Crave Financial Privacy

Crave Core Team

Crave Project

crave.cc

Junio 12, 2018

Abstracto

El sistema de pago descentralizada de Bitcoin ofrece un mecanismo para el registro de las transacciones monetarias en un libro sólo de adición, llamado blockchain. Una limitación importante de esto es que es posible rastrear la historia de cualquier pago, ya que las transacciones se almacenan en un libro de contabilidad pública. Estos datos podrían servir como un enlace para identificar a los usuarios y los patrones de transacción. trabajo comercial y académica ha demostrado que esta vinculación de historial de transacciones es fácil de realizar. En este trabajo, presentamos Crave - un sistema de pago descentralizado, que corrige los problemas de seguridad y privacidad de Bitcoin

Para empezar, damos una breve descripción de los problemas en el protocolo de Bitcoin. Esto cubre problemas con el anonimato, laescalabilidad y la energía ine fi ciencia del sistema de prueba de trabajo. A continuación, el detalle Crave, comenzando con un resumen y descripción del anonimato, untraceability, imposibilidad de vinculación, y las características unforgeability. La escalabilidad de Crave se dirige, así como algunas de las ventajas de su sistema de prueba de participación. A continuación, pasamos a muchas de las características tecnológicas de Crave, incluyendo masternodes, transacciones instantáneas LightX, y el sistema presupuestario y gobernabilidad. También existe información sobre la aplicación del Protocolo Zerocoin. Este es un protocolo basado en blockchain que se rompe el vínculo entre una dirección que recibe fondos no anónimas y la posterior operación que gasta esos fondos. Finalmente, finalizamos con el trabajo futuro de Crave, junto con los desarrollos en la hoja de ruta del año calendario 2018.

I. INTRODUCCION

Contrario a la creencia popular, las transacciones de Bitcoin no son completamente anonimas;

la historia de las transacciones son informacion publica. Lo que significa que cualquiera puede seguir las mascaras que pertenecen a usuarios que realizan transacciones en la cadena de bloques.

A pesar de que Bitcoin hace algunos esfuerzos indecisos para mantener sus cadenas de procesamiento de transacciones anónimas mediante el uso de nuevas claves públicas o hashes de vez en cuando, una violación de su anonimato aún puede ocurrir si un usuario de Bitcoin participa en transacciones de múltiples entradas. Las actividades del usuario se pueden rastrear a través de sus direcciones.

Bitcoin ha sufrido algunas infracciones de privacidad en el pasado, comprometidas a través de la reutilización de anuncios de Bitcoin, los nodos de supervisión de direcciones IP, el pago de Bitcoin contaminado y los métodos de análisis, y mediante otros procesos. Esto hace que Bitcoin sea poco atractivo para los usuarios que desean privacidad y anonimato fuertes y duraderos.

i. Escalabilidad

Bitcoin tiene un problema de escalabilidad que se ha resuelto sin resolver, lo que ha dado lugar a tenedores y divisiones entre la comunidad. Esto se debe a que la base de código de Bitcoin actual es muy similar a la que se creó hace más de nueve años. El antiguo ecosistema de Bitcoin se construyó para manejar un tamaño de bloque pequeño, incluso cuando se llevó a cabo un creciente número de transacciones en la cadena de bloques. Esto ha resultado en una tasa de hash lenta y altas tarifas de transacción. Tecnologías como SegWit y Lightning Network se están implementando para tratar de resolver este problema. Sin embargo, muchas personas creen que esto no será una solución completa, o que habrá una compensación en la descentralización. Es el

costosas tarifas de transacción que hacen que Bitcoin sea poco atractivo (en términos de transacciones diarias) para muchos usuarios.

ii. Uso de la Energia con PoW

Bitcoin utiliza protocolos de prueba de trabajo (PoW) para restringir el número de bloques que los mineros pueden crear a aproximadamente uno cada 10 minutos. Para cumplir con esto, un minero tiene que realizar una programación computacional al proporcionar soluciones a los enigmas criptográficos. Esta acción costosa y que consume mucho tiempo sirve como una forma de verificar que un minero haya realizado un trabajo antes de ser compensado con recompensas y la generación de un nuevo bloque. Estos nuevos bloques se construyen sobre los anteriores para formar una 'cadena'.

Para seguir siendo competitivos, existe la necesidad de plataformas de minería que tengan poco sentido una vez que se vuelvan obsoletas. Mucha gente argumenta que esto es un desperdicio de recursos. Otro inconveniente de usar un modelo de prueba de trabajo es que consume mucha energía. Procesar una transacción de Bitcoin requiere aproximadamente 5000 veces más energía que usar una tarjeta Visa. Esto hace que la capacidad de sostenimiento de Bitcoin sea poco realista a largo plazo. Además, el enorme costo de energía se transfiere a los usuarios como tarifas de transacción. Debido al aumento en la carga de la red y el consumo de energía, el tiempo de procesamiento de la transacción en la cadena de bloques de Bitcoin también aumenta. El tiempo de confirmación para extraer un bloque con Bitcoin oscila entre 30 minutos y 1 hora. Otras cadenas de bloques pueden hacer esto en minutos o segundos.

II. Introduciendo Crave

Crave es una criptomoneda de Prueba de Estaca que utiliza tecnología de vanguardia para proporcionar transacciones totalmente seguras y anónimas. Todo esto se hace mientras se mantienen los costos mínimos de transacción y las velocidades vertiginosas. Crave se lanzó el 20 de marzo de 2015 como la primera moneda para implementar masternodes en una base de código de prueba de estaca. Se han realizado muchos cambios desde entonces, incluido un nuevo equipo, especificaciones actualizadas y avances modernos.

con el código central basado en Bitcoin, DASH y PIVX, la tecnología incluye el protocolo Zerocoin, masternodes, envío instantáneo de confirmación cero de LightX, transmisión de transacciones de una sola vez y una interfaz avanzada y fácil de usar.

