Financial Comments

@canosfm

Disrupting Technologies
4th Industrial Revolution
Blockchain Explained
Session number

(IP-212)

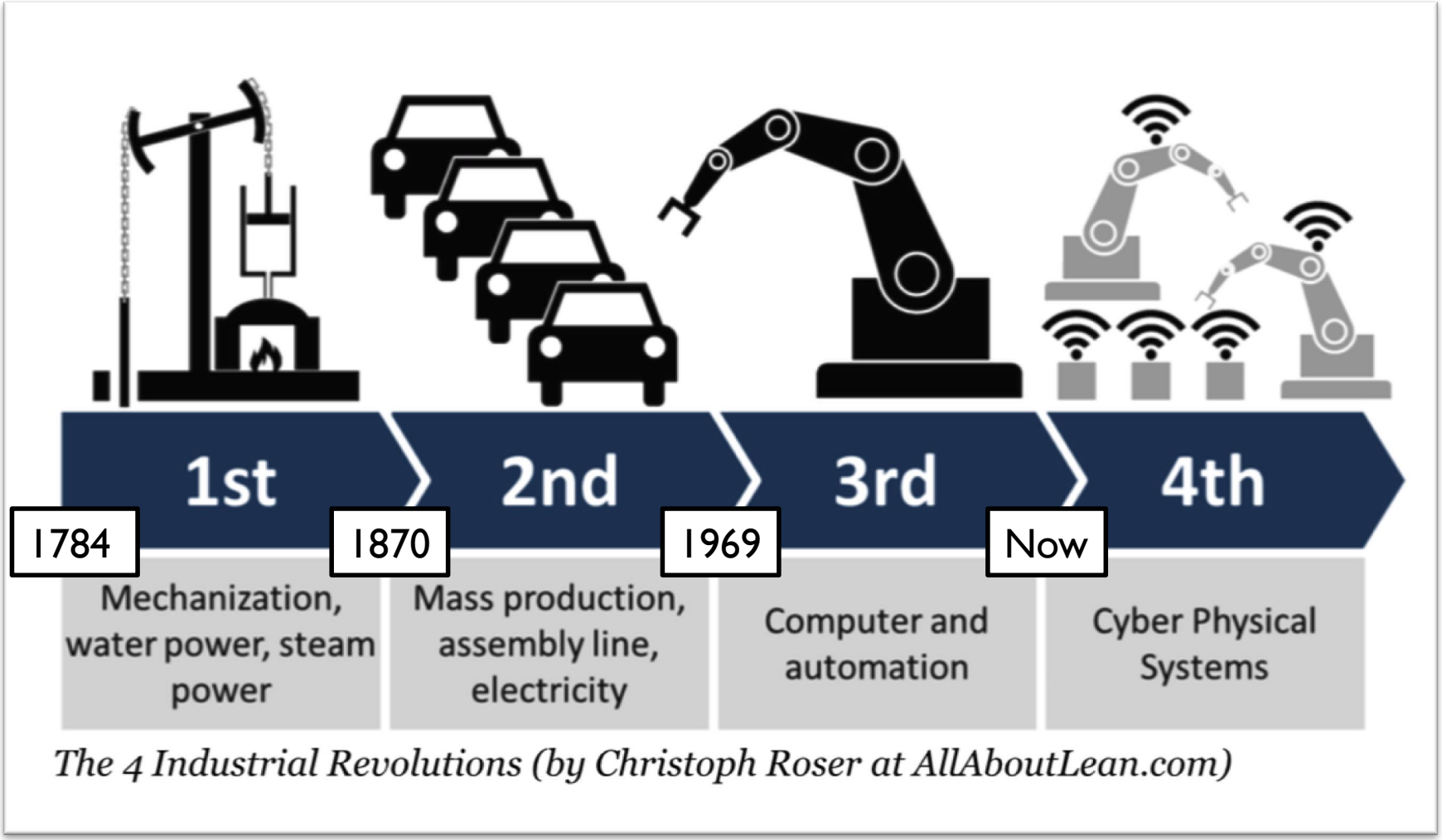
Professor
Francisco Canos
Investor & Advisor

https://fcanos.com/

Index for the session

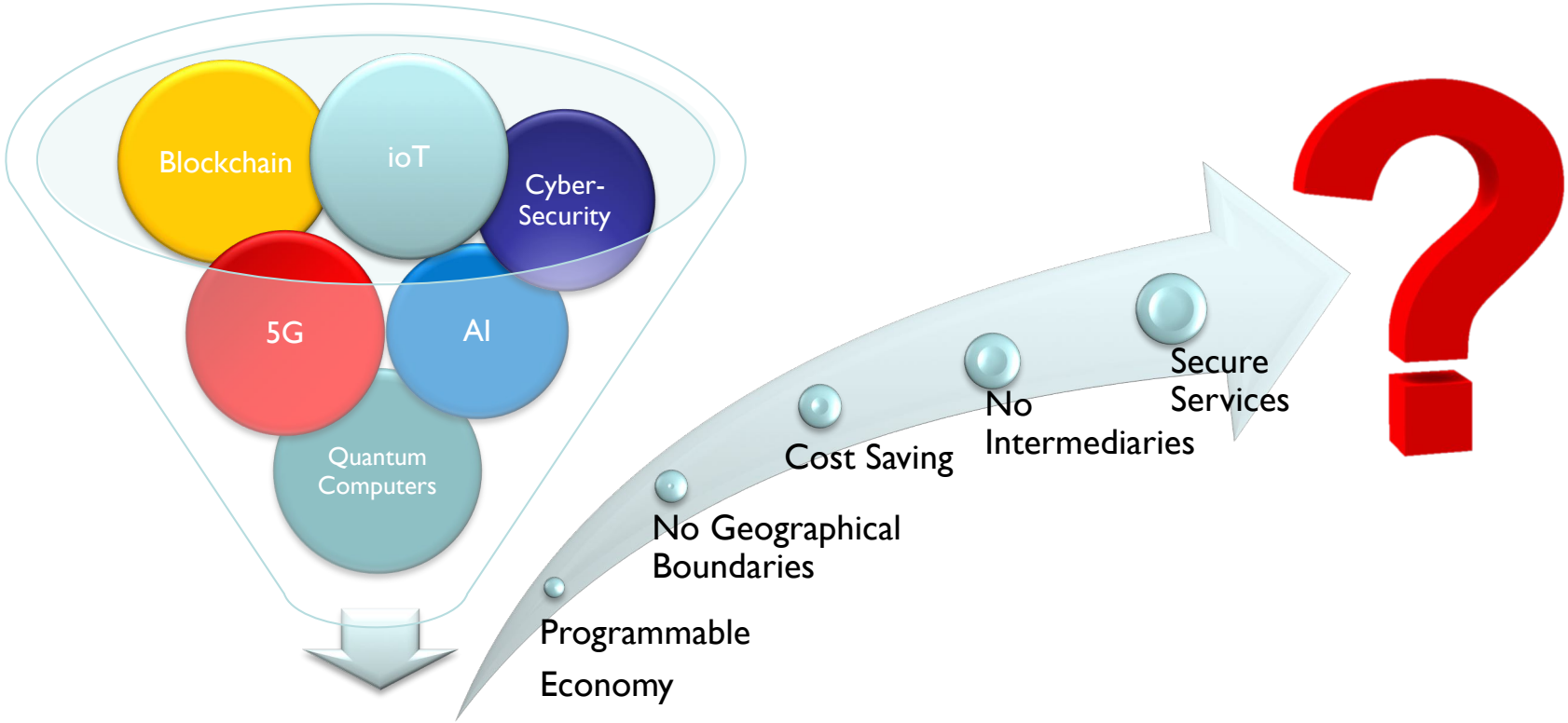
- Introduction to 4th Industrial Revolution: Digital Era
- Pillars of the 4th Industrial Revolution:
    - Quantum Computers / AI / 5G / IoT / CyberSecurity / Blockchain
- Blockchain
  - Basic concepts
  - Cutting out the middleman (Disintermediation)
  - Block validation process
  - Bitcoin and other cryptocurrencies
  - ICO explained
  - Main applications
  - Impact in Banking
  - Forecasting the future

