanya dapat menambang dengan satu algoritma secara efektif sehingga membuat kinerja render GPU menjadi terlihat lemah. Namun ini menajdi salah satu kelemahan yang dia buat, dimana

cryptocurrencies yang hadir lebih baru menyadari, faktanya ini tidaklah adil bagi per mining an. Anda dapat membacanya pada bagian 3, *Multi Algorithm mining for PoW*.

Computer Quantum kini semakin terlihat canggih dan semakin dekat untuk dapat digunakan secara umum. Entah itu untuk peneliti, pemerintah, bisnis atau khalayak umum, akhirnya kita dapat melihat komputasi kuantum tersedia bagi kelompok kelas atas dan individu dengan ketertarikannya masing-masing. Bagaimanapun ini adalah teknologi baru yang luar biasa yang dapat meningkatkan hidup kita, ada juga beberapa alasan yang perlu menjadi perhatian utama dalam pengembangan hal ini. Salah satunya adalah bahwa kriptografi modern dapat dengan mudah diretas oleh computer kuantum masa depan. Bagi banyak cryptocurrencies ini berarti bobolnya sebuah blockchain. Lalu, bagaimana cara kita mengatasi masalah ini akan dibahas pada bagian 4, *Quantum Resistance*.

Perusahaan besar seperti Facebook atau Google semakin handal dalam mengetahui siapa anda dan apa yang anda inginkan. Walaupun mungkin (saat ini) hal ini tidak perlu di khawatirkan, karena ini akan menjadikan hidup kita saat ini dan segala urusan kita diawasi. Namun tidak akan seburuk itu, tapi bukanlah hal yang hebat juga. Banyak sekali currencies yang menyatakan untuk tetap menjadikan pengguna mereka tetap *Anonymous*, yang akan mencegah perusahaan besar dan pemerintah dalam melacak kebiasaan anda dalam menghabiskan dana (belanja). Namun masalahnya dengan beberapa dari jenis koin ini adalah bahwa mereka tidak seefektif seperti yang mereka klaim, yang berarti skalabilitas dan penerapannya sangatlah rendah dan hamper tidak mungkin. Kita akan berbicara banyak mengenai bagaimana cara kita menjaga pengguna kita tetaplah *Anonymous* pada bagian 5, *Privacy Features*.

Beberapa altcoin memiliki roadmap yang sangat menjanjikan; beberapa bahkan memiliki developers yang bertalenta luar biasa. Namun, tanpa pendanaan, hamper tidak mungkin untuk menjaga keberlangsungan hidup koin tersebut. Jika developer tidak menemukan suatu pemasukan dana dari project yang dia buat, ini akan menambah sulit dirinya untuk bekerja secara full time dalam mengelolanya. Kami tidak ingin ini terjadi maka itu kami berencana mengimplementasikan beberapa fitur pada SHIELD (dan beberapa platform yang berjalan pada

SHIELD) yang dapat membantu kami mengatasi masalah pendanaan. Anda dapat membaca terkait solusi ini pada bagian 6, *Funding*.

Masalah lainnya dengan Bitcoin dan sebagian besar currencies adalah bahwa *Miner* harus menambang dengan konsumsi power pada alat (hardware) untuk mendapatkan koin dan konfirmasi saat transaksi. Ini sangatlah inovatif untuk saat ini dan ini masih terlihat baik-baik saja, namun secara nilai ekonomis dan lingkungan untuk dapat menjaga keberlangsungan sebuah Blockchain (yang hanya mengandalkan *Proof of Work* untuk consensus jaringan) ini sangatlah besar (boros). Hal ini dapat diatasi dengan skema *Proof o Stake* milik kami, anda dapat membacanya lebih lanjut pada bagian 9, *PoS Boo*

