



Documento técnico de Viacoin

Equipo de desarrollo de Viacoin
12 de septiembre de 2017

Viacoin Dev Team

Última actualización el 12 de noviembre de 2017

Abstracto

Viacoin es una moneda criptográfica de código abierto creada en 2014, derivada del [6] protocolo de Bitcoin que admite el consenso integrado con un OP_RETURN extendido de

120 bytes (es un comando en el lenguaje de scripting de Bitcoin que se agregó específicamente para permitir la inclusión de metadatos en el blockchain. Actualmente se pueden agregar 80 bytes de información a una transacción usando este script frente a los 120 bytes de viacoin).

Viacoin ofrece la posibilidad de minado Scrypt conjunto con otras monedas, también llamado Auxiliary proof of work o AuxPoW, y transacciones 25 veces más rápidas que Bitcoin. La mitad de la recompensa minera de Viacoin se lleva a cabo cada 6 meses y tiene un suministro total de 23,176,392.41459 monedas.

La tasa de inflación de Viacoin es baja debido a la recompensa mínima de la minería. Como la recompensa de bloque de Viacoin es baja, los mineros reciben incentivos para minar Viacoin a través de la minería fusionada (AuxPoW). Actualmente, Viacoin está explotado por uno de los pools mineros más grandes (F2Pool) con una muy alta tasa de hash, último dato total(8/12/2017) fue de 25 TH/s. Por ejemplo, si una red alcanza un hash rate de 25 TH/s significa que puede hacer 25 billones de cálculos por segundo.

Otras características incluyen un algoritmo de ajuste de dificultad de minería para abordar los defectos en Kimoto Gravity Well (DarkGravityWave), Versionbits es una forma de introducir cambios de reglas compatibles hacia atrás en las reglas de consenso de la red , conocido como bifurcación o soft fork. A su vez permiten a los mineros indicar que pueden validar las reglas del soft fork para permitir hasta 29 cambios simultáneos en el software de la red, esto permite introducir cambios como Segwit y Lightning Network

small Note: The whitepaper, documentation, designs are in research and development phase and subject to change.



Viacoin Whitepaper

1. Scrypt

En criptografía, [7] Scrypt es una función de derivación de clave basada en contraseña creada por Colin Percival. El algoritmo fue diseñado para que sea costoso realizar ataques de hardware personalizados a gran escala al requerir grandes cantidades de memoria. En 2012, el algoritmo fue publicado por el IETF (The Internet Engineering Task Force) como un borrador de Internet destinado a convertirse en un RFC (Request for Comments) informativo, pero una versión de Scrypt es ahora utilizada como una prueba de esquema de trabajo por criptomonedas como Viacoin.

Scrypt es una función de derivación de memoria de acceso con llave (En criptografía, una función de derivación de clave (KDF) deriva una o más claves secretas de un valor secreto como una clave maestra, una contraseña o una frase de contraseña utilizando una función pseudoaleatoria)

Scrypt requiere una cantidad razonablemente grande de memoria de acceso aleatorio para ser evaluada. Esto hace que la implementación en hardware personalizado de propósito especial (ASIC) requiera más área VLSI, lo que haría que no sea rentable construir con el propósito de explotar el minado de Viacoin. La característica del algoritmo Scrypt es una gran cantidad de bits pseudoaleatorios que se guardarán en la memoria y una clave que se deriva de esto. El algoritmo se basa en TMTO (Time-Memory Tradeoff). La ventaja de ASIC en Viacoin se reduce en un factor de 10 en comparación con Bitcoin.

Scrypt usa los siguientes parámetros para generar una clave derivada:

- Frase de contraseña: cadena de caracteres para el hash
- Salt: cadena aleatoria proporcionada a las funciones de Scrypt
- N: parámetro de costo de memoria / CPU
- P: parámetro de paralelización
- R: parámetro Blocksize
- dkLen: longitud prevista de la clave derivada de la clave en bytes

$kd = \text{scrypt}(P, S, N, P, R, dkLen)$

Parámetros de Viacoin donde N = 1024, R = 1, P = 1 y S = 80 bytes aleatorios que producen una salida de 256 bits



Viacoin Whitepaper

2. Minería combinada AuxPoW

[2] La minería fusionada de Viacoin tiene como objetivo reutilizar el poder minero de cualquier otra moneda [7] Scrypt agregando de ese modo seguridad a la Blockchain de Viacoin, permitiendo al minero minar más de una cadena de bloques al mismo tiempo. Por ejemplo, un minero podría minar Viacoin y Litecoin o cualquier otra moneda de Scrypt junto con Viacoin con poco o ningún impacto en el hashrate de cualquiera de los dos.

