BULWARK

CRYPTOCURRENCY

Whitepaper de Moeda Criptográfica

Equipa Principal da Bulwark:

Eatbatterys (Coordenado de Projeto)

Jack (Diretor Marketing)

SerfyWerfy (Desenvolvedor de Cadeia de Blocos)

Frogman (Líder de Comunicação)

Patrick (Design e Marca)

Stu (Desenvolvedor de Ecossistema)

A Equipa Principal da Bulwark

Dezembro de 2017

Nós, a Equipa Principal da Bulwark, confirmamos que o trabalho presente neste relatório branco é nosso. Onde a informação foi derivada de outras fontes, confirmamos que isto foi indicado nas atribuições.

Resumo

A Bulwark (sigla: BWK) é uma moeda orientada para a comunidade, nascida a partir de observações feitas a práticas geralmente injustas dentro do espaço de privacidade da moeda de mastenode. A nossa estratégia de lançamento justa e deliberada, oferece aos participantes a oportunidade de se juntarem a um projeto promissor ainda no seu início. Nós oferecemos uma proposição de valor simples sem grandes promessas: Oferecemos uma moeda de envio privado que funciona hoje e no futuro aproveitando as melhores práticas tanto da DASH como da PIVX. Sem visões fantasiosas e com uma perspectiva limitada de entrega, mas uma moeda funcional numa plataforma de trabalho com suporte para o futuro. Isto não significa que não estamos a planear qualquer inovação, mas sim resultados em vez de grandes expetativas. Existem demasiadas moedas que são alimentadas por expetativas – mas completamente isentas de conteúdo – e nós não queremos fazer parte do crescimento de moedas guiadas pelo mote de fazer promessas que não podem cumprir. Sem ICO, uma rampa de lançamento suave, quantidade de moedas já mineradas pequenas, e alocações de recompensas de blocos favorecidas a mineiros, os adotantes da Bulwark terão acesso completo a uma moeda de privacidade oferecendo uma mistura de masternodes e a melhor tecnologia de privacidade disponível, juntamente a um roteiro de desenvolvimento significativo. As Masternodes estarão disponíveis, e a funcionar, no lançamento e são uma parte fundamental da visão desta moeda e irão estabilizar a circulação, proteger a rede, e fornecer funcionalidades importantes.

Agradecimentos

A Bulwark não teria sido possível sem os trabalhos iniciais das respetivas equipas da Bitcoin, Peercoin, Blackcoin, Talkcoin, Dash e PIVX. Os Softwares de código aberto e os seus contribuidores estão constantemente a abrir caminho em direção a novas e excitantes inovações. Quando a informação e o conhecimento são livres de se construir, a sociedade beneficia como um todo. Agradecemos aos nossos antecessores pela oportunidade de contribuir no crescimento do escossistema.

Índice

Capítulo1

Breve Introdução à Moeda Criptográfica

1.1 Experiência

Em 2009, Satoshi Nakamoto lançou um artigo intitulado *Bitcoin: A Peer-to-Peer Electronic Cash System* detalhando a sua visão do comércio. A visão de Nakamoto, era essencialmente a de um sistema monetário pessoa-para-pessoa sustentado por uma prova de trabalho baseada em hash. A rede iria registar transações, levando-as a um ledger contínuo que não podia ser alterado sem refazer a prova de trabalho. Os nodes iriam escolher a maior cadeia como prova de eventos testemunhados pela maior grupo de poder de hash. Desde que ≥ 51% do poder de hash da rede seja controlado por nodes que não pretendem facilitar um ataque, a cadeia que eles geram irá permanecer como a mais longa (Nakamoto 2009).

1.2 O Bloco (Block)

Cada bloco na rede é precedido por um cabeçalho de 80 bytes que contém, uma cópia hashed dupla do SHA256 pertencente ao cabeçalho do bloco anterior, a ávore de merkle (uma derivação dupla do SHA256 de todos os hashes que ocorreram no bloco), a hora em que começou a prova de trabalho, a dificuldade de atingir o hash deste cabeçalho deve ser inferiour ou igual a, e o nonce (número que apenas pode ser utilizado uma única vez) de quais mineiros chegaram à dificuladde pretendida. Qualquer tentativa de modificar uma transação no bloco, irá resultar na rejeição do bloco pelos mineiros da rede. (Bitcoin Core Team 2017).

