FTS Coin: Un Sistema Peer-to-Peer de Transacciones Privadas Electrónicas

Project FTS
whitepaper@ftscoin.xyz
www.ftscoin.xyz

Resumen. Si bien los sistemas electrónicos peer-to-peer de efectivo han sido una parte creciente del paradigma económico en evolución en los últimos 10 años, emergiendo a medida que adoptamos una nueva era tecnológica, todavía hay mucho margen de mejora para este nuevo software. FTS Coin espera abordar algunas de estas áreas para hacer mejoras, incluyendo, entre otras; Privacidad, centralización POW, tiempos de transacción lentos, altas tarifas de transacción, sistemas de transacción confusos y la pérdida de frases semillas. Al abordar estos temas y ofrecer soluciones a los mismos, y usar FTS Coin para ayudar a difundir la adopción masiva a través de nuestras distribuciones POB, ¡esperamos ayudar a que las criptomonedas se vuelvan de adopción masiva!

1. Introducción

Durante la última década, las criptomonedas ha cementado su lugar en la sociedad global como un medio para almacenar valor y realizar transacciones fácilmente más allá de las fronteras. Si bien Bitcoin, la criptomoneda original, preparó el camino para las variaciones de esta tecnología, tenía deficiencias que se han vuelto claras a lo largo de su década de uso en la sociedad. FTS Coin espera abordar estos problemas, mientras que aprovecha parte de un pequeño pre-minado, del suministro total de monedas de 25,000,000, para ayudar a crear incentivos para que las personas enseñen a las nuevas empresas sobre criptomonedas.

El problema más aparente que existe con Bitcoin es la privacidad; Una vez que se ha realizado una transacción con una billetera bitcoin y otras personas conocen la dirección de la billetera, pueden rastrear todos los negocios financieros de esa billetera. Si esa billetera se puede conectar a un individuo, todas las transacciones realizadas por ese individuo se convierten en información pública. Dado que las monedas de privacidad han encarado bien este problema, FTS es una bifurcación de última generación de la tecnología Cryptonote. Cryptonote utiliza una forma de pagos no vinculables para garantizar la privacidad; Puede encontrar información sobre la tecnología Cryptonote en el Libro Blanco de Cryptonote.

Otro problema que encontramos problemático acerca del Bitcoin fue la capacidad de una persona o entidad de centralizar el poder de minería POW de la moneda creando grandes granjas mineras ASIC o comprando poder de hash de un servicio de renta de hash. Una red de criptomonedas funciona mejor si la distribución está tan extendida como sea posible y una gran cantidad de personas invierten en la competencia POW de suma cero para obtener recompensas de bloque. La sobrecentralización del poder de hash POW disuade este crecimiento de red natural y beneficioso, y su capacidad de atraer nuevas personas a las criptomonedas.

El Bitcoin también está sujeto a tiempos de transacción lentos, aunque la mayor parte de la “obstrucción” en Bitcoin ocurre dentro la mempool del mismo, otro problema

es el tiempo de bloqueo en sí. Redujimos en gran medida el tiempo de bloqueo estándar a un promedio cerca de 2 minutos por bloque. Esta mayor velocidad de bloque y nuestras tarifas de transacción reducidas ayudan a que las transacciones se muevan de manera oportuna, permitiendo que el sistema se use fácilmente para intercambiar bienes.

Los sistemas de software confusos también son comunes en el mundo de las criptomonedas. Dado que la mayoría de las personas inicialmente atraídas por las criptomonedas, la moneda de Internet, son usuarios habituales de computadoras, este es el grupo al que este software se ha adaptado hasta ahora. Esto no conduce a la adopción global de las criptomonedas por parte de la gente; La adopción global de cualquier tecnología nueva se ve impulsada en parte por su facilidad de uso en comparación con otros sistemas. A medida que FTS Coin avance con el desarrollo futuro, este objetivo se mantendrá al frente y en el centro en todo momento, y abordaremos todos los esfuerzos con la esperanza de que algún día sean utilizados por todos.

