RSK: Bitcoin Merge Mining is Here to Stay

Arroyo Joaquin

Universidad Nacional de Rosario
Licenciatura en Ciencias de la Computación
Seguridad Informática

25 de febrero de 2025

Índice

Introducción

Se explica el concepto de *Merge-Mining* a través de un ejemplo concreto de funcionamiento como lo es **RSK**.

Introducción

Se explica el concepto de *Merge-Mining* a través de un ejemplo concreto de funcionamiento como lo es **RSK**.

Se dan detalles sobre el protocolo de *Merge-Mining* en **RSK**:

Introducción

Se explica el concepto de *Merge-Mining* a través de un ejemplo concreto de funcionamiento como lo es **RSK**.

Se dan detalles sobre el protocolo de *Merge-Mining* en **RSK**:

- La reutilización del esfuerzo computacional.
- El concepto de *PoW* y su validación.
- Jerarquía de *targets*.
- Seguridad de la red.

Índice

Minería en Bitcoin

La minería en Bitcoin es el proceso que permite a la red de Bitcoin mantenerse segura, dificultando ataques y además es la base del **Consenso de Nakamoto**.

Minería en Bitcoin

La minería en Bitcoin es el proceso que permite a la red de Bitcoin mantenerse segura, dificultando ataques y además es la base del **Consenso de Nakamoto**.

La red utiliza una **blockchain** donde se registran todas las transacciones.

Minería en Bitcoin

La minería en Bitcoin es el proceso que permite a la red de Bitcoin mantenerse segura, dificultando ataques y además es la base del **Consenso de Nakamoto**.

La red utiliza una **blockchain** donde se registran todas las transacciones.

"Minar" un bloque consiste en realizar cálculos para encontrar un valor (*nonce*) que genere un *hash* que cumpla con la dificultad de la red.

Minería en Bitcoin

La minería en Bitcoin es el proceso que permite a la red de Bitcoin mantenerse segura, dificultando ataques y además es la base del **Consenso de Nakamoto**.

La red utiliza una **blockchain** donde se registran todas las transacciones.

"Minar" un bloque consiste en realizar cálculos para encontrar un valor (*nonce*) que genere un *hash* que cumpla con la dificultad de la red.

Esto permite demostrar que se ha invertido esfuerzo computacional (*PoW*), permitiendo que el bloque sea añadido a la blockchain.

Índice

Merge-Mining

Merge-mining es una técnica que permite reutilizar el esfuerzo computacional empleado en una blockchain primaria para contribuir a la seguridad de una blockchain secundaria.

Merge-Mining

Merge-mining es una técnica que permite reutilizar el esfuerzo computacional empleado en una blockchain primaria para contribuir a la seguridad de una blockchain secundaria.

Este proceso permite a los mineros obtener recompensas en ambas redes al mismo tiempo.

Merge-Mining

Merge-mining es una técnica que permite reutilizar el esfuerzo computacional empleado en una blockchain primaria para contribuir a la seguridad de una blockchain secundaria.

Este proceso permite a los mineros obtener recompensas en ambas redes al mismo tiempo.

Su funcionamiento se basa en los siguientes pasos:

Merge-Mining

Merge-mining es una técnica que permite reutilizar el esfuerzo computacional empleado en una blockchain primaria para contribuir a la seguridad de una blockchain secundaria.

Este proceso permite a los mineros obtener recompensas en ambas redes al mismo tiempo.

Su funcionamiento se basa en los siguientes pasos:

- Se disponen dos blockchains: una primaria y una secundaria.
- La dificultad de la blockchain primaria suele ser **mayor** a la de la blockchain secundaria.
- Un **identificador** (*tag*) de un bloque de la blockchain secundaria se incrusta dentro de un bloque de la blockchain primaria.
- Se mina el bloque de la blockchain primaria.
- Este *tag* se utiliza para validar el bloque en la blockchain secundaria.

Merge-Mining - Seguridad

Para garantizar la seguridad en **Merge-Mining**, el *tag* debe ser **único**.

Merge-Mining - Seguridad

Para garantizar la seguridad en **Merge-Mining**, el *tag* debe ser **único**.

Si esto no se cumple, un atacante puede asociar el mismo bloque de Bitcoin con dos bloques distintos en RSK, creando un *doble gasto* en RSK.

Merge-Mining - Seguridad

Para garantizar la seguridad en **Merge-Mining**, el *tag* debe ser **único**.

Si esto no se cumple, un atacante puede asociar el mismo bloque de Bitcoin con dos bloques distintos en RSK, creando un *doble gasto* en RSK.