III. Distribución Justa

El método de distribución inicial fue un período de prueba de trabajo que tuvo lugar en los primeros 10000 bloques, que fue seguido por un cambio completo a prueba de estaca. Crave fue lanzado sin un ICO o premine. El 26 de febrero de 2018, un intercambio de monedas concluyó con la actualización de una nueva cadena de bloques y una base de códigos. Después de la conclusión del intercambio, todas las monedas restantes reservadas para el intercambio se quemaron.

IV. Anonimato avanzado
Intracabilidad, desvinculación e Informabilidad

Crave ha tenido en cuenta las principales preocupaciones que tienen los usuarios acerca de mantener su privacidad y anonimato intactos de los infractores externos no autorizados. Blockchains puede realizar una gran cantidad de transacciones en minutos. Para salvaguardar estas actividades, se requiere una seguridad máxima del blockchain protegiendo la privacidad y la confidencialidad de la información compartida en este sistema descentralizado.

i. Anonimato

Blockchains puede implicar transacciones financieras serias. Sería un error informar a alguien sobre las transacciones de un usuario, ya que eso sirve como vulnerabilidad para el ataque. Por ejemplo, supongamos que alguien compra una pintura rara. Si su información se divulga al público, los pone en mayor riesgo, ya que otras personas ahora saben que poseen este artículo. También existe el estado financiero implícito que viene junto con la compra. Al usar Crave para completar la transacción, podrían mantener estos detalles en privado.

Crave sirve para proteger la privacidad y el anonimato de sus usuarios mediante el uso de técnicas de criptografía avanzadas, el hash SHA-256 de claves públicas y la implementación de Zerocoin Pro-tocol, que utiliza el cifrado del acumulador RSA-2048.

ii. Intracabilidad y desvinculación

Usando el lenguaje blockchain, los bloques se construyen unos encima de otros para formar una cadena de bloques. Dado que los bloques están vinculados entre sí en la cadena de bloques, es posible que los atacantes externos rastreen la fuente de un bloque para apuntar a los recursos de criptografía de un usuario. Crave incorpora un sistema que evita esta trazabilidad, lo que permite al usuario borrar el historial de transacciones de sus monedas. Al hacer esto, cualquier atacante se encontraría en un callejón sin salida al intentar vincular la transacción a su origen, particularmente si la dirección de recepción se usa solo una vez. Esto se detalla más claramente en una sección posterior sobre el Protocolo de Zerocoin.

iii. Infornabilidad

La criptografía de clave pública permite la generación de un par de claves que están matemáticamente vinculadas entre sí. La clave pública se utiliza para el cifrado, mientras que la clave privada se utiliza para el descifrado. La criptografía de clave pública también se usa para crear una firma digital, que es fundamental para la autenticación y la integridad de los datos. Esto funciona mediante el uso de un algoritmo matemático para combinar la clave privada del usuario con los datos que se desean firmar. Una característica de una firma digital es que los datos firmados son una parte integral de la firma. Si los datos se modifican de la forma más leve, la firma se mostrará como no válida cuando se marque. Esta característica permite la transferencia segura de datos, asegurando que nadie pueda intentar falsificar una firma adjuntándola a otro archivo.

Cuando se crea una transacción, se firma con la clave privada del usuario y luego se transfiere a la red. La red verifica la firma digital para verificar que coincida con la clave pública de la dirección desde la que se envían las monedas. Si se verifica, la transacción se considera válida, retransmitida a otros pares, y colocado en el blockchain. Solo el usuario que posee la clave privada coincidente podría haber producido una firma válida. Si alguien intentara crear una transacción no genuina enviando fondos de una dirección que no le pertenece, la firma se mostrará como inválida y la transacción será rechazada.

V. Escalabilidad y tarifas

Uno de los mayores problemas que enfrenta Bitcoin se relaciona con su escalabilidad. El tamaño de bloque limitado y la tasa de transacción lenta aumentan las tarifas de transacción para los usuarios.

Crave intenta resolver este problema complejo al proporcionar a cada usuario un gran tamaño de bloque para las transacciones y mantener las tarifas en una mini-mamá. Crave tiene un tamaño de bloque máximo de 40 MB, lo que contrasta notablemente con el tamaño de bloque de 1 MB de Bitcoin. El aumento del tamaño del bloque permite un crecimiento continuo en el futuro, debido a la mayor cantidad de transacciones que se pueden incluir en cada bloque. Esto también proporciona un tiempo de verificación de transacción más rápido, ya que a mayores porcentajes de capacidad de bloque, existe una menor probabilidad de que una transacción se incluya en el bloque.

También hay inconvenientes en un tamaño de bloque más grande. Debido al aumento en la cantidad de datos que podrían enviarse con bloques llenos más grandes, podría ser más lento transmitir nuevos bloques. Esto podría resultar en bloques más huérfanos. Además, el tamaño de bloque grande podría conducir a tamaños de base de datos que alcanzan un alto nivel. Los nodos que no tienen la capacidad de aumentar su almacenamiento caerían de la red, disminuyendo la descentralización de la red.

En 2018, Crave está implementando su plan Adaptive Blocks, que permite ajustar el tamaño del bloque a los requisitos actuales de la red. Esto permitirá transacciones más rápidas y aumentará la escalabilidad, sin ninguna limitación observable.

