Ataques de minado

Ricardo Pérez-Marco (CNRS, Univ. Paris Cité)

Meetup Bitcoin Tuesday, Madrid.

November 9, 2022

Teoría elemental de minado

- Si un minero tiene una proporción $0 \leq q \leq 1$ del hashrate total, la probabilidad de validar el bloque siguiente es q.

Teoría elemental de minado

- Si un minero tiene una proporción $0 \leq q \leq 1$ del hashrate total, la probabilidad de validar el bloque siguiente es q.
- Cada bloque minado e incluido en la blockchain retribuye al minero de una recompensa b (ahora $b = 6.25$ BTC) más las comisiones de las transacciones, en media el "block reward" es de $\bar{b} \geq b$.

Teoría elemental de minado

- Si un minero tiene una proporción $0 \leq q \leq 1$ del hashrate total, la probabilidad de validar el bloque siguiente es q.
- Cada bloque minado e incluido en la blockchain retribuye al minero de una recompensa b (ahora $b = 6.25$ BTC) más las comisiones de las transacciones, en media el "block reward" es de $\bar{b} \geq b$.
- Si en media los bloques se producen cada $t_0 = 10$ min, el minero recibe en media $\bar{b}$ bitcoins cada 10 minutos, de lo cual hay que deducir los costes de minado para calcular la rentabilidad neta.

Ataques de minado

- **Ataque del 51%.**

Ataques de minado

- **Ataque del 51%.** La cadena con mayor trabajo es elegida por los nodos.

Ataques de minado

- **Ataque del 51%.** La cadena con mayor trabajo es elegida por los nodos. Cuando un minero tiene $q > 0.5$ entonces puede minar una cadena con mayor trabajo e imponerla a la red.

Ataques de minado

- **Ataque del 51%.** La cadena con mayor trabajo es elegida por los nodos. Cuando un minero tiene $q > 0.5$ entonces puede minar una cadena con mayor trabajo e imponerla a la red.
- **Ataque de doble gasto**.

Ataques de minado

- **Ataque del 51%.** La cadena con mayor trabajo es elegida por los nodos. Cuando un minero tiene $q > 0.5$ entonces puede minar una cadena con mayor trabajo e imponerla a la red.

- **Ataque de doble gasto**. Se realiza un pago y después de su inclusión en la blockchain e intenta invalidar cambiando los últimos bloques que la contienen.

Ataques de minado

- **Ataque del 51%.** La cadena con mayor trabajo es elegida por los nodos. Cuando un minero tiene $q > 0.5$ entonces puede minar una cadena con mayor trabajo e imponerla a la red.

- **Ataque de doble gasto**. Se realiza un pago y después de su inclusión en la blockchain e intenta invalidar cambiando los últimos bloques que la contienen. En la nueva cadena se incluye una transacción incompatible de manera que la transacción original sea inservible en el futuro.

Ataques de minado

- **Ataque del 51%.** La cadena con mayor trabajo es elegida por los nodos. Cuando un minero tiene $q > 0.5$ entonces puede minar una cadena con mayor trabajo e imponerla a la red.

- **Ataque de doble gasto**. Se realiza un pago y después de su inclusión en la blockchain e intenta invalidar cambiando los últimos bloques que la contienen. En la nueva cadena se incluye una transacción incompatible de manera que la transacción original sea inservible en el futuro. (estudiado por S. Nakamoto en la sección 11 del Bitcoin paper)

Ataques de minado

- **Ataque del 51%.** La cadena con mayor trabajo es elegida por los nodos. Cuando un minero tiene $q > 0.5$ entonces puede minar una cadena con mayor trabajo e imponerla a la red.
- **Ataque de doble gasto**. Se realiza un pago y después de su inclusión en la blockchain e intenta invalidar cambiando los últimos bloques que la contienen. En la nueva cadena se incluye una transacción incompatible de manera que la transacción original sea inservible en el futuro. (estudiado por S. Nakamoto en la sección 11 del Bitcoin paper)
- **Ataque de selfish mining o block withholding**.

