¡DI HOLA!

Crysium

El futuro de DeFi en Binance Smart Chain

WHITEPAPER / LIBRO BLANCO

Resumen

El procesamiento de pagos digitales es una función vital en la sociedad moderna, ya que permite transferencias rápidas de valor entre los participantes de las transacciones. Sin embargo, las implementaciones actuales son extremadamente complejas e implican múltiples capas de mediación, todas las cuales requieren una tarifa por sus servicios. Si bien los pagos digitales suelen dar la impresión de completarse en segundos, el dinero suele moverse solo una vez al día en un proceso de liquidación multicapa.

Las soluciones de pago blockchain eliminan la intermediación de la sobrecargada infraestructura global de pagos al permitir la liquidación directa entre los participantes. Desafortunadamente, esto suele tener un costo. Los usuarios deben lidiar con tiempos de transacción lentos, impacto ambiental negativo, requisitos computacionales exorbitantes y altas tarifas, para finalmente experimentar una fricción extrema en el punto de conversión a moneda fiduciaria o criptomonedas. Para mitigar estos inconvenientes, los usuarios suelen recurrir a custodios externos, cediendo el control de sus fondos. Además, todas las soluciones de pago digitales exponen los datos de los usuarios. Desde tarjetas de crédito hasta blockchain, los datos de las transacciones pueden utilizarse para monitorizar la ubicación en tiempo real, venderse para generar oportunidades publicitarias y, en algunos lugares del mundo, conducir a la censura de las libertades individuales.

Este documento presenta el esquema técnico de un verdadero dinero digital: Cryzium. Un protocolo de transacciones basado en un libro mayor proporciona pagos cifrados de extremo a extremo para que los usuarios tengan el control de los datos. El mecanismo de consenso impulsa transacciones globales rápidas y de bajo consumo. CryziumFog es una solución de escalabilidad que proporciona acceso oculto a las transacciones en entornos con recursos limitados, como en un dispositivo móvil. Con las garantías de confidencialidad e integridad de Cryzium, ni siquiera los operadores de los servicios pueden discernir el contenido de la transacción.

1 introducción y antecedentes de diversas soluciones

La infraestructura de pagos tradicional es compleja. Un pago con tarjeta se realiza en dos pasos distintos: una "autorización" de pago reserva el dinero en tiempo real, como en un depósito en garantía; luego, la "liquidación" confirma la transacción y transfiere el dinero a través de múltiples bancos, un proceso que puede tardar días en completarse.

Desde la tarjeta hasta el dispositivo de punto de venta alojado por el comerciante, pasando por el adquirente, el proveedor de servicios de token y el emisor, todas las transacciones a través de la red de pagos, la arquitectura y la cantidad de puntos de contacto en el proceso de un pago son abrumadoras. El costo real de una transacción no siempre es evidente para el cliente, cuyas comisiones son subsidiadas por la industria crediticia masiva que suscribe el crédito o cubiertas directamente por el comerciante. Por esta razón, muchos comerciantes solo pueden permitirse aceptar efectivo.

La infraestructura de pagos blockchain simplifica la arquitectura de un pago al permitir que usuarios, clientes y comerciantes realicen transacciones directamente en una red sin intermediarios. El libro mayor, el mecanismo de consenso y la custodia de la billetera son tres componentes clave de la arquitectura blockchain, necesarios para comprender la evolución de las soluciones de pago que conducen a Cryzium.

1.1 El Libro Mayor

El primer libro mayor de blockchain con un uso significativo fue Bitcoin, que implementa un libro mayor distribuido utilizando el modelo de Salida de Transacción No Gastada (UTXO). En este esquema, una transacción consta de múltiples entradas que se destruyen (marcadas como gastadas), mientras se crean (acuñan) una o más salidas. Estas salidas se gastan como entradas en una transacción posterior. Un objetivo principal del libro mayor es ser descentralizado y distribuido, para ser resiliente y tolerante a fallos. El contenido del libro mayor debe ser público, recuperable y verificable. Para lograrlo, las transacciones se agrupan en "bloques" que, una vez confirmados, se replican en todos los nodos de la red. Cada bloque contiene un hash, o Una huella digital de longitud fija de su bloque principal proporciona una cadena verificable que puede recuperarse y validarse de forma independiente.

