RSK:
Bitcoin Merge Mining is Here to Stay

Sergio Demian Lerner

Facultad de Ciencias Exactas, Ingeniería y Agrimensura
Universidad Nacional de Rosario

Joaquín Caporalini

Febrero 2025

Repaso: Como contruir un bloque de Bitcoin[1]

Versión puramente electrónica de efectivo, sin tener que pasar por medio de una institución financiera.

La solución al problema del doble gasto: Una red *peer-to-peer* basada en el **consenso**.

[1] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System.

Repaso: Como contruir un bloque de Bitcoin[1]

Versión puramente electrónica de efectivo, sin tener que pasar por medio de una institución financiera.

La solución al problema del doble gasto: Una red *peer-to-peer* basada en el **consenso**.

El consenso el logrado a través de un mecanismo de **prueba de trabajo**.

[1] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System.

Repaso: Como contruir un bloque de Bitcoin[1]

Versión puramente electrónica de efectivo, sin tener que pasar por medio de una institución financiera.

La solución al problema del doble gasto: Una red *peer-to-peer* basada en el **consenso**.

El consenso el logrado a través de un mecanismo de **prueba de trabajo**.

[1] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System.

Merge-Mining

Definición

Técnica que permite minar dos o más criptomonedas al mismo tiempo sin gastar poder de cómputo extra.

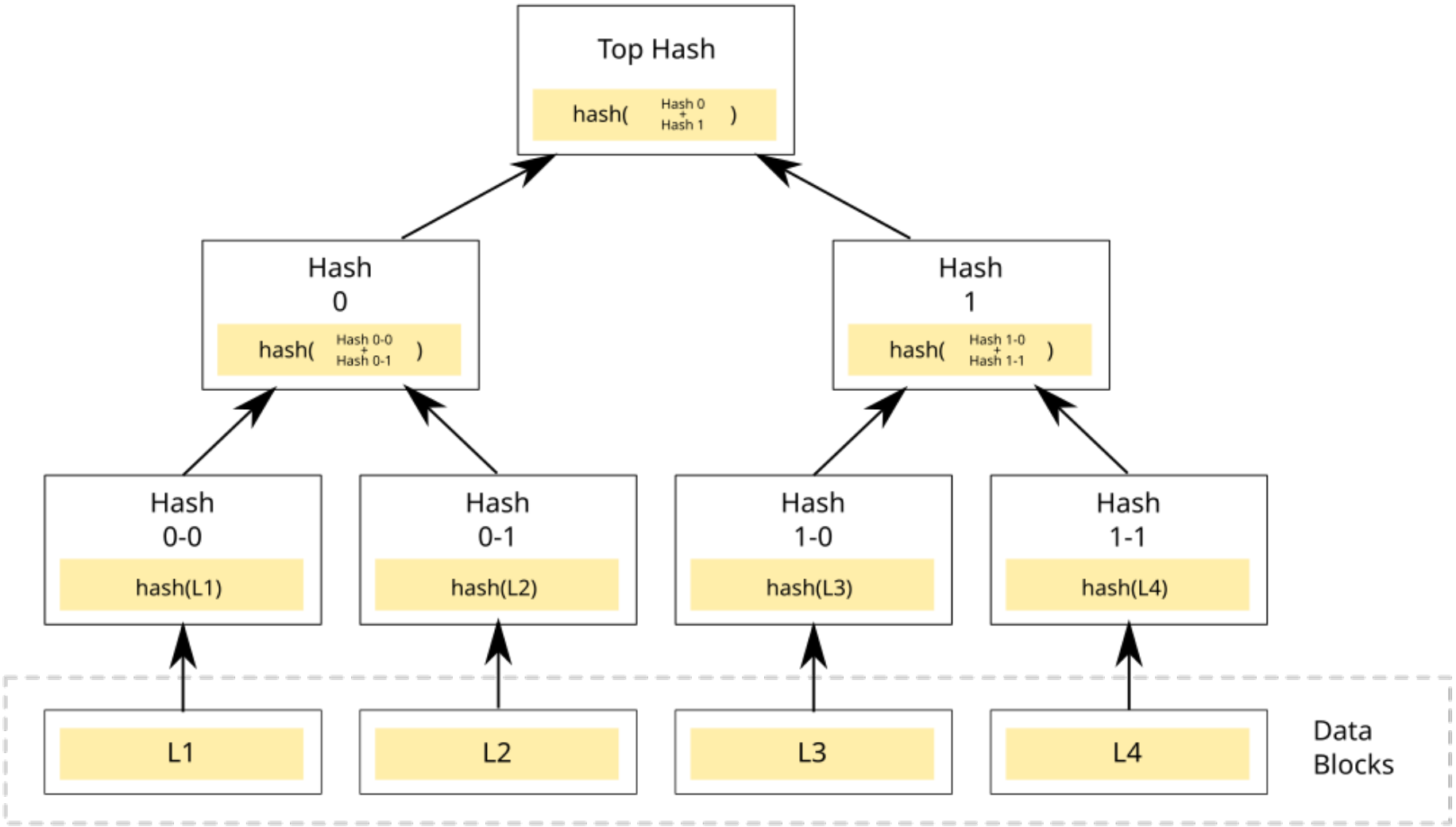
Merge-Mining

Definición

Técnica que permite minar dos o más criptomonedas al mismo tiempo sin gastar poder de cómputo extra.