Ataques de minado

- **Ataque del 51%.** La cadena con mayor trabajo es elegida por los nodos. Cuando un minero tiene $q > 0.5$ entonces puede minar una cadena con mayor trabajo e imponerla a la red.

- **Ataque de doble gasto**. Se realiza un pago y después de su inclusión en la blockchain e intenta invalidar cambiando los últimos bloques que la contienen. En la nueva cadena se incluye una transacción incompatible de manera que la transacción original sea inservible en el futuro. (estudiado por S. Nakamoto en la sección 11 del Bitcoin paper)

- **Ataque de selfish mining o block withholding**. Se guardan los bloques minados para hacerlos públicos en el momento adecuado para invalidar otros bloques de mineros honestos.

Ataques de minado

- **Ataque del 51%.** La cadena con mayor trabajo es elegida por los nodos. Cuando un minero tiene $q > 0.5$ entonces puede minar una cadena con mayor trabajo e imponerla a la red.

- **Ataque de doble gasto**. Se realiza un pago y después de su inclusión en la blockchain e intenta invalidar cambiando los últimos bloques que la contienen. En la nueva cadena se incluye una transacción incompatible de manera que la transacción original sea inservible en el futuro. (estudiado por S. Nakamoto en la sección 11 del Bitcoin paper)

- **Ataque de selfish mining o block withholding**. Se guardan los bloques minados para hacerlos públicos en el momento adecuado para invalidar otros bloques de mineros honestos.

Estrategias de minado

- **Estrategia de minado**.

Estrategias de minado

- **Estrategia de minado**.Cuando un minero mina un bloque, puede mantenerlo en secreto y hacerlo público según la estrategia más provechosa.

Estrategias de minado

- **Estrategia de minado**.Cuando un minero mina un bloque, puede mantenerlo en secreto y hacerlo público según la estrategia más provechosa.
- **Ciclo de una estrategia**.

Estrategias de minado

- **Estrategia de minado**.Cuando un minero mina un bloque, puede mantenerlo en secreto y hacerlo público según la estrategia más provechosa.
- **Ciclo de una estrategia**. El ciclo de la estrategia se inicia cuando el minero mina de forma honesta sobre el último bloque de la blockchain oficial.

Estrategias de minado

- **Estrategia de minado**.Cuando un minero mina un bloque, puede mantenerlo en secreto y hacerlo público según la estrategia más provechosa.

- **Ciclo de una estrategia**. El ciclo de la estrategia se inicia cuando el minero mina de forma honesta sobre el último bloque de la blockchain oficial.El ciclo se acaba cuando vuelve a este estado inicial después de que se haya minado algún bloque.

Estrategias de minado

• **Estrategia de minado**.Cuando un minero mina un bloque, puede mantenerlo en secreto y hacerlo público según la estrategia más provechosa.

• **Ciclo de una estrategia**. El ciclo de la estrategia se inicia cuando el minero mina de forma honesta sobre el último bloque de la blockchain oficial.El ciclo se acaba cuando vuelve a este estado inicial después de que se haya minado algún bloque. La duración de un ciclo es τ y la estrategia es finita si $\mathbb{E}[\tau] < +\infty$.

Estrategias de minado

- **Estrategia de minado**.Cuando un minero mina un bloque, puede mantenerlo en secreto y hacerlo público según la estrategia más provechosa.

- **Ciclo de una estrategia**. El ciclo de la estrategia se inicia cuando el minero mina de forma honesta sobre el último bloque de la blockchain oficial.El ciclo se acaba cuando vuelve a este estado inicial después de que se haya minado algún bloque. La duración de un ciclo es τ y la estrategia es finita si $\mathbb{E}[\tau] < +\infty$.

- **Ganancia en un ciclo**.

Estrategias de minado

• **Estrategia de minado**.Cuando un minero mina un bloque, puede mantenerlo en secreto y hacerlo público según la estrategia más provechosa.