Las primeras implementaciones de blockchain no utilizaban funciones de preservación de la privacidad en las transacciones, exponiendo así a los usuarios a fugas de datos, monitoreo de ubicación y vigilancia. Las iteraciones del protocolo de transacciones, en particular Ring Confidential Transactions (RingCT) y ZCash, han proporcionado conjuntos de funciones mejoradas para los usuarios con las protecciones esenciales necesarias en una red global de pagos.

El libro mayor de Cryzium sigue el modelo UTXO, y el protocolo de transacciones proporciona pagos cifrados de extremo a extremo, donde el remitente, el receptor y el importe solo son conocidos por los participantes de la transacción. Los usuarios mantienen el control sobre sus datos, con funciones para proporcionarlos según sea necesario, como los recibos del remitente.

1.2 El Mecanismo de Consenso

Un problema de computación distribuida con una larga historia, el consenso es el proceso mediante el cual múltiples nodos de una red se comprometen a tomar una decisión. Varios esquemas centralizados, originalmente diseñados para plataformas de supercomputación, allanaron el camino para la revolución descentralizada en la computación distribuida. Un aspecto importante del consenso es que debe ser resiliente a participantes falibles; debe ser tolerante a fallos. Un método de consenso probado es la replicación de máquinas de estados.

Varios mecanismos de consenso que utilizan el enfoque de máquinas de estados han demostrado ser viables en el ámbito global de pagos descentralizados, como la Prueba de Trabajo, la Prueba de Participación y el Acuerdo Bizantino Federado, con diversas desventajas. Por ejemplo, la Prueba de Trabajo incentiva la descentralización al recompensar aleatoriamente a los mineros por contribuir a la confirmación de bloques, pero esta incentivación puede manipularse fácilmente.

Esto resulta en una competencia por superar en CPU a los mineros de la misma categoría, con un impacto ambiental innecesariamente negativo. Además, en redes sin cifrado, los remitentes están sujetos a una práctica de explotación conocida como "Valor Extraído por el Minero", donde los mineros se adelantan a la transacción para obtener un precio más bajo y vender inmediatamente a un precio más alto al transaccionista. La Prueba de Participación, si bien es más respetuosa con el medio ambiente, incentiva la concentración de la riqueza al proporcionar un mayor retorno de la inversión para grandes participaciones. Además, los sistemas de Prueba de Trabajo son vulnerables a cortes descalibrados. Si bien el corte tiene como objetivo penalizar el mal comportamiento del validador, un comportamiento bizantino no malicioso, como un rendimiento defectuoso, puede provocar el corte de un nodo y desincentivar la participación.

El Acuerdo Bizantino Federado (FBA), utilizado en Cryzium, fue pionero en el Protocolo de Consenso Stellar [Maz] y utiliza la votación federada para llegar rápidamente a un consenso sobre la validez de una transacción, sin recursos computacionales innecesarios ni daños ambientales. Dado que los incentivos no están desalineados, los operadores de nodos no manipulan el sistema para extraer valor, por lo que la comisión puede mantenerse baja, externalizando únicamente el coste de las operaciones de la red y previniendo comportamientos indebidos como los ataques de denegación de servicio (DoS), donde los usuarios legítimos no pueden acceder a recursos o servicios.

1.3 Custodia de la billetera

Uno de los retos más difíciles que enfrentan todas las soluciones de efectivo digital es la custodia de los fondos. La razón de la compleja infraestructura que subyace a los pagos tradicionales con tarjeta y digitales actuales es brindar la experiencia de custodiar el efectivo en la billetera, sin tener que gestionar dólares y centavos físicos.

Todo el sistema bancario se construyó hace un milenio bajo la premisa de que los viajeros custodiaban sus fondos en puntos de referencia para evitar llevar grandes sumas y ser víctimas de delincuentes.