4th Industrial Revolution: The Digital Era



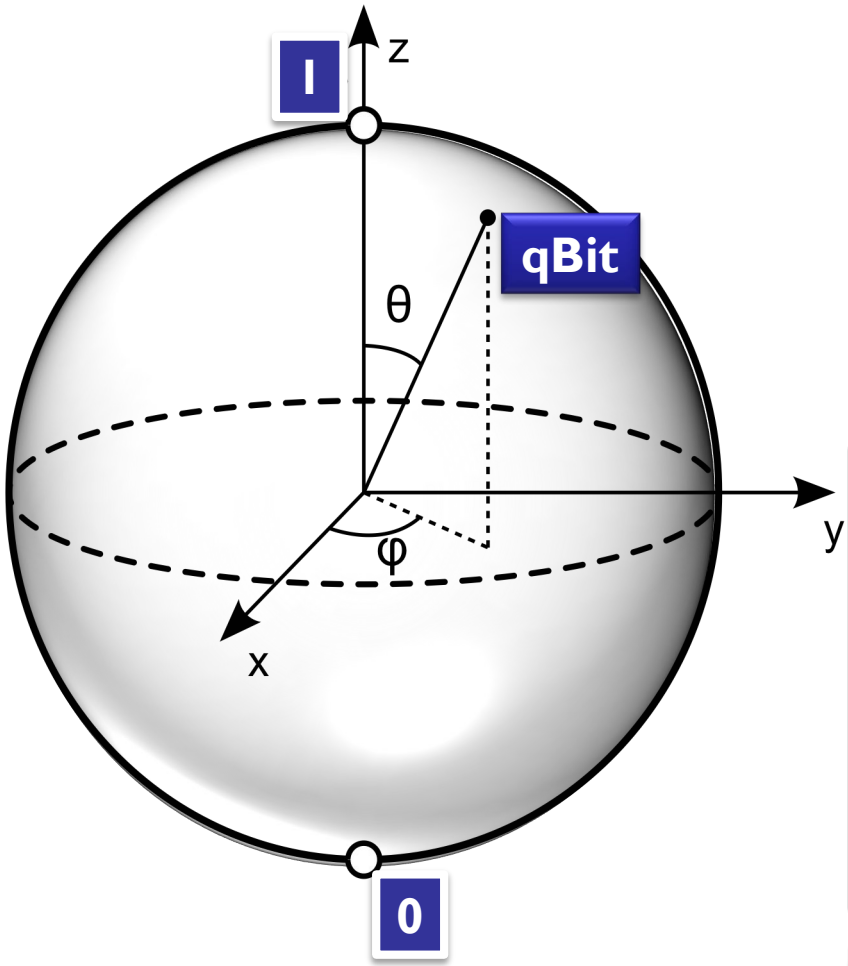
The 4 Industrial Revolutions (by Christoph Roser at AllAboutLean.com)

The Pillars of the New 4th Industrial Revolution

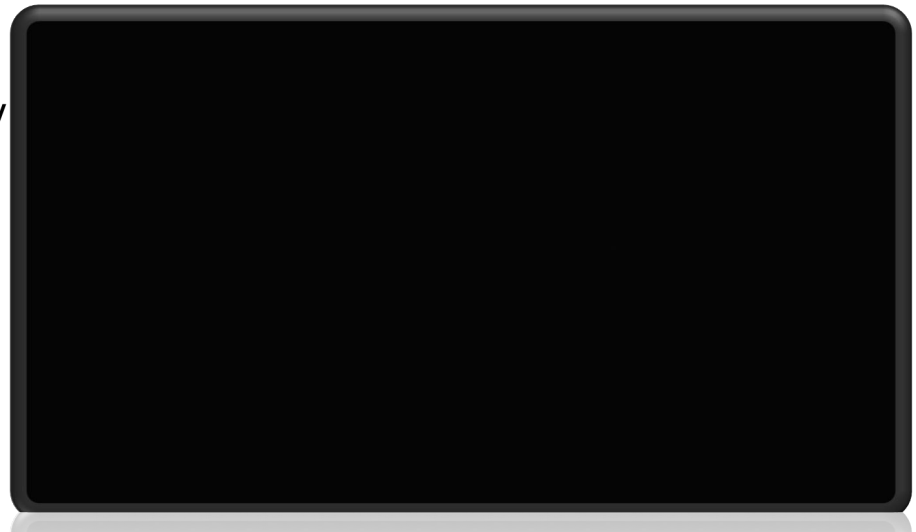


4th Industrial Revolution: Digital Era

Quantum Computers



Actual Computers: **2 ”qBits”**
2016: **5 qBits** for researchers (IBM)
2017: **20 qBits** for researchers (IBM)
2018+: **50 qBits** (IBM & Google)



