BULWARK

CRYPTOCURRENCY

Whitepaper Mata Uang Digital Bulwark

Tim Bulwark Inti:

Eatbatterys (Koordinator Proyek)

Jack (Direktur Pemasaran)

SerfyWerfy (Pengembang Blockchain)

Frogman (Pimpinan Komunikasi)

Patrick (Desain dan Merek)

Stu (Pengembang Ekosistem)

Tim Bulwark Inti

Desember 2017

Kami, Tim Bulwark Inti, mengkonfirmasi bahwa karya yang dipresentasikan di whitepaper ini adalah karya kami sendiri. Informasi yang diturunkan dari sumber lain kami indikasikan dalam penghargaan.

Abstrak

Bulwark (kode: BWK) adalah koin berorientasi komunitas yang lahir dari pengamatan bahwa di bidang koin privasi masternode sering terjadi praktik yang kurang adil. Strategi peluncuran kami yang terencana dan adil memberi peluang pada peserta untuk bergabung dalam proyek yang menjanjikan di tahap kelahiran. Kami menawarkan proposisi nilai yang sederhana tanpa janji muluk: kami memberikan koin privasi yang dapat digunakan kini hingga masa depan dengan memanfaatkan praktik terbaik dari DASH dan PIVX. Tanpa visi fantastis yang sulit tercapai, melainkan koin yang fungsional di atas platform yang fungsional dengan dukungan untuk masa depan. Ini bukan berarti kami tidak akan berinovasi, tapi kami akan memberi bukti bukan janji. Terlalu banyak koin yang beralaskan janji semata – tapi isinya kosong – dan kami tidak berniat menambah jajaran koin yang terlalu banyak janji tapi sedikit bukti nyata. Tanpa melalui ICO, imbalan yang meningkat setelah peluncuran, pratambang yang sedikit, dan alokasi imbalan yang mendukung penambang, para pengadopsi Bulwark akan memperoleh akses lantai dasar ke koin privasi yang menawarkan campuran antara masternode dan teknologi koin privasi terbaik diiringi dengan roadmap pengembangan yang berarti. Masternode akan tersedia, dan fungsional, saat peluncuran dan merupakan bagian fundamental dari visi koin kami untuk menstabilkan sirkulasi, mengamankan jaringan, dan menyediakan layanan penting.

Penghargaan

Bulwark tidak mungkin ada tanpa karya-karya sebelumnya dari tim Bitcoin, Peercoin, Blackcoin, Talkcoin, Dash, dan PIVX. Perangkat lunak sumber terbuka dan para kontributornya terus membuka jalan menuju inovasi-inovasi baru dan menarik. Jika informasi dan pengetahuan bebas dikembangkan di atas pengetahuan sebelumnya, masyarakat secara keseluruhan diuntungkan. Kami berterima kasih kepada para pendahulu kami atas kesempatan yang diberikan untuk dapat berkontribusi di ekosistem yang bertumbuh ini.

Daftar Isi

Bab 1

Pengantar Singkat Mata Uang Digital

1.1 Latar Belakang

Tahun 2009, Satoshi Nakamoto merilis sebuah paper berjudul *Bitcoin: A Peer-to-Peer Electronic Cash System* (Bitcoin: Sistem Uang Tunai Elektronik P2P) yang menjelaskan visi beliau mengenai perdagangan elektronik. Visi Nakamoto berisi tentang sistem mata uang P2P yang didukung oleh bukti-kerja (proof-of-work) berbasis hash. Jaringan Bitcoin akan memberi cap waktu pada transaksi dengan membuat hashnya lalu menambahkannya pada buku besar yang tidak bisa diubah tanpa menghitung ulang hashnya. Simpul jaringan (komputer dalam jaringan) akan memilih rantai transaksi terpanjang sebagai bukti peristiwa yang disaksikan oleh penghitung hash terkuat. Selama ≥ 51% kekuatan hashing dikendalikan oleh simpul-simpul yang tidak ingin menyerang jaringan, rantai yang dihasilkan akan tetap menjadi yang terpanjang (Nakamoto 2009).

1.2 Blok

Setiap blok dalam jaringan diawali dengan header 80 byte berisi salinan hash SHA256 ganda dari header blok sebelumnya, akar merkle (turunan hash ganda SHA256 dari semua hash yang ada di dalam blok), cap waktu bukti-kerja dimulai, target tingkat kesulitan di mana hash header ini harus lebih kecil atau sama dengan nilai tersebut, dan nonce (angka acak) yang menyebabkan penambang menghasilkan hash yang mencapai tingkat kesulitan yang dimaksud. Karena itu, setiap usaha untuk mengutak-atik transaksi manapun dalam blok manapun akan menyebabkan blok ditolak oleh para penambang dalam jaringan (Tim Bitcoin Inti 2017).