• **Ciclo de una estrategia**. El ciclo de la estrategia se inicia cuando el minero mina de forma honesta sobre el último bloque de la blockchain oficial.El ciclo se acaba cuando vuelve a este estado inicial después de que se haya minado algún bloque. La duración de un ciclo es τ y la estrategia es finita si $\mathbb{E}[\tau] < +\infty$.

• **Ganancia en un ciclo**. Durante un ciclo, la ganancia obtenida G es la suma de las recompensas de los bloques validados e incluidos en la blockchain oficial.

Estrategias de minado

• **Estrategia de minado**.Cuando un minero mina un bloque, puede mantenerlo en secreto y hacerlo público según la estrategia más provechosa.

• **Ciclo de una estrategia**. El ciclo de la estrategia se inicia cuando el minero mina de forma honesta sobre el último bloque de la blockchain oficial.El ciclo se acaba cuando vuelve a este estado inicial después de que se haya minado algún bloque. La duración de un ciclo es τ y la estrategia es finita si $\mathbb{E}[\tau] < +\infty$.

• **Ganancia en un ciclo**. Durante un ciclo, la ganancia obtenida G es la suma de las recompensas de los bloques validados e incluidos en la blockchain oficial.La rentabilidad temporal es $\Gamma = \mathbb{E}[G]/\mathbb{E}[\tau]$.

Estrategias de minado

• **Estrategia de minado**.Cuando un minero mina un bloque, puede mantenerlo en secreto y hacerlo público según la estrategia más provechosa.

• **Ciclo de una estrategia**. El ciclo de la estrategia se inicia cuando el minero mina de forma honesta sobre el último bloque de la blockchain oficial.El ciclo se acaba cuando vuelve a este estado inicial después de que se haya minado algún bloque. La duración de un ciclo es τ y la estrategia es finita si $\mathbb{E}[\tau] < +\infty$.

• **Ganancia en un ciclo**. Durante un ciclo, la ganancia obtenida G es la suma de las recompensas de los bloques validados e incluidos en la blockchain oficial.La rentabilidad temporal es $\Gamma = \mathbb{E}[G]/\mathbb{E}[\tau]$.

Ejemplo: Ganancia del minado honesto

- **Ciclo de minado honesto**.

Ejemplo: Ganancia del minado honesto

- **Ciclo de minado honesto**.Empieza minando sobre el último bloque de la blockchain oficial, y acaba cuando alguien encuentra un bloque.

Ejemplo: Ganancia del minado honesto

- **Ciclo de minado honesto.**Empieza minando sobre el último bloque de la blockchain oficial, y acaba cuando alguien encuentra un bloque.
- **Ganancia del minado honesto**.

Ejemplo: Ganancia del minado honesto

- **Ciclo de minado honesto.**Empieza minando sobre el último bloque de la blockchain oficial, y acaba cuando alguien encuentra un bloque.
- **Ganancia del minado honesto**. Tenemos $\mathbb{E}[\tau] = t_0$ y

$$\mathbb{E}[G] = q.\bar{b} + 0.\bar{b} = q\bar{b}$$

Ejemplo: Ganancia del minado honesto

• **Ciclo de minado honesto.**Empieza minando sobre el último bloque de la blockchain oficial, y acaba cuando alguien encuentra un bloque.

• **Ganancia del minado honesto**. Tenemos $\mathbb{E}[\tau] = t_0$ y

$$\mathbb{E}[G] = q.\bar{b} + 0.\bar{b} = q\bar{b}$$

Por lo tanto,

$$\Gamma_0 = \frac{\mathbb{E}[G]}{\mathbb{E}[\tau]} = \frac{q\bar{b}}{t_0}$$

Ejemplo: Ganancia del minado honesto

• **Ciclo de minado honesto.**Empieza minando sobre el último bloque de la blockchain oficial, y acaba cuando alguien encuentra un bloque.

