Prizm Whitepaper
Revision - March, 2017

Dokumen ini menjelaskan konsep dasar PRIZM.

Kata pengantar

Bitcoin mata uang digital desentralisasi pertama di dunia yang memudahkan untuk menyimpan dan mengirimkan koin kriptografi menggunakan jaringan P2P untuk transmisi informasi, hashing sebagai sinyal waktu untuk mencegah pengeluaran ganda dan skenario sistem yang kuat untuk menentukan pemilik koin. Dalam hal ini ada teknologi dan bisnis infrastruktur berkembang. Berdasarkan desain asli Bitcoin dapat ditukarkan, bertindak sebagai media pertukaran netral. Bitcoin mungkin memiliki sifat khusus yang mendukung baik emiten maupun perjanjian publik, dan memiliki nilai independen dari nilai nominal yang terletak pada dasarnya. Bitcoin membuktikan bahwa sistem pembayaran elektronik P2P benar-benar dapat bekerja dan melakukan proses pembayaran, tanpa partisipasi dari pihak ketiga. Namun, untuk memastikan bahwa seluruh ekonomi elektronik berdasarkan pada desentralisasi sepenuhnya, sistem harus dapat melakukan hal berikut:

1) Proses transaksi aman, cepat dan efisien, dapat melakukan seribu atau lebih transaksi per jam;

2) Mendorong orang untuk berpartisipasi dalam keamanan jaringan;

3) Bekerja secara global dengan konsumsi sumber daya minimal;

4) Dan dapat bekerja pada berbagai perangkat, termasuk ponsel.

PZM (diucapkan "Prism") memenuhi semua syarat ini. Dan juga memiliki keuntungan tambahan yang disebut Paramining, yang tidak ada di cryptocurrency yang lain. Tentang hal itu dijelaskan lebih lanjut.

Iktisar

PRIZM adalah cryptocurrency 100% proof-of-stake yang berdasarkan inti NEXT, dibangun pada bahasa open source Java. Algoritma unik PRIZM proof-of-stake yang tidak tergantung pada setiap pelaksanaan konsep "usia koin" yang digunakan oleh cryptocurrency proof-of-stake lain, dan tahan terhadap serangan oleh apa yang disebut *«nothing-at-stake»*. Jumlah koin yang tersedia telah didistribusikan di blok genesis. Kriptografi Curve25519 digunakan untuk menjamin keamanan keseimbangan dan kekuatan pemrosesan yang diperlukan, bersama dengan algoritma hashing SHA256 yang digunakan secara umum. Blok dihasilkan setiap 60 detik, rata-rata oleh rekening yang tidak diblokir di node jaringan. PZM didistribusikan melalui biaya transaksi, yang diberikan ke akun Anda ketika berhasil menciptakan blok. Proses ini dikenal sebagai forging dan mirip dengan konsep "tambang" yang digunakan oleh cryptocurrency lainnya. Transaksi dianggap aman setelah 10 blok diakui, dan arsitektur yang sebenarnya dan ukuran unit PZM dapat menangani hingga 367.200 transaksi per hari. PZM mencakup implementasi fungsi *Forging Transparent* yang akan meningkatkan efisiensi proses transaksi dua perintah yang menggunakan unit pembangkit algoritma deterministik dalam hubungannya dengan mekanisme keamanan tambahan dari jaringan.

Teknologi inti

Proof of Stake

Dalam model tradisional «*Proof-of-Work*», yang digunakan oleh sebagian besar cryptocurrency, keamanan jaringan disediakan oleh peserta yang melakukan "pekerjaan". Mereka menggunakan sumber daya mereka (perhitungan waktu / pengolahan), untuk memverifikasi transaksi dengan tingkat ganda dan membebankan biaya luar biasa pada orang-orang yang mencoba untuk meminimalkan transaksi. Untuk pekerjaan ini, peserta diberikan koin PZM, dimana frekuensi dan jumlah bervariasi tergantung pada parameter operasi cryptocurrency. Proses ini dikenal sebagai Mining. Frekuensi pembangkit unit, yang menentukan hadiah untuk setiap pertambangan cryptocurrency cenderung tetap konstan. Akibatnya, kompleksitas kerja yang dibutuhkan untuk penghargaan harus meningkatkan dengan meningkatkan efisiensi jaringan.
Seiring perkembangan jaringan Proof-of-Work pengguna individu menjadi kurang insentif untuk mendukung jaringan karena potensi pahala mereka akan didistribusikan di antara sejumlah besar pengguna-pengguna lain. Dalam pencarian profitabilitas para penambang terus berinvestasi sumber daya untuk peralatan khusus yang membutuhkan investasi modal yang signifikan dan biaya energi tinggi saat ini. Seiring waktu, jaringan menjadi lebih terpusat, karena mitra yang lebih kecil (orang-orang yang dapat melakukan sedikit pekerjaan) jatuh atau menyatukan sumber daya mereka di "pool". Pencipta Bitcoin Satoshi Nakamoto, menciptakan jaringan Bitcoin sepenuhnya terdesentralisasi. Tapi tidak ada yang bisa memprediksi bahwa insentif yang diberikan oleh Proof-of-Work, akan mengarah pada sentralisasi proses penambangan. Hal ini menyebabkan kerentanan. Pool Bitcoin GHash.io telah mencapai 51% dari kapasitas pertambangan Bitcoin di masa lalu, dan lima pool pertambangan Bitcoin naik 70% dari hashing jaringan listrik. Konsep desentralisasi berada di bawah ancaman kerugian total.
Dalam model Proof-of-Stake yang mengunakan Prizm, keamanan jaringan diatur oleh mitra yang memiliki saham di jaringan. Insentif yang diberikan oleh algoritma ini tidak kondusif untuk sentralisasi sebagai algoritma Proof-of-Work, dan data menunjukkan bahwa jaringan Prizm tetap

sangat terdesentralisasi sejak awal: sejumlah besar (dan yang bertumbuh) unit dari rekening yang unik kontribusi ke grid, dan lima rekening paling atas menghasilkan 35 % dari jumlah total blok.

