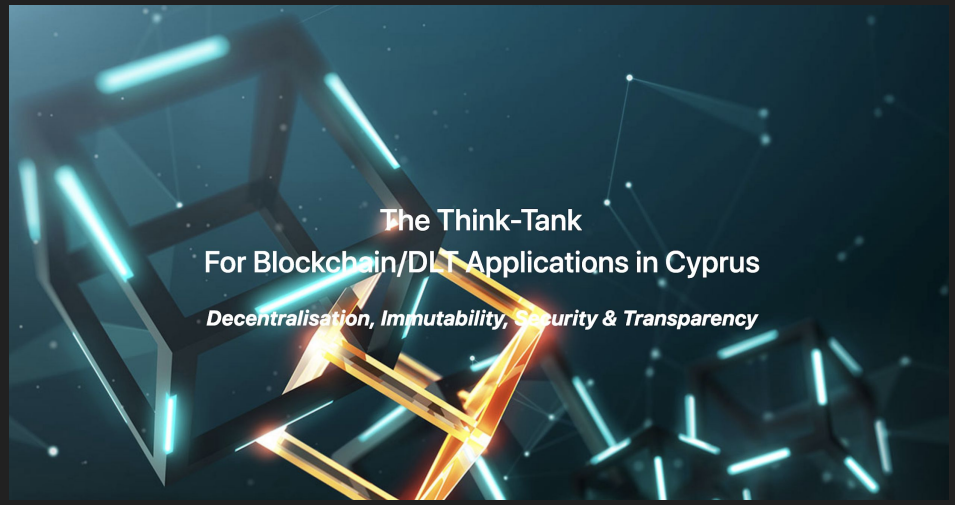
Blockchain, DLTs: Benefits & Challenges

Dr Theodosis Mourouzis

Cyprus Blockchain Technologies

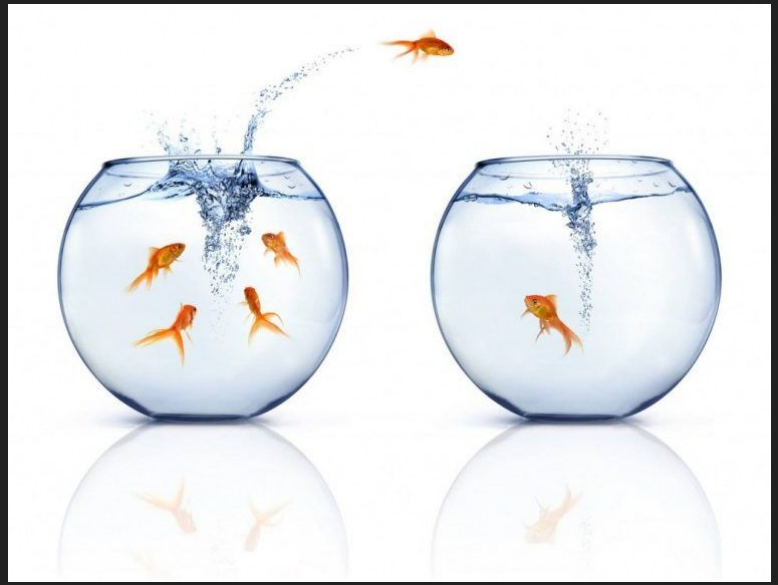


Members

CYPRUS INTERNATIONAL INSTITUTE OF MANAGEMENT
Τράπεζα Κύπρου
KMG CAPITAL MARKE
UCL CBT
HELLENIC BANK
Grant Thornton
An instinct for growth™
UNIVERSITY of NICOSIA
PumaPay
ORACLE
EY
KINANIS LAW FIRM
KPMG Cyprus
JCC PAYMENT SYSTEMS

What is Blockchain?

- Another emerging technology....
- Emerging technologies are technologies that are perceived as capable of challenging/changing the status quo



Emerging Technologies

- Always same characteristics

  - (relatively) fast growth

  - virality at very early stages

  - radical novelty

  - disruptive

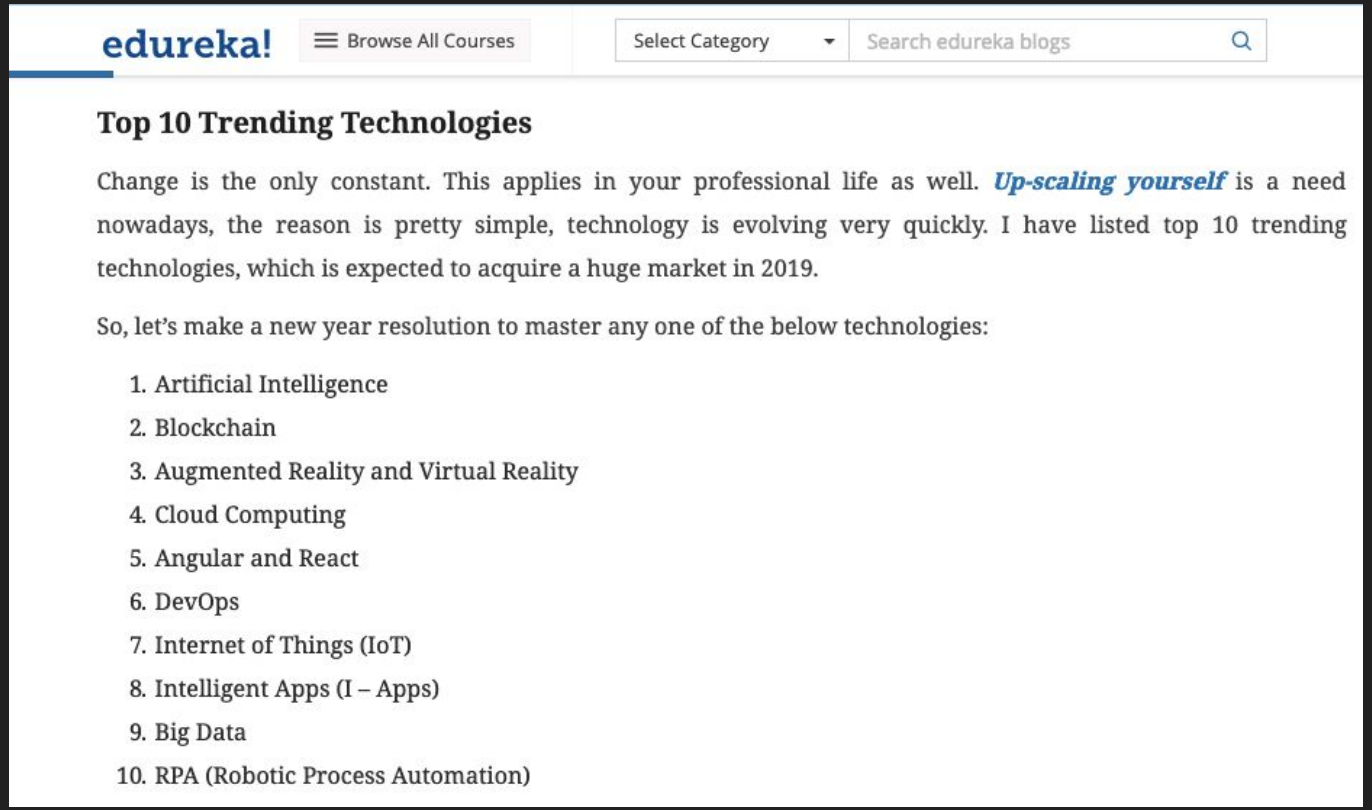
  - prominent (future) impact

  - uncertainty

  - ambiguity

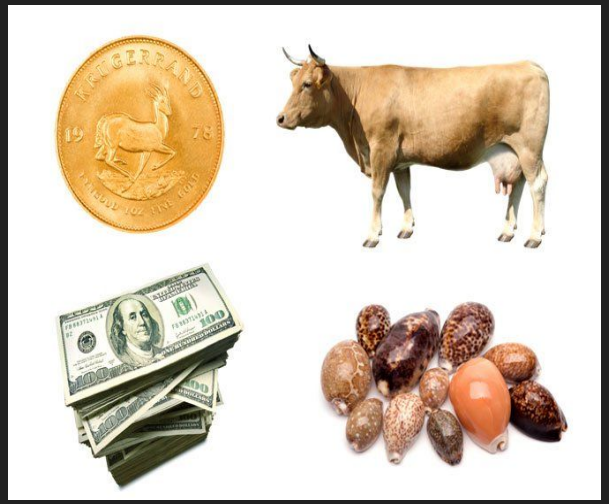
  - scrutiny

Emerging Technologies



Blockchain Behind Bitcoin

- Firstly appeared as the accounting ledger of Bitcoin Cash System
- Historical evolution of research towards e-cash systems



