BULWARK

CRYPTOCURRENCY

Bulwark Cryptocurrency Whitepaper

Bulwark Core Team:

Eatbatterys (Project Coordinator)

Jack (Marketing Director)

SerfyWerfy (Blockchain Developer)

Frogman (Communications Lead)

Patrick (Brand and Design)

Stu (Ecosystem Developer)

Het Bulwark Core Team

December 2017

Wij, het Bulwark Core Team, bevestigen dat het werk dat in deze whitepaper gepresenteerd wordt ons eigen werk is. Als er informatie is verkregen of afgeleid van andere bronnen, bevestigen we dat middels naamsvermeldingen.

Samenvatting

Bulwark (code: BWK) is een op de community georiënteerde munt, geboren uit de observatie van oneerlijke praktijken rondom masternodes van op privacy gerichte munten. Onze goed doordachte en ondubbelzinnige lanceer-strategie staat deelnemers toe om direct vanaf de start deel te nemen aan een veelbelovend project. We bieden een eenvoudige waardepropositie, zonder grootse belofte: we zullen een op privacy gerichte munt leveren, die vandaag én in de toekomst werkt, door gebruik te maken van best-practices van zowel DASH als PIVX. Geen droombeelden met een beperkt uitzicht op levering, maar een werkende munt, op basis van een werkend platform, met ondersteuning voor de toekomst. Dit betekent niet dat we niet van plan zijn te innoveren. We focussen op resultaat, in plaats van hype. Er zijn teveel munten die zich enkel baseren op hype, zonder enige substantie. Wij willen ons niet scharen onder de groep van munten die gedreven worden door het motto van teveel beloven, en te weinig leveren. Wij doen het anders; een soft-launch (geen ICO), een beperkte hoeveelheid vooraf gemined, en op miners gerichte block-beloningen. Daarmee hebben Bulwark-deelnemers vanaf het begin af aan toegang tot een privacy-munt, waarvan masternodes, de best beschikbare technologie voor privacy-munten, en een zinvolle roadmap onderdeel zijn. Masternodes zullen beschikbaar zijn vanaf de lancering, en zijn fundamenteel onderdeel van de visie van de munt. De masternodes stabiliseren de circulatie, beveiligen het netwerk en voorzien in belangrijke functionaliteit.

Erkenningen

Bulwark zou niet mogelijk zijn geweest zonder het voorafgaand werk van de respectabele teams van Bitcoin, Peercoin, Blockcoin, Talkcoin, Dash en PIVX. Open source software en bijdragers daaraan, banen continue een weg voor nieuwe innovaties. Als informatie en kennis vrij verkrijgbaar zijn, en je daarop verder kunt bouwen, heeft de samenleving als geheel daar voordeel van. We zijn dankbaar met onze voorgangers die ons de mogelijkheid hebben gegeven om bij te dragen aan dit groeiende ecosysteem.

Inhoudsopgave

Hoofdstuk 1

Korte introductie tot cryptogeld

1.1 Achtergrond

In 2009 heeft Satoshi Nakamoto een document uitgebracht met de titel *Bitcoin: A Peer-to-Peer Electronic Cash System*. Hierin schrijft hij in detail over zijn visie op handel. Onderdeel van zijn visie is zijn peer-to-peer valuta's, ondersteund door een op hashes gebaseerd 'Proof of Work'-systeem. Het netwerk zou transacties vastleggen door ze middels een hash op een doorlopende grootboekrekening te plaatsen. De transactie zou niet veranderd kunnen worden, zonder de Proof of Work over te doen. Als bewijs van gebeurtenissen, kiezen nodes de langste keten waarvan (cumulatief) de grootste hoeveelheid rekenkracht (hashing power) getuige is geweest. Zolang ≥ 51% van die rekenkracht afkomstig is van nodes die niet de intentie hebben om een aanval te faciliteren, blijft de keten die ze genereren de langste.

1.2 Het block

Elk block op het netwerk wordt voorafgegaan door een 80-byte header. Die header bevat een gehashte kopie (double SHA256) van de header van het vorige block, de zogenaamde Merkle root (een gehashte afgeleide van alle hashes die in het block zijn gegenereerd), het tijdstip waarop Proof of Work begon, de moeilijkheidsgraad waaraan de hash van deze header moet voldoen, en de nonce waarop miners te beoogde moeilijkheidsgraad bereikt hebben. Hierdoor wordt iedere poging om een transactie in een block te wijzigen, geweigerd door het netwerk van miners (Bitcoin Core Team 2017).