Model Proof-of-Stake di Prizm

Prizm menggunakan sistem di mana setiap "koin" di rekening dapat dianggap sebagai rig tambang miniatur. Semakin banyak koin yang terdapat di rekening, semakin besar kesempatan bahwa account akan berhak untuk membuat blok. Secara keseluruhan "reward" yang dihasilkan dari unit penciptaan adalah jumlah biaya transaksi, terletak di dalam blok. PZM tidak membuat koin baru sebagai akibat dari penciptaan blok. Redistribusi PZM terjadi karena generator Unit dibayar komisi per transaksi, sehingga istilah "forging" (digunakan dalam konteks ini, untuk "menciptakan hubungan atau kondisi baru", bukan "Pertambangan"). Blok berikutnya dihasilkan berdasarkan diverifikasi, dan hampir tak terduga informasi yang unik dari blok sebelumnya. Blok terhubung berdasarkan hubungan ini, menciptakan rantai blok (dan transaksi) yang dapat ditelusuri kembali ke blok genesis. Memblokir waktu generasi sekitar 59 detik, tetapi perubahan probabilitas menyebabkan fakta bahwa rata-rata waktu blok generasi dapat menjadi 80 detik dan interval blok lebih panjang. Keamanan adalah hal utama di Blockchain dalam sistem Proof-of-stake.

Prinsip-prinsip dasar yang diterapkan pada algoritma Prizm Proof of Stake:

- Nilai kumulatif disimpan dalam kompleksitas sebagai parameter dalam setiap blok, dan setiap blok berikutnya menerima "kompleksitas" baru dari nilai blok sebelumnya. Dalam kasus ambiguitas, jaringan mencapai konsensus fragmen memilih Unit atau sirkuit dengan kompleksitas kumulatif tertinggi.
- Supaya pemegang rekening tidak memindahkan dana mereka dari satu account ke account lainnya sebagai sarana manipulasi untuk mendapatkan kemungkinan unit pembangkit, koin harus tetap dalam akun untuk 1440 unit, sebelum mereka dapat berkontribusi pada proses generasi unit. Koin yang memenuhi kriteria ini, memberikan kontribusi untuk saldo rekening yang efektif, dan saldo ini digunakan untuk menentukan kemungkinan forging.
- Untuk seseorang penyerang tidak dapat menciptakan sebuah rantai baru sepanjang rantai genesis jaringan blok memungkinkan hanya 720 blok restrukturisasi sirkuit diatur setelah blok terakhir. Setiap blok yang ditampilkan di bawah ambang batas ini akan ditolak. Ambang batas gerakan ini dapat dianggap sebagai referensi titik tetap PZM tunggal.

- Karena probabilitas yang sangat rendah bahwa suatu account akan me-manage seluruh blockchain, menciptakan blok rantai sendiri, transaksi dianggap aman jika mereka dikodekan dalam blok 10 unit yang terletak di luar blok terakhir.

Kesamaan dengan Peercoin Proof of Stake

Peercoin menggunakan parameter usia koin sebagai bagian dari algoritma probabilitas pertambangan. Dalam sistem ini, semakin lama Peercoin Anda berada di akun Anda (sampai 90 hari), semakin besar kekuatan (usia koin) mereka harus membuat blok. Act "minting" block membutuhkan konsumsi koin usia, dan jaringan menentukan konsensus, memilih rantai dengan usia paling umum koin yang dikonsumsi. Ketika Peercoin blok dipisahkan koin usia yang dikonsumsi dikembalikan kembali ke blok akun asli. Akibatnya, biaya menyerang jaringan Peercoin rendah karena penyerang dapat terus mencoba untuk menghasilkan blok (disebut grinding stake) sampai mereka akan berhasil. Peercoin meminimalkan ini dan risiko lainnya melalui pos pemeriksaan publisitas terpusat blockchain beberapa kali sehari untuk "membekukan" blockchain dan blok transaksi. Prizm tidak menggunakan usia koin sebagai bagian dari algoritma forging. Kemungkinan penciptaan memblokir akun apapun tergantung pada saldo saat ini (yang merupakan keuntungan untuk setiap account), waktu sejak blok terakhir (yang berbagi semua account forging) dan nilai target dasar (yang juga umum untuk semua akun pengguna).

Coin

Emisi awal - 10 juta PZM, dan jumlah akhir 6 milyar PZM. Koin ini diterbitkan dengan blok penciptaan genesis (blok pertama dalam rantai). Premining diterapkan di semua negara di dunia, dengan nilai nominal, dalam jumlah terbatas, untuk mencapai desentralisasi Prizm awal. Total volume jumlah PZM 6 milyar koin.
Akun genesis menghasilkan anti-koin ketika dapat sinyal Paramining (koin mengirim sinyal ke dompet khusus) sampai batas minus 6 milyar PZM

Keberadaan anti-koin dalam genesis memiliki beberapa efek samping yang menarik:

- Semua koin yang dikirim ke akun-genesis, dihancurkan karena saldo rekening negatif membatalkan mereka.

- Fungsi utama dari Prizm - sistem pembayaran tradisional, tetapi dirancang untuk melakukan lebih banyak lagi.

Kecapaian tujuan komunitas CWT (www.cwt.top) mungkin jika disediakan paritas PZM dengan mata uang fiat utama.