1980	**Hash tree** for digital signature - Merkle tree (Ralph Merkle, 1979)
	Hash chain for secure login (Leslie Lamport 1981)
1990	e-Cash, first crypto currency, **electronic cash for payments** (David Chaum 1991)
	Hash chain for Unix login application with one-time passwords (Neil Haller 1994)
	Electronic payments with a hash chain (Thorben Petterson 1995)
1995	n-Count a **hash chain for electronic cash** (Chris Stanform & Eduard de Jong 1995)
	ayWord a **hash chain for electronic payments** (Ron Rivest & Adi Shamir 1995)
1997	Hashcash – **proof of work** (Adam Back 1997)
2008	**Bitcoin** (Satoshi Nakamoto 2008)

http://networkcultures.org/moneylab/2015/12/15/eduard-de-jong-a-short-history-of-the-blockchain/

Basic Ingredients behind Blockchain

- **Cryptography**
  - Immutability via hash functions & cryptographic sealing
  - Ownership and double-spending avoidance via hashing & digital signatures
- **Distributed Systems**
  - P2P Architectures
  - Byzantine Fault Tolerance and Consensus Algorithms
- **Economics & Game theory**
  - **Incentives for alignment of stakeholders**

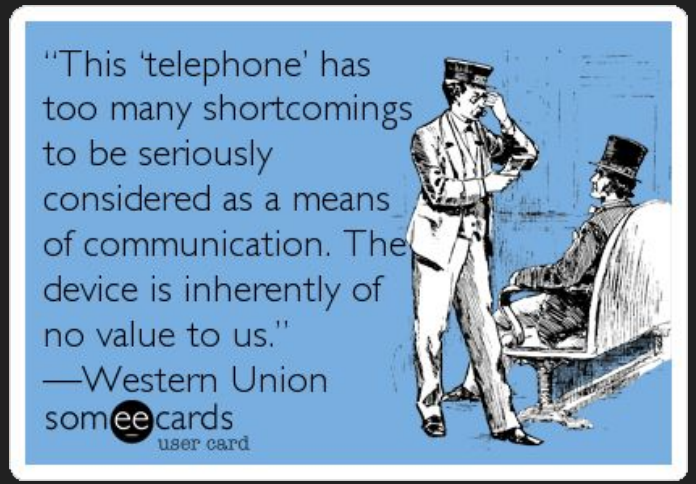
Emerging Technologies: Highly Scrutinized

- When a new technology appears there is always a battle between two groups: **Technology Evangelists** *vs* **The Haters/Opponents**

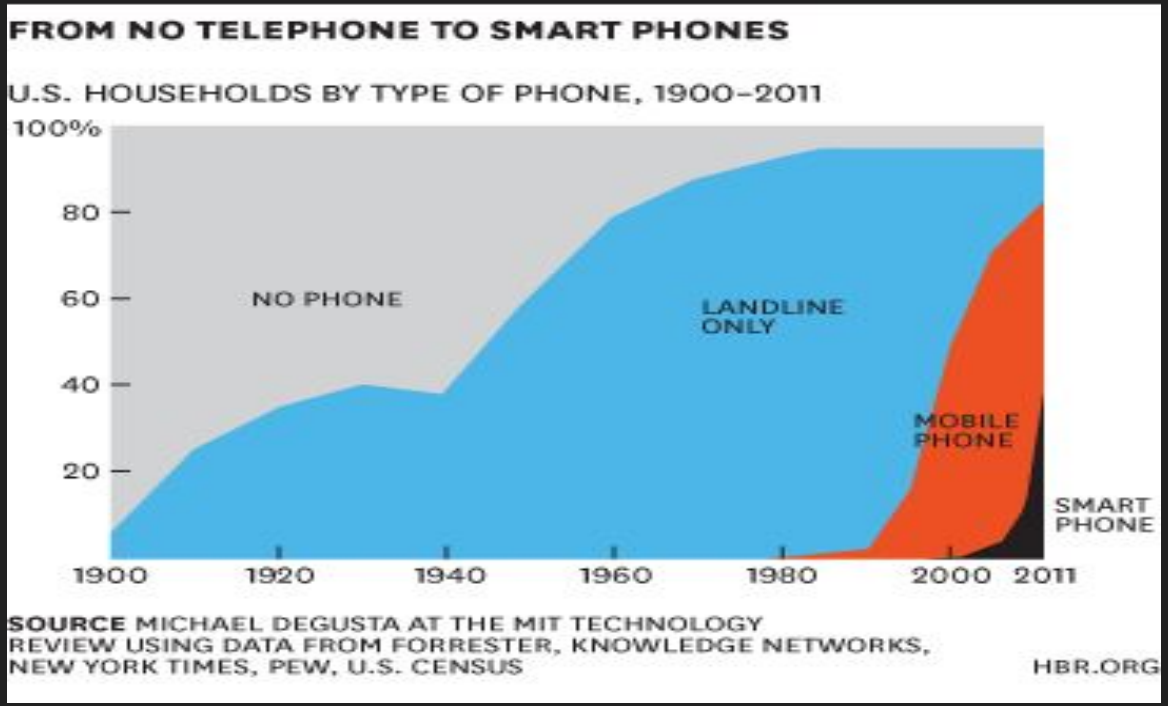
- Nobody 100% correct … Nobody 100% wrong!
- What is the usual result? Well it varies …
- But let's go back in history a bit and see...

Case 1: Telephone

- **1876:** "The Americans have need of the telephone, but we do not. We have plenty of messenger boys." — William Preece, British Post Office.
- **1876:** "This 'telephone' has too many shortcomings to be seriously considered as a means of communication." — William Orton, President of Western Union.



