Blockchain – Mucho más que criptomonedas

Una perspectiva tecnológica y taller practico

Ph.D(c) Juan David Guarnizo
Singapore University of Technology and Design (SUTD)
2020

El problema del dinero digital

Antes de Blockchain, existía el problema con el dinero digital en sistemas descentralizados, era el doble gasto o “double-spending”

El problema del dinero digital

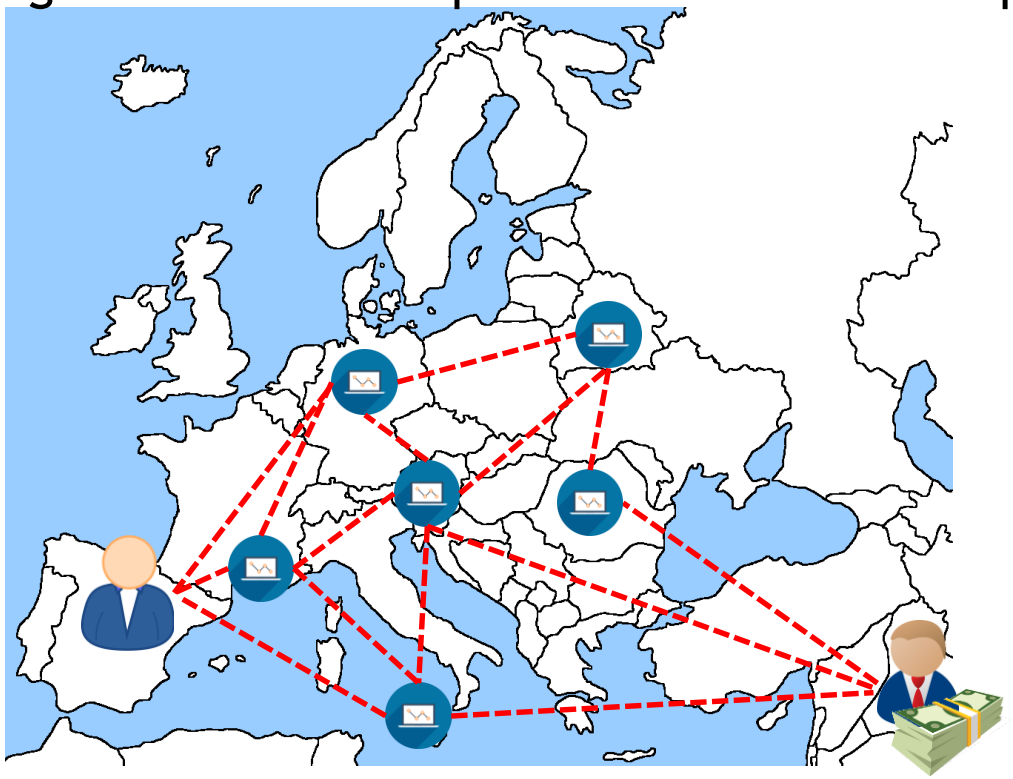
Antes de Blockchain, existía el problema con el dinero digital en sistemas descentralizados, era el doble gasto o “double-spending”

¡Una solución maligna!

Antes de Blockchain, existía el problema con el dinero digital en sistemas descentralizados, era el doble gasto o “double-spending”

El surgimiento de Bitcoin

En 2008, Bitcoin fue diseñado por Satoshi Nakamoto. Esto creo un sistema descentralizado de dinero digital resiliente al problema de “double-spending”



La punta del iceberg

Sin embargo, fue mas interesante como funciona, usando una Blockchain. Una estructura de datos con propiedades como:

- Quienquiera puede leer y escribir (permissionless)
- Distribuida
- Inmutable (Append-only)
- Auditable
- Anti censura

Puntos de interés

Blockchain es una tecnología interesante para investigación para áreas como:

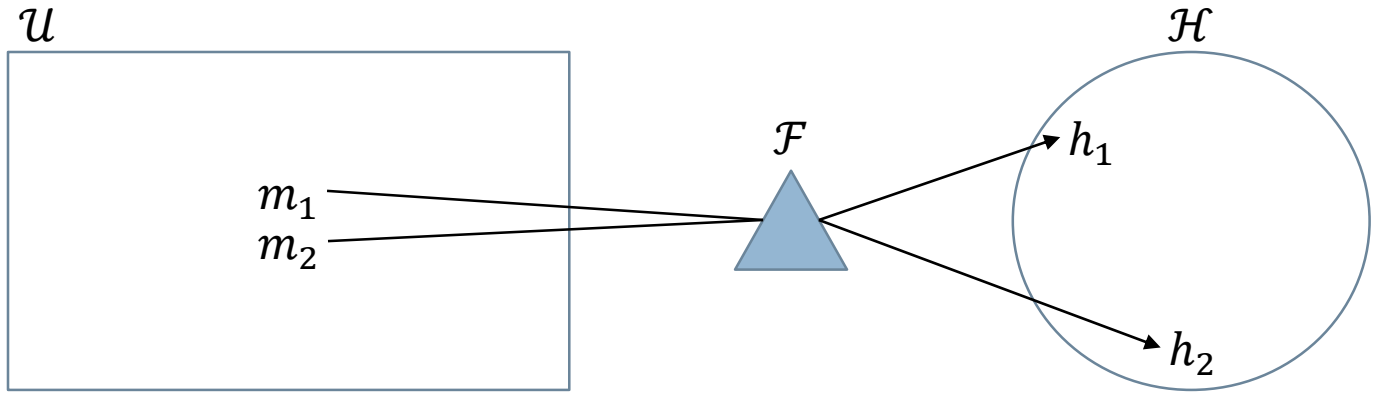
- Redes
  - Tiempos de propragación de datos
- Teoría de juegos
  - Motivar el seguir la reglas del protocolo
  - Desincentivar la trampa o acciones maliciosas
- Criptografía
  - Privacidad (Zero Knowledge Proof)
- Sistemas distribuidos
  - Protocolos de consenso
  - Selección de líder

Recapitular

- Criptografía
  - Funciones Hash
  - Cifrado de clave publica (asimétrica)
  - Firma Digital

Cripto – Funciones Hash

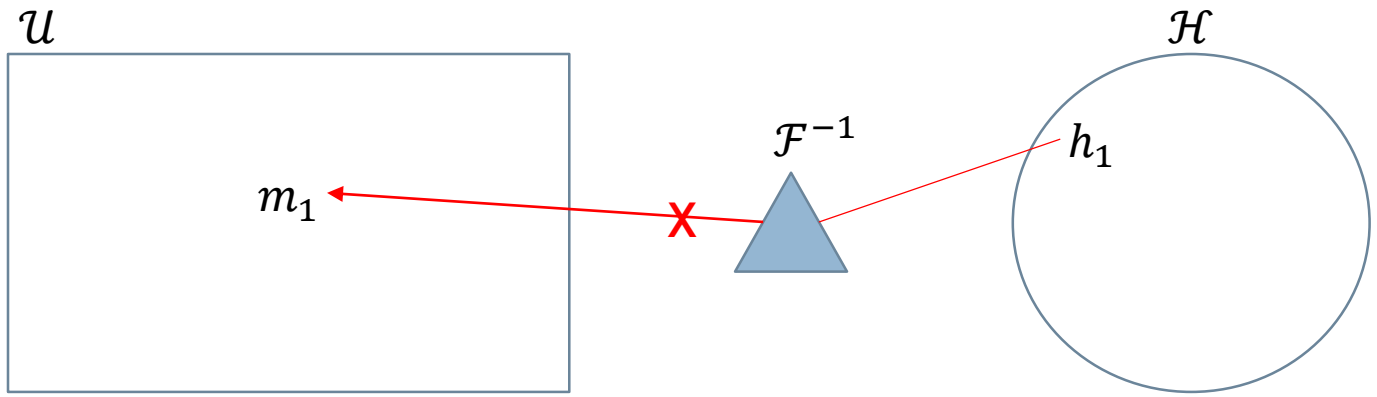
- Funciones de una sola dirección y salida de tamaño fijo
  - MD5, SHA-128, SHA-256, SHA-3, Ripemd-128
- Principalmente usadas para validar integridad de un mensaje
- Propiedades de seguridad:
  - Irreversible
  - Resistente a colisiones
  - Resistente a preimágenes