Node Jaringan

Node jaringan Prizm adalah perangkat yang membuat transaksi atau data blok ke jaringan. Setiap perangkat dengan perangkat lunak PZM dianggap sebagai node. Node dapat dibagi menjadi dua jenis: biasa dan ditandai. Node berlabel adalah node yang ditandai tanda token terenkripsi yang diterima dari kunci akun pribadi; token ini dapat diterjemahkan untuk mengungkapkan akun alamat PZM dan neraca tertentu, yang berhubungan dengan node. Tindakan penempatan tanda di node menambah akuntabilitas dan kepercayaan, sehingga node berlabel lebih dapat diandalkan dibandingkan situs yang tidak memiliki tanda di jaringan. Semakin besar saldo rekening yang terkait dengan situs yang ditandai, makin tinggi kepercayaan yang diberikan kepada situs ini. Pada saat itu, penyerang mungkin ingin menandai situs untuk mendapatkan kepercayaan dari jaringan, dan kemudian menggunakan kepercayaan untuk tujuan jahat; Hambatan masuk (biaya PZM, yang dibutuhkan untuk menghasilkan kepercayaan yang cukup) mencegah penyalahgunaan tersebut. Setiap node di jaringan PZM memiliki kemampuan untuk memproses dan mengirimkan transaksi dan blok informasi. Blok diperiksa sejak diterima dari node lain, dan dalam kasus di mana cek blok tidak dilakukan, node dimasukkan ke "black list" sementara untuk mencegah penyebaran data blok yang tidak valid. Setiap node memiliki mekanisme keamanan DDOS (Distributed Denial of Services) yang sudh terdapat didalamnya (built-in), yang membatasi jumlah permintaan jaringan dari setiap pengguna hingga 30 per detik.

Blok

Seperti di cryptocurrency lainnya, Ledger (buku besar transaksi) operasi PZM dibangun dan disimpan di barisan terkait blok, yang dikenal sebagai blockchain. Buku ini memberikan catatan permanen dari transaksi yang telah terjadi, serta set urutan transaksi yang dilakukan. Salinan Blockchain disimpan pada setiap node dalam jaringan Prizm, dan masing-masing akun yang tidak diblokir di node (dengan cara kunci pribadi dari account) memiliki kemampuan untuk menghasilkan blok, dengan syarat bahwa setidaknya satu transaksi dari rekening dikonfirmasi 1440 kali . Setiap akun yang memenuhi kriteria ini disebut akun yang aktif. Dalam PZM, setiap blok berisi 255 transaksi, mereka didahului Hedera 192 byte, yang berisi parameter identifikasi. Setiap transaksi diwakili di blok 160 byte maksimum, dan ukuran blok maksimum - 32K.

Semua unit berisi pilihan berikut:

• Versi blok, nilai ketinggian blok dan ID blok
• Tanda blok sementara, dinyatakan dalam detik dari blok genesis
• akun ID yang membuat blok, serta open key account.
• ID dan hash dari blok sebelumnya
• Jumlah transaksi yang disimpan di blok
• Jumlah total PZM, transaksi dan komisi di blok
• Transaksi data untuk semua transaksi yang termasuk dalam unit, termasuk pengenal transaksi
• panjang berguna beban blok dan fungsi hash satuan beban berguna
• nilai target dasar dan kompleksitas kumulatif untuk blok

Pembuatan blok (Forging)

Tiga nilai adalah kunci untuk menentukan rekening yang berhak untuk menghasilkan blok, memperhitungkan rekening yang mana mendapat hak untuk menciptakan blok, dan blok mana yang dianggap otoritatif selama konflik: nilai target dasar, nilai target dan total kompleksitas.

Target nilai dasar

Untuk memenangkan Forge (pembangkit) unit yang tepat, semua akun aktif Prizm «bersaing», mencoba untuk membuat nilai hash yang di bawah target nilai dasar yang telah ditentukan. Niilai target dasar ini berubah dari blok ke blok dan output dari nilai target dasar blok sebelumnya dikalikan dengan jumlah waktu yang diperlukan untuk generasi blok.

Nilai Target

Setiap akun memiliki menghitung sendiri nilai target berdasarkan tingkat suku bunga efektif saat ini.
Nilai ini sama dengan:
T = Tb x S x Be

dimana

T target nilai baru

Tb target nilai dasar

S waktu yang berlalu sejak pembuatan blok terakhir

Be saldo akun efektif

Seperti yang terlihat dari rumus, nilai target meningkat dengan setiap detik berlalu sejak satuan waktu sebelumnya. nilai target maksimum 1,53722867 x 1017, dan nilai target minimal adalah setengah nilai target dasar blok sebelumnya.
Nilai target dan target nilai dasar yang sama untuk semua akun mencoba Forge di bagian atas unit tertentu. Satu-satunya pilihan akun tertentu adalah pengaturan parameter saldo yang efektif.

Kompleksitas total

Nilai kumulatif diperoleh dari kompleksitas dasar dari nilai target, dengan rumus:
Dcb = Dpb + 264 / Tb

Dimana:

Dcb	kompleksitas blok terkini
Dpb	kompleksitas blok sebelumnya
Tb	nilai target dasar blok terkini

Algoritma Forging

Setiap unit dalam rantai memiliki generasi parameter tanda tangan. Untuk berpartisipasi dalam proses blok forging, akun aktif secara kriptografi ditandatangani oleh unit sebelumnya yang dihasilkan oleh kunci publik sendiri. Hal ini menciptakan tanda tangan 64-byte kemudian hash dengan menggunakan SHA256. 8 byte pertama dari hash yang dihasilkan memberikan nomor yang disebut hit account. Hit dibandingkan dengan nilai target saat ini. Jika Hit dihitung di bawah target, blok berikutnya dapat dihasilkan. Seperti tercantum dalam rumus nilai target, nilai target meningkat setiap detik. Bahkan jika dalam jaringan hanya beberapa rekening aktif, salah satu dari mereka akhirnya akan menghasilkan blok, karena nilai target akan sangat besar. Konsekuensi dari ini adalah bahwa Anda dapat memperkirakan waktu yang diperlukan untuk setiap akun unit Forge dengan membandingkan nilai hit rekening dengan nilai target. Titik terakhir adalah penting. Karena setiap node dapat meminta saldo yang efektif untuk setiap akun yang aktif, adalah mungkin untuk melalui semua account aktif untuk menentukan masing-masing nilai hit. Ini berarti bahwa untuk memprediksi dengan akurasi yang wajar apa account berikutnya akan memenangkan hak untuk pemblokiran palsu.