1.3 De blockchain

Blocks worden gevormd door groepen transacties, en die blocks worden chronologisch in een ketting geplaatst. Die ketting wordt de blockchain genoemd. De blockchain vormt een geschiedenis van alle activiteit in een netwerk en dient als gedistribueerd consensusmodel, waarin alle transacties op elk moment geverifieerd kunnen worden (Crosby et al. 2015).

1.4 Proof-Of-Work

Proof of work is een verificatiesysteem, waarin miners concrete middelen moeten gebruiken (elektriciteit, hardwarekosten), om een arbitraire probabilistische *woordpuzzel* op te lossen. Als een kwaadwillende de blockchain zou willen vervuilen met een fraudulente transactie, zou hij alle Proof of Work tot op dat moment (opnieuw) moeten afronden (Okupski 2016).

Hoofdstuk 2

Bulwark; een introductie

2.1 Een solide basis

Elk huis heeft een solide basis nodig, en dat is voor Bulwark niet anders. Bulwark is gebouwd op *PIVX*, die zelf weer gebouwd is op de populaire *DASH*-cryptovaluta. Hoewel de afkomst teruggebracht kan worden naar de originele Satoshi Core, heeft elk project eigen doelen en idealen ten behoeve van de community die het representeert. Zo bouwen wij verder aan en leggen we de nadruk op de privacy-features van onze voorgangers, door nieuwe technologieën te ontdekken, en tools en mogelijkheden te bouwen voor de integratie van Bulwark in de op technologie gerichte platforms van vandaag.

2.2 Een team dat toegewijd is aan de community

Voor sommige projecten is de community een bijkomstigheid. Bulwark's nummer 1 prioriteit is de community. Bulwark streeft ernaar om hét cryptogeld te worden voor alle soorten eindgebruikers. Daar werken we aan met onder andere weggeefacties, wedstrijden, een levendig discussieplatform, en een zero-tolerance beleid gericht op het lastigvallen van nieuwkomers. Leden van Bulwark dragen al bij met handige scripts en gidsen om de gebruiksvriendelijkheid te verbeteren.

2.3 Eerlijk en gebalanceerd

Op het moment van schrijven, is er een instroom van cryptovaluta die gebruik maken van een vergelijkbare basis. Hoewel de onderliggende technologie solide is, komen regelmatig minder eerlijke praktijken aan het licht bij nadere inspectie van specificaties en blockchain-parameters.

2.4 Het probleem van vooraf minen

2.4.1 Casus: FooBarBazCoin

Een groeiende trend in de wereld van cryptovaluta, is om een arbitraire datum ver in de toekomst te kiezen, om vervolgens een percentage van het aanbod van munten op die datum als vooraf gemined te bestempelen (premined). Laten we eens kijken naar de denkbeeldige munt FBC (*FooBarBazCoin*), een afgeleide van *DASH*.

- Block-beloning: 15
- Block-tijd: 2.5 minutes
- Deel PoW/Masternode: 50/50%
- Initiële difficulty-algoritme: KGW
- Subsidie neemt jaarlijks met 12% af
- Maximaal aantal munten: ~25 miljoen
- 2,5% vooraf gemined

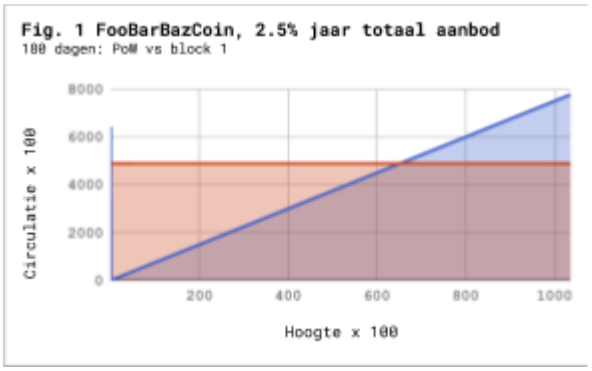
In dit voorbeeld staat de geadverteerde 2,5% dat vooraf gemined is voor ~643.000 munten (van de 25 miljoen). Dat lijkt redelijk. Maar om dat aantal munten te bereiken op basis van PoW- en masternode-beloningen, zouden er 43.000 gevonden blocks voor nodig zijn. Op basis van 2,5 minuten per block, zou dat grofweg 150 dagen in beslag nemen voor miners (of 75 dagen in het geheel). Met andere woorden: na 75 dagen zouden ontwikkelaars van de munt nog steeds over de helft van de munten in omloop beschikken.