Case 1: Telephone

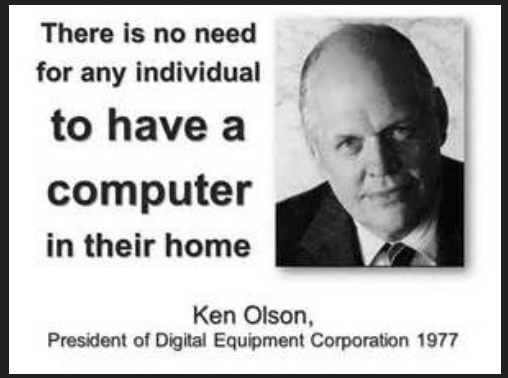


Case 2: Computers

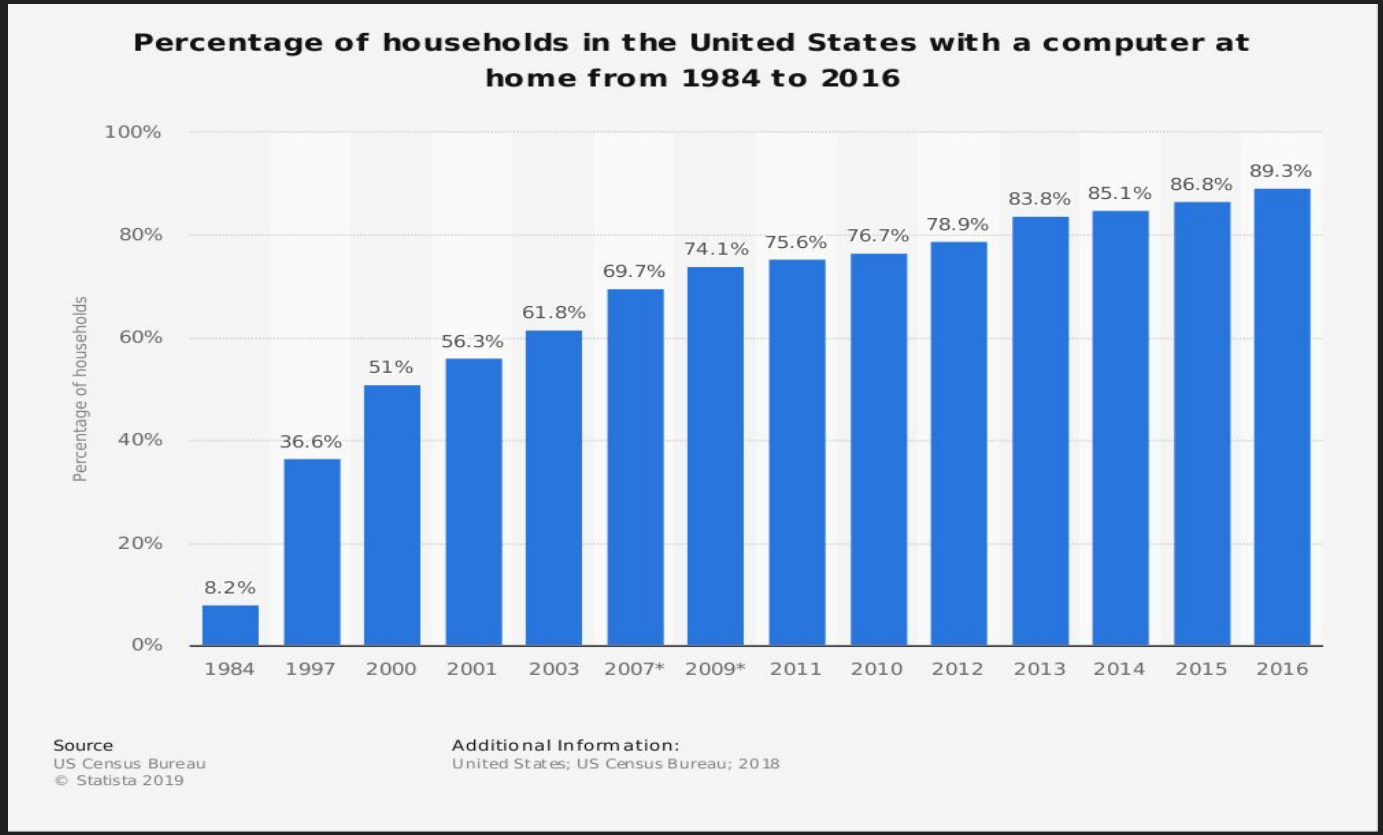
History of Computers

Famous Quotes about Computers

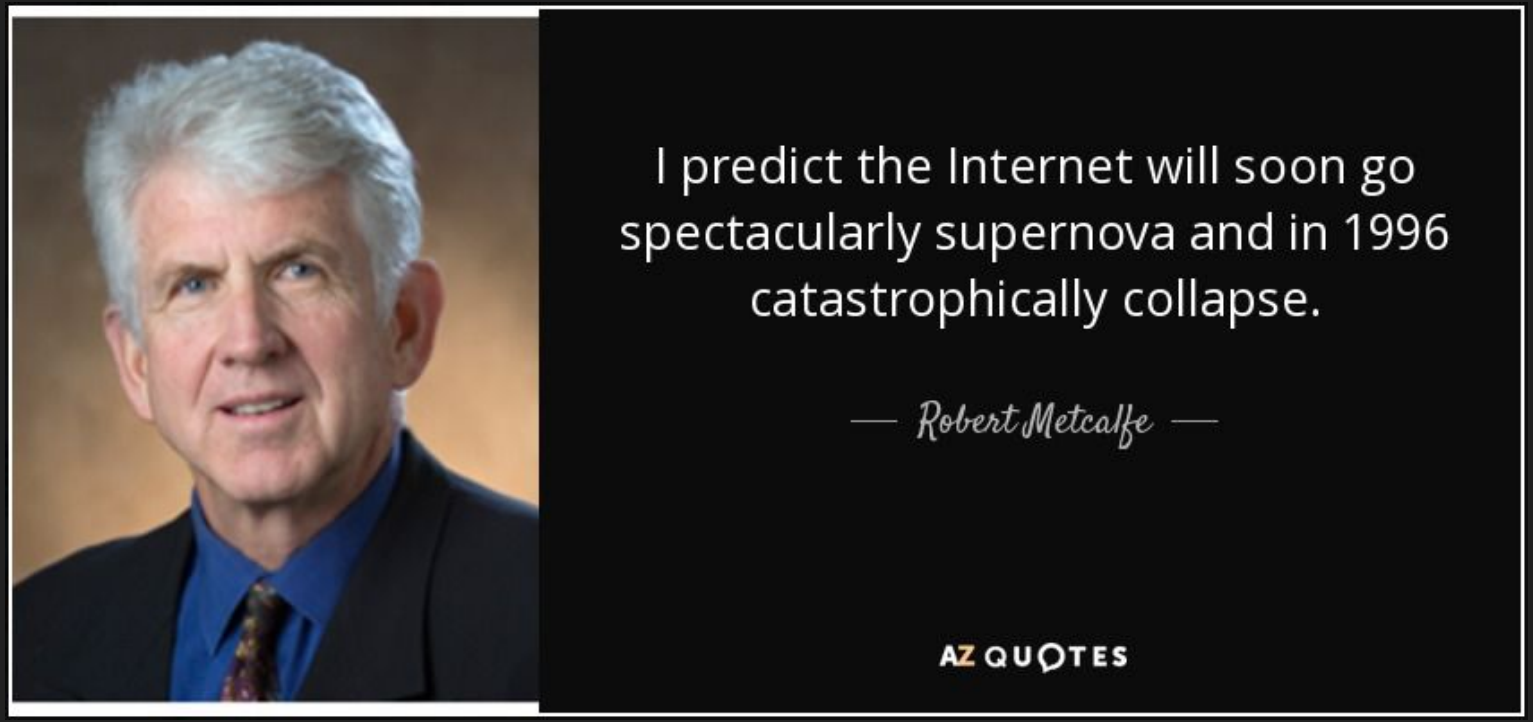
- "I think there is a world market for maybe five computers." – Thomas Watson, chairman of IBM, 1943
- "Computers in the future may weigh no more than 1.5 tons." – Popular Mechanics, 1949
- "There is no reason anyone in the right state of mind will want a computer in their home." – Ken Olson, President of Digital Equipment Corp, 1977.