MD5(“hello”) = “8b1a9953c4611296a827abf8c47804d7”

Cripto – Funciones Hash

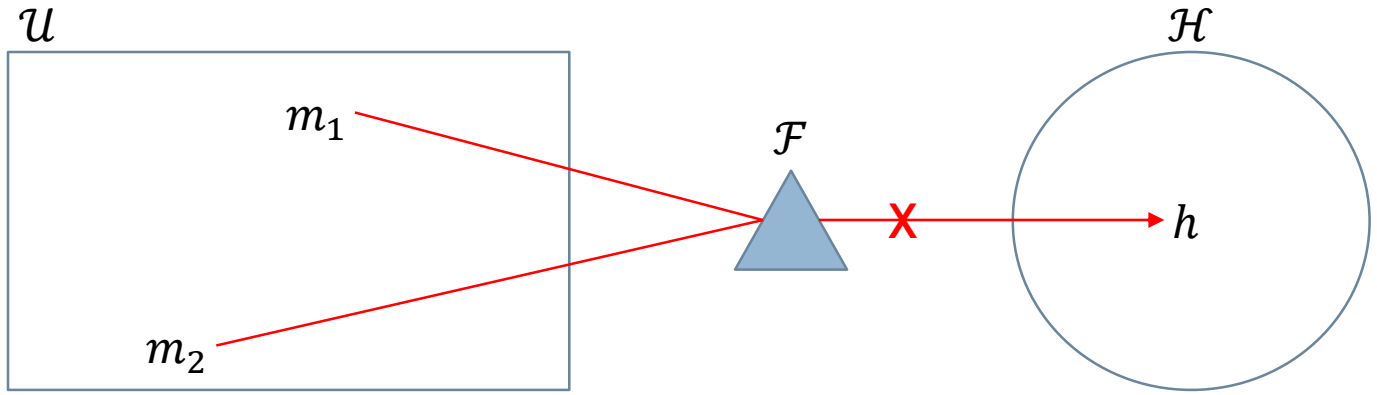
- Funciones de una sola dirección y salida de tamaño fijo
  - MD5, SHA-128, SHA-256, SHA-3
- Principalmente usadas para validar integridad de un mensaje
- Propiedades de seguridad:
  - Irreversible
  - Resistente a colisiones
  - Resistente a preimágenes



MD5(“hello”) = “8b1a9953c4611296a827abf8c47804d7”

Cripto – Funciones Hash

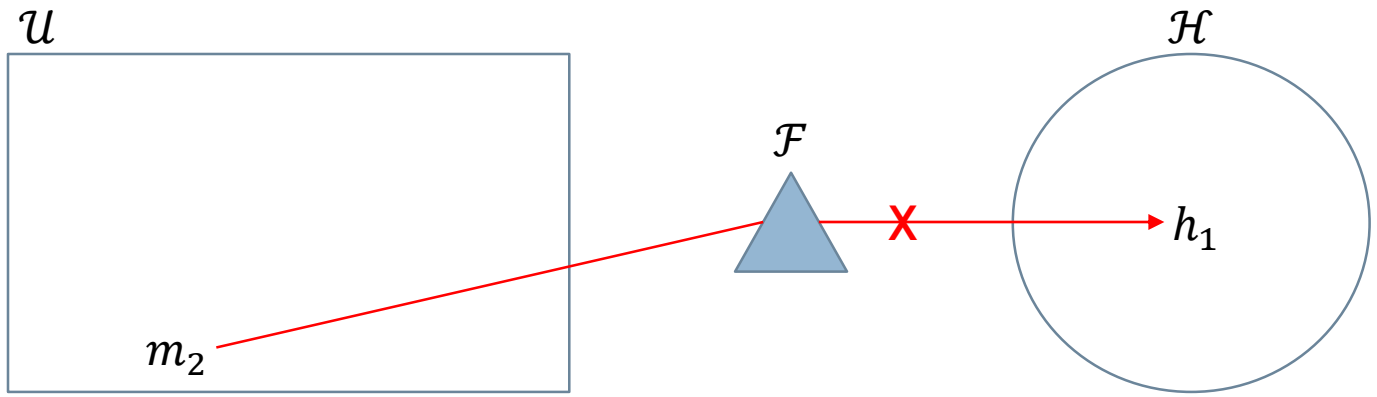
- Funciones de una sola dirección y salida de tamaño fijo
  - Ej: MD5, SHA-128, SHA-256, SHA-3
- Principalmente usadas para validar integridad de un mensaje
- Propiedades de seguridad:
  - Irreversible
  - Resistente a colisiones
  - Resistente a preimágenes



MD5(“hello”) = “8b1a9953c4611296a827abf8c47804d7”

Cripto – Funciones Hash

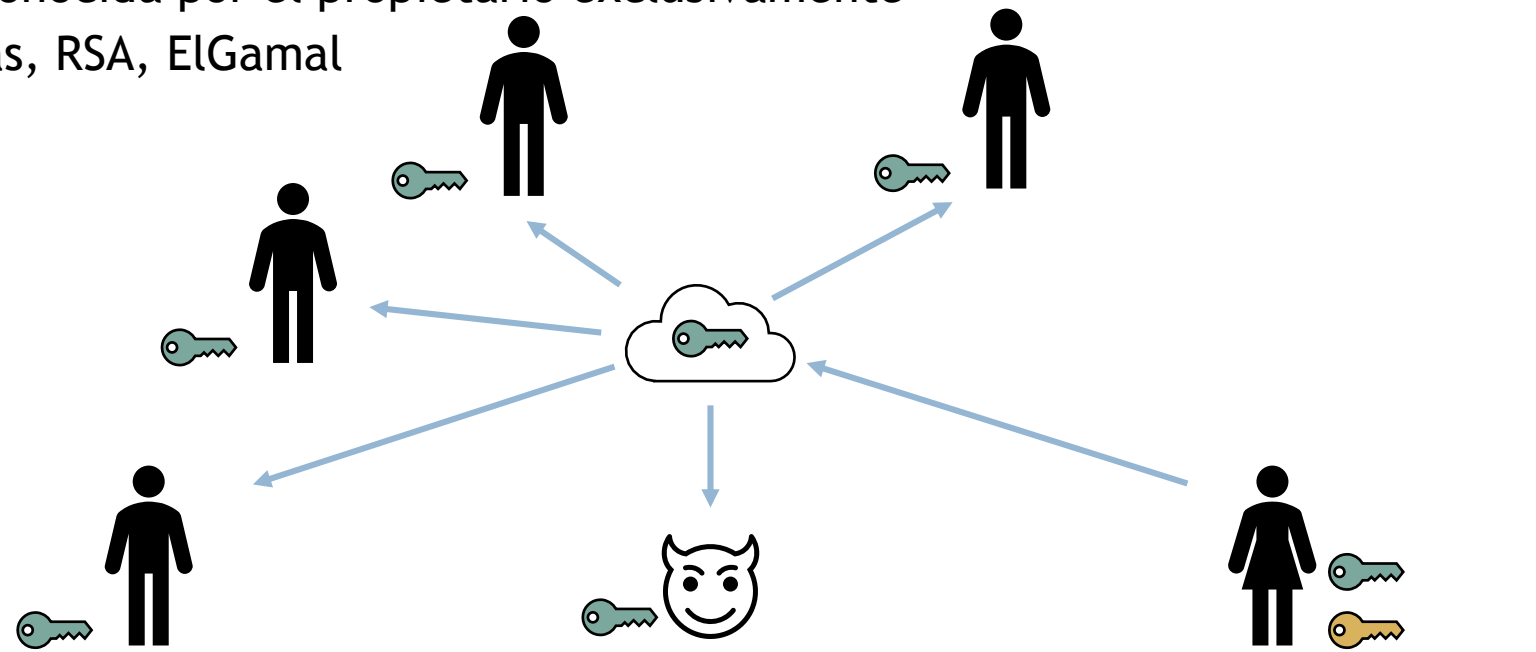
- Funciones de una sola dirección y salida de tamaño fijo
  - MD5, SHA-128, SHA-256, SHA-3
- Principalmente usadas para validar integridad de un mensaje
- Propiedades de seguridad:
  - Irreversible
  - Resistente a colisiones
  - Resistente a preimágenes