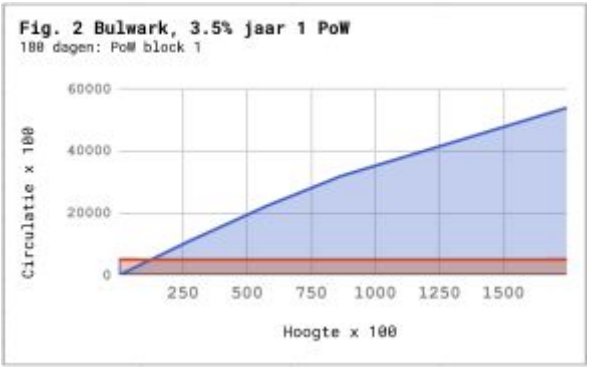
2.5 Een eerlijker alternatief

Het Bulwark Team (h)erkent dit, en heeft besloten om er vooraf open over te zijn. We hebben vooraf 489.720 munten gemined (3.5%). Dat representeert iets meer dan 12 dagen

PoW-mining, of iets meer dan 10 dagen van totale productie. We hopen dat we hiermee de community kunnen geruststellen, dat na een bepaald punt, de markt niet meer significant gedevalueerd kan worden als resultaat van munten die in het bezit zijn van het Bulwark-team. Zoals je in onderstaande figuren kunt zien, die beide een scenario van 180 dagen representeren, is het verschil duidelijk. We hopen dat we, door dit onderwerp op een open en eerlijke manier aan te vliegen, hiermee duidelijk maken dat het Bulwark-team ten dienste en ten bate staat van de community.

2.5.1 Vergelijking van beide methodes





2.5.2 Insta-mines en onze aanpak

Dash (Darkcoin) is een interessante case die de noodzaak voor bescherming tegen insta-mines aan het licht brengt. Bijna 10-15% van het totale Dash-aanbod is in de eerste dagen van het bestaan van de munt gemaakt, met dank aan een aantal ondernemende gebruikers (Wiecko 2017). Onze benadering ten aanzien van insta-mining was tweeledig. Allereerst hebben we een trage subsidie gebruikt. De opbrengsten van de eerste 960 blocks (1 dag) zijn lineair opgehoogd tot de volledige beloning. Daarnaast is 100% van de block-beloningen die dag ook naar miners gegaan. Historisch gezien, is dit altijd anders benaderd, namelijk met een hele lage block-beloning, die plotseling verandert naar de volledige beloning. Dit heeft regelmatig als gevolg gehad dat er pools geDDoSt werden, of werden overwelmd door verkeer van nieuwe miners. Met een lineair toenemende beloning, is er geen reden meer om miners en pool-beheerders te hinderen voor eigen winst.

2.5.3 ICO? Wij zien liever IC-NO!

Laten we eerlijk zijn, op het moment van schrijven worden we overspoeld met *ICO*'s. Ondanks dat ze een legitieme plaats hebben in het ecosysteem van cryptogeld, zien we regelmatig dat ze enkel gebruikt worden om geconcentreerde punten van rijkdom te

creëren. Gegeven dat Bulwark zowel masternode-beloningen, en in de tweede fase, 'Proof of Stake'-beloningen uitkeert, zou deze concentratie van rijkdom grote marktschommelingen kunnen veroorzaken. Daarnaast zou het bestuur van de munt daarmee sterk in het voordeel van early adopters zijn. Hoewel dit soort concentraties van rijkdom niet te voorkomen zijn, geloven we dat het goed is om elke mogelijkheid aan te grijpen om een eerlijk speelveld te creëren. We lanceerde de munt met een geschaald block-beloningssysteem; een eerlijk systeem die een wijdverbreide distributie van Bulwark aanmoedigt. Idealiter vermijden we daarmee geconcentreerde rijkdom zoals bekend van andere projecten.

2.6 Snel en functioneel

Met een block-tijd van 90 seconden, masternode-consensus, het vastzetten van transacties, een schappelijk uitgaveschema, en een staking-methode die vriendelijke is voor het ecosysteem, streeft Bulwark ernaar om een echt snelle en functionele cryptovaluta te zijn.