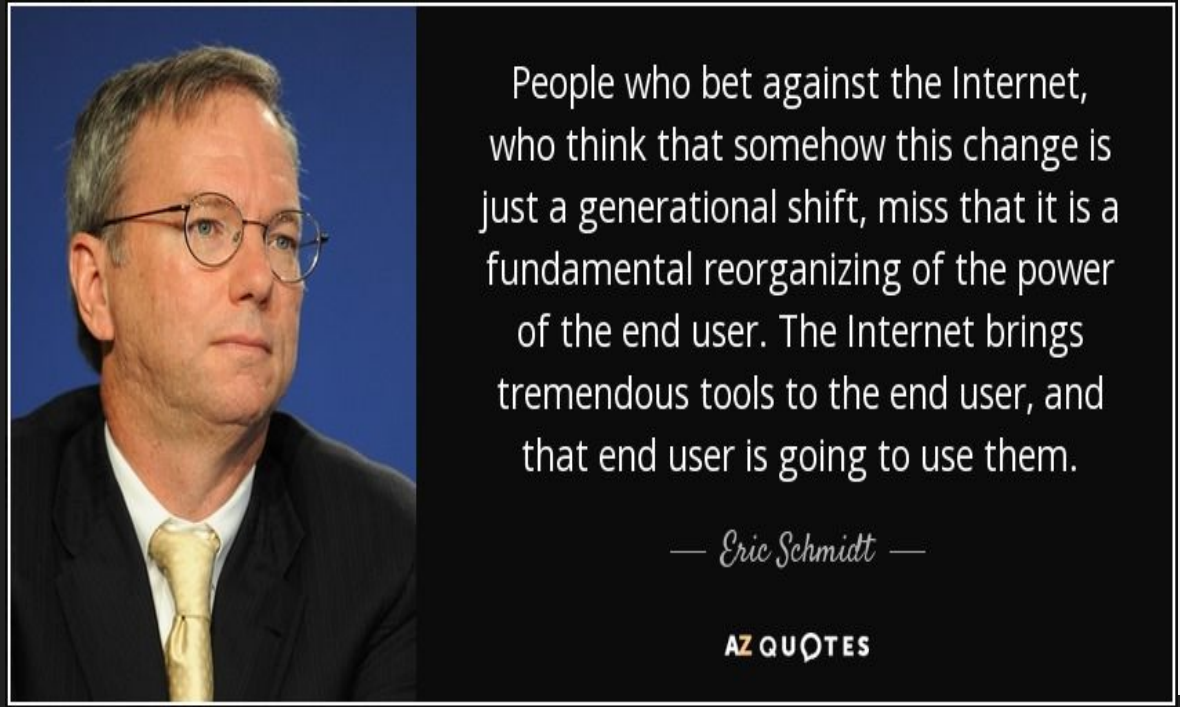
Case 2: Computers

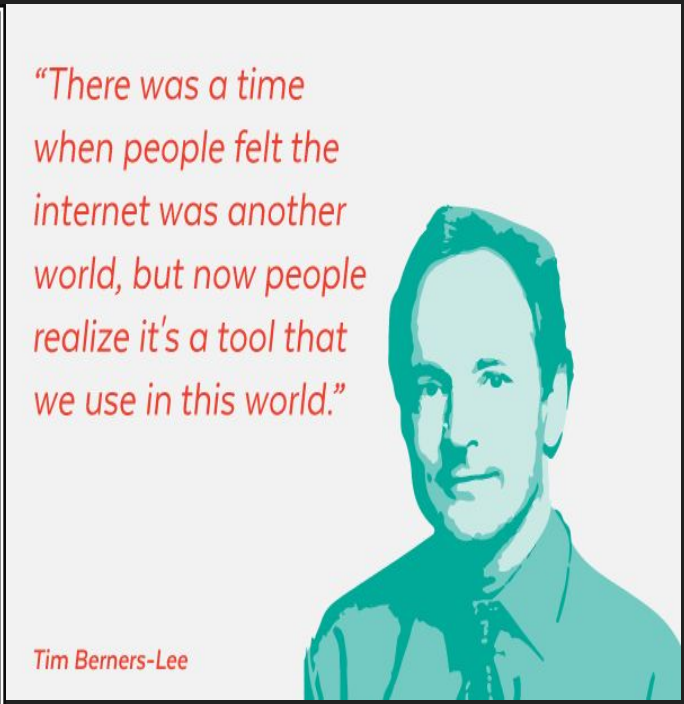


Case 3: The Internet

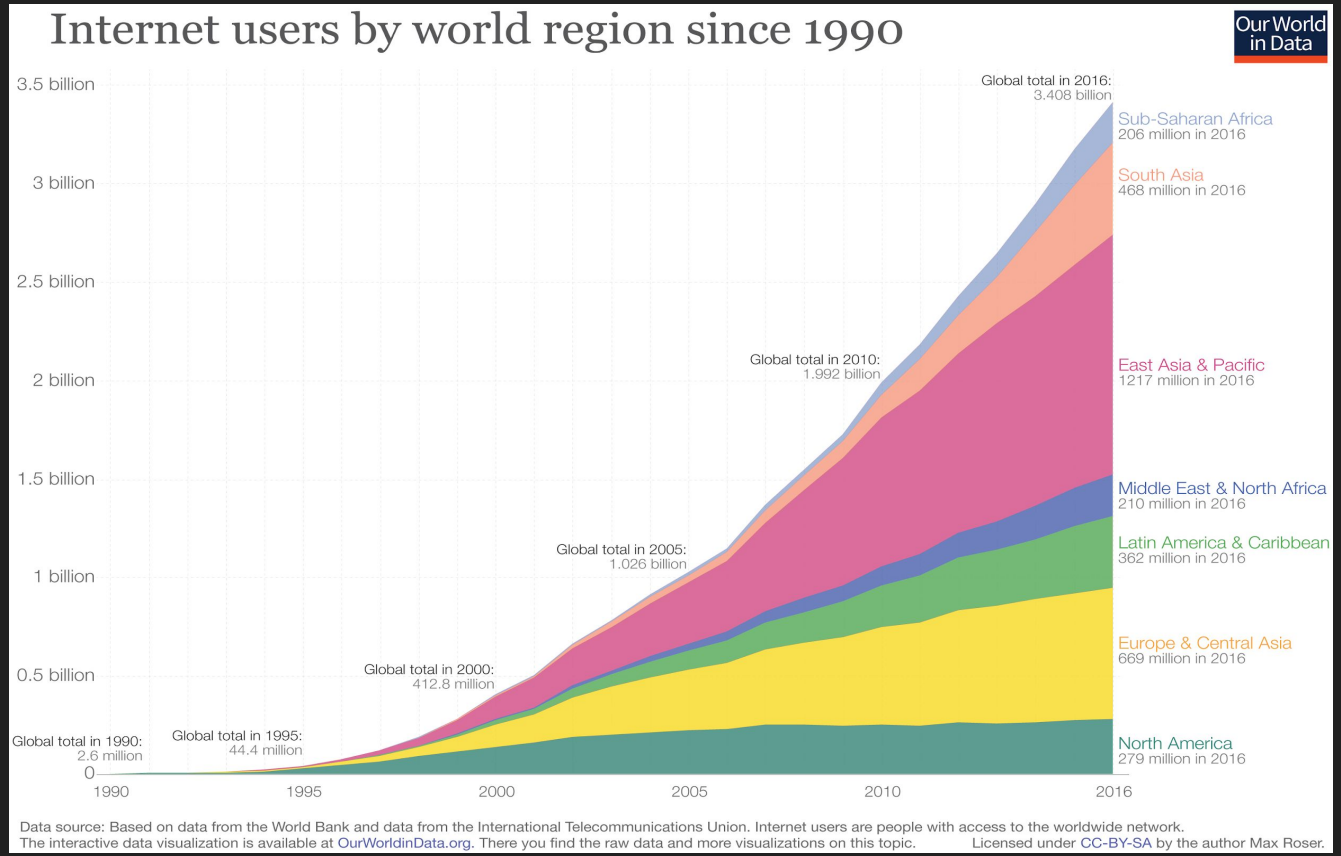


Case 3: The Internet





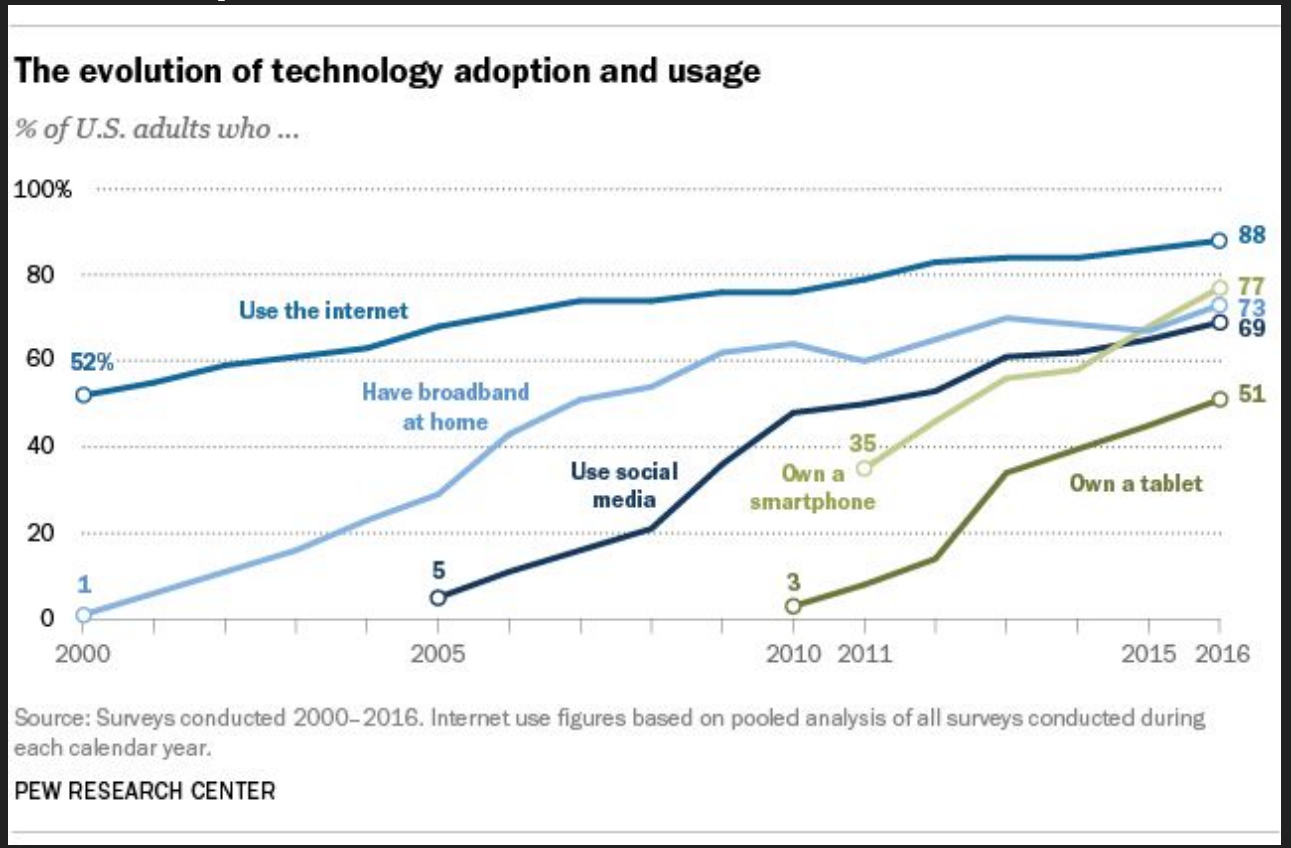
Case 3: The Internet



Case 4: Smartphones

- **2006:** "Everyone's always asking me when Apple will come out with a cell phone. My answer is, 'Probably never.'" — David Pogue, The New York Times.
- **2007:** “There’s no chance that the iPhone is going to get any significant market share.” — Steve Ballmer, Microsoft CEO.

Case 4: Smartphones



Case 5: Encryption

Case 5: Encryption

Encryption...is a powerful defensive weapon for free people. It offers a technical guarantee of privacy, regardless of who is running the government... It's hard to think of a more powerful, less dangerous tool for liberty.

— Esther Dyson —

AZ QUOTES

So end-to-end encryption, keeps things encrypted and that means that law enforcement, without a warrant, cannot read that information.

— Rod Beckstrom —

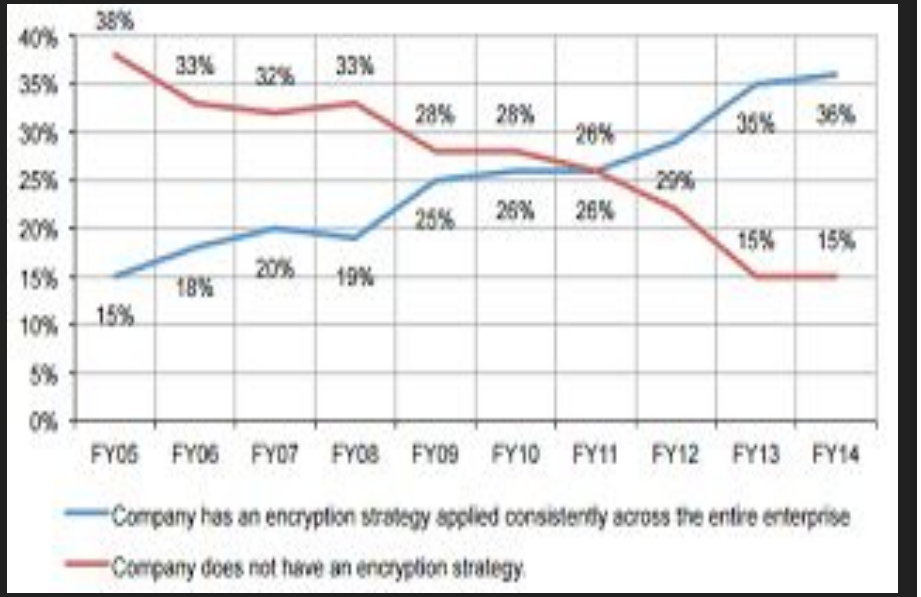
AZ QUOTES

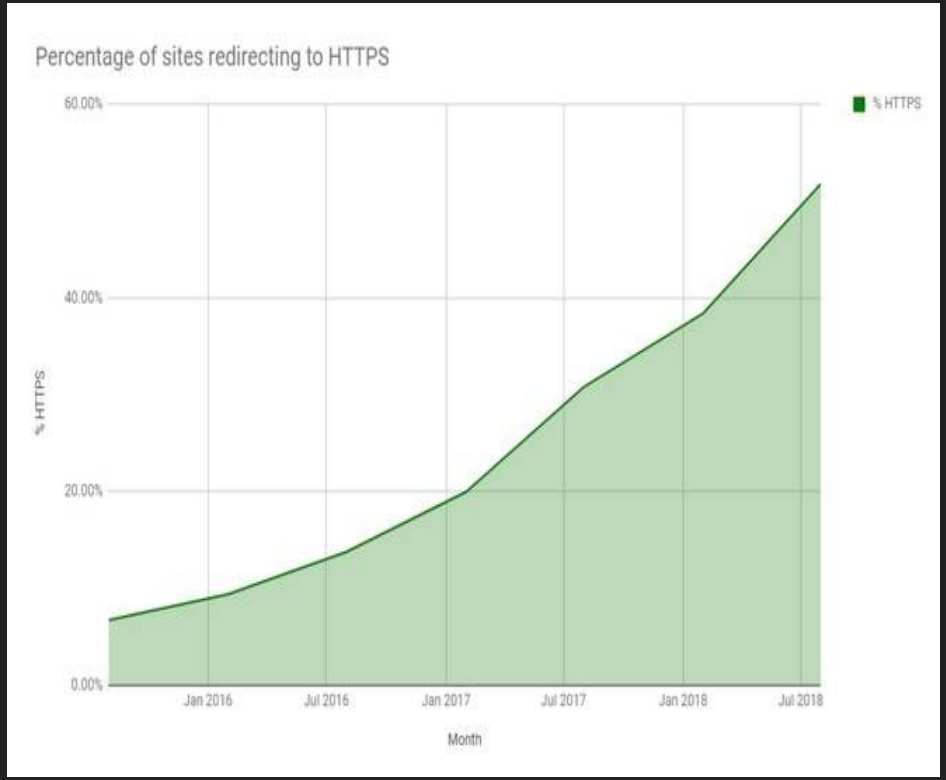
Without encryption, you and I wouldn't be able to do our banking online. We wouldn't be able to buy things online, because your credit cards - they've probably been ripped off anyway, but they would be ripped off left and right every day if there wasn't encryption.