• **Ganancia del minado honesto**. Tenemos $\mathbb{E}[\tau] = t_0$ y

$$\mathbb{E}[G] = q.\bar{b} + 0.\bar{b} = q\bar{b}$$

Por lo tanto,

$$\Gamma_0 = \frac{\mathbb{E}[G]}{\mathbb{E}[\tau]} = \frac{q\bar{b}}{t_0}$$

Rentabilidad de una estrategias de minado

- **Rentabilidad media de un ciclo**.

Rentabilidad de una estrategias de minado

- **Rentabilidad media de un ciclo**.Además de la ganancia G el minero tiene unos costes operativos en cada ciclo de C.

Rentabilidad de una estrategias de minado

• **Rentabilidad media de un ciclo**.Además de la ganancia G el minero tiene unos costes operativos en cada ciclo de C. La rentabilidad media temporal de un ciclo es

$$\frac{\mathbb{E}[G]}{\mathbb{E}[\tau]} - \frac{\mathbb{E}[C]}{\mathbb{E}[\tau]}$$

Rentabilidad de una estrategias de minado

- **Rentabilidad media de un ciclo**.Además de la ganancia G el minero tiene unos costes operativos en cada ciclo de C. La rentabilidad media temporal de un ciclo es

$$\frac{\mathbb{E}[G]}{\mathbb{E}[\tau]} - \frac{\mathbb{E}[C]}{\mathbb{E}[\tau]}$$

- **Rentabilidad media de una estrategia**.

Rentabilidad de una estrategias de minado

• **Rentabilidad media de un ciclo**.Además de la ganancia G el minero tiene unos costes operativos en cada ciclo de C. La rentabilidad media temporal de un ciclo es

$$\frac{\mathbb{E}[G]}{\mathbb{E}[\tau]} - \frac{\mathbb{E}[C]}{\mathbb{E}[\tau]}$$

• **Rentabilidad media de una estrategia**. Se obtiene como límite cuando $n \to +\infty$ de la rentabilidad de n ciclos sucesivos:

$$\frac{G_1 + \ldots + G_n}{\tau_1 + \ldots + \tau_n} - \frac{C_1 + \ldots + C_n}{\tau_1 + \ldots + \tau_n} \to \frac{\mathbb{E}[G]}{\mathbb{E}[\tau]} - \frac{\mathbb{E}[C]}{\mathbb{E}[\tau]}$$

Rentabilidad de una estrategias de minado

• **Rentabilidad media de un ciclo**.Además de la ganancia G el minero tiene unos costes operativos en cada ciclo de C. La rentabilidad media temporal de un ciclo es

$$\frac{\mathbb{E}[G]}{\mathbb{E}[\tau]} - \frac{\mathbb{E}[C]}{\mathbb{E}[\tau]}$$

• **Rentabilidad media de una estrategia**. Se obtiene como límite cuando $n \to +\infty$ de la rentabilidad de n ciclos sucesivos:

$$\frac{G_1 + \ldots + G_n}{\tau_1 + \ldots + \tau_n} - \frac{C_1 + \ldots + C_n}{\tau_1 + \ldots + \tau_n} \to \frac{\mathbb{E}[G]}{\mathbb{E}[\tau]} - \frac{\mathbb{E}[C]}{\mathbb{E}[\tau]}$$

Comparando rentabilidades

- **Obsevación fundamental!**

Comparando rentabilidades

- **Obsevación fundamental!** Los costes de una estrategia de minado continuo no dependen de la estrategia de liberación de bloques!

Comparando rentabilidades

- **Obsevación fundamental!** Los costes de una estrategia de minado continuo no dependen de la estrategia de liberación de bloques!
- **Comparando rentabilidades**.

Comparando rentabilidades

• **Obsevación fundamental!** Los costes de una estrategia de minado continuo no dependen de la estrategia de liberación de bloques!

• **Comparando rentabilidades**. Para comparar las rentabilidades de estrategias de minado, únicamente es necesario comparar las ganancias medias de minado $\Gamma = \mathbb{E}[G]/\mathbb{E}[\tau]$.

Comparando rentabilidades

• **Obsevación fundamental!** Los costes de una estrategia de minado continuo no dependen de la estrategia de liberación de bloques!

