DAPSCOIN

DECENTRALIZED-ANONYMOUS-PAYMENT-SYSTEM

WHITEPAPER
2019

«La Privacidad es un derecho, no un privilegio»

INTRODUCCIÓN

DAPS es un bloqueo de privacidad planificado que se centra en la seguridad, la escalabilidad y la privacidad total. El objetivo del protocolo DAPS es crear un sistema de apuestas y pagos anónimos con una estructura de gobierno sin confianza, basada en las últimas tecnologías derivadas de Monero y PIVX. Esta es la primera vez en criptomonedas. Los modelos de verificación y consenso de la cadena DAPS se basarán en los nodos de PoS (replanteo y Masternodes) y los mineros de PoA.

¿Cómo lo haremos? Hemos seleccionado cuidadosamente ciertos protocolos probados y el uso conjunto de estas características permitirá una red de blockchain totalmente privada. Planeamos ofrecer el paquete de anonimato más completo en cualquier protocolo hasta la fecha, con una solución en cadena para el "Problema de Confianza". Nuestra solución única al "Problema de confianza" se llama Prueba de Auditoría (PoA), que es la clave de nuestro protocolo.

El objetivo principal de DAPS es anonimizar los activos y asegurar una infraestructura para el desarrollo de una tecnología adicional que establezca precedentes. La privacidad es un derecho, no un privilegio.

DAPS se enorgullece de decir que al momento de escribir este documento técnico, somos la primera moneda en implementar con éxito una cadena de privacidad completa de Staking y Masternode (PoW - PoS - PoA) que incorpora completamente RingCT y Bulletproofs (Prueba de balas).

¿POR QUÉ DAPS?

En cadenas de bloques tradicionales y varias cadenas de anonimato "parcial", los usuarios están expuestos a análisis y vectores de ataques maliciosos. Muchos en todo el mundo utilizan estos datos expuestos para explotar a los usuarios de criptomonedas. Nuestro objetivo es preservar el derecho de todos a controlar sus finanzas cuando lo consideren adecuado. DAPS combinará protocolos de privacidad exitosos y probados en un intento de crear la cadena de bloques más privada hasta la fecha.

Los usuarios están expuestos a análisis y vectores de ataques maliciosos.

HISTORIA DEL PROTOCOLO HARPOCRATES (DAPS)

El Protocolo de Zerocoin (libzerocoin) es la base de muchas de las monedas de privacidad que vemos hoy. Utilizado por otros activos para crear activos de privacidad relativamente seguros y protegidos, este protocolo es altamente examinado y se considera el estándar para la implementación de la privacidad.

Usando esta base de privacidad, muchas monedas expandieron las ideas del protocolo Zerocoin (libzerocoin) de muchas maneras, con un ejemplo notable que es DASH.

El equipo DASH creó una nueva capa llamada "Masternodes" en la parte superior de Bitcoin, esencialmente creando un nodo "incorporado" que se ejecuta 24/7, para fortalecer la red y permitir que se agreguen características adicionales de la cadena. Estas características incluyen Instantsend, Privatesend y permitir a Masternodes votar sobre propuestas, descentralizando la gobernanza de la red de las manos del desarrollador.

* *Nodo incentivado que se ejecuta 24/7*

PIVX fusionó el protocolo Zerocoin con el protocolo Masternode. PIVX amplió este concepto al habilitar un "esquema de recompensa para See-Saw" para Masternodes, para fortalecer los incentivos de Masternode contra el replanteo.

Siguiendo la definición del protocolo del esquema de Pago Anónimo Descentralizado según lo descrito por Sasson et al (2014), el esquema DAP se describe como un método de pago que permite a los usuarios realizar pagos directos y privados entre sí ocultando el origen y el destino del pago, incluyendo el monto del pago. Este enfoque de la criptomoneda emplea pruebas de "conocimiento cero" que impiden el análisis de transacciones o direcciones.

Otra metodología que ha demostrado ser extremadamente robusta y exitosa es RingCT implementada por Monero.
A continuación se muestra un extracto y un enlace al documento.
["Una forma obvia de negar las desventajas del protocolo CryptoNote ... sería implementar importes ocultos para cualquier transacción" Shen Noether, transacciones confidenciales con firma de anillo (RingCT) para Monero]

EL PROBLEMA DE BITCOIN

Bitcoin no es anónimo. Por diseño para evitar gastos dobles, el blockchain es totalmente público y visible para todos. Esto hace que Bitcoin sea confiado. No necesita "confiar" en ningún operador de nodo de Bitcoin ni en la persona que le envía Bitcoin para ser sincero, puede verificar el estado de la cadena con medios de terceros. Puede verificar fácilmente sus propios saldos y transacciones en un libro público. Esta es una de las formas en que la red Bitcoin asegura el estado de la red, al costo de exponer completamente a los usuarios finales a análisis y seguimiento. Pero, hay una desventaja de esta red "sin confianza" (totalmente transparente): las transacciones, los saldos y otros datos son fácilmente rastreados y utilizados por los malos actores. Este problema ha impulsado la idea de las cadenas de bloques "privadas" para convertirse en un foco para la industria.

