EL BLOCKCHAIN
SISTEMAS INFORMÁTICOS (1ªeva)

ERIC MOROS PÉREZ

1º DAW (DUAL)

Contenido

Bibliografía 2

¿Qué es blockchain? 3

¿Cómo funciona la validación de blockchain? 3

¿Cómo se almacenan los datos? 5

Características/Configuraciones 7

Acceso a los datos 7

- Pública 7
- Privada 7

Permisos 7

- Activados 7
- Desactivados 7

Conclusiones 8

- Seguro 8
- Distribuido 8
- Barato 8
- Abierto 8

Bibliografía

(30 de 11 de 2017). Obtenido de web.ua.es: https://web.ua.es/en/recsi2014/documentos/papers/bitcoins-y-el-problema-de-los-generales-bizantinos.pdf

bit2me. (19 de Noviembre de 2017). Obtenido de http://blog.bit2me.com/es/

Bitcoin.org. (30 de 11 de 2017). Obtenido de https://bitcoin.org/es/faq

Blockchain.info. (30 de 11 de 2017). Obtenido de https://blockchain.info/es

Brownworth, A. (28 de 11 de 2017). *Blockchain Demo*. Obtenido de https://anders.com/blockchain/

es.wikipedia.org. (26 de 11 de 2017). Obtenido de https://es.wikipedia.org/wiki/Problema_de_los_generales_bizantinos

slideshare.net . (28 de 11 de 2017). Obtenido de https://www.slideshare.net/boolberry/boolberry-reduces-blockchain-bloat

wikipedia.org. (30 de 11 de 2017). Obtenido de https://es.wikipedia.org/wiki/Cadena_de_bloques

¿Qué es blockchain?

Como primer punto básico lo que hay que entender es que blockchain es una base de datos, solo que, a diferencia de las habituales, ha sido diseñada para ser lineal en el tiempo e inmodificable.

Una vez sabemos esto, ya se nos quita de la cabeza el que, por el hecho, de que Bitcoin usara este concepto por primera vez en 2009, esté extralimitado a almacenar las transacciones de algo "tan sencillo como una criptomoneda".

Y como segundo punto es importante destacar que es una base de datos distribuida, lo que significa que no funciona con un equipo servidor o varios con el cual se accede a los datos, funciona a base de nodos, que mantienen una copia de la base de datos, la cual se la distribuye con el fin de mejorar su seguridad, su velocidad y su estabilidad contra la perdida de datos (La cual debería ser imposible siempre y cuando quede un nodo en pie).

Blockchain es un software muy potente y difícil de entender, por eso pienso que deberían aclararse más estos conceptos. Que a mí por ejemplo, me ha llevado bastante tiempo e informarme sobre muchas fuentes.

¿Cómo funciona la validación de blockchain?

Existe un ejemplo principal al cual es habitual referirse (Probablemente porque será en el que se basaron para crear el software). El problema matemático de los generales bizantinos: En el cual se presentan varias situaciones, en las que los generales han de comunicarse entre ellos a base de mensajeros, con la intención de coordinarse para atacar o retirarse en las distintas ciudades a las cuales están atacando, pero el problema se encuentra en que entre esos generales hay un traidor y hay que descubrirlo para ponerse de acuerdo (Prefiero proponer el mío propio).
(Para leer sobre dicho problema encontrarás información siguiendo este enlace: https://es.wikipedia.org/wiki/Problema_de_los_generales_bizantinos)

Pongamos que un profesor de sistemas nos pone un trabajo, en el cual debemos de hablar sobre el tema que nos de la gana con algunas condiciones, las cuales no especifica, nos dice que nos mandará al e-mail y además que entregaremos a un profesor sustituto porque él se encontrará ausente (Este profesor es muy estricto, y el que no siga al pie de la letra las instrucciones automáticamente tendrá un 0 en la evaluación).

Al día siguiente aprovechando que el profesor sustituto tarda en venir porque hay un problema con la red del instituto, los 12 alumnos nos ponemos a comparar trabajos por aburrimiento, pero resulta que 4 de clase han hecho un trabajo de 500 palabras en lugar de 1000 como se especificaba en el e-mail, total que el resto de alumnos les comentamos sobre dicha condición, pero dicen que en su e-mail ponía que era solo de 500. ¿Quién crees que tiene razón?

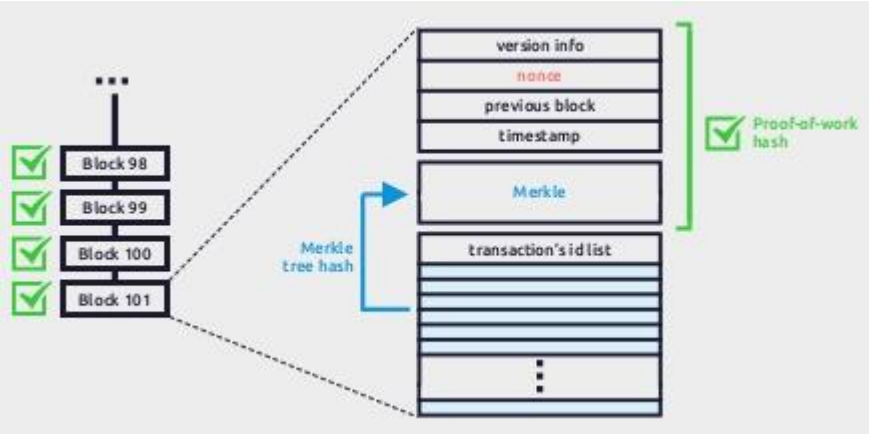
Pues siguiendo el algoritmo que usa blockchain, esos 4 alumnos se equivocan, porque el porcentaje de alumnos que están de acuerdo en que el trabajo era de 1000 palabras y no de 500 es superior al que dice lo contrario. Y por ello en nuestro caso, ellos son los traidores que pretendían hacer un trabajo más pequeño y van a tener un 0 en la evaluación.

También dejo este enlace a otro ejemplo sobre un suricato gigante volador que vi en una plaza el otro día: http://blog.bit2me.com/es/que-es-cadena-de-bloques-blockchain/

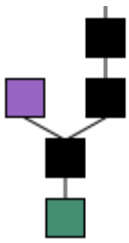
Creo que es un sistema de validación muy potente y que es muy poco probable que se pueda engañar sobre todo para sistemas en los que participen muchos usuarios.
Pero para sistemas pequeños la verdad es que no es muy práctico.

¿Cómo se almacenan los datos?

Los datos se almacenan e indexan en un árbol de Merkel. Luego [se incluyen con el resto de atributos: Versión, fecha y hora, el bloque anterior y el nonce (Que servirá para sustituir temporalmente al bloque siguiente).



Y finalmente con todo ello se genera un hash, que identificará al propio bloque] ✓.



En caso de que se pudiera modificar los datos de **un bloque,** todos los bloques hijos que se hubiesen generado quedarían invalidados y se convertirían en **bloques huérfanos** que no servirían para nada. Pero no significa que todos los datos se vallan a perder, puesto que los mineros pueden validar los datos de los bloques huérfanos y generar con ellos unos nuevos.

En este gráfico además se está representando un bloque verde queriendo destacar el **bloque matriz**: Que es el primer bloque del que parten todos los demás.

Bloques #496502

Resumen	
Número de Transacciones	2635
Total de productos	30,204.73191491 BTC
Volumen Estimado de la Transacción	2,308.63597025 BTC
Comisiones de la Transacción	1.9780184 BTC
Altura	496502 (Cadena principal)
Fecha y Hora	2017-11-28 10:52:38
Hora de Recepción	2017-11-28 10:52:38
Resuelto por	GBMiners
Dificultad	1,347,001,430,558.57
Bits	402706678
tamaño	1105.891 kB
Peso	3992.857 kWU
Versión	0x20000000
Mientras tanto	4079951441
Recompensa del Bloque	12.5 BTC

Hashes	
Hash	00000000000000000069e1740a192650b492b36ab789b26602255bfc6bb6ae66
Bloque Anterior	000000000000000005c9f45595060249e9af4b5053fc5c01c5439f56c23d9d
Bloque(s) siguiente(s)	00000000000000000007bd2c77c9a6b69903956cbbf3a486cdfccce07de687db6
Raíz de Merkle	aed2b8b1b43867580acd056d4ace9f2743e0d44944807e3e9ffb4b367b9016506