1.3 A Cadeia de Blocos (Blockchain)

Grupos de transações são formados em blocos e esses blocos são colocados cronologicamente na cadeia de blocos. A cadeia de blocos cria um histórico em movimento de toda a atividade dentro da rede e serve como um modelo de consenso distribuído onde qualquer transação pode ser verificada a qualquer altura. (Crosby et al. 2015).

1.4 Prova de Trabalho (Proof-Of-Work)

A Prova de Trabalho é um sistema de verificação onde mineiros devem aplicar recursos tangíveis (eletrecidade, custo de hardware) para resolver um puzzle arbitrário de palavras probabilísticas. (Okupski 2016).

Capítulo 2

Apresentando a Bulwark

2.1 Uma base sólida

Cada casa precisa de uma base sólida, e a Bulwark não é diferente. A Bulwark é construída sobre *PIVX*, que é construído com base na popular moeda criptográfica *DASH*. Enquanto que as linhagens podem ser seguidas até ao Satoshi Core original, cada projeto escolheu uma direção indivídual com objetivos e ideias que representam as comunidades que servem. Vamos ampliar e colocar em ênfase, os recursos da moeda de privacidade das nossas plataformas antecessoras, explorando novas tecnologias, ao criar conjuntos de ferramentas e oportunidades para a integração da Bulwark nas plataformas tecnológicas atuais.

2.2 Uma equipa dedicada à comunidade

Para alguns projetos, as comunidades são uma opinião tardia. A prioridade número um da Bulwark é a comunidade. Com giveaways, concursos, uma plataforma de discussão animada e uma política de tolerância zero para o assédio dos recém-chegados, a Bulwark esforça-se para ser a moeda criptográfica para todas as variedades de utilizadores finais.

2.3 Justa e equilibrada

No momento da escrita, houve um influxo de moedas criptográficas utilizadoras da mesma base. Embora a tecnologia subjacente seja sólida, uma examinação mais profunda das suas especificações e parâmetros da cadeia de blocos revelam práticas menos justas.

2.4 O problema com práticas de pré-mineração

2.4.1 Caso de estudo: FooBarBazCoin

Uma tendência crescente no espaço de moedas criptográficas é, escolher uma data arbitrária no futuro, e em seguida basear uma percentagem de pré-mineração no stock em circulação a partir dessa data. Vamos dar uma vista de olhos no FBC (*FooBarBaz Coin*) fictício, uma bifurcação (fork) da *DASH*.

- Prémio por Bloco: 15
- Tempo de Bloco: 2.5 minutos
- POW/Masternode Split: 50/50%
- Algorítmo de dificuldate inicial: KGW
- Subsídio diminui 12% a cada ano

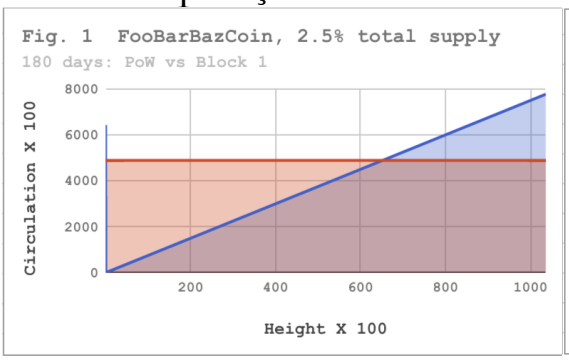
- Stock máximo da moeda: ~25 Milhões
- 2.5% de pré-mineração