"PRIVACIDAD" Y SEGURIDAD

No todas las monedas de privacidad son totalmente privadas. En teoría, en una cadena completamente anónima, sin importar el protocolo, los propietarios de nodos pueden coludir fuera de cadena para ejecutar sus nodos de manera maliciosa. Esto puede ser desastroso de muchas maneras para cualquier red y representa un riesgo de seguridad incorporado a las iteraciones actuales de blockchains privadas. Si los nodos se pusieran de acuerdo, generen monedas infinitas para ellos mismos en secreto y se las gasten, el mundo no podría descubrir esto, ya que las transacciones y los saldos se ocultarán de la vista pública.

Como no se pueden "deshacer" estos ataques sin causar una división de la cadena, es crítico poder detectar ataques o colusión fuera de la cadena a medida que ocurren. ¿Cómo verificar el estado de la red, cuando las personas que le informan de su estado tiene algún tipo de falta de honradez?

La mayoría de los equipos evitan la idea de blockchains privados debido a la explotabilidad inherente. Esta vulnerabilidad es causada por la incapacidad de rastrear el estado de la red y las emisiones de un tercero neutral. El ejemplo más prominente de esta debilidad crítica es la explotación constante de las redes de "crianza de Zerocoin" y CryptoNote.

¿QUÉ ES EL "PROBLEMA DE CONFIANZA"?

Para ser confiado, un tercer objetivo debe ser capaz de verificar el suministro de monedas, verificar las emisiones de las monedas y asegurarse de que los nodos no se usan de manera malintencionada. No creemos que confiar en la honestidad de los propietarios de nodos deba ser el único respaldo contra las acciones maliciosas.

Para las cadenas de bloques de privacidad basadas en Masternode, se debe dar un grado de confianza a estos "Masternodes" como gobierno central del suministro de monedas, de la inflación y de varias especificaciones. Para las redes de privacidad que no son de Masternode y que usan zk-SNARK, la red requiere una ceremonia de implementación complicada, en la que se expone una información de control de la red a un pequeño grupo de miembros. Si estos miembros no borran completamente estos datos (y no los memorizan), la red puede ser controlada por ellos.

Este es el "problema de confianza". Debe confiar en los nodos o en un grupo de "administradores" y figuras centrales que puedan controlar la red completa a su antojo. Las iteraciones actuales de Masternodes y las cadenas de bloques totalmente privadas (zk-SNARK, Ring CT con ofuscación completa) divergen del estado "confiado" de las cadenas de bloques públicas.

Muchas monedas no privadas también ignoran completamente estas estructuras de gobierno y configuraciones de red confiables, declarándose una red dominada por la autoridad central totalmente centralizada.

Creemos que estas redes son peligrosas para bloquear en conjunto y violan los principios de la visión de Satoshi. Ninguna constitución, convenio o acuerdo por escrito hecho por el hombre puede ser tan seguro como los fundamentos de un libro mayor de blockchain asegurado por un tercero.

¿Cómo abordaremos estos problemas? Prueba de Auditoría (PoA) presentará falta de confianza al sistema basado de Confianza de otras monedas de privacidad.

**Esto permitirá el despliegue de cadenas de bloques totalmente privadas utilizando las herramientas disponibles actualmente y puede expandirse a muchas redes existentes.*

¿QUÉ NOS DIFERENCIA?

La idea de Prueba de Auditoría y la implementación del protocolo DAPS se llama el protocolo HARPOCRATES y se establecerá como un nuevo estándar de la industria.

Utilizando las siguientes tecnologías clave:

- **Ring CT (Transacciones Confidenciales con firma de anillo)**
- **Bulletproofs (Prueba de balas)**
- **Stealth Addresses (Direcciones de Sigilo u Ocultas)**
- **Stealth Transactions (Transacciones Ocultas)**
- **Proof of Audit (Prueba de Auditoría - PoA)**

Logramos la ofuscación completa de todos los usuarios y transacciones. Esta combinación de características, que incluye la Prueba-de-Auditoría, que llamamos "El Protocolo de Harpócrates", crea una red de cadenas de bloques anónimas totalmente confiables.

DESCRIPCIÓN DE DAPS

DAPS es un sistema híbrido de cadena de bloques PoW-PoS-PoA (Prueba de Auditoría) que se centra en la privacidad de los usuarios. DAPS ofrece las siguientes características únicas:

- Un sistema de blockchain centrado en la privacidad que garantiza que cada transacción de usuario en la red se mantenga privada. Esto significa que aunque todas las transacciones de los usuarios se publican completamente en la cadena de bloques, ningún tercero (excepto el remitente y el receptor de la transacción) puede revelar la información detallada dentro de la transacción. Específicamente, la siguiente información se mantiene privada en el sistema DAPS:
  - Remitente de la transacción: el remitente de la transacción está totalmente ofuscado
  - Receptor de transacciones: además de una clave pública generada por mí como receptor de la transacción, ningún tercero puede revelar la identidad del receptor de la transacción ni las relaciones entre la clave pública del receptor y su identidad
  - El monto de la transacción se codifica para que ningún tercero pueda revelar dicha cantidad dentro de la transacción.
- Un sistema híbrido de cadena de bloques que se compone de diferentes tipos de bloques en la misma cadena:
  - Los 500 bloques iniciales son bloques de PoW que son extraídos por la fundación DAPS para proporcionar el suministro inicial, que se indica en el documento técnico de DAPS.
  - Desde el bloque 501, la cadena de bloques DAPS se convierte en un híbrido de bloques PoS y PoA. Los bloques de PoS se acuñan de forma contundente al apilar nodos para verificar las transacciones de los usuarios de la cadena de bloques DAPS. Se crea un bloque PoS cada minuto.
  - Los bloques de PoA tienen un bloque de 1 hora. Los bloques de PoA son extraídos por actores externos para auditar que el sistema ha estado funcionando correctamente según las reglas especificadas. Un bloque de PoA debe volver a auditar al menos 59 bloques de PoS para su corrección. Por este trabajo, los mineros en bloque de PoA también son recompensados por continuar con la auditoría del sistema.

MECANISMOS DE CONSENSO DE DAPS COIN:
MASTERNODES, STAKING Y PRUEBA DE AUDITORÍA

Se requiere que los Masternodes de DAPS tengan 1.000.000 de DAPS Coin de garantía colateral, una dirección IP dedicada, y que puedan funcionar las 24 horas del día sin una pérdida de conexión de más de 1 hora. A los Masternodes se les paga utilizando el método See-Saw como se describe en la siguiente sección. Por ofrecer sus servicios a la red, a los Masternodes se les paga una parte de las recompensas del bloque para mantener el ecosistema. Este pago se realizará en DAPS y sirve como una forma de ingreso pasivo para los propietarios de Masternodes.

El sistema Masternode de DAPS está modelado después del sistema Masternode de PIVX. Esto tiene muchas bonificaciones, incluida la prevención de un ataque del 51% a menos que las capas de Prueba de estaca y Masternode estén comprometidas simultáneamente.

El SBRS (sistema de recompensa de equilibrio See-Saw) tendrá una compensación de recompensa dividida en MN 60% /PoS 40% hasta MN 40%/PoS 60% como máximo. Esto dará una justa recompensa a los titulares.

La verificación de la cadena se realizará utilizando Prueba de auditoría, Masternodes y Prueba de Stake (v3). Esto le dará a la red DAPS resistencia contra la mayoría de los ataques conocidos y garantizará que la cadena sea segura y, al mismo tiempo, se pueda analizar públicamente

Si bien DAPS no es confiable, es necesario que haya un elemento de confianza.
Los Masternodes en cualquier cadena de Masternode se ven como un nodo confiable. Esto se debe a la garantía en monedas que se guarda como parte de garantía en la transacción para que el Masternode se considere de confianza. DAPS es por diseño, anónimo con transacciones ocultas en montos. Esto presenta un problema específico al colateralizar un Masternode y garantizar que el colateral sea correcto y esté bloqueado.
Por lo tanto, todas las garantías para transacciones de Masternodes tienen una cantidad visible que no es ni a prueba de balas ni parte de la firma de un anillo.
Tan pronto como se descolateraliza el Masternode, el UTXO que fue colateralizado se devuelve a la billetera designada y se trata como una transacción normal.