Sin embargo, la custodia por parte de terceros tiene un coste. En primer lugar, el control final de los fondos se cede a un gran sistema con un alto nivel de apalancamiento. Si un sistema mal gestionado falla, pueden producirse pánicos bancarios, como los que se vieron en la década de 1930 en Estados Unidos. En segundo lugar, la custodia es costosa. Sin embargo, guardar el efectivo bajo llave no es una solución real para la mayoría de los usuarios actuales, quienes aprecian la comodidad de los pagos con tarjetas y aplicaciones de pago en dispositivos móviles.

Blockchain mejora la custodia de fondos al permitir a los usuarios la autocustodia mediante implementaciones de billeteras que protegen sus claves privadas. Sin embargo, la mayoría de las soluciones de billetera son difíciles de usar, exponen al usuario a conceptos desconocidos como "entropía" (una semilla aleatoria de la que se derivan las claves privadas), "base58" (una codificación transcribible que se usa frecuentemente para direcciones públicas) y "mnemónicos" (un conjunto de palabras que codifican secretos, como la entropía), y carecen de características como la recuperabilidad, lo que conlleva el riesgo de fallos catastróficos. Además, la mayoría de las cadenas de bloques, especialmente las cifradas, requieren la sincronización local de todo el libro contable para construir una transacción válida. Este requisito computacional es prohibitivo e inviable en entornos informáticos restringidos, como los dispositivos móviles.

2

Ante la disyuntiva entre la comodidad y la seguridad de sus fondos, la mayoría de los usuarios optan por confiar la custodia de sus fondos a un tercero. Por lo tanto, ceden toda la descentralización, seguridad y liquidación directa que ofrece la cadena de bloques a un servicio centralizado, que cobra una tarifa adicional y tiene acceso total a los datos del usuario.

Cryzium no compromete la custodia, ofreciendo una solución de escalabilidad, Cryzium Fog, que permite a los usuarios mantener la custodia de sus fondos mientras disfrutan de la comodidad, la velocidad y el cifrado de datos que requiere el dinero digital.

2. Libro Mayor y Protocolo de Transacciones de Cryzium

Para que cualquier red de pagos funcione, debe mantener un historial de transacciones.

El Libro Mayor de Cryzium almacena registros de pago cifrados y se implementa como una cadena de bloques. Cada bloque contiene salidas de transacción (TXO) que sus propietarios podrían gastar en el futuro. Cada transacción también incluye una prueba de que todo el valor gastado en ella nunca se ha gastado antes. El diseño subyacente se basa en el protocolo de libro mayor Ring Confidencial Transactions (RingCT), que preserva la privacidad y oculta la identidad de todos los propietarios de TXO mediante direcciones de destinatario únicas. El vínculo entre el remitente y el destinatario está protegido mediante anillos de entrada que custodian las TXO realmente gastadas en un amplio conjunto de TXO posiblemente gastados.

El valor monetario de cada TXO se cifra mediante RingCT, implementado con tecnología a prueba de balas para un mejor rendimiento. Solo el receptor de la transacción puede revelar el valor monetario cifrado y gastar las nuevas TXO que se escriben en el libro mayor. El control criptográfico del receptor sobre los gastos garantiza que todas las transacciones en Cryzium sean irreversibles, similar a las transacciones en efectivo en el mundo real.

Cada TXO en el anillo de entrada de una transacción se anota con una prueba de inclusión de Merkle en la blockchain de MobileCoin Ledger. Esto permite validar nuevas transacciones con menos operaciones de lectura de la blockchain, lo que mejora la eficiencia y reduce la filtración de información a los canales de acceso a datos.

Además, Cryzium Ledger mejora drásticamente la privacidad básica ofrecida por RingCT al requerir que los anillos de entrada de cada transacción se eliminen antes de que el nuevo pago se agregue al libro mayor público. Se agregan firmas digitales al libro mayor en lugar de los registros completos de las transacciones para proporcionar una base para la auditoría.