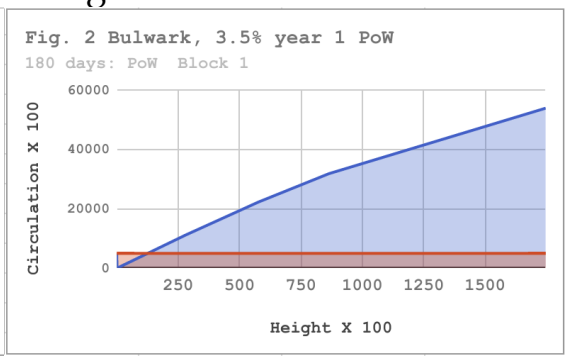
Neste exemplo, uma pré-mineração anunciada de 2.5%, que equivale a ~ 643,000 moedas (num total de ~ 25 milhões) parece razoável para o observador comum. No entanto, para que as recompensas de PoW e Masternode correspondam às moedas que os desenvolvedores possuem, demoraria aproximadamente 43,000 blocos. Com um objetivo de 2,5 minutos por bloco, demoraria cerca de 150 dias aos mineiros (ou 75 dias no geral) para gerar a mesma quantidade de moedas. Após 75 dias, os desenvolvedores ainda controlariam metade das moedas existentes.

2.5 Uma alternativa mais justa

A equipa da Bulwark reconheceu isso, e decidiu ser frontal. A nossa pré-mineraçao de 489,720 moedas (3.5%) representa pouco mais de 12 dias de mineração ou pouco mais de 10 dias de produção total. Esperançosamente isto servirá para incutir uma paz de espírito na comunidade que, ao fim de certo ponto, o mercado não pode ser significativamente desvalorizado devido às moedas detidas pela equipa equipa principal. Como pode ver nos gráficos em baixo, ambos representando 180 dias em cada cenário, a diferença é bastante clara. Esperamos que ao abordar o assunto de forma franca, crie precêdencia e sirva para beneficier a comunidade como um todo.

2.5.1 Comparaçao de ambas as abordagens





2.5.2 Instamine e a nossa abordagem

A Dash (Darkcoin) apresenta um caso de estudo interessante sobre a necessidade de proteção de instamine. Quase 10-15% de todo o stock da Dash foi criado nos primeiros dias de existência, graças a alguns utilizadores empreendedores (Wiecko 2017).

A nossa abordagem à questão da instamine foi dupla. Nós utilizamos um subsídio lento, em que os primeiros 960 blocos (1 dia) foram linearmente aumentando até a recompensa máxima do bloco, com 100% das recompensas do bloco serem para os mineiros naquele dia também. Historicamente, isto foi abordado por uma pequena recompensa de bloco que muda de repente, a uma certa altura muda para um bloco de recompensa máxima, contudo, muitas vezes isto resultou em piscinas (pools) serem deliberadamente DDoSed ou sobrecarregadas com novo tráfego de mineração. Com uma recompensa aumentada

linearmente, não haveria qualquer razão para interferir com mineiros ou operadores de piscinas por ganho monetário.

2.5.3 Admitamos, no momento da escrita, estamos constantemente a ser bombardeados

com ICOs. Enquanto elas têm o seu legítimo lugar no ecossistema das moeda criptográicas, muitas vezes elas só servem para criar bolsas de riqueza concentradas. Considerando que a Bulwark tanto oferece recompensas de Masternodes, e numa segunda fase, recompensas de prova de trabalho (PoS), esta concentração de riqueza pode causar grandes desvios no mercado e inclina fortemente o sistema de governo a favor dos mais antigos (e ricos) adotantes.

2.6 Rápida e funcional

Com um tempo de bloco de 90 segundos, consenso de masternode e bloqueio de transações, cronograma de emissões razoável e staking eco-amigável, a Bulwark aspira a ser uma moeda criptográfica verdadeiramente rápida e funcional.

Capítulo 3

Nossos Parâmetros da Cadeia de Blocos

3.1 das Especificações da Bulwark

Tabela 3.1: Resumo das Especificações da Bulwark

Especificação	Descritor
Ticker	BWK
Algorítmo	NIST5
Porta RPC	52541
Porta P2P	52543
Espaçamento de Bloco	90 Segundos
Algorítmo de Dificuldade	Dark Gravity Wave v3.0
Tamanho de Bloco	1MB
Maturidade de Mineradas	67 Blocos (~100 Minutos)
Confirmação	6 Blocos (~9 Minutos)
Circulação (1 Ano)	14,505,720 BWK
Circulação (5 Anos)	27,668,220 BWK
Período de PoW	*nHeight* ≤ 345,600
Período de PoS	*nHeight* ≥ 345,601
Protocolo de Suporte	IPV4, IPV6, TOR
PoS	Blackcoin v3.0 PoS, Recompensas PIVX SeeSaw