Una parte de la confusión que rodea a las criptomonedas es la gestión, y muchas veces la pérdida, de la semilla de origen para los fondos de las billeteras con las que se almacenan. Aunque este problema no existiría si las personas fueran cuidadosas con sus semillas de billetera y las trataran como efectivo, creemos que hemos encontrado una solución que permitirá a las personas tener sus semillas de billetera en todo momento, sin crear un riesgo de seguridad. Al permitir a un usuario seleccionar una combinación de datos biométricos para reemplazar las palabras que representan la semilla de billetera estándar, esperamos cerrar la brecha perdida al no tener un cajero; Con fondos siempre a solo un escaneo de ser generado fuera de la cadena de bloques.

FTS Coin ofrecerá opciones tanto de POW como de POS en el futuro cercano, pero se lanzará con un POW configurado para recompensas de bloque, con un sistema adicional de ganancias POB. El sistema de ganancias POB, un diseño único vinculado a esta moneda, implica dar incentivos a las personas para ayudar a difundir la adopción masiva de las criptomonedas. Este sistema POB se administrará a través del sitio web FTSMothership.info y se pagará con una porción del pre-minado de FTS Coin.

Por el bien del crecimiento y desarrollo, durante el lanzamiento de la moneda se realizó un pequeño pre-minado del FTS Coin. FTS Coin tiene un suministro total de 25,000,000 monedas, que se distribuirá lentamente durante un siglo, 2,000,000 de las cuales fueron pre-minadas. Eso significa que el 8% del suministro de FTS Coin fue pre-minado, quedando el 92%, o 23,000,000, disponibles para los próximos 100 años. El uso de este pre-minado se describirá para la transparencia más adelante en este libro blanco.

2. Privacidad de Transacción**

****¡La sección 2 ha sido tomada palabra por palabra del libro blanco de Cryptonote!**

Proponemos una solución (de privacidad) que permite al usuario publicar una única dirección y recibir pagos incondicionales no vinculables. El destino de cada salida de CryptoNote (por defecto) es una clave pública, derivada de la dirección del destinatario y de los datos aleatorios del remitente. La principal ventaja frente a Bitcoin es que cada clave de destino es única por defecto (a menos que el remitente use los mismos datos para cada una de sus transacciones con el mismo destinatario). Por lo tanto, no existe el problema de “reutilización de dirección” por diseño y ningún observador puede determinar si alguna transacción se envió a una dirección específica o vincular dos direcciones.

Primero, el remitente realiza un intercambio Diffie-Hellman para obtener un secreto compartido de sus datos y la mitad de la dirección del destinatario. Luego calcula una clave de destino única, utilizando el secreto compartido y la segunda mitad

de la dirección. Se requieren dos ec-keys diferentes del destinatario para estos dos pasos, por lo que una dirección CryptoNote estándar es casi el doble de grande que una dirección de billetera de Bitcoin. El receptor también realiza un intercambio Diffie-Hellman para recuperar la clave secreta correspondiente.
Una secuencia de transacción estándar se realiza así:
1. Alice quiere enviar un pago a Bob, quien ha publicado su dirección estándar. Ella desempaqueta la dirección y obtiene la clave pública de Bob (A, B).

2. Alice genera un $r \in [1, l-1]$ aleatorio y calcula una clave pública única $P = H_s$

(rA)G+B.
3. Alice usa P como una clave de destino para la salida y también incluye el valor R=rG (como parte del intercambio Diffie-Hellman) en algún lugar de la transacción. Tenga en cuenta que ella puede crear otras salidas con claves públicas únicas: las claves de diferentes destinatarios (A_i, B_i) implican un P_i diferente incluso con la misma r.
4. Alice envía la transacción.
5. Bob verifica cada transacción que pasa con su clave privada (a, b) y calcula $P=H_s(aR)G+B$. Si la transacción de Alice con Bob como destinatario fue entre ellos, entonces aR=arG=rA y $P'=P$.
6. Bob puede recuperar la clave única privada correspondiente: $x=H_s(aR) + b$, así como P=xG. Él puede usar esta salida en cualquier momento firmando una transacción con x.