Actas

77d34563669b7e55282b65f7262a7bdcc26f4e81d2478975fabd7093f3863d7b — 2017-11-28 10:52:38

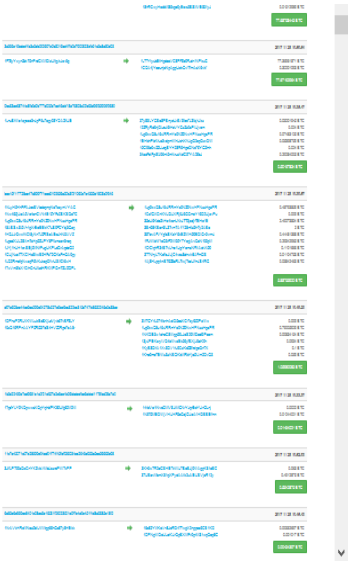
No hay entradas (monedas recién generadas) → 1J7FCFaafPRxqu4X9VsaiMZr1XMemx69GR 0.14478018 BTC
131RUhDyyjxXSbSPxGRCm3t6voei1TB6MB 14.33323822 BTC
No se puede decodificar la dirección de salida 0 BTC
14.4780184 BTC

9eb12b09a986e38a978c2a20a3da44e9cb3cf860d89f548937c3aa15a17f503 — 2017-11-28 10:51:50

1HtEnRRUHW8Vwix5EhwhQXArsz7qMr23Rk → 125DhhEWpJsic8UVKz7MimH1VMnCVuVkQM 0.731354 BTC

Este es un ejemplo del resultado de un bloque de la blockchin de bitcoin.

Presentado en la web de https://blockchain.info/es/



Muy eficiente y rápido, pero cuando se manejan cantidades ingentes de datos como muestro en las imágenes, igual no es muy conveniente realizar consultas desde clientes webs.

Características/Configuraciones

Se pueden hacer múltiples combinaciones de las capacidades de las siguientes opciones en todos los niveles.

Acceso a los datos

- Pública

  Todos los datos son explorables y todas las entidades pueden incluir información, para la cual se halla preparado la cadena de bloques.

- Privada

  Tanto la exploración como la inclusión de información está limitada a unas entidades definidas.

Permisos

- Activados

  Las entidades que crearán nuevos bloques estarán definidas además de los validadores. Con lo cual no es necesario aplicar incentivos

- Desactivados

  Cualquier entidad puede participar en la creación de la cadena de bloques y en el proceso de validación los datos. Para incentivar la participación, se aplican recompensas por dicha creación y validación. Puesto que requiere altos costes computacionales.

Muy completo y configurable, pero creo que el punto fuerte de verdad de esta tecnología es mantener los permisos desactivados y con el acceso a datos públicos, porque gracias a tener recompensas y ser transparente en cuanto a los datos, hace que incremente mucho más el poder computacional por la cantidad de gente que se une, que la que puede recabar cualquier empresa.

Conclusiones

Este nuevo sistema de base de datos es la próxima evolución que todos los sistemas van a acabar implementado, puesto que ya no hay que estar dependiendo de la confianza de un tercero y con esto me refiero a ámbitos como: Votaciones, Transacciones de cualquier tipo, servicios de comunicaciones, de almacenamiento de datos, etc…

Porque a ver… ¿A quien no le gusta que en cuanto se le acabe los Petit-suisse a la nevera se los encargue directamente a la tienda y te los traiga en un dron y con los pagos automatizados?

- ¬ Seguro

  Todos los datos encriptados y validados continuamente por redes de equipos compitiendo por ser los más potentes y llevarse las máximas recompensas por aportar el servicio.

- ¬ Distribuido

  Con una copia completa por cada nodo de la base de datos para mejorar las velocidades y la estabilidad de los datos

- ¬ Barato

  Diseñar un software que interactúe con este sistema y lanzarlo a la red.

- ¬ Abierto

  Todo el mundo puede diseñar su propio blockchain y configurarlo tanto de una forma transparente como privada

Apreciación personal sobre el tema

Es un tema para mi gusto muy complicado, debido a que es un tema del cual la información es muy dispersa y de explicaciones ambiguas, por ello hay que buscar mucha información para entenderlo con precisión.
Pero la me gusta mucho y es entretenido.