UNPSJB

LICENCIATURA EN SISTEMAS OPGCPI

ADMINISTRACIÓN DE REDES Y SEGURIDAD

Bitcoin

Qué elementos de criptografía utiliza la primer criptomoneda

Cátedra
Lic. Bruno Damián Zappellini

Integrantes:
Luciano Serruya Aloisi

12 de diciembre de 2018

Índice

1. Introducción

El presente trabajo de investigación se tratará sobre la *criptomoneda*[1] bitcoin, haciendo foco principlamente sobre los sistemas de criptografía que utiliza.

La primer parte explicará de manera amplia lo que es la criptografía, y hará hincapié en los tipos de criptografía que implementa el protocolo Bitcoin. También incluirá las funciones de *hash* que utiliza, y los algoritmos de codificación. Luego, desarrollará sobre las transacciones en Bitcoin (su ciclo de vida y cómo son validadas), siempre incluyendo los elementos de criptografía utilizados.

Por último, el trabajo explicará brevemente la red de comunicaciones en la que corre el protocolo Bitcoin -*blockchain*- y cómo es la inclusión de nuevos datos a la red.

1.1. Qué es Bitcoin

Bitcoin es la primer aplicación de la tecnología blockchain. Comenzó una revolución con la introducción de la primer moneda digital totalmente descentralizada, y demostró ser extremadamente segura y estable [1]

El *paper* titulado *Bitcoin: A Peer-to-Peer Electronic Cash System*, escrito por *Satoshi Nakamoto*, introduce la idea de un *dinero digital* que no necesita un banco intermediario para transferir pagos entre pares.

Bitcoin se puede definir de varias maneras; es un **protocolo**, es una **moneda digital**, y es una **plataforma**. Es una combinación de redes *peer-to-peer*, protocolos de comunicación, y software que facilitan la creación y uso de la moneda digital llamada bitcoin. Nótese que Bitcoin con *B* mayúscula se refiere al protocolo, mientras que bitcoin con *b* minúscula se refiere a la moneda. Los nodos en la red *peer-to-peer* se comunican utilizando el protocolo Bitcoin [1].

Una de las principales ventajas de bitcoin frente a otros proyectos para generar un dinero electrónico, es la forma en la que soluciona el **problema del doble gasto**[2].

1.2. Criptografía

La criptografía es un área de estudio que consiste de varios esquemas y técnicas para transformar un mensaje en texto plano en un mensaje cifrado; este proceso de transfor-

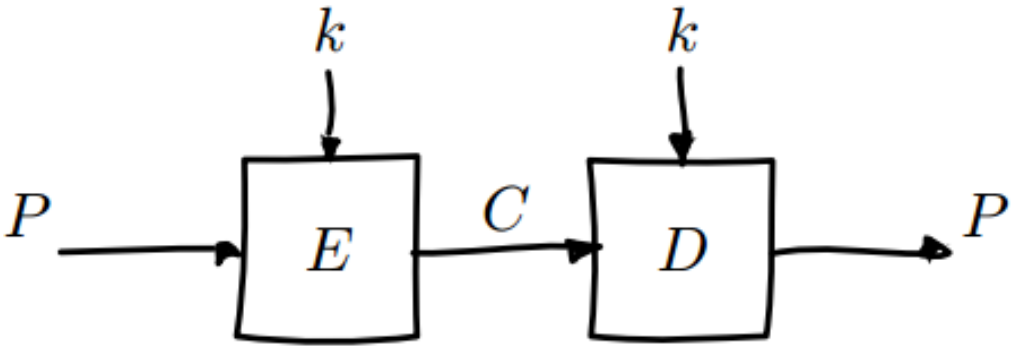
[1] Moneda digital o virtual diseñada para funcionar como medio de intercambio. Utiliza la criptografía para asegurar y verificar transacciones [2]

[2] Situación en la que se realizan dos o más transacciones con un mismo dinero

mación se conoce como **encripción**, mientras que el proceso de conseguir el mensaje original a partir del cifrado se llama **desencripción** [4]

1.2.1. Simétrica

La criptograía simétrica (o *encripción de clave secreta*) encripta un mensaje utilizando **una única llave** - la misma llave que encripta el mensaje desencripta el mensaje cifrado para obtener de nuevo el original.



Cifrado y descifrado simétrico (`P` representa el texto plano, `C` el mensaje cifrado, `E` y `D` las funciones de cifrado/descifrado respectivamente, y `k` la clave secreta) [3]

Los algoritmos de encriptación simétricos pueden trabajar con *bloques* (encriptando bloques de un mismo tamaño), o con *flujos* (encriptando flujos de datos, pueden ser flujos de 1 bit).

Este tipo de encriptación es muy performante y no incrementa el tamaño del mensaje, pero introduce una vulnerabilidad al tener que compartir la clave secreta entre las partes que se están queriendo comunicar.

1.2.2. Asimétrica

La encriptación asimétrica (o *encripción de clave pública*), a diferencia de la simétrica que utiliza una única clave, necesita de dos llaves para funcionar: una **una privada** y **una pública**.

Este sistema de encriptación se basa en que se utiliza una clave para encriptar el mensaje, y otra clave (diferente de la primera, pero relacionada) para desencriptar el mensaje. Su característica principal se trata de que se computacionalmente inviable determinar la

clave de desencripción solamente sabiendo el algoritmo de cifrado y la clave de encripción [5].

Teniendo este par de claves, se puede operar de dos modos distintos:

- Modo encripción: el emisor encripta el mensaje con la clave pública del receptor, de modo que sólo el receptor sea capaz que de desencriptar el mensaje (utilizando su clave privada)
- Modo autenticación: el emisor encripta el mensaje (o un *digesto* del mensaje) con su clave privada y los anexa al mensaje. El receptor desencripta este anexo con la clave pública del emisor, y compara el anexo desencriptado con el mensaje (o el digesto pudo generar el receptor). Si son iguales, entonces se garantiza que el mensaje fue enviado por el emisor, y que no fue alterado en el camino

Claramente este tipo de encripción genera mayor seguridad en la comunicación, debido a que las claves para desencriptar los mensajes no se deben intercambiar entre las partes previamente a comenzar la comunicación (son privadas a cada cliente y no deben ser reveladas). Sin embargo, aumentan el tamaño del mensaje y no son algoritmos tan performantes como los simétricos.

Criptografía de curva elíptica

1.3. Funciones de *hash*

1.3.1. *SHA256*

1.3.2. *RIPEMD160*

1.4. Codificaciones

1.4.1. *Base58Check*

2. Transacciones

2.1. Ciclo de vida

2.2. Verificación de una transacción

3. *Blockchain*

3.1. Estructura de un bloque

4. Minería de bloques

4.1. Prueba de trabajo

Referencias

[1] Imran Bashir. «Mastering Blockchain». En: primer edición. Packt Publishing, mar. de 2017. Cap. 4 - *Bitcoin*.

[2] Cointelegraph. *¿Qué es criptomoneda? Guía para principiantes*. URL: https://es.cointelegraph.com/bitcoin-for-beginners/what-are-cryptocurrencies#futuro-de-las-criptomonedas.

[3] Laurens Van Houtven. «Crypto 101». En: Creative Commons, 2013. Cap. 6 - *Block ciphers*.

[4] Williams Stallings. «Cryptography and Network Security». En: septima edición. Pearson, 2017. Cap. 3 - *Classical Encryption Techniques*.

[5] Williams Stallings. «Cryptography and Network Security». En: septima edición. Pearson, 2017. Cap. 9.1 - *Principles of Public-Key Cryptosystems*.