Observación 1: En este documento técnico, los conceptos se presentan de forma sucinta para proporcionar orientación técnica, pero no una especificación completa. Para una revisión detallada de la construcción de Cryzium, consulte la sección "Mecánica de Cryzium" [koe21]. 2.1 Construcción de Transacciones

2.1.1 Protección de Datos del Remitente: Firmas de Anillo

Una transacción consta de entradas y salidas. Las entradas de una transacción de MobileCoin utilizan una construcción de Firma de Anillo para demostrar que la entrada real del pago está en el conjunto, sin revelar exactamente qué entrada se gastó. Una Firma de Anillo es una prueba de uno entre muchos, que comienza con la clave pública A, para la cual el probador conoce la clave privada a, con un valor aleatorio $v \in Zp$. Sea g un generador en el grupo G, y el probador establece c como:

$$c = H(g\,v\,,\, gr1A\,c1\,) - c1$$

Donde r1 y c1 son valores aleatorios.

El demostrador tiene c, r, como

$$r = v - ca$$

De la construcción Shnorr para demostrar la propiedad a un observador con la clave pública.

El conjunto (A, r, c, B, r1, c1) se envía al verificador, donde B es una clave pública adicional sobre la cual el verificador no retiene la propiedad, construyendo así el anillo de posibles claves públicas que se utilizan en la transacción.

El verificador calcula el hash.

$$H(g\ rA\ c\ ,\ gr\ 1B\ c\ 1\ )$$

que es idéntico a c + c1 = H(gvc + c1 = H(g v , gr1Ac1), lo que demuestra que el demostrador conocía a para A o b para B, sin que el verificador sepa si el demostrador conocía a o b.

Esta construcción se puede generalizar a cualquier número de claves públicas adicionales.

2.1.2 Prevención de doble gasto: Imágenes de clave

Una imagen de clave es un compromiso único con la clave pública de una entrada, sin revelar las claves pública o privada:

$$I = H(y)\ x$$

La imagen de la clave debe estar vinculada a la Firma de Anillo y, por lo tanto, se incluye en el hash de cada clave pública de la Firma de Anillo y en el conjunto de términos proporcionados al verificador: (I, A, r, c, B, r1, c1), quien comprueba que el hash sea equivalente a c + c1. Esto evita el doble gasto al vincular la imagen de la clave I con la firma, rastreando qué I se ha utilizado y rechazando nuevas firmas con una I previamente utilizada.

Para optimizar el uso del espacio, las Firmas de Grupos Anónimos Espontáneos Vinculables (LSAG) utilizan un proceso iterativo para construir c términos, lo que resulta en el envío de una sola c. Con las Firmas LSAG Multicapa (MLSAG), la clave real se puede asociar con datos intercalados mediante vectores de clave en lugar de claves individuales.

2.1.3 Prohibición de la acuñación no autorizada: RingCT y Bulletproofs

Para validar que la suma de las entradas de una transacción sea igual a la suma de las salidas sin revelar el importe, lo cual podría exponer innecesariamente los datos del usuario, utilizamos un compromiso de Pedersen [Ped92] para el importe, que consiste en el generador de grupo h = H(g) elevado al valor v del importe de TXO, con un factor de cegamiento s, para evitar la fuerza bruta en todo el rango de valores (264). Por lo tanto, el compromiso es:

$$C = g\ sh\ v$$

y se firma a cero para que el verificador pueda validar que la transacción esté equilibrada.

También incluimos una prueba de rango para evitar compromisos con valores negativos (acuñación de monedas) que, de otro modo, parecerían válidos siempre que sumaran cero con las TXO de entrada. Una prueba de rango consiste en una expansión binaria con un compromiso, firmada en una firma de anillo no enlazable de tamaño 2 para cada bit.

Las pruebas de rango nos permiten consolidar las pruebas de rango que consumen mucho espacio y son una primitiva potente que puede representar circuitos aritméticos arbitrarios, similares a zkSNARKs, sin una configuración de confianza.

