

# Blockchain Monterrey

Meetup de comunidad



BLOCKCHAIN  
MONTERREY

**Blockchain  
Monterrey**

# Agenda

1

Blockchain 101

2

Cryptography

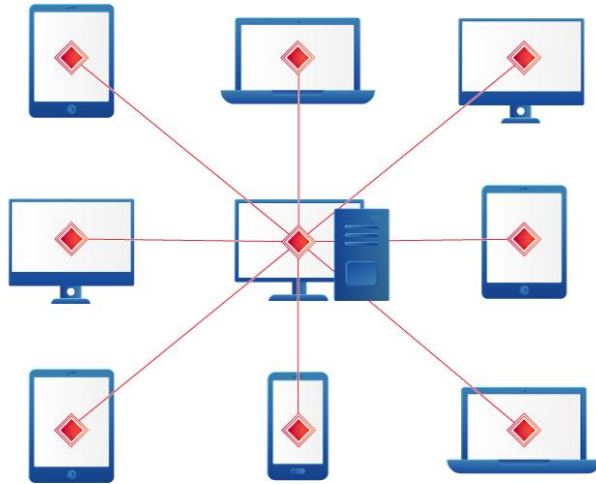
3

Economics

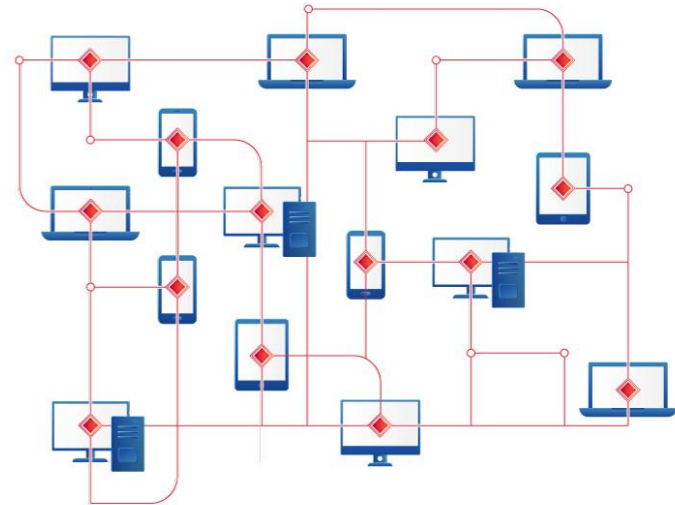
# 101 – Redes

## Centralized vs. P2P

Centralized network

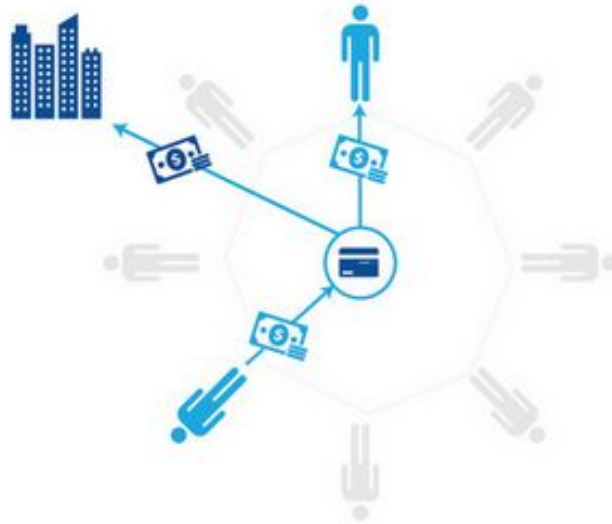


P2P network



# 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 ...

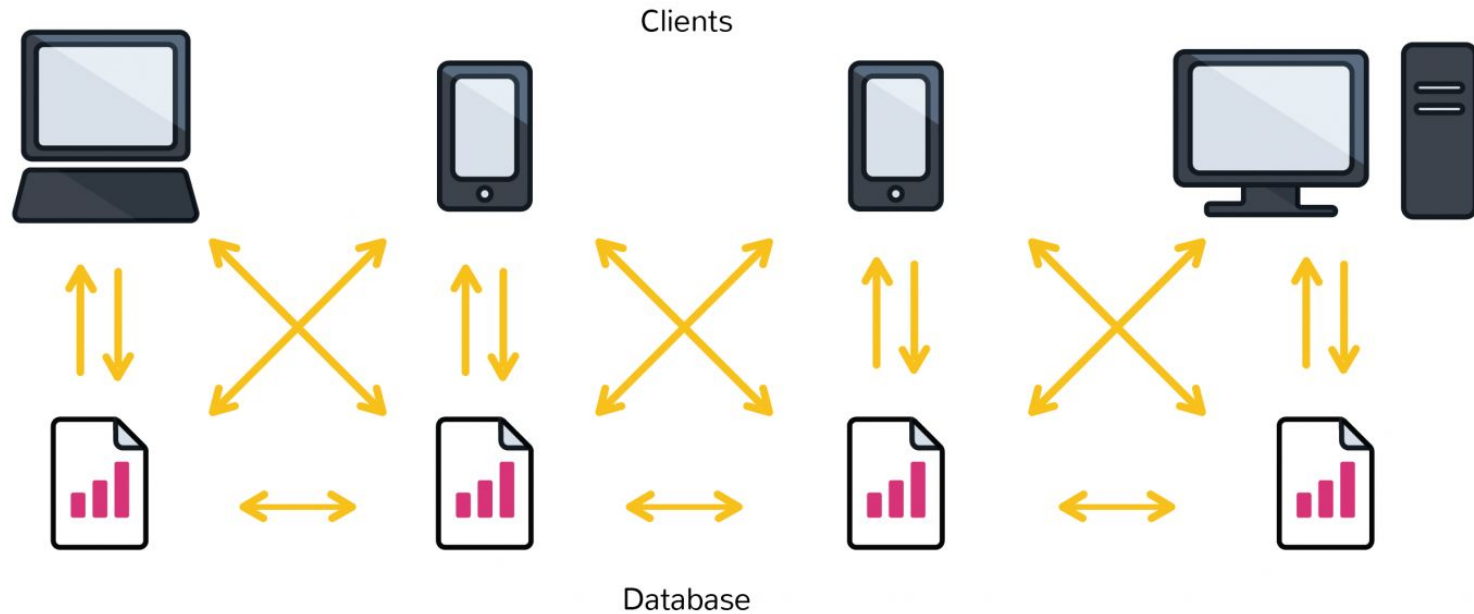


... but machine-to-machine payment using the Bitcoin protocol could allow for direct payment between individuals, as well as support micropayments.

# 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 través 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

## 4 types of **blockchain** networks



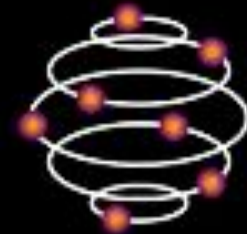
Consortium blockchains



Semi-private blockchains



Private blockchains



Public blockchains

# 101 - Características

	Public Blockchain	Private Blockchain	Federated/Consortium Blockchain
Access	<ul style="list-style-type: none"><li>• Anyone</li></ul>	<ul style="list-style-type: none"><li>• Single organization</li></ul>	<ul style="list-style-type: none"><li>• Multiple selected organizations</li></ul>
Participants	<ul style="list-style-type: none"><li>• Permissionless</li><li>• Anonymous</li></ul>	<ul style="list-style-type: none"><li>• Permissioned</li><li>• Known identities</li></ul>	<ul style="list-style-type: none"><li>• Permissioned</li><li>• Known identities</li></ul>
Security	<ul style="list-style-type: none"><li>• Consensus mechanism</li><li>• Proof of Work / Proof of Stake</li></ul>	<ul style="list-style-type: none"><li>• Pre-approved participants</li><li>• Voting/multi-party consensus</li></ul>	<ul style="list-style-type: none"><li>• Pre-approved participants</li><li>• Voting/multi-party consensus</li></ul>
Transaction Speed	<ul style="list-style-type: none"><li>• Slow</li></ul>	<ul style="list-style-type: none"><li>• Lighter and faster</li></ul>	<ul style="list-style-type: none"><li>• Lighter and faster</li></ul>