1.3 Blockchain

Transaksi dikelompokkan dalam blok dan blok-blok ini ditempatkan secara kronologis menjadi sebuah rantai yang disebut blockchain. Blockchain adalah sejarah berjalan dari seluruh aktivitas di dalam jaringan dan menjadi model konsensus terdistribusi di mana transaksi manapun dapat diverifikasi kapan saja (Crosby et al. 2015).

1.4 Bukti-Kerja (Proof-Of-Work)

Proof-of-work adalah sistem verifikasi di mana penambang harus mendedikasikan sumberdaya berwujud (listrik, perangkat keras) untuk menyelesaikan teka-teki kata probabilistik acak. Seseorang yang berniat jahat dan memasukkan transaksi curang ke dalam blockchain harus menyelesaikan semua proof-of-work sampai pada titik terbaru (Okupski 2016).

Bab 2

Memperkenalkan Bulwark

2.1 Fondasi yang kokoh

Setiap rumah butuh fondasi yang kokoh, Bulwark pun demikian. Bulwark didasarkan dari *PIVX*, yang pada gilirannya didasarkan dari mata uang digital popular *DASH*. Walaupun jika dirunut semua kode pada gilirannya didasarkan dari kode Satoshi Inti original, tiap proyek memilih arah dengan tujuan dan idealisme yang mewakili komunitas masing-masing. Kami akan memperluas, dan menekankan pada, fitur-fitur koin privasi dari platform pendahulu kami dengan mengeksplorasi teknologi baru, sambil membuat set perangkat dan mencari peluang integrasi Bulwark ke platform teknologi saat ini.

2.2 Tim yang berdedikasi pada komunitas

Bagi sebagian proyek, komunitas adalah urutan kesekian. Prioritas pertama Bulwark adalah komunitas. Melalui giveaway, platform diskusi yang hidup, dan kebijakan yang tidak mentoleransi mereka yang mengganggu pendatang baru, Bulwark berusaha menjadi mata uang digital bagi semua kalangan pengguna-akhir. Anggota pengguna kami sudah menyumbangkan skrip-skrip dan panduan yang berguna untuk memperbaiki pengalaman pengguna.

2.3 Adil dan berimbang

Saat artikel ini ditulis, sudah banyak mata uang digital baru yang menggunakan fondasi serupa. Walaupun teknologi fondasinya kuat, kadang-kadang jika diamati spesifikasi dan parameter blockchain yang mereka gunakan mengungkapkan praktik yang kurang adil.

2.4 Kendala dengan praktik pratambang (premine)

2.4.1 Studi Kasus: KoinAnu

Tren yang berkembang di bidang mata uang digital adalah memilih tanggal sembarang di masa depan lalu mendasarkan persentasi pratambang terhadap jumlah koin yang ada dalam sirkulasi pada tanggal tersebut. Mari kita ambil contoh koin fiktif FBC (FooBarBazCoin), sebuah fork dari DASH.

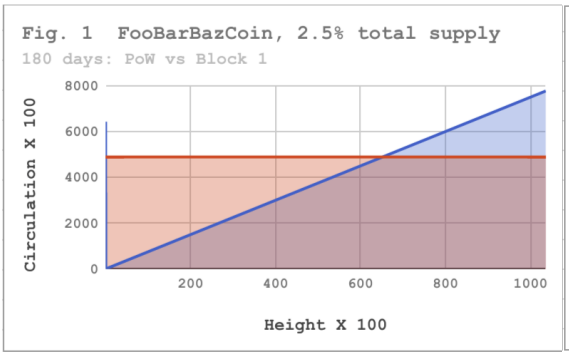
- Imbalan blok: 15
- Waktu blok: 2,5 menit
- Pembagian POW/Masternode: 50/50%
- Algoritma tingkat kesulitan awal: KGW
- Subsidi berkurang 12% per tahun
- Suplai koin maksimum: ~25 juta
- 2,5% pratambang

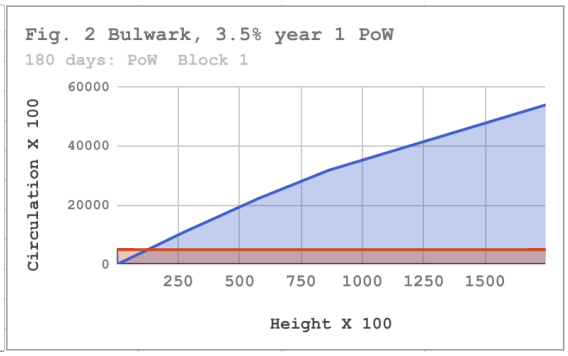
Di contoh ini, jumlah pratambang yang diiklankan 2,5% setara dengan ~643.000 koin (dari ~25 juta) seolah-olah adil jika dilihat sekilas. Tapi, agar imbalan PoW dan Masternode mencapai jumlah koin yang dipegang oleh pengembang, diperlukan sekitar 43.000 blok. Jika target waktu blok adalah 2,5 menit, dibutuhkan sekitar 150 bagi penambang (atau 75 hari totalnya) untuk menghasilkan jumlah koin tersebut. Setelah 75 hari pun, pengembang masih mengendalikan separuh koin yang ada.

