HACK & BEERS CUENCA VOL.IV

HACK &BEERS

SOPHOS

LOS CLASICOS

TORMO
CERVEZA ARTESANAL
CUENCA


Ay hooooo, Ay hooooo,
A la Web a
Minar!!!
HACK
&BEERS

¿Quién soy?

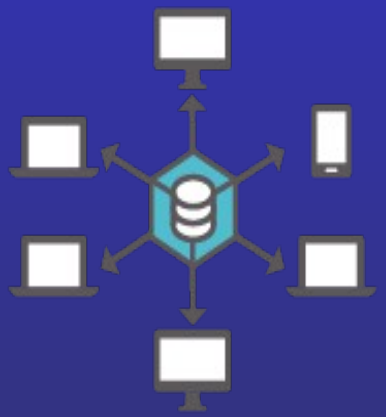
- Mariano Rodríguez (@marianelas)
- Graduado Ingenieria Sistemas Audiovisuales y de Telecomuniaciones en la UCLM
- Rookie Morteruelo'16
- Desarrollador Novel Blockchain y Cryptomonedas
- Profesor de Matemáticas, Física y Qímica

Índice

- App's o Dapp's
  - Blockchain
  - Creacion de Bloques
  - Actualizaciones
  - Ventajas y desventajas
- Ataques comunes(exitosos?)
  - Sybil Attack
  - Routing Attack
  - DdoS
  - 51% Mayority Attack
- Blockchain Ethereum
  - Smart Contracts
  - PoW & PoS
- Minado de Bloques
  - Que son los mineros
  - Scripts de mineros
  - Cryptojacking

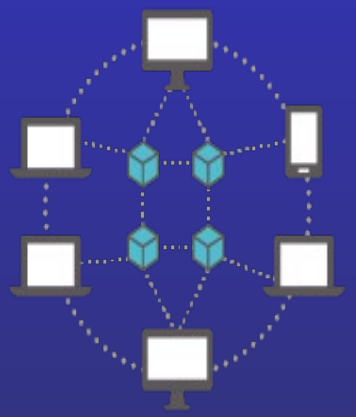
App's Or DApp's

- Centralizadas
  - Servidores de datos
  - Terminales
  - App's



TRADITIONAL APP

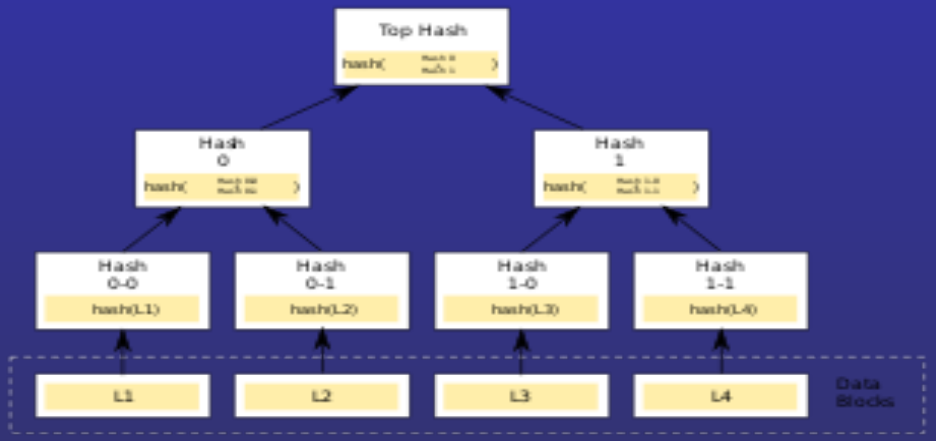
- Descentralizadas
  - Blockchain
  - Terminales
  - App's