Tenga en cuenta que, dado que tenemos un anillo de entradas, del cual solo conocemos la cantidad real de la que poseemos, necesitamos poder demostrar que las cantidades de entrada y salida equilibran sin comprometer cuál es la entrada real. Por esta razón, la firma de la transacción contiene un pseudocompromiso de salida para cada entrada. 2.1.4 Protección de datos del destinatario: Direcciones de un solo uso

Para proteger los datos del destinatario, cada destino de salida se construye como una dirección de un solo uso. Partiendo de un par de claves R = gr

para la TXO y una clave pública de destino (A, B), la dirección de un solo uso, y, es:

$$y = g\,H(A\,r\,)B = g\,x$$

Para recuperar la transacción, el destinatario debe escanear la dirección única de cada TXO y aplicar su clave privada (a, b) para recuperar la clave privada única x:

$$x = H(R\,a\,) + b$$

Luego, levante g para reconstruir la clave pública y

$$g\,x = g\,H(R\,a\,)\,g\,b = y$$

Si g x = y, la clave de destino es igual a la clave utilizada para construir la dirección de un solo uso y, por lo tanto, es un secreto compartido. El propietario conoce la clave privada x y puede firmar la clave y en una firma circular, marcando la TXO como gastada.

Tenga en cuenta que solo se requieren (a, B) para determinar si una salida pertenece a esa cuenta de destino. Esto se denomina "Clave de Vista", ya que puede compartirse para revelar las transacciones entrantes sin otorgar autoridad de gasto sobre los fondos.

2.1.5 Defensa contra el Análisis de Gráficos de Transacciones: Enclaves Seguros

Las transacciones de Cryzium son validadas por Nodos Validadores de Consenso para producir cada bloque siguiente en el libro mayor. Al utilizar la tecnología de enclaves seguros, específicamente las Extensiones de Protección de Software (SGX) de Intel, la cadena de bloques de Cryzium logra una confidencialidad e integridad superiores.

Los enclaves seguros son una región de memoria que permite la ejecución de código cifrado. Existen muchas implementaciones diferentes de enclaves seguros, con diferentes ventajas y desventajas. En el contexto de la infraestructura en la nube, los enclaves seguros transforman el paradigma de la

computación remota al ampliar la base de computación confiable de los usuarios para incluir la máquina remota. Al iniciarse cada nodo validador de consenso, establece una conexión certificada con sus pares. Si no ejecutan exactamente el mismo código de enclave, las mediciones del enclave no coincidirán y la conexión será rechazada. De igual forma, cuando los clientes envían una transacción a la red, solicitan la evidencia de certificación a los validadores de consenso y solo proceden con una conexión certificada si las mediciones son las esperadas.

Los enclaves seguros garantizan que todos los nodos que participan en el consenso ejecuten exactamente el mismo código, que es de código abierto, auditado y con una compilación reproducible, de modo que cualquiera pueda verificar que el código que se ejecuta es exactamente el publicado. La validación que se realiza dentro del enclave puede, por lo tanto, descartar las entradas de las transacciones, ya que el enclave firma el bloque con una clave que genera al iniciarse y publica una firma sobre el bloque junto con la clave pública correspondiente. Esto proporciona una cadena de confianza que determina qué nodos participaron en cada bloque de consenso. El nodo observador recopila los informes de verificación de atestación (AVR), que incluyen firmas sobre las claves públicas en las firmas de bloque, lo que confirma que esos nodos ejecutaban la misma versión de enclave.

Al eliminar las entradas, la blockchain ahora es resistente a ataques de análisis estadístico que, según se ha demostrado, reducen la protección de datos en otras cadenas que siguen el modelo UTXO con firmas de anillo.

2.1.6 Impacto de la vulneración de SGX en la privacidad de las transacciones

Los enclaves seguros pueden proporcionar una mayor integridad y confidencialidad, funcionando según lo previsto. Como la mayoría de las nuevas tecnologías complejas, inevitablemente se descubrirán fallos de diseño. Se han publicado varios ataques de canal lateral contra secretos protegidos por Intel SGX, que posteriormente se han parcheado o mitigado. Cryzium está diseñado para proporcionar una defensa en profundidad en caso de un ataque basado en una vulnerabilidad de enclave seguro. Las transacciones de Cryzium utilizan la tecnología CryptoNote para garantizar que, incluso en claro, el destinatario se oculte con una dirección de un solo uso, el remitente con una firma de anillo y los importes con RingCT.