2.5 Alternatif yang lebih adil

Tim Bulwark menyadari hal ini, dan memutuskan untuk terbuka di awal. Pratambang kami sebanyak 489.720 koin (3,5%) setara dengan hanya sekitar penambangan PoW 12 hari atau sedikit lebih dari 10 hari total produksi. Semoga ini dapat menenangkan hati komunitas karena, setelah titik tertentu, pasar tidak dapat turun nilainya secara signifikan akibat koin yang dipegang oleh pengembang. Seperti dapat dilihat di gambar-gambar di bawah, keduanya memperlihatkan skenario 180 hari, perbedaannya sangat besar. Kami berharap bahwa dengan terbuka dan jujur di awal prioritas menjadi jelas dan akan bermanfaat bagi komunitas keseluruhan.

2.5.1 Perbandingan kedua pendekatan





2.5.2 Penambangan instan (instamine) dan pendekatan kami

Dash (dahulu Darkcoin) merupakan sebuah studi kasus menarik mengenai kebutuhan akan perlindungan terhadap penambangan instan. Sekitar 10-15% total suplai Dash diciptakan dalam waktu beberapa hari pertama keberadaan koin karena beberapa pengguna yang giat (Wieko 2017). Pendekatan kami terhadap penambangan instan ada dua. Yang pertama, kami menggunakan subsidi lambat di mana imbalan di 960 blok pertama (1 hari) dinaikkan secara linear sampai mencapai nilai penuhnya di mana penambang memperoleh 100% imbalan blok. Sebelumnya, umumnya imbalan blok mulai dari nilai amat kecil lalu tiba-tiba menjadi imbalan penuh di ketinggian blok tertentu; namun hal ini berakibat pool-pool penambang sengaja diserang (DDOS) atau kebanjiran trafik penambang baru. Dengan peningkatan secara perlahan-lahan, insentif mengganggu penambang atau operator pool menjadi tidak menarik.

2.5.3 ICO? Lebih tepatnya IC-NO!

Seperti kita tahu, saat penulisan artikel ini kita setiap harinya dibanjiri oleh penawaran ICO (initial coin offering, penawaran koin perdana). Walaupun ICO dapat berguna dalam kasus-kasus tertentu di dunia mata uang digital, namun seringkali ICO hanya menciptakan kantung-kantung kekayaan yang terkonsentrasi. Mengingat Bulwark menawarkan Masternode maupun, di tahap keduanya, imbalan dari bukti-saham (proof-of-stake), maka konsentrasi kekayaan ini dapat mengakibatkan ayunan pasar yang besar dan membuat sistem tata kelola yang lebih menguntungkan pengadopsi paling awal (dan paling kaya). Walaupun konsentrasi kekayaan tak terhindarkan secara umum, namun kami beranggapan bahwa menjaga pemerataan patut diperjuangkan. Kami meluncurkan koin yang memiliki strategi imbalan blok yang terskala, mekanisme peluncuran yang adil untuk mendorong distribusi Bulwark yang luas di berbagai macam pengguna, yang idealnya bisa menghindari sebagian konsentrasi kekayaan seperti terlihat di proyek-proyek lain.

2.6 Cepat dan fungsional

Dengan waktu blok hanya 90 detik, konsensus masternode dan penguncian transaksi, jadwal pengeluaran yang masuk akal, dan penaruhan (staking) yang ramah lingkungan, Bulwark berharap menjadi mata uang digital yang benar-benar cepat dan fungsional.

Bab 3

Parameter Blockchain Kami

3.1 Spesifikasi Bulwark, Selayang Pandang

Tabel 3.1: Spesifikasi Bulwark, selayang pandang

Spesifikasi	Keterangan
Simbol	BWK
Algoritma	NIST5
Port RPC	52541
Port P2P	52543
Jeda antarblok	90 detik
Algoritma tingkat kesulitan	Dark Gravity Wave v3.0
Ukuran blok	1MB
Maturitas pencetakan/penambangan	67 blok (~100 menit)
Konfirmasi	6 blok (~9 menit)
Sirkulasi (1 tahun)	14.505.720 BWK
Sirkulasi (5 tahun)	27.668.220 BWK
Periode PoW	*nHeight* ≤ 345.600
Periode PoS	*nHeight* ≥ 345.601
Dukungan protokol	IPV4, IPV6, TOR
PoS	Blackcoin v3.0 PoS, Imbalan SeeSaw PIVX