• **Comparando rentabilidades**. Para comparar las rentabilidades de estrategias de minado, únicamente es necesario comparar las ganancias medias de minado $\Gamma = \mathbb{E}[G]/\mathbb{E}[\tau]$.

Corolario.

Comparando rentabilidades

• **Obsevación fundamental!** Los costes de una estrategia de minado continuo no dependen de la estrategia de liberación de bloques!

• **Comparando rentabilidades**. Para comparar las rentabilidades de estrategias de minado, únicamente es necesario comparar las ganancias medias de minado $\Gamma = \mathbb{E}[G]/\mathbb{E}[\tau]$.

Corolario. *Una estrategia de minado finita es más rentable que la estrategia honesta cuando* $\Gamma > \Gamma_0 = \frac{q\bar{b}}{t_0}$.

Comparando rentabilidades

• **Obsevación fundamental!** Los costes de una estrategia de minado continuo no dependen de la estrategia de liberación de bloques!

• **Comparando rentabilidades**. Para comparar las rentabilidades de estrategias de minado, únicamente es necesario comparar las ganancias medias de minado $\Gamma = \mathbb{E}[G]/\mathbb{E}[\tau]$.

Corolario. *Una estrategia de minado finita es más rentable que la estrategia honesta cuando* $\Gamma > \Gamma_0 = \frac{q\bar{b}}{t_0}$.

Blockwithholding, dificultad y tiempo entre bloques

- **Dificultad**.

Blockwithholding, dificultad y tiempo entre bloques

- **Dificultad**. Cada 2016 bloques se ajusta la dificultad para que el tiempo medio entre bloques sea de 10 minutos.

Blockwithholding, dificultad y tiempo entre bloques

- **Dificultad**. Cada 2016 bloques se ajusta la dificultad para que el tiempo medio entre bloques sea de 10 minutos.
- Estrategias de minado de blockwithholding provocan la ralentización de la red.

Blockwithholding, dificultad y tiempo entre bloques

- **Dificultad**. Cada 2016 bloques se ajusta la dificultad para que el tiempo medio entre bloques sea de 10 minutos.
- Estrategias de minado de blockwithholding provocan la ralentización de la red. Esto disminuye la rentabilidad temporal.

Blockwithholding, dificultad y tiempo entre bloques

- **Dificultad**. Cada 2016 bloques se ajusta la dificultad para que el tiempo medio entre bloques sea de 10 minutos.
- Estrategias de minado de blockwithholding provocan la ralentización de la red. Esto disminuye la rentabilidad temporal.
- Sin ajuste de dificultad durante el ciclo, el tiempo medio $\mathbb{E}[\tau]$ es proporcional al incremento H de la blockchain oficial, $\mathbb{E}[\tau] = \mathbb{E}[H].t_0$.

Blockwithholding, dificultad y tiempo entre bloques

- **Dificultad**. Cada 2016 bloques se ajusta la dificultad para que el tiempo medio entre bloques sea de 10 minutos.
- Estrategias de minado de blockwithholding provocan la ralentización de la red. Esto disminuye la rentabilidad temporal.
- Sin ajuste de dificultad durante el ciclo, el tiempo medio $\mathbb{E}[\tau]$ es proporcional al incremento H de la blockchain oficial, $\mathbb{E}[\tau] = \mathbb{E}[H].t_0$.Sólo es necesario comparar $\mathbb{E}[G]/\mathbb{E}[H]$ para comparar rentabilidades de diferentes estrategias. Para la estrategia honesta $\mathbb{E}[H] = 1$ y $\mathbb{E}[G]/\mathbb{E}[H] = q\bar{b}$.