Serangan dapat dipicu dengan memindahkan saham di rekening, yang akan menghasilkan blok berikutnya, yang merupakan alasan lain mengapa tingkat PZM harus tetap 1440 unit sebelum dapat berkontribusi untuk forging (melalui nilai keseimbangan yang efisien). Menariknya, nilai dasar baru untuk blok target berikutnya tidak dapat diprediksi, sehingga proses menentukan siapa yang akan menjadi blok Forge berikutnya menjadi lebih stokastik karena upaya untuk memprediksi

blok masa depan. Fitur forging algoritma PZM membantu untuk membentuk dasar pengembangan dan implementasi algoritma Forging Transparan (forging jelas). Ketika akun aktif berhak untuk membuat unit, ia menggabungkan hingga 255 transaksi yang belum diverifikasi dalam blok baru dan mengisi unit dengan semua parameter yang diperlukan. Blok ini kemudian ditransmisikan ke jaringan sebagai calon blockchain.

Nilai beban yang membangkit akun dan semua tanda tangan di setiap blok dapat diuji oleh semua node jaringan yang diterimanya. Dalam situasi di mana beberapa blok dihasilkan, node akan memilih blok dengan nilai tertinggi dari akumulasi kompleksitas sebagai satu unit otoriter. Karena data blok didistribusikan di antara peserta (rekan-rekan), fork (fragmen chain tidak sah) terdeteksi dan dibongkar melalui pemeriksaan kompleksitas agregat nilai rantai yang disimpan di setiap Fork.

Paramining

Paramining - keuntungan kunci PRIZM atas cryptocurrency lainnya.
Dalam mekanisme forging dasar, pengembang PRIZM menambahkan mekanisme linear-retrograde yang unik untuk menentukan penghargaan atas penyimpanan, ditujukan untuk daya tarik ekonomi dan penggantian bertahap dari semua instrumen keuangan yang ada di dunia ke PZM. Artinya, selain kerangka forging, yang tidak meningkatkan jumlah dana dalam sistem, PZM menambahkan mekanisme Paramining yang menciptakan uang logam baru, menurut metrik dari normalisasi matematika standar sistem keuangan dalam ekonomi dunia. Dengan perhitungan kami - hanya Format ini pertumbuhan pasokan koin dapat memberikan penggantian semua instrumen ekonomi yang ada saat ini secara bertahap.

Tingkat produksi koin baru melalui Paramaynig dihitung dari dua parameter utama, jumlah koin di dompet sendiri dan jumlah koin dompet pengikutnya sampai 888 tingkat. Menurut karakteristiknya Paramining adalah sistem MLM 2,0 yang tidak melibatkan hal-hal yang tidak disukai oleh orang biasa di bisnis jaringan, tetapi pada saat yang sama melibatkan pengembangan jaringan untuk meningkatkan kecepatan produksi koin di dompet pribadi.

Sistem Paramining ketika membuat transaksi di dompet Anda menulis blockchain berisi nilai dari jumlah koin pemilik dompet dan jumlah koin di dompet pengikutnya dan menghasilkan koin baru dalam Saldo Wallet.

Misalnya: *Dengan 99 PZM dan 100.000 PZM di 888 tingkat struktur yang diterapkan persentase kenaikan jumlah koin 0,12% dan faktor 2,77 yang memungkinkan untuk menghasilkan 3,3 koin baru per hari, untuk itu cukup untuk membuat transaksi. Dengan demikian, kita memperoleh sistem bunga majemuk untuk meningkatkan kapitalisasi dan mendorong pengguna untuk melakukan transaksi dengan menghubungkan pemegang dompet baru, sehingga meningkatkan*

omset strukturnya. Menurut perkiraan konservatif peningkatan bulanan dalam jumlah koin pengguna tersebut tidak kurang dari 10%

Sistem Paramining adalah alat yang sempurna untuk promosi dan popularisasi, karena tidak memiliki analog dalam cryptocurrency modern. Keuntungan utama dari Paramining adalah tidak ada pengguna jaringan yang dapat campur tangan dalam mekanisme ini dan memalsukan koin baru, semua pengguna bisa belacak secara real-time jumlah koin yang dikeluarkan oleh sistem. Paramining bekerja pada setiap dompet dengan saldo lebih dari 1PZM dan secara otomatis berhenti bila saldo sebesar 1 juta PZM

Juga untuk pertama kalinya digunakan sistem membangun hubungan rujukan tanpa referensi. Setelah pendaftaran dompet baru sistem membuat catatan di blockchain dari siapa datang transaksi pertama dan selamanya membuat rantai rujukan yang tidak dapat diubah, itu memudahkan untuk membangun jaringan MLM global dan meningkatkan tingkat produksi koin baru.

Pelaksanaan teknis saat ini tidak dijelaskan secara rinci dengan alasan bahwa bagi kita semua hal utama adalah bukan membuat 100 alat "mati", tetapi satu yang beroperasi dengan baik. Jika, bagaimanapun, know-how kami akan diungkapkan, maka seseorang akan mencoba membuatnya lagi dan secara tidak sengaja menyebabkan gangguan dan penyalahgunaan ide ini untuk tujuan tidak mulia, sedangkan kami selalu berniat positif untuk planet kita.

Untuk memulai produksi PZM baru, hanya cukup satu koin di dompet elektronik, yang secara otomatis meluncurkan Paramining. Ini adalah proses yang memungkinkan tanpa biaya listrik meningkatkan jumlah koin di dompet. Paramining dimulai dengan 1 koin dan berhenti secara otomatis ketika mencapai 1 juta koin di dompet.
Paramining - metode unik untuk menciptakan koin baru oleh semua pengguna pada saat yang sama, diatur oleh dua parameter:

1. Jumlah koin di dompet elektronik pribadi.

Kecepatan pertumbuhan jumlah koin %	**Jumlah koin di dompet elektronik**
0,12%	dari 1 s/d 99
0,14%	dari 100 s/d 999
0,18%	dari 1000 s/d 9999
0,21%	dari 10000 s/d 49999
0,25%	dari 50000 s/d 99999
0,28%	dari 100000 s/d 499999
0,33%	dari 500000 s/d 1000000

Menurut perkiraan awal, penyelesaian Paramining dapat terjadi setelah sekitar 500 tahun, sejak generasi blok pertama.