Lograr este ataque debería ser más costoso que simplemente minar dos bloques de Bitcoin independientes junto con sus respectivos bloques en RSK.

Merge-Mining - Seguridad

Para garantizar la seguridad en **Merge-Mining**, el *tag* debe ser **único**.

Si esto no se cumple, un atacante puede asociar el mismo bloque de Bitcoin con dos bloques distintos en RSK, creando un *doble gasto* en RSK.

Lograr este ataque debería ser más costoso que simplemente minar dos bloques de Bitcoin independientes junto con sus respectivos bloques en RSK.

De esta forma, se desincentiva su ejecución.

Índice

PoW Proxy y *SPV Proofs*

El *tag* mencionado anteriormente se obtiene a partir del *hash* del *header* del bloque de RSK.

PoW Proxy y *SPV Proofs*

El *tag* mencionado anteriormente se obtiene a partir del *hash* del *header* del bloque de RSK.

Una vez que se consigue el *PoW* del bloque de Bitcoin, solo basta con buscar el *tag* en dicho bloque.

PoW Proxy y *SPV Proofs*

El *tag* mencionado anteriormente se obtiene a partir del *hash* del *header* del bloque de RSK.

Una vez que se consigue el *PoW* del bloque de Bitcoin, solo basta con buscar el *tag* en dicho bloque.

Si se encuentra, el *PoW* de Bitcoin **demuestra** que se ha encontrado una solución válida para el bloque de RSK.

PoW Proxy y *SPV Proofs*

El *tag* mencionado anteriormente se obtiene a partir del *hash* del *header* del bloque de RSK.

Una vez que se consigue el *PoW* del bloque de Bitcoin, solo basta con buscar el *tag* en dicho bloque.

Si se encuentra, el *PoW* de Bitcoin **demuestra** que se ha encontrado una solución válida para el bloque de RSK.

La forma de conseguir el *PoW* de un bloque es la siguiente:

PoW Proxy y *SPV Proofs*

El *tag* mencionado anteriormente se obtiene a partir del *hash* del *header* del bloque de RSK.

Una vez que se consigue el *PoW* del bloque de Bitcoin, solo basta con buscar el *tag* en dicho bloque.

Si se encuentra, el *PoW* de Bitcoin **demuestra** que se ha encontrado una solución válida para el bloque de RSK.

La forma de conseguir el *PoW* de un bloque es la siguiente:

1. Cada blockchain define un valor *target*.

PoW Proxy y *SPV Proofs*

El *tag* mencionado anteriormente se obtiene a partir del *hash* del *header* del bloque de RSK.

Una vez que se consigue el *PoW* del bloque de Bitcoin, solo basta con buscar el *tag* en dicho bloque.

Si se encuentra, el *PoW* de Bitcoin **demuestra** que se ha encontrado una solución válida para el bloque de RSK.

La forma de conseguir el *PoW* de un bloque es la siguiente:

1. Cada blockchain define un valor *target*.
2. Se asigna un valor al *nonce* del bloque.

PoW Proxy y *SPV Proofs*

El *tag* mencionado anteriormente se obtiene a partir del *hash* del *header* del bloque de RSK.

Una vez que se consigue el *PoW* del bloque de Bitcoin, solo basta con buscar el *tag* en dicho bloque.

Si se encuentra, el *PoW* de Bitcoin **demuestra** que se ha encontrado una solución válida para el bloque de RSK.

La forma de conseguir el *PoW* de un bloque es la siguiente:

1. Cada blockchain define un valor *target*.
2. Se asigna un valor al *nonce* del bloque.
3. Se calcula su *hash*.

PoW Proxy y *SPV Proofs*

El *tag* mencionado anteriormente se obtiene a partir del *hash* del *header* del bloque de RSK.

Una vez que se consigue el *PoW* del bloque de Bitcoin, solo basta con buscar el *tag* en dicho bloque.

Si se encuentra, el *PoW* de Bitcoin **demuestra** que se ha encontrado una solución válida para el bloque de RSK.

La forma de conseguir el *PoW* de un bloque es la siguiente:

1. Cada blockchain define un valor *target*.
2. Se asigna un valor al *nonce* del bloque.
3. Se calcula su *hash*.
4. Si $hash < target$, entonces la solución es válida. Caso contrario, se vuelve al paso 2.

PoW Proxy y *SPV Proofs*

El *tag* mencionado anteriormente se obtiene a partir del *hash* del *header* del bloque de RSK.