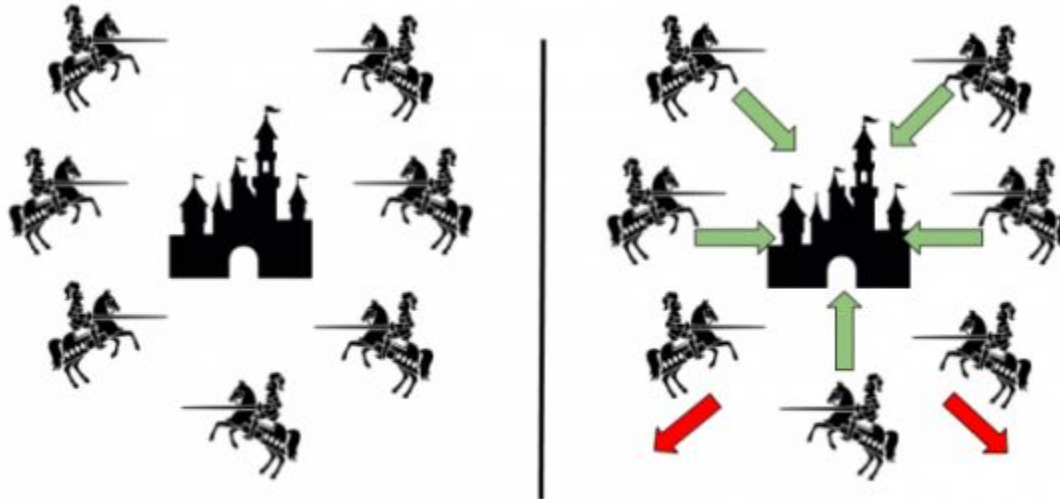


# Cryptography

- 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

## Bitcoin Block Reward Halving Countdown

Days Hours Minutes Seconds

695:16:55:07

Reward-Drop ETA date: 25 May 2020 17:32:42

The Bitcoin block mining reward halves every 210,000 blocks, the coin reward will decrease from 12.5 to 6.25 coins.

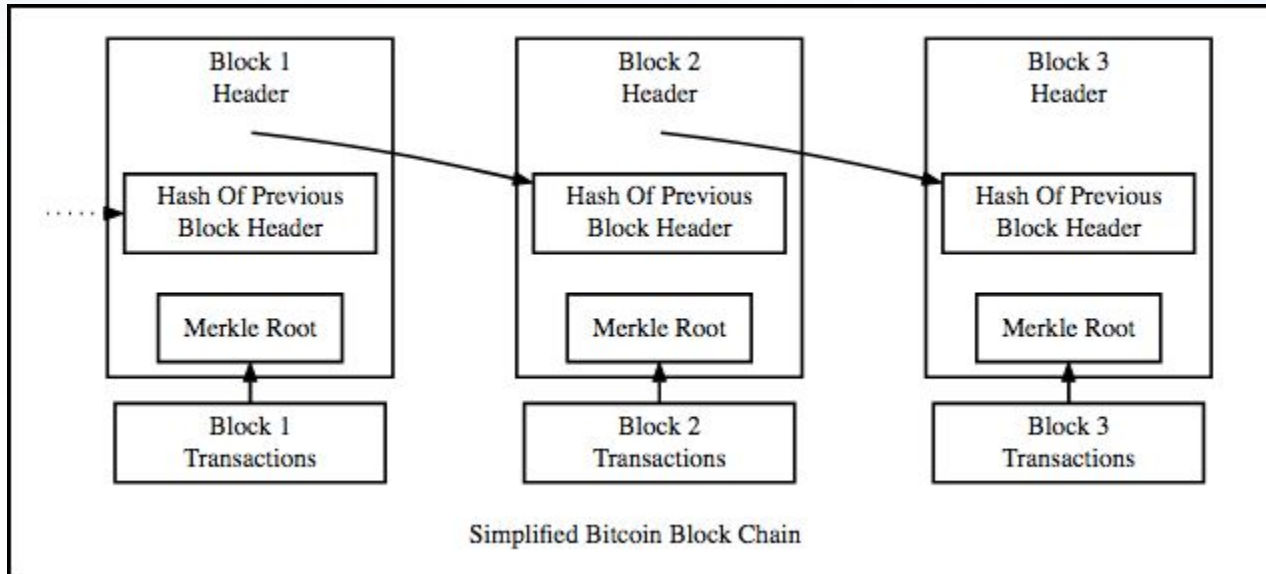
Total Bitcoins in circulation:	17,122,088
Total Bitcoins to ever be produced:	21,000,000
Percentage of total Bitcoins mined:	81.53%
Total Bitcoins left to mine:	3,877,913
Total Bitcoins left to mine until next blockhalf:	1,252,913

<https://www.bitcoinblockhalf.com/>

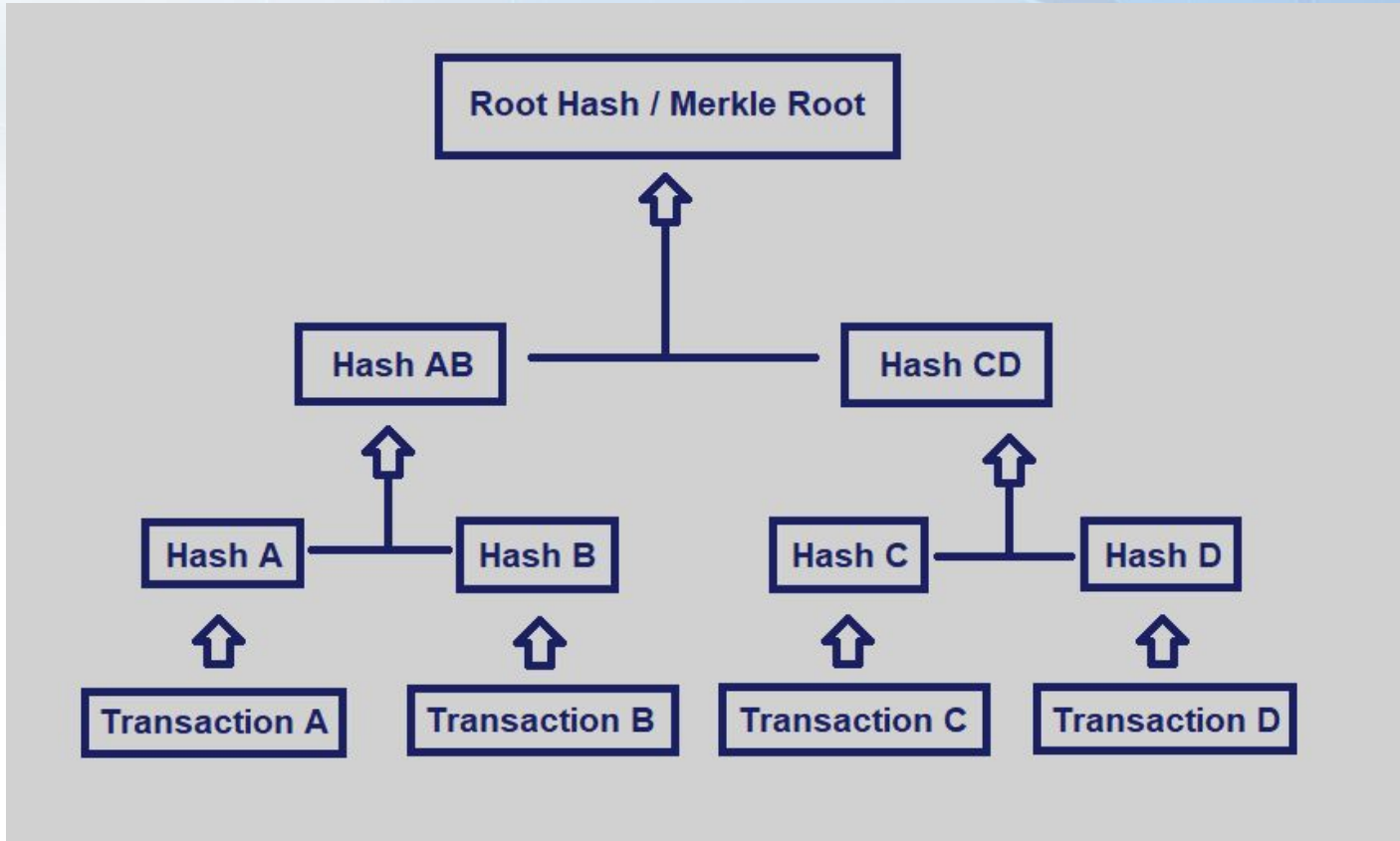
# Cryptography - Hashing

- SHA256, una cadena de 256 bits o 64 caracteres

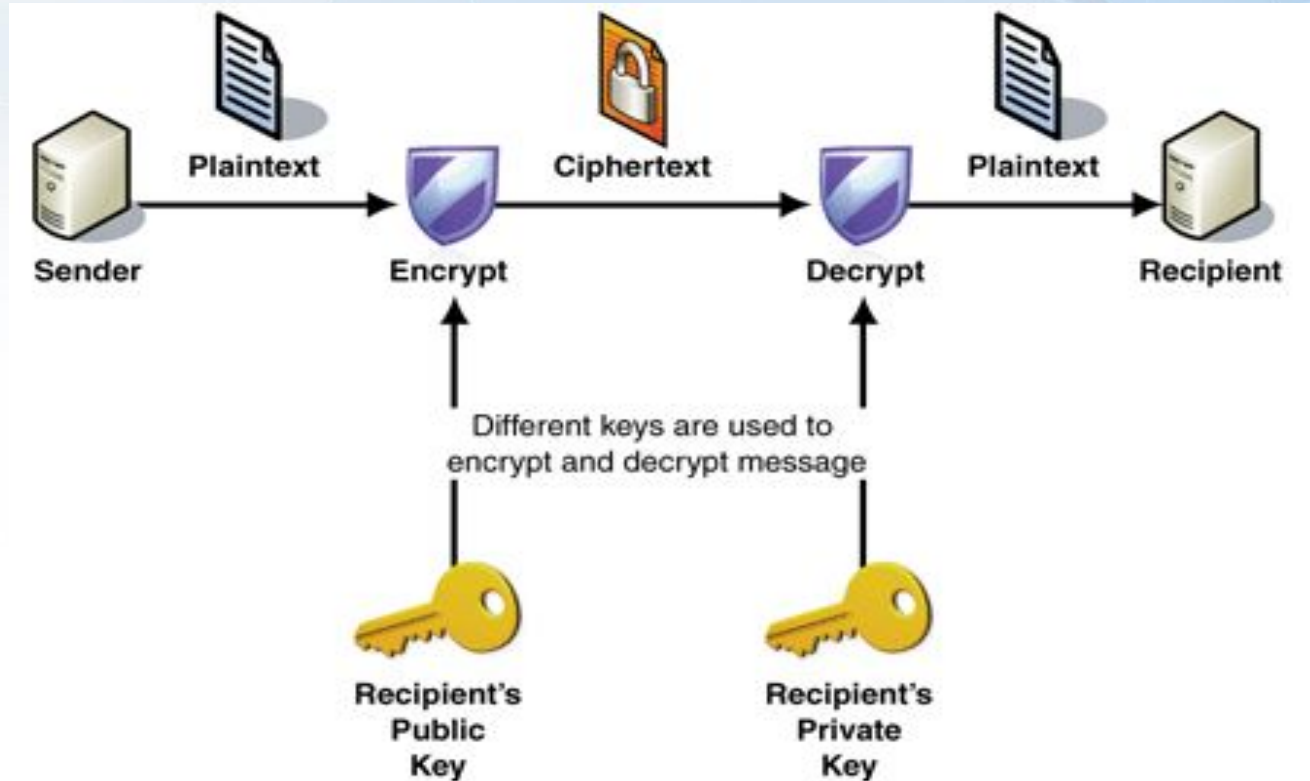
“Luis” es : 1BE075B9041A58B82BE347B54E9F3D7F5D84DC57935BCC769106748A9EB237E8 (Hexadecimal, 4 bits)