2. Jumlah koin di dompet pengikut di 888 level.

Faktor/pengganda	Volume koin struktur pengikut
2,18	dari 1000 s/d 9999
2,36	dari 10000 s/d 99999
2,77	dari 100000 s/d 999999
3,05	dari 1000000 s/d 9999999
3,36	dari 10000000 s/d 99999999
3,88	dari 100000000 s/d 999999999
4,37	dari 1000000000

Prinsip Paramining didasarkan pada hukum-hukum dasar fisika, dari "radiasi Visible". Seperti model alam semesta kita, sistem ini terus berkembang, menambah kecepatan.

Akun PRIZM

Prizm mengimplementasikan dompet pintar sebagai bagian dari desain: semua account yang disimpan di jaringan dengan kunci pribadi untuk setiap alamat akun yang dikeluarkan dari pass-phrase untuk setiap akun dengan menggunakan kombinasi SHA256 dan operasi Curve25519. Setiap akun diwakili oleh sejumlah 64-bit, dan jumlah itu dinyatakan sebagai alamat akun menggunakan error correction kode Solomon, yang dapat mendeteksi hingga empat kesalahan dalam alamat akun atau memperbaiki hingga dua kesalahan. Format ini dilaksanakan dalam menanggapi kekhawatiran bahwa alamat yang salah dari akun dapat mengakibatkan koin, nama panggilan atau aset akan secara permanen ditransfer ke rekening yang salah. Alamat account selalu didahului oleh «PRIZM-», membuat alamat account Prizm mudah dikenali dan dibedakan dari format alamat yang digunakan oleh cryptocurrency lainnya. Alamat account terenkripsi oleh Kode Solomon terkait dengan frase rahasia, yang dihasilkan sebagai berikut:

1. Pass-phrase Rahasia di-hash menggunakan SHA256 untuk kunci akun pribadi.
2. Kunci pribadi dienkripsi menggunakan Curve25519 untuk mendapatkan kunci open account.
3. Kunci publik di-hash dengan SHA256 untuk mendapatkan ID akun.
4. 64-bit ID akun pertama adalah nomor rekening.
5. Kode Solomon, nomor rekening dengan awalan «PRIZM -» menghasilkan alamat akun tersebut.

Ketika account memiliki akses melalui frase rahasia untuk pertama kalinya, akun tsb tidak dilindungi oleh kunci publik. Ketika dilakukan transaksi keluar pertama dari rekening, kunci publik 256-bit yang berasal dari pass-phrase disimpan dalam blockchain, dan melindungi akun Anda. Ruang alamat untuk kunci publik (2256) lebih besar dari ruang alamat untuk nomor rekening (264), sehingga tidak ada ambigu pencocokan rekening dengan kata kunci dan kemungkinan tabrakan dihindari. Konflik-konflik ini diidentifikasi dan dihindari sebagai berikut: untuk mengakses akun Anda menggunakan frase kode tertentu hanya sekali, dan akun ini dilindungi oleh 256-bit kunci publik, tidak ada pasangan lain dari kunci publik yang dapat mengakses nomor rekening Anda.

Properti saldo akun

Untuk setiap akun Prizm ada tingkat saldo yang berbeda. Setiap jenis memiliki tujuan yang berbeda, dan banyak dari nilai-nilai ini diperiksa sebagai bagian dari verifikasi dan pengolahan transaksi.

- saldo rekening efektif digunakan sebagai dasar untuk perhitungan forging. saldo rekening yang efektif terdiri dari semua koin, yang tetap pada account ini untuk 1440 unit. Selain itu, fungsi "akun Leasing" memungkinkan Anda untuk mengatur saldo yang efektif ke akun lain untuk sementara.
- saldo rekening yang terjamin terdiri dari koin yang tetap pada account untuk 1440 unit. Beda dari saldo yang efektif, saldo ini tidak dapat ditugaskan untuk setiap akun lainnya.
- saldo rekening dasar mencakup semua transaksi yang telah memiliki setidaknya satu dikonfirmasi.
- saldo rekening Forging merupakan jumlah total PZM, sehingga blok forging sukses.
- saldo rekening yang belum dikonfirmasi - adalah salah satu yang muncul di klien Prizm. Itu adalah neraca transaksi berjalan, koin bersih yang terlibat dalam transaksi yang dikirim tapi belum diakui.

- daftar neraca terjamin membuat daftar saldo semua aset yang terkait dengan akun tertentu.
- neraca daftar saldo yang belum dikonfirmasi menghitung semua aset yang terkait dengan akun tertentu.

Wallet.dat

Bitcoin dan mata uang terkait sering menggunakan file terenkripsi, judul dan sebuah dompet untuk menyimpan alamat yang dihasilkan untuk mendapatkan koin. Inti NEXT yang digunakan dalam Prizm tidak meniru fungsi ini, tetapi tidak mengecualikan itu. Pengembang- pelanggan dapat menerapkan sistem di mana sekelompok kunci pribadi untuk catatan pengguna Prizm disimpan dalam file terenkripsi secara offline.

Konfirmasi transaksi

Semua transaksi PZM dianggap belum dikonfirmasi sampai saat mereka tidak termasuk dalam unit jaringan yang sebenarnya. Blok baru dialokasikan ke jaringan simpul yang menciptakan mereka, dan transaksi yang termasuk dalam unit akan dianggap menerima satu konfirmasi. Karena blok berikutnya ditambahkan ke rantai yang sudah ada (blockchain), setiap unit tambahan menambah satu lagi konfirmasi ke jumlah transaksi. Jika transaksi tidak termasuk dalam blok untuk tanggal kedaluwarsa, ia dihapus dari pool transaksi.