- Misma tasa de emisión de bloques.
- Mismo algoritmo de prueba de trabajo(*PoW*).
- Un bloque de la primaria y uno o ninguno de la secundaria.
- Distintas dificultades de minado (*target*)

Árboles de Merkle



Las pruebas SPV

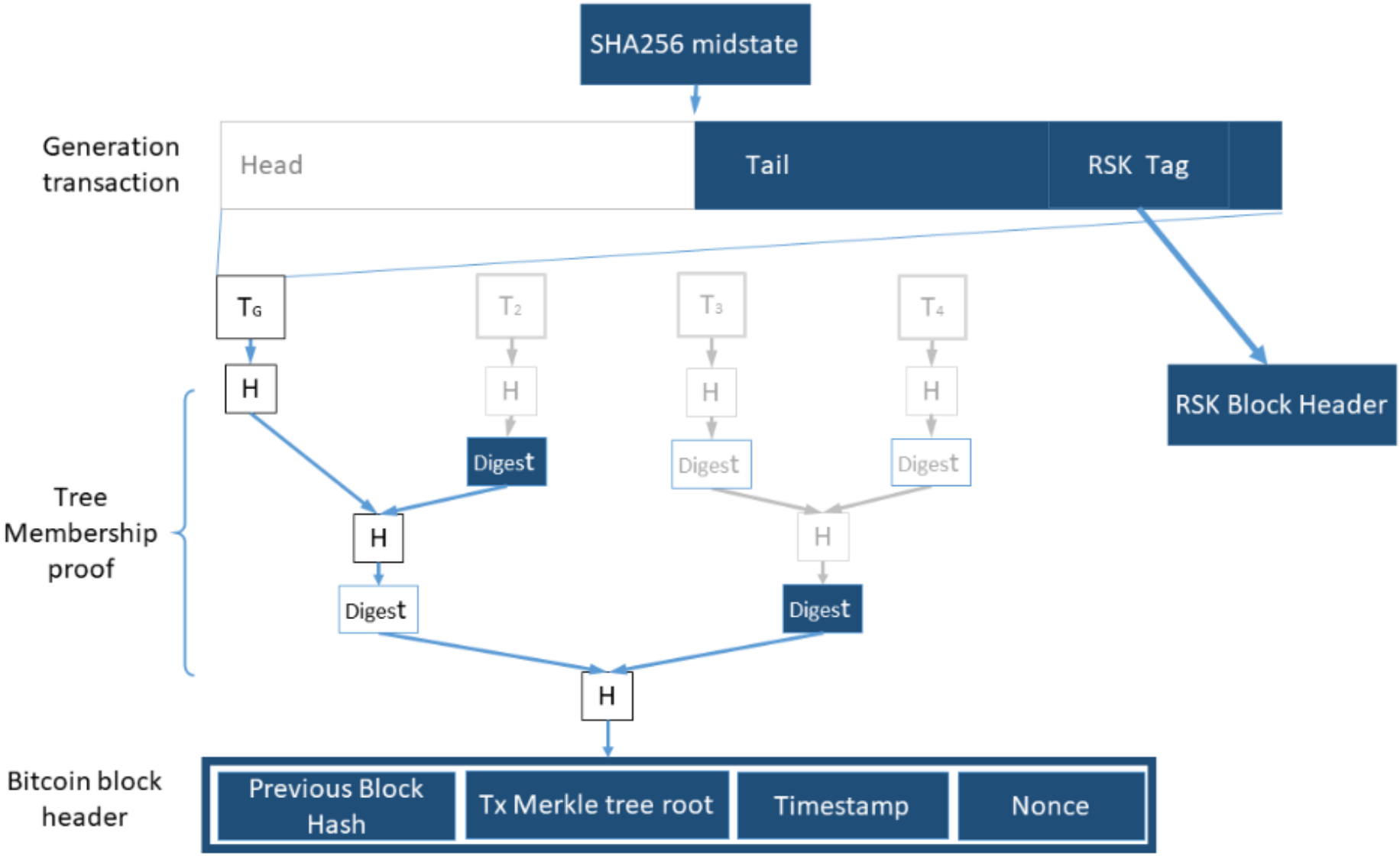
Verificar que una transacción está incluida en la blockchain.