3.2 SlowStart

O nosso início justo é fornecido com o seguinte código (crédito *Zcash*):

```
int64_t nSlowSubsidy = 50 * COIN;

if (nHeight < 960 / 2) {      // Se altura do bloco é inferior a 480,
    nSlowSubsidy /= 960;            // Meta nSubsidy como .05208333
    nSlowSubsidy *= nHeight;  // Multiplique a altura em .05208333
} else if (nHeight < 960 {    // ex: Bloco 200, RB será 10.41666600
    nSlowSubsidy /= 960;            // Créditos: Equipa da ZCASH
```

```
nSlowSubsidy *= nHeight;
```

3.3 Dark Gravity Wave 3.0

A Dark Gravity é empregada pela Bulwark desde o início, como um método de mudar a dificuldade da PoW. Usa uma simples média móvel, que pode responder a grandes aumentos ou quedas de nethash em apenas alguns blocos. Isso alivía o "stuck block effect" normalmente causado por multipools e previne uma pessoa, que adicione uma quantidade substancial de poder de computaç ão, de resolver instantaneamente mais do que alguns blocos.

Capítulo 4

Recompensas de Bloco

4.1 Recompensa de Bloco PoW

Tabela: Especificações do Período da Recompensa de Bloco PoW

Subsídio	Bloco	PoW	MN	Circulação
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

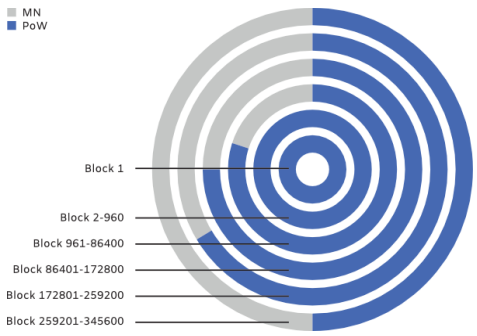


Figure 4.1: Período da Recompensa de Bloco PoW

4.2 Recompensa de Bloco PoS

Tabela 4.2: Especificações do Período da Recompensa de Bloco PoS

Subsídio	Bloco	Orçamento	PoS/Masternode	Note
25.000	345601-432000	10%	SeeSaw	Ano 2

21.875	432001-518400	10%	SeeSaw	Ano 2
18.750	518401-604800	10%	SeeSaw	Ano 2
15.625	604801-691200	10%	SeeSaw	Ano 2
10.250	691201-777600	10%	SeeSaw	Ano 3
10.938	777601-864000	10%	SeeSaw	Ano 3
9.3750	864001-950400	10%	SeeSaw	Ano 3
7.8120	950401-1036800	10%	SeeSaw	Ano 3
6.2500	1036801-1123200	10%	SeeSaw	Ano 4
5.4690	1123201-1209600	10%	SeeSaw	Ano 4
4.6880	1209601-1296000	10%	SeeSaw	Ano 4
3.9060	1296000-1382400	10%	SeeSaw	Ano 4
3.1250	1382401-1468800	10%	SeeSaw	Ano 5
2.7340	1468801-1555200	10%	SeeSaw	Ano 5
2.3440	1555201-1641600	10%	SeeSaw	Ano 5
1.9530	1641601-1728000	10%	SeeSaw	Ano 5
1.6250	1728000+	10%	SeeSaw	Daí em diante

Capítulo 5

NIST5 Hashing

5.1 Porquê NIST5

Popularizado pelo TalkCoin em 2014, o algorítmo de hashing NIST5 obteve um uso modesto. NIST5 pode ser minerado numa vasta gama de hardware para consumidores normais, incluindo CPUs, assim como GPUs AMD e Nvidia. O NIST5 não é tão resistente à ASIC como outros algorítmos de memória rígida, mas acreditamos que os benefícios que traz são aceitáveis para melhorar a estabilidade do sistema e reduzir o consumo de energia relativo a esses algorítmos de memória rígida. No caso de surgirem atualizações de firmware, para dar suporte de NIST5 às ASICs antes do final do nosso período PoW, estamos preparados com um algorítmo alternativo como substituto. Iremos pedir que a comunidade vote sobre o curso de ação (se existir) e implementaremos de acordo. Sentimos que o nosso curto período de PoW e a vontade de mudar de algorítmos, desincentivem os fabricantes de ASIC e não prevêem problemas futuros.