DECENTRALIZED APP

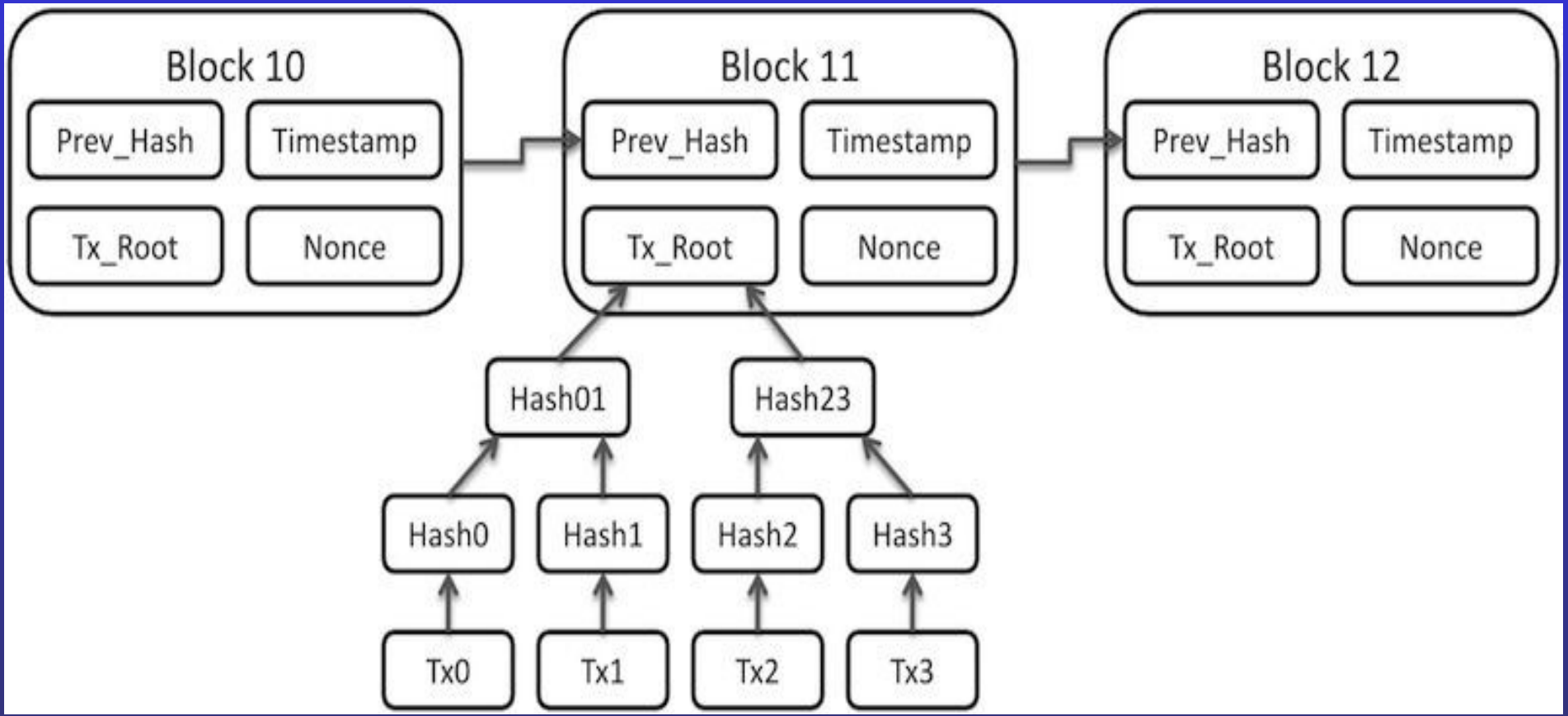
Blockchain

- Las 3 tecnologías en las que se basa Blockchain:
  - Red Peer-to-Peer
  - Cryptografía Asimétrica
  - Hash Cryptográfico (árbol de Merkle)



- Nodos de datos(libros de Cuentas)
- Nodos mineros
- Transacciones (datos)
- Estructura agrupada en bloques
- Se añade metadatos del bloque anterior en línea temporal
- Entorno distribuido

Cómo se crean los Bloques



Bloques #551286

Resumen	
Número de Transacciones	1657
Total de salida	346.72292262 BTC
Volumen Estimado de la Transacción	49.00886317 BTC
Comisiones de la Transacción	0.02859453 BTC
Altura	551286 (Cadena principal)
Fecha y Hora	2018-11-24 06:46:48
Hora de Recepción	2018-11-24 06:46:48
Resuelto por	AntPool
Dificultad	6,653,303,141,405.96
Bits	388648495
tamaño	931.766 kB
Peso	3602.039 kWU
Versión	0x20000000
Mientras tanto	2549849305
Recompensa del Bloque	12.5 BTC

Hashes	
Hash	00000000000000000006b63332e316f8dfa07115d5bb6724bcab1077e8385bb3
Bloque Anterior	00000000000000000163dce6314cc9675072e44f2ad97d9163375b2eaa7730f
Bloque(s) siguiente(s)	
Raíz de Merkle	3bed212eae951d15294613335c92581050055162a3087974b5a8a5c9fed46ef2

6e4bf60a5cc2165d728fb81eec09cbf53bdb3d4f8fb0dd44bf9b835217d0ad3f **(Tamaño: 209 bytes) 2018-11-24 06:46:48**

Sin Entradas (Monedas Recién Generadas)	1Nh7uHdvY6fNwtQtM1G5EZAFPLC33B59rB - (No gastado)	12.52859453 BTC
	No se puede decodificar la dirección de salida - (No gastado)	0 BTC
		12.52859453 BTC

2211b42fb70f024e6cb6283f458d7e476f60d3aee72445fd10cc4c13aa16004d **(Cuota: 0.00206974 BTC - 63.26 sat/WU - 253.02 sat/B - Tamaño: 818 bytes) 2018-11-24 06:46:00**

1EqHjmswNyCEkgUTX9TFmGSnG2EpuwBUsA (0.0008483 BTC - Salida)	1GcoD4nd7Zwxqy2YgY4LYmHRSddZtS12CD - (Gastado)	0.001 BTC
1EjZe84jsoztKuQveTReNWKYv6Lb8xBZ5W (0.0008483 BTC - Salida)	1CXACoQhqaZWgU3uMvBejHKb8QAnTgY685 - (No gastado)	0.01035449 BTC
17qJWw4sZmLN1ymG7cerMyhRbwC9NwXpQH (0.00084773 BTC - Salida)		
17BcCrhHaS3tfhbNa934EqUNsvbt9rdx1v (0.00084773 BTC - Salida)		
1NCJazhWkD8eoheyAcrYHBWJDNjxvJ4j5y (0.01003217 BTC - Salida)		
		0.01135449 BTC

1b8bd59ecabd06c4dd0cf85d24f78dff5b2c242f513a2264b7dc8a0a945e7313 **(Cuota: 0.00075174 BTC - 50.52 sat/WU - 202.08 sat/B - Tamaño: 372 bytes) 2018-11-24 06:46:01**

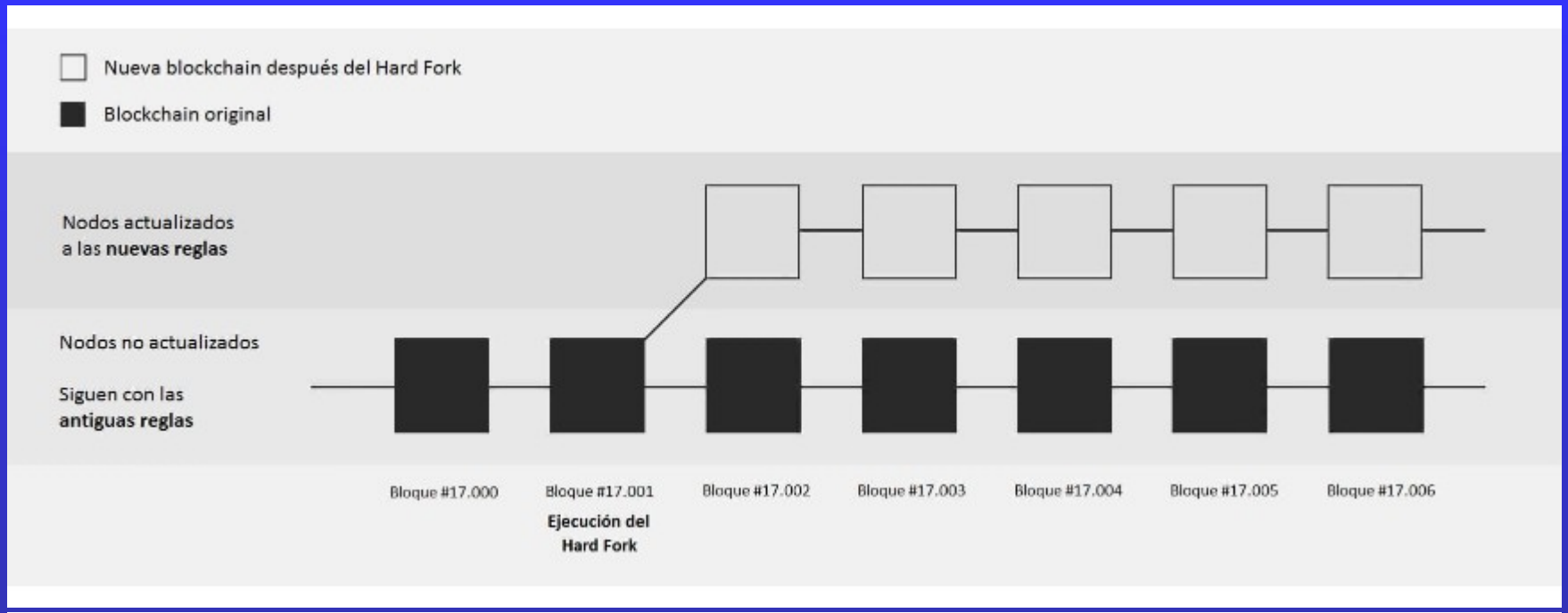
1MEYE4tpv7Wf47ewTB4zojsxAJwc7Q743x (0.003116 BTC - Salida)	1356EM1VeVCnX2zmXAuNYdVN2fFJCiHiJm - (No gastado)	0.0088 BTC
1N8PWHdqWq1PaCHkEpkKPmZPiGmf4JpGSN (0.015684 BTC - Salida)	1NMSmPaeSZnPMftiTrkzTsxGooJaSWRsda - (No gastado)	0.00924826 BTC
		0.01804826 BTC

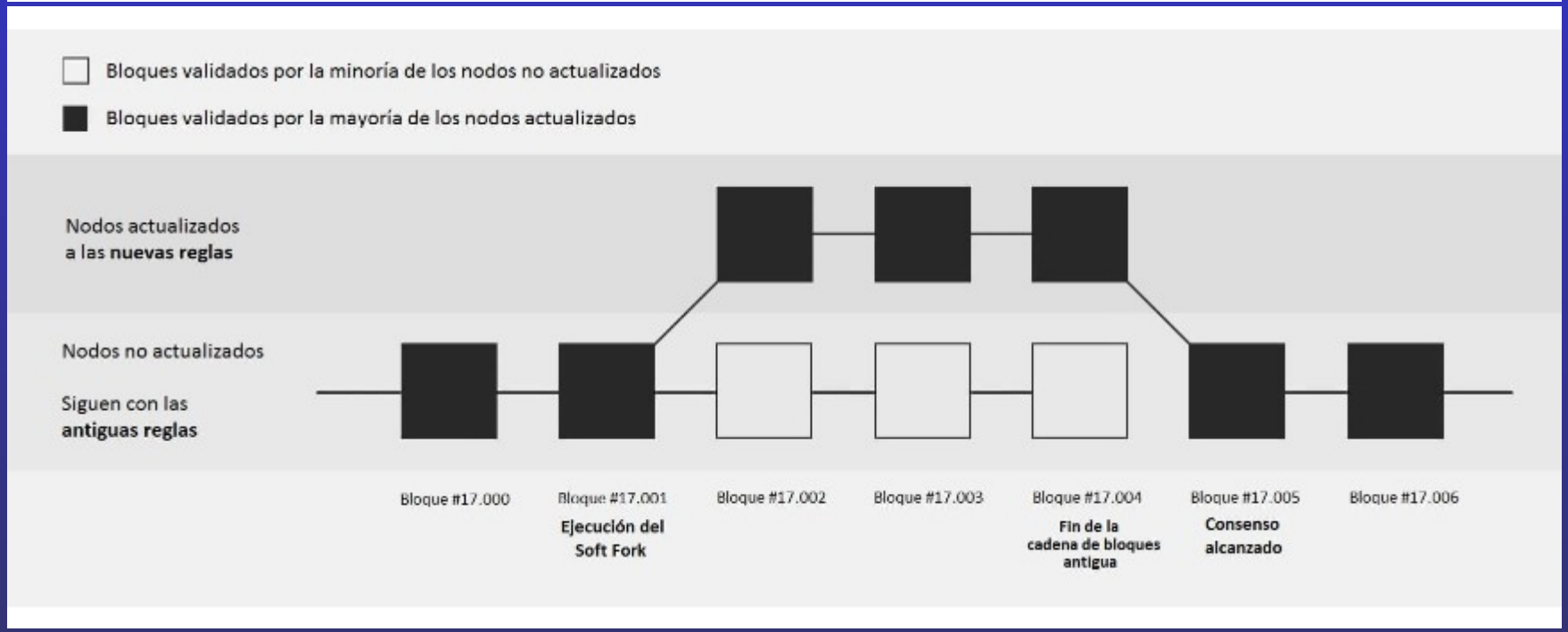
f1101a085bb9abbddd878a8f778383fbd90d4246dbe8eef56e63e3be5a80332b **(Cuota: 0.00075174 BTC - 50.52 sat/WU - 202.08 sat/B - Tamaño: 372 bytes) 2018-11-24 06:46:00**

112XCLjTqVw4wrQwHsJtFQp5nfTyNzLxHd (0.18 BTC - Salida)	15jKibUaUFYa2xsXfrRViwQxNLiwHs84Cd - (No gastado)	0.01022921 BTC
1EzjJHDZTcbX7vBGCZzXejMLuKKUEwLYa8 (0.0034876 BTC - Salida)	17ToUZjFkDyZqcqYpLu1L7sQgC7HLxxAHD - (No gastado)	0.17250665 BTC
		0.18273586 BTC

Actualizacion de la Blockchain

- Hard Fork
  - Bifurcación Dura
  - Definitiva
  - Cambia los protocolos de la blockchain
  - El caso DAO
- Soft Fork
  - Bifurcación Suave
  - Temporal
  - Permite nodos sin actualizar


Nueva blockchain después del Hard Fork
Blockchain original
Nodos actualizados a las nuevas reglas
Nodos no actualizados
Siguen con las antiguas reglas
Bloque #17.000
Bloque #17.001
Ejecución del Hard Fork
Bloque #17.002
Bloque #17.003
Bloque #17.004
Bloque #17.005
Bloque #17.006


Bloques validados por la minoría de los nodos no actualizados
Bloques validados por la mayoría de los nodos actualizados
Nodos actualizados a las nuevas reglas
Nodos no actualizados
Siguen con las antiguas reglas
Bloque #17.000
Bloque #17.001
Ejecución del Soft Fork
Bloque #17.002
Bloque #17.003
Bloque #17.004
Fin de la cadena de bloques antigua
Bloque #17.005
Consenso alcanzado
Bloque #17.006

HACK &BEERS

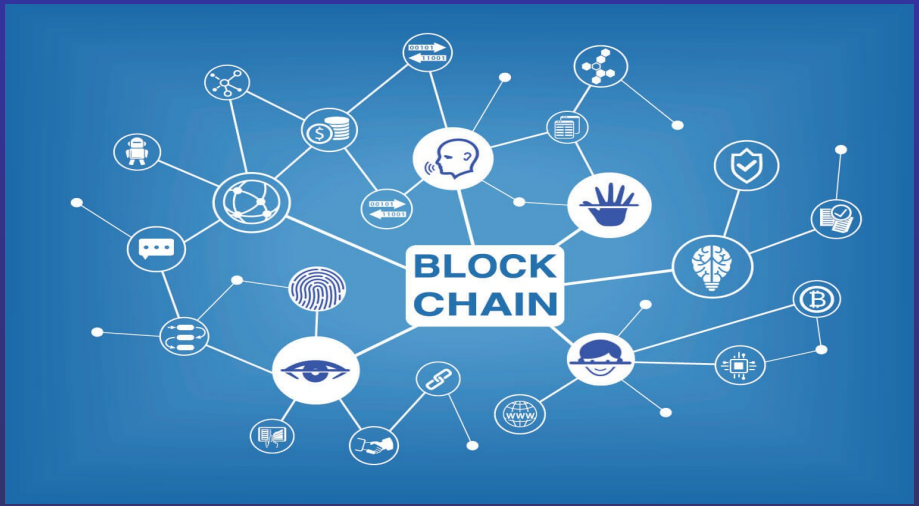
EJEMPLOS BLOCKCHAIN

- Cryptomonedas
  - Bitcoin, Ethereum, Litecoin...
- Bases de datos
  - Namecoin
- Navegadores
  - Brave
- Redes Sociales
  - Steemit

Ventajas y Desventajas

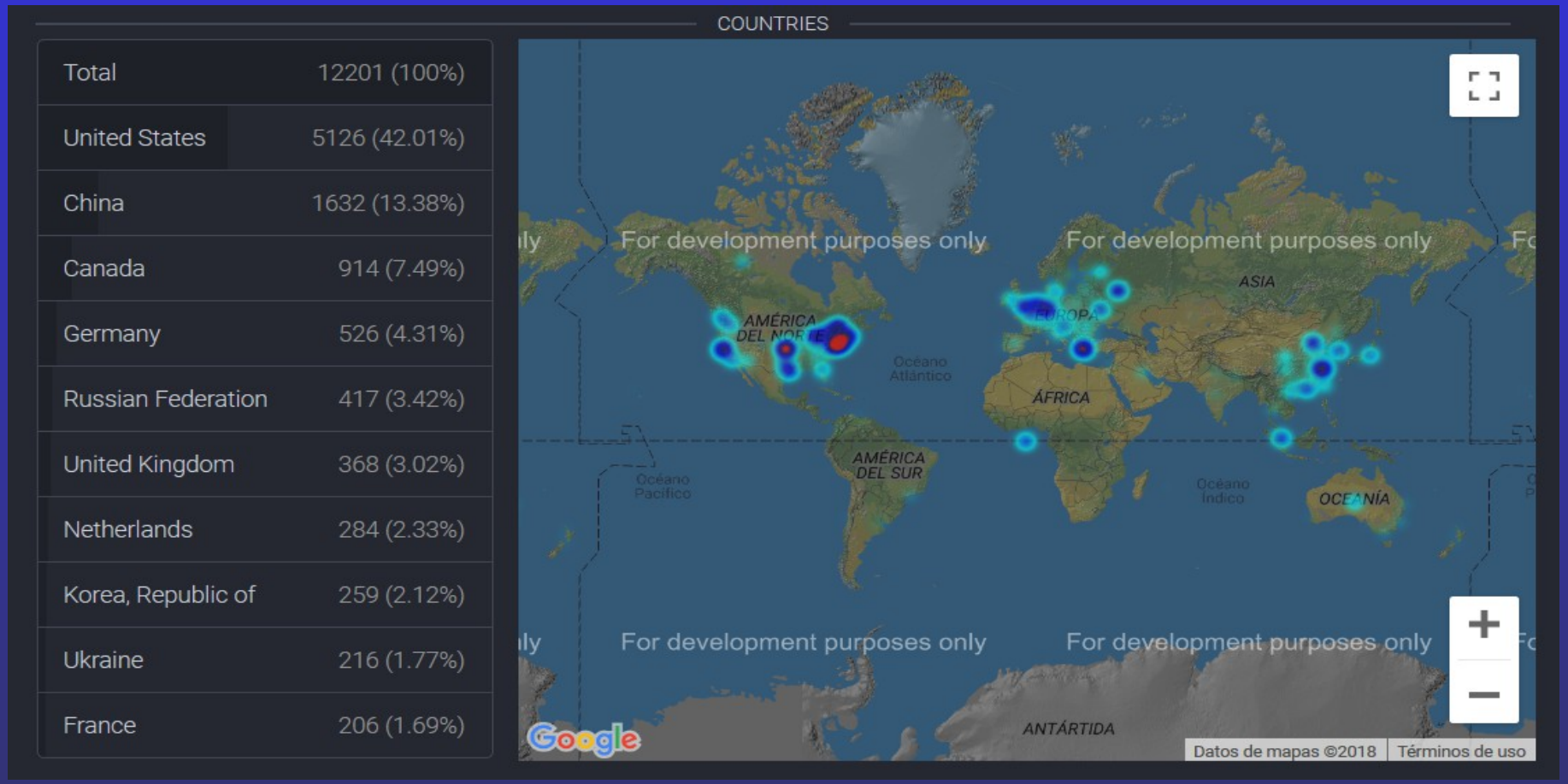
- Irreversibilidad e inmutabilidad
- Cryptografía y Seguridad
- Carácter público
- Privacidad y Transparencia

- Lento
- Necesita consenso
- Escalabilidad
- Alto coste computacional
- Requiere Minería



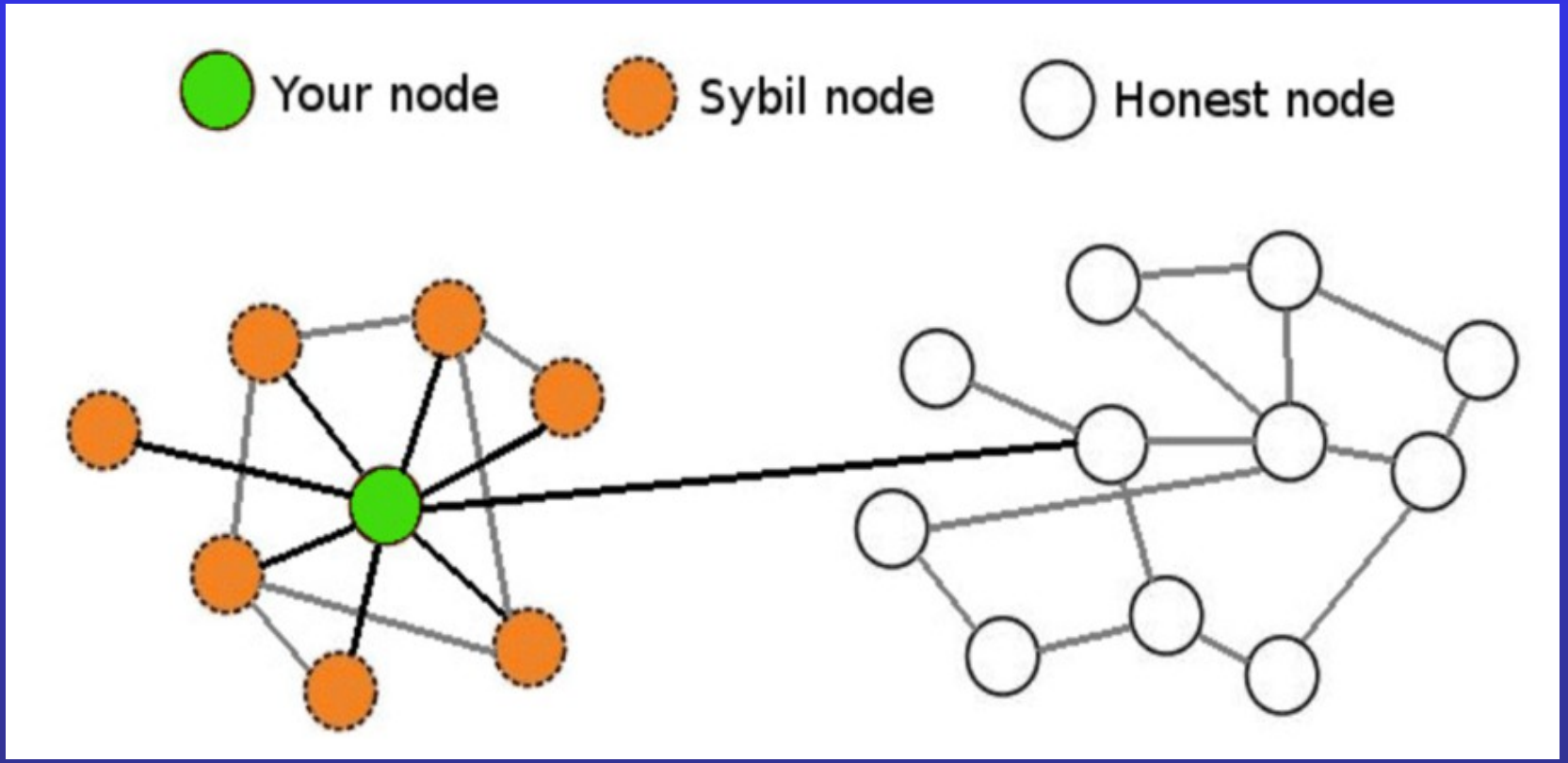
Ataques (¿Eficientes?)

- Nueva tecnología = Nuevas formas de ataque



HACK &BEERS

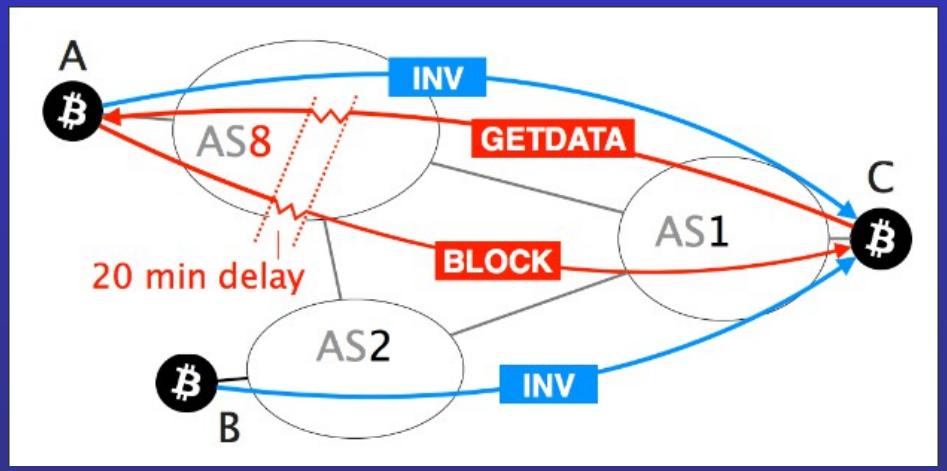
Sibyl Attack



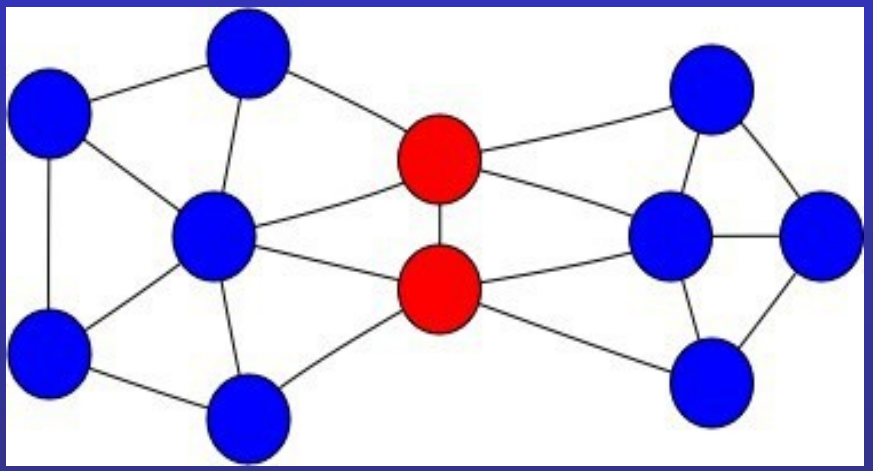
- Existen 3 soluciones para prevenir:
  - Coste en creación de Identidad
  - Cadena de confianza
  - Reputación usuarios

Routing Attacks

- Delay Attack
- Se usa para retrasar un bloque 20 minutos



- Partitioning Attack
  - Atacante intenta separar varios nodos

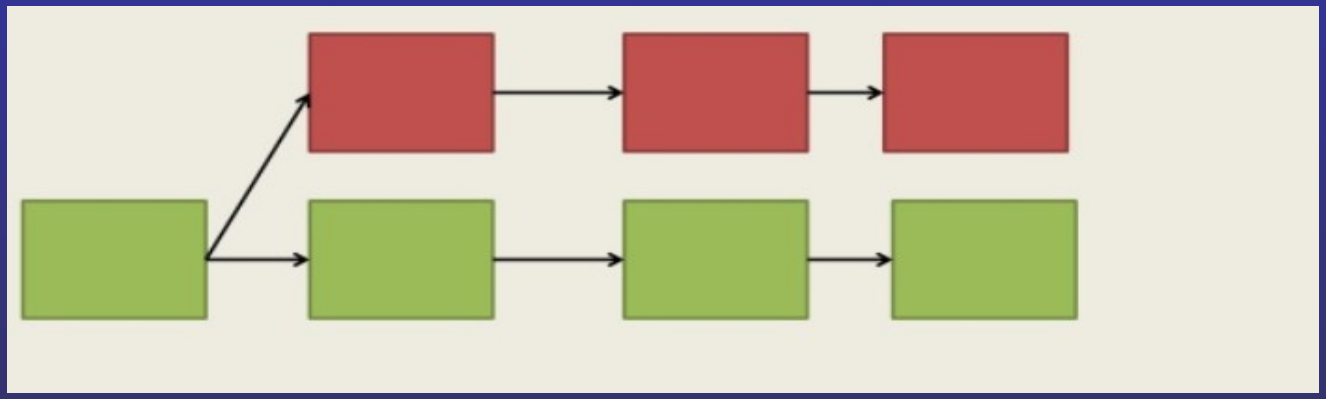


DDoS Attack

- Ataque de denegación de servicio
- Congestión de los nodos de la red
- Es inevitable
- Pero podemos mitigarlo
  - Variando tamaño de bloque

51% Majority Attack

- Grupo de mineros
- Intentan gastar sus crypto dos veces en la blockchain
- Se produce cuando existe una bifurcación de la blockchain



Blockchain Ethereum

- Vitalik Buterin
- White papper 2013
- 2014 crowfunding
- Recaudacion 18Mill$
- 2015 lanza 1ª fase Frontier

- Tiene 4 fases:
  - Frontier(2015)
  - Homestead(2016)
  - Metropolis(2017)
  - Serenity(sin fecha)

Ethereum

- Se basa en Bitcoin:
  - Distribuido
  - Moneda
  - Mineros
  - Blockchain
- Intérprete más extenso (Turing completo)
- EVM (Ethereum Virtual Machine)
  - Permite ejecutar Smart Contracts entre nodos sin servidor
- Ethash (Proof-of-work)

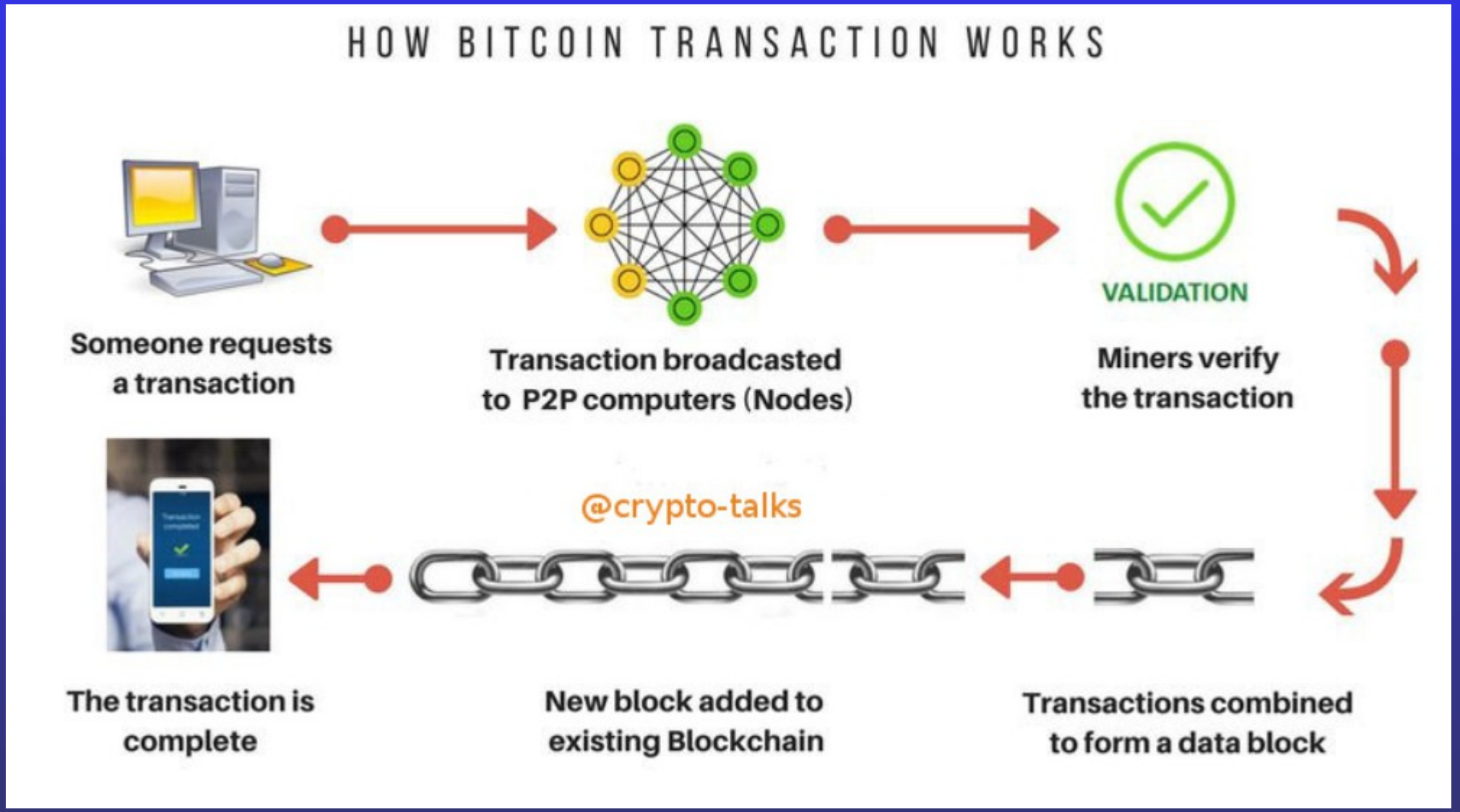
Comparativa

	ETHEREUM	BITCOIN
Nº Total de Monedas	No tiene una cantidad fija	21 millones
Algoritmo	Ethash (Proof-of-work)	SHA-256 (Proof-of-work)
Tiempo de Emisión de Bloques	12-20 segundos	10 minutos
Tamaño de bloques	menos de 1 MB	2 MB

PoW & PoS

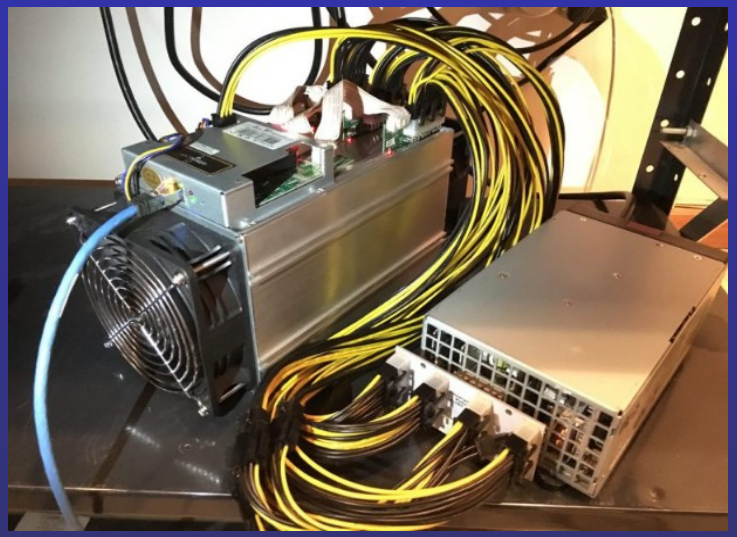
- Proof to Work
  - Recompensa por Trabajo
  - Minan bloques
  - Realizan algoritmos complejos
  - Excesivo gasto de energía
- Proof to Stake
  - Recompensa por Participación
  - Directamente proporcional al nº de monedas
  - Quién mas monedas tiene, tiene interés en la supervivencia de la moneda

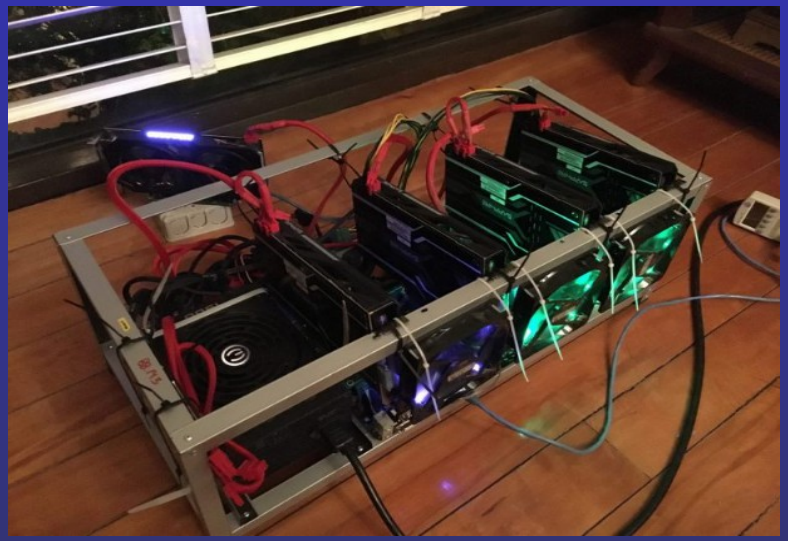
Minado de Bloques



Mineros

- Suelen ser equipos configurados con una GPU's,CPU's, FPGA o ASIC's
- Alto consumo energético
- Lentos
- Usan scripts de minado:
  - SHA256,Scrypt y X11





Cryptojacking

- Método de minado “más rápido”
- Infectar a la víctima (pc, movil o tablet) y utilizar sus recursos para minar sin que el usuario se entere.
- Problemas de batería, mala eficiencia en nuestros terminales, incluso daño irreparable de la batería del teléfono.
- Inyectado en la propia página web.

Ejemplo Cryptojacking

```
<script src="https://authedmine.com/lib/authedmine.min.js"></script>
<script>
    var miner = new
CoinHive.Anonymous('nom2KNN1a8m7mJIHdNcI4FbluQ7lmpYA', {throttle:
0.5});

    // Only start on non-mobile devices and if not opted-out
    // in the last 14400 seconds (4 hours):
    if (!miner.isMobile() && !miner.didOptOut(14400)) {
        miner.start();
    }
</script>
```

Evitar Cryptojacking?

- Utilizar extensiones que bloquean software de minería como No Coin (Google Chrome/Mozilla Firefox) o MinerBlock (Google Chrome/Mozilla Firefox).
- Actualizar regularmente las extensiones de los navegadores.
- Actualizar nuestro navegador, solución antimalware/antivirus y sistema operativo a la última versión.
- Herramienta española Notmining (www.notmining.org)

Muchas Gracias por asistir!!!!!

¿Preguntas, Sugerencias?