Hoofdstuk 3

Onze blockchain-parameters

3.1 Bulwark-specificaties in één oogopslag

Tabel 3.1: Specificaties van Bulwark in één oogopslag

Specificatie	Beschrijving
Ticker	BWK
Algoritme	NIST5
RPC-poort	52541
P2P-poort	52543
Block-tijd	90 seconden
Difficulty-algoritme	Dark Gravity Wave v3.0
Block-grootte	1MB
Mined/Minted Maturity	67 Blocks (~100 minuten)
Bevestiging	6 Blocks (~9 minuten)
Circulatie (na 1 jaar)	14,505,720 BWK
Circulatie (na 5 jaar)	27,668,220 BWK
PoW-periode	*nHeight* ≤ 345,600
PoS-periode	*nHeight* ≥ 345,601
Protocol-ondersteuning	IPV4, IPV6, TOR
PoS	Blackcoin v3.0 PoS, PIVX SeeSaw-beloningen

3.2 SlowStart

We hebben voorzien in de eerlijke start middels de volgende code (credit *ZCash*):

```
int64_t nSlowSubsidy = 50 * COIN;

if (nHeight < 960 / 2) {      // If block height less than 480,
    nSlowSubsidy /= 960;            // Set nSubsidy to .05208333
    nSlowSubsidy *= nHeight;  // Multiply present height by .05208333
} else if (nHeight < 960 {    // ex: Block 200, BR will be 10.41666600
    nSlowSubsidy /= 960;            // Credits: ZCASH Team
    nSlowSubsidy *= nHeight;
```

3.3 Dark Gravity Wave 3.0

Dark Gravity Wave wordt door Bulwark vanaf de start gebruikt als methode om de PoW-difficulty in te regelen. Het gebruikt een eenvoudig gewogen gemiddelde dat kan omgaan met grote toe- of afname van rekenkracht binnen een aantal blocks. Dit verzacht het 'stuck block effect', doorgaans veroorzaakt door multi-pools, en oorkomt dat een persoon in één keer meerdere blocks kan oplossen door een grote hoeveelheid rekenkracht toe te voegen.

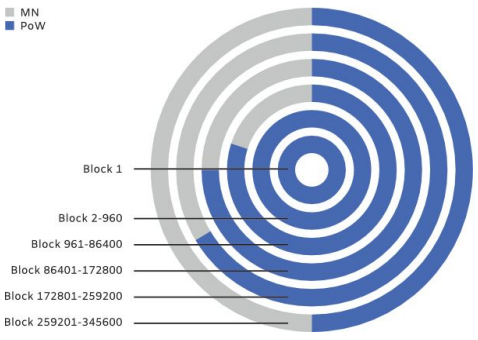
Hoofdstuk 4

Block-beloningen

4.1 Block-beloningen voor Proof of Work

Tabel 4.1: Specificatie periodes van PoW-block-beloningen

Beloning	Block	PoW	MN	Circulatie
489720	1	100%	-	489200
~25 (gem.)	2-960	100%	-	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



Figuur 4.1: Periodes van PoW-block-beloningen

4.2 Block-beloningen voor Proof of Stake

Tabel 4.2: Specificatie periodes van PoS-block-beloningen

Beloning	Block	Budget	PoS/Masternode	Opmerking
25.000	345601-432000	10%	SeeSaw	Jaar 2
21.875	432001-518400	10%	SeeSaw	Jaar 2
18.750	518401-604800	10%	SeeSaw	Jaar 2
15.625	604801-691200	10%	SeeSaw	Jaar 2
10.250	691201-777600	10%	SeeSaw	Jaar 3
10.938	777601-864000	10%	SeeSaw	Jaar 3
9.3750	864001-950400	10%	SeeSaw	Jaar 3
7.8120	950401-1036800	10%	SeeSaw	Jaar 3
6.2500	1036801-1123200	10%	SeeSaw	Jaar 4
5.4690	1123201-1209600	10%	SeeSaw	Jaar 4
4.6880	1209601-1296000	10%	SeeSaw	Jaar 4
3.9060	1296000-1382400	10%	SeeSaw	Jaar 4
3.1250	1382401-1468800	10%	SeeSaw	Jaar 5
2.7340	1468801-1555200	10%	SeeSaw	Jaar 5
2.3440	1555201-1641600	10%	SeeSaw	Jaar 5
1.9530	1641601-1728000	10%	SeeSaw	Jaar 5
1.6250	1728000+	10%	SeeSaw	Voor altijd