5.2 ã

Os cinco algorítmos de hashing que compõem o NIST5 são os finalistas da Competição de Hashing do NIST (Chang et al., 2012). Eles são: (na ordem em que os blocos são hashed)
Blake (Aumasson 2013), **Grøstl** (Gauravaram1 et al. 2012), **JH** (Wu 2012), **Keccak** (Bertoni et al. 2012), e **Skein** (Ferguson et al. 2010).

5.3

Keccak eventualmente passou à ronda final, para ser a nova função de hasing SHA-3, enquanto os restantes algorítmos (mesmo sendo considerados criptograficamente seguros) perderam alguns pontos dos juízes, devido a pequenos problemas técnicos. Nós acreditamos que a conbinação do novo SHA-3 Standard juntamente com as escolhas dos outros finalistas, permitem um rápido, seguro e estabelecido algorítmo de hashing.

5.4 de Mineração Disponível

Na altura da escrita, existem várias opções para os mineiros:

Nome	Plataforma	Link
SGMiner-5.0	OpenCL	
ccminer-2.2.2	CUDA	
cpuminer-opt	CPU	

Chapter 6

Destaques

6.1 Masternodes

As Masternodes são, essencialmente, uma rede descentralizada de computadores que servem a rede da Bulwark. As Masternodes desempenham funções de rede importantes e por isso, recebem parte da recompensa dos blocos. Elas servem o ecossistema da Bulwark, estabilizando o stock de moedas, processando transações e protegendo a rede. Para criar uma Masternode, são necessários 5000 BWK e um conhecimento técnico modesto para operar. Qualquer carteira que possua 5000 BWK pode configurar uma masternode.

6.2 Obfuscation / Mistura de Moedas

A Bulwark apresenta a Obfuscation, baseada na CoinJoin, mas com várias melhorias em relação ao original e feito através de mistura de moedas de forma descentralizada, facilitada pela rede de masternodes. Isto garante uma camada adicional de privacidade nas transações. Embora não seja perfeitamente anónima, a Obfuscation através de mistura de nós (nodes) é muito melhor que as transações padrão da Bitcoin. Por exemplo, todas as transações da Bitcoin são transparentes. Para a Bulwark, um ator nefasto, tinha de controlar 50% das masternodes operacionais, para ter uma hipótese inferior a 0.5%, de tornar uma única transação pública, que foi misturada com 8 rndas de Obfuscation (Kiraly 2017b). Esta importante caraterística, permite um alto nível de anonimato aos utilizadores da BWK, que optam por ofuscar as suas transações.

6.3 SwiftTX

A SwiftTX fornece masternodes com autorização de bloqueio e consenso para transações. Quando uma transação é submetida para a rede, um grupo de masternodes irá validar a transação. Se essas masternodes chegarem a um consenso na validade da transação, ela será bloqueada para uma posterior introdução na cadeia de blocos, aumentando consideravelmente a velocidade de transação, comparativamente à velocidade de transação de sistemas convencionais (como os tempos de bloco de 10 minutos com múltiplas confirmações da Bitcoin). A SwiftTX possibilita que múltiplas transações ocorram, antes que um bloco na rede seja minado com as mesmas entradas. Este sistema é baseado no InstantSend da Dash (Kiraly 2017

6.4 Sporks

A rede Bulwark utiliza o mecanismo de múltiplas fases de fork chamado "sporking". Isto irá permitir que a rede BWK implemente novos funções, minimizando as chances de um fork de rede não desejado, durante a implantação. As mudanças de Spork são implantáveis através da rede e podem ser ativadas e desativadas, quando necessário, sem necessidade de atualizações de software de node (strophy 2017). Esta função é extremamente útil e permite que a rede reaja rapidamente às vulnerabilidades de segurança.