En caso de una vulnerabilidad de Intel SGX, la vista del atacante del libro mayor dentro del enclave seguiría protegida tanto por las firmas de anillo como por las direcciones de un solo uso, y los importes permanecerían ocultos con RingCT. Durante el ataque, este atacante tendría visibilidad de las entradas efímeras de una transacción y podría realizar ataques estadísticos basados en el rastreo de las entradas en las firmas de anillo para determinar relaciones probabilísticas entre transacciones. Sin embargo, este ataque solo es aplicable a las transacciones realizadas durante el tiempo en que se conoce la vulnerabilidad del enclave seguro, pero no se ha parcheado. Una vez que se descubre y soluciona la vulnerabilidad de Intel SGX, los ataques estadísticos ya no son posibles, por lo que se preserva la confidencialidad directa. 3 Consenso de Cryzium

Los nodos de Cryzium llegan a un consenso sobre la validez de una transacción mediante FBA. Mediante una serie de rondas de votación, las papeletas se nominan, preparan, comprometen y externalizan progresivamente al libro mayor.

Una vez que cada nodo valida la transacción, el consenso se basa en los hashes de la transacción, ya que no se requiere el contenido completo para lograrlo.

3 Consenso de Cryzium

Los nodos de Cryzium llegan a un consenso sobre la validez de una transacción mediante FBA. Mediante una serie de rondas de votación, las papeletas se nominan, preparan, comprometen y externalizan progresivamente al libro mayor.

Una vez que cada nodo valida la transacción, el consenso se basa en los hashes de la transacción, ya que no se requiere el contenido completo para lograrlo.

La implementación de FBA utilizada en Cryzium se inspira en el Protocolo de Consenso Stellar [Maz] y logra un consenso rápido y de bajo consumo, con control descentralizado. Permite una confianza flexible al requerir que los participantes especifiquen su conjunto de pares de confianza. El cierre transitivo de todos los conjuntos de confianza (Conjuntos de Cuórum) define el Umbral de Bloqueo y el Umbral de Cuórum, tras los cuales la votación puede pasar a la siguiente ronda. El conjunto de confianza se puede modificar en cualquier momento, lo que permite a la red responder dinámicamente a actores maliciosos o falibles. La Fundación Cryzium mantiene una lista de nodos de confianza. Esta lista no representa la totalidad de los nodos que operan en la red Cryzium, pero proporciona un conjunto para impulsar la participación de cualquier nuevo operador. La red ofrece participación abierta, ya que los nodos actualmente en funcionamiento pueden añadir nuevos nodos como pares de confianza a su conjunto de quórum, y cualquier nuevo nodo comenzará a participar inmediatamente en el consenso.

3.1 Mejoras de SGX para el consenso

Una propiedad de SGX que Cryzium Consensus utiliza es la integridad. Al proporcionar evidencia de atestación entre pares en la red, los nodos están configurados para rechazar conexiones de cualquier nodo que no coincida con la medición del enclave, junto con parámetros de inicio seleccionados, como la tarifa mínima. Esto aumenta la tolerancia a fallos de la red, ya que un agente malicioso solo puede modificar la región no confiable del software (fuera del enclave), que no participa en la validación de transacciones.

4 Escalabilidad y Autocustodia Potenciada: Cryzium Fog

Como se describe en las direcciones de un solo uso [2.1.4], el destinatario debe escanear cada TXO para verificar su propiedad.

Este requisito computacional resulta prohibitivamente costoso a medida que el libro mayor crece, especialmente en entornos con recursos limitados, como los dispositivos móviles.

Cryzium Fog es un servicio que preserva la privacidad, diseñado para soportar el uso de la Red de Pagos Cryzium en dispositivos móviles, que pueden usar Fog para consultar su saldo y enviar pagos, sin necesidad de sincronizar todo el libro mayor localmente.