3.2 SlowStart

Permulaan Bulwark yang adil diimplementasi dengan kode seperti ini (kredit: *ZCash*):

```
int64_t nSlowSubsidy = 50 * COIN;

if (nHeight < 960 / 2) {      // Jika ketinggian blok < 480
    nSlowSubsidy /= 960;      // Set nSubsidy ke .05208333
    nSlowSubsidy *= nHeight;  // Kalikan ketinggian blok saat ini
                              // dengan .05208333
} else if (nHeight < 960 {    // mis: Blok 200, BR menjadi 10.41666600
    nSlowSubsidy /= 960;      // Kredit: Tim ZCASH
    nSlowSubsidy *= nHeight;
```

3.3 Dark Gravity Wave 3.0

Dark Gravity Wave digunakan oleh Bulwark sejak awal untuk menarget tingkat kesulitan PoW. Algoritma ini menggunakan rerata bergerak sederhana yang dapat merespon terhadap peningkatan atau penurunan nethash hanya dalam beberapa blok. Ini menghindari efek "blok macet" yang seringkali disebabkan oleh multipool dan mencegah agar jika ada satu orang tunggal yang meningkatkan kemampuan komputasinya, dia tidak serta merta dapat menyelesaikan beberapa blok secara instan.

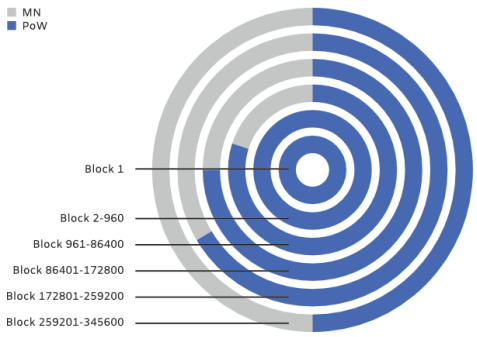
Bab 4

Imbalan Blok

4.1 Imbalan Blok PoW

Tabel: Spesifikasi Imbalan di Periode PoW

Subsidi	Blok	PoW	MN	Sirkulasi
489720	1	100%	NA	489200
~25(avg)	2-960	100%	NA	513150
50,000	961-28800	80%	20%	1953150
50,000	28801-57600	75%	25%	3393150
50,000	57601-86400	66%	33%	4833150
43,750	86401-172800	50%	50%	8613150
37,500	172801-2 59200	50%	50%	11853150
31,250	259201-345600	50%	50%	14553150



Gambar 4.1: Imbalan Blok di Periode PoW

4.2 Imbalan Blok PoS

Tabel 4.2: Spesifikasi Imbalan Blok di Periode PoS

Subsidi	Blok	Anggaran	PoS/Masternode	Catatan
25,000	345601-432000	10%	SeeSaw	Tahun 2
21,875	432001-518400	10%	SeeSaw	Tahun 2
18,750	518401-604800	10%	SeeSaw	Tahun 2
15,625	604801-691200	10%	SeeSaw	Tahun 2
10,250	691201-777600	10%	SeeSaw	Tahun 3
10,938	777601-864000	10%	SeeSaw	Tahun 3
9,3750	864001-950400	10%	SeeSaw	Tahun 3
7,8120	950401-1036800	10%	SeeSaw	Tahun 3
6,2500	1036801-1123200	10%	SeeSaw	Tahun 4
5,4690	1123201-1209600	10%	SeeSaw	Tahun 4
4,6880	1209601-1296000	10%	SeeSaw	Tahun 4
3,9060	1296000-1382400	10%	SeeSaw	Tahun 4
3,1250	1382401-1468800	10%	SeeSaw	Tahun 5
2,7340	1468801-1555200	10%	SeeSaw	Tahun 5
2,3440	1555201-1641600	10%	SeeSaw	Tahun 5
1,9530	1641601-1728000	10%	SeeSaw	Tahun 5
1,6250	1728000+	10%	SeeSaw	Selamanya

Bab 5

Hashing NIST5

5.1 Kenapa NIST5

Algoritma hashing NIST5, yang dipopularkan oleh TalkCoin tahun 2014, dipakai secara tidak terlalu meluas. NIST5 dapat ditambang oleh berbagai perangkat keras konsumen termasuk CPU, dan juga AMD dan GPU NVidia. NIST5 tidak seresistan terhadap ASIC seperti beberapa algoritma memory hard lainnya, namun kami percaya bahwa kekurangan ini dapat diterima karena algoritma ini lebih stabil dan irit konsumsi daya dibandingkan algoritma-algoritma memory hard tersebut. Jika ASIC mulai mendukung NIST5 sebelum periode PoW kami berakhir, maka kami sudah menyiapkan algoritma alternatif sebagai penggantinya. Kami akan mengundang komunitas untuk memungut suara untuk tindakan apa yang diperlukan (jika ada) lalu mengimplementasikannya. Kami berpendapat bahwa periode PoW kami yang singkat dan kesediaan untuk mengganti algoritma akan menghindari memberikan insentif bagi produsen ASIC.