6.5 Masternodes TOR & IPV6

A Bulwark permite que o utilizador execute seu node completo ou masternode, tanto de um endereço de onion ou um endereço IPV6. Trabalhamos para adicionar nodes de TOR completos, para fortalecer a própria rede TOR e a experiência do utilizador da Bulwark operando apenas em modo TOR. Uma característica única do suporte de TOR masternode é poder operar a sua masternode como um serviço de TOR escondido. Os nodes de TOR permitem que os utilizadores com conexões de internet estáveis, possam operar as masternodes fora da sua rede doméstica sem as implicações de privacidade de revelar sua localização ou os perigos de expor a sua rede doméstica a um potencial ataque ou compromisso.

6.6 Importância da Comunidade e o Sistema de Governo

A comunidade da Bulwark é o fator mais importante por de trás do sucesso a longo prazo do projeto, e sua capacidade de influenciar significativamente o futuro da moeda é primordial. Como tal, no final da fase PoW pretendemos ativar superblocos de orçamento na rede. Estes superblocos, pagos mensalmente, permitirão à comunidade exercer um controle significativo sobre todos os aspectos de desenvolvimento da Bulwark, presença da marca e assuntos comunitários. Ao atrasar a ativação deste sistema, teremos tempo suficiente para desenvolver a estrutura subjacente necessária para uma experiência positiva por parte do utilizador, de forma a maximizar as recompensas de blocos disponíveis, tanto para mineiros como masternodes.

Vamos utilizar um processo composto por várias fases para criar e enviar propostas. Cada etapa precisa de ser totalmente concluída. Se uma das etapas descritas falhar, provavelmente resultará numa proposta que não será ativada. Uma ideia básica dessas etapas seria algo como o descrito em baixo:

- Comece no chat do nosso Discord, e fale com alguns dos nossos utilizadores experientes. Gere interesse e se a resposta por positiva, siga para a próxima fase.
- Utilize várias plataformas de redes sociais para discutir e obter feedback. Lembre-se que a Bulwark tem uma base de utilizadores bastante diversificada e diferentes níveis de participação na governo, por isso, alcançar uma parte da base de utilizadores, muitas vezes exigirá trabalho duro.
- Seja aberto a sugestões da comunidade e dos desenvolvedores. Seja flexível e disposto a incorporar ideias e sugestões externas na sua proposta.
- Crie uma pré-proposta formal na seção Governo (Governance) -> Pré-proposta (Pre-Proposal) do nosso site. Forneça citações de todas as discussões que ocorreram no passo anterior. Trate da sua pré-proposta como se fosse submetida à cadeia de blocos para votação.
- Após a conclusão destas etapas, envie a sua proposta para a cadeia de blocos. Esteja preparado para duas taxas, uma no momento da submissão e uma taxa de cédula paga ao desenvolvedor que ativa a sua proposta na cadeia de blocos. A taxa de inscrição não é reembolsável e a taxa de voto apenas será paga após a aprovação e ativação da sua proposta.
- Toda a gente é livre de ajustar a sua proposta de forma a incluir o custo de reembolso dessas duas taxas. Certifique-se de que, na sua proposta formal, você declara que está a adicionar o reembolso ao saldo solicitado.
- Certifique-se de voltar a entrar em contato com toda a gente que falou, de forma a que a sua ideia seja votada. Para que uma proposta seja paga, 10% das masternodes elegíveis devem votar "sim" na sua proposta. Este processo de obtenção de um