Los costos de transacción estándar son alrededor de 0.0001 Crave / kb, aunque esto se adapta según la carga de la red. Debido al crecimiento lineal del suministro de monedas, este costo será mínimo, incluso en el caso de una adopción masiva. Las transacciones de Crave también se pueden procesar como tarifa cero, en la cual hasta

Se pueden enviar 6 entradas sin ningún costo de transacción.

i. Sistema de prueba de estaca y energía y eficiencia

En lugar de utilizar los protocolos de prueba de trabajo para validar las actividades mineras de los usuarios, Crave adopta una tecnología más puntual y menos costosa. Prueba de estaca requiere que el probador muestre la propiedad de las monedas (la "estaca") para verificar los bloques y las transacciones. Los verificadores dentro de la red no necesitan resolver acertijos com-putacionales intensos. Este enfoque es práctico para las aplicaciones del mercado de masas de los sistemas blockchain, mostrando una ventaja en promover la escalabilidad

También se admite apostar en una Raspberry Pi si así lo desea, ya que consume menos energía y aumenta la eficiencia energética. Una Raspberry Pi es (en términos generales) una computadora muy pequeña y barata que casi no consume electricidad. Esto es atractivo para aquellos que no quieren desperdiciar electricidad al dejar su computadora encendida, o ejecutar su billetera en un servidor privado virtual.

VI. Características Tecnológicas

La siguiente sección ofrece información sobre las características tecnológicas de Crave, junto con las características que distinguen a la criptomoneda de las demás.

VII. Proof-of-Stake v3.0

PoS v3.0 ha resuelto algunos de los problemas con versiones anteriores del protocolo de consenso. A continuación se enumeran algunas de estas ventajas:

- **Eficiencia energética:** PoS v3.0 reduce el costo de la energía durante las operaciones de forja o minería, ya que no se basa en resolver acertijos criptográficos intensos.
- **Sin edad de monedas:** PoS v3.0 hace no se debe tener en cuenta la edad de la moneda como criterio para adjudicar reconstrucciones de bloque para el replanteo. Esto protege contra los ataques consecutivos de doble gasto y ayuda a mantener conectados tantos nodos como sea posible, lo que es imprescindible para la seguridad.
- **Sin Precomputación de Blockchain:** En versiones anteriores, era posible bifurcar un bloque cambiando sus marcas de tiempo previas. En esa situación, un modificador de apuesta no ofuscaría por completo el hash para evitar revelar las pruebas futuras. PoS v3.0 hace que sea obligatorio cambiar el modificador de apuesta en cada intervalo de modificación. Hacer esto ofusca cualquier cálculo que pueda revelar la próxima prueba de participación.
- **Recompensa de bloque:** Una recompensa en bloque de hasta 11 Crave sirve para incentivar a los nodos a permanecer conectados a la red. En un entorno descentralizado, una mayor cantidad de nodos conectados a la red aumenta la seguridad. Esto ocurre a través del cambio de confianza de un solo usuario a varios usuarios.

i. Distribución de recompensa de Bloque

La recompensa del bloque 11 Crave se divide para tres propósitos diferentes:

- 6 para masternodes
- 4 para staking
- Hasta 1 para presupuestos, desarrollo de infraestructura y gobierno.

ii. Presupuesto Recompenza del Bloque

Técnicamente solo hay 10 Crave acuñados por bloque, con 1 Crave por bloque temporalmente 'reservado' para presupuestar. Como el espaciado entre bloques es de 60 segundos (se agrega un bloque a la cadena de bloques por minuto), hay 1440 bloques por día y 43200 bloques por mes. Esto significa que cada 30 días, 43200 Crave se reservan para el gobierno.

Cualquiera puede enviar propuestas para promover el crecimiento y desarrollo de Crave. Si a la comunidad le gusta la idea detrás de una propuesta, los titulares de los masternode pueden votar para que se apruebe. Por el contrario, también pueden rechazar la proposición. Una parte de la propuesta es un monto de pago único o mensual. Esto introduce un poco de competencia entre los que envían propuestas, ya que todos luchan por una porción de los 43200 reservados mensuales de Crave.

Cada 30 días (43200 bloques) ocurre un superbloque. El objetivo del superbloque es recompensar las direcciones asociadas con las propuestas aceptadas. No es hasta este superbloque en el que los fondos reservados se acuñan y se agregan a la fuente circulante. Por ejemplo, diga que durante un cierto mes, se aceptan 6 propuestas, y se tomarán 40000 de los 43200 posibles fondos del presupuesto. Los 3200 Crave adicionales no van a ninguna billetera Crave ni a una dirección de desarrollo: simplemente nunca se crean.

En resumen, si las propuestas aceptadas tuvieran que tomar el 100% de los fondos reservados, sería el equivalente a tener una recompensa constante de bloqueo de 11 Crave en términos de emisión de oferta. Sin embargo, si no se aceptaron propuestas y se asignó el 0% de esta reserva, también sería el equivalente a tener una recompensa de bloque de 10 Crave.

iii. Replantear el sistema de recompensas

El modelo más simple de este sistema se llama 'equipo de minería simulada', en el cual cada cuenta tiene una cierta probabilidad por segundo de generar un bloque válido, muy parecido a una pieza de hardware de minería. Esta posibilidad es proporcional al saldo de la cuenta. Una ecuación general para esto se puede mostrar como ...

$$SHA256(prevhash + address + timestamp) \Rightarrow \frac{2^{256} * balance}{diff} \quad (1)$$

... donde 'prevhash' es el hash del anteriorblo ck, 'address' es la dirección del stake-miner, 'timestamp' es el tiempo actual de Unix en segundos, 'balance' es el saldo de cuenta del stack-miner y 'diff' es un parámetro de dificultad global ajustable. Si una cuenta dada satisface esta ecuación en cualquier segundo en particular, puede producir un bloqueo válido, dando a esa cuenta una recompensa en bloque por replanteo.