5.2 Lima Finalis (Kompetisi SHA-3 NIST)

Lima algoritma hashing yang digunakan di NIST5 adalah finalis-finalis dalam kompetisi hashing NIST (Chang et al. 2012). Kelima finalis ini adalah (dalam urutan blok yang dihash):

Blake (Aumasson 2013), **Grøstl** (Gauravaram1 et al. 2012), **JH** (Wu 2012), **Keccak** (Bertoni et al. 2012), dan **Skein** (Ferguson et al. 2010).

5.3 Standar baru SHA-3

Keccak akhirnya keluar sebagai pemenang dan berhak dinamai fungsi hashing SHA-3 yang baru, sedangkan keempat finalis lain (walaupun tetap dipandang aman secara kriptografis) mendapat pengurangan poin dari para juri karena isu-isu teknis yang minor. Kami percaya bahwa kombinasi fungsi SHA-3 baru beserta empat finalis lainnya ini memberikan algoritma hashing yang cepat, aman, dan mapan.

5.4 Software Tambang Yang Dapat Digunakan

Saat artikel ini ditulis, ada beberapa opsi yang tersedia bagi penambang:

Nama	Platform	Taut
SGMiner-5.0	OpenCL	GitHub
ccminer-2.2.2	CUDA	GitHub
cpuminer-opt	CPU	GitHub

Bab 6

Set Fitur

6.1 Masternode

Masternode pada dasarnya adalah jaringan komputer terdesentralisasi yang melayani jaringan Bulwark. Masternode melakukan fungsi-fungsi jaringan penting dan menerima sebagian imbalan blok. Masternode memberi manfaat bagi ekosistem Bulwark karena menstabilkan suplai koin, memroses transaksi, dan mengamankan jaringan. Setiap masternode membutuhkan 5.000 BWK dan sedikit pengetahuan teknis untuk beroperasi. Setiap dompet yang berisi 5000 BWK dapat dijadikan masternode.

6.2 Penyamaran / Pencampuran Koin

Bulwark memiliki fitur Penyamaran, didasarkan dari CoinJoin namun dengan berbagai perbaikan dari originalnya, dan dilakukan melalui pencampuran koin secara terdesentralisasi melalui jaringan masternode. Fitur ini memberikan lapisan privasi tambahan bagi transaksi. Meskipun tidak anonim secara sempurna, Penyamaran lewat pencampuran node jauh lebih baik dari transaksi bitcoin standar. Contoh, setiap transaksi bitcoin bersifat transparan. Di Bulwark, seorang aktor jahat harus mengendalikan setidaknya 50% masternode agar dapat memiliki peluang 0,5% untuk mendeanonimkan sebuah transaksi yang dicampur melalui 8 ronde Penyamaran (Kiraly 2017b). Fitur penting ini menyediakan anonimitas level tinggi bagi pengguna BWK yang memilih untuk menyamarkan transaksi mereka.

6.3 SwiftTX

SwiftTX memberi otoritas penguncian dan konsensus untuk transaksi. Saat sebuah transaksi dikirim ke jaringan, sekelompok masternode akan memvalidasi transaksi tersebut. Jika masternode-masternode tersebut mencapai konsensus mengenai validitas transaksi maka

transaksi tersebut akan dikunci untuk dimasukkan ke dalam blockchain nanti, sehingga membuat transaksi menjadi jauh lebih cepat daripada cara konvensional (mis: waktu blok 10 menit bitcoin ditambah beberapa konfirmasi). SwiftTX memungkinkan beberapa transaksi terjadi sebelum blok dengan masukan yang sama ditambang. Sistem ini berdasarkan InstantSend dari Dash (Kiraly 2017a).

6.4 Spork

Jaringan Bulwark menerapkan fork multifase yang disebut "sporking". Ini memungkinkan jaringan BWK mengimplementasi fitur baru sambil meminimalkan terjadinya fork jaringan yang tidak diinginkan selama proses penyebaran fitur. Perubahan di spork dapat disebarkan lewat jaringan lalu diaktifkan/dinonaktifkan seperlunya tanpa mengharuskan software di node diperbarui (strophy 2017). Fitur ini amat berguna dan memungkinkan jaringan bereaksi cepat terhadap kelemahan keamanan.