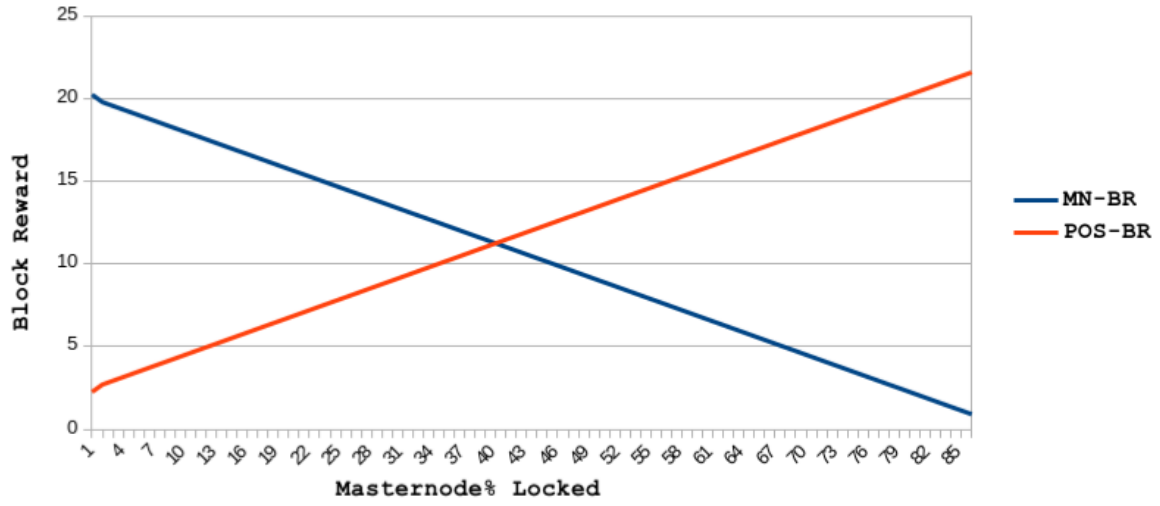
consenso de 10% pode ser bem mais difícil do que parece, portanto seja diligente, informativo e respeitoso na obtenção dos votos necessários para que sua proposta seja paga.

6.7

Decidimos utilizar o sistema de recompensas SeeSaw popularizado pela PIVX (jakiman 2017). O sistema de recompensa SeeSaw começa com uma proporção de recompensa de bloco de 9:1 (favorecendo masternodes) e ajusta suavemente a proporção de recompensa entre operadores de staking e de nodes até 41,5% das moedas em circulação serem bloqueadas em masternodes, momento em que as recompensas de staking atingem uma ligeira vantagem sobre as recompensas de masternode numa base moeda-por-moeda. A razão pela qual temos a SeeSaw, que favorece ligeiramente as recompensas de staking, é porque queremos evitar certos problemas problemas - como volatilidade de preços significativa e baixa liquidez – que têm impacto em moedas com percentagens muito altas de stock bloqueado em nodes. Esta estratégia mitiga a frustração do utilizador sobre o acesso ao stock de moedas e mantém a relevância da nossa rede robusta. Com um dos nossos objetivos, é ter uma plataforma bem apoiada para o comércio anônimo, a transactabilidade é de extrema importância para aqueles que aceitam o Bulwark e aqueles que seguram a Bulwark.

Fig 3. SeeSaw @ Height 345601 - 432000

(after budget percentage)



Capítulo 7
Futuro

7.1

Uma coleção de fragmentos de código, APIs, bibliotecas, scripts e conhecimento que servirão para formar um ambiente parecido a um bazar, onde os desenvolvedores que estão à procura da incorporação do suporte da criptografia nos seus projetos são livres de trocar conhecimento, informação e código. Acreditamos que ao oferecer aos desenvolvedores estas ferramentas, equivale a dar ao carpinteiro as ferramentas necessárias para criar projetos excitantes e magistrais.

7.2 e Aprimoramento do Software

Estamos empenhados em adotar novos protocolos que irão melhorar a privacidade da nossa base de utilizadores. Existem vários caminhos que estamos a avaliar neste momento e planeamos iniciar testes internos e desenvolvimento no primeiro semestre de 2018. Alguns desses aprimoramentos incluem:

- Rede de privacidade I2P.
- Protocolo Zerocoin ou endereçamento Stealth (Quando estivermos confiantes na maturidade da solução).
- Sincronizar o nosso código base mais próximo à linha principal da bitcoin.
- Racionalização / atualização da carteira QT.
- Integração da Libtox.
- Virtualização / contentorização da carteira da Bulwark para adicionar uma camada extra de segurança.

7.3 Bulwark Secure Home Node

Iremos trabalhar com especialistas em CAD para projetar um node de Bulwark pequeno, autónomo e doméstico. Os utilizadores conseguirão ligar e configurar isso à sua rede doméstica usando uma IU da Web. As funções que pretendemos lançar são as seguintes:

- Para aqueles com conexões de internet estáveis, é fácil de configurar a masternode totalmente onionizado (ou o node completo) usando serviços ocultos TOR.
- Opção de funcionar como um relé para melhorar a rede TOR geral.
- VPN e/ou proxy que podem ser utilizados para determinar o tráfego de Internet em casa através da rede TOR / I2P.
- Bulwark staking através de virtualização ou um dispositivo adicional.