Blockwithholding, dificultad y tiempo entre bloques

- **Dificultad**. Cada 2016 bloques se ajusta la dificultad para que el tiempo medio entre bloques sea de 10 minutos.
- Estrategias de minado de blockwithholding provocan la ralentización de la red. Esto disminuye la rentabilidad temporal.
- Sin ajuste de dificultad durante el ciclo, el tiempo medio $\mathbb{E}[\tau]$ es proporcional al incremento H de la blockchain oficial, $\mathbb{E}[\tau] = \mathbb{E}[H].t_0$.Sólo es necesario comparar $\mathbb{E}[G]/\mathbb{E}[H]$ para comparar rentabilidades de diferentes estrategias. Para la estrategia honesta $\mathbb{E}[H] = 1$ y $\mathbb{E}[G]/\mathbb{E}[H] = q\bar{b}$.
- **Teorema**.

Blockwithholding, dificultad y tiempo entre bloques

• **Dificultad**. Cada 2016 bloques se ajusta la dificultad para que el tiempo medio entre bloques sea de 10 minutos.

• Estrategias de minado de blockwithholding provocan la ralentización de la red. Esto disminuye la rentabilidad temporal.

• Sin ajuste de dificultad durante el ciclo, el tiempo medio $\mathbb{E}[\tau]$ es proporcional al incremento H de la blockchain oficial, $\mathbb{E}[\tau] = \mathbb{E}[H].t_0$.Sólo es necesario comparar $\mathbb{E}[G]/\mathbb{E}[H]$ para comparar rentabilidades de diferentes estrategias. Para la estrategia honesta $\mathbb{E}[H] = 1$ y $\mathbb{E}[G]/\mathbb{E}[H] = q\bar{b}$.

• **Teorema**. *Sin ajuste de dificultad, la estrategia de minado óptima es la estrategia honesta.*

Blockwithholding, dificultad y tiempo entre bloques

• **Dificultad**. Cada 2016 bloques se ajusta la dificultad para que el tiempo medio entre bloques sea de 10 minutos.

• Estrategias de minado de blockwithholding provocan la ralentización de la red. Esto disminuye la rentabilidad temporal.

• Sin ajuste de dificultad durante el ciclo, el tiempo medio $\mathbb{E}[\tau]$ es proporcional al incremento H de la blockchain oficial, $\mathbb{E}[\tau] = \mathbb{E}[H].t_0$.Sólo es necesario comparar $\mathbb{E}[G]/\mathbb{E}[H]$ para comparar rentabilidades de diferentes estrategias. Para la estrategia honesta $\mathbb{E}[H] = 1$ y $\mathbb{E}[G]/\mathbb{E}[H] = q\bar{b}$.

• **Teorema**. *Sin ajuste de dificultad, la estrategia de minado óptima es la estrategia honesta.*

La demostración usa la Teoría matemática de Martingalas.

Estrategias deshonestas rentables

- El Teorema no es cierto con ajuste de dificultad.

Estrategias deshonestas rentables

- El Teorema no es cierto con ajuste de dificultad.
- El protocolo Bitcoin no es consistente.

Estrategias deshonestas rentables

- El Teorema no es cierto con ajuste de dificultad.
- El protocolo Bitcoin no es consistente.
- Existen estrategias de minado de blockwithholding que son más rentables que la estrategia de minado honesta.

Estrategias deshonestas rentables

- El Teorema no es cierto con ajuste de dificultad.
- El protocolo Bitcoin no es consistente.
- Existen estrategias de minado de blockwithholding que son más rentables que la estrategia de minado honesta.
- El ejemplo más simple: Estrategia 1+2.

Estrategia 1+2

Estrategia 1+2

- El objetivo del minero atacante es minar un bloque, guardarlo en secreto y minar encima de su bloque secreto.

Estrategia 1+2

- El objetivo del minero atacante es minar un bloque, guardarlo en secreto y minar encima de su bloque secreto.
- Si la red mina antes un bloque, el ciclo se acaba. Entonces se empieza de nuevo a minar encima del último bloque de la blockchain oficial.

Estrategia 1+2

- El objetivo del minero atacante es minar un bloque, guardarlo en secreto y minar encima de su bloque secreto.
- Si la red mina antes un bloque, el ciclo se acaba. Entonces se empieza de nuevo a minar encima del último bloque de la blockchain oficial.
- Si el atacante consigue minar un bloque antes que la red, entonces espera que se minen 2 bloques más para acabar el ciclo.

