

# Unavoidable Rise of Blockchain Yet, How Far?

## Keynote Talk

Atilla ELCI

SIN 2018

atilla.elci@gmail.com

# Abstract

Blockchain of BitCoin caught most by surprise by its recent rise to stardom. There is hardly any realm of computing left without its tentacles touching or about to touch soonest. Besides its simple database roots it has been picked up for roles eventually and necessarily combining security, privacy and trust premises in recently evolved information systems. This talk will survey Blockchain and related technologies, their uses and limits with a view towards how to take advantage of its eminent rise.

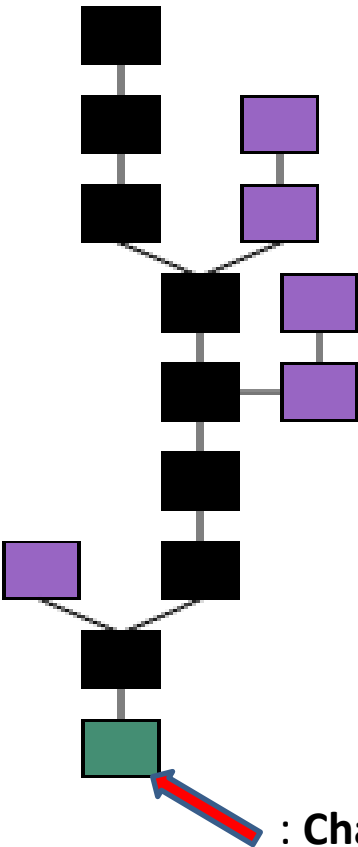
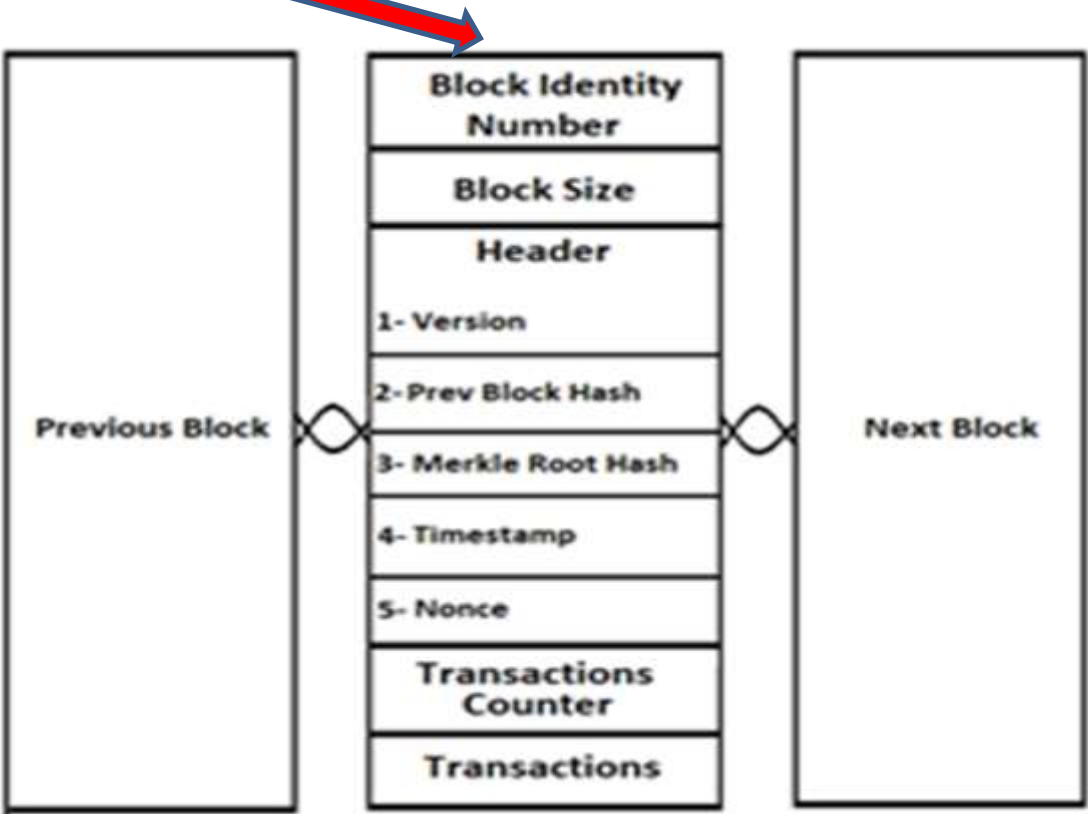
# Definitions

