BULWARK

CRYPTOCURRENCY

Whitepaper de criptomoneda

Directiva de Bulwork:

Eatbatterys (Coordinador del proyecto)

Jack (Director de mercadeo)

SerfyWerfy (Desarrollador de cadena de bloques)

Frogman (Líder de comunicaciones)

Patrick (Diseño y marca)

Stu (Desarrollador de ecosistema)

La directiva de Bulwork

Diciembre 2017

Nosotros, la directiva de Bulwork, aseguramos que el proyecto presentado en este whitepaper es de nuestra autoría. Confirmamos que la información extraída de otras fuentes ha sido indicada en las atribuciones.

Resumen

Bulwark (símbolo bursatil: BWK) es una moneda orientada a la comunidad, nacida de una observación en las prácticas, generalmente injustas, sobre la privacidad en el espacio de los masternodes. Nuestra estategia de lanzamiento, deliberada y justa, permite a sus participantes la oportunidad de unirse a un prometedor proyecto desde sus inicios. Ofrecemos una propuesta de valor simple, sin ninguna premisa grandiosa: entregaremos una moneda privada que funcione, hoy y en el futuro, para aprovechar mejores prácticas, tanto para DASH como PIVX. Sin visiones imaginarias, con una perspectiva limitada de entrega, pero con una moneda funcional en una plataforma funcional con soporte en el futuro. Esto no significa que descartemos la innovación, en lugar de eso entregaremos resultados y no ilusiones. Existen muchas monedas que son potenciadas por ilusiones – evadiendo la sustancia – y nosotros no buscamos unirnos al creciente cuadro de monedas conducidas por la consigna de exceder sus promesas y bajo desarrollo. Sin ICO, una rampa de recompensa de lanzamiento, preminado pequeño y asignaciones de recompensas de bloque favorecidas a mineros, los adoptantes de Bulwark tendrán una base de acceso a una moneda privada, ofreciendo una mezcla de masternodes y la mejor tecnología disponible en monedas privadas, junto a una hoja de ruta de desarrollo significativa. Los masternodes estarán disponibles, y en funcionamiento, desde el lanzamiento y son una parte fundamental de la visión de esta moneda y estabilizarán la circulación, asegurarán la red y proveerán funcionalidad importante.

Agradecimientos

Bulwark no hubiera sido posible sin los trabajos previos realizados por los respectivos equipos de Bitcoin, Peercoin, Blackcoin, Talkcoin, DASH y PIVX. El software de código abierto y sus contribuidores están continuamente construyendo el camino hacia nuevas y emocionantes innovaciones. Cuando la información y el conocimiento son libres de construir, la sociedad, como un todo, se beneficia. Estamos agradecidos con nuestros predecesores por la oportunidad de contribuir en este ecosistema en crecimiento.

Tabla de contenido

Capítulo 1

Breve introducción a la criptomoneda

1.1 Trasfondo

En 2009, Satoshi Nakamoto lanzó un documento titulado *Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario*, describiendo su visión del comercio. La visión de Nakamoto detalló un sistema de monedas de usuario-a-usuario respaldado por una estructura de prueba de trabajo (PoW). La red marcaría el tiempo de las transacciones, enviándolas a un continuo libro de contabilidad que no podría cambiarse sin rehacer la prueba de trabajo. Los nodos elegirían la cadena más larga como prueba de los eventos presenciados por el mayor grupo con potencia de función de resumen (hash). Siempre que ≥ 51% de la potencia de hash de la red estén controlada por nodos que no tengan la intención de facilitar un ataque, la cadena que generen seguirá siendo la más larga (Nakamoto 2009).

1.2 El bloque (Block)

Cada bloque de la red está precedido por un encabezado de 80 bytes que contiene una copia doble hash SHA256 del encabezado del bloque anterior, raíz de merkle (una doble derivación hash SHA256 de todos los hashes que ocurrieron en el bloque), la marca de tiempo en la que empezó la prueba de trabajo, la dificultad de este hash de encabezado debe ser menor que o igual a, y en el momento en que los mineros alcanzan el objetivo de dificultad. Como tal, cualquier intento de modificar cualquier transacción, en cualquier bloque, dará como resultado el rechazo del bloque por parte de los mineros de la red (Bitcoin Core Team 2017).