4.1 Servicio de Mensajería Duradera y Sin Custodia

Fog proporciona acceso escalable a las TXO en el Libro Mayor Cryzium, sin que los clientes tengan que escanear cada TXO en su dispositivo local. Fog realiza esto sin acceder a las claves privadas de los usuarios. Esto contrasta con la mayoría de las demás soluciones de escalabilidad, que requieren que el

usuario proporcione sus claves privadas a un tercero que escanea el libro mayor en su nombre, lo cual tiene importantes implicaciones de seguridad y privacidad.

Definición 4.1 (Sin custodia): Un servicio sin custodia proporciona un servicio a la cadena de bloques sin que un tercero posea ni acceda a las claves privadas de los usuarios. A veces, estos servicios también se denominan servicios "de confianza", ya que el usuario debe confiar plenamente en el servicio para no comprometer su confidencialidad ni la integridad de sus fondos.

Fog funciona posprocesando el libro mayor de Cryzium en RAM cifrada e inadvertida, etiquetando los TXO con números aleatorios de trinquete que el cliente puede generar de forma única para recuperar los TXO y sirviendo dichos TXO desde la RAM inadvertida (ORAM).

Las propiedades de confidencialidad de Fog preservan las mismas garantías de confidencialidad del protocolo de transacciones de Cryzium, incluso para los operadores del servicio. Es decir, el remitente, el destinatario y el importe solo son conocidos por los participantes de la transacción. Fog está diseñado para que los operadores de los servicios Cryzium y Fog no tengan información no trivial sobre su pago. Además, decimos que el servicio es ajeno, porque ni siquiera un observador atento con un exploit de canal lateral degradaría las garantías de confidencialidad.

Definición 4.2 (Ajeno) En teoría computacional, se dice que una máquina de Turing es ajena si, para dos entradas cualesquiera de la misma longitud, los movimientos de los cabezales de la cinta permanecen iguales [Obl22]. Decimos que un servicio de posprocesamiento de libro mayor es ajeno si, para cualquier salida en el libro mayor, un operador con acceso completo al servicio no puede discernir más información de la que ya era discernible del libro mayor, en particular, el remitente, el destinatario o el importe de una transacción.

4.2 Secreto Compartido de Ingesta de Fog

Utilizamos un intercambio de claves ECDH estático y efímero [Res21] para crear un secreto compartido entre el Enclave de Ingesta de Fog y Alice. Este secreto compartido es fundamental para que Alice pueda recuperar sus TXO sin que el operador de Fog observe el contenido de lo que recupera. Podemos considerar el diseño de este protocolo como un mecanismo simplificado de generador de números aleatorios (RNG) y compararlo con otros esquemas de mecanismo, como los utilizados en mensajeros cifrados [Mar16].

El proceso es el siguiente:

1. El Enclave de Ingesta de Fog recibe la clave pública estática de Alice, A, (al descifrar una pista de TXO, como se explica más adelante en 4.3). A se considera el primer mensaje en el intercambio de claves.

2. El enclave de ingesta de niebla mantiene un par de claves de salida (E, e), cuya clave pública, E, se almacena junto con el rango de bloques para el que es válida en la base de datos de recuperación externa al enclave, visible para el operador de niebla. E se considera el segundo mensaje en el intercambio de claves.

3. El enclave de ingesta de niebla calcula el secreto compartido:

$$S = eA = aE$$

y utiliza S como semilla para un generador de números aleatorios (RNG)

4. El enclave de ingesta de niebla escribe un registro en el RngStore, que se encuentra en ORAM y es privado del enclave de ingesta de niebla:

```
{
    user_public_viewkey: A,
    nonce_table: {
      egress_public_key: E,
      stored_rng: NewRng(S)
    }
}
```

4.3 Pistas cifradas: Etiquetas TXO para el destinatario

Cada TXO en el libro mayor de Cryzium tiene un campo de pista cifrada, que etiqueta la TXO para el usuario de una forma que solo Fog sabe procesar.