— Tim Cook —

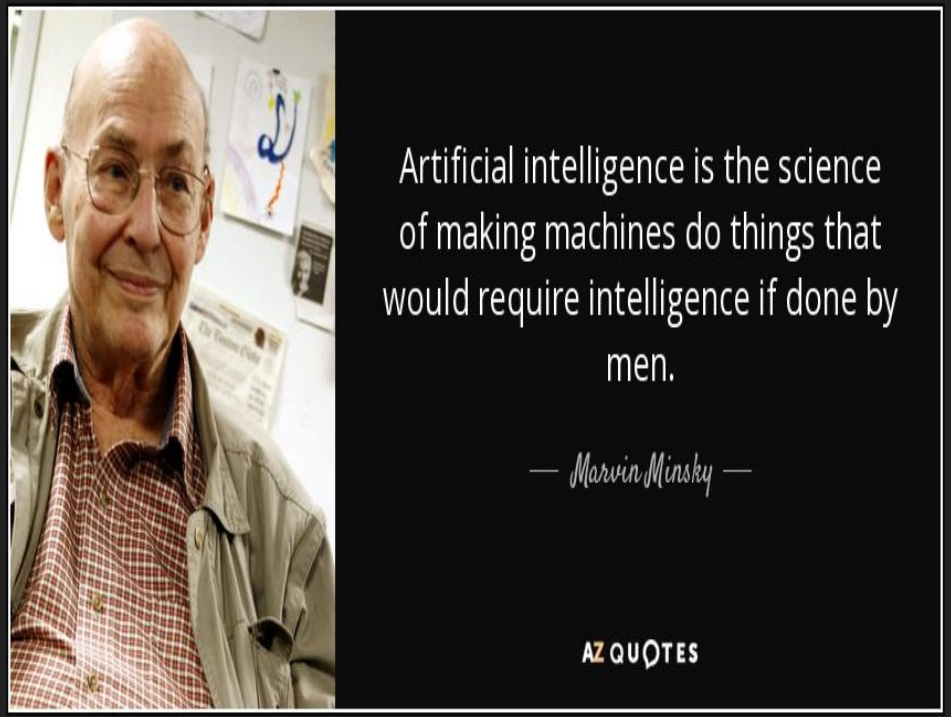
AZ QUOTES

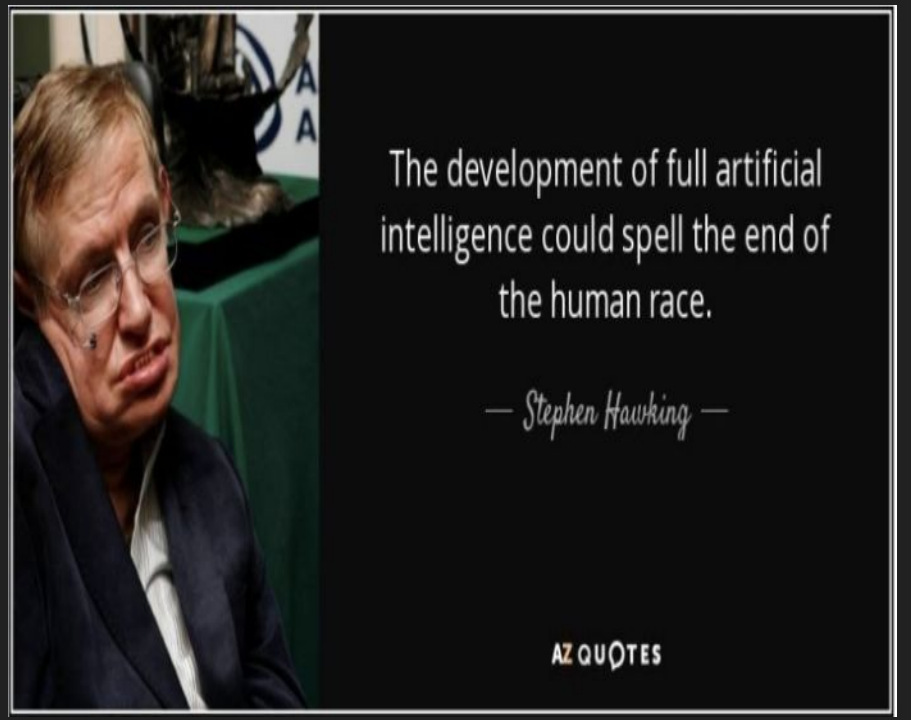
Case 5: Encryption





Case 6: Artificial Intelligence





Case 7: Cryptocurrencies & Bitcoin

Interesting Story: The JPM COIN

JPMorgan CEO Jamie Dimon Returns to Bitcoin Bashing, Calls Cryptocurrency a 'Scam'

CNBC

MENU | MARKETS | BUSINESS | INVESTING | TECH | POLITICS | CNBC TV

FINANCE

BANKS | HEDGE FUNDS | DEALS AND IPOS | WALL STREET

JP Morgan is rolling out the first US bank-backed cryptocurrency to transform payments business

- Engineers at the lender have created the "JPM Coin," a digital token that will be used to instantly settle transactions between clients of its wholesale payments business.
- Only a tiny fraction of payments will initially be transmitted using the cryptocurrency, but the trial represents the first real-world use of a digital coin by a major U.S. bank.
- While J.P. Morgan's Jamie Dimon has bashed bitcoin as a "fraud," the bank chief and his managers have consistently said blockchain and regulated digital currencies held promise.

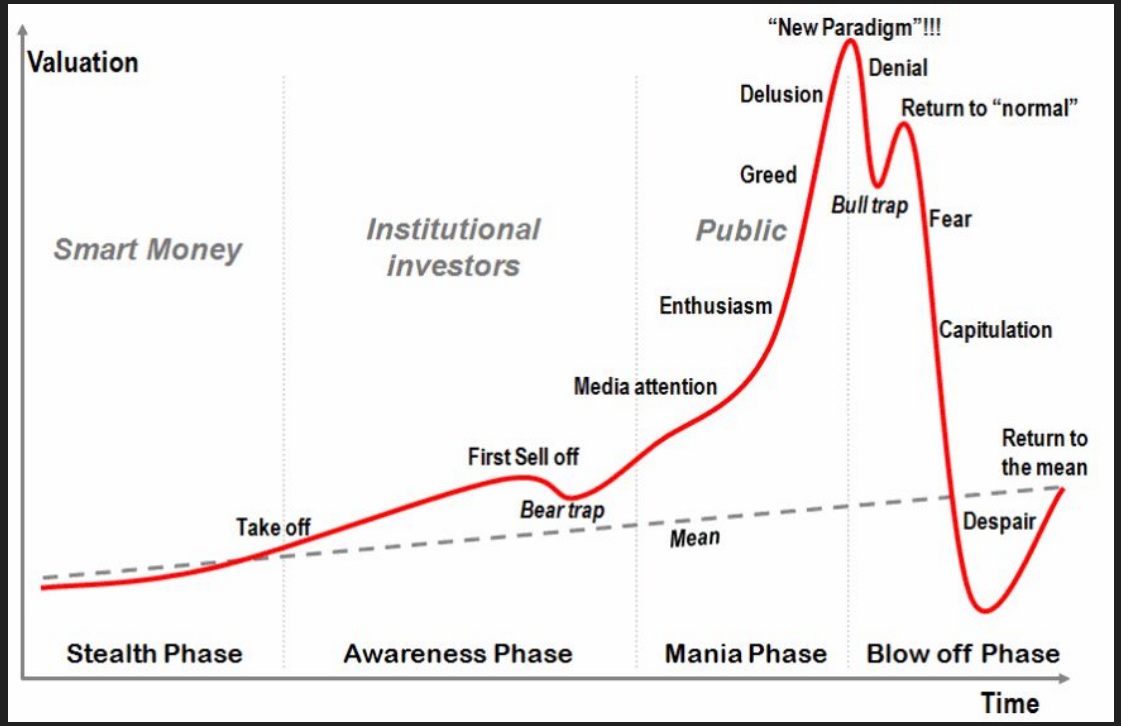
Hugh Son | @hugh_son

Published 5:59 AM ET Thu, 14 Feb 2019 | Updated 7:13 PM ET Thu, 14 Feb 2019

CNBC

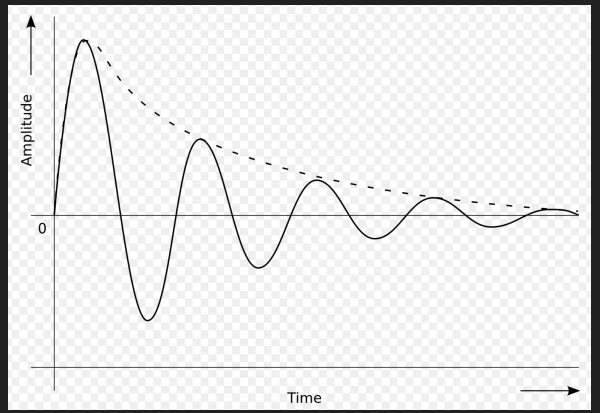
Hype or Hope

- A lot of confusion initially...however the trend is persistent as always



Hype or Hope

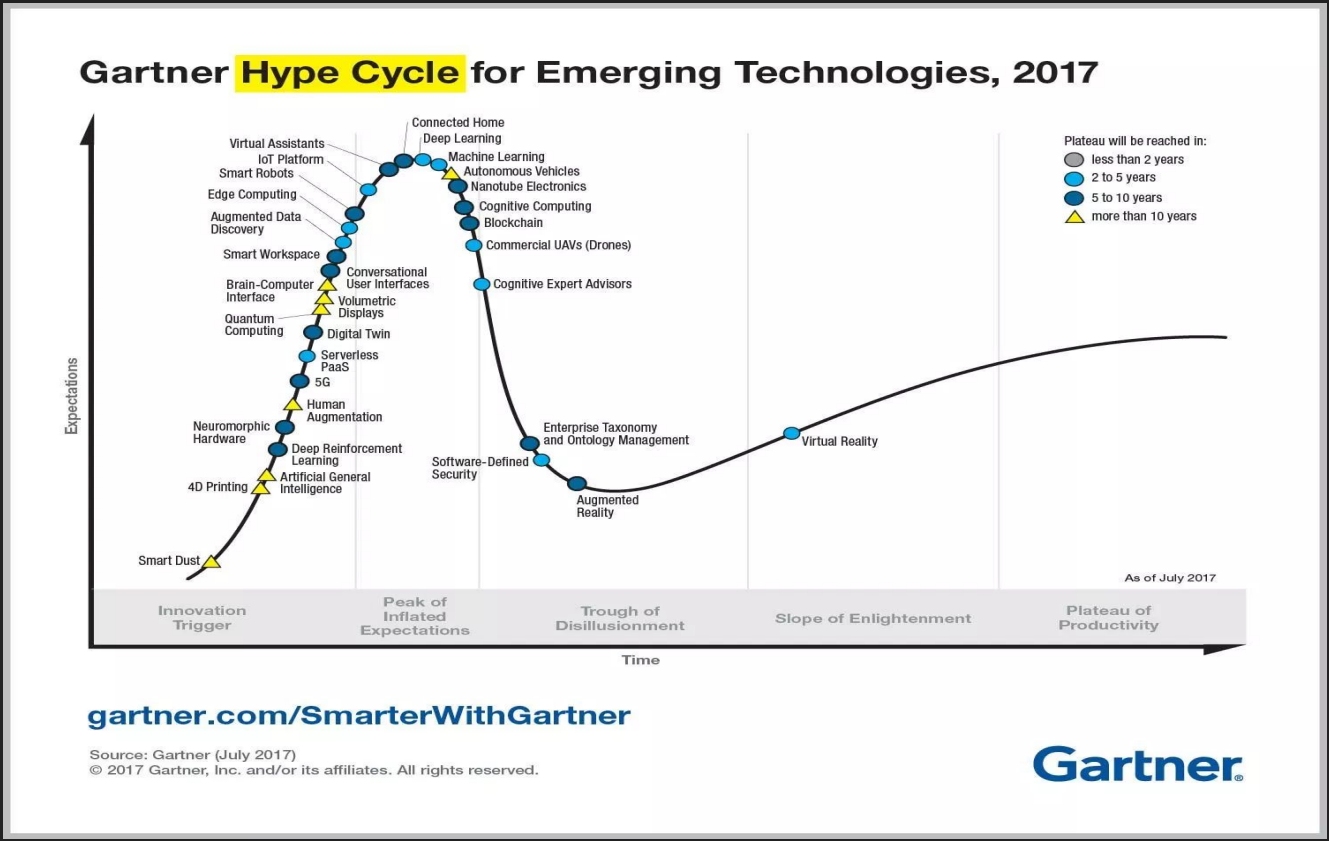
- People get excited initially
- Initiatives to reinvent the wheel using the new technology from everywhere
- **What happens next? Guess?**
  - Regression to the Mean
  - Only a few survive with deep knowledge and real use-cases
  - However large numbers enable magic to happen!
  - Low prob. success stories become a reality!



What we have observed in the Crypto space?

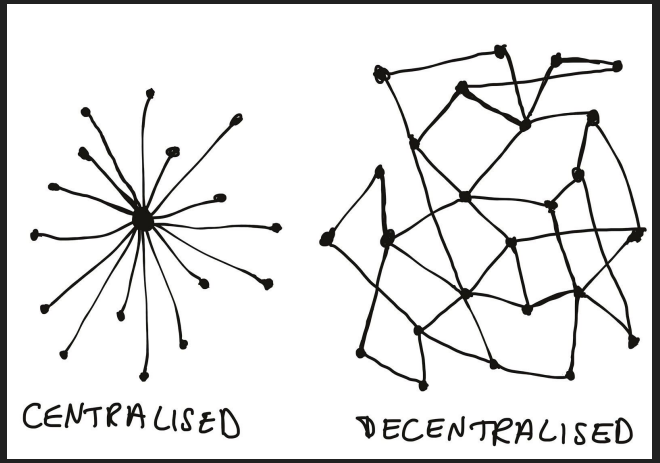
- Most of the use-cases are not real and do not solve real business problems
- Most of the decentralised use-cases are … centralised!
- Most of the cases that claim decentralisation have a hidden agenda … guess what?
  - Getting some power/money as a central authority
  - Circumvent obstacles and other complexities to facilitate their business
- However same use cases will definitely succeed as happened with previous technologies!