3 –Multi Algoritma dalam menambang PoW

Kami meningkatkan distribusi dalam reward dalam jumlah yang sama dan pada tingkat resistensi hingga 51% (kutipan dibutuhkan). Menambang dengan multi algoritma adalah cara untuk memungkinkan banyak jenis pengolahan untuk menambang block, pendekatan yang kami lakukan adalah memungkinkan banyak perangkat yang berbeda bai itu GPU dan Asics untuk dapat menambang bersama pada SHIELD Blockchain. Disribusi dari rewards tiap algoritma hampir memiliki proporsi yang sama dari total reward waktu ke waktu. Sebagai contoh, andaikan dalam satu algoritma memiliki 300gh/s dan yang lainnya hanya 50 mh/s, mereka akan tetap menerima jumlah koin yang sama dalam waktu satu jam. Ini meningkatkan system keamanan dalam pencegahan terjadinya serangan atas system sebesar 51% saat block didistribusikan; setiap algoritma memiliki "jadwal" mereka masing-masing yang berarti anda membutuhkan 51% dari jumlah hashing untuk setiap algoritma agar bisa melakukan "hack" atas system. Aspek yang terpenting dalam system ini adalah bagaimana kesulitan (diff) dari setiap algoritma disesuaikan secara terpisah.

Penyesuaian tingkat kesulitan (diff) dikelola dengan skema "Dark Gravity Wave v3" yang dikembangkan oleh Dash namun telah diterapkan juga di berbagai cryptocurrencies yang lainnya.

4 –Quantum resistance

Protocol SHIELD adalah Quantum-Proof dari transaksi yang ditujukan pada alamat tertentu. Cryptocurrencies lainnya seringkali bukanlah Quantum-Proof yang sebenarnya karena penggunaan ECDS mereka (yang mana rentan terhadap Shor's Algorithm, [9] yang dapat dilakukan oleh computer Quantum)

Kami berencana menggunakan Lamport Signatures, atau skema sejenisnya untuk dapat mengatasi itu. Lamport Digital Signatures berfungsi berdasarkan *hash*, dan fungsi *hash* ini tidak rentan terhadap algoritma Shor. Dengan ECDS, setiap kali anda melakukan transaksi, alamat (address) anda akan rentan karena anda bisa melakukan crack terhadap ECDS signature anda karena ia terbuka (exposed). Cracking tanda tangan (signature) semacam itu akan memungkinkan seseorang mengakses secara tidak sah ke dana/ saldo yang terkait dengan alamat terkait. Berbeda dengan *Hash*, ia tidak rentan terhadap algoritma Shor, jad *hash* berbasis Signatures Digital ini meningkatkan keamanan alamat (address) yang akan terkena dampak atas ancaman semacam ini.

5 –Fitur Privasi

Project Perdu SHIELD adalah salah satu yang baru saja mengalami perubahan rencana. Pada awalnya kami berencana untuk menerapkan protocol *Wraith VergeCurrency*[6], namun karena spesifikasi yang relative rendah, kami telah memutuskan untuk memilih *Private Send* (dikembangkan oleh Dash) sebagai gantinya, ini bekerja lebih baik bagi kita karena kita akan

menuju penerapan Masternodes. Perubahan ini akan secara opsional meningkatkan kecepatan transaksi via *InstSsend*. Bagaimanapun ini adalah sebuah perbaikan, *PrivateSend* tetap tidak melakukan transaksi secara penuh *Private*, itu juga sebabnya Zerocoin[5] atau zk-SNARKs[4]/ zk-STARKs masih dalam pertimbangan.

Kita akan menuju pembahasan mendetail mengenai ini dalam kuartal ini saat hal ini diterapkan.

Untuk Privasi fisik, kita akan menggunakan Tor[8]/I2P[7] Wallets/Nodes lah yang akan menyembunyikan alamat IP address dan lokasi pengguna.

6 –Pendanaan

Pendanaan SHIELD secara mandiri dapat dilakukan dengan menggunakan persentase blok masternode dan reward dari hasil menambang. Persentase ini tentunya sangatlah kecil karena ini dibutuhkan hanya untuk agar tim tetap berjalan untuk bekerja dan selebihnya digunakan untuk pemasaran. Kami juga akan memiliki beberapa sumber dukungan external yang diperoleh dengan membuat dan menggabungkan platform yang dapat membantu kedua pihak baik itu developer maupun pengguna/user.

7 -Application Seccurity

SHIELD adalah mengenai keamanan. Kami berusaha memperbaiki banyak hal ini dengan hal yang sudah disebutkan dengan *Quantum Proofing*, namun kami telah melihat kecenerungan banyak aplikasi yang rentan, antara lain berinteraksi dengan Blockchain, dan melihat bahwa celah hamper selalu ada pada interfaces pengguna. Kami pikir inilah mengapa kami perlu memiliki banyak produk original kami yang diuji, ini akan dapat dilakukan dengan menggunakan komunitas Open-source, pertemuan para penguji untuk mengujinya secara terpisah, dan meyakinkan bahwa semua team pengembangan kami telah memeriksa

kemungkinan sebuah kode bahkan mengakui setiap commit sebelum di perkenalkan (dan tidak hanya untuk update resmi).