Hoofdstuk 5

NIST5 Hashing

5.1 Waarom NIST5?

Populair geworden door TalkCoin in 2014, is het NIST5 hashing-algoritme beperkt mainstream gebruikt. NIST5 kan gemined worden op een groot scala van consumentenhardware, waaronder CPU's en GPU's van AMD en NVIDIA. NIST5 is niet zo ASIC-resistent als sommige andere aan geheugen gebonden algoritmes, maar we geloven dat de trade-off acceptabel is: een hogere stabiliteit en een lager stroomverbruik. Mocht het zo zijn dat er via firmware updates NIST5-ondersteuning wordt toegevoegd aan ASICs, voor het einde van onze PoW-periode, zijn we (voor)bereid om een alternatief algoritme als vervanging van NIST5 te gebruiken. Mocht het zo ver komen, betrekken we onze community daar uiteraard bij. We gaan er vanuit dat onze korte PoW-periode, en onze bereidheid van algoritme te veranderen, de stimulans om met firmware-updates te komen bij ASIC-fabrikanten wegneemt.

5.2 De vijf finalisten (NIST SHA-3 Competition)

De vijf hashing-algoritmes die NIST5 vormen, zijn de finalisten van de NIST Hashing Competition (Chang et al. 2012). De algoritmes zijn (op volgorde van de manier waarop blocks gehased worden):

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

5.3 De nieuwe SHA-3 standaard

Keccak is uiteindelijk na de laatste ronde benoemd tot nieuwe SHA-3 hashing-functie, waar de andere vier algoritmes (ondanks dat ze cryptografisch gezien veilig zijn) een klein aantal punten verloren op een klein aantal technische details. We geloven dat we met de combinatie van de nieuwe SHA-3 standaard en de andere finalisten, een snel, veilig en gevestigd hashing-algoritme gekozen hebben.

5.4 Beschikbare mining-software

Op het moment van schrijven, zijn er verschillende opties voor miners:

Naam	Platform	Link
SGMiner-5.0	OpenCL	GitHub
ccminer-2.2.2	CUDA	GitHub
cpuminer-opt	CPU	GitHub

Hoofdstuk 6

Features

6.1 Masternodes

Masternodes zijn, in essentie, een gedecentraliseerd web van computers die als Bulwark-netwerk dienen. Masternodes voeren belangrijke netwerkfuncties uit, en ontvangen een deel van de block-beloningen. Ze dienen het Bulwark-ecosysteem door het aanbod van de munt te stabiliseren, transacties te verwerken en het netwerk te beveiligen. Masternodes vereisen 5000 BWK en technische kennis om te bedienen. Elke wallet (portemonnee) met minimaal 5000 BTW kan een masternode oprichten.

6.2 Obfuscatie / Coin Mixing

Bulwark gebruikt 'Obfuscation' (obfuscatie, opzettelijk verwarren, vervagen, vertroebelen), gebaseerd op CoinJoin, maar met verschillende verbeteringen ten opzichte van het origineel. Het wordt toegepast via Coin Mixing (muntvermenging); gedecentraliseerd en gefaciliteerd door het netwerk van masternodes. Dit zorgt voor een extra laag privacy in transacties. Het is niet perfect anoniem, maar obfuscatie met muntvermenging is veel beter dan de standaard Bitcoin-transactie. Ter illustratie: alle Bitcoin-transacties zijn transparant. Voor Bulwark, een slechte actor zou 50% van alle masternodes onder controle moeten hebben om minder dan 0.5% kans te hebben om een enkele transactie te de-anonimiseren na vermenging via 8 rondes van obfuscatie (Kiraly 2017b). Deze belangrijke feature biedt een hoog niveau van anonimiteit aan BWK-gebruikers die er voor kiezen om hun transacties te obfusceren.

6.3 SwiftTX

SwiftTX maakt mogelijk dat masternodes transacties kunnen vastzetten en biedt consensus-autoriteit over transacties. Als een transactie verzonden is naar het netwerk, wordt de transactie gevalideerd door een group masternodes. Als deze masternodes consensus bereiken over de validiteit van de transactie, wordt het vastgezet om later geïntroduceerd te worden in de blockchain. Dit verhoogt de transactie-snelheid aanzienlijk ten opzichte van conventionele systemen (zoals Bitcoin's block-tijd van 10 minuten met meerdere bevestigingen). SwiftTX maakt het mogelijk dat meerdere transacties plaatsvinden voordat een block op het netwerk gemined is met dezelfde invoer. Dit systeem is gebaseerd op Dash's InstantSend (Kiraly 2017a).