1.3 La cadena de bloques (Blockchain)

Grupos de transacciones son formados en bloques y estos bloques son colocados cronológicamente en una cadena – formando la cadena de bloques (blockchain). La cadena de bloques crea un historial de movimiento de toda la actividad dentro de la red y sirve como un modelo de consenso distribuido donde cualquier transacción se puede verificar en cualquier momento (Crosby y otros 2015).

1.4 Sistema de prueba de trabajo (Proof-of-Work)

Proof-of-work es un sistema de verificación en donde los mineros deben dedicar recursos tangibles (costos de hardware, electricidad) para resolver un *crucigrama de palabras* probabilístico arbitrario. En caso de que un estafador intente burlar la cadena de bloques con una transacción fraudulenta, debe completar toda la prueba de trabajo hasta el momento actual (Okupski 2016).

Capítulo 2

Introducción a Bulwark

2.1 Una fundación sólida

Todo hogar necesita una fundación sólida, y Bulwark no es la excepción. Bulwark está construido en base a PIVX, que a su vez está construido en base a la famosa criptomoneda DASH. Si bien todos los linajes se remontan al núcleo original de Satoshi, cada proyecto ha elegido una dirección particular con objetivos e ideales que representan las comunidades a las que estos sirven. Ampliaremos y haremos énfasis en las características de monedas de privacidad de nuestras plataformas predecesoras mediante la exploración de nuevas tecnologías, al tiempo que crearemos conjuntos de herramientas y oportunidades para la integración de Bulwark en las plataformas tecnológicas actuales.

2.2 Un equipo dedicado a la comunidad

Para algunos proyectos, las comunidades son la idea secundaria. La prioridad número uno de Bulwark es la comunidad. Con sorteos, concursos, una animada plataforma de discusión y una política de cero tolerancias hacia el hostigamiento de los recién llegados, Bulwark se esfuerza por ser la criptomoneda para todas las variedades de usuarios. Los miembros de nuestra base de usuarios ya están contribuyendo con guías y scripts útiles para mejorar aún más la experiencia del usuario.

2.3 Balanceado y justo

Al momento de escribir, ha habido una afluencia de criptomonedas que utilizan una base similar. Si bien la tecnología subyacente es sólida, a menudo un examen más profundo de sus especificaciones y los parámetros de blockchain revela prácticas menos que justas.

2.4 El problema con las prácticas de preminado

2.4.1 Estudio de caso: FooBarBazCoin

Una tendencia creciente en el espacio de las criptomonedas es elegir una fecha arbitraria en el futuro para luego basar un porcentaje de preinicio en el suministro circulante a partir de esa fecha. Echemos un vistazo a la ficticia FBC (*FooBarBaz Coin*), una bifurcación (fork) de *DASH*:

- Recompensa del bloque: 15
- Tiempo del bloque: 2.5 minutos

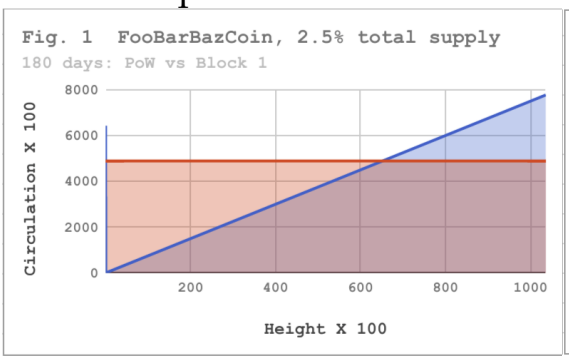
- Separación de Masternode/PoW: 50/50%
- Algoritmo de dificultad inicial: KGW
- El subsidio disminuye en un 12% cada año
- Suministro máximo de monedas: ~25 millones
- 2.5% preminado