Estrategia 1+2

- El objetivo del minero atacante es minar un bloque, guardarlo en secreto y minar encima de su bloque secreto.
- Si la red mina antes un bloque, el ciclo se acaba. Entonces se empieza de nuevo a minar encima del último bloque de la blockchain oficial.
- Si el atacante consigue minar un bloque antes que la red, entonces espera que se minen 2 bloques más para acabar el ciclo. Hace público sus bloques secretos si ha conseguido minar al menos un bloque más (en ese caso su blockchain es más larga y se impone).

Posibles ciclos de la estrategia 1+2

Posibles ciclos de la estrategia 1+2

- Posibles ciclos (A bloque atacante, B bloque honesto):

$$\Omega = \{B, AAA, AAB, ABA, ABB\}$$

Posibles ciclos de la estrategia 1+2

- Posibles ciclos (A bloque atacante, B bloque honesto):

$$\Omega = \{B, AAA, AAB, ABA, ABB\}$$

- Probabilidades correspondientes (q hashrate del atacante y $p = 1 - q$ el del resto de la red):

$$\mathbb{P}[B] = p, \mathbb{P}[AAA] = q^3, \mathbb{P}[AAB] = \mathbb{P}[ABA] = pq^2, \mathbb{P}[ABB] = p^2 q$$

Posibles ciclos de la estrategia 1+2

- Posibles ciclos (A bloque atacante, B bloque honesto):

$$\Omega = \{B, AAA, AAB, ABA, ABB\}$$

- Probabilidades correspondientes (q hashrate del atacante y $p = 1 - q$ el del resto de la red):

$$\mathbb{P}[B] = p, \mathbb{P}[AAA] = q^3, \mathbb{P}[AAB] = \mathbb{P}[ABA] = pq^2, \mathbb{P}[ABB] = p^2 q$$

Rentabilidad de la estrategia 1+2

Calculamos las ganancias (rentabilidades en unidades de $\bar{b}$):

Rentabilidad de la estrategia 1+2

Calculamos las ganancias (rentabilidades en unidades de $\bar{b}$):

$$G(B) = G(ABB) = 0, G(AAA) = 3, G(AAB) = G(ABA) = 2$$

Rentabilidad de la estrategia 1+2

Calculamos las ganancias (rentabilidades en unidades de $\bar{b}$):

$$G(B) = G(ABB) = 0, G(AAA) = 3, G(AAB) = G(ABA) = 2$$

y también las alturas

$$H(B) = 1, H(ABB) = H(AAB) = H(ABA) = 2, H(AAA) = 3$$

Rentabilidad de la estrategia 1+2

Calculamos las ganancias (rentabilidades en unidades de $\bar{b}$):

$$G(B) = G(ABB) = 0, G(AAA) = 3, G(AAB) = G(ABA) = 2$$

y también las alturas

$$H(B) = 1, H(ABB) = H(AAB) = H(ABA) = 2, H(AAA) = 3$$

Por lo tanto, tenemos las esperanzas:

$$\mathbb{E}[G] = p \cdot 0 + q^3 \cdot 3 + pq^2 \cdot 2 + pq^2 \cdot 2 + p^2 q \cdot 0 = q^2(4 - q)$$
$$\mathbb{E}[H] = p \cdot 1 + q^3 \cdot 3 + pq^2 \cdot 2 + pq^2 \cdot 2 + p^2 q \cdot 2 = 1 + q + q^2$$

Comparando rentabilidades

La rentabilidad de la estrategia 1+2 es mayor que la de la estrategia honesta cuando

$$\Gamma = \frac{\mathbb{E}[G]}{\mathbb{E}[H]} = \frac{q^2 \cdot (4 - q)}{1 + q + q^3} > \Gamma_0 = q$$