6.5 TOR & Masternode IPV6

Bulwark mengizinkan pengguna menjalankan node penuh atau masternode dari alamat onion TOR atau IPV6. Kami telah berusaha menambahkan node TOR penuh untuk memperkuat jaringan TOR itu sendiri maupun untuk memperbaiki pengalaman pengguna saat beroperasi di mode TOR-only. Fitur unik Masternode TOR yaitu dapat mengoperasikan masternode sebagai layanan tersembunyi TOR. Node TOR mengizinkan pengguna yang memiliki koneksi Internet stabil untuk mengoperasikan masternode mereka dari jaringan rumah tanpa ada implikasi keamanan memperlihatkan lokasi mereka atau risiko menampakkan jaringan rumah mereka terhadap potensi serangan atau kompromi.

6.6 Pentingnya Komunitas Dan Sistem Tata Kelola

Komunitas Bulwark adalah faktor terpenting untuk kesuksesan proyek jangka panjang, sehingga kemampuan mereka untuk mempengaruhi masa depan koin amat penting. Karena itu, di akhir periode PoW kami berniat mengaktifkan superblok anggaran di jaringan. Superblok ini, dibayarkan bulanan, akan mengizinkan komunitas untuk mengendalikan segala macam aspek pengembangan Bulwark, kehadiran merek, dan urusan komunitas. Dengan menunda aktivasi sistem ini, kami memiliki waktu untuk mengembangkan kerangka yang diperlukan untuk pengalaman pengguna yang positif, dan memaksimalkan imbalan blok yang tersedia bagi penambang dan masternode.

Kami akan memanfaatkan proses multifase dalam membuat dan mengirimkan proposal. Setiap langkah perlu dilakukan. Kegagalan melengkapi langkah yang telah dijelaskan akan berakibat proposal tidak diaktivasi. Garis besar langkah-langkah ini sebagai berikut:

- Mulai dari obrolan di Discord, berbicara dengan sebagian pengguna lama. Ukur tingkat minat dan jika respon positif, berpindah ke fase berikutnya.
- Gunakan beberapa platform media sosial untuk berdiskusi dan memperoleh umpan balik. Perlu diingat bahwa Bulwark memiliki basis pengguna beragam dengan keikutsertaan tata kelola yang berbeda-beda, mencapai kelompok pengguna tertentu mungkin lebih sulit. Catat hasil diskusi dan pastikan dapat diacu nanti di praproposal formal. Semakin banyak yang bisa diacu, semakin baik.
- Terbuka terhadap masukan dari komunitas dan pengembang. Fleksibel dan mau memasukkan ide-ide dari luar terhadap proposal.
- Buat praproposal formal melalui bagian Governance -> Pre-Proposal di situs kami. Sebutkan acuan/rujukan terhadap semua diskusi-diskusi yang telah dilakukan di tahap sebelumnya. Anggap praproposal Anda adalah apa yang akan dikirimkan ke blockchain untuk proses pemungutan suara.
- Setelah langkah-langkah ini selesai, Anda akan mengirim proposal Anda ke blockchain. Akan ada dua biaya, yang pertama saat pengiriman dan yang kedua biaya surat suara yang dibayarkan kepada pengembang untuk mengaktifkan proposal di blockchain. Biaya pengiriman tidak bisa dikembalikan, sementara biaya surat suara hanya perlu dibayar jika proposal disetujui dan diaktifkan.
- Setiap orang berhak memasukkan proposal untuk membayar kembali kedua biaya ini dalam proposal mereka. Pastikan bahwa dalam proposal formal Anda, Anda mencantumkan akan menambah pembayaran biaya ini.
- Pastikan Anda mengontak kembali mereka-mereka yang sudah berdiskusi dengan Anda agar mereka dapat memberikan suara mereka. Agar proposal dapat dibayar, 10% masternode yang memenuhi syarat harus memberikan suara ‘ya’ pada proposal

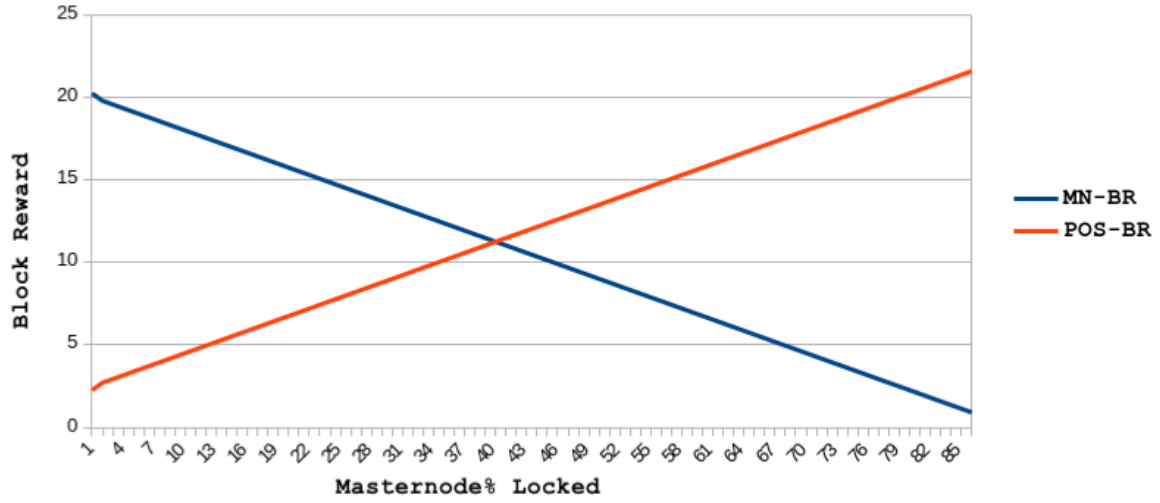
Anda. Proses mendapatkan konsensus 10% ini bisa jauh lebih susah dari yang semula dibayangkan, jadi pastikan kita giat, informatif, dan bersikap hormat dalam mengumpulkan suara.