MODO SIGILO OBLIGATORIO

DAPS tiene un sistema de direcciones de sigilo obligatorio y todas las cantidades en las transacciones de los usuarios se ocultan mediante codificación. Al crear una transacción, el remitente genera una clave pública de transacción por UTXO, que luego se utiliza para generar una clave pública generada una sola vez (correspondiente a una dirección de Bitcoin). La clave privada de esta última solo la obtiene el receptor de la transacción, que tiene claves privadas de gasto y visualización (que se describen más adelante). Los montos de transacción se codifican utilizando un esquema de cifrado simétrico que utiliza la Curva-Elíptica de Diffie-Hellman (ECDH) para codificar los montos de transacción, que sólo pueden ser revelados por el remitente y el receptor de la transacción. La clave pública de la transacción permitirá al titular de la clave privada generada revelar sólo el monto de esa transacción. Ninguna otra transacción puede ser desbloqueada con la misma llave.

EMISIONES

Las emisiones de monedas de DAPS serán de 1050 DAPS por bloque. Habrá una tarifa de 50 DAPS por bloque ("tarifa del Fundador") asignada al fondo de desarrollo de DAPS, que se utilizará para desarrollar y sostener el proyecto a largo plazo.

La estructura tarifaria será como tal:

1050 emisiones por bloque PoS
50 DAPS al fondo de desarrollo.
900 para dividir entre el nodo de replanteo que acuñó el bloque y un Masternode
El sistema de See-Saw 60/40 significa una división de 540/360 como arriba
100 reservados para el minero PoA que audita el bloque.

El “Sistema de Balanceo de recompensa See-Saw” es un método por el cual la red equilibra el porcentaje de la recompensa pagada al staking y a los masternodes.
Si hay 1000 MN y 1000 nodos de replanteo, el sistema lo ve igual y mantiene el sistema 60/40 See-Saw a favor de los Masternodes. Esto se debe a que han “invertido” el millón de DAPS mediante la garantía de su Masternode.

Si el número de nodos cambia drásticamente en la dirección de más Masternodes, la red reequilibra la ecuación a 40/60, esta vez favoreciendo a los nodos de replanteo.

Esto asegurará la salud de la red a largo plazo, al equilibrar las recompensas de Masternode contra staking, lo que evitará el crecimiento desbocado de Masternodes.

ESPECIFICACIONES DE DAPS TOKEN:

Token ERC-20
Suministro: 60.000.000.000
Distribución de DAPS: vía AIRDROP

ESPECIFICACIONES DE DAPS COIN:

Suministro inicial: 60.000.000.000 DAPS
Capacidad de suministro: 60.000.000.000 [inicial]+10.000.000.000 [emisión] Consenso DAPS: Prueba-de-Auditotia, Prueba-de-Stake v3, Masternodes (recompensas See-saw)
Técnicas de privacidad: Firma de anillo basada en Secp256k1, RingCT, y prueba de rango Bulletproof
Tiempo de bloque: 1 minuto
Recompensa por bloque: Ver Emisiones arriba.
Confirmaciones requeridas para gastar: 4 bloques.
Maduración de estaca: 100 bloques.
Emisiones aproximadas: ~551 milliones de DAPS por año hasta 10 mil millones de DAPS.

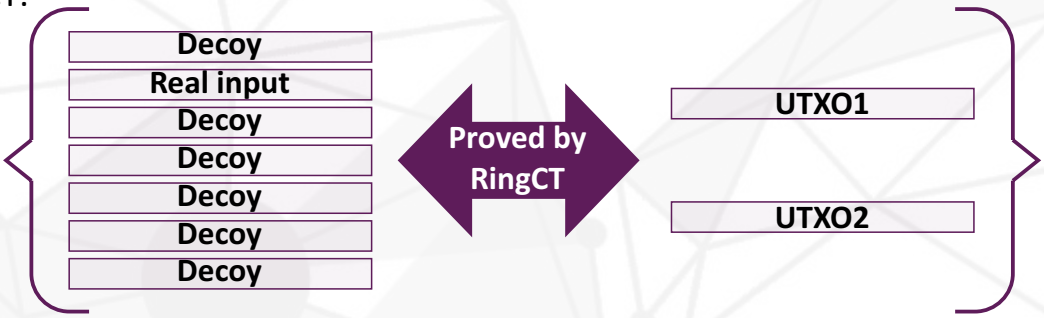
LA CADENA DE BLOQUES DE DAPS:

RINGCT

RingCT o "Ring Confidential Transaction" es una forma de mezclar en una transacción real con un número predeterminado de transacciones falsas. El tamaño del anillo determina el número de transacciones falsas adicionales que se agregan. Esto significa que la transacción real está oculta en una mezcla de transacciones falsas y, por lo tanto, la transacción real y su monto son mucho más difíciles de discernir.

Mientras que Monero ha implementado un tamaño de anillo establecido - actualmente 11 - DAPS tendrá un tamaño de anillo generado aleatoriamente por transacción dentro de un rango determinado (6 -12). Esto permite que la red sea aún más segura al garantizar que el usuario no siempre seleccione un tamaño específico, lo que crea una trazabilidad mediante el hábito.