6.4 Sporks

Het Bulwark-netwerk gebruikt een gefaseerd fork-mechanisme, beter bekend als 'sporking'. Dit zorgt ervoor dat het BWK-netwerk nieuwe features kan implementeren, en de kans op een onbedoelde netwerk-fork minimaliseert tijdens het uitrollen van die nieuwe features. Spork-wijzigingen zijn in gebruik te nemen via het netwerk en kunnen aan- of uitgezet worden zonder dat node-software geüpdate hoeft te worden (strophy 2017). Deze feature is extreem nuttig, en stelt het netwerk in staat om snel te reageren op beveiligingsrisico's of -problemen.

6.5 TOR & IPV6 Masternodes

Bulwark staat de gebruiker toe om een node of masternode vanaf een onion-adres of IPV6-adres te draaien. We hebben eraan gewerkt om volledige TOR-nodes toe te voegen, enerzijds om het TOR-netwerk te versterken, en anderzijds om de gebruiksvriendelijkheid van Bulwark in TOR-only modus te verbeteren. Een unieke feature van TOR masternode-ondersteuning is dat het mogelijk is om de masternode als verborgen TOR-service te opereren. TOR-nodes staan gebruikers met een stabiele internetverbinding toe om masternodes te bedienen buiten hun eigen thuisnetwerk, zonder de privacy-implicaties die het heeft om de locatie ervan te onthullen, of de gevaren die het heeft om het thuisnetwerk open te stellen voor een potentiële aanval.

6.6 Het belang van de community en het bestuurssysteem

De Bulwark-community is de belangrijkste factor achter langetermijn-succes van het project. De mogelijkheid om als community op een betekenisvolle manier invloed uit te kunnen oefenen op de munt is zeer belangrijk. Daarom zijn we van plan om, aan het eind van de PoW-fase, budget-superblocks te activeren op het netwerk. Deze superblocks, maandelijks betaald, stellen de community in staat om invloed uit te oefenen op alle aspecten van Bulwark's ontwikkeling, merk en community. Het vertragen van de activatie van dit systeem geeft ons tijd om het onderliggende framework dat nodig is voor een positieve gebruikerservaring te ontwikkelen, en om block-beloningen voor miners en masternodes te maximaliseren.

We gebruiken een gefaseerd proces voor het creëren en inbrengen van voorstellen. Elke stap moet volledig afgerond zijn. Een stap niet afronden, zorgt er zeer waarschijnlijk voor dat een voorstel niet geactiveerd wordt. Op hoofdlijnen zijn de stappen als volgt (voor verandering vatbaar):

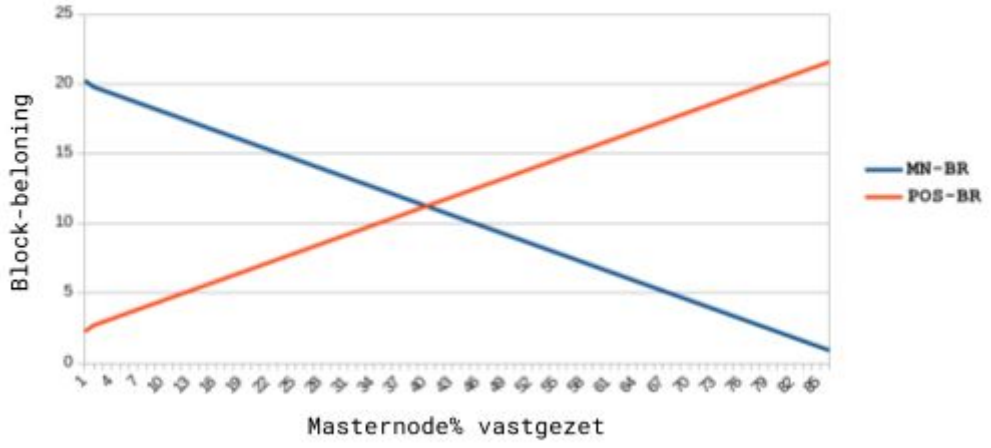
- Start in onze Discord-chat, en spreek met een aantal geroutineerde gebruikers. Peil interesse en als de reactie positief is, ga dan door naar de volgende fase.
- Gebruik meerdere social media platforms om te discussiëren en vraag feedback. Onthou dat Bulwark gebruikt wordt door verschillende mensen, die in meer of mindere mate betrokken zijn bij het bestuur van de munt. Waarschijnlijk heeft het wat voeten in de aarde om een deel van de gebruikers te bereiken. Noteer uitkomsten van de discussie, zodat je ze kunt citeren in het formele deel van het proces. Hoe meer citaten je kunt leveren, hoe beter.
- Sta open voor suggesties van de community en ontwikkelaars. Wees flexibel en sta ervoor open om andere ideeën en suggesties in je voorstel op te nemen.
- Maak een formeel voorstel op de Governance->Pre-Proposal-sectie op onze website. Lever citaten aan van alle discussies die zijn gevoerd in de vorige stap. Behandel je voorstel alsof het ter stemming wordt voorgelegd aan de blockchain.
- Na het afronden van deze stappen, stuur je het voorstel in aan de blockchain. Wees voorbereid op twee heffingen, één voor het insturen van het voorstel, en één voor het activeren van je voorstel op de blockchain (door een ontwikkelaar). Deze heffingen kan je niet terugvragen. De heffing voor het activeren van het voorstel wordt alleen betaald als het voorstel goedgekeurd en geactiveerd is.
- Het staat iedereen vrij om deze heffingskosten op te nemen in het voorstel. Maak in het voorstel duidelijk dat dit onderdeel is van de verzochte bezoldiging.