# Cryptography – Merkle Tree



# Cryptography - Signatures



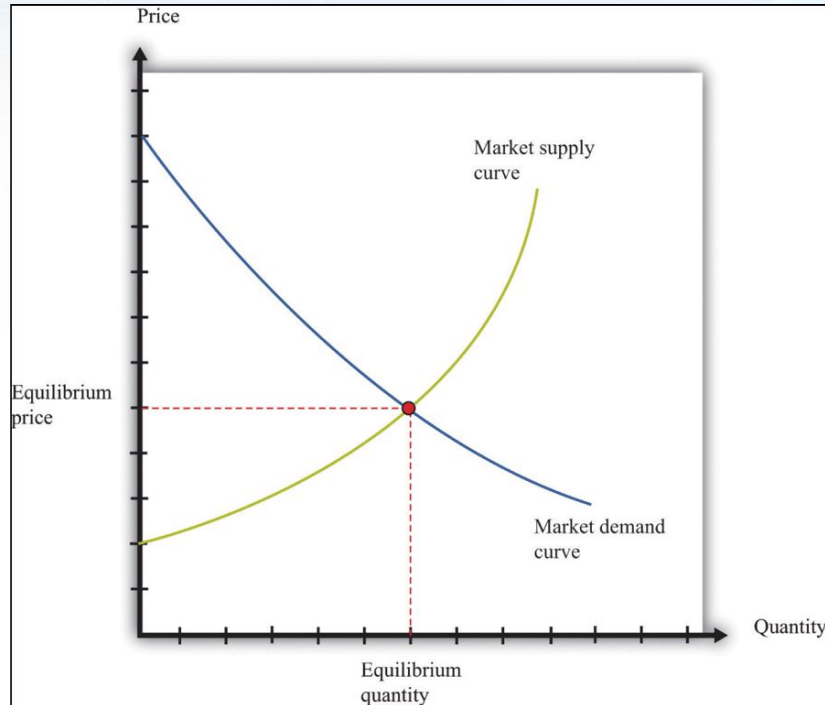
# Economics

- 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

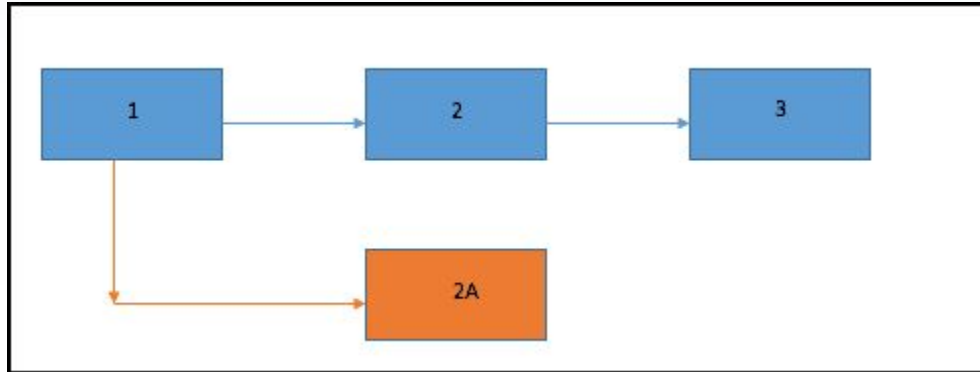
¿Porqué conserva el valor?

- 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)