Waktu transaksi

Setiap transaksi mengandung parameter batas waktu (deadline) yang dipasang pada jumlah menit dari saat pengiriman transaksi ke jaringan. Batas waktu default adalah 1440 menit (24 jam). Transaksi, yang telah diserahkan, tetapi tidak termasuk dalam blok disebut transaksi tidak mengikat.

Jika transaksi tidak termasuk dalam unit sebelum batas waktu, transaksi dihapus dari jaringan. Transaksi dapat dibiarkan tidak terkonfirmasi karena tidak sah atau rusak, atau karena blok dipenuhi dengan transaksi yang menawarkan komisi yang lebih tinggi. Di masa depan transaksi dengan beberapa tanda tangan dapat menggunakan batas waktu sebagai cara untuk memastikan kepatuhan kepada jangka waktu.

Penciptaan dan pengolahan transaksi

Informasi rinci tentang penciptaan dan pengolahan transaksi PZM adalah sebagai berikut:
Pengirim menunjukkan parameter transaksi. Jenis transaksi berubah, dan tipe yang diinginkan ditentukan saat membuat transaksi, tetapi untuk semua transaksi harus menentukan beberapa parameter:

- Kunci pribadi untuk mengirim
- batas waktu transaksi
- transaksi opsional dengan ikatan

Dasar kriptografi PRIZM

Penukaran kunci Prizm didasarkan pada algoritma Curve25519 yang menghasilkan kunci rahasia bersama kurva elips yang cepat dan efektif Diffie-Hellman dengan tingkat perlindungan yang tinggi. Algoritma ini pertama kali ditunjukkan oleh Daniel J. Bernstein pada tahun 2006. Realisasi Next dalam Jawa dianggap oleh DoctorEvil di bulan Maret 2014. Penandatanganan pesan Prizm dilakukan dengan menggunakan algoritma Elliptic-Curve (EC-KCDSA) tanda tangan digital yang didefinisikan kelompok IEEE P1363a pada tahun 1998 oleh tim KCDSA. Kedua algoritma dipilih untuk menyeimbangkan kecepatan dan keamanan untuk ukuran kunci dari 32 byte.

Keunggulan utama

Klien JavaScript yang canggih

Aplikasi klien yang nyaman generasi kedua dibangun ke dalam distribusi perangkat lunak Prizm utama, dan dapat diakses melalui web browser lokal.
Klien memberikan dukungan penuh untuk semua fungsi utama Prizm, sehingga kunci privat user tidak akan tersedia di jaringan. Ini juga termasuk antarmuka administrasi dan dokumentasi Javadoc yang *built-in* untuk prioritas rendah antarmuka pemrograman aplikasi Prizm.

Pembayaran dasar

Fitur yang paling mendasar dari cryptocurrency apapun adalah kemampuan untuk mentransfer koin dari satu akun ke akun yang lain. Ini adalah jenis transaksi yang paling mendasar Prizm, dan itu memungkinkan penggunaan fungsi pembayaran dasar.

Perangkat portabel

Karena cross-platform yang berdasarkan Java roots, hashing Proof-of-Stake dan kemampuan masa depan untuk mengurangi ukuran dari blok rantai, Prizm sangat cocok untuk digunakan pada perangkat daya rendah kecil dengan sumber daya yang rendah. Aplikasi untuk Android dan iPhone dan perangkat lunak telah porting ke ARM atau perangkat dengan daya rendah seperti platform Raspberry Pi dan CubieTruck.
Kemampuan untuk menerapkan Prizm di perangkat dengan daya rendah yang selalu terhubung seperti smartphone, memungkinkan kita untuk membayangkan sebuah skenario di mana sebagian besar jaringan Prizm didukung oleh perangkat mobile. Biaya rendah dan konsumsi sumber daya dari perangkat ini sangat mengurangi biaya jaringan dibandingkan dengan cryptocurrency tradisional berdasarkan Proof-of-Work.

KEUNGGULAN UTAMA PRIZM

1. Jenis forging POS
2. Pencampuran dua teknologi paramining + penempaan secara bersamaan
3. Paramining. Kode sumber tertutup (tidak berbaris), sampai waktu tertentu, sebagai pertahanan terhadap klon, sebagai jaminan bahwa sistem akan cair.
4. Program afiliasi 888 tingkat dalam struktur
5. inti kriptografi NEXT /Proof-of-Stake
6. antarmuka user-friendly untuk perangkat mobile,
7. password user tidak disimpan di server

Masalah

Nothing at stake.

Dalam serangan "*nothing at stake*" para forgers mencoba untuk membangun blok di atas fork yang mereka lihat, karena hampir tidak dikenakan biaya, karena pengabaian fork berarti hilangnya blok reward yang akan diterima jika telah fork ini dirancang untuk menjadi rantai dengan kesulitan kumulatif yang tertinggi. Meskipun serangan ini secara teoritis mungkin, namun tidak praktis. Jaringan Prizm tidak mengalami fork panjang blockchain, dan reward untuk blok rendah tidak menguntungkan; Selain itu, mengorbankan keamanan jaringan dan kepercayaan untuk keuntungan kecil dapat membuat setiap kemenangan pirrikoy.

Serangan terhadap sejarah

Dalam "Serangan pada sejarah" seseorang mendapat sejumlah besar koin, menjual mereka, dan kemudian mencoba untuk membuat fork yang sukses sebelum koin dijual atau ditukar. Jika serangan gagal, upaya tidak bernilai, karena koin telah dijual atau dialihkan; Jika serangan berhasil, penyerang mendapat chip-nya kembali. Bentuk ekstrim dari serangan ini adalah jika kunci pribadi diperoleh dari rekening lama dan digunakannya untuk membangun rantai langsung dari blok genesis. Dalam Prism serangan dasar pada sejarah biasanya tidak bekerja, karena semua suku harus tetap pada 1440 unit, sebelum mereka dapat digunakan untuk forging; Selain itu, saldo yang efektif dari rekening, yang menghasilkan setiap unit diperiksa sebagai bagian dari unit verifikasi. Bentuk ekstrim dari serangan ini biasanya tidak dipicu karena blockchain PRIZM tidak dapat dibentuk kembali lebih dari 720 unit setelah perbatasan blok terakhir. Hal ini membatasi kerangka waktu di mana seorang aktor yang buruk bisa membangun bentuk serangan.