- Blockchain or (public) distributed ledger technology (DLT)



# Blockchain design

Block:

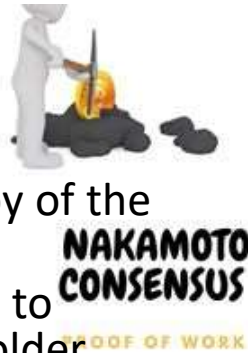


# Attributes, and reasons for popularity

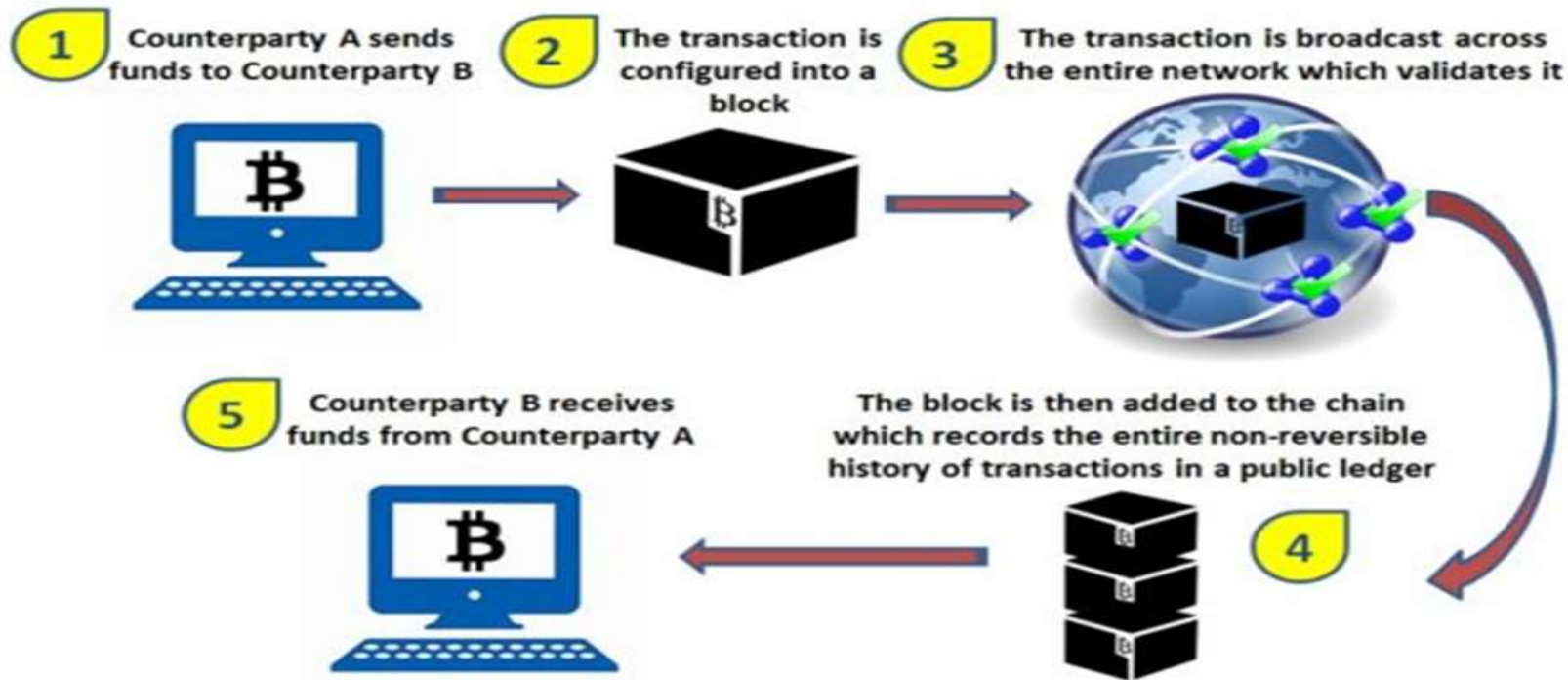
- Immutability: No alteration (w/o producing a change in the subsequent blocks).
- Decentralized: The entire blockchain is shared among all nodes. No single authority.
- Digital asset: Digital asset and the data concerning the sender and recipient of it is exchanged and verified among blocks.
- No third-party fees.
- Anonymous yet public: The blocks are anonymous yet anyone can check the transactions using mining, promoting transparency.
- Frequent verification: Transactions are verified every 10 minutes through mining.
- Provenance: Proof of ownership complete with timestamp.