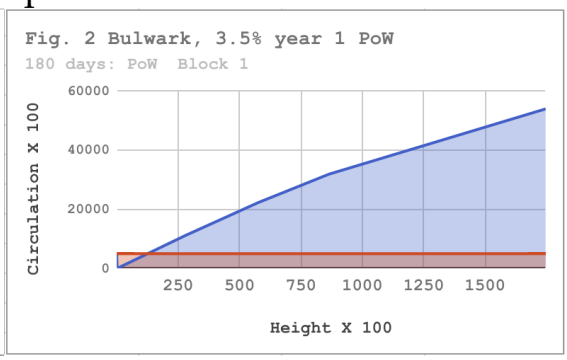
En este ejemplo, una preventa anunciada del 2.5%, que se traduce en ~643.000 monedas (de ~25 millones) parece razonable para el observador promedio. Sin embargo, para que las recompensas Masternode y PoW coincidan con las monedas que tienen los desarrolladores, tomaría aproximadamente 43.000 bloques. Con un objetivo de 2,5 minutos por bloque, los mineros, difícilmente, tardarían unos 150 días (o 75 días en total) en generar la misma cantidad de monedas. Después de 75 días, los desarrolladores aún controlarían la mitad de las monedas existentes.

2.5 Una alternativa más justa

El equipo de Bulwark reconoció esto y decidió estar al frente. Nuestra mina previa de 489.720 monedas (3.5%) representa un poco más de 12 días de minería PoW o un poco más de 10 días de producción total. Esperamos que esto sirva para inculcar la tranquilidad en la comunidad de que, después de cierto punto, el mercado no se puede devaluar significativamente como resultado de las monedas en poder del equipo central. Como se puede observar en las figuras a continuación, ambas representando 180 días en cada escenario, la diferencia es muy clara. Esperamos que al abordar el tema de una manera franca se establezca la precedencia y que ser sirva para beneficiar a la comunidad en general.

2.5.1 Comparación de ambos enfoques





2.5.2 Nuestro enfoque y la mina instantánea

Dash (Darkcoin) presenta un interesante caso de estudio sobre la necesidad de protección en la mina instantánea. Cerca del 10-15% del suministro total de Dash se creó en los primeros días de la existencia de la moneda gracias a algunos usuarios emprendedores (Wiecko 2017). Nuestro enfoque al problema de la mina instantánea fue doble. Usamos un subsidio lento en el que los primeros 960 bloques (1 día) aumentaron linealmente la recompensa del bloque completo, y el 100% de las recompensas del bloqueo también se destinaron a los mineros ese día. Históricamente, a esto se le ha acercado una pequeña recompensa por bloque que

cambia repentinamente, a cierta altura, a una recompensa de bloque completo, sin embargo, esto a menudo ha dado lugar a que las agrupaciones se vuelvan DDoS deliberadamente o se abrumen con el tráfico de mineros nuevos. Con una recompensa que aumenta linealmente, no tendría sentido intentar interferir con los mineros o los operadores del grupo para obtener ganancias monetarias.

2.5.3 ¿ICO? ¿Más como IC-NO!

Enfrentémoslo, al momento de escribir esto constantemente estamos siendo bombardeados con ICOs. Si bien tienen su lugar legítimo en el ecosistema de la criptomoneda, a menudo solo sirven para crear bolsillos llenos de riqueza. Teniendo en cuenta que Bulwark ofrece recompensas de masternodes y, en su segunda fase, recompensas de prueba de estado (PoS), esta concentración de riqueza puede causar enormes oscilaciones del mercado e inclinar el sistema de gobierno fuertemente a favor de los primeros (y más ricos) adoptantes. Si bien las concentraciones de riqueza son inevitables en su conjunto, creemos que cualquier oportunidad que podamos tomar para mantener el campo de juego, es una oportunidad para tomar. Lanzamos con una estrategia de recompensa de bloque a escala, una mecánica de lanzamiento justo para alentar una amplia distribución de Bulwark entre muchos usuarios, lo que idealmente evitaría parte de la concentración de riqueza vista en otros proyectos.