El enclave de ingesta de Fog mantiene un par de claves de entrada de Fog, I, i, para que los remitentes de transacciones puedan usar criptografía de clave pública para cifrar un mensaje para el enclave de ingesta de Fog, etiquetando la TXO para su procesamiento.

Cuando Bob desea enviar una transacción a Alice:

1. Bob valida completamente los materiales de Fog en la dirección pública de Alice, lo que también le proporciona la clave pública de entrada del enclave de ingesta de Fog, I, que obtiene, junto con los materiales de verificación autenticados, de un punto final público en el servicio de informes de Fog.

2. Bob cifra la clave de vista pública de Alice, A, con la clave pública de entrada del enclave de ingesta de Fog, I, y adjunta esta pista cifrada, h, a la TXO, que se escribe en el libro mayor.

$$h = \{A\}KI$$

4.4 Posprocesamiento del libro mayor

Cuando el enclave de ingesta de niebla procesa la TXO de Alice desde el libro mayor, ocurre lo siguiente:

1. El enclave de ingesta de niebla descifra la pista para revelar la clave pública de Alice, A

2. Fog Ingest Enclave retrieves the stored RNG for A, and increments the RNG once to obtain a FogSearchKey, f, unique to this transaction output, and overwrites the current state of the nonce table’s stored RNG

```
{
    user_public_viewkey: A,
    nonce_table: {
     kex_rng_once: E,
     stored_rng: Rng
    }
 }
```

3. El enclave de ingesta de niebla cifra el contenido TXO con la clave pública de vista de Alice, A,

$$t = \{T\ XO\}KA$$

e inserta lo siguiente en el almacén de transacciones

```
{
    fog_search_key: F,
    transaction_contents: t
}
```

4.5 Consulta de Saldo: Obtención de TXO

Para realizar una consulta de saldo, Alice completa el intercambio de claves y recupera y descifra estos registros:

1. Alice contacta con el Enclave de Fog View, quien devuelve todos los registros RNG que contienen las claves públicas de salida E, de la Base de Datos de Recuperación. Completa el intercambio de claves utilizando su clave privada para obtener el secreto compartido S.

$$S = aE$$

2. Alice usa el secreto compartido para generar su generador de números aleatorios (RNG). Lo hace para cada clave de salida, según el bloque de inicio asociado.

3. Alice incrementa los valores del RNG para generar FogSearchKeys, fi, y envía cada clave de búsqueda al Enclave de Vista de Fog hasta que ya no haya coincidencias para un fi dado.

4. El Enclave de Vista de Fog devuelve registros para cada fi con una coincidencia.

5. Alice descifra el contenido de la transacción t con su clave de vista privada a y realiza una coincidencia de clave de vista adicional en el propio TXO, como lo haría al escanear el libro mayor para determinar que la salida de la transacción es, de hecho, suya.

5 Resumen

Al utilizar el Protocolo de Libro Mayor y Transacción de Cryzium, el Consenso de Cryzium y CryziumCoinFog, Cryzium es ideal para casos de uso móvil, como la integración con aplicaciones de mensajería populares como WhatsApp y Signal, o en aplicaciones de billetera orientadas a dispositivos móviles. Las claves permanecen custodiadas en el dispositivo, bajo el control total del usuario. Por primera vez, los usuarios pueden experimentar la seguridad, la finalidad y la facilidad del dinero digital sin comprometer el control sobre sus propios datos.

Referencias

[koe21] koe. Mecánica de Cryzium, 2024.

[Mar16] Marlinspike, Moxie. El algoritmo de doble trinquete, 2016.

[Maz] Mazieres, Eddard. El protocolo de consenso estelar.

[Obl22] Oblivious RAM. Oblivious RAM — Wikipedia, la enciclopedia libre, 2022.

[Ped92] T.P. Pederesen. Intercambio de secretos seguro, verificable y no interactivo basado en la teoría de la información.

Feigenbaum, CRYPTO 91 (Apuntes de la Clase en Ciencias de la Computación, vol. 576): Springer, Berlín, Heidelberg, 1992.

[Res21] Rescorla, Eric. Método de acuerdo de claves Diffie-Hellman — IETF RFC 2631, 2021.