# Definitions

- Bitcoin: “Bitcoin is the world’s first decentralized cryptocurrency; invented in 2008.
- Block: Transactions are combined into single blocks of roughly 1MB size every 10 minutes,.
- Mining: adding transaction records to the blockchain ledger after confirming the validity of the transactions.
- Double Spending: not allowed by design
- Proof of Work (POW): essentially a hashed block is considered as a POW.
- Hashcash: Bitcoin uses the hashcash POW function.
- Nodes: Nodes are distributed computers in the network that all have a copy of the entire blockchain.
- Address: A bitcoin address is a long string of alphanumeric characters used to send, receive or hold currency. To confirm a transaction, a bitcoin wallet holder needs two encrypted keys- a wallet address and a private key.
- Smart Contract: A digital agreement stored on the blockchain.



## Exhibit 1: The Blockchain is a distributed, public ledger, most commonly known as the core underlying technology for Bitcoin



Source: Goldman Sachs Global Investment Research.

# Quote!

- «The more foundational a technology is, the more impact it can have. Blockchain technology is not a process improvement technology. At its fullest deployment potential, it is rather a disruptive technology; therefore it must be given that potential when being implemented.” – Mougayar, 2016.



# Quote ...

- «Distributed ledger technologies offer institutions a once-in-a-generation opportunity to transform the industry to their benefit, or not.» - PWC Report, 2016.

# Quote ...

- “Arguably the most significant development in information technology over the past few years, blockchain has the potential to change the way that the world approaches big data, with enhanced security and data quality just two of the benefits afforded to businesses using Satoshi Nakamoto’s landmark technology.”
- «blockchain is versatile enough to handle any kind of information that can be digitized» - Smyth, 2016.

# Quote ...

- “The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.”
- “I’ve been at this 35 years, writing about the digital age. I’ve never seen a technology that I thought had greater potential for humanity.”
- “The first generation of the digital revolution brought us the Internet of information. The second generation — powered by blockchain technology — is bringing us the Internet of value: a new platform to reshape the world of business and transform the old order of human affairs for the better.
- Blockchain is a vast, global distributed ledger or database running on millions of devices and open to anyone, where not just information but anything of value — money, but also titles, deeds, identities, even votes — can be moved, stored and managed securely and privately. Trust is established through mass collaboration and clever code rather than by powerful intermediaries like governments and banks.” – Tapscott & Tapscott, 2018

# Predictions

- «According to a 2015 World Economic Forum survey of 800 executives and information and communications technology sector experts, 57.9 percent of the respondents believe that 10 percent of the global GDP information will be stored on blockchain technology by 2025.» - WEF & DCFS, 2015.

# Predictions ...

- «Blockchain technology can potentially provide the IRS with a greater impact than E-filing. It will help the IRS save costs, allow for real time tax related data analysis, reduce fraud, as well as help agents better manage audits. The next time Congress is formulating a budget for the IRS, they would be wise to consider the many benefits that blockchain technology related investments can better the agency. Failing to do so could prove to be an IRS nightmare.» - Bergman, 2018.

# Applications-

## Blockchain as payment instrument

- Deloitte Center for Financial Services (DCFS):
  - «permissioned blockchain payment systems will see "significant transaction volume" by 2020.
  - Such systems, ..., could reach the scale of the Automated Clearing House (ACH) network, which processes 23 billion transactions annually, by 2025.» - Rizzo, 2016.

# Apps- Blockchain as Commercial Real Estate Tool

- How can blockchain technology elevate Commercial Real Estate (CRE) leasing, and purchase and sale transactions?
- Suggests use cases, agents and processes employing blockchain for CRE related transactions. – DCFS, 2017.

# Apps- Online Casino

- Vegas Casino, a provider of bitcoin blackjack, poker, and slots, offers immediate and irreversible payouts using blockchain. – Smyth, 2016.