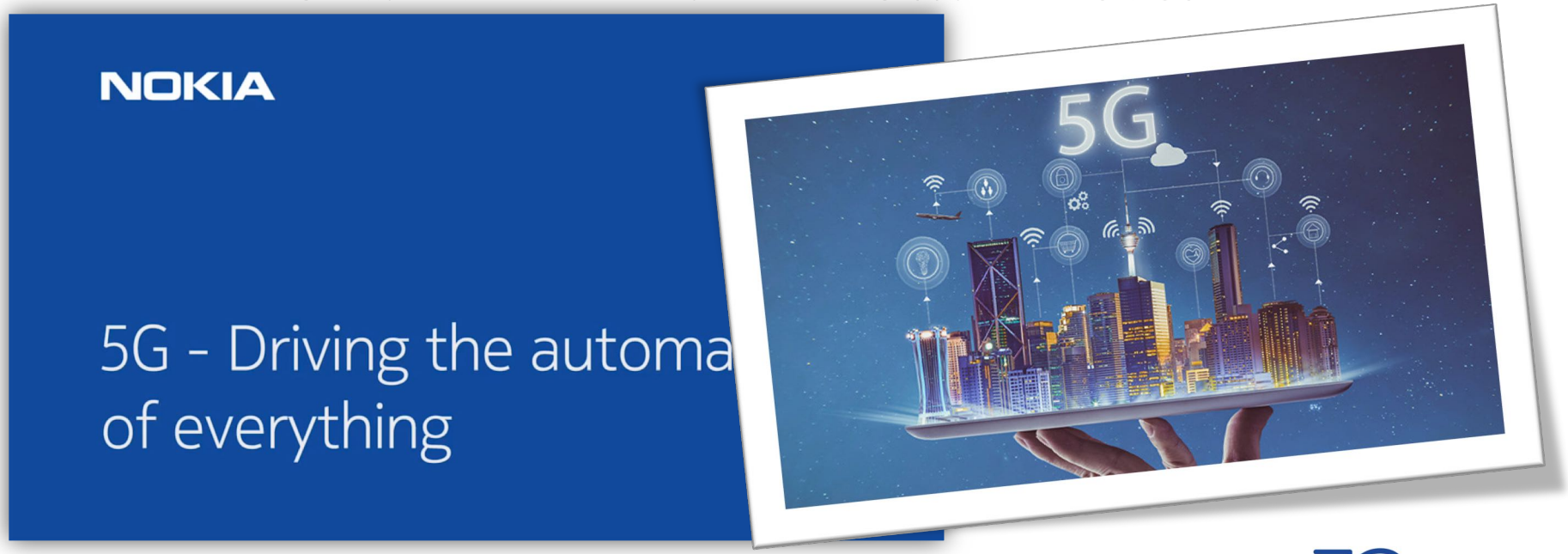
Q-Computer by IBM

AI: Artificial Intelligence

- Build Systems that "think" exactly like humans do

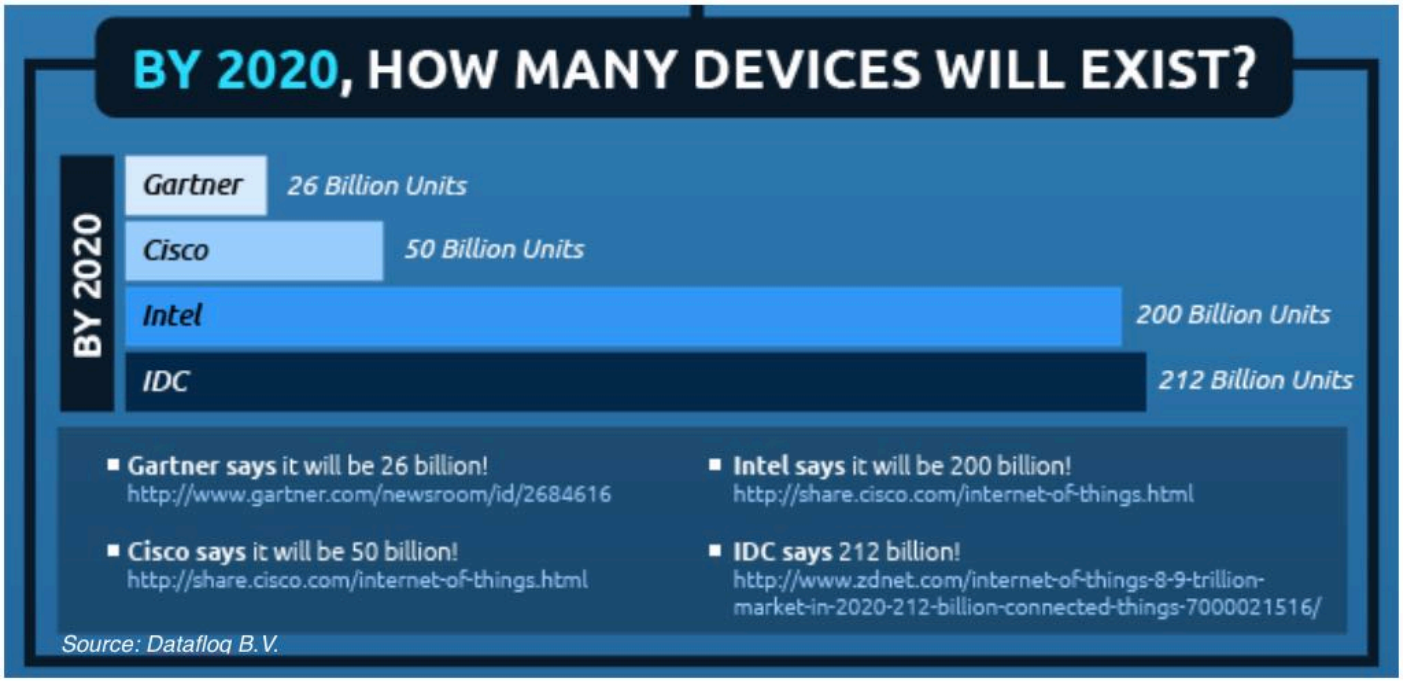
- Able to perform actions not being "programmed" by its creators

- High Speed like never before (1 Gbyte/sec)
- Low Latencies
- Example: Downloading HD movie (1-2 Gb):
  - Before: 10-15 min. - Now: 1-2 secs



IoT : Internet of Things

- The Internet of Things, or IoT, refers to billions of physical devices around the world that are now connected to the internet, collecting and sharing data



Smart TV Case: Too Smart?

- The policy explains that the TV set will be listening to people in the same room to try to spot when commands or queries are issued via the remote.

It goes on to say: "If your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party."

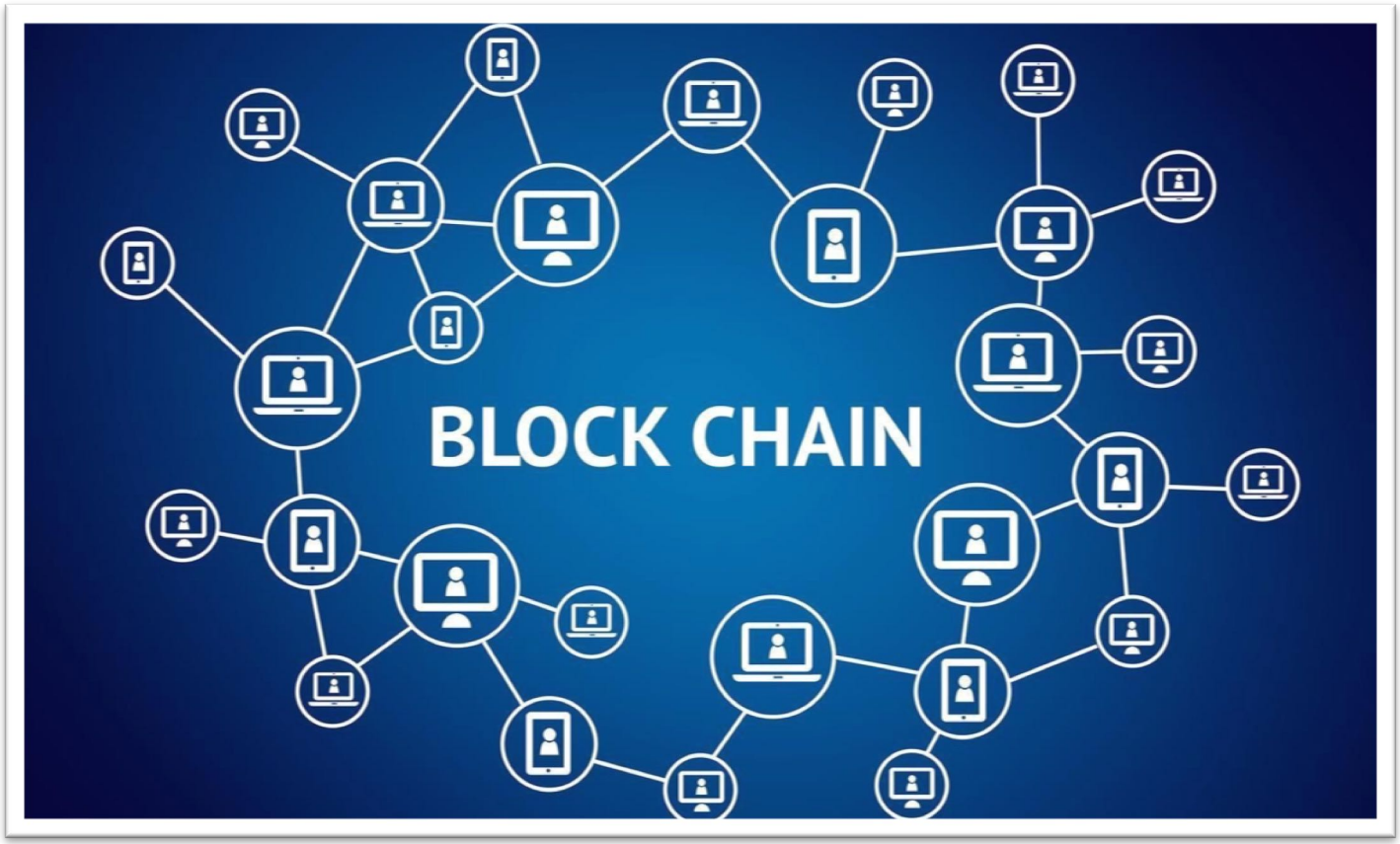
http://www.bbc.com/news/technology-31296188
Samsung Global Privacy Policy - Smart TV Supplement

Cyber-Security

- Ashley Madison
- 32 million accounts
- $115 million annual income
- €350,000 ransom rescue
- Hacked data:
  - Profile
  - Purchases
  - Credit card
  - Confidential information (pics, links, etc.)