Recibir recompensas del replanteo depende de la cantidad apostada. En otras palabras, mientras más apuestas tenga un usuario, mayor es la probabilidad de recibir una recompensa. Sin embargo, sigue siendo un proceso aleatorio, lo que significa que un usuario podría ir a semana sin recibir una recompensa, luego proceda a obtener tres en una fila. Se puede encontrar una calculadora de apuestas en el sitio web de Crave, que calcula el tiempo de las recompensas.

VIII. Masternodes

Un masternode es un nodo lleno de criptomoneda o billetera de computadora que posee la copia completa de la cadena de bloques asociada en tiempo real. Los nodos principales siempre están en funcionamiento para que las transacciones se puedan procesar sin bloqueos en cualquier momento.

i. Propósito de Masternodes

Las funciones de los masternodes son diferentes de las de los nodos normales, y algunas de estas funciones se destacan a continuación:

- ◇ Facilite las transacciones instantáneas.
- ◇ Instrumental en el gobierno y la gestión de blockchain a través de la participación activa de los usuarios en los procesos de votación.
- ◇ Hacer posible emprender presupuestos y la rendición de cuentas del tesoro.

ii. Cómo Crave incorpora Masternodes

Los masternodes de Crave se pueden ejecutar en cualquier puerto y múltiples masternodes pueden usar el mismo IP-dress. El monitoreo está disponible en la billetera Crave para verificar el estado de los nodos principales y las transacciones. Junto con esto, se permiten múltiples direcciones de billetera fría para la seguridad transaccional máxima.

La garantía requerida para configurar un mastern-ode es 5000 Crave. Un masternode se puede detener en cualquier momento, y las monedas luego se desbloquean para que el operador las use como lo deseen.

iii. Sistema de recompensa Masternode

El sistema de recompensa masternode de Crave sigue la lógica de pago que se describe a continuación.

- **Lista global:**
  Cada masternodo que se ejecuta durante más de 8000 segundos está disponible en una lista global descentralizada. Su posición en esta lista depende del tiempo transcurrido desde que se realizó el último pago de acuerdo con la red. Los nuevos nodos maestros elegibles que se unen a la red, los nodos maestros reiniciados y los nodos maestros que reciben el último pago se colocan al final de la lista global. Con el tiempo, los masternodes migran hacia la parte superior de la lista hasta que ingresen al grupo de selección.
- **Grupo de selección:** El grupo de selección se estima como el 10% superior de la lista global. Si hay 1000 masternodes totales esperando en la cola de la lista global, los primeros 100 nodos maestros estarán disponibles para la recompensa del bloque. El grupo de selección no tiene orden, por lo que la probabilidad de que un masternode reciba una recompensa viene determinada por las probabilidades.

- **Probabilidades:** Una vez en el grupo de selección, la selección de recompensa de masternode se basa en probabilidades determinadas por entropía de hash de bloque y aleatoriedad. Cada masternode en el grupo debe tener la posibilidad de recibir un pago en cada bloque, de acuerdo con:

$$\frac{1}{\#\ of\ Masternodes\ in\ Selection\ Pool} \quad (2)$$

La excepción a esta lógica de pago se encuentra en los nuevos masternodes, que tienen un período de tiempo más largo antes de recibir un retorno inicial. La transacción de blockchain que colocó la garantía de 5000 Crave debe tener tantas confirmaciones como la cantidad total de nodos maestros actuales en la red. Solo entonces el masternode podrá recibir una recompensa. Esto está contenido en el siguiente código:

$$if(mn.GetMasternodeInputAge() < nMnCount)\ continue; \quad (3)$$

También hay un control adicional para el primer pago de masternode:

$$if(fFilterSigTime\ \&\&\ mn.sigTime + (nMnCount * 2.6 * 60) > GetAdjustedTime())\ continue; \quad (4)$$

En otras palabras, si un usuario comenzara su masternode con 1100 masternodes totales que se ejecutan en la red, será elegible para recibir su primera recompensa después de 1100 * 2.6 * 60 segundos = 47.67 horas.

iv. Soporte Tor Masternode

Tor usa una técnica llamada enrutamiento de cebolla para ocultar información sobre la actividad del usuario. Esto significa que protege al usuario mediante el rebote de las comunicaciones en una red distribuida de retransmisiones que se ejecuta en todo el mundo. El uso de Tor encripta todo el tráfico de red para que no se pueda acceder a la dirección IP ni a los datos del usuario. En lugar de estar asociado con una dirección IP, permite el uso de direcciones de sufijo .onion, que no son nombres DNS reales.

IX. Protocolo Zerocoin y zCrave

La función principal del Protocolo de Zerocoin es utilizar pruebas de cero conocimiento para romper el vínculo entre una dirección que recibe fondos no anónimos y la transacción subsiguiente que gasta esos fondos. En otras palabras, actúa como un escudo de seguridad para las transacciones.

zCrave es el nombre de la unidad utilizada en la versión de Crave de este servicio de mezcla de monedas.