Aplikasi

Masalah Bitcoin yang dilihat oleh Prizm

Prizm diciptakan sebagai cryptocurrency 2.0 - respon kepada Bitcoin. Prizm menggunakan fitur yang mapan di Bitcoin, dan mempertimbangkan aspek perhatian. Lampiran ini membahas masalah dengan protokol dan jaringan Bitcoin, yang dirapikan oleh teknologi Prizm.

Ukuran Blockchain

Blockchain Bitcoin adalah koleksi blok data lengkap yang dihasilkan seri yang berisi buku register elektronik untuk semua transaksi Bitcoin yang terjadi sejak diluncurkan pada bulan Januari 2009. Empat tahun kemudian, pada Januari 2013 ukuran blockchain Bitcoin adalah 4 gigabyte (GB) - jumlah data rata-rata yang dibutuhkan untuk menyimpan film dua jam dalam DVD. Delapan belas

bulan kemudian, pada bulan Juli 2014, jumlah blockchain Bitcoin meningkat hampir lima sampai 19 gigabyte (GB) 37. Blockchain Bitcoin mengalami pertumbuhan eksponensial, dan modifikasi dari protokol Bitcoin asli akan membutuhkan solusi untuk itu.

Jumlah transaksi per hari

Pada akhir 2013 jumlah transaksi yang diproses dalam jaringan Bitcoin, memuncak sampai dengan 70.000 per hari, yaitu sekitar 0,8 transaksi per detik (tps). Ukuran standar sebuah blok Bitcoin yaitu satu megabyte yang dihasilkan (rata-rata) setiap sepuluh menit pada node klien dan membatasi kapasitas maksimum jaringan Bitcoin sekitar 7 TPS. Bandingkan ini dengan jaringan VISA dimana kapasitas bandwidth untuk menangani 10.000 TPS, dan Anda akan melihat bahwa Bitcoin tidak dapat bersaing, seperti dilihat saat ini.

Jawaban PRIZM

Dalam keadaan saat ini jaringan Prizm dapat menangani hingga 367.200 transaksi per hari - sembilan kali lebih tinggi dari nilai puncak Bitcoin. Pelaksanaan Forging Transparan memungkinkan untuk memproses transaksi hampir seketika yang sangat meningkatkan batas ini.

Waktu konfirmasi transaksi

Waktu konfirmasi transaksi Bitcoin bervariasi dari 5 sampai 10 menit untuk sebagian besar di tahun 2013. Setelah pengumuman bahwa bank-bank Cina tidak akan diizinkan untuk menangani Bitcoin pada akhir 2013, waktu rata-rata transaksi Bitcoin meningkat secara signifikan hingga 8-13 menit, dengan puncak periodik dalam 19 menit. Sejak itu waktu konfirmasi bergeser dalam kisaran 8-10 menit. Tetapi untuk menyelesaikan transaksi Bitcoin membutuhkan sejumlah pemeriksaan (setidaknya enam pengakuan), satu jam dapat dengan mudah berlalu sebelum penjualan aset dibayar oleh bitcoin.

Jawaban PRIZM

Waktu generasi blok PZM rata-rata menjadi sekitar 80 detik, dan waktu proses rata-rata sama dengan nilai transaksi yang sama. Transaksi dianggap aman setelah sepuluh bukti, yang berarti bahwa transaksi menjadi permanen dalam waktu kurang dari 14 menit.
Pelaksanaan Forging Transparanmemungkinkan Anda untuk melakukan transaksi hampir seketika dan mengurangi waktu ini.

Masalah sentralisasi

Peningkatan kompleksitas yang dikombinasikan dengan kecepatan jaringan hash untuk Bitcoin menciptakan sebuah penghalang yang tinggi untuk masuk bagi pendatang baru, dan keuntungan yang lebih rendah untuk peralatan pertambangan yang ada. Insentif untuk mendorong blok yang digunakan di bitcoin, telah menyebabkan penciptaan peralatan pertambangan 44 yang single-level dan khusus, serta ketergantungan pada satu set pool pertambangan yang kecil sebesar 45. Hal ini menyebabkan efek "sentralisasi", di mana volume besar pertambangan difokuskan pada kontrol penurunan jumlah orang. Hal ini tidak hanya menciptakan kekuatan struktur yang dikembangkan

oleh Bitcoin untuk memotong, tetapi juga merupakan kemungkinan nyata bahwa salah satu operasi pertambangan atau pool dapat mengumpulkan 51% dari total kapasitas pertambangan di 46 jaringan dan melakukan serangan 51%. Ada juga serangan yang membutuhkan hanya 25% dari total kapasitas jaringan hash. Pada awal Januari 2014 GHash.io mulai secara sukarela mengurangi kekuatan pertambangan mereka sendiri, karena ia mendekati level 51%. Beberapa hari kemudian kekuasaan di pool turun menjadi 34% dari total kapasitas jaringan, namun kecepatan segera mulai tumbuh, dan pada Juni 2014 kembali mencapai tingkat berbahaya.

Jawaban PRIZM

Insentif yang diberikan algoritma Proof-of-Stake, yang digunakan dalam Prizm, memberikan pengembalian atas investasi yang rendah sekitar 0,1%. Karena masing-masing unit tidak menghasilkan koin baru, tidak ada tambahan "reward untuk Pertambangan", yang mendorong upaya bersama untuk membuat blok. Data menunjukkan bahwa jaringan Prizm sangat desentralisasi sejak awal: jumlah rekening tinggi (dan meningkat) yang unik membuat blok ke jaringan, dan lima rekening terbesar menghasilkan 35% dari jumlah total blok.