Comparando rentabilidades

La rentabilidad de la estrategia 1+2 es mayor que la de la estrategia honesta cuando

$$\Gamma = \frac{\mathbb{E}[G]}{\mathbb{E}[H]} = \frac{q^2 \cdot (4-q)}{1+q+q^3} > \Gamma_0 = q$$

Esto ocurre exactamente cuando

$$q > \sqrt{2} - 1 = 0.4142\ldots$$

Solución: Cambiar la fórmula de ajuste de dificultad

- La raíz del problema es la fórmula de ajuste de dificultad

$$\Delta' = \Delta \cdot \frac{n_0 \times 10}{T}$$

donde T es el tiempo en minutos que ha durado el periodo de 2016 bloques y $n_0 = 2016$.

Solución: Cambiar la fórmula de ajuste de dificultad

- La raíz del problema es la fórmula de ajuste de dificultad

$$\Delta' = \Delta \cdot \frac{n_0 \times 10}{T}$$

donde T es el tiempo en minutos que ha durado el periodo de 2016 bloques y $n_0 = 2016$.

- La fórmula utiliza los bloques validados para estimar el hashrate total, pero se olvida de los bloques huérfanos.

Solución: Cambiar la fórmula de ajuste de dificultad

- La raíz del problema es la fórmula de ajuste de dificultad

$$\Delta' = \Delta \cdot \frac{n_0 \times 10}{T}$$

donde T es el tiempo en minutos que ha durado el periodo de 2016 bloques y $n_0 = 2016$.

- La fórmula utiliza los bloques validados para estimar el hashrate total, pero se olvida de los bloques huérfanos.
- Podemos mejorarla incluyendo bloques huérfanos:

$$\Delta' = \Delta \cdot \frac{(n_0 + n_1) \times 10}{T}$$

con n_1 el número de bloques huérfanos en el periodo de dificultad constante.

Solución: Cambiar la fórmula de ajuste de dificultad

- La raíz del problema es la fórmula de ajuste de dificultad

$$\Delta' = \Delta \cdot \frac{n_0 \times 10}{T}$$

donde T es el tiempo en minutos que ha durado el periodo de 2016 bloques y $n_0 = 2016$.

- La fórmula utiliza los bloques validados para estimar el hashrate total, pero se olvida de los bloques huérfanos.
- Podemos mejorarla incluyendo bloques huérfanos:

$$\Delta' = \Delta \cdot \frac{(n_0 + n_1) \times 10}{T}$$

con n_1 el número de bloques huérfanos en el periodo de dificultad constante.

Señalización de los bloques huérfanos

• La existencia de bloques huérfanos no figuran el la blockchain, pero se puede diseñar un sistema para su señalización por los mineros honestos.

Señalización de los bloques huérfanos

- La existencia de bloques huérfanos no figuran el la blockchain, pero se puede diseñar un sistema para su señalización por los mineros honestos.
- Incluso se puede hacer mejor: Se puede recompensar el minado de bloques huérfanos, lo cual incentiva su señalización.

Señalización de los bloques huérfanos

• La existencia de bloques huérfanos no figuran el la blockchain, pero se puede diseñar un sistema para su señalización por los mineros honestos.

• Incluso se puede hacer mejor: Se puede recompensar el minado de bloques huérfanos, lo cual incentiva su señalización.

Teorema. *Si recompensamos los bloques huérfanos con una recompensa* $< b$ *y modificamos como antes la fórmula de ajuste de dificultad, entonces la estrategia de minado óptima es la estrategia honesta.*

Señalización de los bloques huérfanos

• La existencia de bloques huérfanos no figuran el la blockchain, pero se puede diseñar un sistema para su señalización por los mineros honestos.

• Incluso se puede hacer mejor: Se puede recompensar el minado de bloques huérfanos, lo cual incentiva su señalización.

Teorema. *Si recompensamos los bloques huérfanos con una recompensa* $< b$ *y modificamos como antes la fórmula de ajuste de dificultad, entonces la estrategia de minado óptima es la estrategia honesta.*

Gracias por vuestra atención!

Gracias por vuestra atención!