El uso de zCrave permite una total imposibilidad de rastreo y el anonimato de las transacciones. Esto protege contra ladrones potenciales que de lo contrario podrían intentar seguir la historia de la transacción de vuelta a la dirección original.

i. Cómo funciona el protocolo Zerocoin

Para simplificar cómo funciona, lea esta breve analítica de Matthew Green:

"La gente arroja dólares en un sombrero. Cada vez que tiran un dólar, reciben una ficha a cambio,

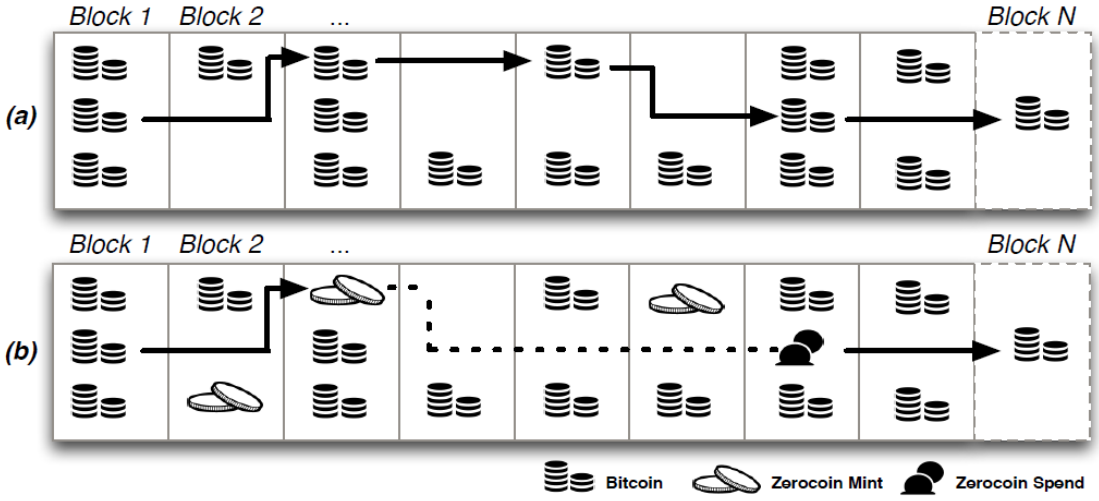

Figura 1: *Ejemplo de cadenas de bloques que muestran historiales de transacciones de Bitcoin. En (a), se puede ver que cada transacción se puede vincular a una transacción anterior. El uso del Protocolo de Zerocoin puede verse en (b), en el que el vínculo entre acuñar y gastar (la línea punteada) no se puede determinar a partir de la cadena de bloques.*

y todos los tokens se ven exactamente iguales. Bob recibe una ficha y se aleja. Bob regresa una hora más tarde con una máscara puesta. Bob intercambia su ficha y saca un dólar totalmente diferente ".

Zerocoin funciona permitiendo pagos directos anony-mous entre las partes. Hay dos pasos que deben tomarse

1. Minando
2. Gastando

Veamos un ejemplo.

1. Minando
   (a) Bob quiere enviar 1250 Crave a Amy usando una transacción anónima.
   (b) Bob primero convierte el 1250 Crave a 1250 zCrave, que se divide automáticamenteen denominaciones. En este caso, el zCrave de Bob se conferiría en las siguientes denominaciones ...
      ◇ 1 x 1000 zCrave
      ◇ 2 x 100 zCrave
      ◇ 1 x 50 zCrave
   (c) El saldo de Bob ahora refleja que posee 1250 menos de Crave y 1250 más de zCrave de los que comenzó.
   (d) Ahora existe una "clave secreta de conocimiento" asociada con Bob, utilizada para verificar la propiedad de sus denominaciones específicas de zCrave.
2. Gastando
   (a) Después de la celebración de las denominaciones zCrave, Bob ahora envía el zCrave 1250 a la dirección de Amy's Crave.
   (b) La "clave de conocimiento secreta" se verifica mediante el Protocolo de Zerocoin.
   (c) La cuenta de Amy se acredita con 1250 Crave de un remitente anónimo, mientras que el saldo zCrave de Bob muestra una disminución de 1250.
   (d) Amy ahora tiene 1250 Crave que no muestra ningún historial de transacciones anterior, por lo que es imposible hacer un seguimiento de sus ori-gins a la dirección de Bob's Crave.
   (e) La "clave de conocimiento secreta" utilizada ahora se vuelve inválida, lo que impide que el saldo acuñado se vuelva a gastar.

ii. Denominaciones

Las denominaciones admitidas de zCrave son 1, 5, 10, 50, 100, 500, 1000 y 5000.

Estos valores se eligieron para promover la anulación de la trazabilidad y reducir el tamaño de la transacción, al tiempo que permiten al usuario cierta flexibilidad en la cantidad que puede gastarse. Debido a estas denominaciones zCrave, solo se pueden enviar números enteros de monedas de una dirección a otra usando el Protocolo de Zerocoin.

iii. Ventajas de usar zCrave

- ◇ Limpia el historial de transacciones de las monedas enviadas, ya que se acuñan monedas completamente nuevas, mientras que las monedas antiguas con historial se queman.
- ◇ Las transacciones anónimas solo demoran 1-2 segundos en completarse.
- ◇ Permite el gasto directo de zCrave directo a otra dirección de Crave.
- ◇ Reduce el tamaño de las transacciones.

X. LightX

El sistema bancario tradicional ha desarrollado los medios por los cuales las personas pueden enviar dinero a otra parte en cuestión de minutos, incluida West-ern Union o Moneygram. Con el advenimiento de la criptomoneda, ahora existe un método mucho más rápido para enviar un pago: transacciones que se envían casi al instante. LightX es el modelo de Crave del sistema de envío de envío instantáneo.

i. Proposito de LightX

El objetivo principal de Crave LightX es facilitar el proceso de envío de pagos de una parte a otra en muy poco tiempo. Las personas que utilicen LightX podrán pagar sus actividades de compra u otros pagos necesarios lo más rápido posible. Por ejemplo, cuando se utiliza una tarjeta de crédito para el pago, no es posible confirmar el pago a los vendedores inmediatamente, demorando días o semanas para hacerlo. Con LightX, la verificación de los pagos hacerse en un instante cercano, lo que significa que las monedas serán gastables segundos después de ser enviadas.

ii. Como funciona LightX

Los nodos principales juegan un papel importante en el proceso de envío instantáneo Crave. Con LightX, se pueden enviar pagos seguros a los propietarios de las tiendas y a cualquier otra parte con la que alguien tenga que liquidar los pagos.