MD5(“hello”) = “8b1a9953c4611296a827abf8c47804d7”

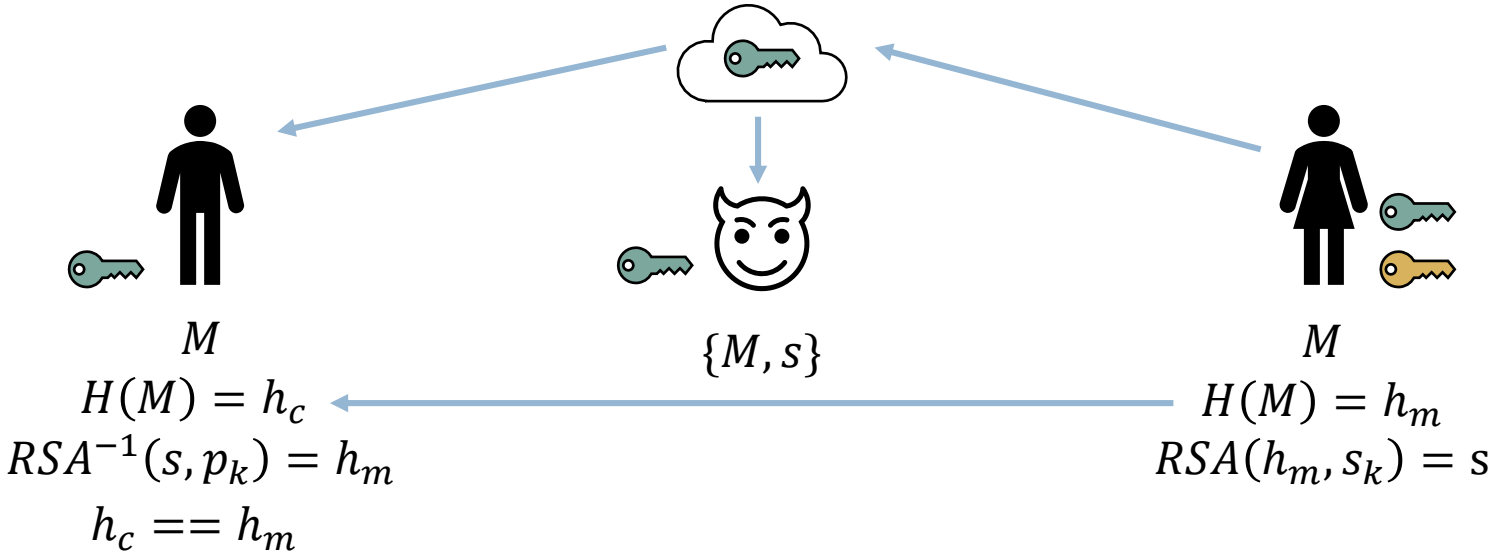
Cripto – Cifrado de clave publica (asimétrico)

- Transformación reversible de datos usando un par de llaves, publica y privada.
  - Llave publica es ampliamente difundida
  - Llave privada es conocida por el propietario exclusivamente
  - Ej: Curvas elípticas, RSA, ElGamal



Cripto – Firma Digital

- Usando la llave privada para cifrar, se hace una autenticación de los datos, pero todo aquel que tenga la llave publica podrá descifrar
  - ECDSA, EdDSA, RSA



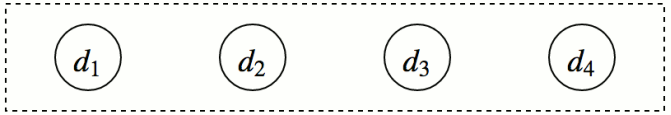
Crypto – Merkle Trees

Es un árbol binario con propiedades interesantes que permiten verificación de datos de manera eficiente. Los nodos son descritos de la siguiente manera:

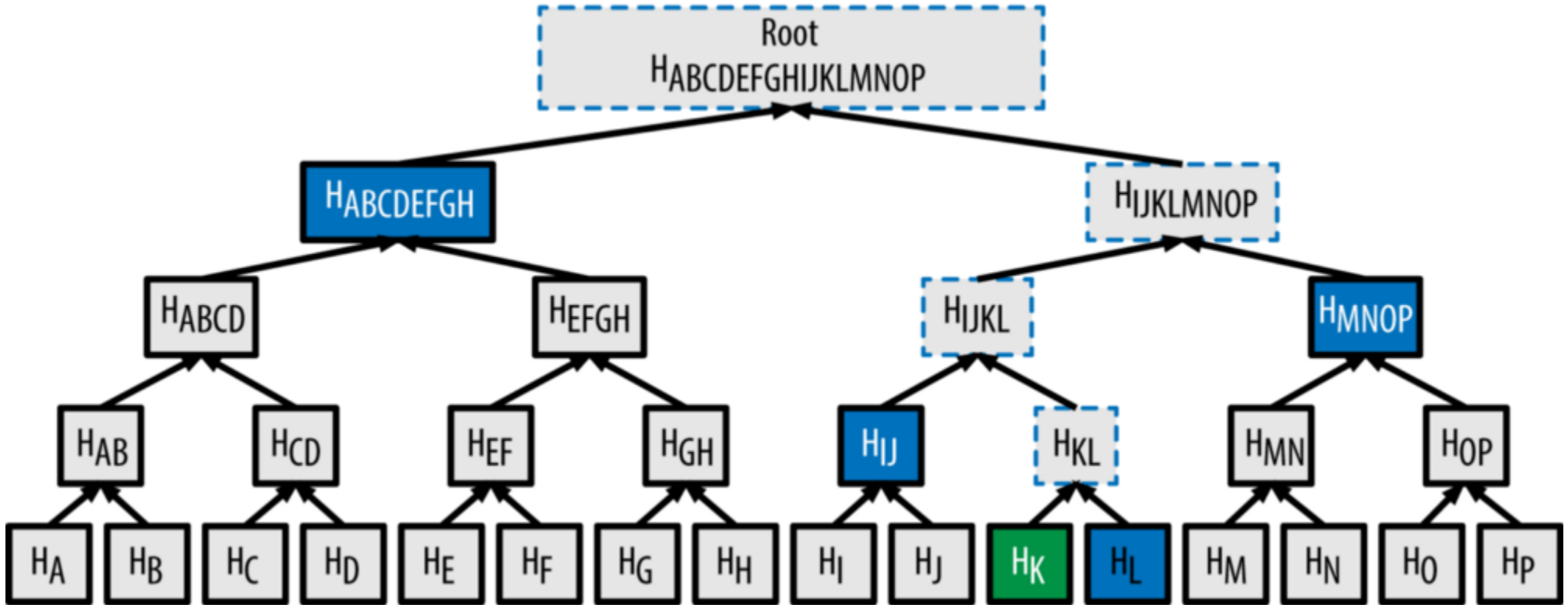
- Las hojas con el *hash* de cada correspondiente dato
- Nodos en el medio con el *hash* de los hijos

$$h_{12} = H(h_1 || h_2)$$

El *root* se convierte en un valor de integridad agregada de todos los datos contenidos en el árbol.

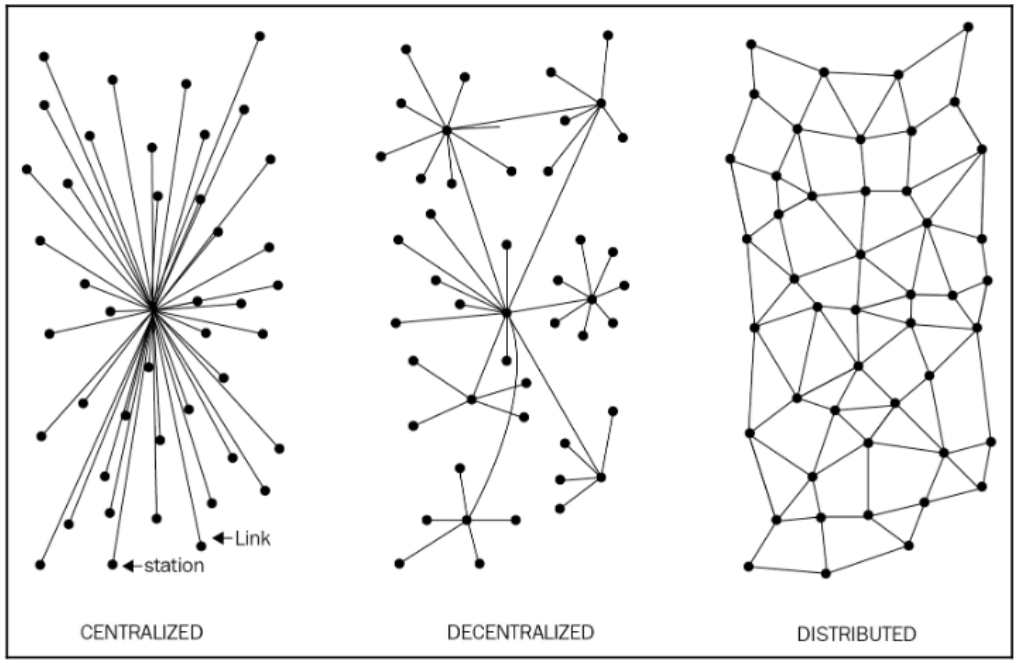


Crypto – Merkle Trees



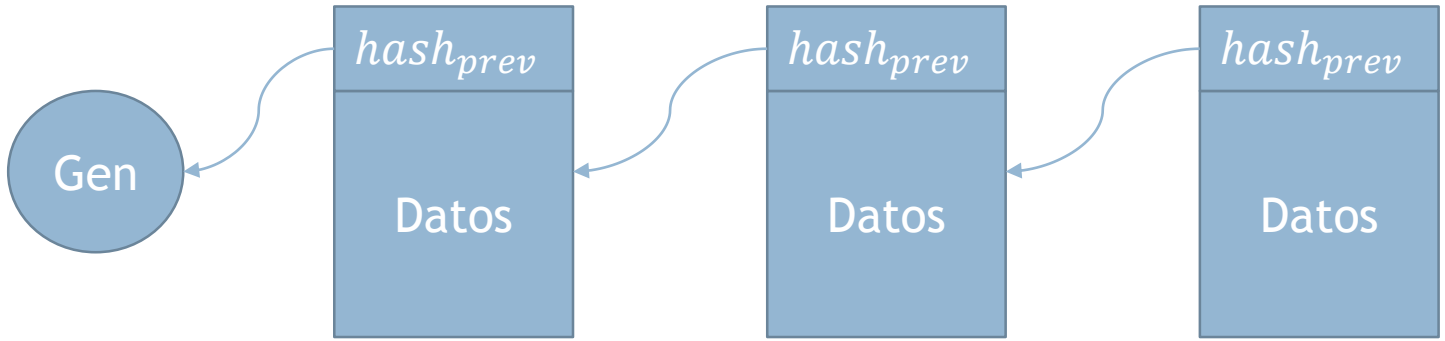
Blockchain – Publica y Distribuida

Es un libro contable (ledger) distribuido en todos los nodos quienes tienen una copia completa, por tanto todos saben el estado general de las cuentas. Ningún nodo es confiable (trusted), todos tienen el “mismo nivel de autoridad”.



Blockchain – Cadena de Bloques

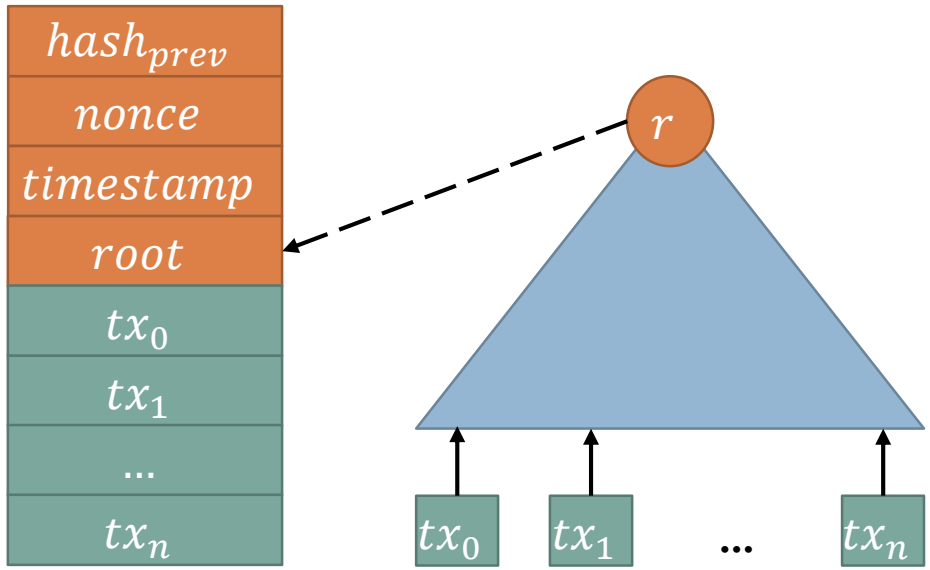
El libro contable crece en unidades llamadas “bloques”. Cada uno apunta a un bloque anterior y contiene datos específicos de cada Blockchain; por ejemplo: transacciones



Blockchain – Bloque

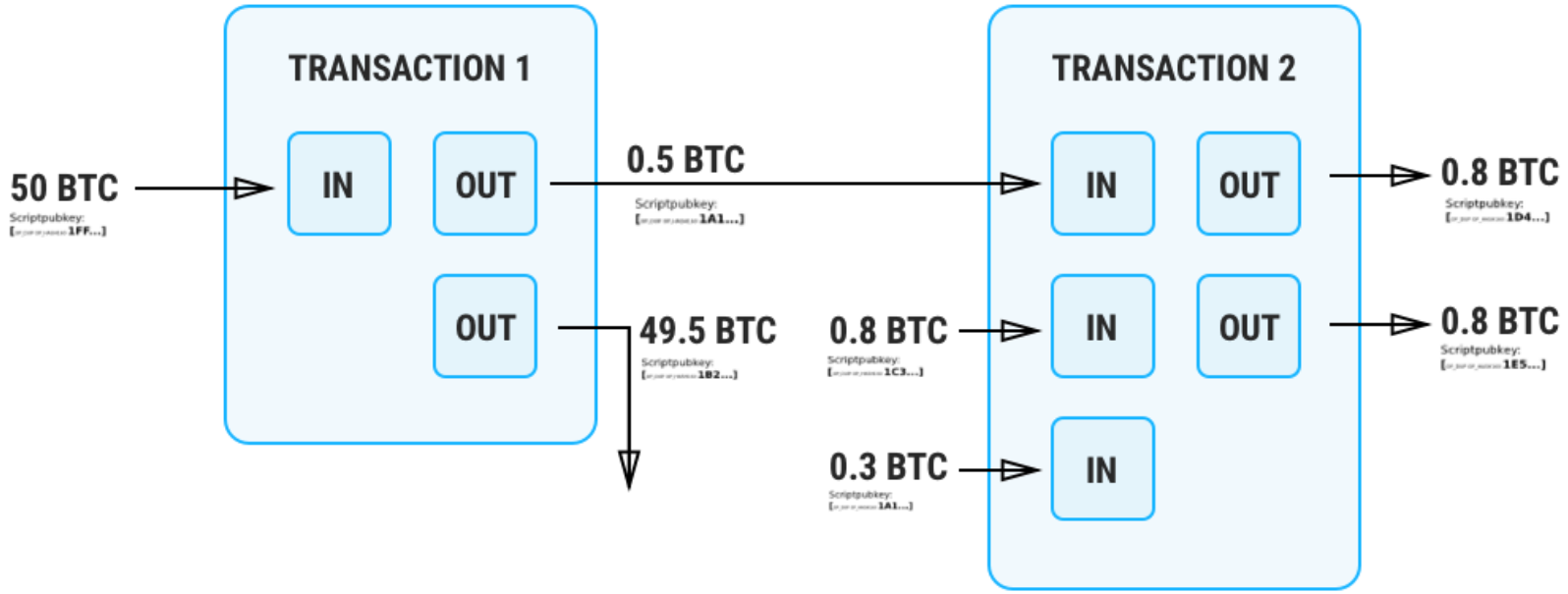
Cada bloque se divide en dos partes: Cabecera (Header) y el cuerpo (Body).

- tx_0 es una transición espacial (coinbase)
- $nonce$ es usado para el consenso



Blockchain – transacciones

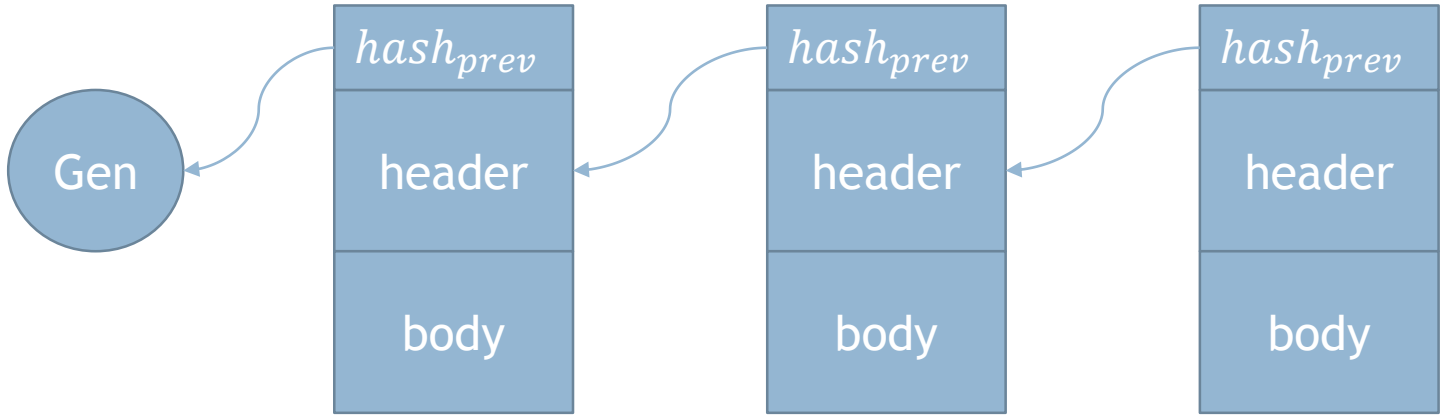
Bitcoin se basa en un modelo de transacciones sin usar, también conocida como Unspent Transaction Output (UTXO)



Blockchain – Cadena de bloques

El libro contable crece en unidades llamadas “bloques”. Cada uno apunta a un bloque anterior y contiene datos específicos de cada Blockchain; por ejemplo: transacciones. Sin embargo:

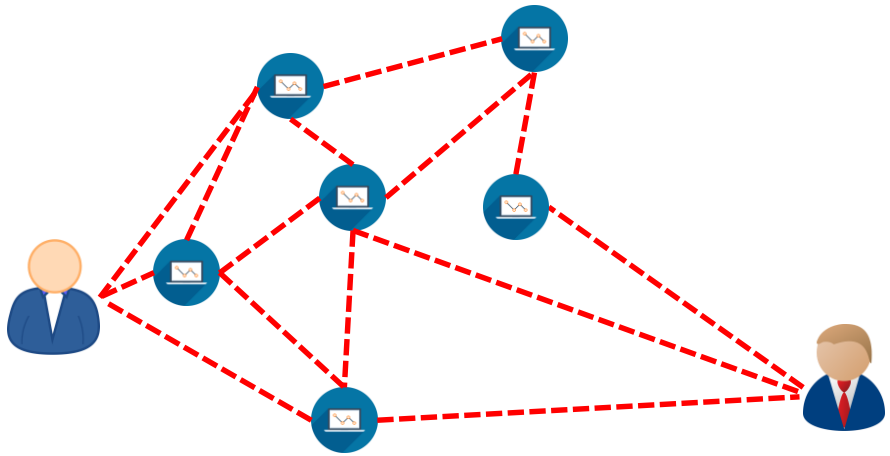
- ¿Quién puede escribir? ¿Cómo? (todos pueden leer)
- ¿Qué pasa si hay algún nodo malicioso?



Blockchain – Consenso

Objetivo:

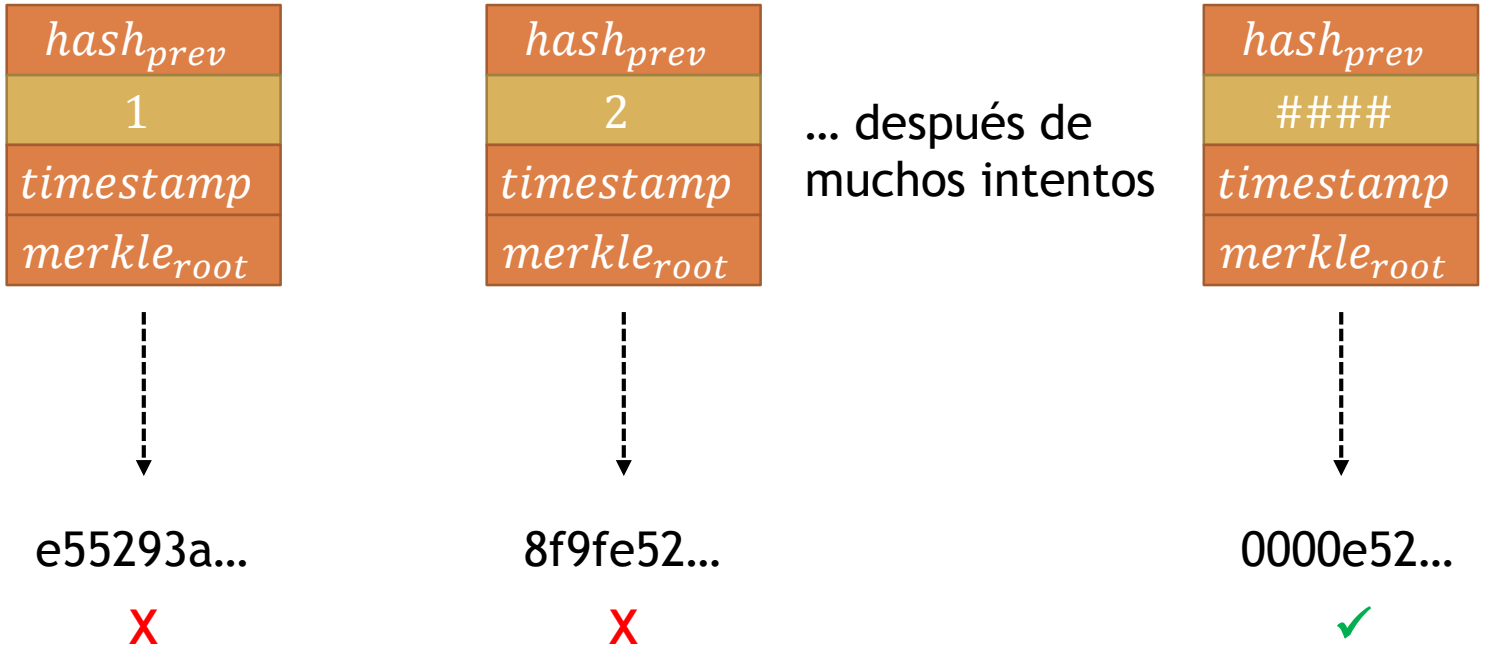
- Mantener la seguridad e integridad de la Blockchain entre N nodos, e incluso algunos pueden fallar (desconectarse) o ser maliciosos.
- Un líder es elegido aleatoriamente, cualquier nodo es elegible
- Líder propone un bloque nuevo
- Otros nodos verifican que se cumplan las reglas
  - Bloque previo
  - Transacciones correctas
  - Merkle tree root
  - Otros