Seguindo com o espírito da descentralização, os arquivos de impressão 3D e todo o código fonte estarão disponíveis para a comunidade para montagem em casa.

7.4 ã da nossa Marca

Continuaremos a ampliar a nossa marca e pretendemos trabalhar com fornecedores de hardware e integradores de sistemas que partilham a mesma paixão e ideais que fazemos. Dentro de cinco anos, queremos que o nome 'Bulwark' seja sinónimo não apenas de moeda criptográfica, mas também de privacidade, segurança e respeito pela liberdade de um utilizador. O principal objetivo da Bulwark é proporcionar liberdade de escolha através da privacidade.

7.5 Design e Visual

Através de Pesquisa e Desenvolvimento, pretendemos criar uma linguagem de design visual para a Bulwark que o distingue da concorrência no mercado de criptografia. A nossa equipa de design planeia inovar e experimentar o UI / UX / Branding atual de forma a conseguir obter o melhor design possível, procurando um local que permita a melhor experiência por parte do utilizador, aliada a uma estética bonita e inovadora. Isto será feito pesquisando pelos nossos concorrentes, mantendo-nos no topo das tendências e padrões tecnológicos atuais, trabalhando continuamente de forma a trazer novos e excitantes visuais aos utilizadores finais.

Capítulo 8

Conclusão

8.1 Sumário

A Bulwark é uma moeda orientada para privacidade das masternodes, governo e um ecossistema de ferramentas em evolução. O projeto começou com um lançamento justo e focado numa ampla distribuição de moeda. O início lento, a divisão de recompensas por bloco e o algorítmo de hashing foram deliberadamente selecionados para criar oportunidades para uma participação significativa por parte da comunidade. A Bulwark foi lançada com uma variedade de características importantes sobre a privacidade da moeda, e a equipa de desenvolvimento está a trabalhar fortemente de forma introduzir novas características e aproveitar as tecnologias existentes. A Bulwark pretende dar poder de escolha através da privacidade e concentrará grandes esforços nesse sentido.

8.2 Trabalho futuro

O ecossistema de privacidade da moeda da masternode foi recentemente inundado por moedas que procuravam atrair novos utilizadores através de promessas de retornos de investimento substanciais, mapas de objetivos enormes, cheios de promessas improváveis e um foco geral no marketing, em vez de uma melhoria real do espaço. A Bulwark planeia ser exatamente o oposto: baixa criação de hype juntamente com a criação de um produtal real. Os nossos objetivos atuais e futuros para o projeto seguirão a fórmula de serem específicos, mensuráveis, atingíveis, relevantes e vinculadoe ao tempo.

References

Aumasson, L.M., Jean-Phillipe Henzen, 2013. SHA-3 proposal: BLAKE. Disponível em: .

Bertoni, G., Daemen, J., Peeters, M. & Van Assche, G., 2012. The keccak sha-3 submission. Disponível em: .

Bitcoin Core Team, T., 2017. Bitcoin developer reference. Disponível em: .

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. Disponível em: .

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., et al., 2015. BlockChain technology. Disponível em: .

Ferguson, N.L., Schneier, S., Whiting, B., Bellare, D., et al., 2010. The skein hash function family. Disponível em: .

Gauravaram1, P., Knudsen, L.R., Matusiewicz, K., Mendel, F., et al., 2012. Grøstl – a sha-3 candidate. Disponível em: .

jakiman, 2017. PIVX purple paper. Disponível em: .

Kiraly, B., 2017a. InstantSend. Disponível em: .

Kiraly, B., 2017b. PrivateSend. Disponível em: .

Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system. Disponível em: .

Okupski, K., 2016. Bitcoin developer reference., pp.3–4. Disponível em: .

strophy, 2017. Understanding sporks. Dísponivel em: .

Wiecko, R., 2017. Dash instamine issue clari cation. Disponível em: .

Wu, H., 2012. The hash function jh. Disponível em: .