Blockchain Monterrey

Meetup de comunidad

BLOCKCHAIN MONTERREY

Blockchain Monterrey

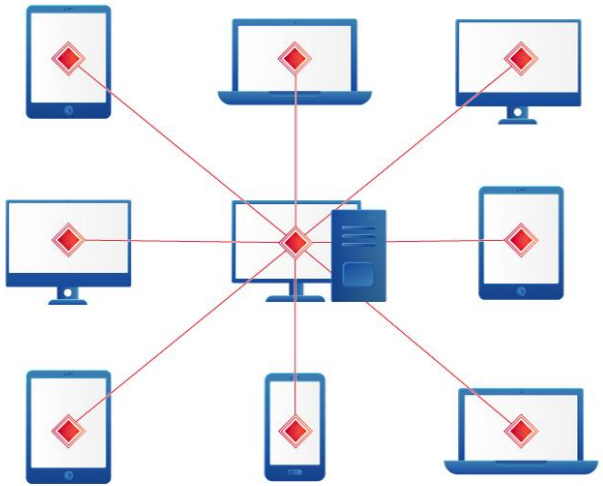
Agenda

1. Blockchain 101
2. Cryptography
3. Economics

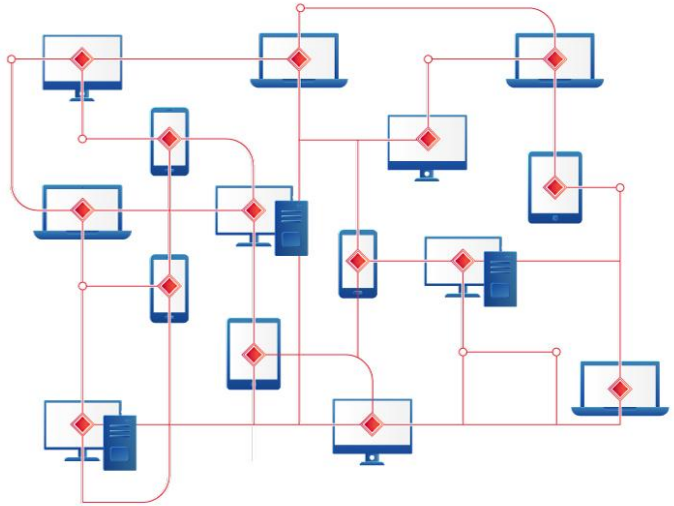
101 – Redes

Centralized vs. P2P

Centralized network

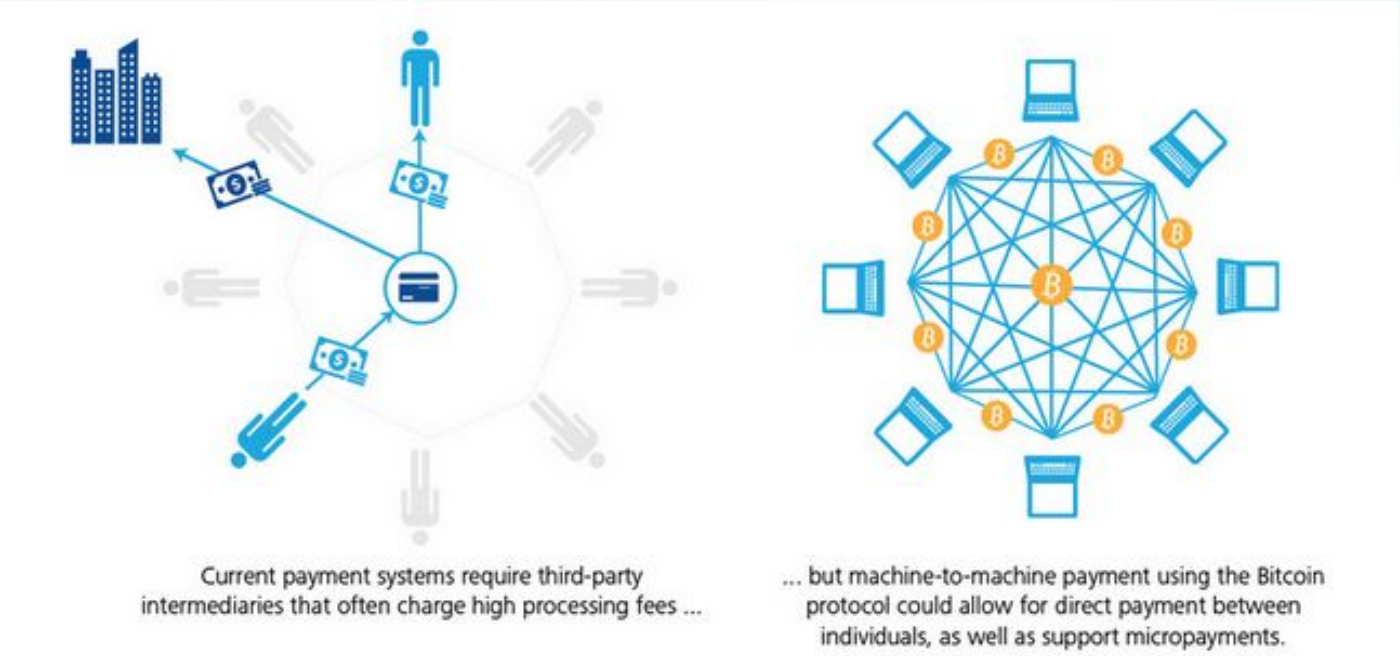


P2P network



101 - ¿Cómo nace la blockchain?