Dari pengalaman kami mengunakan Bot Discord kami, -kami telah mengamati hal itu dengan backend yang aman-, link yang menuju pada fronted adalah salah satu hal terpenting dalam aplikasi yang aman.

8 –Integrasi

Integrasi teknologi baru ke platform baru atau yang sudah ada dapat berpengaruh dalam menentukan kegunaan dan penerapannya. Kami akan menggunakan banyak platform yang populer dan gratis, seperti Discord dan Twitter digunakan sebagai cara untuk meningkatkan pengalaman pengguna. Kami akan melakukan ini dengan mengembangkan plugin dan 'bots' untuk platform seperti Discord, Twitter, Facebook (dan lainnya). Integrasi ini akan memberi Anda kemampuan untuk mengirim SHIELD kepada seseorang tanpa perlu bertanya kepada mereka alamat dompet (wallet address) mereka. Integrasi ini mungkin juga termasuk dompet untuk platform ini, dengan cara ini anda bahkan tidak perlu mendapatkan dompet khusus pada PC Anda untuk menggunakan SHIELD.

Integrasi juga semakin banyak digunakan untuk konsumsi khalayak. Dimana kombinasi dengan jaringan, adalah hal yang terpenting dalam memperluas audiens dan kasus penggunaan kami. Oleh karena itu, kita akan hubungi beberapa bisnis terkait untuk meningkatkan faktor-faktor tersebut. Ini akan menjadikannya berpengaruh kepada stabilitas dalam harga dan kita akan lebih banyak memiliki penerapannya.

9 –PoS Boo

SHIELD Boo adalah skema PoS milik kita sendiri berdasarkan PoS Casper[2]. Skema Casper banyak meningkatkan pada “POSv3”[3] dengan diperkenalkannya faktor resiko bagi staker berbahaya (malicious stakers). Sistemnya sangat progresif dengan cara membuatnya

sangat sulit untuk terjadi serangan seperti serangan 51%; Anda memerlukan sebagian besar dari semua koin yang ditambang/dicetak, dan Anda juga memiliki potensi kehilangannya semua saat meluncurkan serangan seperti itu [2]. Pada akhirnya, hal ini secara utama akan ditentukan oleh faktor risiko dan *Stake*, Karena itulah sangat sulit untuk melakukan serangan dengan sukses bahkan dengan 51% sirkulasi (Gambar 2), situasi yang sangat mengkhawatirkan seharusnya bagi koin seperti bitcoin.

Masalah lain yang dihadapi PoS Casper / Boo adalah dalam menyensor transaksi. Dengan PoW, penambang blok bisa "Memilih" untuk tidak menambang blok yang berisi alamat tertentu, sehingga dapat menyensor alamat dari jaringan. Semenjak pembuat blok dipilih secara acak dan validator bersifat global melalui skema PoS ini, sangatlah sulit untuk menyensor alamat dari jaringan (anda akan dapat bonus tambahan jika Anda mencoba untuk memaksa/force jaringan, justru kemungkinan besar anda hanya akan kehilangan *Stake* anda).

10 –Studi lanjut

Seperti yang sudah Anda perhatikan di misalnya-Bagian 5, kita membahas beberapa kemungkinan fitur / spesifikasi yang belum final. Beberapa fitur dari Roadmap juga dihilangkan, seperti “Sharding” dan “Smart Contracts”. Ini karena banyak bagian dari SHIELD masih dalam pengembangan yang sulit dan memerlukan pertimbangan yang cermat.

Kami akan memperbarui whitepaper ini atau membuat yang baru tergantung pada apa yang kita ubah di masa depan. Ini bukan finalisasi rencana pengembangan SHIELD. Selain itu, makalah ini akan memiliki beberapa revisi yang meningkatkan kemampuan dalam mendekati, mudah dipahami, dan menawarkan lebih banyak detail terkait hal-hal yang dibutuhkan.

11 –Spesifikasi Core

Catatan: spesifikasi ini termasuk rencana di masa depan

Kami akan menggunakan spesifikasi berikut untuk Core dari SHIELD: