La Cadena de Bloques

Promesas y Retos

Jesús Fernández-Villaverde[1]

28 Junio de 2018

[1]University of Pennsylvania

Verificación de situaciones

- Un problema fundamental en la actividad económica es la verificación de condiciones:

  1. ¿Quién es el propietario de este inmueble?
  2. ¿Ha sido un paquete entregado a su destinatario?
  3. ¿Qué tenemos en el almacén?
  4. ¿Cuál es la situación de mi cuenta corriente?
  5. ¿Quién ha pagado la comunidad de vecinos este mes?
  6. ¿Cuántos créditos de enseñanza he acumulado con mi departamento?

- Versiones complejas de este problema aparece también en la gestión interna de sistemas industriales (por ejemplo, en aviónica), pero hoy no las discutiré.

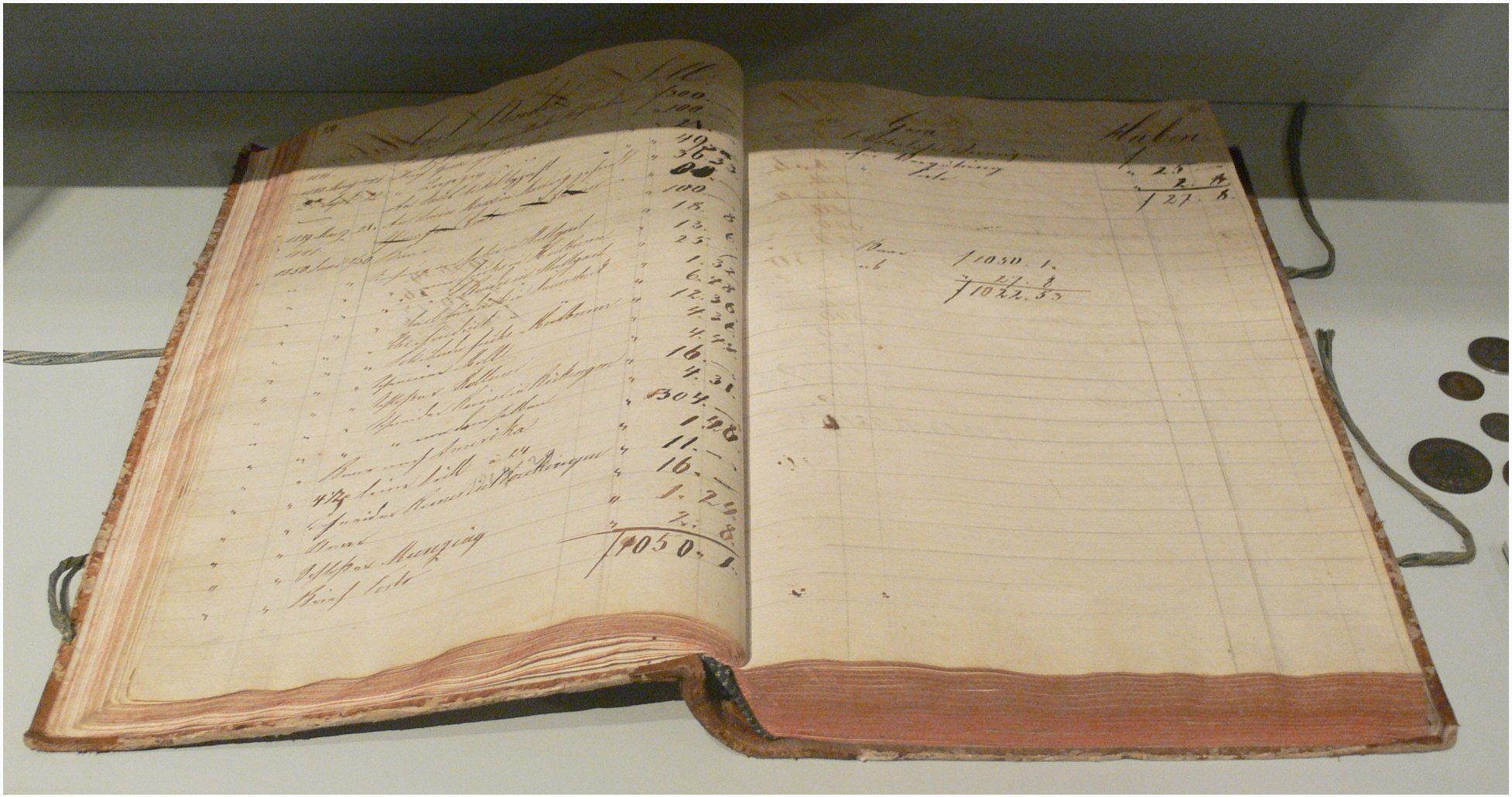
Consecuencias

- La dificultad en verificar las condiciones impide (o encarece) las transacciones económicas.
- En buena medida, los sistemas de derecho privado están (o deberían estar) diseñados para facilitar esta labor de verificación y con ello maximizar el tráfico jurídico y la generación de excedente en las transacciones.