Cada hash que el minero contribuye es para el hashrate total de ambas criptomonedas y da como resultado una blockchain más segura. Un bloque AuxPoW es un tipo de bloque similar a un bloque Bitcoin estándar con dos diferencias. El hash del encabezado del bloque no cumple con el nivel de dificultad de la cadena de bloques. En segundo lugar, tiene elementos de datos adicionales que muestran que el minero que creó un bloque hizo la minería en la blockchain padre y que el minado cumple con el nivel de dificultad de la cadena aux.

Los mineros tienen un incentivo para minar Viacoin, incluso si la recompensa es baja, ya que pueden extraer cualquier otra moneda Scrypt simultáneamente, Viacoin "gratis". Dado que la extracción de Viacoin no está impulsada por grandes recompensas de bloque, esto permite que Viacoin tenga una menor tasa de inflación en comparación con otras criptomonedas que no admiten minería fusionada.

3. Dark Gravity Wave

[3] Dark Gravity Wave (DGW) es un algoritmo de dificultad de código abierto. DGW fue escrito por Evan Duffield, el desarrollador y creador de X11 / Darkcoin / Dash. El algoritmo fue diseñado para abordar defectos como el Tiempo warp attack en el algoritmo de Kimoto Gravity Well.

Dark Gravity Wave se introdujo por primera vez en Dash (Darkcoin). DGW hace uso de múltiples medias móviles exponenciales y medias móviles simples para suavizar el mecanismo de reajuste.

Fórmula:

$$2222222 / (((\text{Difficulty} + 2600) / 9)^2)$$



Viacoin Whitepaper

4. Segwit

Viacoin tiene [12] Segwit (BIP 141) activado. Segregated Witness ayuda a reducir el tamaño de una transacción y hacer frente al crecimiento UTXO. Segregated Witness es un formato de transacción donde los datos de testigos están segregados de la transacción. También tiene como objetivo aumentar el rendimiento de la transacción por bloque en un factor de 2 o 3, mientras que simultáneamente, la sincronización de bloques es más rápida para los nuevos nodos.

El principal objetivo de la implementación de Segwit en Viacoin no es aumentar la capacidad, sino solucionar la maleabilidad y hacer que el código sea más fáciles de actualizar. La corrección de la maleabilidad permite agregar características en Viacoin como [1] swaps atómicos, canales de pago bidireccionales y redes Lightning que podrían aumentar Interoperabilidad de Viacoin con Bitcoin.

Segwit incluye versiones para scripts para que los códigos de operación adicionales (que normalmente requieren un hard-fork en transacciones no segwit) pueden usarse en su lugar. Cambios más fáciles en los códigos de operación de los scripts harán que Viacoin avance más fácilmente. Esto hace posible agregar firmas Schnorr, cadenas laterales, MAST y otras características.

5. The Lightning Network (la red lightning)

[8] La Lightning Network es una red de transferencia que opera en una capa por encima de la cadena de bloques de Viacoin utilizando la funcionalidad de contratos inteligentes en la blockchain para permitir pagos instantáneos a través de una red de participantes. Esta permite mejoras de varios órdenes de magnitud en el rendimiento de transacción moviendo la mayoría de transacciones fuera de los libros de consenso a canales de pago. Esto permite de millones a miles de millones de transacciones por segundo en toda la red. Una capacidad que sortea los carriles de pago heredados. Esto es posible gracias a scripts en cadena en los que las partes entran en contratos de estado bilaterales, en los cuales el estado puede actualizarse compartiendo una firma digital y se puede cerrar publicando evidencia en el blockchain.

Lightning Network permite tarifas excepcionalmente bajas. Para una transacción de bajo valor, Lightning Network es la bala de plata. Permite nuevos tipos de comercio. Al abrir un canal de pago con muchos participantes en la LN, éstos pueden convertirse en un punto focal para enrutar el pago de otros, lo que conduce a una red de pagos completamente conectada. Los pagos se aplican mediante un script que aplica la atomicidad a través del decremento de los bloqueos de tiempo (time-locks).



Viacoin Whitepaper

Otro beneficio es la posibilidad de transacciones atómicas cruzadas, que permiten a los usuarios intercambiar viacoin, bitcoin, Litecoin y otras monedas Segwit de forma instantánea, lo que permite intercambios extremadamente eficientes y descentralizados o una forma descentralizada de 'Shapeshift.io'.