Mientras que las firmas de anillo ocultan los verdaderos UTXO utilizados como entradas en una transacción (consulte la siguiente figura) y detecta cualquier gasto doble, RingCT permite que los nodos completos demuestren que la suma de los importes de entrada de la transacción es igual a la suma de las cantidades de UTXO más la tarifa de la transacción. Esto es importante porque todos los montos de transacción en DAPS están ocultos por defecto y solo existen en forma de compromisos de Pederson y montos codificados. RingCT no requiere la revelación de los montos de las transacciones, al mismo tiempo que puede demostrar que las sumas en ambos lados de entrada y salida son iguales. La siguiente figura muestra cómo se utilizan juntas la firma Ring y la RingCT.



LA CADENA DE BLOQUES DE DAPS:

BULLETPROOFS

Los Bulletproofs son pruebas cortas de conocimiento cero que no requieren interacción y que no requieren una configuración confiable. Se puede usar una prueba de balas para convencer a un verificador de que un texto plano cifrado está bien formado. Por ejemplo, compruebe que un número encriptado está dentro de un rango determinado, sin revelar nada más sobre el número. En comparación con los SNARK, los Bulletproofs no requieren una configuración confiable. Sin embargo, verificar un Bulletproof requiere más tiempo que verificar un SNARK.

Los Bulletproofs están diseñados para permitir transacciones confidenciales eficientes en Bitcoin y otras criptomonedas. Las transacciones confidenciales ocultan el monto que se transfiere en la transacción. Cada transacción confidencial contiene una prueba criptográfica de que la transacción es válida. Bulletproofs reduce el tamaño de la prueba criptográfica de más de 10kB a menos de 1kB. Además, Bulletproofs admite la agregación de pruebas, de modo que la prueba de que *m* valores de transacción son válidos agrega solo O (log (m)) elementos adicionales al tamaño de una sola prueba. Si todas las transacciones de Bitcoin fueran confidenciales y usaran pruebas de balas, entonces el tamaño total del conjunto UTXO sería de solo 17 GB, en comparación con los 160 GB de las pruebas utilizadas actualmente.

DAPS utiliza Bulletproofs como pruebas de rango para demostrar que los montos de transacción en la transacción son positivos. Esto es crítico porque secp256k1 funciona con un número de espacio circular y no hay forma de que un nodo completo pueda verificar que las cantidades codificadas son siempre positivas. Sin que Bulletproofs compruebe que los montos de las transacciones son positivos, un atacante puede crear una transacción con un UTXO que tenga un monto positivo enorme, mientras que el otro UTXO tendrá un monto negativo y la suma de estos dos montos más las tarifas de transacción igualan a la suma de las entradas, lo que resulta en una omisión de la verificación de RingCT.

LA CADENA DE BLOQUES DE DAPS:

DIRECCIONES DE SIGILO

Las direcciones de sigilo, al igual que las transacciones de sigilo, son otra piedra angular de DAPS. Donde las direcciones estándar son bastante fáciles de leer y pueden ser fácilmente identificadas como:
3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

Las direcciones sigilosas de DAPS son bastante diferentes. El siguiente es un ejemplo de una dirección pública DAPS

41k8JcYj2EG4eDHbpPNneDdKvFqHFpQNMMGykRUorNnihiY4RaRNdLiUUfThfzugo5auHkq
ThwQgZ3EixmxyoDkj17c7Qy6BVWP

Las llamamos "Cuentas de Privacidad".

Se podría argumentar que si esta dirección es pública, ¿cómo se logra el anonimato entonces?
En DAPS, si un remitente desea enviar a un destinatario, la dirección pública del destinatario se usará para generar una clave / dirección pública generada por única vez basada en una clave pública de transacción generada por el remitente según UTXO.

La particularidad de este esquema es que al generar esta clave pública generada una sola vez, el remitente no tiene forma de generar la clave privada correspondiente para canjear el UTXO más adelante. Dicha clave privada solo puede obtenerla el propietario de la dirección pública, que tiene ambos pares de claves privadas en nuestro sistema de clave doble que se explica a continuación.

SISTEMA DE DIRECCIÓN PÚBLICA DUAL-KEY

DAPS utiliza un sistema de doble clave para proporcionar direcciones ocultas para ofuscar las direcciones. Una dirección pública se deriva de un par de claves de vista-gasto privado. Una dirección pública puede contener una ID de pago opcional, que generalmente se utiliza en los intercambios.
DAPS utiliza la curva EC secp256k1 para derivar claves públicas de las claves privadas correspondientes.

Field	Description
Header	1-byte length. Header = 19 if it is an integrated address, otherwise Header=18
Public spend key	Public spend key in compressed form, whose length is 33 bytes.
Public view key	Public view key in compressed form, whose length is 33 bytes.
paymentID	8-byte field used by exchanges for recognizing transactions from different users
Checksum	4 first bytes of the hash of the above fields

LA CADENA DE BLOQUES DE DAPS:

La dirección pública se codifica en formato base58 para cada bloque de 8 bytes de la dirección pública de la siguiente manera:

- Dirección Pública normal: 71 bytes, dividida en ocho bloques de 8-byte y un bloque de 7-byte. Cada bloque de dirección está codificado en formato base58, lo que da como resultado 11 caracteres base58 por bloque de dirección => 99 caracteres Base58.
- Dirección integrada: 79 bytes, dividida en nueve bloques de 8-byte y un bloque de 7-byte, dando como resultado 110 caracteres Base58.

TRANSACCIONES DE SIGILO

La dirección pública / dirección integrada del receptor para una transacción debe enviarse al remitente, cuya billetera realiza los siguientes pasos para crear una transacción totalmente privada:

- Analizar la dirección pública para extraer la clave de vista pública Pv, la clave de gasto público Ps y la ID de pago (opcional) del receptor.
- Comprueba si la cartera tiene saldo suficiente para enviar.
- Genera una clave pública P una sola vez para el receptor de la siguiente manera:
  - Genera una transacción en la clave privada Ts y su transacción en la clave pública Tp
  - P = H(Ts*Pv) * G + Ps donde;
    - H es una función hash
    - * y + son la multiplicación y la suma en la curva secp256k1
    - G es el punto generador de base en la curva secp256k1
  - Una vez generada la clave pública por cada salida de transacción en la transacción realizada. Cada transacción en la salida tiene una transacción diferente en la clave privada para evitar cualquier fondo no canjeable con firma de anillo que se describe a continuación.
- Crea una salida de transacción con el destino como la clave pública anterior generada y la cantidad de envío esperada.
  - Crea un compromiso Pedersen para la transacción en la salida.
  - Genera la curva elíptica Diffie-Hellman secreta EECDHS .
  - Codifica la cantidad de la transacción en la salida con el secreto de ECDHS.
  - Genera Bulletproofs para el importe de salida de la transacción.
- Selecciona un conjunto de UTXO gastable para ser entradas de transacciones.
  - Calcula la tarifa de transacción basada en una tarifa estimada
  - Calcula el cambio = Suma de entradas de transacciones - monto enviado - tarifa Tx
  - Hace explícita la tarifa de la transacción.
  - Genera imágenes clave y las pone en la entrada de la transacción.
- Genera la firma de anillo.
  - Genera un numero aleatorio de tamaño de anillo (6-12)
  - Para cada transacción entrante, selecciona señuelos de tamaño de anillo.
  - Calcula la firma de anillo multikey basada en Monero RingCT y la firma de anillo.

MASTERNODES Y STAKING EN DAPS

En los sistemas basados en masternode como PIVX, los masternodes son recompensados por proporcionar servicios adicionales como el "envío instantáneo" y las recompensas se envían a la dirección que tiene las monedas garantizadas. Si se usara un mecanismo de este tipo en DAPS, los fondos para masternodes se perderían porque las firmas de anillo detectarán o marcarán una transacción como doble gasto incluso si se gastan dos UTXO diferentes de la misma dirección en la transacción. Esto significa que solo una de las recompensas UTXO de masternode se puede canjear si las recompensas se envían a la misma dirección.

DAPS está diseñado para que este mecanismo de incentivo de masternode genere una nueva dirección / clave pública cada vez que se recompense el masternode. DAPS lo hace exigiendo a los usuarios que introduzcan la dirección pública (la dirección larga) en la transacción de garantía. La dirección pública de masternode se pondrá en la cola de pago. Durante la creación de un bloque de PoS, un nodo de replanteo tomará una de las direcciones públicas en la cola y generará una clave pública por única vez para el pago de masternode. Esto asegurará que todas las recompensas UTXO de masternode se gastarán.