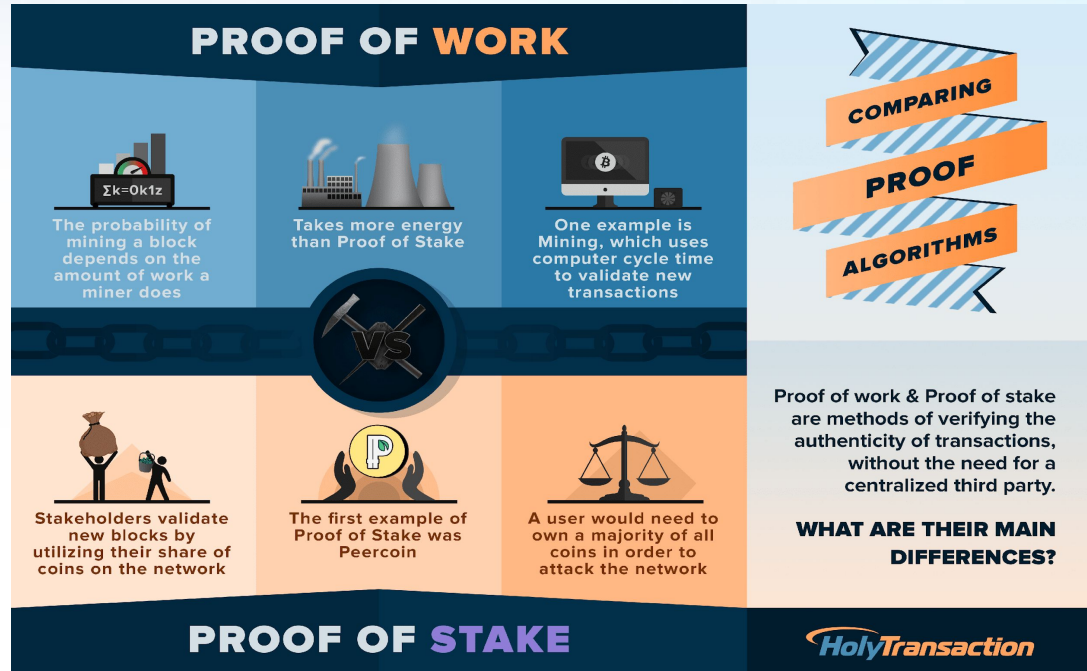
# Economics – Forks

- ¿Porqué no son tan viables?
- Schelling Point



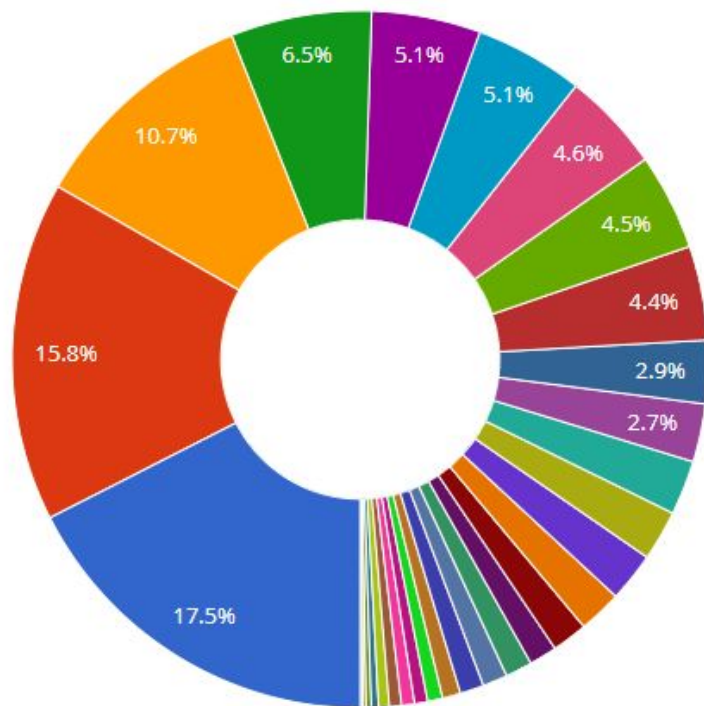
# Economics – Proof of Stake

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



# Economics - ICOs

## ICOs by Category 2018



- Communications 17.5% (\$2,044,841,847)
- Finance 15.8% (\$1,840,979,808)
- Trading & Investing 10.7% (\$1,252,900,076)
- Governance 6.5% (\$765,000,000)
- Events & Entertainment 5.1% (\$591,136,575)
- Gaming & VR 5.1% (\$590,559,373)
- Infrastructure 4.6% (\$540,617,433)
- Payments 4.5% (\$523,107,437)
- Commerce & Advertising 4.4% (\$510,653,921)
- Supply & Logistics 2.9% (\$341,991,493)
- Marketplace 2.7% (\$315,180,290)
- Machine Learning & AI 2.5% (\$295,283,928)
- Social Network 2.3% (\$272,453,900)
- Privacy & Security 2.3% (\$267,055,378)
- Energy & Utilities 2.0% (\$235,085,897)
- Gambling & Betting 1.7% (\$193,404,805)
- Drugs & Healthcare 1.3% (\$151,103,479)
- Data Storage 1.2% (\$145,852,711)

▲ 1/2 ▼

# Thank You

Luis Miguel Garcia

[Luis@privasee.io](mailto:Luis@privasee.io)

[Luis.garcia@quetzichain.com](mailto:Luis.garcia@quetzichain.com)