6.7 Imbalan PoS/Masternode Jungkat-Jungkit (SeeSaw)

Kami memutuskan memakai sistem imbalan SeeSaw yang dipopularkan oleh PIVX (jakiman 2017). Sistem imbalan SeeSaw dimulai dari rasio imbalan blok 9:1 (masternode lebih besar), lalu dengan halus menyetel rasio imbalan untuk penaruhan (staking) dan operator node hingga sekitar 41,5% koin dalam sirkulasi dikunci dalam masternode, di mana pada saat itu imbalan untuk penaruhan berbasis waktu akan memiliki sedikit lebih banyak keuntungan dibandingkan masternode secara koin-per-koin. Alasan kami membuat SeeSaw lebih menguntungkan penaruhan adalah ingin menghindari masalah – seperti volatilitas harga yang signifikan dan likuiditas yang rendah – yang biasanya terjadi di koin di mana persentasi yang terkunci dalam masternode amat tinggi. Strategi ini akan menghindari rasa frustrasi pengguna saat akan mengakses suplai koin dan menjaga relevasi jaringan kami. Karena salah satu tujuan kami adalah menjadi platform perdagangan aninom yang banyak didukung, transaksibilitas menjadi hal yang paling penting bagi mereka yang ingin menerima pembayaran dalam mata uang Bulwark maupun yang ingin menyimpannya.

Fig 3. SeeSaw @ Height 345601 - 432000

(after budget percentage)



Bab 7

Masa Depan

7.1 Kotak Peralatan Bulwark

Koleksi potongan kode, API, pustaka, skrip, dan pengetahuan untuk mendorong lingkungan pengembangan bazaar di mana pengembang yang ingin mencari dukungan tambahan dalam proyek mereka dapat bebas bertukar pengetahuan, informasi, dan kode. Kami percaya bahwa menyediakan kotak peralatan ini bagi pengembang analogis dengan menyediakan perkakas bagi tukang kayu untuk menciptakan proyek-proyek yang menarik dan bagus.

7.2 Privasi dan Perbaikan Software

Kami berkomitmen mengadopsi protokol-protokol baru yang memperbaiki privasi basis pengguna kami. Ada beberapa jalur yang sedang kami evaluasi saat ini dan rencananya akan kami uji dan kembangkan di paruh pertama 2018. Beberapa perbaikan ini di antaranya:

- Jaringan privasi I2P.
- Protokol zerocoin atau alamat tersembunyi (stealth) (Saat kami yakin terhadap tingkat maturitas solusi ini).
- Mensinkronkan kode kami lebih dekat dengan kode bitcoin utama.
- Merampingkan/memperbarui dompet QT.
- Integrasi libtox.

- Virtualisasi/kontainerisasi dompet Bulwark untuk lapisan keamanan tambahan.

7.3 Secure Home Node Bulwark

Kami akan bekerja sama dengan spesialis CAD untuk mendesain perangkat home node Bulwark yang kecil dan self-contained. Pengguna dapat tersambung ke jaringan rumah mereka lalu mengkonfigurasi node ini lewat antarmuka web. Fungsi yang akan kami sediakan sebagai berikut:

- Bagi mereka yang memiliki koneksi internet stabil, masternode (atau node penuh) onion menggunakan layanan TOR tersembunyi.
- Opsi untuk berfungsi sebagai relay untuk memperbaiki jaringan TOR secara keseluruhan.
- VPN dan/atau proksi yang dapat dipakai untuk menjadi router jaringan rumah melewati TOR/I2P.
- Penaruhan Bulwark lewat virtualisasi atau device tambahan.

Untuk menjaga semangat desentralisasi, berkas yang dapat dicetak 3D dan semua kode sumber akan tersedia bagi komunitas untuk dirakit sendiri.