Biaya pemeliharaan Proof of Work

Konfirmasi transaksi untuk Bitcoin yang ada dan penciptaan Bitcoin baru membutuhkan banyak daya komputasi, yang bekerja terus-menerus. Kekuatan pemrosesan ini disediakan oleh apa yang disebut "tambang Riggs" yang diatur oleh para "penambang." Penambang Bitcoin bersaing satu sama lain untuk menambahkan transaksi blok berikutnya dalam total rantai Bitcoin. Hal ini dilakukan dengan "hashing" - menggabungkan semua transaksi Bitcoin terjadi dalam sepuluh menit terakhir, dan usaha mereka untuk mengenkripsi data blok yang kebetulan juga memiliki sejumlah nol berturut-turut di dalamnya. Sebagian besar blok uji yang yang dihasilkan melalui hash tidak memiliki sejumlah nol yang diperlukan, sehingga mereka membuat perubahan kecil dan coba lagi.

Miliar upaya untuk menemukan unit yang "memenangkan" disebut gigahash, dan rig Pertambangan dinilai oleh berapa banyak gigahash dapat ia melakukan per detik, ditandai dengan GH/detik. Penambang pemenang, yang pertama menciptakan blok kriptografi Bitcoin yang benar, mendapat hadiah sebesar 25 Bitcoin baru - biaya pada saat penulisan ini adalah sekitar 15 750 USD. Kompetisi ini antara penambang berulang lagi dan lagi setiap sepuluh menit atau lebih. Pada awal 2014 dipicu lebih dari 3.500 Bitcoin per hari, setara dengan sekitar 2,2 juta dolar AS per hari. Dengan begitu banyak uang taruhan, penambang didukung oleh perlombaan senjata yang cepat dalam teknologi pertambangan rig untuk meningkatkan kesempatan mereka untuk menang. Awalnya Bitcoin diekstrak menggunakan prosesor sentral (CPU), komputer desktop yang khas.

Kemudian untuk meningkatkan kecepatan chip yang digunakan khusus prosesor grafis (GPU) di kartu grafis high-end. Kemudian, mikroprosesor digunakan dengan matrix gerbang (FPGA), dan kemudian diterapkan chip sirkuit khusus yang terintegrasi (ASIC). Teknologi ASIC adalah atas baris untuk para penambang bitcoin, tapi perlombaan senjata berlanjut dengan munculnya berbagai generasi chip ASIC. Generasi saat ini - chip ASIC yang disebut-perangkat 28-nm berdasarkan jumlah transistor mikroskopis di nanometer. Mereka harus diganti dengan modul ASIC 20-nm pada akhir 2014. Sebuah contoh dari pertambangan rig mutakhir baru bisa menjadi peta ASIC 28-nm «Monarch» oleh Butterfly Labs, yang harus menyediakan 600GH / sec untuk konsumsi listrik 350 watt dan biaya 2200 dolar AS.

Infrastruktur Pertambangan rig yang saat ini digunakan untuk mendukung operasi Bitcoin yang sedang berlangsung sangatlah menakjubkan. ASIC Bitcoin seperti Ilmuwan-autis- mereka Hanya DAPAT melakukan perhitungan Bitcoin blok Dan TIDAK LEBIH, tetapi mereka DAPAT melakukannya dengan KECEPATAN Satu superkomputer. Pada November 2013, majalah Forbes menerbitkan Sebuah artikel berjudul "Daya komputasi global Bitcoin 256 kali LEBIH Cepat Dari 500 superkomputer yang dikombinasikan!" [6]. Pada Pertengahan Januari 2014 statistik yang disimpan di situs blockchain.info, menunjukkan bahwa untuk dukungan Transaksi Bitcoin yang terus menerus memerlukan tingkat hash yang terus menerus Sekitar 18 juta GC / detik. Dalam satu hari kekuasaan hash seperti itu dihasilkan 1,5 triliun unit uji yang dihasilkan dan ditolak oleh penambang Bitcoin yang mencari satu hal - 144unit yang misteris, yang akan menutupi 2,2 juta dolar AS yang mereka menghabiskan..

Hampir semua pembayaran bitcoin tidak ditujukan untuk mengoreksi bencana dengan DNA atau mencari sinyal radio dari pemodelan E.T .; Sebaliknya, mereka benar-benar sia-sia. Kekuatan dan biaya yang berkaitan dengan dukungan latar belakang Bitcoin sangat besar dan boros. Jika semua pertambangan rig Bitcoin memiliki tingkat "Monarch", seperti dijelaskan di atas - (dan mereka tidak akan ada sampai mereka dimodernisasi), - mereka akan merupakan pool sebesar 30.000 kendaraan senilai lebih dari $ 63 juta AS dan mengkonsumsi lebih dari 10 megawatt dengan tagihan listrik lebih dari $3,5 juta. per hari. Angka-angka yang sebenarnya jauh lebih tinggi daripada saat ini, kurang efisien untuk mesin tambang rig yang mendukung Bitcoin. Dan angka-angka ini sekarang makin meningkat pada kurva pertumbuhan eksponensial, karena bitcoin memulai sejak transaksi terakhir per detik sampai maksimal tujuh transaksi per detik.

Solusi Prizm

Biaya jaringan dan analisis efisiensi Prizm menunjukkan bahwa seluruh ekosistem PRIZM dapat dipertahankan sekitar 60 000 dolar AS per tahun, sekarang hampir 2.200 kali lebih murah daripada biaya menjalankan jaringan Bitcoin.

Biaya pemeliharaan POW yang dibayar oleh pemegang coin

Selain biaya besar listrik ada biaya tersembunyi untuk kepemilikan sederhana Bitcoin. Untuk masing-masing blok yang ditemukan seorang yang menghasilkan blok menerima hadiah. Pada saat penulisan ini hadiah adalah sebesar 25 BTC, termasuk 10% inflasi total supply Bitcoin tahun

ini saja. Untuk setiap $ 1.000 pengguna membayar $100 per bitcoin tahun ini, untuk "membayar" kepada para penambang atas keselamatan jaringan.

Semoga kekuatan PRIZM menyertai Anda!