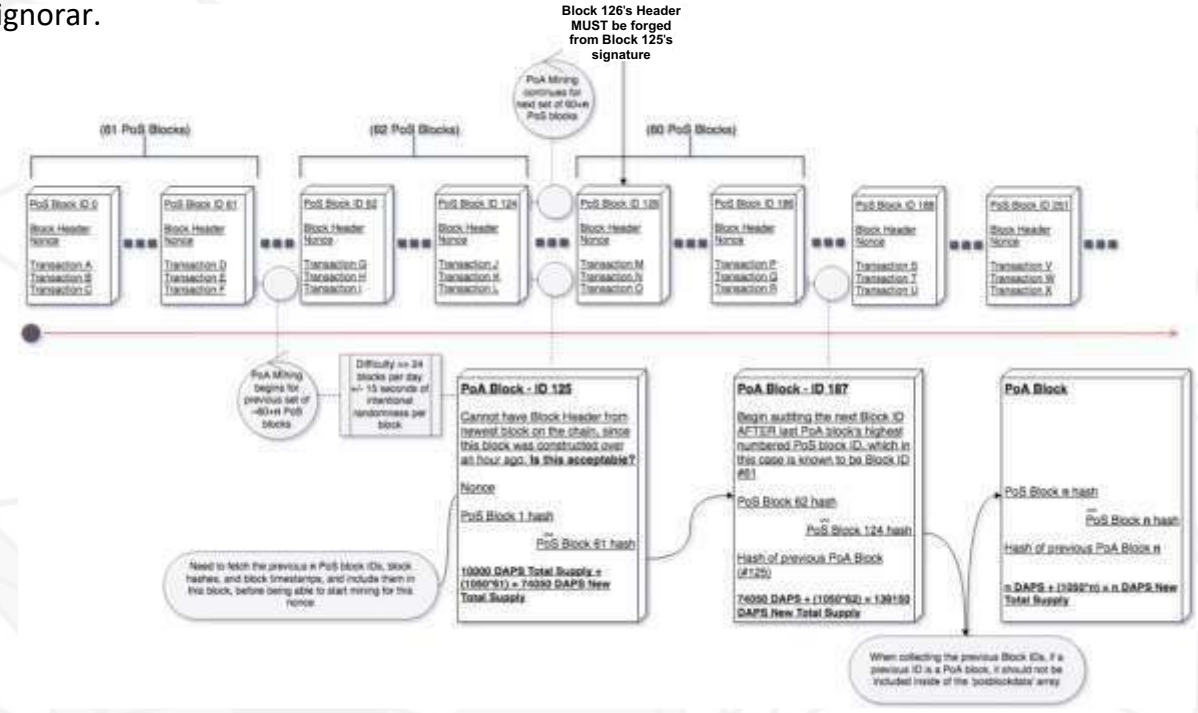
Este mecanismo también se aplica al nodo de replanteo al crear bloques de PoS para garantizar que todas las recompensas de reparto se envíen a diferentes claves públicas.

DETALLES DE CONSENSO EN POA Y POS

1. No se aceptará ningún bloque PoA en la cadena a menos que hayan transcurrido al menos 59-60 minutos desde la marca de tiempo del bloque PoA previo aceptado. *Esto debería garantizar que los bloques PoA permanezcan espaciados a lo largo de la cadena y no puedan terminar espalda con espalda por ninguna razón.*
2. 2. Un bloque PoA debe contener el hash del bloque PoA anterior, formando así una sub-cadena de bloques PoA de cadena continua.
3. Un bloque PA no debe incluir el hash de otro bloque PoA, la altura o marca de tiempo en su propio array `posblocksaudited´.
4. Cada hash de bloque incluido en `posblocksaudited´ debe ser un hash válido de un bloque PoS que actualmente se puede ver en la cadena.
5. Cada marca de tiempo de bloque incluida en `posblocksudited´ debe ser desde un momento anterior a la marca de tiempo del bloque PoA. No se permite que ningún bloque PoA audite bloques que hayan ocurrido después de sí mismo.
6. No se permite que un bloque PoA audite el hash de un bloque PoS que otro bloque PoA ya haya auditado.

Un bloque de PoA se puede agregar a la cadena en cualquier momento. Esto permite que los bloques de PoS continúen con su proceso mínimo de inhibición, y un bloque de PoA tendría que seleccionar un cierto número de bloques de PoS secuenciales existentes para auditar, hacer un registro de sus ID de bloque + hashes de bloque + marcas de tiempo como un relacional lista ordenada por ID de bloque, y luego se agrega a la cadena como la siguiente ID de bloque en línea.

Los futuros bloques de PoA buscan el ID de bloque PoA anterior, buscan en su interior el ID de bloque de PoS con el número más alto y luego inician su proceso de auditoría, teniendo en cuenta que si cualquiera de esos ID de bloque es un bloque PoA, se debe ignorar.