6. Firmas Schnorr

La agregación de firmas Schnorr también forma parte de próximos desarrollos. Esta funcionalidad también ha sido propuesta en Bitcoin como el sucesor de ECDSA, ya que es un algoritmo más eficiente. Hasta hace poco, en Viacoin y en muchas otras criptomonedas, no fue posible implementar las firmas Schnorr sin un hardfork. Ahora con la maleabilidad de Segwit es posible. Todos los datos de firma se mueven al testigo. Viacoin actualmente utiliza firmas digitales de curvas elípticas (ECDSA) como prueba de propiedad zk para autorizar la transferencia de una salida a otra. En 2015, Daniel J. Bernstein propuso usar Schnorr como una firma encima de una curva elíptica.

Algunas ventajas:

- Más seguro bajo supuestos estándar
- Inmunidad a la maleabilidad
- Resistencia a las colisiones con función hash
- Validación de lotes para una aceleración 2-3x
- Implementación nativa de multifirmas k-of-k...

Las firmas Schnorr soportan la validación de lotes, lo que significa que si tienes un grupo de pares de mensajes de clave pública y firmas en lugar de solo uno, puedes verificar la autenticidad del grupo como un todo a una velocidad superior que si se hiciera a cada uno de ellos individualmente. Este método es ideal ya que bloques son sólo grandes lotes de firmas para validar.



Viacoin Whitepaper

Las firmas múltiples nativas k-of-k, la idea de Schnorr es que puedes tomar varias claves juntas y tener una sola firma que demuestre que todos están firmados. Un grupo puede crear una firma válida para suma de llaves. Si U1, U2 y U3 son los usuarios. Hay un esquema de interacción de 2 rondas donde todos vienen con un nonce (número arbitrario que sólo puede usarse una vez) k1, k2, k3 y todos ellos calculan un punto público correspondiente R1, R2, R3. Se comunican entre sí y los suman con un valor total de R. Este valor total de R firma este nonce con su propia clave que resulta en un S1, 2, S3 y luego se combinan todos los valores de S en una final S. Siendo una firma que será válida por la suma de sus llaves. Esta es la ventaja de k-of-k multisig.

$$\begin{array}{c|c} U_1 \rightarrow k_1, R_1 & U_1 \rightarrow (R, s_1) \\ U_2 \rightarrow k_2, R_2 & U_2 \rightarrow (R, s_2) \\ U_3 \rightarrow k_3, R_3 & U_3 \rightarrow (R, s_3) \end{array} \longrightarrow R \longrightarrow \begin{array}{c} (R, s) \end{array} \quad (1)$$

Incluso si no hay una situación k-of-k, cualquier otra política de qué combinación de claves se puede firmar. Todo lo que uno necesita es un árbol de merkle más la capacidad de Schnorr para sumar y construir un árbol donde cada hoja del nodo del árbol es una combinación de claves que se pueden firmar. Estos deben ser mezclados juntos y la raíz es la dirección.

OP_CHECKSIG & OP_CHECKMULTISIG se modificará para que puedan apilar pubkeys, delinear y asociar entradas validadas y producir una firma combinada para la transacción resultante consiguiendo una reducción del 20% en el tamaño del bloque.

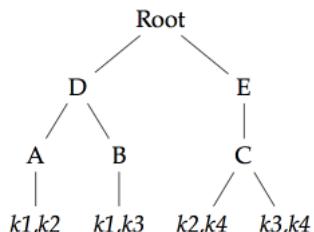
2 de 4 {k1...k4}

O(1) tiempo de verificación

O(log n) tamaño de firma

O(n) tiempo de firmado

Es posible hacer agregación sobre todas las firmas en una sola transacción. La idea detrás de esto es habilitar validadores de sistema como los nodos de Viacoin para calcular una sola clave para cada entrada con todas las transacciones.





Viacoin Whitepaper

7. Non-atomic flushing (Vaciados de memoria no atómicos)

Para que el sistema sea robusto, el estado en el disco debe ser persistente con un bloque. Ante un cierre inesperado de la billetera, el sistema debe poder iniciar y retroceder o avanzar dentro de ella y ser capaces de obtener un punto consistente en el disco. Normalmente cada vez que la caché se llena, se realizaría una limpieza. Si está presente al inicio significa que nos estrellamos durante el proceso de vaciado, y retrocedimos / avanzamos bloques dentro de él para obtener un punto consistente sobre disco antes de proceder.