Una vez que se consigue el *PoW* del bloque de Bitcoin, solo basta con buscar el *tag* en dicho bloque.

Si se encuentra, el *PoW* de Bitcoin **demuestra** que se ha encontrado una solución válida para el bloque de RSK.

La forma de conseguir el *PoW* de un bloque es la siguiente:

1. Cada blockchain define un valor *target*.
2. Se asigna un valor al *nonce* del bloque.
3. Se calcula su *hash*.
4. Si $hash < target$, entonces la solución es válida. Caso contrario, se vuelve al paso 2.

Notar que a **menor** *target*, **mayor** es la dificultad del problema.

PoW Proxy y *SPV Proofs*

Al momento de validar el *PoW* del *header* de Bitcoin, no es necesario el bloque completo para asociar su *header* con el de **RSK**.

PoW Proxy y *SPV Proofs*

Al momento de validar el *PoW* del *header* de Bitcoin, no es necesario el bloque completo para asociar su *header* con el de **RSK**.

Este proceso se realiza de la siguiente forma:

PoW Proxy y *SPV Proofs*

Al momento de validar el *PoW* del *header* de Bitcoin, no es necesario el bloque completo para asociar su *header* con el de **RSK**.

Este proceso se realiza de la siguiente forma:

- Se obtiene el *header* del bloque de Bitcoin.
- Se obtiene un *midstate* de la transacción *Coinbase*.
- Se obtiene un *fragmento* de la transacción *Coinbase*.
- Se obtiene el *camino de Merkle*.

PoW Proxy y *SPV Proofs*

Al momento de validar el *PoW* del *header* de Bitcoin, no es necesario el bloque completo para asociar su *header* con el de **RSK**.

Este proceso se realiza de la siguiente forma:

- Se obtiene el *header* del bloque de Bitcoin.
- Se obtiene un *midstate* de la transacción *Coinbase*.
- Se obtiene un *fragmento* de la transacción *Coinbase*.
- Se obtiene el *camino de Merkle*.

A partir de estos se realiza la prueba *SPV*.

PoW Proxy y *SPV Proofs*

Al momento de validar el *PoW* del *header* de Bitcoin, no es necesario el bloque completo para asociar su *header* con el de **RSK**.

Este proceso se realiza de la siguiente forma:

- Se obtiene el *header* del bloque de Bitcoin.
- Se obtiene un *midstate* de la transacción *Coinbase*.
- Se obtiene un *fragmento* de la transacción *Coinbase*.
- Se obtiene el *camino de Merkle*.

A partir de estos se realiza la prueba *SPV*.

Si se verifica que la **transacción** está incluida en el bloque de Bitcoin, la prueba se considera válida.

PoW Proxy y *SPV Proofs*

Al momento de validar el *PoW* del *header* de Bitcoin, no es necesario el bloque completo para asociar su *header* con el de **RSK**.

Este proceso se realiza de la siguiente forma:

- Se obtiene el *header* del bloque de Bitcoin.
- Se obtiene un *midstate* de la transacción *Coinbase*.
- Se obtiene un *fragmento* de la transacción *Coinbase*.
- Se obtiene el *camino de Merkle*.

A partir de estos se realiza la prueba *SPV*.

Si se verifica que la **transacción** está incluida en el bloque de Bitcoin, la prueba se considera válida.

Notar que el uso del *midstate* para comprimir la transacción es posible debido a la propiedad de **resistencia a colisiones en freestart**.

Índice

Jerarquía de *Targets*

La **dificultad** de la blockchain secundaria (**RSK**) suele ser menor que la de la blockchain primaria (**Bitcoin**), debido al diseño de *merge-mining*.

Jerarquía de *Targets*

La **dificultad** de la blockchain secundaria (**RSK**) suele ser menor que la de la blockchain primaria (**Bitcoin**), debido al diseño de *merge-mining*.

A partir de esto, se define una **jerarquía de targets** en el servidor:

Jerarquía de *Targets*

La **dificultad** de la blockchain secundaria (**RSK**) suele ser menor que la de la blockchain primaria (**Bitcoin**), debido al diseño de *merge-mining*.

A partir de esto, se define una **jerarquía de targets** en el servidor:

- T_1: *target* de Bitcoin
- T_2: *target* de RSK
- T_3: *target* específico del servidor

donde $T_1 < T_2 < T_3$

Jerarquía de *Targets*

La **dificultad** de la blockchain secundaria (**RSK**) suele ser menor que la de la blockchain primaria (**Bitcoin**), debido al diseño de *merge-mining*.