2.6 Funcional y rápido

Con un tiempo de bloqueo de 90 segundos, el consenso de masternodes y bloqueos de transacciones, programa de emisiones razonable y replanteo ecológico, Bulwark aspira a ser una criptomoneda verdaderamente funcional y rápida.

Capítulo 3

Parámetros en la cadena de bloques

3.1 Especificaciones de Bulwark en un vistazo

Tabla 3.1: De un vistazo, las especificaciones de Bulwark

Especificación	Descriptor
Código bursátil	BWK
Algoritmo	NIST5
Puerto RPC	52541
Puerto P2P	52543
Espacio entre bloques	90 segundos
Dificultad del algoritmo	Dark Gravity Wave v3.0
Tamaño del bloque	1MB
Vencimiento de minado/ Minted	67 bloques (~100 minutos)
Confirmación	6 bloques (~9 minutos)
Circulación (1 año)	14,505,720 BWK
Circulación (5 años)	27,668,220 BWK
Período de PoW	*nHeight* ≤ 345,600
Período de PoS	*nHeight* ≥ 345,601
Protocolo de soporte	IPV4, IPV6, TOR
PoS	Blackcoin v3.0 PoS, recompensas de PIVX SeeSaw

3.2 SlowStart

Nuestro justo comienzo se proporciona con el siguiente fragmento de código (créditos a *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 es empleada por Bulwark desde el principio como un método para reorientar la dificultad del sistema de prueba de trabajo. Utiliza un promedio móvil simple que puede responder a grandes aumentos o disminuciones de nethash en solo unos pocos bloques. Esto alivia el "efecto de bloqueo bloqueado" a menudo causado por multipools y evita que una persona agregue una cantidad sustancia de potencia de cómputo para resolver instantáneamente más de unos pocos bloques.

Capítulo 4

Recompensas del bloque

4.1 Recompensas del bloque PoW

Tabla: Especificaciones de recompensas de período de bloque PoW

Subsidio	Bloque	PoW	MN	Circulación
489720	1	100%	NA	489200
~25(media)	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

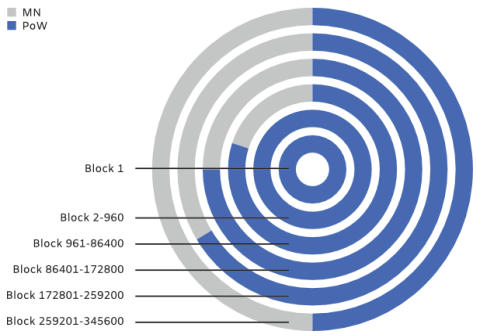


Figura 4.1: Recompensa del bloque PoW

4.2 Recompensas del bloque PoS

Tabla 4.2: Especificaciones de recompensas de período de bloque PoS

Subsidio	Bloque	Presupuesto	PoS/Masternode	Nota
25.000	345601-432000	10%	SeeSaw	Año 2
21.875	432001-518400	10%	SeeSaw	Año 2

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

Capítulo 5

Función de resumen o hashing NIST5

5.1 ¿Por qué NIST5?

Popularizado por TalkCoin en 2014, el algoritmo hash NIST5 ha tenido un modesto uso general. El NIST5 puede explotarse en una amplia gama de hardware de consumo, incluyendo CPUs, así como las GPU de NVidia y AMD. NIST5 no es tan resistente a ASIC como algunos otros algoritmos de memoria dura, pero creemos que la compensación es aceptable para mejorar la estabilidad del sistema y reducir el consumo de energía en relación con los algoritmos de memoria dura. En caso de que surjan actualizaciones de firmware que agreguen compatibilidad con NIST5 a los ASIC antes de que finalice nuestro período de PoW, estamos preparados con un algoritmo alternativo como reemplazo. Solicitaremos un voto de la comunidad sobre el curso de acción (si corresponde) y lo implementaremos en consecuencia. Creemos que nuestro breve período de PoW y la disposición a cambiar los algoritmos desincentivan a los fabricantes de ASIC y no prevén que surja un problema.