# Apps- Diamond trade

- The [Kimberley Process](#) (KP), an international organization that oversees the diamond trade, is using blockchain to affect a so-called "system of warranties," whereby parties provide a written guarantee that shipped gems aren't involved in funding conflict. «The 81 participating countries, which [account for roughly 99 percent](#) of the world diamond trade, also only deal with each other.»
- The United Nations General Assembly adopted a resolution supporting the creation of an international certification scheme for rough diamonds (Dec. 2000). Governments, international diamond industry and civil society organisations resolved to create the [Kimberley Process Certification Scheme \(KPCS\)](#), Nov. 2002). The KPCS entered into force in 2003.
- « ... blockchain technology would "help to eradicate false KP certificates and reduce the impact of human error while uploading data significantly." » - Pearson, 2016

# Apps- Big Data: Data Infrastructure

- Omnilytics.co:
  - Its vision is to build a cross-industry data infrastructure.
  - The Omnilytics Platform is a distributed data network which processes global aggregated datasets and combines artificial intelligence, as well as machine learning tools across various industries.
  - Blockchain technology acts as the catalyst to the company's architecture by powering smart contracts, distributed data fingerprinting, data exchange and other protocols and APIs. Users can easily develop and utilise data services without a background in blockchain or data with full transparency and auditability.
  - Thus, blockchain technology ensures the price competitiveness of services, and provides a key strategic advantage in the verifiable and transparent quality of data to the community.

# Apps- Big Data: Healthcare

- «Placing healthcare databases on the blockchain would create a single, unchangeable resource for practitioners to use when treating a patient.»
- The most significant benefit the blockchain could offer healthcare is security. [Cases of patient data loss \(more than 100m in 2015\)](#) by US insurers to hackers are well publicized; a breach leaves patients at risk of identity theft.
- «A blockchain-based healthcare system would also allow providers to share records with justice departments, insurers, employers and any other sector with an interest in people's health without the exponential increase in risk factors that comes with stretching a network thin ...» - Smyth, 2016.

# Apps- Data Monetization

- When it comes to big data, the big task ahead is essentially

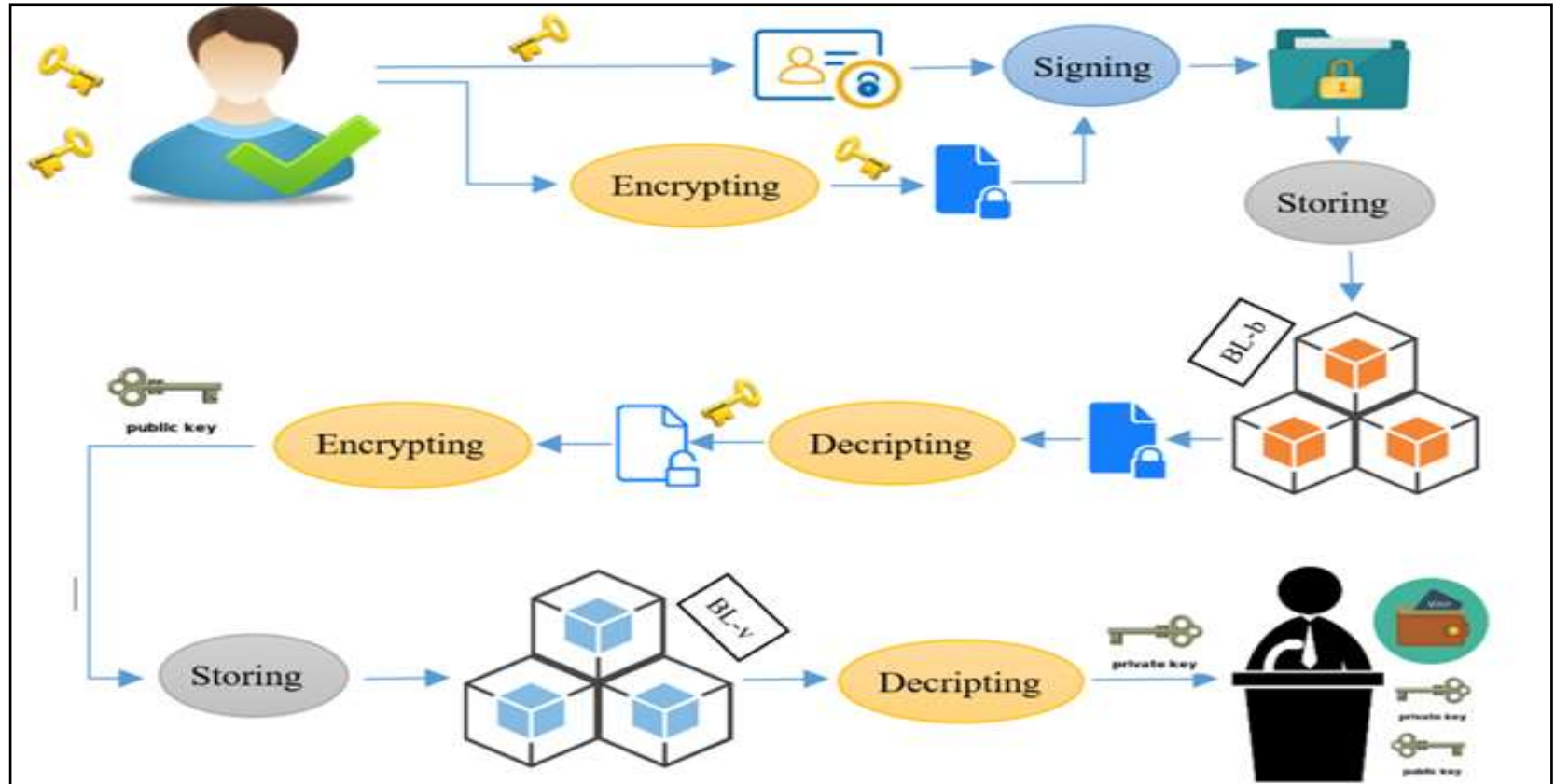
## **Uncovering new forms of data monetization:**

- . How to convert data to financial value?

# Apps- Securities Exchange

- «The **Australian Securities Exchange (ASX)** has become the first major bourse to announce the adoption of **blockchain** technology—the same kind of tech that underpins the bitcoin cryptocurrency—to record shareholdings and manage the clearing and settlement of equity transactions.»
- Digital Asset, the vendor/implementer, has the backing of Deutsche Börse Group, JPMorgan, Chase, Accenture, IBM, Goldman Sachs, and of course ASX. – Meyer, 2017.

# Digital Voting- Al-Rawy & Elci, 2018



# Digital Voting- Al-Rawy & Elci, 2018

- Uses two blockchains for voter/vote privacy, safeguarding the results from manipulation and counterfeiting.
- Provides solutions to problems of impersonation and vote selling.
- Additional measures are spelled out to preclude:
  - Cross-Site Scripting (XSS)
  - FREAK attack (Factoring Attack on RSA-Export Keys)
  - Malwares

# Apps- eVoting

- Other recently published acclaimed academic research exists on eVoting:
  - Nir Kshetri & Jeffrey Voas (July 2018): Blockchain-Enabled E-Voting. IEEE Software 35(4):95-99. DOI: 10.1109/MS.2018.2801546
  - Jerome Mizzi & Frankie Inguanez (Sept, 2018): Blockchain based E-Voting System. Journal of E - Technology, Volume 9, Issue 2, Pages 44-48.
  - And, numerous others listed at:  
<https://www.researchgate.net/search.Search.html?type=researcher&query=e-vote%20%20blockchain>



# Apps ... many others

- Many banks are also [participating in a UBS-led project](#) to develop a blockchain-based “utility settlement coin” that could speed up inter-bank settlements.
- Nasdaq has also developed blockchain technology that it has [provided to the New York Interactive Advertising Exchange](#)
- [The World Bank Just Issued a Bond That Relies On Blockchain Technology From Start to Finish](#)

# Apps ... many others

- **Walmart Inc.**, big US retail corporation and the world's largest discount retailer, has started using blockchain technology in its live food business. - Russo, 2018:
  - Getting suppliers to put food on a Blockchain, which it says will reduce waste, as well as improve contamination management and transparency.
  - Has been testing blockchain since 2016 in collaboration with IBM.
  - It is able to cut the time it took to track produce to two seconds from six days.
  - Submitted an application for a patent on its “Smart Package” system in March 2018.
- The leading Chinese e-commerce site, **JD.com**, is implementing blockchain technology to assure the quality and origin of meat, from the farm in Australia all the way to the customer.

# Apps ... many others

- IEEE launched [Blockchain Initiative](#) in Jan. 2018 in the distributed ledger technology;
- The Initiative collaborates with the [IEEE Computer Society](#), the [IEEE Reliability Society](#), and the [IEEE Standards Association](#). - Rosenfeld, 2018.



# Apps ...many others

- «Almost one in every 10 people around the world get a foodborne disease each year. Of those 600 million people, [420,000 die as a result](#), according to the World Health Organization.
- «IEEE and several other organizations are exploring how blockchain technology could track the source of an outbreak and help contain it.
- To help provide definitions and protocols for such a ledger, the IEEE Standards Association formed the [IEEE 2418.3 Standard for the Framework of Distributed Ledger Technology \(DLT\) Use in Agriculture](#) working group. - Pretz, 2018.

# Apps ...many others

- «A newly proposed "quantum blockchain" could lead to blockchain systems impervious to quantum-computer hacking, a new study finds.
- This new quantum blockchain can be interpreted as influencing its own past, making it behave like a time machine, the researchers add.» – Choi, 2018.



**Best Distributed  
Ledger Initiative** at  
Central Banking's  
'FinTech RegTech  
Global Awards 2018'.  
Sept. 9, 2018

In the latest announcement by IOTA, along with Volkswagen they will be launching the Digital CarPass, which will see performance data tracked via IOTA, to ensure vehicle data collection is both reliable and secure. This is one of the latest 'real-world' integration's of IOTA, and is expected to be launched in 2019.

The [IOTA](#) protocol is a Distributed Ledger Technology developed by the IOTA Foundation.

12.09.2018



SIN 2018, Cardiff U., UK

31

Research by Thomson Reuters shows that 56 percent of all 406 blockchain patents issued around the world in 2017 came from China, with the United States a distant second with 22 percent. Combined with the rapid rise in blockchain patent filings from 134 in 2016 to 406 in 2017, the data tells a story of an ongoing intellectual property rights race that China is currently winning convincingly.



# Critics- «snake oil»

- «Within a private blockchain there is also no ‘race’; there’s no incentive to use more power or discover blocks faster than competitors. This means that many in-house blockchain solutions will be nothing more than cumbersome databases.»
- «There is also no need for a ‘51 per cent’ attack on a private blockchain, as the private blockchain (most likely) already controls 100 per cent of all block creation resources. If you could attack or damage the blockchain creation tools on a private corporate server, you could effectively control 100 per cent of their network and alter transactions however you wished.»
  - NB: Having a single blockchain server (node) is not a proper implementation!!!!
- «Sure, blockchains are an exciting new development, but the devil is in the detail. Without a clear security model, proprietary blockchains should be eyed with suspicion.» - Hampton, 2016.

# Critics ...

- «The point is that blockchain / cryptocurrencies / smart contracts are an entirely new type of technology that give us something that has never existed before (a decentralized method of establishing consensus among potentially untrusted parties), and right now developers and blockchain businesses are still figuring out what the technology can best be applied to.» - Puterio, 2017.

# Critics ...

- Tom Cusack (of KD Nuggets) introduced blockchain idea in a short blog entitled '**Blockchain Explained in 7 Python Functions**' (Cusack, 2018):
  - This is a highly over-simplified and misleading article, in a way highlighting what people think a cryptocurrency blockchain does.
  - It is not quite how it works as it defines a single server node private blockchain not a distributed ledger, thus missing the partners' consensus issue.
  - The ideals of replication, consensus algorithm and mining are missing.

# Critics ...

- Drag affects of establishment:
  - For example, take healthcare:
    - «... blockchain integration in healthcare is a long way off. The need to rebuild database infrastructure, train and hire new staff, and to persuade directors that blockchain is worth the financial outlay means that the system's growth will be confined to health-based start-ups for the foreseeable future.» - Smyth, 2016.

# Critics ...

- Deloitte Center for Financial Services on blockchain as payment instrument:
  - «In our view, while the promise is real, the path to actualizing the potential will not be easy. There is simply too much legacy overhang in making this transition. It will take enormous effort on a collective basis to migrate to a blockchain-based trading and settlement infrastructure.» - Rizzo, 2016.

# Conclusion

- Acceptance of blockchain as instrument is a big hurdle. This is so especially in sectors with established legal & standard procedures of *modus operandi*.
- Proper analysis, design, development, implementation and maintenance of blockchain-based systems are of utmost importance to draw the expected benefits.
- Yet, considerable shortage of capable experts and practitioners exist. Structured approach to training/educating/licensing professionals is direly needed.
- It seems at this time the demand for expertise is increasing much faster than the speed of raising expert supply.

- Questions?