Photograph by Philippe Lopez — AFP/Getty Images

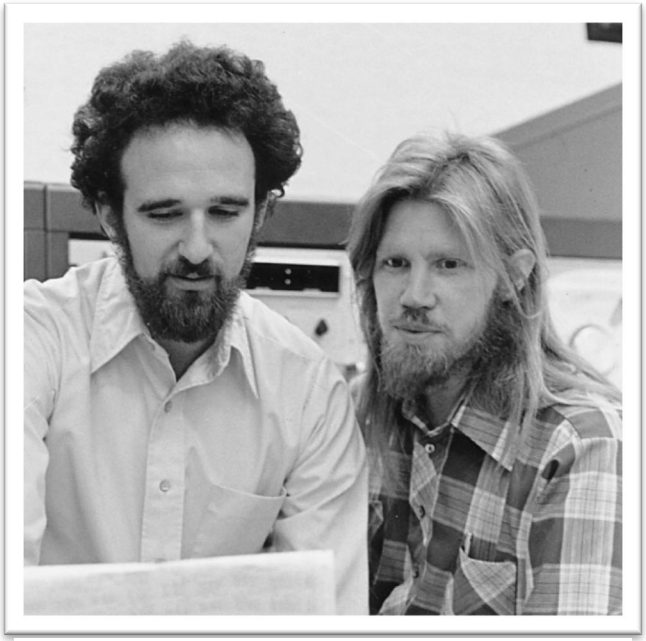
Cyber-Security: Examples


BLOCK CHAIN

Blockchain - Definition

- A blockchain, also known as a distributed ledger, is a new type of financial database whose records operate like transferable financial instruments
- Records are digital assets contained into Blocks
- Block (Nodes) are controlled by participants (each one has a full copy of all nodes in the Chain
- Each participant maintains a set of private keys
- Transaction is done between two parties that have to sign it with its private keys

Blockchain basics: Codification – Encryption & Integrity



Martin E. Hellman, left, and Whitfield Diffie in 1977. Source: Chuck Painter/Stanford News Service NYTimes

- **CODIFICATION**: from "human" language to "computer" language

  0 -> Binary: 011 0000

- **ENCRYPTION**: makes content access a great deal of difficulty (logarithm (elliptical) functions)

  $$X = logY_{\propto} \; mod \; q$$

  Y from X -> 400 operations

  X from Y -> 10^{30} operations

- **INTEGRITY**: raises a flag if content has been changed (hashing)

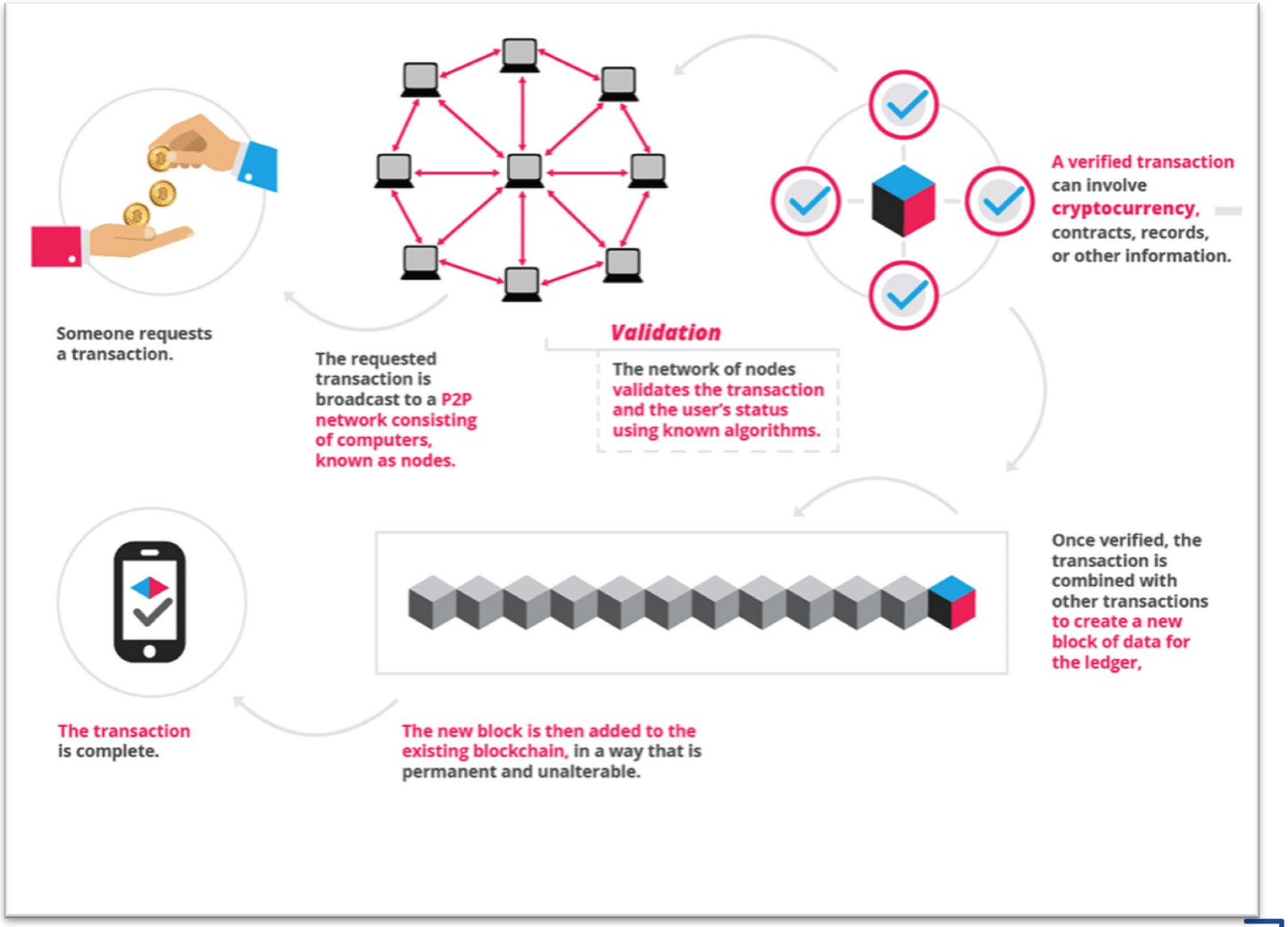
"Blockchain impact in Banking"
B98d4e82d294b3fa630f161a33bbd9c307e79d4ab2d69e01a7541ae999357f6f

"blockchain impact in Banking"
51137777e28bf149d8f915133374a5a2d5b599abdaef7c80247085aeaad3fbd3

Best Things in Life vs. Intermediaries…

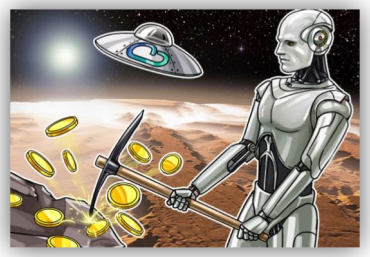
- Proof of identity
- Owning a house
- Having a Higher Education Degree, etc.

…and, if an intermediary was not necessary? : Blockchain



Key question: How a block is validated?

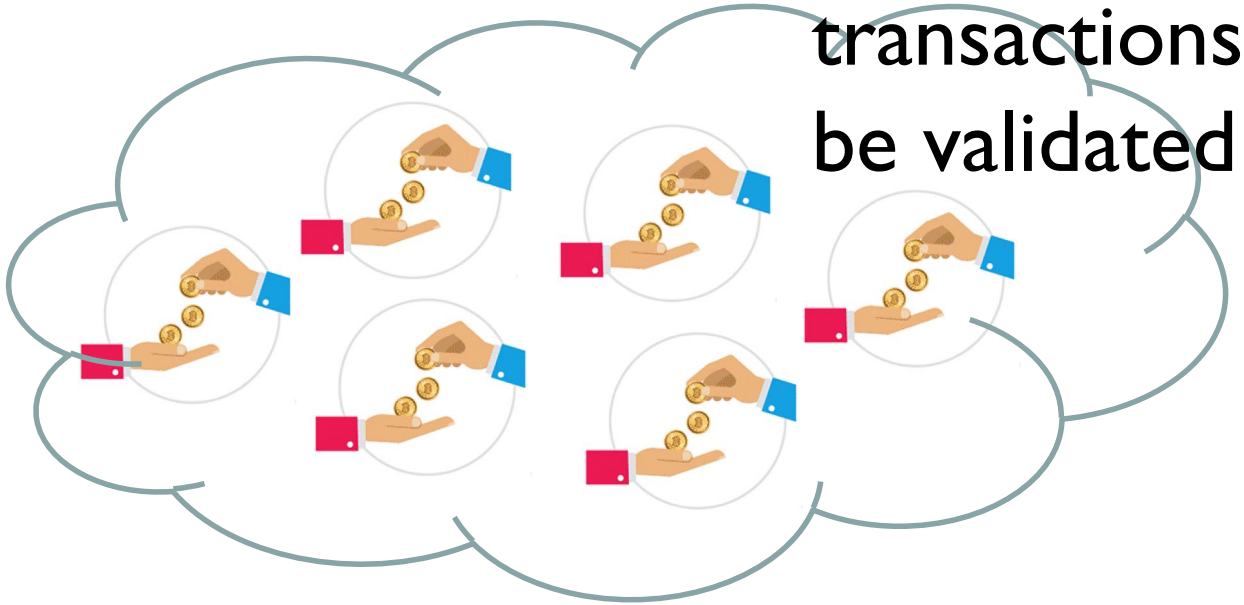
Validation = Proof-of-Work (creates a Block)



Validation Process:

Step 1:Seller and buyer agree into a transaction, and send it for validation

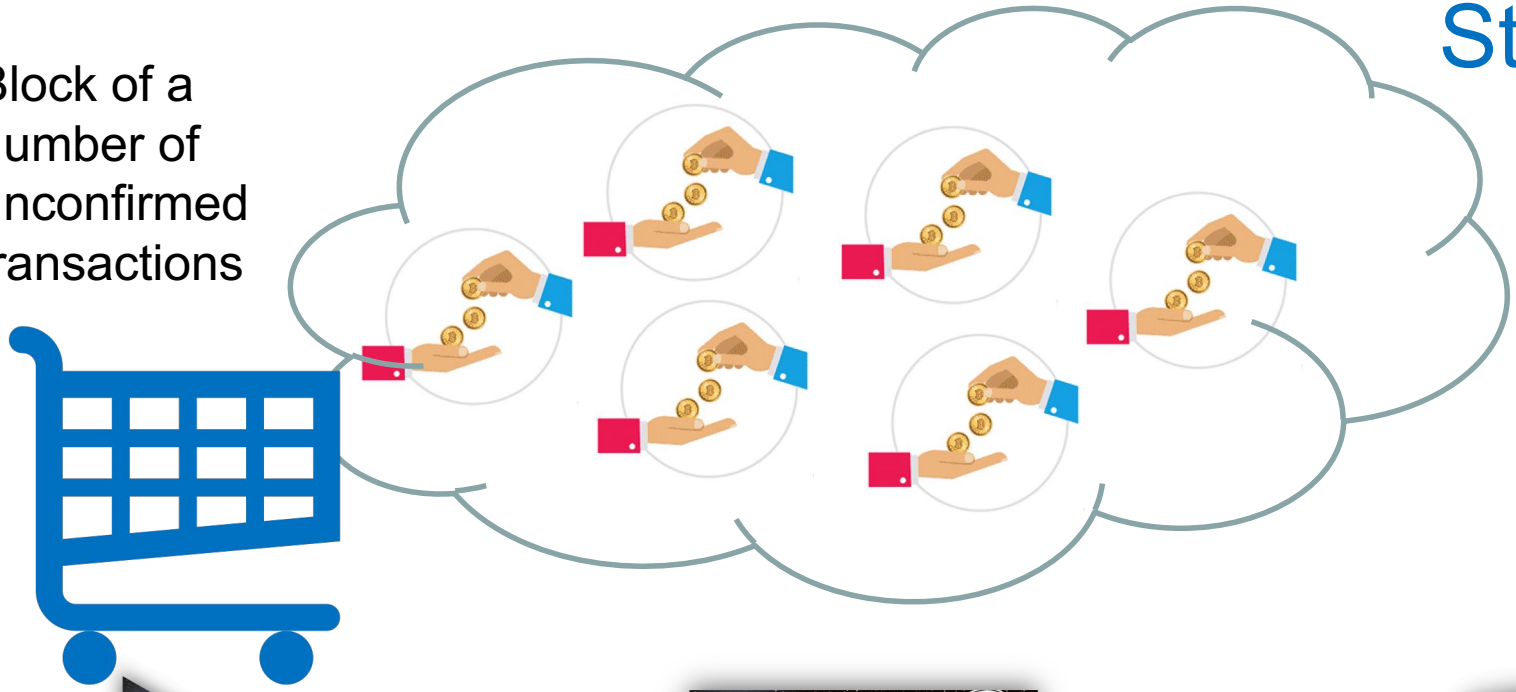
Step 2: Pool of transactions waiting to be validated



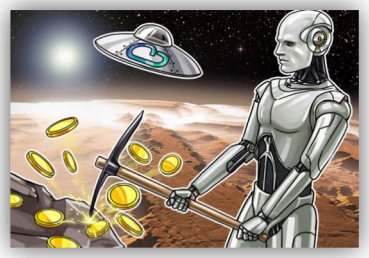
Validation Process

Step 3

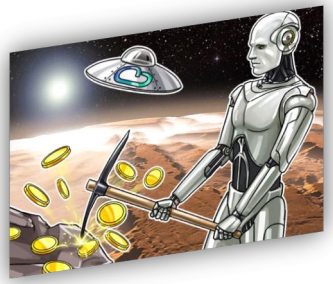
Block of a number of unconfirmed transactions



Miner 1 (or Node1)



Miner 2



Miner 3

Validation Process: Step 4

Step 4: Miner 1, using a predefined algorithm (hashing or **Merkle Root**), tried to transform the unconfirmed transaction's data (transaction's technical data or **Hash Input**) into a 32 bits hash starting with an specific number of zeros (mathematical solution or **Hash Output**).

The transaction's technical data alone won't necessarily have a mathematical solution. In order to achieve that, Miner1 will add a random number (called **Nonce**) to the transaction's technical data and will hope that then it will have a mathematical solution.

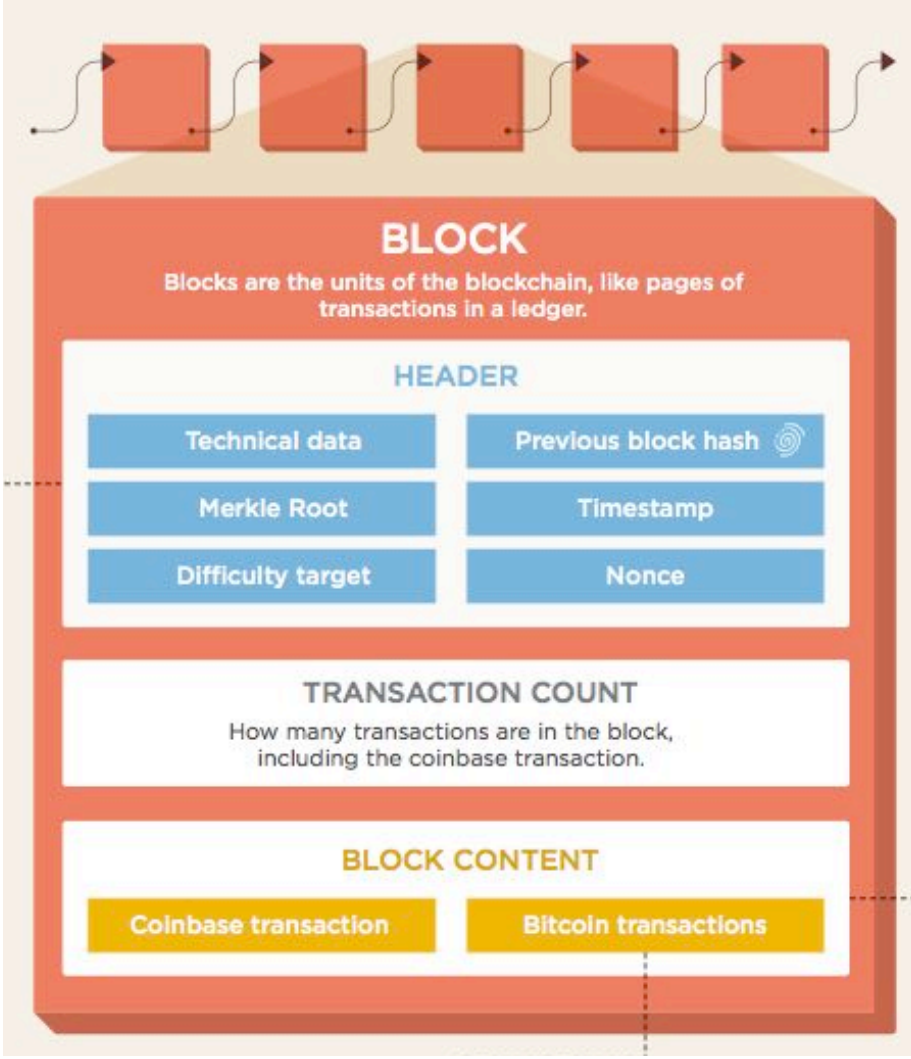
This trial and error effort cost time and money, and has to be remunerated (**Miner Fee**)

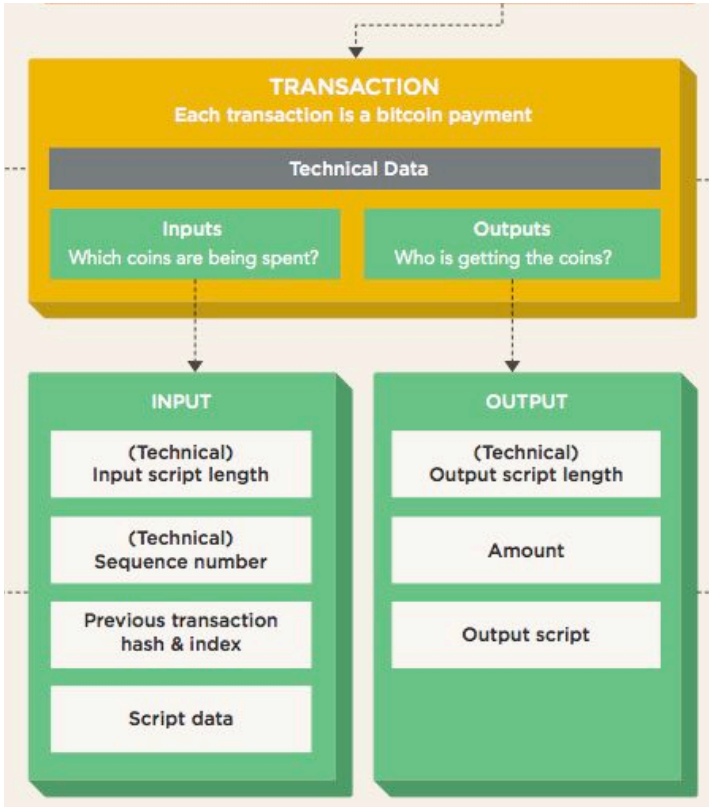
Step 5: When Hash Output is reached Miner 1 will broadcast this solution to all other Miners.

Step 6: Other Miners will check validity of Hash Output (**Proof of Work**), and in the transactions included by Miner1 in its newly created Block.

Step 7: If consensus is reached (51%+), the block gets added to the blockchain.

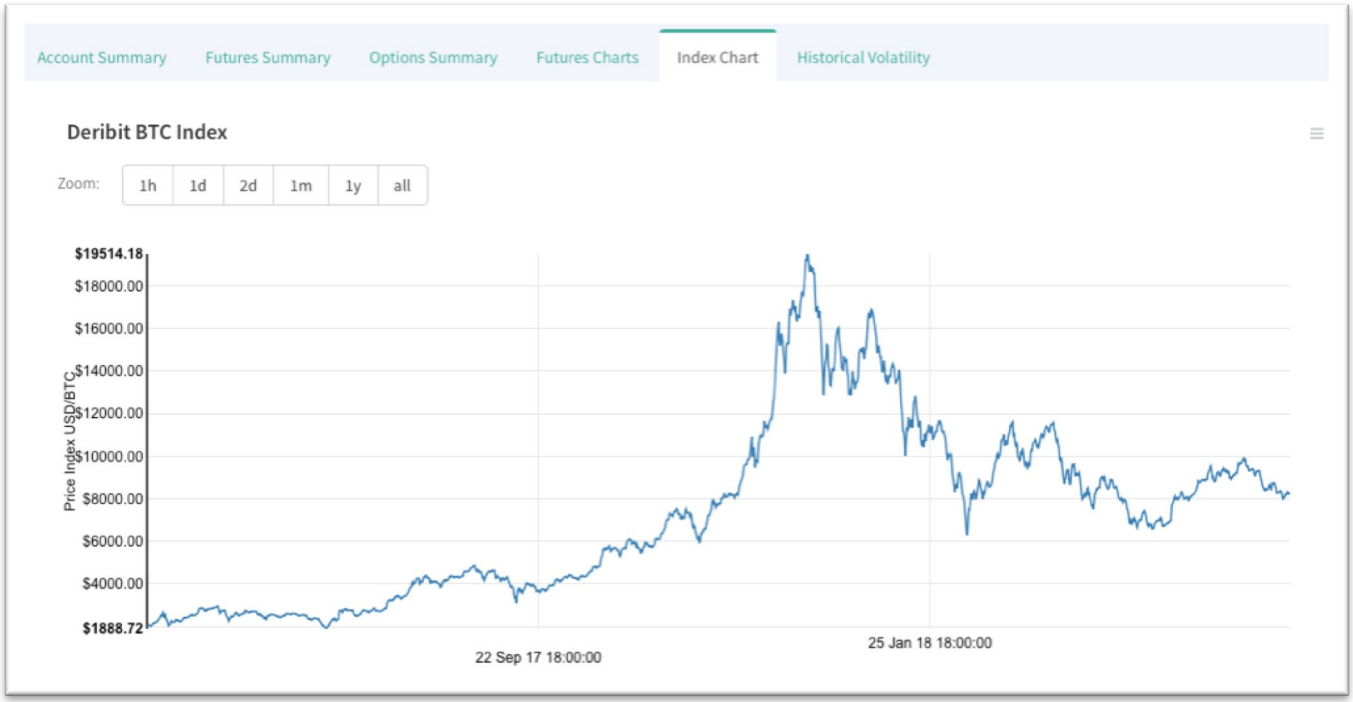
Inside a Block (bitcoin)