- En 2008, Satoshi Nakamoto publicó un artículo en la lista de criptografía de metzdowd.com donde propone el protocolo Bitcoin para un sistema de pagos tipo “peer-to-peer”.



Current payment systems require third-party intermediaries that often charge high processing fees ...

... but machine-to-machine payment using the Bitcoin protocol could allow for direct payment between individuals, as well as support micropayments.

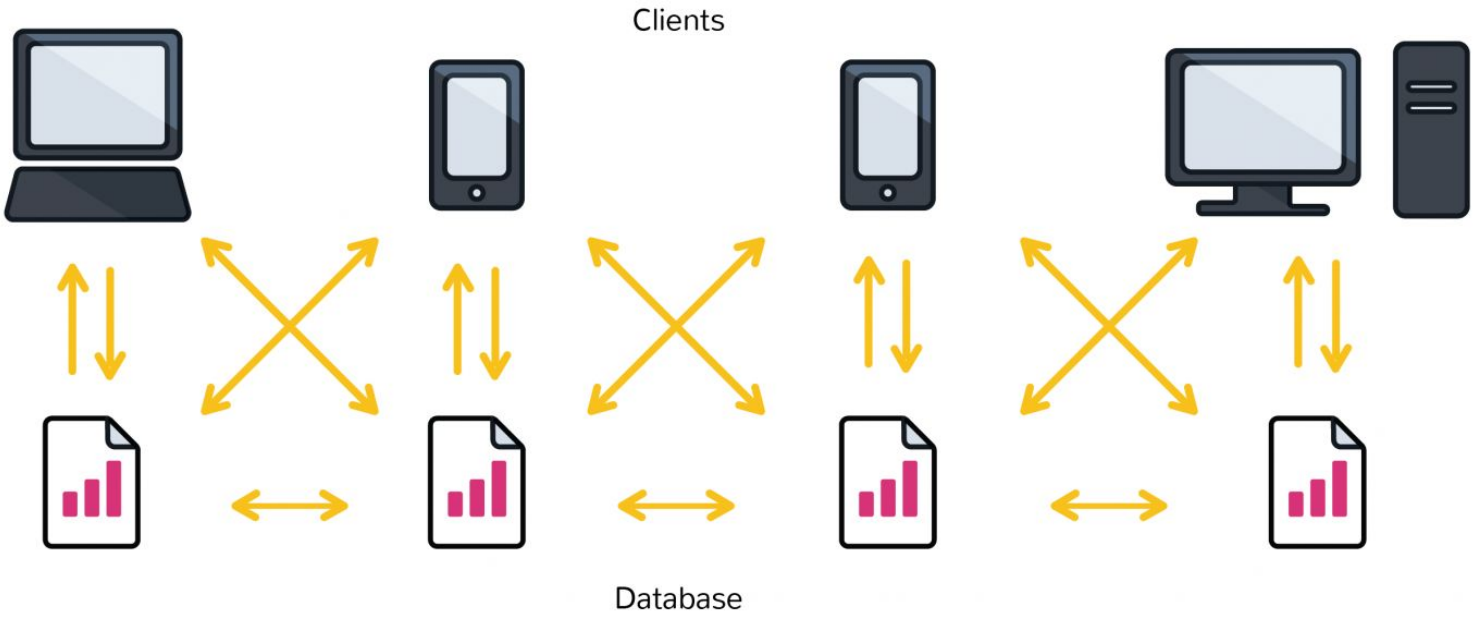
101 - ¿Qué es la Blockchain?

- La definición más simple:

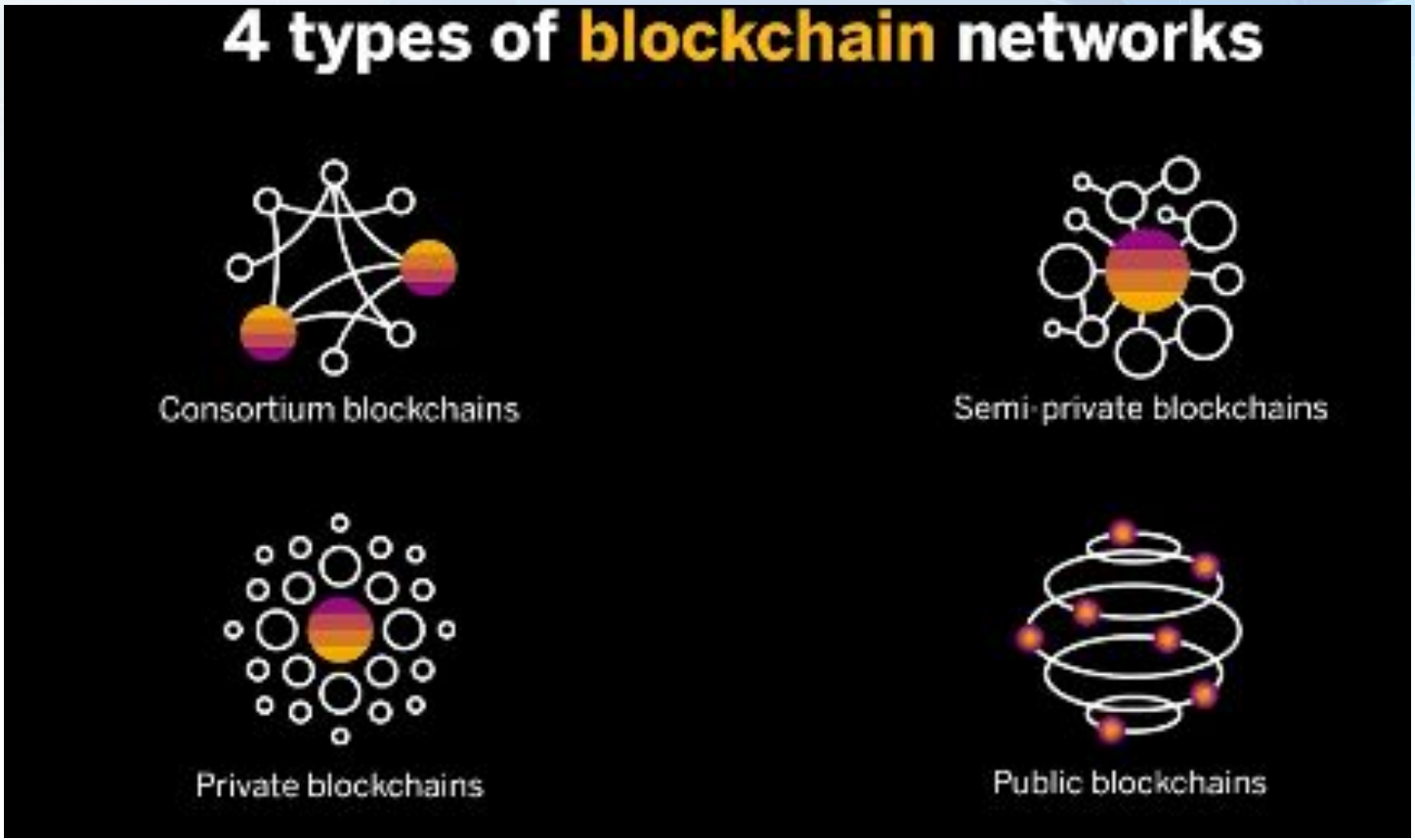
- Un registro de transacciones confiable, casi imposible de hackear, de quien tiene la propiedad de alguna cosa.

- Blockchain está basada en “distributed ledger technology”, la cual de forma segura registra información a traves de una red peer to peer. Aunque fue creada originalmente para negociar Bitcoins, el potencial de blockchain va más allá.

101 - DLT



101 – Tipos de Blockchain



101 - Características

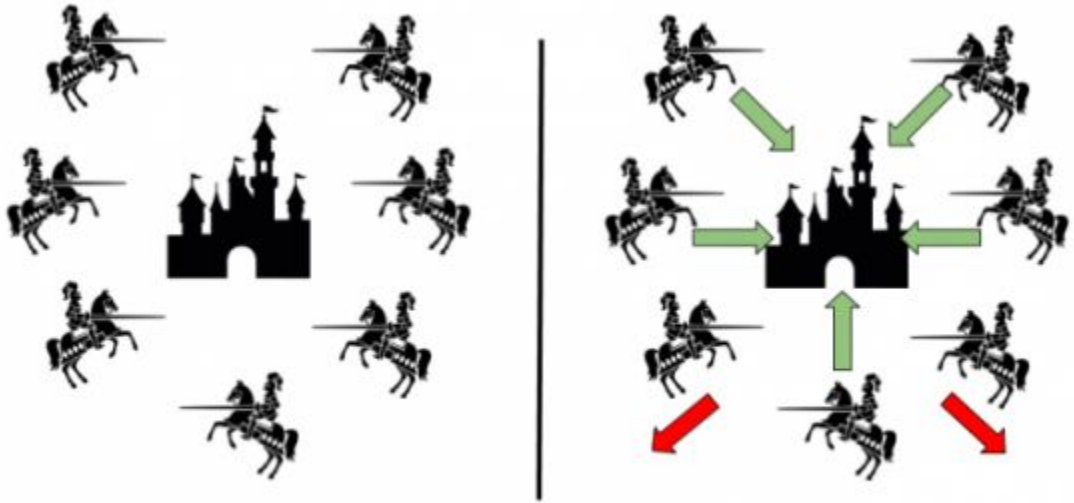
	Public Blockchain	Private Blockchain	Federated/Consortium Blockchain
Access	• Anyone	• Single organization	• Multiple selected organizations
Participants	• Permissionless • Anonymous	• Permissioned • Known identities	• Permissioned • Known identities
Security	• Consensus mechanism • Proof of Work / Proof of Stake	• Pre-approved participants • Voting/multi-party consensus	• Pre-approved participants • Voting/multi-party consensus
Transaction Speed	• Slow	• Lighter and faster	• Lighter and faster

Cryptography

- Proof of work
- Hashing
- Signatures

Cryptography – Proof of work

- PoW resuelve el problema de los generales bizantinos, es decir quien no trabaje para el bien común es descartado.
- Problema matemático con complejidad de resolución de aproximadamente 10 minutos. El que lo resuelve agrega el bloque y gana la recompensa.



Cryptography – Proof of work

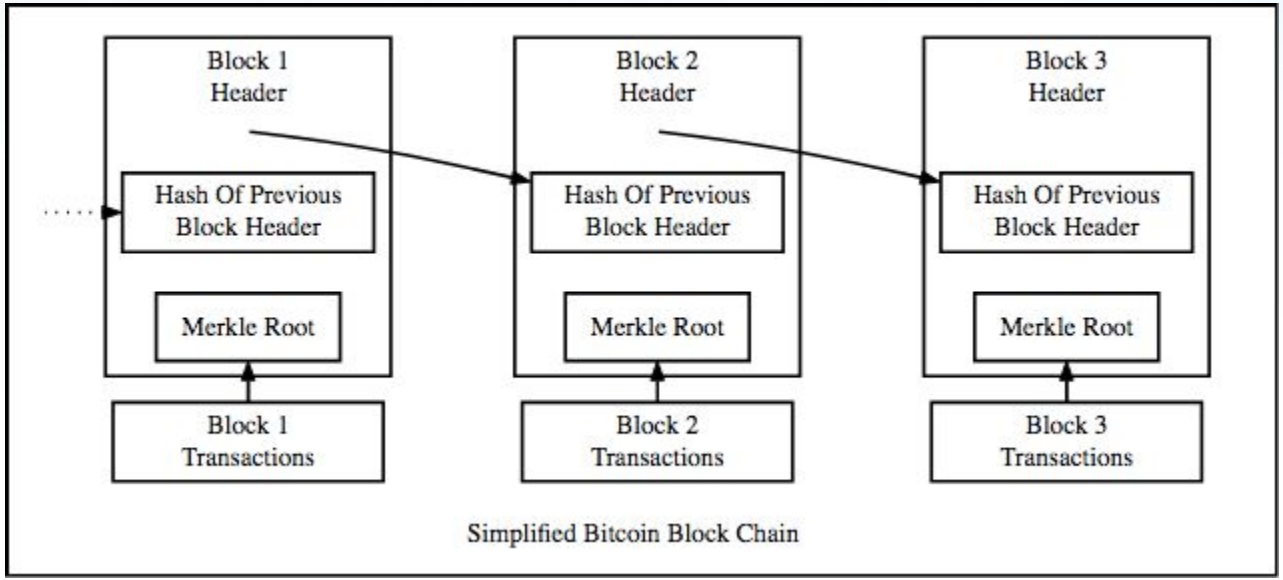
Total Bitcoins in circulation:	17,122,088
Total Bitcoins to ever be produced:	21,000,000
Percentage of total Bitcoins mined:	81.53%
Total Bitcoins left to mine:	3,877,913
Total Bitcoins left to mine until next blockhalf:	1,252,913

https://www.bitcoinblockhalf.com/

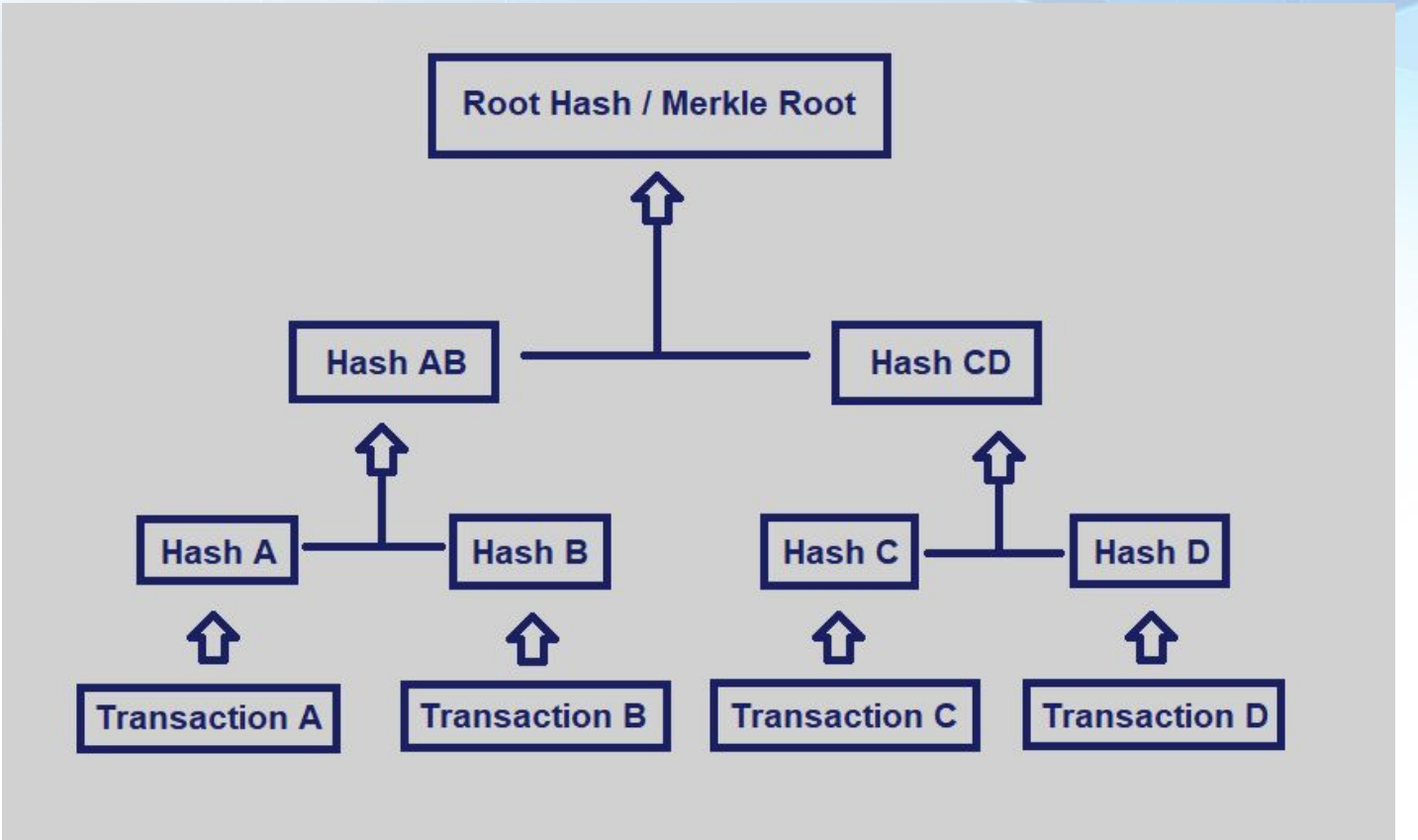
Cryptography - Hashing

- SHA256, una cadena de 256 bits o 64 caracteres

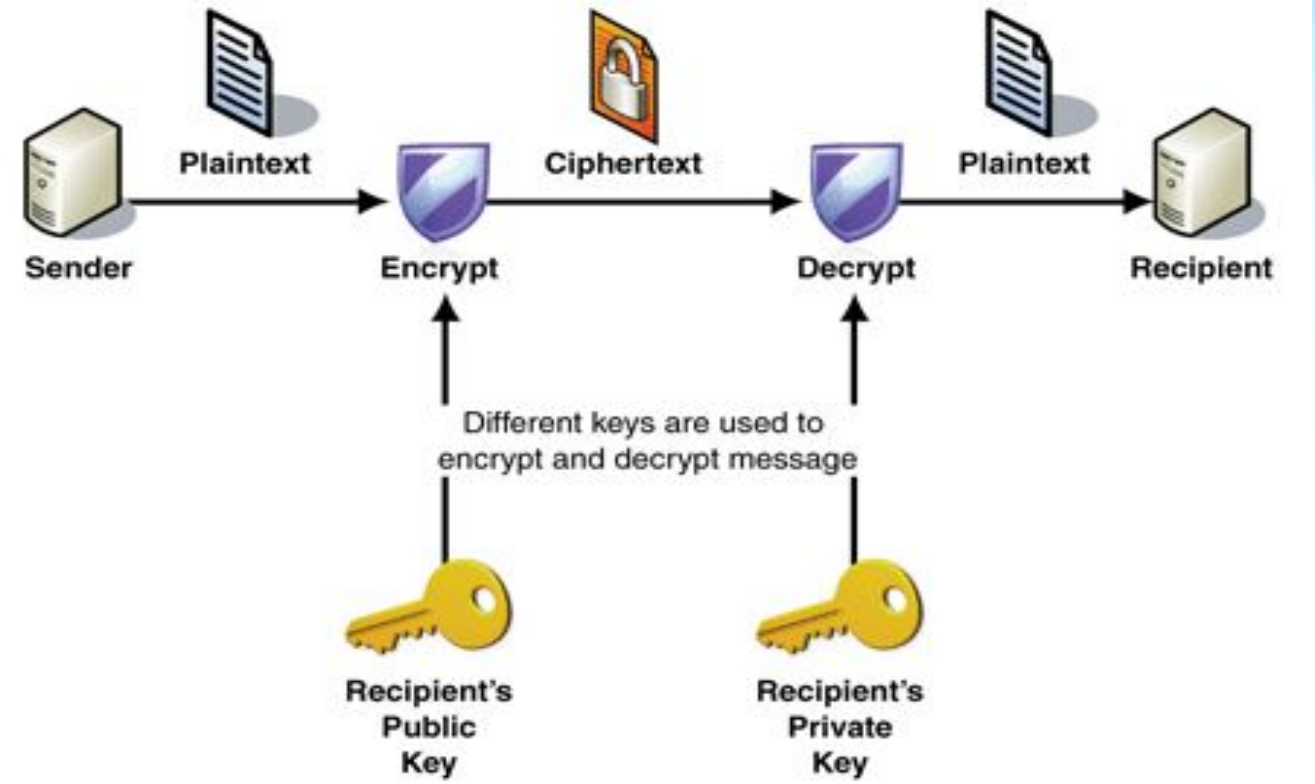
"Luis" es : 1BE075B9041A58B82BE347B54E9F3D7F5D84DC57935BCC769106748A9EB237E8 (Hexadecimal, 4 bits)