Como resultado, Bob recibe pagos entrantes, asociados con claves públicas únicas que no son vinculables para un espectador. Algunas notas adicionales:
• Cuando Bob "reconoce" sus transacciones (ver el paso 5), prácticamente usa solo la mitad de su información privada: (a, B). Este par, también conocido como la clave de seguimiento, se puede pasar a un tercero (Carol). Bob puede delegarle el procesamiento de nuevas transacciones. Bob no necesita confiar explícitamente en Carol, porque ella no puede recuperar la clave secreta única p sin la clave privada completa de Bob (a, b). Este enfoque es útil cuando a Bob le falta ancho de banda o potencia de cálculo (teléfonos inteligentes, billeteras de hardware, etc.).
• En caso de que Alice quiera demostrar que envió una transacción a la dirección de Bob, puede revelar r o usar cualquier tipo de protocolo de conocimiento cero para demostrar que conoce r (por ejemplo, firmando la transacción con r).
• Si Bob desea tener una dirección compatible con auditoría donde todas las transacciones entrantes sean vinculables, puede publicar su clave de seguimiento o usar una dirección truncada. Esa dirección representa solo una ec-key pública B, y la parte restante requerida por el protocolo se deriva de ella de la siguiente manera: $a=H_s(B)$ y $A=H_s(B)G$. En ambos casos, cada persona puede "reconocer" todas las transacciones entrantes de Bob, pero, por supuesto, ninguna puede gastar los fondos contenidos dentro de ellas sin la clave secreta b.

3. El Pre-minado

FTS tuvo un pre-minado del 8% que se lanzó desde el bloque cero, esta pre-minado de 2,000,000 de monedas se está utilizando para promover la moneda y respaldar el sistema POB. La distribución de estas 2.000.000 de monedas se presentará

en esta sección con el mayor detalle posible.

500,000 de este pre-minado se utilizarán para recompensas tecnológicas para un mayor desarrollo. A medida que la moneda se desarrolle, y la comunidad que la usa crezca, será un lugar común para que el equipo de FTS Coin libere las recompensas disponibles para los codificadores y desarrolladores que pueden realizar ciertas tareas. Estas recompensas se basarán en la necesidad y la dificultad del trabajo que se busca.

500,000 de este pre-minado se utilizarán para marketing y promoción. Esto incluirá una combinación de air drops promocionales, recompensas de actividades promocionales IRL, recompensas por promoción en redes sociales, así como cualquier otra publicidad o promoción que el equipo de FTS considere que ayudará a la moneda a avanzar.

500,000 de este pre-minado se utilizarán para el sistema POB. El sistema POB ofrecerá a los individuos FTS Coins por enseñar a los negocios sobre las criptomonedas y hacer que comiencen a aceptar cualquier criptomoneda actualmente en el mercado. Más adelante en este libro blanco estarán disponibles más detalles sobre el sistema POB.

50,000 de este pre-minado se utilizarán para el desarrollo del ecosistema, en cualquier forma que pueda tomar; Incluyendo criptotiendas de solo FTS, servicios financiados por FTS Coin o cualquier otra actividad que ayude a respaldar el valor de FTS Coin.

Los 450,000 FTS Coins restantes se están utilizando para las tarifas iniciales de desarrollo.

4. La Hoja de Ruta

FTS Coin se lanzará en sus formas iniciales como una moneda de privacidad bifurcada Cryptonote, con un suministro total de 25,000,000 monedas. Esta distribución de 25,000,000 de monedas debería completarse después de 100 años con la recompensa por cada bloque disminuyendo constantemente con el tiempo. Esta es la hoja de ruta para nuestros planes actuales con la tecnología; Aunque es probable que agreguemos elementos a esta agenda, es muy poco probable que eliminemos cualquiera de estos elementos de nuestros planes futuros.

4.1 Fase 1-Génesis

Los bloques tienen un promedio de menos de 2 minutos cada uno con transacciones manejadas de forma privada como se detalla anteriormente, y los bloques son minaos con un algoritmo POW resistente a ASIC. La moneda se lanzará con opciones de minería con CPU y billeteras de terminal, así como con billeteras GUI fáciles de usar para Windows, Linux y Mac.

4.2 Fase 2-Pool de Minería y billeteras telefónicas

En esta etapa, FTS Coin agregará Pools de Minería y billeteras Android y/o IOS para la moneda. Estas opciones adicionales ayudarán a expandir tanto la base del minero como la del usuario para la moneda. Agregar billeteras telefónicas se convertirá en una parte crucial de la etapa 4.5

4.3 Fase 3: Minería Fácil , Mensajes y Exchange

La Fase 3 de FTS Coin implicará agregar un botón fácil de “minar ahora” a las billeteras GUI, así como también agregar la capacidad de enviar mensajes privados desde la billetera.