This is just the beginning...More to Come



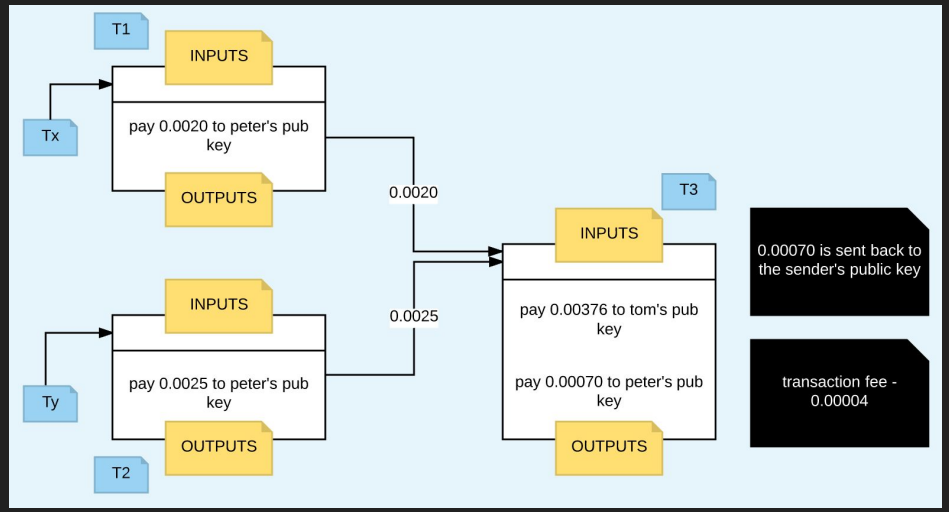
Benefits from Blockchain

- Decentralisation
- No-single point of failure
- No dependency on third-parties



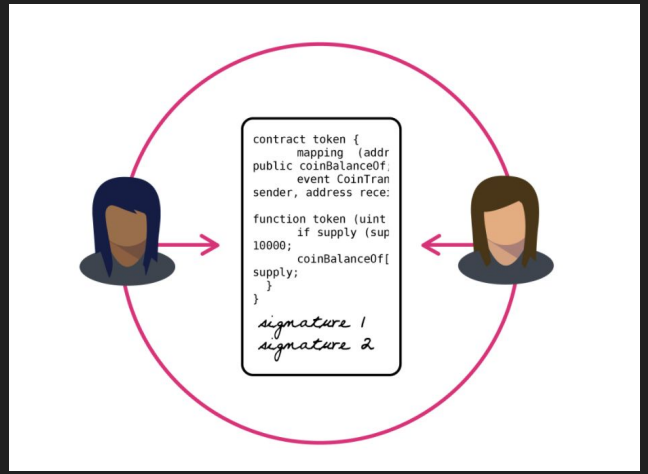
Benefits from Blockchain

- Greater Transparency
- Improved Traceability up to the point of origin
- Immutability



Benefits from Blockchain

- Pre-set conditions for agreements using smart-contracts
- Improved contractual optimisation
- Reduced counterparty risks
- Automated enforcement and execution of contracts



Benefits from Blockchain

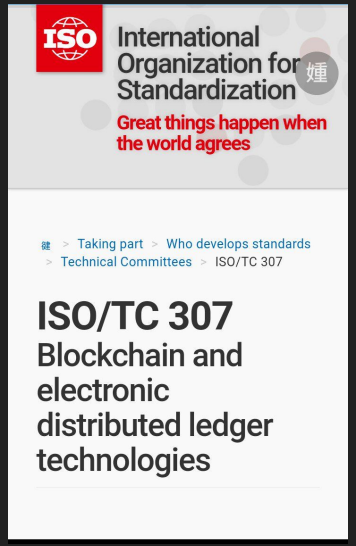
- Cross-border payments made instantly and at a lower cost
- Streamlining of complex supply chains
- Financing of new projects (tokenization)

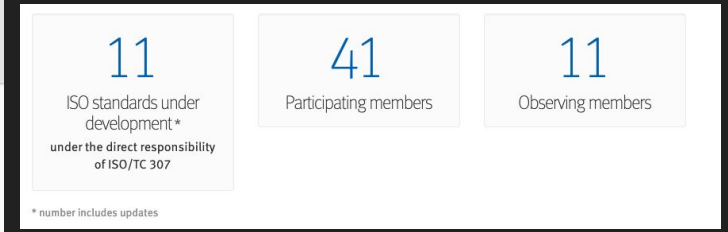
Challenges with Blockchain

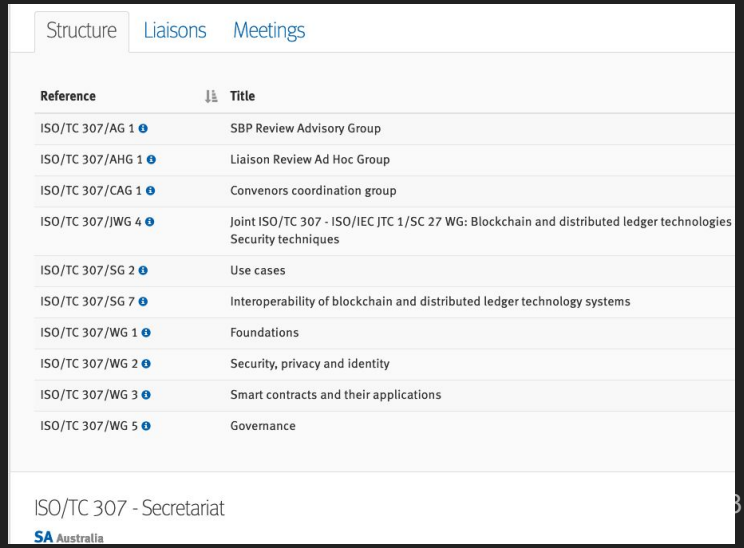
- **Interoperability**
- With an increasing number of players in an ever-expanding industry like blockchain, some worry that with so many different networks, no standard exists to allow them to interact with each other. This standardization is what the industry calls interoperability.

Challenges with Blockchain

- According to Deloitte, the lack of interoperability "grants blockchain coders and developers freedom — and can give IT departments headaches as they discover that platforms can't communicate without translation help."
- For this reason we need standards like ISO/TC 307







Challenges with Blockchain

- **Privacy**
- Reaching critical mass is important for privacy-preserving tools to be efficient (ZK-SNARKS, ring signatures, mixnets etc)
- DLTs & Blockchain have very nice features such as accountability and transparency
- The main concept behind transparency is the existence of the public ledger that includes all the approved transactions
- In addition, all assets can be verified or not if they are associated to a given secret key and that implies full non-repudiation related to the funds

Challenges with Blockchain

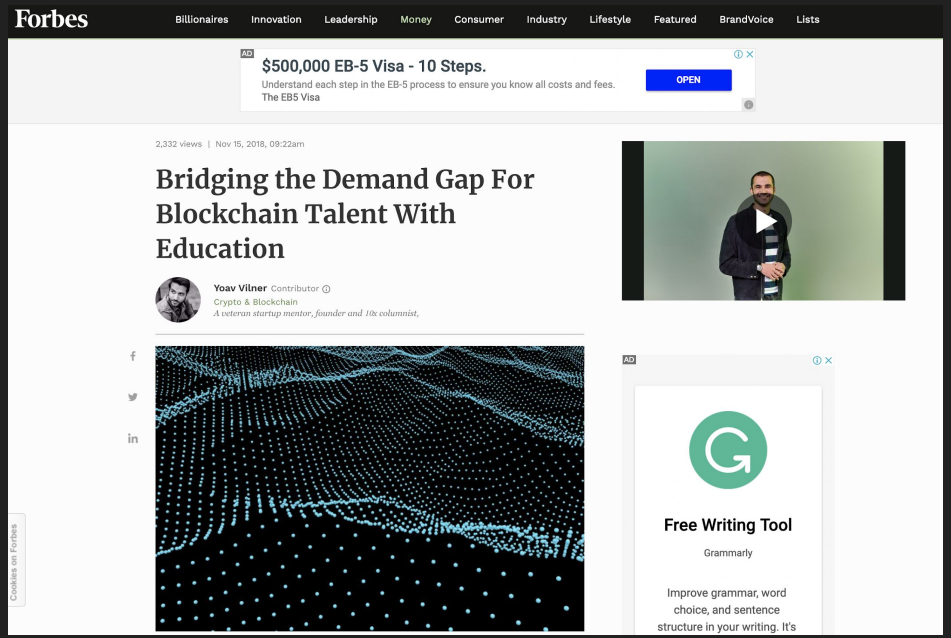
- **Scalability**
- Blockchains are having trouble effectively supporting a large number of users on the network.
- Both Bitcoin and Ethereum, the leading blockchain networks, have experienced slowed transaction speeds and higher fees charged per transaction as a result of a substantial increase in users.
- Scalable Blockchains is the holy grail in the space.
- Some solutions exist: Raiden Network & Lightning Network

Challenges with Blockchain

- **Security and (yet unknown) complex attack scenarios**
- 51% attack
- Eclipse attack
- Routing Attack
- Sybil Attack
- Selfish Miner attack
- Public key crypto attacks, especially with quantum algorithms
- Hot-wallet attacks
- Smart-contract attacks
- Phishing
- Vulnerable signatures

Challenges with Blockchain

- **Lack of awareness and talented people in the space**
  - This is always the case with all emerging technologies (same with data scientists)
  - Education is the solution



Thanks