5.2 Los cinco finalistas (Competencia NIST SHA-3)

Los cinco algoritmos de hashing que componen el NIST5 son los finalistas de la competencia de hash de NIST (Chang 2012). Ellos son (en el orden en que los bloques han sido procesados):

Blake (Aumasson 2013), **Grøstl** (Gauravaram1 y otros 2012), **JH** (Wu 2012), **Keccak** (Bertoni y otros 2012), y **Skein** (Ferguson y otros 2010).

5.3 El nuevo estándar SHA-3

Keccak finalmente pasó la ronda final para ser nombrada la nueva función de hash SHA-3, mientras que los otros cuatro algoritmos (a pesar de ser considerados criptográficamente seguros) perdieron algunos puntos de los jueces por detalles técnicos menores. Creemos que la combinación del nuevo estándar SHA-3 junto con las otras opciones de los finalistas proporciona un algoritmo hash establecido, seguro y rápido.

5.4 Software de minado disponible

Al momento de escribir, hay varias opciones para los mineros:

Nombre	Plataforma	Enlace
SGMiner-5.0	OpenCL	
ccminer-2.2.2	CUDA	
cpuminer-opt	CPU	

Capítulo 6

Conjunto de características

6.1 Nodos maestros (Masternodes)

Los nodos maestros (masternodes) son, esencialmente, una red descentralizada de computadoras que sirven a la red de Bulwark. Los masternodes realizan importantes funciones de red y reciben parte de las recompensas del bloque. Sirven al ecosistema de Bulwark, estabilizando el suministro de monedas, procesando transacciones y asegurando la red. Los masternodes requieren 5000 BWK y moderado conocimiento técnico para operar. Cualquier billetera que controle 5000 BWK puede configurar un masternode.

6.2 Obfuscation / Mezcla de monedas

Bulwark presenta Obfuscation, basado en CoinJoin, pero con varias mejoras sobre el original, y se realiza a través de la mezcla de monedas de forma descentralizada facilitada por la red de masternodes. Esto proporciona una capa adicional de privacidad en las transacciones. Aunque no es perfectamente anónimo, la confusión a través de la mezcla de nodos es mucho mejor que la transacción de bitcoin estándar. Por ejemplo, todas las transacciones de Bitcoin son transparentes. Para Bulwark, un estafador necesitaría controlar el 50% de los masternodes operativos para tener menos del 0.5% de posibilidades de anonimizar una sola transacción que se mezcló con 8 rondas de Obfuscation (Kiraly 2017b). Esta característica importante proporciona un alto nivel de anonimato para los usuarios de BWK que eligen ofuscar sus transacciones.

6.3 SwiftTX

SwiftTX proporciona masternodes con autorización de bloqueo y consenso para las transacciones. Cuando se envía una transacción a la red, un grupo de nodos principales validará la transacción. Si esos nodos principales llegan a un consenso sobre la validez de la transacción, se bloqueará para su posterior introducción en la cadena de bloques, aumentando en gran medida la velocidad de transacción en comparación con los sistemas convencionales (como los tiempos de bloque de 10 minutos de Bitcoin con múltiples confirmaciones). SwiftTX hace posible que se realicen transacciones múltiples antes de que un bloque en la red se extraiga con las mismas entradas. Este sistema se basa en InstantSend de Dash (Kiraly 2017a)

6.4 Sporks

La red de Bulwark emplea el mecanismo de bifurcación (fork) de varias fases conocido como "sporking". Esto permitirá que la red BWK implemente nuevas características y a la vez minimiza las posibilidades de una bifurcación de red no deseada durante el despliegue. Los cambios de Spork se pueden implementar a través de la red y se pueden activar y desactivar según sea necesario sin requerir actualizaciones de software de nodo (strophy 2017). Esta característica es extremadamente útil y permite que la red reaccione rápidamente a las vulnerabilidades de seguridad.