- En ausencia de estos sistemas legales, nos encontramos con muy pocas transacciones.


© Alamy Stock Photo

Sistemas centralizados

- Una solución común es emplear sistemas centralizados de verificaciones.
- Están compuestos de tres elementos:
  1. un libro mayor.
  2. un registrador.
  3. reglas (y metarreglas).
- El ejemplo más sencillo: registro de la propiedad.
- El objetivo de un registro de la propiedad *"no es publicar actos y contratos sino crear titularidades inatacables en virtud de un acto de poder público."*
- Comparación con el sistema de common law de registro de títulos ("deeds registration").

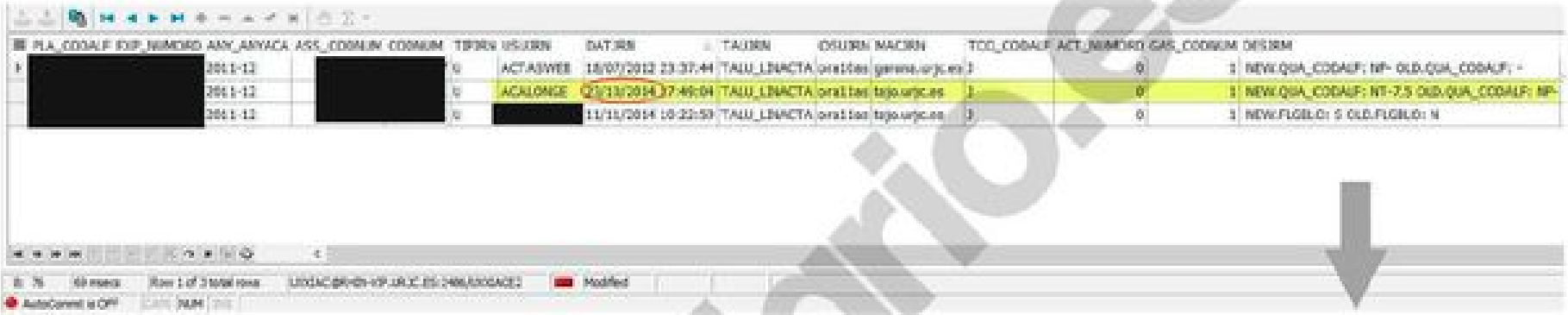


Problemas con los sistemas centralizados

- Sin embargo, los sistemas centralizados sufren de problemas:

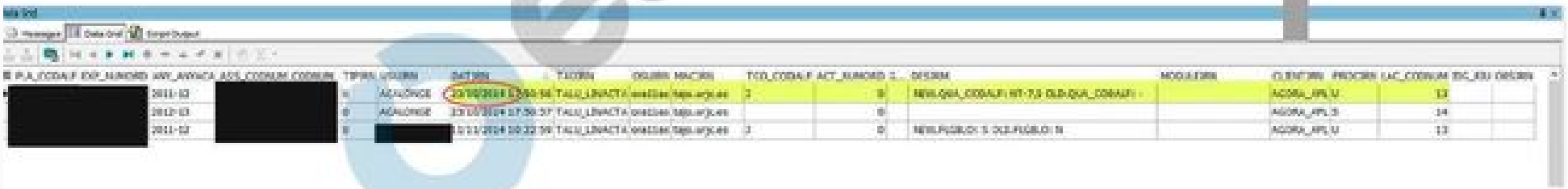
    1. Requieren confianza en el registrador.
    2. Son caros.
    3. Son lentos.
    4. Sufren de problemas de latencia.
    5. Son poco flexibles.
    6. Limitan la introducción de innovación tecnológica.
    7. Hay casos donde no pueden ser aplicados (al menos de manera realista).

Pantallazo correspondiente a la asignatura
« 610705 - La financiación de las Comunidades Autónomas y las entidades locales »



La leyenda muestra que la antigua calificación (OLD.QUA) es No Presentado (NP-). Y se cambia a una nueva calificación (NEW.QUA) Notable-7,5 (NT-7,5).

Pantallazo correspondiente a la asignatura
« 610713 - Trabajo fin de máster Derecho Autonómico »



Sistemas descentralizados I

- ¿Podríamos diseñar sistemas descentralizados de verificaciones?
- Los mismos permitirían, potencialmente, una verificación de condiciones más rápida y eficaz.
- Reducción del riesgo de contraparte y de disputas.
- Con ello, se incrementaría la actividad económica.
- Por ejemplo, permitiendo la creación de “contratos inteligentes” y regulación automática.

Sistemas descentralizados II

- De hecho, ya empleamos sistemas (parcialmente) descentralizados:

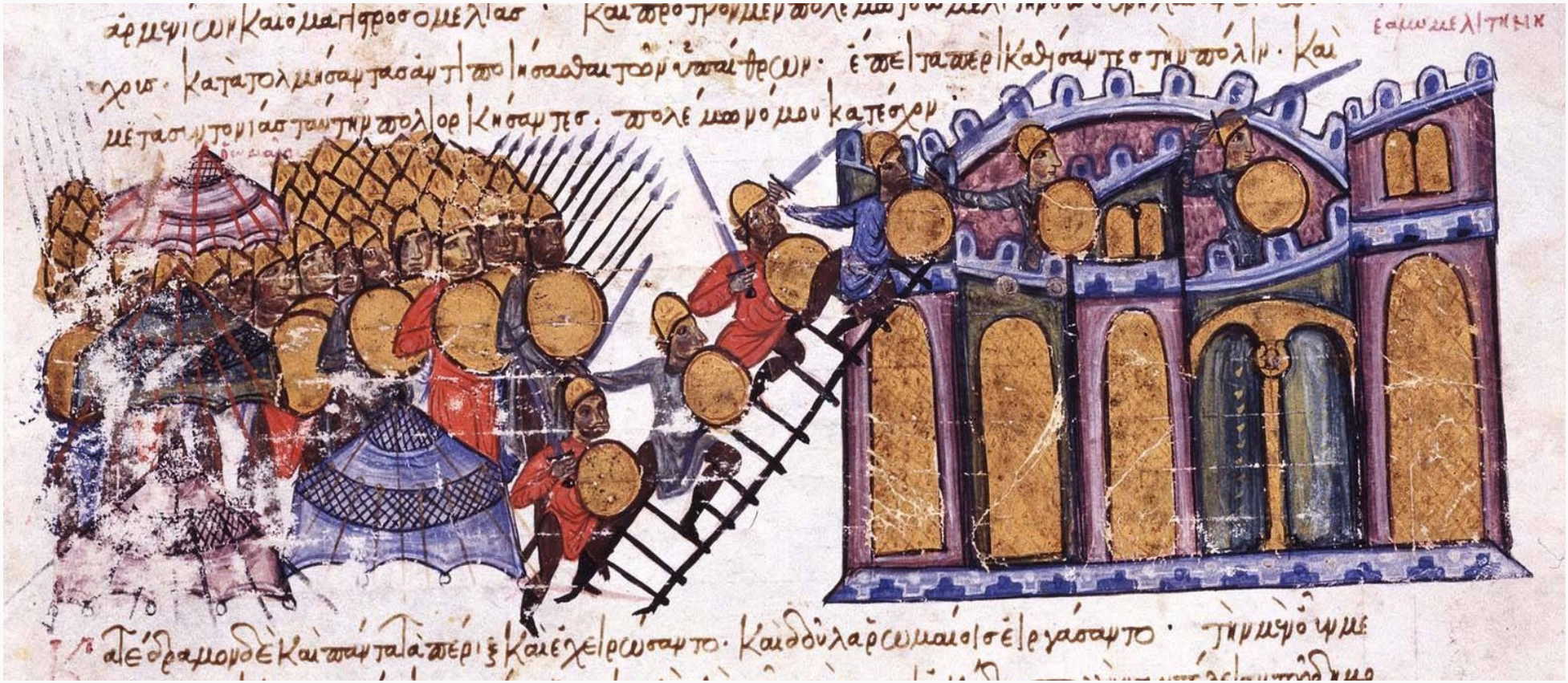
  1. El dinero fiduciario ("el dinero es memoria").

  2. Correo electrónico (Protocolo para transferencia simple de correo, SMTP).

- Centralización vs. descentralización es un continuo.

- Podemos pensar, por tanto, en sistemas mixtos con componentes adaptados a cada situación.

- Pero, ¿cómo podemos conseguir la descentralización?



Problema de los generales bizantinos I

- Propuesto por Lamport, Shostak y Pease (1982):

Problema de los generales bizantinos I

- Propuesto por Lamport, Shostak y Pease (1982):

    1. Varias divisiones del ejército de Bizancio están asediando una ciudad en Capadocia (centro de Anatolia).

Problema de los generales bizantinos I

- Propuesto por Lamport, Shostak y Pease (1982):

  1. Varias divisiones del ejército de Bizancio están asediando una ciudad en Capadocia (centro de Anatolia).

  2. Un general distinto está al cargo de cada división.

Problema de los generales bizantinos I

- Propuesto por Lamport, Shostak y Pease (1982):

  1. Varias divisiones del ejército de Bizancio están asediando una ciudad en Capadocia (centro de Anatolia).

  2. Un general distinto está al cargo de cada división.

  3. Los generales tienen que ponerse de acuerdo en un plan de ataque (por ejemplo, atacar por la mañana o por la tarde).

Problema de los generales bizantinos I

- Propuesto por Lamport, Shostak y Pease (1982):

  1. Varias divisiones del ejército de Bizancio están asediando una ciudad en Capadocia (centro de Anatolia).

  2. Un general distinto está al cargo de cada división.

  3. Los generales tienen que ponerse de acuerdo en un plan de ataque (por ejemplo, atacar por la mañana o por la tarde).

  4. Los generales solo se pueden comunicar entre ellos sus planes de ataque por medio de mensajeros.

Problema de los generales bizantinos I

- Propuesto por Lamport, Shostak y Pease (1982):

  1. Varias divisiones del ejército de Bizancio están asediando una ciudad en Capadocia (centro de Anatolia).

  2. Un general distinto está al cargo de cada división.

  3. Los generales tienen que ponerse de acuerdo en un plan de ataque (por ejemplo, atacar por la mañana o por la tarde).

  4. Los generales solo se pueden comunicar entre ellos sus planes de ataque por medio de mensajeros.

  5. Al menos uno de los generales puede ser un miembro secreto de *Juntos por Capadocia (JxC)* que intenta evitar que los restantes generales acuerden un buen plan de ataque ($\approx$ al problema de las juntas tóricas).

Problema de los generales bizantinos II

- Buscamos un mecanismo que

    1. Asegure que todos los generales leales se ponen de acuerdo en el mismo plan de acción.

    2. Evite que un grupo reducido de generales traidores fuerce la adopción de un mal plan.

Primero, las malas noticias

- El problema no se puede resolver si al menos $1/3$ de los generales son traidores.

Primero, las malas noticias

- El problema no se puede resolver si al menos $1/3$ de los generales son traidores.
- El teorema de Fischer-Lynch-Paterson (FLP) establece que no se puede alcanzar consenso en un sistema de envío de mensajes asincrónico si al menos un general puede ser un traidor excepto si se aumenta el mecanismo (por ejemplo, con aleatorización o sensores de detección de fallos).

Primero, las malas noticias

- El problema no se puede resolver si al menos $1/3$ de los generales son traidores.
- El teorema de Fischer-Lynch-Paterson (FLP) establece que no se puede alcanzar consenso en un sistema de envío de mensajes asincrónico si al menos un general puede ser un traidor excepto si se aumenta el mecanismo (por ejemplo, con aleatorización o sensores de detección de fallos).
- El teorema es sencillo de extender a sistemas de memoria compartida asincrónicos.

Primero, las malas noticias

- El problema no se puede resolver si al menos $1/3$ de los generales son traidores.
- El teorema de Fischer-Lynch-Paterson (FLP) establece que no se puede alcanzar consenso en un sistema de envío de mensajes asincrónico si al menos un general puede ser un traidor excepto si se aumenta el mecanismo (por ejemplo, con aleatorización o sensores de detección de fallos).
- El teorema es sencillo de extender a sistemas de memoria compartida asincrónicos.
- Una exposición detallada aparece en *Distributed Algorithms*, de Nancy A. Lynch (1996).

Primero, las malas noticias

- El problema no se puede resolver si al menos $1/3$ de los generales son traidores.
- El teorema de Fischer-Lynch-Paterson (FLP) establece que no se puede alcanzar consenso en un sistema de envío de mensajes asincrónico si al menos un general puede ser un traidor excepto si se aumenta el mecanismo (por ejemplo, con aleatorización o sensores de detección de fallos).
- El teorema es sencillo de extender a sistemas de memoria compartida asincrónicos.
- Una exposición detallada aparece en *Distributed Algorithms*, de Nancy A. Lynch (1996).
- ¿Quiere esto decir que no hay esperanza?

Primero, las malas noticias

- El problema no se puede resolver si al menos $1/3$ de los generales son traidores.
- El teorema de Fischer-Lynch-Paterson (FLP) establece que no se puede alcanzar consenso en un sistema de envío de mensajes asincrónico si al menos un general puede ser un traidor excepto si se aumenta el mecanismo (por ejemplo, con aleatorización o sensores de detección de fallos).
- El teorema es sencillo de extender a sistemas de memoria compartida asincrónicos.
- Una exposición detallada aparece en *Distributed Algorithms*, de Nancy A. Lynch (1996).
- ¿Quiere esto decir que no hay esperanza?
- No exactamente, ya que podemos diseñar mecanismos que soluciones "casi siempre" el problema de los generales bizantinos.

La cadena de bloques

- Una cadena de bloques es un mecanismo de verificación descentralizado propuesto por Satoshi Nakamoto en 2008 basándose en trabajos previos de Haber y Stornetta (1991) y Bayer, Haber y Stornetta (1992).

- En concreto, es un libro mayor (una estructura de datos) con apuntes en bloques y que se actualiza por consenso de los participantes ("nodos").

- Aunque la primera aplicación (y el desarrollo) de la cadena de bloques ha estado vinculado con las criptomonedas, ambos conceptos son diferentes.

- Uno puede emplear la cadena de bloques para muchas cosas muy alejadas de las criptomonedas y se pueden diseñar criptomonedas que no emplean una cadena de bloques.

- De igual manera, los detalles criptográficos de implementación del protocolo, si bien interesantes, es algo que podemos obviar hoy.

La cadena de bloques como protocolo de consenso distribuido

- Imaginémonos que tenemos n nodos, cada uno de los cuales produce un valor de una variable.
- Algunos de los nodos genera un valor erróneo, con o sin dolo.
- Un protocolo de consenso distribuido ha de satisfacer:
    1. Que todos los nodos honestos terminen con el mismo valor de la variable.
    2. Que este valor haya sido generado por uno de los nodos honestos.
- La cadena de bloques intenta generar tal consenso.

Un ejemplo de cadena de bloques en acción I

- A las 9.00 am, todos los miembros de la red de nodos de repartidores de paquetes tienen un libro mayor en memoria con todos los repartos efectuados hasta las 8.59 am y sobre el que ya se ha alcanzado consenso.

Un ejemplo de cadena de bloques en acción I

- A las 9.00 am, todos los miembros de la red de nodos de repartidores de paquetes tienen un libro mayor en memoria con todos los repartos efectuados hasta las 8.59 am y sobre el que ya se ha alcanzado consenso.

- Alicia entrega un paquete a Borja a las 9.01 am.

Un ejemplo de cadena de bloques en acción I

- A las 9.00 am, todos los miembros de la red de nodos de repartidores de paquetes tienen un libro mayor en memoria con todos los repartos efectuados hasta las 8.59 am y sobre el que ya se ha alcanzado consenso.

- Alicia entrega un paquete a Borja a las 9.01 am.

- Alicia envía un mensaje a las 9.02 am a toda la red de nodos de repartidores de paquetes indicando que el paquete ha sido entregado (por ejemplo, adjuntando un PIN encriptado que Borja ha introducido en un dispositivo al recibir un paquete como prueba que tal entrega se ha efectuado).

Un ejemplo de cadena de bloques en acción I

- A las 9.00 am, todos los miembros de la red de nodos de repartidores de paquetes tienen un libro mayor en memoria con todos los repartos efectuados hasta las 8.59 am y sobre el que ya se ha alcanzado consenso.

- Alicia entrega un paquete a Borja a las 9.01 am.

- Alicia envía un mensaje a las 9.02 am a toda la red de nodos de repartidores de paquetes indicando que el paquete ha sido entregado (por ejemplo, adjuntando un PIN encriptado que Borja ha introducido en un dispositivo al recibir un paquete como prueba que tal entrega se ha efectuado).

- A las 9.10 am, un nodo aleatoriamente seleccionado entre todos los participantes propone a toda la red un nuevo bloque de repartos para añadir al libro mayor existente a las 9.00 am. Este bloque incluye, según el nodo, todas entregas realizadas en los últimos 10 minutos.

Un ejemplo de cadena de bloques en acción II

- Los restantes nodos de la red aceptan el nuevo bloque si pueden verificar que unas condiciones en las transacciones se han cumplido.

Un ejemplo de cadena de bloques en acción II

- Los restantes nodos de la red aceptan el nuevo bloque si pueden verificar que unas condiciones en las transacciones se han cumplido.

- Si una mayoría de los nodos de la red aceptan el bloque propuesto, el mismo se añade al libro mayor y el proceso de repite de 9.10 am a 9.20 am.

Un ejemplo de cadena de bloques en acción II

- Los restantes nodos de la red aceptan el nuevo bloque si pueden verificar que unas condiciones en las transacciones se han cumplido.

- Si una mayoría de los nodos de la red aceptan el bloque propuesto, el mismo se añade al libro mayor y el proceso de repite de 9.10 am a 9.20 am.

- Si, por problemas de latencia, una transacción no se liquida en estos 10 minutos, pasa al siguiente periodo de 10 minutos.

Preguntas más frecuentes

- ¿Cómo seleccionamos el nodo que propone un nuevo bloque? Sistemas de prueba de trabajo vs. prueba de participación. Bitcoin, por ejemplo, emplea un protocolos de solución-verificación (los "mineros").