Consenso – Proof of Work (PoW)

- Nodos son llamados mineros, y uno tiene cierto poder de decisión (voting) relacionado a capacidad de computo
- Derecho de proponer un bloque nuevo b_{i+1} solo cuando: el valor hash del bloque tiene cierto numero de ceros (0) al inicio (dificultad)
- Solo en campo $nonce$ es modificable por el minero para encontrar el hash deseado (fuerza bruta)
- Todos los nodos compiten porque hay un premio por bloque (motivación)

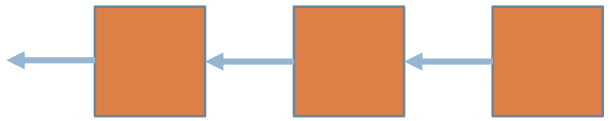
Consenso – Proof of Work (PoW)

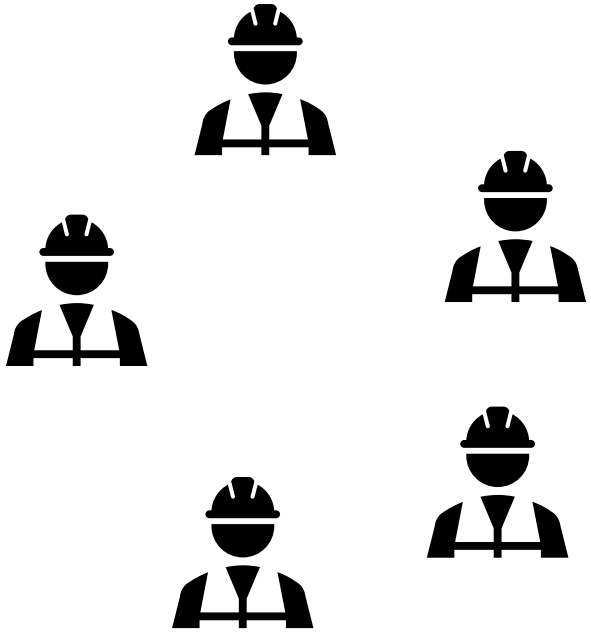


Blockchain – Bitcoin

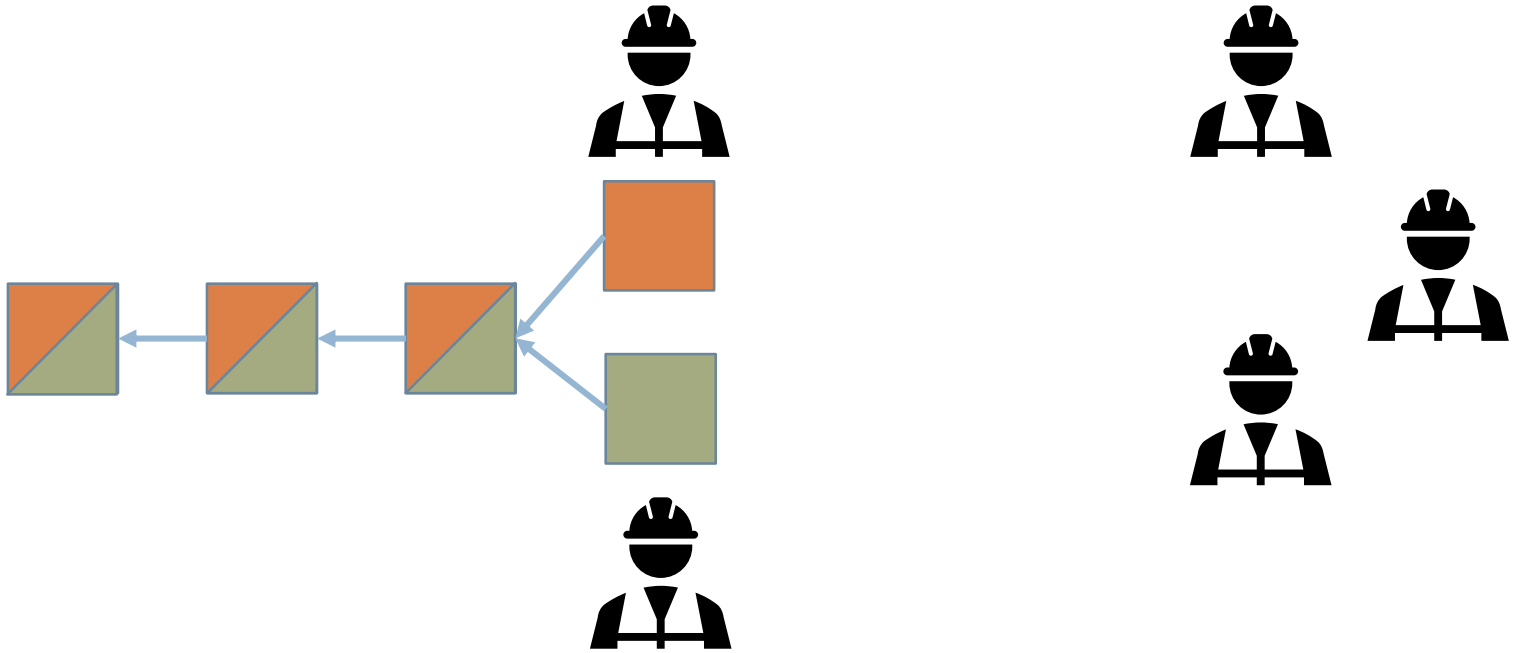
- Bloque tiene un tamaño máximo de 1 MB
- Se genera un bloque cada 10 minutos
  - La dificulta se adapta cuando aumenta el poder de computo de los nodos
  - ACID = 1 TH/s, GPU = 1 GH/s, CPU = 6 KH/s
- PoW consume mucha energía
  - En 2018, se consumió 73 TW/h (similar a lo que consume toda Austria)
- Seguro y Robusto
  - Mineros honestos son premiados (comisión por transacción + comisión por bloque)
  - Mínimo 6.4 BTC = COP $371M cada 10 minutos
  - Extremadamente costoso ser malicioso, COP $2 Mil Millones