Cryptography – Merkle Tree



Cryptography - Signatures

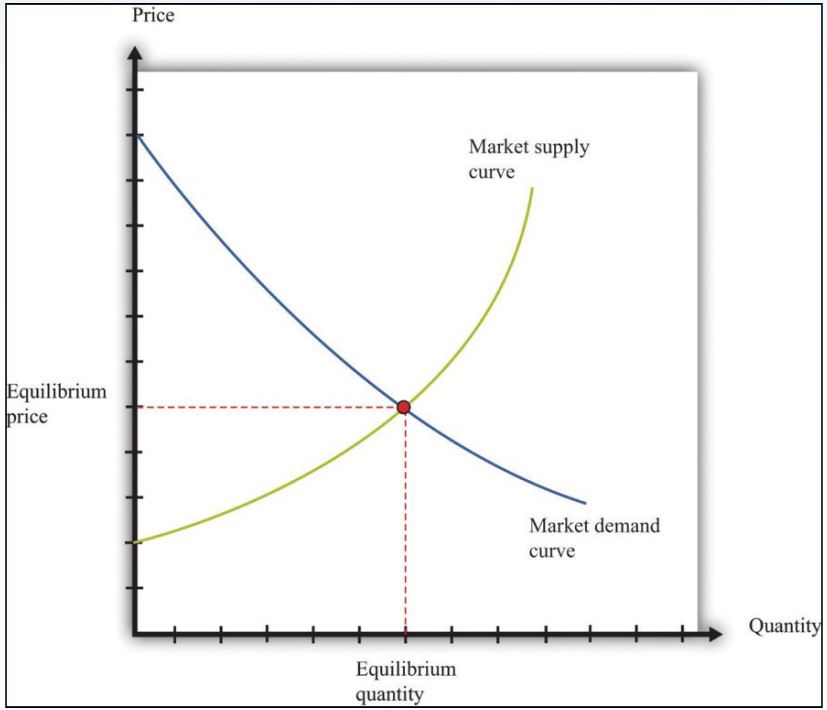


Economics

- Lo que mantiene al systema P2P de las blockchains públicas trabajando correctamente es el incentivo económico… y así debería continuar.

Economics – Value

- ¿Porqué tienen valor las Cryptomonedas?



Economics – Equilibrio de Nash

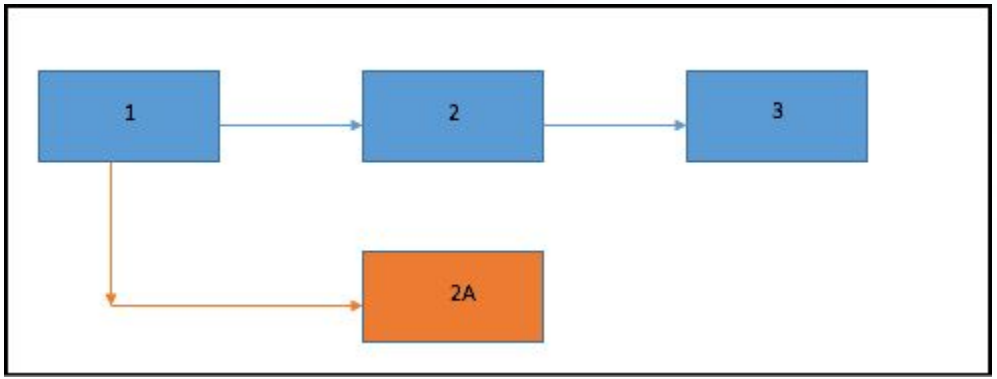
¿Porqué conserva el valor?

- Es más redituable trabajar para el bien común de la blockchain que para hacerla fallar.

	B Takes Action	B Doesn't Take Action
A Takes Action	(4,4)	(4,0)
A Doesn't Take Action	(0,4)	(0,0)