6.5 Masternodes TOR & IPV6

Bulwark permite al usuario ejecutar su nodo completo o masternode desde una dirección onion o dirección IPV6. Hemos estado trabajando para agregar nodos de TOR completos tanto para fortalecer la red de TOR como para la experiencia de usuario de Bulwark que opera en modo solo TOR. Una característica única del soporte de masternode TOR es poder operar su masternode como un servicio TOR ocultos. Los nodos TOR permiten a los usuarios con conexiones a internet estables operar los nodos principales fuera de su red doméstica sin las implicaciones de privacidad de revelar su ubicación o los peligros de exponer su red doméstica a un potencial ataque o compromiso.

6.6 Importancia de la comunidad y el sistema de gobernanza

La comunidad de Bulwark es el factor más importante detrás del éxito a largo plazo del proyecto, y su capacidad para influir significativamente en el futuro de la moneda es primordial. Como tal, al final de la fase PoW pretendemos activar los superbloques de presupuesto en la red. Estos superbloques, pagadas mensualmente, permitirán a la comunidad ejercer un control significativo sobre todos los aspectos del desarrollo de Bulwark, la presencia de la marca y los asuntos de la comunidad. Retrasar la activación de este sistema nos dará tiempo de desarrollar el marco subyacente necesario para una experiencia positiva del usuario y maximizar las recompensas en bloque disponibles para los mineros y los nodos principales.

Utilizaremos un proceso de varias fases para crear y enviar propuestas. Cada paso deberá realizarse por completo. Si no se completan los pasos descritos, es probable que una propuesta no se active. Un esquema básico de estos pasos es el siguiente:

- Comience en nuestro chat de Discord y hable con algunos de los usuarios experimentados. Calcule el interés y si la respuesta es positiva, pase a la siguiente fase.
- Utilice múltiples plataformas de medios sociales para discutir y obtener comentarios. Recuerde que Bulwark tiene una base de usuarios diversa y diferentes niveles de participación en la gobernanza, por lo que llegar a una parte de la base de usuarios a menudo requerirá algunos pasos. Tome nota de estas discusiones y sea capaz de citarlas en la pre-propuesta formal. Cuantas más citas se proporcionen, mejor.
- Esté abierto a las sugerencias de la comunidad y los desarrolladores. Sea flexible y esté dispuesto a incorporar ideas y sugerencias externas en su propuesta.
- Elabore una propuesta previa formal en la sección Governance-> Pre-Proposal de nuestro sitio web. Proporcione citas para todas las discusiones que ocurrieron desde el paso anterior. Trate su propuesta previa como si fuera lo que se enviará a la cadena de bloques para votar.
- Al completas estos pasos, enviará su propuesta a la cadena de bloques. Esté preparado para dos tarifas, una en el momento de la presentación y una tarifa de papeleta pagada al desarrollador que activa su propuesta en la cadena de bloques. La tarifa de presentación no es reembolsable, y la tarifa de votación solo se pagará una vez aprobada y activada su propuesta.
- Todos tienen la libertad de ajustar su propuesta para incluir el costo de reembolso de estas dos tarifas. Asegúrese de que en su propuesta formal declare que está agregando el reembolso al estipendio solicitado.
- Asegúrese de volver a ponerse en contacto con todas las personas con quienes habló para que su idea sea votada. Para que una propuesta se pague, el 10% de los nodos