Los pagos de LightX usan la red maestra para bloquear de inmediato la cantidad exacta de fondos remitidos en la cuenta del usuario. Esto evita que los fondos se gasten dos veces. Se enviará una notificación una vez que los fondos hayan sido bloqueados. Dado que se acaba de llevar a cabo una transacción, Crave blockchain lo registra en el libro de contabilidad público donde todos los demás usuarios pueden verlo. Los fondos bloqueados se entregan a la parte designada y se recibe una notificación para el pago completo en cuestión de segundos.

El costo de completar una transacción LightX instantánea es una constante de 0.01 Crave, un poco más que el costo de transacción predeterminado de 0.0001 Crave / kb. Esta es una función opcional que se puede activar y desactivar según lo desee.

XI. Sistema de Presupuesto y Gobernabilidad

Crave es un proyecto dependiente de la comunidad, lo que significa que depende de la participación activa de sus usuarios para ayudar a llevar a cabo y desarrollar sus servicios y usabilidad.

Cada nuevo bloque es creado por los usuarios de Crave, que a su vez son recompensados por su actividad para mantener la red fuerte y segura. Durante este proceso, hasta 1 Anhelo de cada recompensa de bloque se reserva para su uso en el sistema de presupuestación. Se describió más información sobre esto en la sección de Recompensas del Bloque de Presupuesto. Este monto se otorga a cualquier propuesta aceptada en forma de superbloques mensuales. Las instrucciones específicas para enviar una propuesta y votar se encuentran en la guía de instalación de Crave o en el sitio web oficial.

i. Vote por propuestas creadas por la comunidad

Crave está completamente descentralizado, y los dueños de masters de todo el mundo podrán participar en los procesos de votación. Cada masternode recibe 1 voto. La votación se lleva a cabo para decidir sobre cualquier propuesta presentada por los miembros de la comunidad, que puede incluir (pero no se limita a):

◇ Expansión de los esfuerzos de marketing.
◇ Contratación de nuevos miembros para el equipo.
◇ Agregar funciones a la arquitectura actual
◇ Cualquier otra propuesta que tenga como objetivo mejorar las operaciones de la red Crave.

ii. Guiado por la comunidad

Como se resumió anteriormente, Crave depende de que sus miembros realicen regularmente las siguientes funciones para mantenerse activos y utilizables para cualquier persona en todo el mundo.

◇ **Staking y Masternodes:**Los que ejecutan los nodos de maestro o las monedas de estaca ayudan a proteger la red y son recompensados por hacerlo.

◇ **Gobernancia:**Crave está descentralizado, lo que significa que no existe un sistema central de gestión para la criptomoneda. Los usuarios de Crave tienen la capacidad de proponer ideas y votar para ayudar a determinar la dirección del proyecto.

◇ **Mejora:** Si bien muchas de las mejoras de Crave se deben a un equipo de desarrollo calificado, los miembros de la comunidad pueden contribuir de la manera que consideren adecuada para mejorar el ecosistema.

◇ **Administración:** Se confía a los miembros de la comunidad para ayudar a explicar las características de Crave a los usuarios nuevos y potenciales. Esto ayuda a expandir la red y hacer crecer la comunidad.

XII. Trabajo futuro

Todavía queda mucho por hacer, y estamos siempre en constante estado de desarrollo. los la hoja de ruta contiene lanzamientos de características principales a tener en cuenta en 2018, incluyendo una nueva cartera única, replanteo zCrave, tamaños de bloques adaptativos y la integración de una capa de red anónima.

XIII. Hoja de Ruta

El trabajo planificado para el resto del año calendar 2018 se ha detallado en el Plan de trabajo de Crave. Puede haber pequeños ajustes, adiciones o eliminación de artículos si se considera apropiado.

i. 1er Cuatrimestre

◇ **Lanzamiento de la hoja de ruta:** orientación para futuros desarrollos.

◇ **Fin del intercambio de monedas:** Crave tenía una moneda swap para implementar una nueva base de código, blockchain, características y billetera. La oferta también se aumentó para ajustarse mejor a las denominaciones zCrave. Las monedas restantes se quemaron, manteniéndose fieles al aspecto 'No Premine' de Crave.

◇ **Listado en Cryptopia:** Aplicación ypayment fee for listing Crave on the exchange, Cryptopia.

◇ **Integracion Coinomi**: Coinomi es una billetera HD de múltiples activos y segura para Bitcoin, altcoins y tokens. Es amigable para dispositivos móviles y funciona como una billetera móvil.

◇**Actualizaciones del sitio web:** adición de estadísticas de actualización automática, hoja de ruta y soporte de idiomas adicionales para el sitio web oficial de Crave.

ii. 2do Cuatrimestre

◇ **Re Diseño Crave:** Crave recibirá un nuevo diseño para adoptar un público más amplio, cambiando el logotipo y el diseño del sitio web.

◇ **Activación del sistema de gobernanza y presupuesto:** los miembros de la comunidad pueden proponer ideas y proyectos, por lo que los titulares de masternode podrán votar a favor o en contra. Este método asigna fondos establecidos

además de la recompensa del bloque Crave para financiar proyectos que respaldan la red.

◇**Brainwallet Integration**: El almacenamiento del zCrave del usuario estará disponible con una frase de recuperación nemotécnica de una sola semilla.