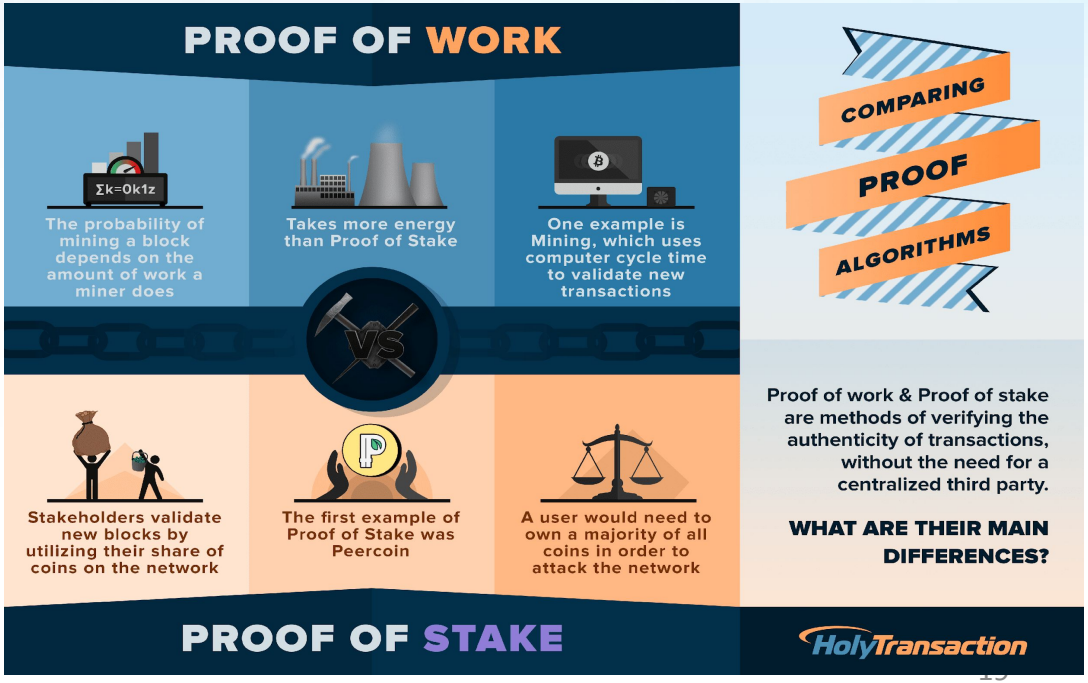
Economics – Forks

- ¿Porqué no son tan viables?
- Schelling Point

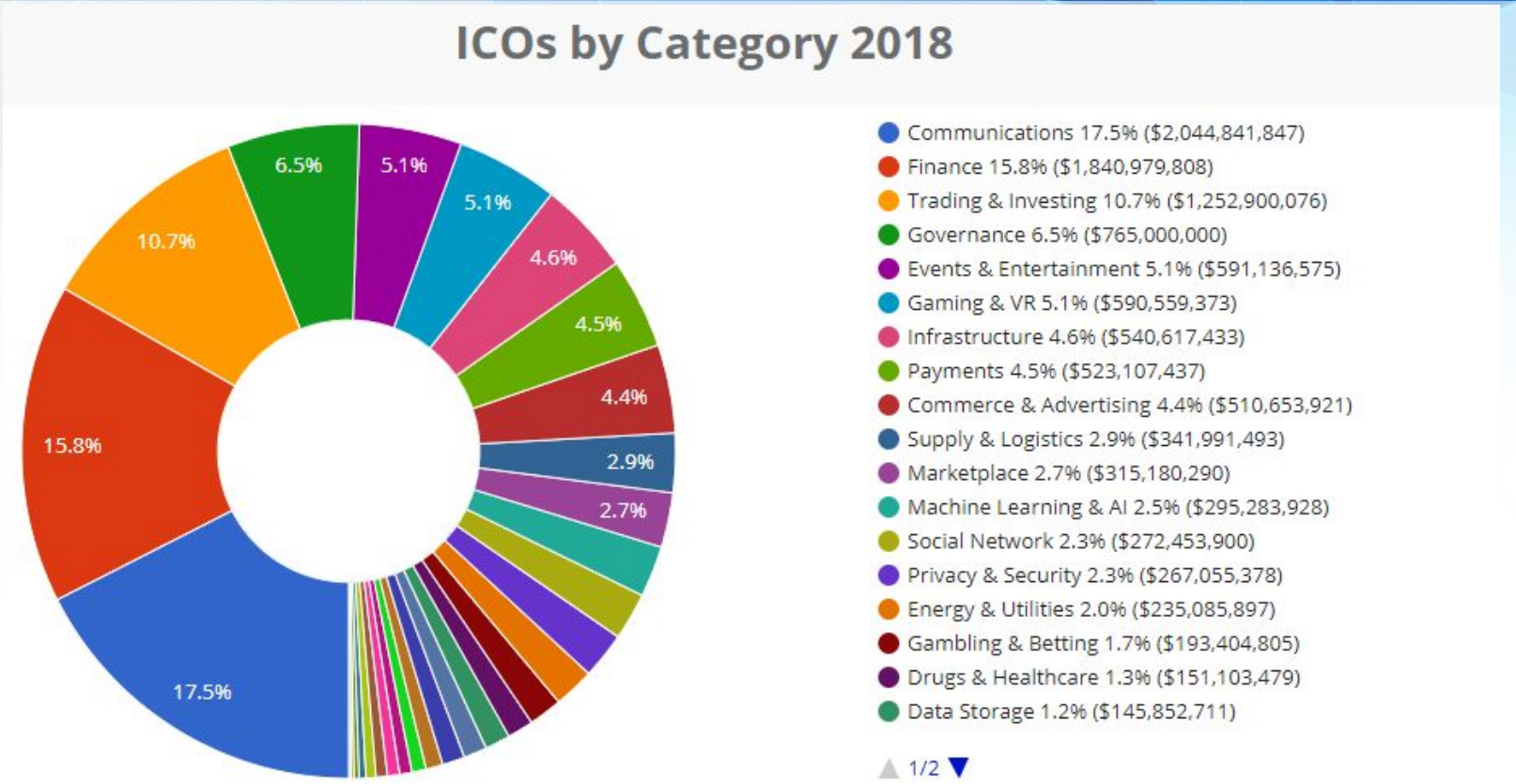


Economics – Proof of Stake

- Resuelve muchos problemas actuales
  - Baja probabilidad de ganar tokens en PoW
  - Consumo de energía
  - Ataque por soborno



Economics - ICOs



https://www.coinschedule.com/stats.html

Thank You

Luis Miguel Garcia
Luis@privasee.io
Luis.garcia@quetzichain.com