A partir de esto, se define una **jerarquía de targets** en el servidor:

- T_1: *target* de Bitcoin
- T_2: *target* de RSK
- T_3: *target* específico del servidor

donde $T_1 < T_2 < T_3$

Para generar un *share*, el *hash* debe ser, como mínimo, menor que T_3.

Jerarquía de *Targets*

La **dificultad** de la blockchain secundaria (**RSK**) suele ser menor que la de la blockchain primaria (**Bitcoin**), debido al diseño de *merge-mining*.

A partir de esto, se define una **jerarquía de targets** en el servidor:

- T_1: *target* de Bitcoin
- T_2: *target* de RSK
- T_3: *target* específico del servidor

donde $T_1 < T_2 < T_3$

Para generar un *share*, el *hash* debe ser, como mínimo, menor que T_3.

Estas *shares* permiten distribuir equitativamente las recompensas futuras.

Jerarquía de *Targets*

La **dificultad** de la blockchain secundaria (**RSK**) suele ser menor que la de la blockchain primaria (**Bitcoin**), debido al diseño de *merge-mining*.

A partir de esto, se define una **jerarquía de targets** en el servidor:

- T_1: *target* de Bitcoin
- T_2: *target* de RSK
- T_3: *target* específico del servidor

donde $T_1 < T_2 < T_3$

Para generar un *share*, el *hash* debe ser, como mínimo, menor que T_3.

Estas *shares* permiten distribuir equitativamente las recompensas futuras.

Además, incentivan la participación activa en la red, lo que contribuye a mejorar su seguridad.

Índice

Seguridad en RSK

Lo principal a garantizar en una blockchain es la **integridad**, **disponibilidad** y **autenticidad**.

Seguridad en RSK

Lo principal a garantizar en una blockchain es la **integridad**, **disponibilidad** y **autenticidad**.

La criptografía garantiza la **autenticidad** de las transacciones y la **integridad** de los bloques.

Seguridad en RSK

Lo principal a garantizar en una blockchain es la **integridad**, **disponibilidad** y **autenticidad**.

La criptografía garantiza la **autenticidad** de las transacciones y la **integridad** de los bloques.

La **disponibilidad** se asegura por la naturaleza descentralizada de la blockchain.

Seguridad en RSK

Lo principal a garantizar en una blockchain es la **integridad**, **disponibilidad** y **autenticidad**.

La criptografía garantiza la **autenticidad** de las transacciones y la **integridad** de los bloques.

La **disponibilidad** se asegura por la naturaleza descentralizada de la blockchain.

Además, para disuadir posibles ataques, la teoría del Consenso Nakamoto se apoya en la **seguridad termodinámica** y **teoría de juegos**.

Seguridad en RSK

Lo principal a garantizar en una blockchain es la **integridad**, **disponibilidad** y **autenticidad**.

La criptografía garantiza la **autenticidad** de las transacciones y la **integridad** de los bloques.

La **disponibilidad** se asegura por la naturaleza descentralizada de la blockchain.

Además, para disuadir posibles ataques, la teoría del Consenso Nakamoto se apoya en la **seguridad termodinámica** y **teoría de juegos**.

Un atacante **irracional** deberia ser capaz de realizar 2^{80} operaciones de *hash* en menos de 30 segundos para atacar RSK.

Seguridad en RSK

Lo principal a garantizar en una blockchain es la **integridad**, **disponibilidad** y **autenticidad**.

La criptografía garantiza la **autenticidad** de las transacciones y la **integridad** de los bloques.

La **disponibilidad** se asegura por la naturaleza descentralizada de la blockchain.

Además, para disuadir posibles ataques, la teoría del Consenso Nakamoto se apoya en la **seguridad termodinámica** y **teoría de juegos**.

Un atacante **irracional** deberia ser capaz de realizar 2^{80} operaciones de *hash* en menos de 30 segundos para atacar RSK.

Sin embargo, un atacante **racional** preferiría hacer *merge-mining* en RSK en lugar de intentar otro tipo de ataques.

Índice

Conclusiones

- Entre el **40 %** y el **51 %** de los mineros de Bitcoin están actualmente realizando merge-mining en **RSK**.

Conclusiones

- Entre el **40 %** y el **51 %** de los mineros de Bitcoin están actualmente realizando merge-mining en **RSK**.
- Esto hace que **RSK** sea la plataforma de *smart contracts* **más segura** del planeta.

¿Dudas?