7.4 Perluasan Merek Kami

Kami akan terus memperluas merek kami dan berencana bekerja sama dengan penyedia perangkat keras dan integrasi sistem yang sama-sama memiliki semangat dan idealisme serupa. Dalam lima tahun, kami ingin nama 'Bulwark' sinonim tidak hanya dengan mata uang digital tapi juga privasi, keamanan, dan menghormati privasi pengguna. Tujuan utama Bulwark adalah menyediakan kebebasan memilih melalui privasi.

7.5 Desain dan Visual

Melalui Penelitian dan Pengembangan, kami ingin menciptakan bahasa desain visual bagi Bulwark yang membedakannya dari kompetitor di ranah mata uang digital. Tim desain kami berencana berinovasi dan bereksperimen dengan UI/UX/merek saat ini untuk mencapai keunggulan desain dengan mencari medium yang mengizinkan pengalaman pengguna terbaik dan estetika yang inovatif dan indah. Ini akan dilakukan dengan meneliti

para pesaing, tetap unggul dalam tren dan standar teknologi, serta terus-menerus berupaya membawa visual yang baru dan menarik bagi pengguna akhir.

Bab 8

Kesimpulan

8.1 Ringkasan

Bulwark adalah koin yang berorientasi privasi dengan masternode, tata kelola, dan ekosistem peralatan yang terus berevolusi. Proyek ini dimulai dengan peluncuran yang adil dan fokus terhadap distribusi koin yang luas. Slow start, pembagian imbalan blok, dan algritma hashing sengaja dipilih untuk menciptakan peluang bagi partisipasi besar dari komunitas. Bulwark diluncurkan dengan sekumpulan fitur koin privasi yang penting dan tim pengembang bekerja keras memperkenalkan fitur baru dan membangun di atas teknologi yang sudah ada. Bulwark bertujuan untuk memberdayakan pilihan melalui privasi dan akan memfokuskan usaha yang kuat untuk mencapai tujuan ini.

8.2 Tugas Masa Depan

Ekosistem koin privasi masternode saat ini dibanjiri oleh koin-koin yang berusaha menarik pengguna baru lewat janji ROI yang besar, rencana yang bombastis yang penuh dengan janji yang sulit dipenuhi, serta fokus pada pemasaran ketimbang penyempurnaan yang sesungguhnya. Bulwark berencana menjadi yang sebaliknya: sedikit sensasi dan banyak menciptakan. Tujuan proyek saat ini dan masa depan akan mengikuti formula: spesifik, terukur, dapat dicapai, relevan, dan berbatas waktu.

Referensi

Aumasson, L.M., Jean-Phillipe Henzen, 2013. SHA-3 proposal: BLAKE. Tersedia di: https://131002. net/blake/blake.pdf.

Bertoni, G., Daemen, J., Peeters, M. & Van Assche, G., 2012. The keccak sha-3 submission. Tersedia di: https://keccak.team/files/Keccak-submission-3.pdf.

Bitcoin Core Team, T., 2017. Bitcoin developer reference. Tersedia di: https://bitcoin.org/en/ developer-reference#block-headers.

Chang, S.-J., Perlner, R., Burr, W.E., Turan, M.S., et al., 2012. Laporan ronde ketiga kompetisi algoritma hashing sha-3. Tersedia di: http://nvlpubs.nist.gov/nistpubs/ir/2012/ NIST.IR.7896.pdf.

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., et al., 2015. BlockChain technology. Tersedia di: http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.

Ferguson, N.L., Schneier, S., Whiting, B., Bellare, D., et al., 2010. Keluarga fungsi hashing skein. Tersedia di: http://www.skein-hash.info/sites/default/files/skein1.3.pdf.

Gauravaram1, P., Knudsen, L.R., Matusiewicz, K., Mendel, F., et al., 2012. Grøstl – a sha-3 candidate. Tersedia di: http://www.groestl.info/Groestl.pdf.

jakiman, 2017. PIVX purple paper. Tersedia di: https://pivx.org/wp-content/uploads/2017/03/ PIVX-purple-paper-Technincal-Notes.pdf.

Kiraly, B., 2017a. InstantSend. Tersedia di: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/ 1146928/InstantSend.

Kiraly, B., 2017b. PrivateSend. Tersedia di: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/ 1146924/PrivateSend.

Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system. Tersedia di: https://bitcoin.org/ bitcoin.pdf.

Okupski, K., 2016. Referensi pengembang Bitcoin, pp.3–4. Tersedia di: https://lopp.net/pdf/Bitcoin_ Developer_Reference.pdf.

strophy, 2017. Memahami spork. Tersedia di: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/128319489/Understanding+Sporks.

Wiecko, R., 2017. Klarifikasi isu penambangan instan Dash. Tersedia di: https://dashpay.atlassian.net/wiki/spaces/OC/pages/19759164/Dash+Instamine+Issue+Clarification.

Wu, H., 2012. Fungsi hashing jh. Tersedia di: http://www3.ntu.edu.sg/home/wuhj/research/jh/ jh_round3.pdf.