TOR/OBFS4

En las versiones anteriores de este informe se habló sobre el uso de TOR y OBFS4. Después de una investigación exhaustiva, se ha tomado la decisión de excluirlos de la pila de tecnología por ahora.
Las razones para esto son simples pero tienen un peso significativo. TOR está bloqueado por muchos ISP's a nivel mundial, lo que requiere extensos procedimientos de configuración para "puentear"
En las comunicaciones, esto puede hacer que muchas personas no quieran utilizar DAPS debido a una gran barrera de entrada.
Otro problema relacionado con los ISP y los TOR es que muchos ISP, al ver a alguien que usa los TOR, independientemente de la razón, le advierten a la persona que no lo haga de nuevo; de lo contrario, su cuenta podría cerrarse o simplemente cerrar la cuenta sin previo aviso. De cualquier manera, esto es
malo y, a veces, incluso puede terminar con una visita de la policía. Esto no es algo que queremos
Estamos investigando activamente los TOR en profundidad y el consenso general es que podemos introducir TOR como "opcional" en una versión futura. Debido a que estos son sistemas periféricos que usan TOR, la cadena no tendrá que ser restablecida, dividida o bifurcada para esto.

OTRAS CARACTERÍSTICAS

- Emisiones estáticas: No hay modelos de inflación elegantes, emisiones planas.
- Hasta 2MB de tamaño de bloque.
- Masternodes: Incentivados los nodos 24/7 que pueden usarse para funciones avanzadas.
- Multinodes: Múltiples masternodes por instancia. ¡No más spam de servidor!

Al utilizar las funciones de la cadena anterior, esperamos ofuscar completamente las transacciones, direcciones, saldos y nodos / IP. Con una auditoría de suministro de monedas incorporada en la cadena, el sistema será confiado y evitará el problema de "confianza" de las monedas totalmente privadas. Esta combinación única de características basadas en una red de apuestas se llamará Protocolo Harpocrates y creemos que cambiará el estándar para las monedas de privacidad. Creemos que Proof-Of-Audit también puede aumentar y mejorar otros protocolos contemporáneos, haciendo que la misión de nuestro proyecto sea beneficiosa para la industria en general.

- Ecosistema DAPS & el Mundo: Se emprenderán iniciativas para incorporar a DAPS en el uso y utilidad real para estimular la adopción masiva.

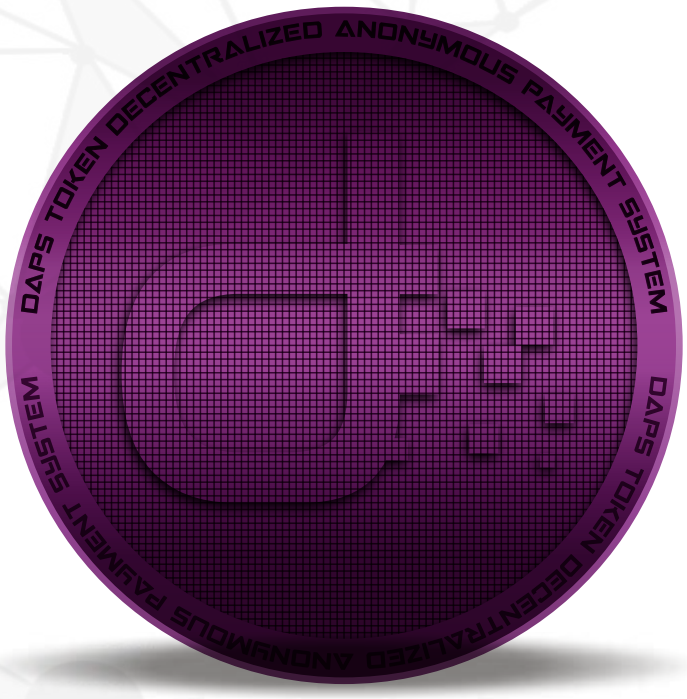
NOTAS:

Tenga en cuenta que este documento no es un prospecto. Se constituyó solo con fines informativos, para presentar el proyecto DAPS Coin a partir de 2019. Tenga en cuenta que no es necesario realizar ninguna compra. Eres libre de participar en el proyecto o no. Es su responsabilidad revisar las leyes vigentes en su país antes de comprar o unirse a DAPS. Debe leer, comprender y aceptar los términos de este documento antes de involucrarse en el proyecto.

Las especificaciones y la información técnica pueden estar sujetas a cambios.

DAPS completó una prueba exitosa en marzo de 2019.

DAPS se someterá a una auditoría de código de terceros antes del lanzamiento de mainnet.



DOCUMENTACIÓN:

Bitcoin trustless

Z-cash Trust Problem

Libzerocoin Protocol

DAP Protocol, by Sasson et al

Masternodes

Masternodes

See-saw reward scheme

Posv3

Ring CT

Bulletproofs

Stealth Addresses