Esperamos implementar el botón fácil “minar ahora” como parte de nuestro esfuerzo para difundir la adopción masiva de criptomonedas. Creemos que un sistema resistente a ASIC proporciona fácilmente a las personas la capacidad para participar en

la red y ayudar a contribuir a su seguridad, no solo proporciona una red más descentralizada y sólida, sino que también proporciona una plataforma para que nuevas personas inviertan en el sistema de las criptomonedas en sí participando en la competencia por las recompensas de bloque.

Al proporcionar un medio para que las personas envíen mensajes cifrados, con un mecanismo de autodestrucción temporizado, a través de una red segura que también permite transacciones privadas, esperamos proporcionar un medio para interacciones comerciales privadas completas en el campo de las consultas legales y médicas. Esto será extremadamente útil para las personas que deseen interactuar con abogados o profesionales médicos de manera remota y privada, al simplificar tanto el pago como las consultas al pagar bajo un mecanismo de software.

En este punto, también estaremos comprando nuestro camino a un exchange si no hay uno disponible para la moneda, de forma gratuita, desde la comunidad cripto.

4.4 Fase 4-Híbrido POS/POW

Prueba de anticipación vendrá en esta etapa. Para ayudar a crear un incentivo para que las personas contengan sus FTS Coin, realizaremos una fuerte bifurcación del sistema para agregar opciones de POS, permitiendo así que las personas obtengan FTS Coin conteniéndolo, proporcionando POW para ayudar a la seguridad de la red o introduciendo nuevos negocios a FTS Coin con nuestro sistema POB en www.ftsmothership.info

4.5 Fase 5- Integración de Semilla Biométrica

La quinta y última etapa de la hoja de ruta planificada para el software de FTS Coin implica agregar un medio secundario para la generación de billeteras. En este punto, las personas podrán generar una dirección heredada estándar con una palabra semilla, como es común actualmente en las criptomonedas. De manera alternativa, podrán comenzar a usar la cámara y el escáner de huellas digitales de su teléfono para elegir una combinación de datos biométricos que se utilizarán en conexión con un algoritmo que traduzca esta información en la semilla para su algoritmo SHA 256. A través de este método, las personas se asegurarán de que, mientras tengan partes del cuerpo claves, tendrán la semilla misma para su billetera y serán capaces de usar cualquier teléfono para descargar el software de la billetera y recuperar sus fondos.

5. Prueba de Negocio

500,000 FTS del pre-minado se destinarán al mecanismo de Prueba de Negocio, o POB. Las personas podrán entregar un video de más de 10 segundos del dueño de un negocio diciendo que ahora acepta criptomonedas gracias al que grabó el video, y la persona que envía el video recibirá FTS Coin en compensación.

Las primeras 2,000 entregas recibirán 50 FTS Coins cada una por enviar estos videos a www.ftsmothership.info después de que se haya verificado la información. Las siguientes 4,000 entregas recibirán 25 FTS Coins por su envío. La cantidad de FTS Coins recibida por envío seguirá a la mitad de esta manera cada 100,000 FTS Coins hasta que queden 50,000 FTS Coins en el fondo POB. En el momento en que la billetera de fondos de FTS POB tenga solo 50,000 FTS Coins, las personas recibirán 1 FTS por cada negocio que presenten.

Para los envíos de FTS POB; No es necesario que el negocio haya comenzado a aceptar FTS Coin. Lo único que importa es que hayan comenzado a aceptar cualquier tipo de criptomoneda y estén dispuestos a grabar un video agradeciéndote por enseñarles del tema. ¡El objetivo de esto es apoyar la adopción masiva de criptomonedas, no solo la adopción de FTS!

6. Conclusión

Hemos propuesto una serie de mejoras a los sistemas actuales de criptomonedas que mejorarán el ecosistema de criptomonedas en su conjunto y proporcionarán una criptomoneda diseñada para ser fácilmente adoptada y utilizada por el público en general. Los sistemas actuales de criptomonedas, incluido Bitcoin, pavimentaron el camino para todos los sistemas modernos de efectivo peer-to-peer sin fronteras, pero esta década de pruebas beta ha dejado muy claras las fallas en los sistemas actuales. Esperamos solucionar estos problemas proporcionando una combinación de cambios técnicos e ideológicos que ayuden a la adopción continua de esta increíble tecnología.