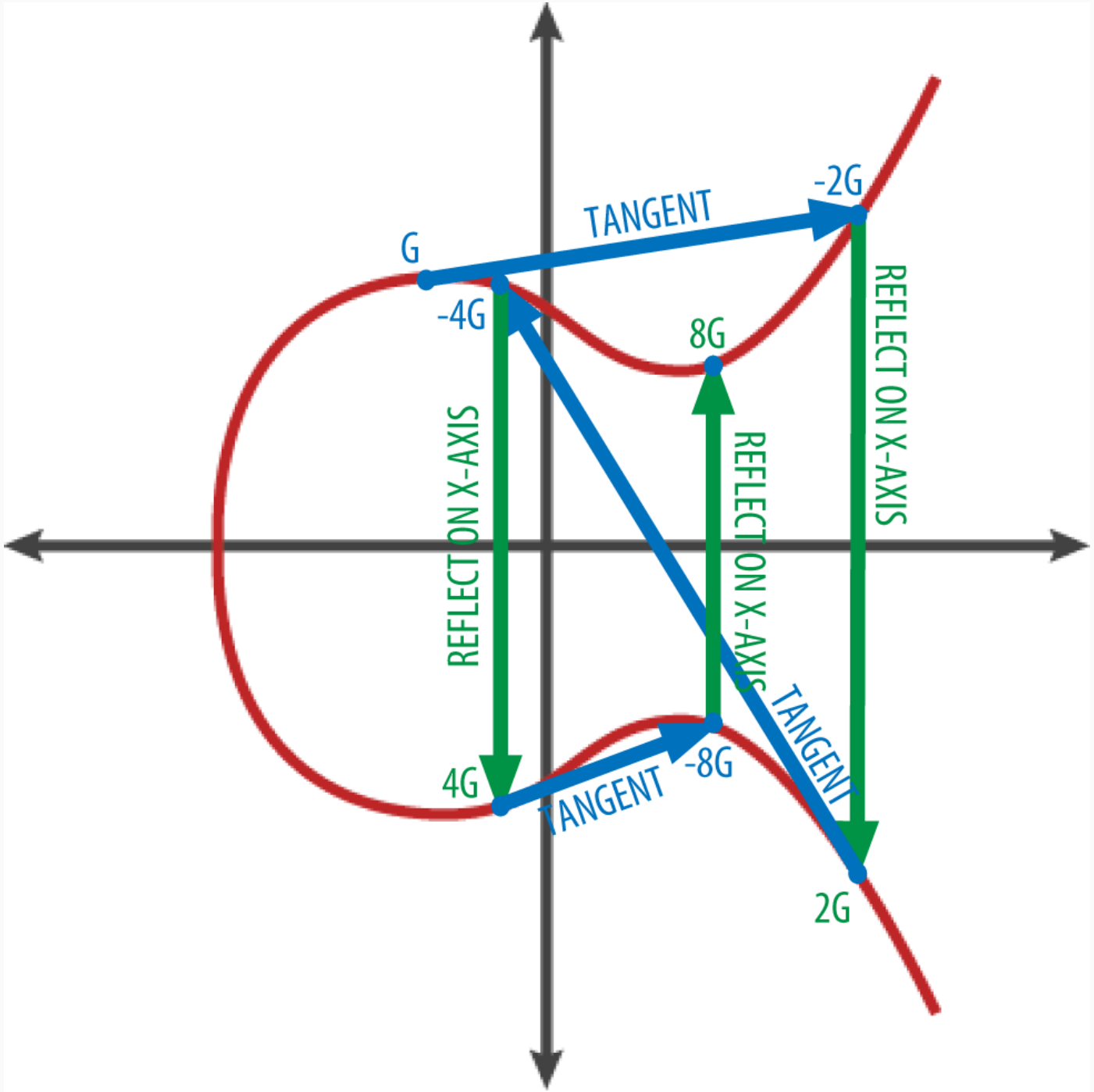
- ¿Por qué participan los nodos en este protocolo? Sistemas de pago vs. sistemas voluntarios.

- ¿Qué incentivos tienen los nodos a intentar agregar el nuevo bloque? Nodo proponente vs. nodos aceptantes.

- ¿Qué nodos pueden participar? Cadenas de bloques autorizadas vs. públicas.

- ¿Cómo resiste la cadena de bloques algunos de los ataques más comunes?

- ¿Es imposible entonces atacar una cadena de bloques? No, especialmente si es pública.


G
TANGENT
-2G
-4G
8G
REFLECT ON X-AXIS
REFLECT ON X-AXIS
REFLECT ON X-AXIS
4G
TANGENT
-8G
TANGENT
2G

Ventajas de la cadena de bloques

- Una cadena de bloques permite crear mecanismos de verificación descentralizados de manera relativamente sencilla.
- Existen muchísimas situaciones en que tales mecanismos son altamente útiles.
- La tecnología es relativamente transparente y desarrollado, en su mayor parte, en código abierto.
- Existen importantes economías de escala.
- Amplias posibilidades de futuro que son difíciles de predecir. Sistemas abiertos generan creatividad inusitada.

Desventajas de la cadena de bloques

- Una cadena de bloques no soluciona siempre el problema de verificación descentralizada.
- Una cadena de bloques aún tiene que suministrar incentivos a los nodos participantes en la verificación de transacciones.
- Sistemas de prueba de trabajo, sobre todo en cadenas de bloque públicas, generan "guerras armamentísticas".
- Problemas de gestión de memoria.
- Problemas de gestión de metareglas y reglas (privadas y públicas).
- No todos los problemas necesitan de una cadena de bloques o es la cadena de bloques la mejor solución a los mismos.


pets.com

Conclusiones

- La cadena de bloques es una nueva tecnología con grades posibilidades porque nos da nuevos instrumentos para afrontar un problema fundamental en la actividad económica.

- Es, probablemente, la parte más productiva del ecosistema que generó las criptomonedas (y que, en mi investigación, he argumentado no son una idea particularmente atractiva).

- Existe, sin embargo, muchísima incertidumbre sobre como terminará siendo aplicada esta tecnología.

- En particular, necesitamos de una *lex cryptographica* adecuada y de reguladores preparados.

- Problemas de gestión de metareglas y reglas.