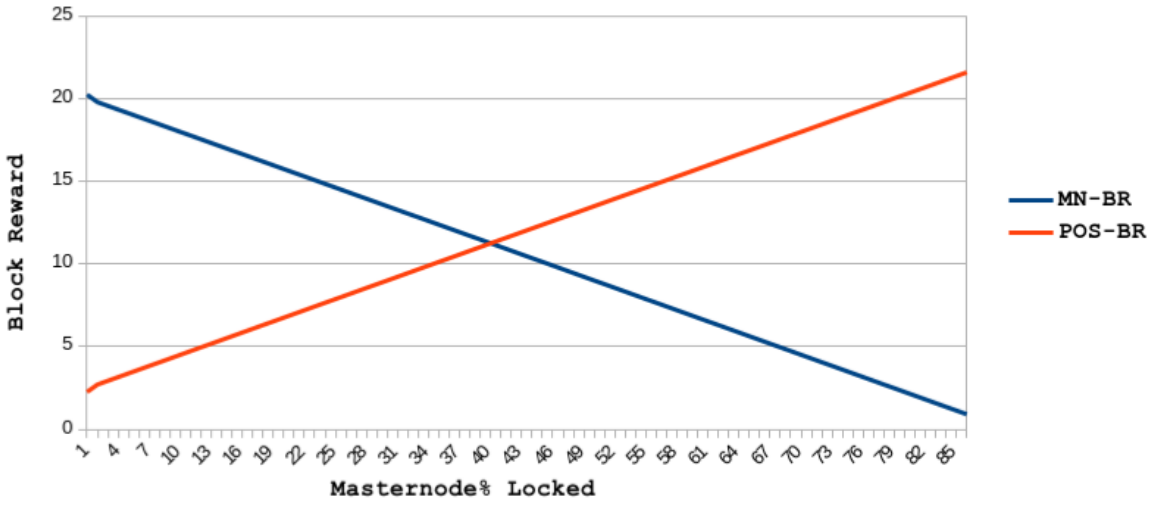
elegibles deben votar 'sí' en su propuesta. Este proceso de obtener un consenso del 10% puede ser mucho más difícil de lo que parece, así que sea diligente, informativo, y respetuoso en la obtención de los votos necesarios para que su propuesta sea pagada.

6.7 SeeSaw PoS/Recompensas de los masternodes

Hemos decidido utilizar el sistema de recompensa SeeSaw popularizado por PIVX (jakiman 2017). El sistema de recompensa SeeSaw comienza con una proporción de recompensar de 9: 1 (que favorece los nodos principales) y ajusta suavemente la proporción de recompensa entre replanteo y operadores de nodos hasta que el 41,5% de las monedas en circulación se bloquean en nodos principales; la ligera ventaja sobre las recompensas de replanteo es porque queremos evitar los problemas, como la significativa volatilidad de los precios y la baja liquidez que afectan a las monedas con porcentajes muy altos de suministro circulante bloqueados en los nodos. Esta estrategia mitigará la frustración de los usuarios por el acceso al suministro de monedas y mantiene la relevancia de nuestra robusta red. Dado que uno de nuestros objetivos es una plataforma bien respaldada para el comercio anónimo, la transitabilidad es la mayor importancia para aquellos que aceptan a Bulwark y los que tienen Bulwark.

Fig 3. SeeSaw @ Height 345601 - 432000

(after budget percentage)



Capítulo 7
El futuro

7.1 El cofre de herramientas de Bulwark

Una colección de fragmentos de código, API, bibliotecas, scripts y conocimiento que servirá para alentar un entorno tipo bazar donde los desarrolladores que puedan estar buscando la adición de soporte de criptomoneda en sus proyectos pueden intercambiar conocimiento, información y código. Creemos que brindarles a los desarrolladores estas herramientas equivale a proporcionarle a un carpintero las herramientas que necesita para crear proyectos emocionantes y magistrales.

7.2 Privacidad y mejoras de software

Nos comprometemos a adoptar nuevos protocolos que mejorarán la privacidad de nuestra base de usuarios. Hay varios caminos que estamos evaluando actualmente y planeamos comenzar las pruebas internas y el desarrollo en la primera mitad de 2018. Algunas de estas mejoras incluyen:

- Red de privacidad I2P.
- Protocolo Zerocoin o direccionamiento sigiloso (cuando tenemos confianza en la madurez de la solución)
- Sincronizar nuestra base de código más cerca con la línea principal de bitcoin.
- Racionalización/Actualización de QT Wallet.
- Integración de Libtox.
- Virtualización/contenedorización de la billetera de Bulwark para agregar una capa adicional de seguridad.