Blockchain – Forks

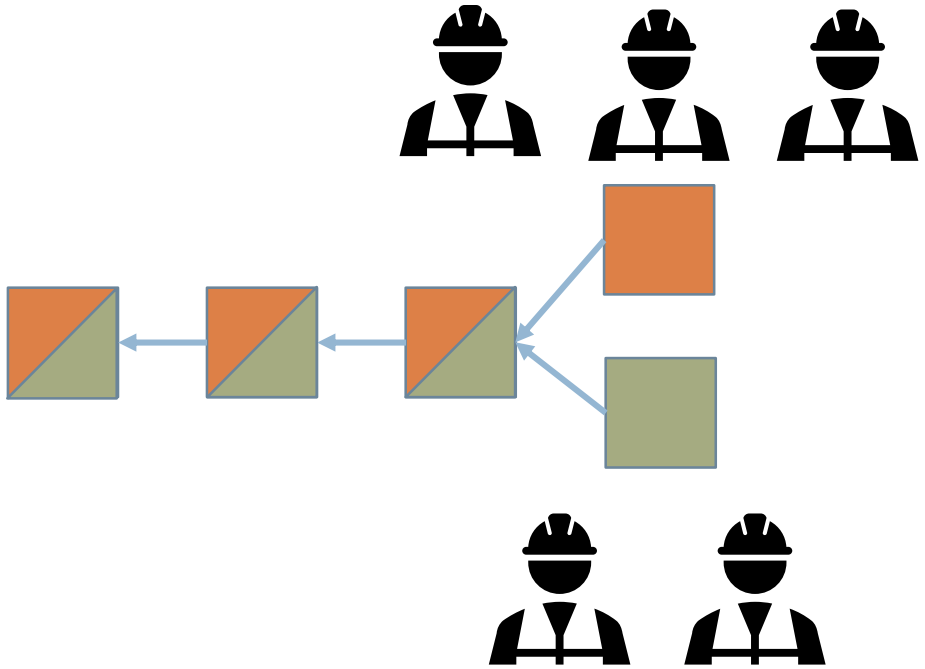




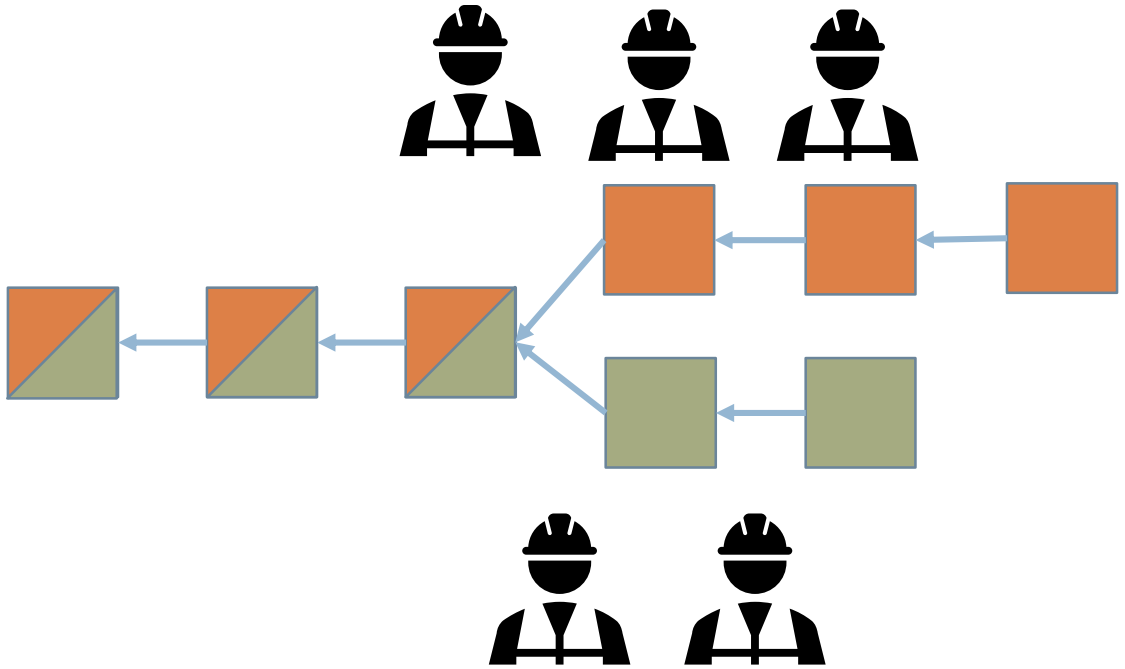
Blockchain – Forks



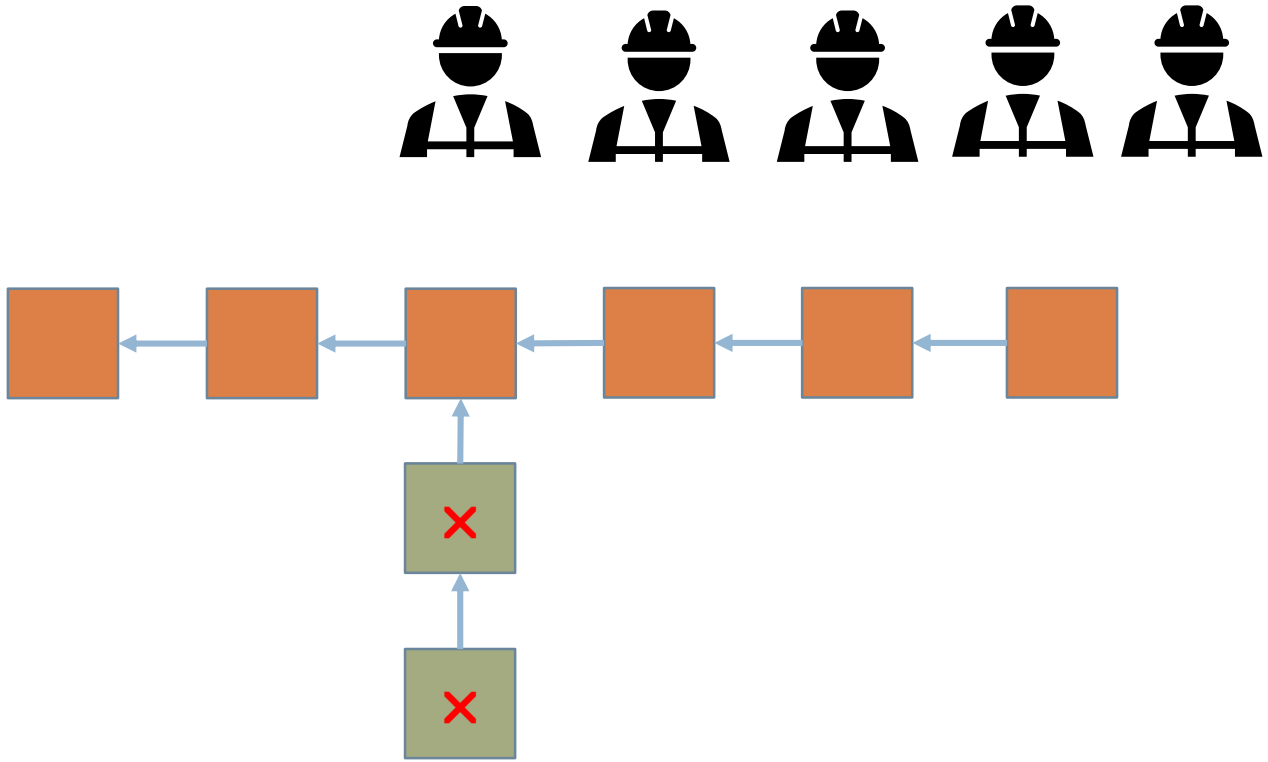
Blockchain – Forks



Blockchain – Forks



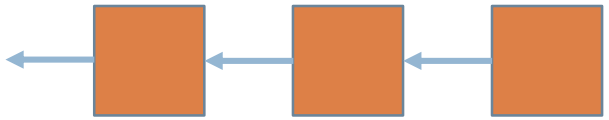
Blockchain – Forks

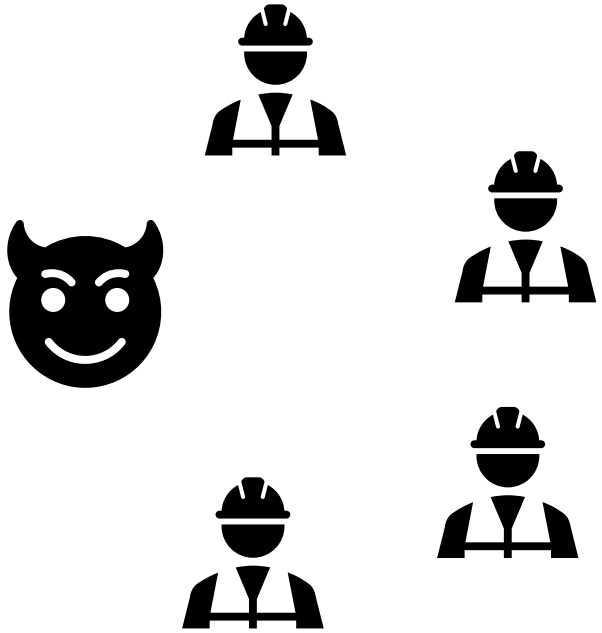


Blockchain – Vulnerabilidades

Blockchain basadas en PoW no son totalmente libre de ataques. Los mas conocidos son:

- 51% Attack
- Eclipse
- Sybil Attacks

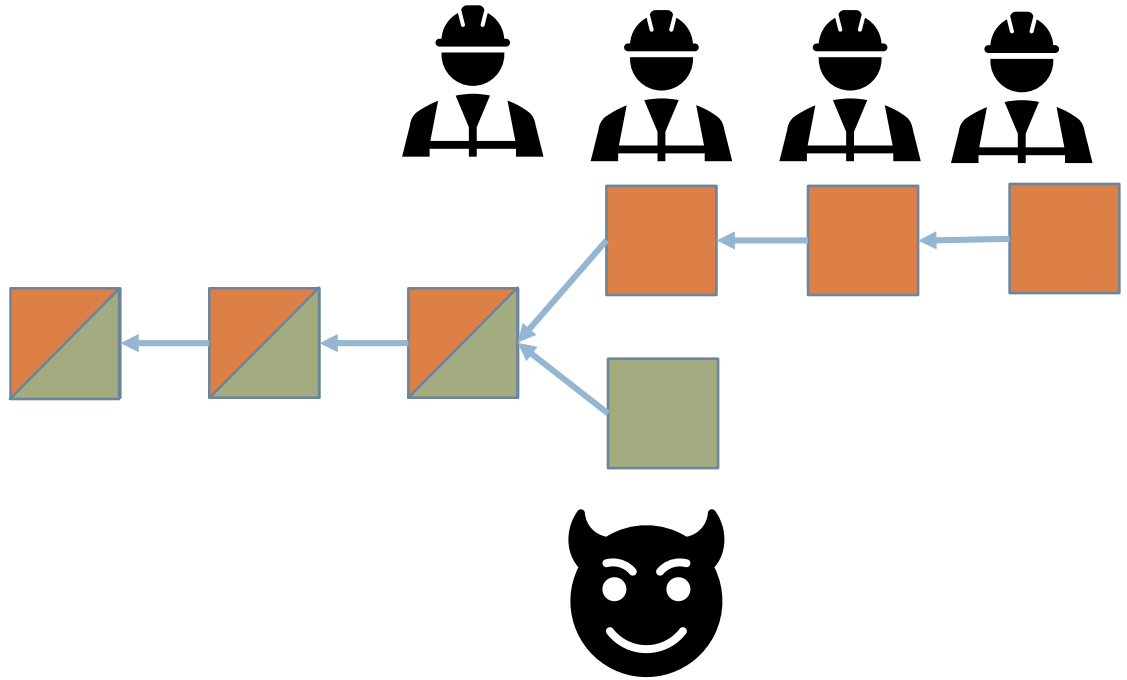




Blockchain – Vulnerabilidades

Blockchain basadas en PoW no son totalmente libre de ataques. Los mas conocidos son:

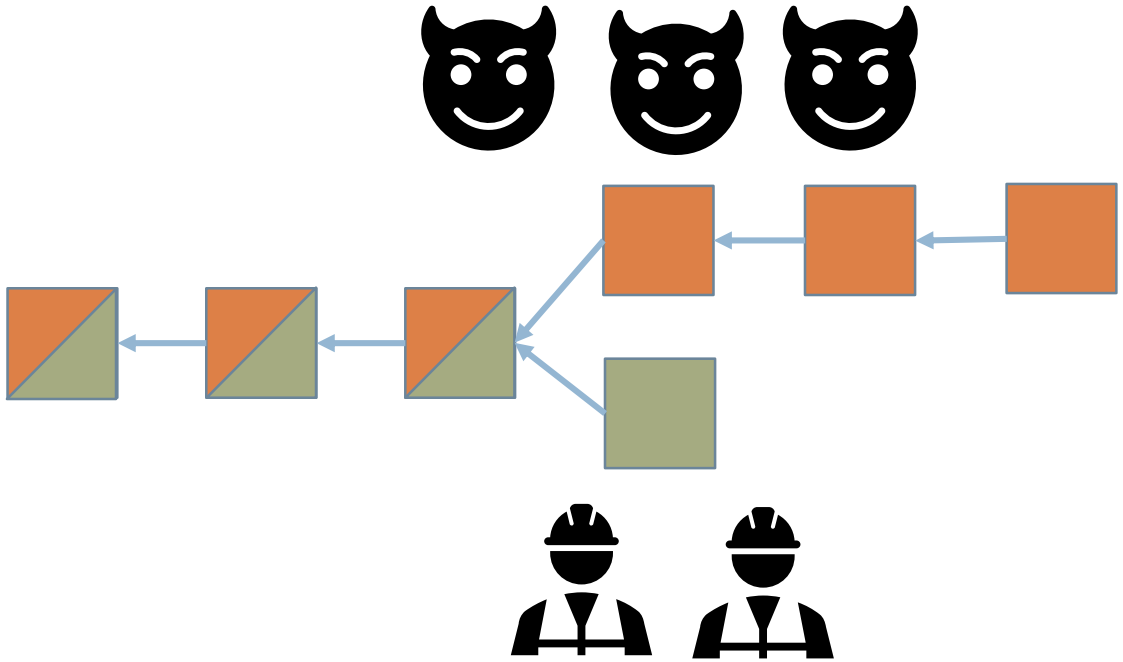
- 51% Attack
- Eclipse
- Sybil Attacks



Blockchain – Vulnerabilidades

Blockchain basadas en PoW no son totalmente libre de ataques. Los mas conocidos son:

- 51% Attack
- Eclipse
- Sybil Attacks



La Revolution Blockchain

Desde Bitcoin, muchas mas blockchain y criptomonedas han surgido con diferente características y/o solucionando problemas de Bitcoin. Hasta el momento las mas populares son:

- v1.0 – Bitcoin (2008) – transacciones end-to-end.
- v2.0 – Ethereum (2015) – Asegurar transacciones usando **Smart Contracts**
- v3.0 – pronto?
  - Privacidad
  - Seguridad de Smart Contracts
  - Escalabilidad
  - Amigable con el medio ambiente
  - Precios estables
  - IoT
  - …

Proyectos Interesantes

- Registros de propiedad e identificación
- Economías del Internet de las Cosas (IoT)
- Voto electrónico
- Cadenas de distribución
- Originalidad (antifalsificación)
  - Medicinas
- Juegos
  - cryto-kitties
- Acciones transparentes
  - Gobierno
  - Entidades Certificadoras
  - Distribución de Software