# References

- Don Tapscott and Alex Tapscott (2018): *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World* Paperback. Portfolio Penguin. **ISBN-13:** 978-0241237861
- Abhinav Venkat (September 1, 2017): Introduction to Blockchains & What It Means to Big Data. <http://www.noahdatatech.com/introduction-blockchains-means-big-data/>
- Daniel Smyth (Dec. 16, 2016): Why blockchain? What can it do for big data? <http://bigdata-madesimple.com/why-blockchain-what-can-it-do-for-big-data-2/>
- Jordan Pearson (Aug. 31, 2016): The World's Blood Diamond Watchdog Is Looking to the Blockchain. But can new technology fix a broken process? [https://motherboard.vice.com/en\\_us/article/gv58qw/blood-conflict-diamond-trade-watchdog-blockchain-kimberley-process](https://motherboard.vice.com/en_us/article/gv58qw/blood-conflict-diamond-trade-watchdog-blockchain-kimberley-process)
- Pete Rizzo (Mar 10, 2016): Deloitte: Blockchain Systems Could Rival ACH Network By 2025. <https://www.coindesk.com/deloitte-blockchain-ach-2025/>



# Refs ...

- DCFS (Deloitte Center for Financial Services, 2017):  
Blockchain in commercial real estate: The future is here!
- WEF (World Economic Forum, September 2015): “Deep Shift: Technology Tipping Points and Societal Impact”,  
Global Agenda Council on the Future of Software & Society.
- Matt Puterio (Dec 27, 2017) @ Medium.com.  
<https://medium.com/@mputerio/blockchain-technology-is-still-in-its-infancy-16dec9619b5d>

# Refs ...

- Omnilytics Platform Whitepaper (nd): Omnilytics: Powering the future of the data economy- Cross-industry data infrastructure.  
<https://platform.omnilytics.co/>
- Blockchain. <https://en.wikipedia.org/wiki/Blockchain>
- Hampton, Nikolai (September 5, 2016): "[Understanding the blockchain hype: Why much of it is nothing more than snake oil and spin](#)". *Computerworld*.
- David Meyer (December 7, 2017): The Australian Securities Exchange Just Made Blockchain History.  
<http://fortune.com/2017/12/07/blockchain-technology-australian-securities-exchange-asx/>

# Refs ...

- William Mougayar (2016): The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley. ISBN: 978-1-119-30031-1
- Bergman Adam (Jun 4, 2018): How Blockchain Technology Can Save The IRS. Forbes. <https://www.forbes.com/sites/greatspeculations/2018/06/04/how-blockchain-technology-can-save-the-irs/>
- Tom Cusack (April 2018): Blockchain Explained in 7 Python Functions. <https://www.kdnuggets.com/2018/04/blockchain-explained-7-python-functions.html>
- Mahmoud Al-Rawy and Atilla Elci (2018): A Design for Blockchain-Based Digital Voting System. In proc. DSIC'18 – The 2018 International Conference on Digital Science, Budva, Montenegro, 19 – 21 October 2018.

# Refs ...

- Monica Rosenfeld (Aug. 1, 2018): IEEE Blockchain Initiative Helps to Advance the Decentralized Ledger- Members are developing standards and e-learning courses, and forming local groups. The Institute: The IEEE news source, <http://theinstitute.ieee.org/technology-topics/computing/ieee-blockchain-initiative-helps-to-advance-the-decentralized-ledger>
- Ana Alexandre (Apr. 28, 2018): Walmart is ready to use blockchain for its live food business. <https://cointelegraph.com/news/walmart-is-ready-to-use-blockchain-for-its-live-food-business>
- Camila Russo (Apr. 23, 2018): Walmart is getting suppliers to put food on the blockchain. <https://www.bloomberg.com/news/articles/2018-04-23/walmart-is-getting-suppliers-to-put-food-on-blockchain-to-track>
- Kathy Pretz (Aug. 29, 2018): How blockchain technology could track and trace food from farm to fork. IEEE standards working group is using the distributed ledger to improve and secure the supply chain. <http://theinstitute.ieee.org/resources/standards/how-blockchain-technology-could-track-and-trace-food-from-farm-to-fork>

# Refs ...

- Charles Q. Choi (Apr. 23, 2018): Quantum Blockchains Could Act Like Time Machines. Quantum blockchain systems could resist hacks by quantum computers. IEEE Spectrum. <https://spectrum.ieee.org/tech-talk/computing/networks/quantum-blockchains-could-act-like-time-machines>