◇ **Crave Knowledge Base:** el propio medio de Crave para responder las preguntas comunes que los usuarios tienen, desde niveles para principiantes hasta niveles avanzados.

◇ **Actualizaciones del sitio web:** se realizarán mejoras para agregar toda la información importante en una única ubicación fácil de usar.

◇ **Paper Wallet Generator:** Soporte para un mecanismo fuera de línea para almacenar claves públicas y privadas en papel.

iii. 3er Cuatrimestre

◇ **zCrave Staking:** la seguridad de la mezcla de red se incrementará al permitir el replanteo de zCrave.

◇**Nuevo diseño de billetera QT:** reelaboración completa de la IU de la billetera para una mayor usabilidad.

◇**Votación en la billetera:** soporte para realizar todas las votaciones presupuestarias desde la GUI interna de la billetera QT.

◇**Votación en la billetera:** soporte para realizar todas las votaciones presupuestarias desde la GUI interna de la billetera QT.

iv. 4to Cuatrimestre

◇ **Bloques adaptables:** los tamaños de bloques se ajustarán automáticamente a los requisitos de red actuales, lo que permite transacciones más rápidas y una mayor escalabilidad.

◇ **Integración de red I2P:** Proyecto de Internet invisible (I2P) es una capa de red anónima que permite la comunicación entre iguales resistente a la censura. Cuando se implemente con Crave, esto también servirá para encriptar el tráfico de la red de manera que no se pueda acceder a la dirección IP del usuario.

XIV. Expresiones de Gratitud

Un agradecimiento especial a los miembros de la comunidad que ayudaron en la redacción, edición y comentarios de este libro blanco.

◇ Asif Rahman
◇ HP3480
◇ MichaelJackson
◇ CryptoADavid
◇ Wonkee
◇ Wayne

El libro blanco original v1.00 Crave fue re-arrendado el 9 de mayo de 2018. Este libro blanco es un documento vivo, y la fecha indicada en el encabezado indica la revisión más reciente.

Referencias

[1] M. Conti, S. K. E, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," Jun. 2017.

[2] F. Saleh, "Blockchain Without Waste: Proof-of-Stake," p. 39

[3] G. Zyskind, O. Nathan, and A. ' Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in 2015 IEEE Security and Privacy Workshops, 2015, pp. 180-184.

[4] H. Vranken, "Sustainability of bitcoin and blockchains," Current Opinion in Environmental Sustainability, vol. 28, pp. 1-9, Oct. 2017.

[5] 'The Blockchain Is Only as Strong as Its Weakest Link," Security Intelligence, 27-Oct-2017.

[6] R. Yap, "Understanding how Zerocoin in Zcoin works and how it compares to other anonymity solutions Part 1," Zcoin, 10-Mar-2017.

[7] 'Bitcoin Explained Like You're Five: Part 3 - Cryptography," Escape Velocity, 07-Sep-2013. [Online]. Available: https://chrispacia.wordpress.com/2013/09/07/bitcoin-cryptography-

digital-signatures-explained/. [Accessed: 02-Apr-2018].

[8] wiki: The Ethereum Wiki -. ethereum, 2018. [Online]. Available: https://github.com/ethereum/wiki. [Accessed: 20-Mar-2018].

[9] dash: Dash - Reinventing Cryptocurrency. Dash, 2018. [Online]. Available: https://github.com/dashpay/dash/blob/master/src/masternodeman.cpp. [Accessed: 09-Apr-2018].

[10] 'Understanding Masternodes - Dash latest documentation." [Online]. Available: https://docs.dash.org/en/latest/masternodes/understanding.html. [Accessed: 09-Apr-2018].

[11] 'On Stake," Ethereum Blog, 05-Jul-2014. [Online]. Available: https://blog.ethereum.org/2014/07/05/stake/. [Accessed: 02-Apr-2018].

[12] 'Bitcoin Energy Consumption Index," Digiconomist. [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption. [Accessed: 28-Feb-2018].

[13] 'Bitcoin Scaling Problem, Explained," Cointelegraph. [Online]. Available: https://cointelegraph.com/explained/bitcoin-scaling-problem-explained. [Accessed: 27-Feb-2018].

[14] 'Dash: Solving the Challenges of Instant, Private Payments," CoinCentral, 11-Jan-2018. [Online]. Available: https://coincentral.com/what-is-dash/. [Accessed: 10-Mar-2018].

[15] 'How zerocash works | Zerocash." [Online]. Available: http://zerocash-project.org/how_zerocash_works.html. [Accessed: 10-Mar-2018].

[16] 'Proof of work - Bitcoin Wiki." [Online]. Available: https://en.bitcoin.it/wiki/Proof_of_work. [Accessed: 27-Feb-2018].

[17] 'Zerocoin Project." [Online]. Available: http://zerocoin.org/index. [Accessed: 10-Mar-2018].

[18] 'Staking Sidechains? New Paper Proposes Twist on Bitcoin Tech," CoinDesk, 27-Sep-2017. [Online]. Available: https://www.coindesk.com/staking-sidechains-new-paper-proposes-twist-bitcoin-tech/. [Accessed: 09-Mar-2018].

[19] A. Nordrum, "Wall Street Firms to Move Trillions to Blockchains in 2018," IEEE Spectrum: Technology, Engineering, and Science News, 29-Sep-2017. [Online]. Available: https://spectrum.ieee.org/telecom/internet/wall-street-firms-to-move-trillions-to-blockchains-in-2018. [Accessed: 03-Mar-2018].

[20] 'What Is A Masternode And How Is It Useful For Cryptocoin Investors," CoinSutra - Bitcoin Community, 04-Jan-2018. [Online]. Available: https://coinsutra.com/masternodes/. [Accessed: 09-Mar-2018].