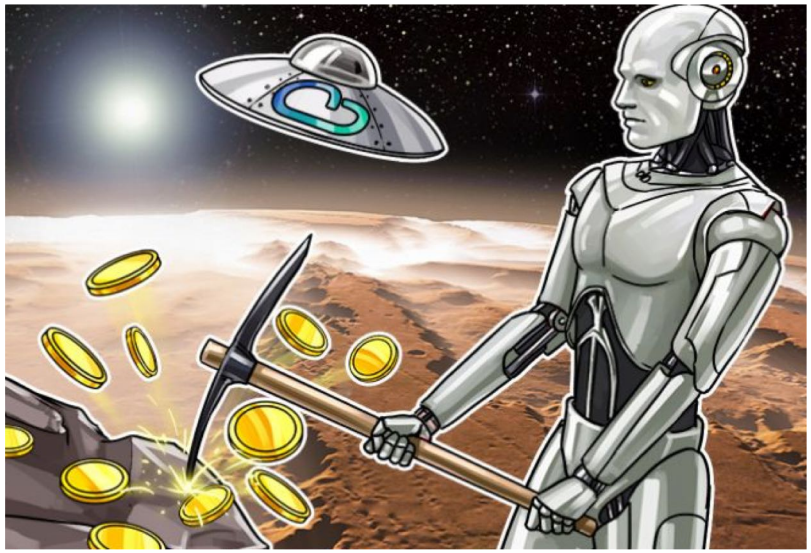


Blockchain & Bitcoin

- Born in 2008/2009 by (supposedly) Satoshi Nakamoto
- Market Cap: €138billion



Blockchain: Mining (& Remuneration)



Total Number of Bitcoins

A = Number of blocks in each n-series * Bitcoins per Block Remuneration

$$= \sum_{n=0}^{\infty} \frac{A}{2^n} \qquad = A * \frac{1}{1-1/2}$$

$$= \sum_{n=0}^{\infty} \frac{210,000 * 50}{2^n} = \frac{210,000 * 50}{1-1/2} =$$

$$= 21,000,000$$

Blockchain examples

Link: https://blockchain.info/es
Speed: 20 - 60 min
Cost / transaction: 1.58 $

Link:
https://live.blockcypher.com/ltc/
Speed : 2,5 min
Cost / transaction : 0,19 $

ethereum

Link: https://etherscan.io/
Speed : 14 s
Cost / transaction : 0,49 $

Link: https://ripple.com/build
Speed : 3,5 s
Cost / transaction : 0,0056 $

ICO: Initial Coin Offering

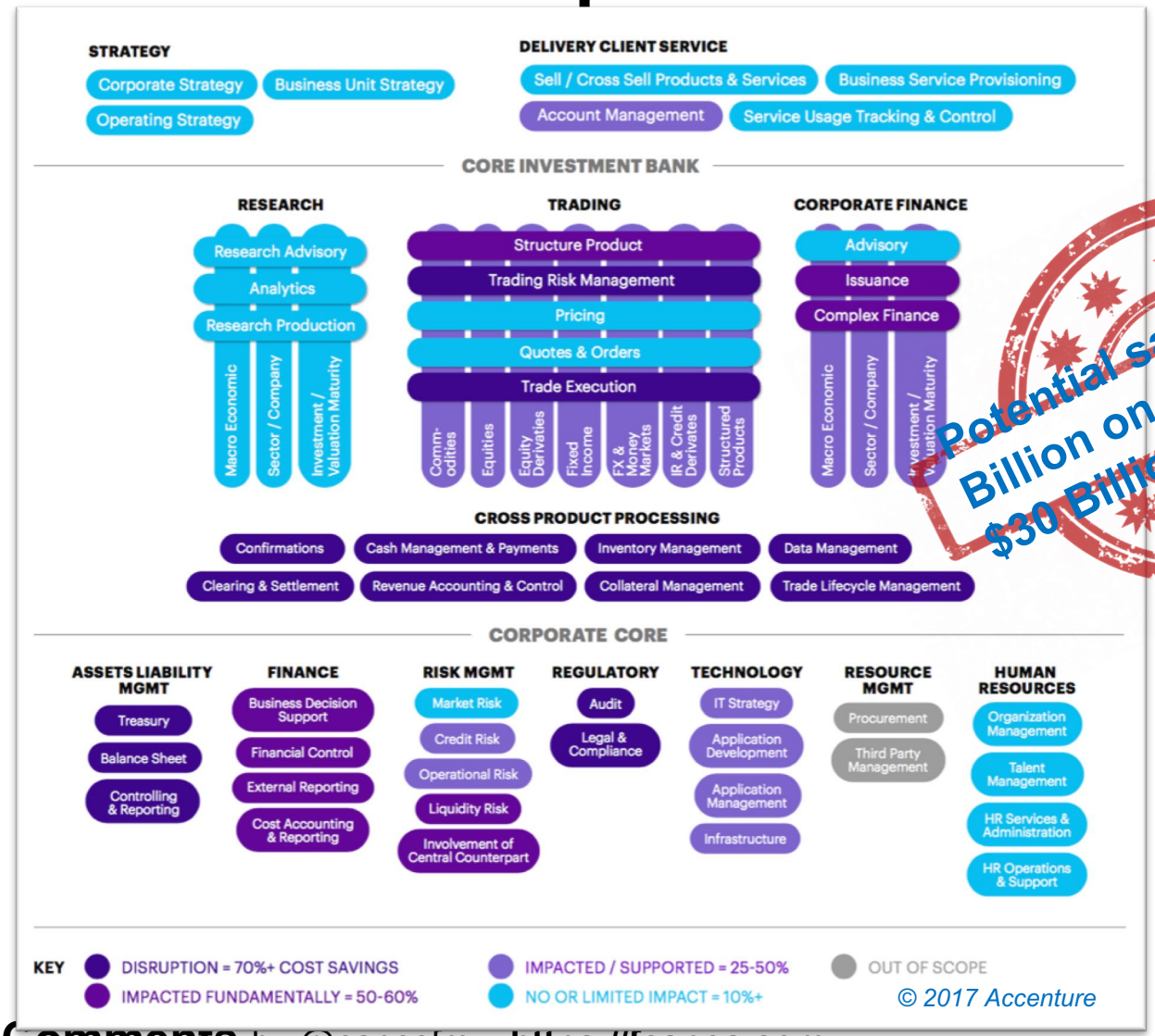
- An unregulated means by which funds are raised for a new cryptocurrency venture
- An Initial Coin Offering (ICO) is used by startups to bypass the rigorous and regulated capital-raising process required by venture capitalists or Banks
- In an ICO campaign, a percentage of the cryptocurrency is sold to early backers of the project in exchange for legal tender or other cryptocurrencies, but usually for Bitcoin.

Source: Investopedia https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp#ixzz5G2ZkBTpl

Do you want to invest in an ICO?

- Sign-in into newsletter, Telegram, etc. (sources of notification)
- Apply to Whitelist (and KYC)
- Bounty Programs, Airdrops
- Pre-sale – Bonus
- Day of the ICO– GAS War
- Tokens blocked / returned
- Exchange Listed