Para verificar que una transacción pertenece a un bloque, el nodo SPV solo necesita la ruta Merkle (*Merkle Path*) para reconstruir la *Merkle Root*.

RSK

Puede verificar que la relación está hecha sin necesidad de leer el bloque de Bitcoin.

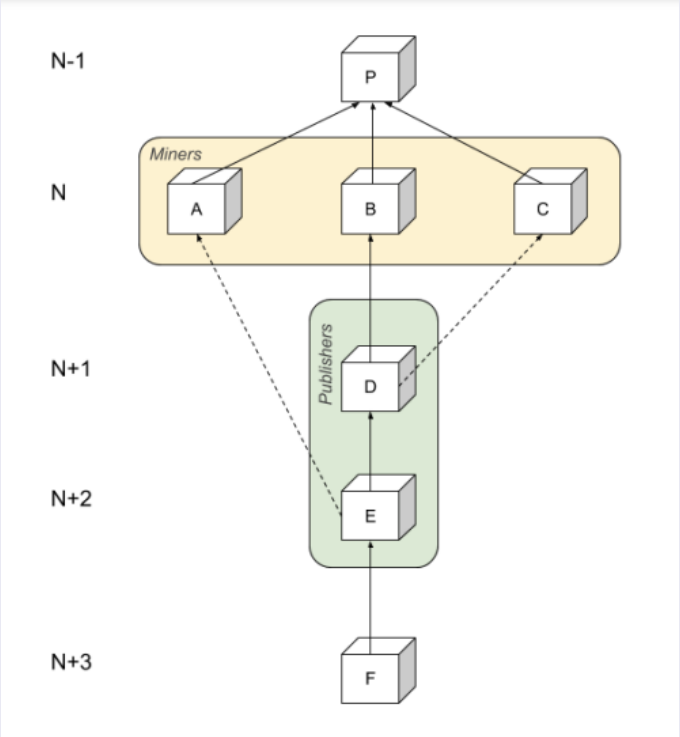
Las pruebas SPV



Como se relacionan las cadenas

Lograr una relación bidireccional entre cadenas

RSK



- A, B y C comparten el mismo padre P.
- B es el *best block*, A y C son *siblings*.
- D incluye a C como *uncle*. E incluye a C como *uncle*.
- F es un nuevo bloque agregado a la mainchain

[1] Medina, M. G. (2021) Un estudio del rendimiento del minado Bitcoin en escenarios de Merged Mining

Jerarquia de targets

Definición

Es la dificultad definida para una PoW. Más alta implica menos dificultad.

Jerarquia de targets

Definición

Es la dificultad definida para una PoW. Más alta implica menos dificultad.

Resolver el problema de la cadena principal (mayor costo) y paralelamente la solución para la secundaria (menor costo).

Las soluciones para la red secundaria son 20 veces más comunes, son validos para ella pero no para la principal

Etiquetas RSK

`RSKBLOCK:<blockHash>`

Puede estar: *codebase ó Output of the generation transaction*

Etiquetas RSK

`RSKBLOCK:<blockHash>`

Puede estar: *codebase ó Output of the generation transaction*

Consideraciones:

- *Luego de la etiqueta debe haber menos de 128bits.*
- *No debería haber etiqueta en los bits libres.*
- *Pueden aparecer por casualidad, ponerlas al final.*
  - *codebase: No es un problema si está la etiqueta `ExtraNonce2`*

Por cuestiones de tamaño suelen estar en la codebase o entre los últimos 4 de la transacción. La segunda permite generar prueba SPV.

Seguridad de la Merge-Mining(RSK)

En general los sistemas de consenso brindan seguridad sobre teoría de juegos y caos.

Ataques:

- Ataque irracionales de 2^{80} operaciones en 30 segundos
- Ataque racional de 2^{69} operaciones.

Posibles lugares de ataque

Usa un truco criptográfico no estándar para comprimir la transacción.

- Solo trasmite su final

Requiere asumir una propiedad fuerte de SHA-256, *freestar collision*. Poder comenzar desde estados intermedios sin tener coliciones en estos.

Posibles lugares de ataque

Usa un truco criptográfico no estándar para comprimir la transacción.

- Solo trasmite su final

Requiere asumir una propiedad fuerte de SHA-256, *freestar collision*. Poder comenzar desde estados intermedios sin tener coliciones en estos.

No hay beneficios por encontrar colisiones a bloques. Tampoco por minar bloques antiguos. Existe la capa de seguridad dada por la PoW.

Cierre:

- Aprovechar la seguridad de Bitcoin.
- Extender los comportamientos de una red (sin modificar su protocolo)
- No necesitar una red de mineros dedicada.
- El minado resulte más atractivo.