8. Colored coins (monedas coloreadas)

El lenguaje de scripts de Viacoin permite almacenar pequeñas cantidades de metadatos en la cadena de bloques que pueden representar instrucciones de manipulación de activos. Una transacción de Viacoin puede codificarse de modo que x unidades de un nuevo activo fueron creados y se acreditan a una dirección de Viacoin. El término se deriva de la idea de "colorear" una cantidad nominal de monedas. Al colorear un Viacoin, se convierte en una ficha que puede representar cualquier cosa que un usuario desee comercializar como acciones de una empresa o bienes físicos. Esto parece muy similar a 'Counterparty', pero hay algunas diferencias clave. Utiliza la cadena de bloques de Viacoin (por ejemplo, NXT).

No emite una moneda auxiliar (por ejemplo, Counterparty y Mastercoin). Los metadatos le dan sentido a un [9] transacción de moneda de color que generalmente se almacena en uno de los códigos de operación OP_RETURN. El resultado contiene El OP_RETURN se llama salida de marcador. Este marcador puede tener un valor de cero o distinto de cero. Las salidas de marcadores comienzan con el código de operación OP_RETURN y pueden ser seguidas por cualquier secuencia de códigos de operación que debe contener un código de operación PUSHDATA que contenga una carga útil de activos de mercado abiertos analizables. El campo lista de cantidad de activos se usa para determinar la cantidad de cada salida del activo y cada entero usa codificación LEB128. Si esto excede los 9 bytes, la salida del mercado se considera inválida.



Viacoin Whitepaper

La cantidad máxima de activos para una salida es 263-1 unidades.

El protocolo de activos abiertos de monedas de coloreadas [4] se encuentra sobre el protocolo de Viacoin. No requiere de ningún cambio en el protocolo de Viacoin en sí.

9. MAST (Árboles sintácticos abstractos merkleizados)

[10] Mast permite que los scripts de validación de transacción de Viacoin se almacenen en forma parcialmente troceada y permite a los nodos interactuar con los árboles de Merkle . "Cuando se gasta, los usuarios pueden proporcionar solo las ramas que están ejecutando, y los trozos (hashes) que conectan las ramas a la raíz de tamaño fijo del árbol de Merkle. Esto reduce el tamaño del cumplimiento de apilado desde $O(n)$ hasta $O(\log n)$ (con n como el número de ramas). Esto permite complicadas condiciones de canje que actualmente no es posible debido al tamaño del script y al límite de código de operación, mejora la privacidad al ocultar ramas no ejecutadas, y permite la inclusión de datos forzados no consensuados con muy bajo costo o sin costo adicional ".

Es importante porque MAST permite la creación de contratos inteligentes sin obstruir la cadena de bloques. Por lo general, todos los contratos inteligentes serían visibles en la cadena de bloques y ocuparían espacio.

Con MAST es posible revelar solo los contratos inteligentes que se han completado, ahorrando espacio, ya que los nodos solo tienen que leer el capa superior del Merkle Tree. Esto puede parecer familiar al sistema de contratos inteligentes de Ethereum, pero hay una diferencia.

Ethereum accede a una VM(máquina virtual) directamente donde VIA obtendrá acceso a una VM a través de RootStock (RSK). RSK pretende ser lo que Ethereum debería haber sido: una plataforma de contratos inteligentes descentralizada y completa de Turing.



Viacoin Whitepaper

10. Contratos inteligentes de Viacoin RSK

[5] Rootstock es una plataforma de contratos inteligentes que tiene una vinculación de dos vías. La idea es permitirle trabajar con contratos inteligentes. Rootstock ejecuta una máquina virtual de Turing completa llamada Rootstock Virtual Machine (que ¡también es compatible con la máquina virtual de Ethereum!) y permite la ejecución de contratos inteligentes compilados en el lenguaje de programación solidity. Podría funcionar mediante la fusión de minería con Viacoin, que permite que la cadena de bloques RSK tenga el mismo nivel de seguridad que Viacoin. Debe permitir aproximadamente 2000 transacciones por segundo en la cadena y 20000 transacciones por segundo fuera de la cadena.

11. Transacciones anónimas

[11] Un centro de pagos atómico anónimo desvinculado para Viacoin basado en Tumblebit.

<https://github.com/viacoin/documents/blob/master/whitepapers/styx/Viacoin-Styx-Whitepaper.pdf>