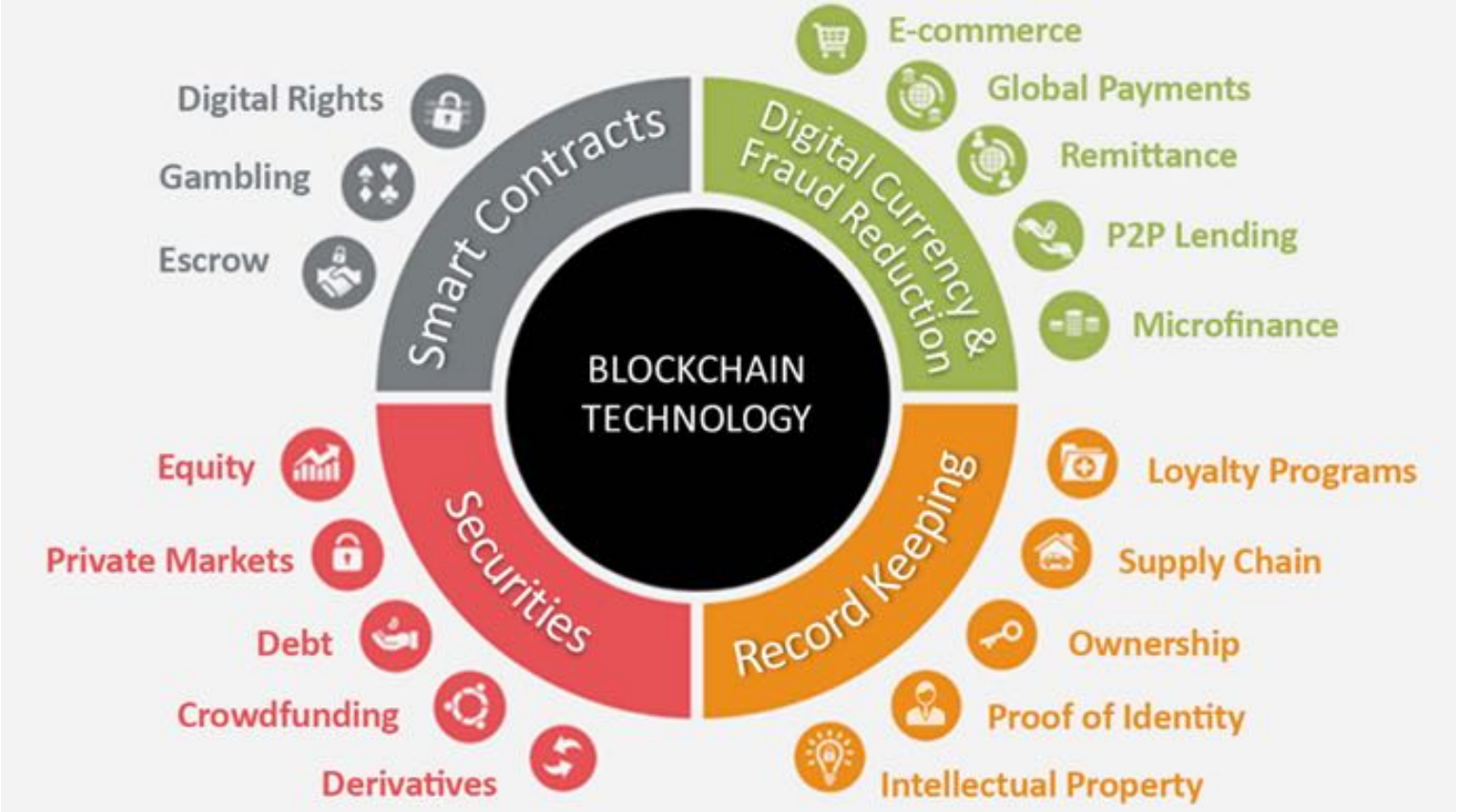
Blockchain impact in banking



Potential savings of $8 Billion on a cost base of $30 Billion

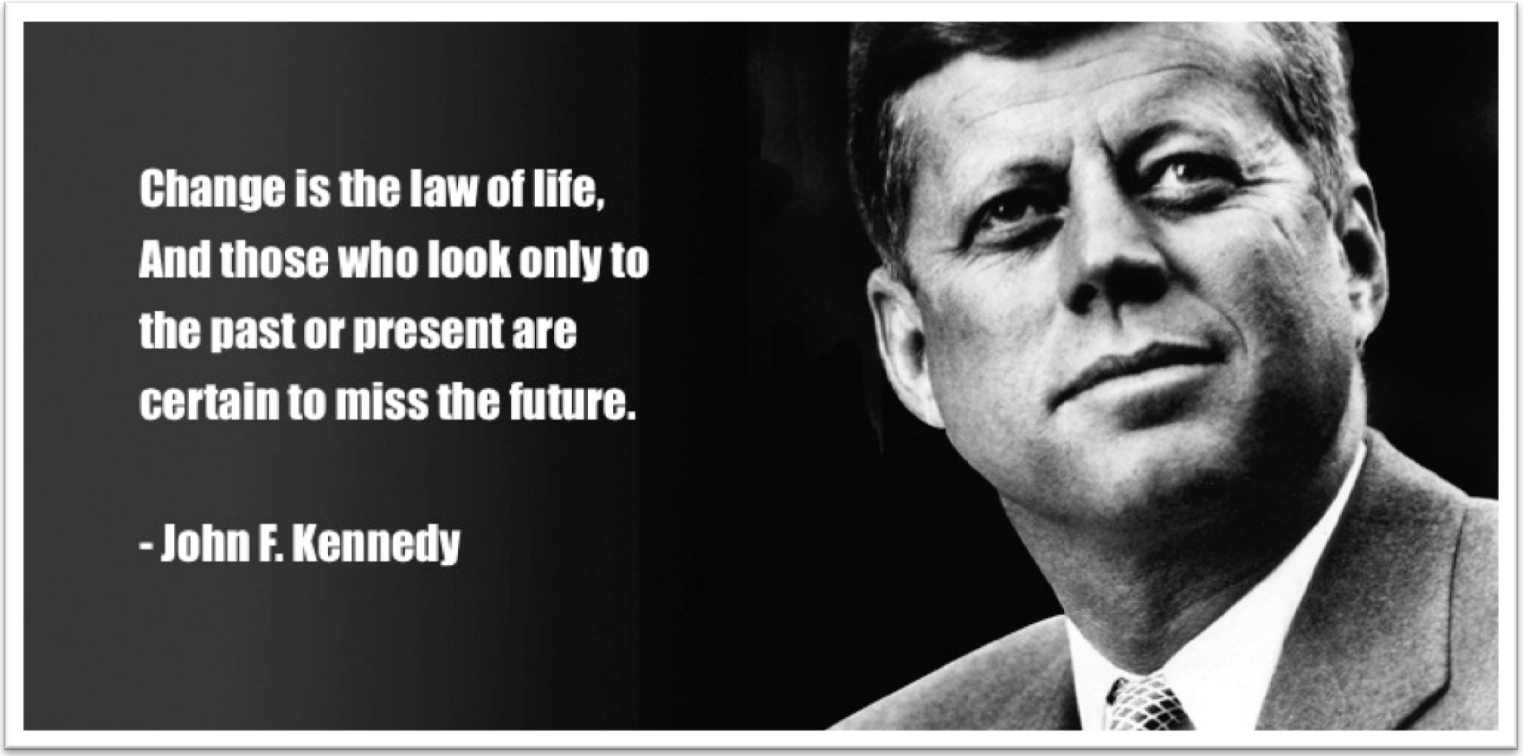
Forecasting the future

Blockchain: Main applications



© 2017 www.aciworldwide.com

Thanks


Change is the law of life,
And those who look only to
the past or present are
certain to miss the future.
- John F. Kennedy

Sources & References

- Nokia: 5G Driving the Automatization of everything
- Investopedia: Initial Coin Offering
- Chris McCann: Guide to launching an Initial Coin Offering (ICO)
- abc (News10): Smart TV, too Smart?
- AFP/Getty Images
- ATLAS: Data Cynosure Prime
- Datafloq B.V.
- Whitfield Diffie & Martin E. Hellman, member IEEE "New Directions in Cryptography" (IEEE Transactions on Information Theory, vol. IT-22, No. 6, November 1976)
- The 4 Industrial Revolutions by Christoph Roser at AllAboutLearn.com
- LiteCoin: Link: https://live.blockcypher.com/ltc/
- BitCoin: Link: https://blockchain.info/es

Sources & References

- Ethereum: Link: https://etherscan.io/
- Ripple: Link: https://ripple.com/build
- Blockgeeks: What is Blockchain Technology?
- Inside Bitcoin's blockchain: www.bitsonblocks.net
- Accenture
- Citigroup
- Nasdaq
- Gartner
- The Wall Street Journal
- www.aciworldwide.com
- IBM: IBM Research Quantum Computers