[21] 'Security Analysis of Proof-of-Stake Protocol v3.0," BlackCoin, 17-Oct-2016. [Online]. Available: https://bravenewcoin.com/assets/Whitepapers/Blackcoin-POS-3.pdf. [Accessed: 10-Mar-2018].

Apendices

A. Crave Core Team

- **CooleRRSA**: Core Development
- **Slothman**: Communications
- **tkon**: Support
- **zrero**: Front-End Development
- **DruMn**: Front-End Development
- **Green_crypto_and_ham**: Marketing
- **SoundDrGenie**: Video and Film Outreach

Mas informacion: `https://crave.cc/team`

B. Enlaces útiles

Listed here are important links, social media channels, and exchanges that support Crave. Please check our website for a full list.

i. Oficial

- **Website**: `https://crave.cc/`
- **GitHub**: `https://github.com/Crave-Project/Crave-NG/`
- **Emails**: `https://crave.cc/team`
- **Wallets**: `https://crave.cc/wallets/`
- **Mobile Wallet**: `https://coinomi.com/`
- **Block Explorer**: `http://explorer.crave.cc/`

ii. Masternodos

- **Masternode Setup Guide [PDF]**: `https://crave.cc/pdf/Complete_Masternode_Guide_for_Crave_NextGen.pdf`
- **Masternode Setup Guide [Video]**: `https://www.youtube.com/watch?v=GUDvUz7gkBA`
- **Masternode Compilation Script [Linux]**: `https://cdn.discordapp.com/attachments/373145814643638282/420218710826156032/crave-install.sh`
- **Masternode Hosting**: `http://nodeshare.in/coins/crave/order/`

iii. Estadisticas

- **CoinMarketCap**: `https://coinmarketcap.com/currencies/crave`
- **Masternodes.online**: `https://masternodes.online/currencies/CRAVE/`
- **Masternodes.pro**: `https://masternodes.pro/stats/crave`
- **Staking Calculator**: `https://crave.cc/staking`

iv. Comunidad

- **Crave Forum**: `https://forum.crave.cc`
- **Twitter**: `https://twitter.com/craveproject`
- **Discord**: `https://crave.cc/discord`
- **Telegram**: `https://t.me/craveproject`
- **Medium**: `https://medium.com/@CraveProject`
- **Facebook**: `https://www.facebook.com/craveproject/`
- **BitcoinTalk**: `https://bitcointalk.org/index.php?topic=2547950`
- **Reddit**: `https://www.reddit.com/r/craveproject/`

v. Intercambios y pares de negociación

CRAVE/BTC

- **Cryptopia**: `https://www.cryptopia.co.nz/Exchange?market=CRAVE_BTC`
- **CoinExchange.io**: `https://www.coinexchange.io/market/CRAVE/BTC`
- **CryptoBridge**: `https://wallet.crypto-bridge.org/market/BRIDGE.CRAVE_BRIDGE.BTC`
- **TradeSatoshi**: `https://tradesatoshi.com/Exchange?market=CRAVE_BTC`
- **BiteBTC**: `https://bitebtc.com/trade/crave_btc`
- **altilly**: `https://www.altilly.com/market/CRAVE_BTC`

CRAVE/USD

- **BiteBTC**: `https://bitebtc.com/trade/crave_usd`

CRAVE/LTC

- ◇ **Cryptopia**: https://www.cryptopia.co.nz/Exchange?market=CRAVE_LTC
- ◇ **CoinExchange.io**: https://www.coinexchange.io/market/CRAVE/LTC
- ◇ **TradeSatoshi**: https://tradesatoshi.com/Exchange?market=CRAVE_LTC
- ◇ **BiteBTC**: https://bitebtc.com/trade/crave_ltc
- ◇ **altilly**: https://www.altilly.com/market/CRAVE_LTC

CRAVE/ETH

- ◇ **CoinExchange.io**: https://www.coinexchange.io/market/CRAVE/ETH
- ◇ **BiteBTC**: https://bitebtc.com/trade/crave_eth
- ◇ **altilly**: https://www.altilly.com/market/CRAVE_ETH

CRAVE/DOGE

- ◇ **CoinExchange.io**: https://www.coinexchange.io/market/CRAVE/DOGE
- ◇ **TradeSatoshi**: https://tradesatoshi.com/Exchange?market=CRAVE_DOGE

CRAVE/BCH

- ◇ **TradeSatoshi**: https://tradesatoshi.com/Exchange?market=CRAVE_BCH

CRAVE/USDT

- ◇ **TradeSatoshi**: https://tradesatoshi.com/Exchange?market=CRAVE_USDT
- ◇ **altilly**: https://www.altilly.com/market/CRAVE_USDT

C. ESPECIFICACIONES

Especificacion	Descripcion
Abreviacion	CRAVE
Bloque de espaciado	60 seconds
Tamaño de bloque máx.	40 MB
Recompensa total Bloq.	Up to 11 Crave
Recompensa de MN	6 Crave per block
Recompensa x Interes	4 Crave per block
Recompensa de Ppto.	Up to 1 Crave per block
Madurez	88 blocks
Vencimiento	8 hours
Colateral Masternode	5000 Crave
Puerto de nodo maestro.	48882
Puerto de RPC Predet.	48883
Límite Suministro Max.	Infinite
Algoritmo	SHA-256
Preminado	0 Crave
Costo Min. Transaccion	0.0001 Crave/kb
Costo LightX Trans.	0.01 Crave
Zero-Fee Transactions	Yes
Protocolo de soporte	IPV4, IPV6, Tor
Algoritmo Consenso	Blackcoin v3.0 PoS