- Zorg ervoor dat je terugkoppeling geeft aan iedereen die je het gesproken over het voorstel, zodat erop gestemd wordt. Om een voorstel uitbetaald te krijgen, moet minimaal 10% van de (beroepbare) masternodes 'ja' gestemd hebben op het voorstel. Het proces om 10% consensus te verkijrgen kan lastiger zijn dan het klinkt, dus wees informatief en respectvol in het aanvragen van de benodigde stemmen.

6.7 SeeSaw PoS/Masternode-beloningen

We hebben besloten om het SeeSaw-beloningssysteem te gebruiken, populair geworden door PIVX (jakiman 2017). Het SeeSaw-beloningssysteem begint met een 9:1 block-beloning ratio (in het voordeel van masternodes). Daarna wordt de ratio evenwichtig aangepast tussen staking- en node-operators, totdat ongeveer 41.5% van de munten in circulatie vergrendeld is in masternodes. Op dat moment is de beloning voor staking iets voordeliger dan de beloning voor masternodes. De reden dat we staking iets voordeliger maken, is dat we problemen zoals wisselvalligheid van de prijs en lage liquiditeit willen ontlopen. Munten die een hoog percentage van het aanbod vergrendeld hebben in nodes kunnen daar gevoelig voor zijn. Deze strategie beperkt frustratie over toegang tot het munt-aanbod bij gebruikers, en onderhoud de relevantie van ons robuuste netwerk. Aangezien het één van onze doelen is om een breed ondersteund platform te worden voor anonieme handel, is het kunnen uitvoeren van transacties van groot belang voor diegene die Bulwark accepteren en gebruiken.

Fig 3. SeeSaw @ hoogte 3456 - 432000
(na budget-percentage)



Hoofdstuk 7

De toekomst

7.1 De Bulwark Tool Chest

Een collectie van code snippets, API's, libraries, scripts en kennis, met als doel om een bazaar-achtige omgeving te ontwikkelen. Daar kunnen ontwikkelaars die cryptocurrency-ondersteuning in hun projecten willen inbouwen kennis, informatie en code uitwisselen. We zien hierin een vergelijking met het werk van een timmerman; om opwindende en grootse projecten te creëren, zijn goede tools nodig. Wij willen ontwikkelaars daarin graag voorzien.

7.2 Privacy- en software-verbeteringen

We zetten er ons voor in om ons nieuwe protocollen eigen te maken, die de privacy van onze gebruikers verbeteren. Er zijn diverse paden die we op dit moment evalueren, en zijn van plan om te starten met interne tests en ontwikkeling in de eerste helft van 2018. Sommige van deze verbeteringen zijn:

- I2P privacy netwerk
- Zerocoin-protocol, of Stealth-addressing (als we vertrouwen op de volwassenheid van deze oplossing)
- Synchroniseren van onze codebase met die van de Bitcoin
- Stroomlijnen en updaten van de QT-wallet
- Libtox-integratie
- Virtualisatie van de Bulwark-wallet (portemonnee), als extra beveiligingslaag

7.3 Bulwark Secure Home Node

We gaan samenwerken met CAD-specialisten om een kleine, op zichzelf staande, Bulwark-node te ontwerpen voor thuis. Gebruikers kunnen ermee met hun thuisnetwerk verbinden en de node configureren met een Web UI. We zijn van plan met de volgende functionaliteiten te lanceren:

- Voor mensen met een stabiele internetverbinding, een eenvoudig op te zetten onionized masternode (of full node), met gebruik van TOR's hidden services.
- De mogelijkheid om te dienen als TOR relay, ter verbetering van het TOR-netwerk.
- VPN en/of proxy die kan worden gebruikt om verkeer op het thuisnetwerk door het TOR/I2P-netwerk te leiden.
- Bulwark-staking door middel van virtualisatie of een add-on apparaat.

