UNIVERSIDADE DA CORUÑA

Blockchain

¿Qué es blockchain?

- Tecnología (o más bien conjunto de tecnologías) que:
  - Permite que transacciones se almacenen de forma conjunta en bloques
  - Se guarden como cadenas de bloques criptológicamente seguras de forma cronológica
  - Permite el acceso distribuido a las anotaciones
- Origen ligado a la moneda digital BitCoin

¿Qué es blockchain?

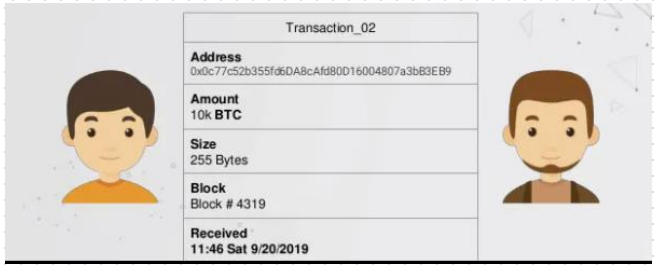
- Propiedades
  - Conjunto digital de transacciones
  - Distribuido
    - no es necesaria una autoridad central
  - Seguro
    - Es virtualmente imposible añadir, modificar o eliminar transacciones sin que sea detectado por el resto de usuarios.

¿Qué es blockchain?

Libro de contabilidad

Funcionamiento distribuido de un Libro de Contabilidad

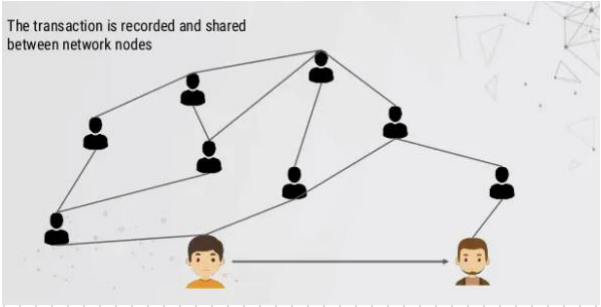
- Usuarios inician transacciones empleando sus Certificados Digitales



- Usuarios envían sus transacciones a todos los nodos de la red
- La transacción se valida y se añade a un bloque
- Nodos añaden las transacciones validadas a un bloque
- Nodos envían los bloques validados al resto de nodos
- Mineros y Protocolo de consenso
- Bloque con “true state” es encadenado al anterior bloque

Funcionamiento distribuido de un Libro de Contabilidad

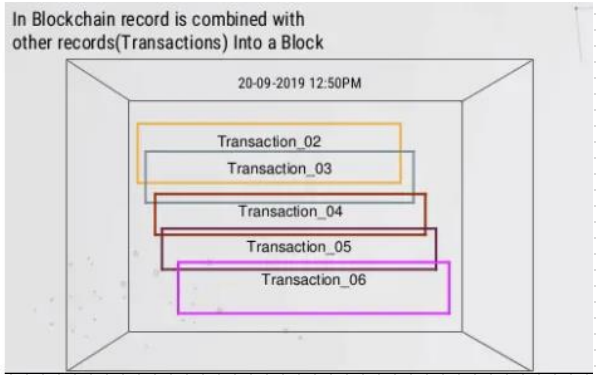
- Usuarios inician transacciones empleando sus Certificados Digitales
- Usuarios envían sus transacciones a todos los nodos de la red



- La transacción se valida y se añade a un bloque
- Nodos envían los bloques validados al resto de nodos
- Mineros y Protocolo de consenso
- Bloque con “true state” es encadenado al anterior bloque

Funcionamiento distribuido de un Libro de Contabilidad

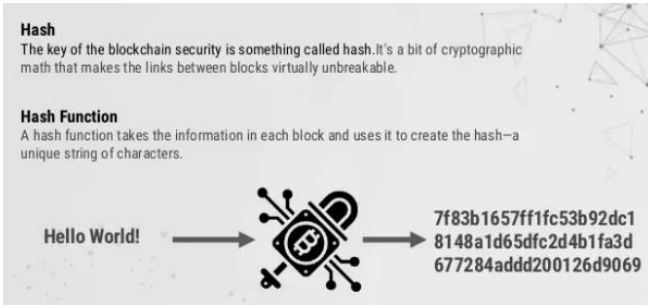
- Usuarios inician transacciones empleando sus Certificados Digitales
- Usuarios envían sus transacciones a todos los nodos de la red
- La transacción se valida y se añade a un bloque



- Nodos envían los bloques validados al resto de nodos
- Mineros y Protocolo de consenso
- Bloque con “true state” es encadenado al anterior bloque

Funcionamiento distribuido de un Libro de Contabilidad

- Usuarios inician transacciones empleando sus Certificados Digitales
- Usuarios envían sus transacciones a todos los nodos de la red
- La transacción se valida y se añade a un bloque
- Nodos envían los bloques validados al resto de nodos
- Mineros y Protocolo de consenso



- Bloque con “true state” es encadenado al anterior bloque

Aplicaciones

- Ámbito financiero: bitcoin, Ethereum…
- Garantizar Autoría
  - Firma digital. Autenticidad. No repudio
- Integridad
  - Mensajes son inmutables, inalterables e imborrables
- Sellado de tiempo
  - TimeStamp
- Históricos
  - Logs, accesos, trazabilidad
- Pruebas de autoría
  - NFT
- Smart Contracts
- …

Smart Contracts

* Contrato definido mediante software que automatiza y garantiza su cumplimiento.

* Eliminan al sistema judicial / burocrático / legal como intermediario.

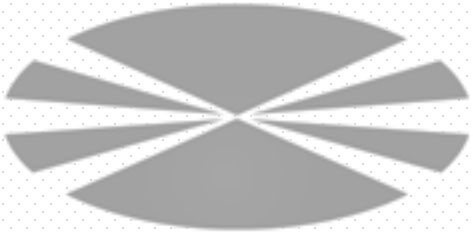
* Son almacenados en un blockchain y ejecutados por su red de nodos.

* Requieren que el dinero sea un token digital.

- ¿Costos? ¿Incentivos? ¿Arbitraje?

Principales ámbitos de uso de técnicas de cifrado dentro de blockchain

- Iniciación y broadcast de la transacción
  - Firma Digital
  - Cifrado asimétrico
- Validación de transacciones
  - Pruebas de carga (Proof of Work) - Minería
- Encadenamiento de bloques
  - Funciones hash



UNIVERSIDADE DA CORUÑA

Profesor

Marcos Gestal Pose

mgestal@udc.es

http://sabia.tic.udc.es/mgestal