7.3 Nodo de inicio seguro de Bulwark

Trabajaremos con especialistas de CAD para diseñar un nodo de inicio seguro para Bulwark, pequeño e independiente. Los usuarios podrán conectar esto a su red doméstica y configurar mediante una interfaz de usuario web. Las funciones con las que intentamos lanzar son las siguientes:

- Para aquellos con conexiones a internet estables, es fácil configurar un masternode completamente onionizado (o un nodo completo) usando los servicios ocultos de TOR.
- Opción para funcionar como un relé para mejorar la red general de TOR.
- VPN y/o proxy que se puedan utilizar para enrutar el tráfico de internet a casa a través de la red TOR/I2P.
- Bulwark apostando a través de la virtualización o un dispositivo adicional.

De acuerdo con el espíritu de descentralización, los archivos imprimibles en 3D y todo el código fuente estarán disponibles para la comunidad para el ensamblaje en el hogar.

7.4 Extensión de nuestra marca

Seguiremos ampliando nuestra marca y tenemos la intención de trabajar con proveedores de hardware e integradores de sistemas que comparten la misma pasión e ideales que nosotros. En cinco años, queremos que el nombre 'Bulwark' sea sinónimo de criptomoneda, privacidad, seguridad y respeto por la libertad del usuario. El objetivo principal de Bulwark es proporcionar libertad de elección a través de la privacidad.

7.5 Diseño y visual

A través de la investigación y el desarrollo, nuestro objetivo es crear un lenguaje de diseño visual para Bulwark que lo diferencie de su competencia en el mercado de cifrado. Nuestro equipo de diseño planea innovar y experimentar con la UI / UX / marca actual para lograr finalmente la excelencia en el diseño buscando un medio que permita la mejor experiencia de usuario y una estética innovadora y hermosa. Esto se llevará a cabo investigando a nuestros competidores, manteniéndonos al día de las tendencias y estándares tecnológicos actuales y esforzándonos continuamente por ofrecer visuales nuevas y emocionantes a nuestros usuarios.

Capítulo 8

Conclusión

8.1 Sumario

Bulwark es una moneda orientada a la privacidad con masternodes, gobierno y un ecosistema de herramientas en evolución. El proyecto comenzó con un lanzamiento justo y un enfoque en la distribución amplia de monedas. Los algoritmos de inicio lento, división de recompensa de bloque y algoritmo hash fueron seleccionados deliberadamente para crear oportunidades para la participación significativa de la comunidad. Bulwark se lanzó con una variedad de características importantes de monedas de privacidad y el equipo de desarrollo está trabajando arduamente para presentar nuevas funciones y aprovechar las tecnologías existentes. Bulwark tiene como objetivo potenciar la elección a través de la privacidad y se centrará un esfuerzo considerable para este fin.

8.2 Trabajo futuro

El ecosistema del masternode de la moneda de privacidad ha sido inundado recientemente por monedas que buscan atraer a nuevos usuarios a través de promesas de retornos de inversión sustanciales, gigantescos mapas de ruta llenos de entregas improbables y un enfoque general en la comercialización sobre la mejora real dentro del espacio. Bulwark planea ser lo opuesto: bajo en ilusiones y alto en la creación real. Las metas actuales y futuras del proyecto seguirán la fórmula de ser específico, mensurable, alcanzable, relevante y de duración determinada.

Referencias

Aumasson, L.M., Jean-Phillipe Henzen, 2013. SHA-3 proposal: BLAKE. Disponible en: .

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

Bitcoin Core Team, T., 2017. Bitcoin developer reference. Disponible en: .

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. Disponible en: .

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., et al., 2015. BlockChain technology. Disponible en: .

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

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

jakiman, 2017. PIVX purple paper. Disponible en: .

Kiraly, B., 2017a. InstantSend. Disponible en: .

Kiraly, B., 2017b. PrivateSend. Disponible en: .

Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system. Disponible en: .

Okupski, K., 2016. Bitcoin developer reference., pp.3–4. Disponible en: .

strophy, 2017. Understanding sporks. Disponible en: .

Wiecko, R., 2017. Dash instamine issue clari cation. Disponible en: .

Wu, H., 2012. The hash function jh. Disponible en: .