In de geest van decentralisatie, publiceren we bestanden voor 3D-printers (inclusief alle broncode), zodat leden van de community het thuis kunnen printen en monteren.

7.4 Uitbreiding van ons merk

We gaan verder met het uitbreiden van ons merk, en zijn va plan om samen te werken met verkopers van hardware en systeem-integrators met wie wij dezelfde passie en idealen delen. Over 5 jaar willen we dat de naam 'Bulwark' niet alleen synoniem staat met de cryptovaluta, maar ook met privacy, veiligheid en respect voor de vrijheid van gebruikers. Bulwark's hoofddoel is het voorzien van keuzevrijheid door middel van privacy.

7.5 Design en grafische vormgeving

Door middel van onderzoek en ontwikkeling, streven we ernaar om een stijl neer te zetten voor Bulwark die het onderscheid van zijn concurrenten in de crypto-markt. Ons designteam is van plan te innoveren en experimenteren met de huidige UI/UX/branding, met als doel om een excellent design en stijlgids te ontwikkelen. In het kader daarvan zoeken we continue naar het medium dat de beste gebruiksvriendelijkheid biedt, en gepaard gaat met innovatieve en mooie esthetiek. Dit doen we door onderzoek te doen naar onze concurrentie, op de hoogte te blijven van technologische trends en standaarden, en er continue naar te streven nieuwe design-elementen te brengen naar onze eindgebruikers.

Hoofdstuk 8

Conclusie

8.1 Samenvatting

Bulwark is een munt die op privacy is georiënteerd, met masternodes, bestuur, en een evoluerend ecosysteem van tools. Het project begon met een eerlijke lancering, en een focus op een wijdverspreide muntdistributie. De langzame en doordachtzame start, het splitsen van block-beloningen, en het hashing-algoritme zijn bewust geselecteerd om kansen te creëren voor significante community-participatie. Bulwark is gelanceerd met verschillende belangrijke privacy-features, en het team van ontwikkelaars is hard bezig met de introductie van nieuwe features, en het voortbouwen van en op huidige technologieën. Bulwark heeft als hoofddoel om in keuzevrijheid te voorzien door middel van privacy, en zal zich zeer inspannen om dat te bereiken.

8.2 Toekomstig werk

Het ecosysteem van privacy-munten met masternodes is recent onder water gezet door munten die gebruikers aantrekken met beloftes van een substantieel rendement op investeringen, gigantische roadmaps gevuld met onwaarschijnlijke producten, en een focus op marketing, in plaats van echte verbetering in het ecosysteem. Bulwark heeft zich voorgenomen anders te zijn: we beperken het creëren van hype, en richten ons op echte creatie. Van huidige en toekomstige doelen van dit project vinden we het belangrijk dat ze specifiek. meetbaar, haalbaar, relevant en tijdsgebonden zijn.

Referenties

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

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

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

Chang, S.-J., Perlner, R., Burr, W.E., Turan, M.S., et al., 2012. Third-round report of the sha-3 cryptographic hash algorithm competition. Beschikbaar op: http://nvlpubs.nist.gov/nistpubs/ir/2012/ NIST.IR.7896.pdf.

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

Ferguson, N.L., Schneier, S., Whiting, B., Bellare, D., et al., 2010. The skein hash function family. Beschikbaar op: 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. Beschikbaar op: http://www.groestl.info/Groestl.pdf.

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

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

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

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

Okupski, K., 2016. Bitcoin developer reference., pp.3–4. Beschikbaar op: https://lopp.net/pdf/Bitcoin_ Developer_Reference.pdf.

strophy, 2017. Understanding sporks. Beschikbaar op: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/128319489/Understanding+Sporks.

Wiecko, R., 2017. Dash instamine issue clari cation. Beschikbaar op: https://dashpay.atlassian.net/wiki/ spaces/OC/pages/19759164/Dash+Instamine+Issue+Clarification.

Wu, H., 2012. The hash function jh. Beschikbaar op: http://www3.ntu.edu.sg/home/wuhj/research/jh/ jh_round3.pdf.