FACTS MA

FOSTERING ADVOCACY AND
COLLABORATION THROUGH SCIENCE

Blockchain Technology

COMMITTEES

House Energy and Commerce Committee; Science, Space, and Technology Committee

Senate Commerce, Science, and Transportation Committee; Committee on Finance

For further information contact
FACTS•MA
contact@factsma.org

Follow us @FACTS-MA

www.factsma.org

Updated February 11, 2018

The Concept

- Blockchain is a computer technology that creates a permanent, public record of every transaction for virtual or real objects[1,2], such as:
  - Every transaction of a unit of cryptocurrency (e.g., a bitcoin)
  - Every step in a supply chain for a product such as a car part.
- As the name implies, each transaction is represented within a block of information; blocks are chained together to form a complete record.
- A blockchain is a permanent, unforgeable record of an object's history.
  - Only the owner of an object can authorize the inclusion of information in a block that would modify its record.
  - Once a block is added, it cannot be changed.
- Blockchains are shared and continuously updated across all of the computers in a decentralized network, such as the Bitcoin network.
- A potential advantage of blockchains is that their public and tamper-evident nature eliminates the need for (and thus the cost and inefficiency of) a trusted intermediary (such as a bank or a broker) in commercial transactions.

The Implementation

- Blockchain technology is based on cryptography that allows anyone to read the blockchain, but only owners of items to authorize the addition of a block modifying an item's record.
- This type of cryptography (known as “public key systems”) relies on asymmetric mathematical problems, which are hard to solve, but easy to verify, once the solution is known[3]. For instance, it is hard to determine that the prime factors of 102550703 are 7759 and 13217, but easy to calculate that 7759 x 13217 = 102550703.
- Because it is computationally hard to add a new block to a chain, no one computer in the network is powerful enough to do it. The problem must be shared across the entire network. Someone who tries to add selfish blocks (eg excluding a competitor’s transactions) will fail, because they will not be able to add blocks as quickly as the rest of the network, which is cooperating to add valid blocks.

Applications

- Blockchains were developed for the Bitcoin cryptocurrency[4,5].
  - They record ownership and transfer of bitcoins on the Bitcoin network without requiring a trusted broker[6].
- Blockchains could (although have not yet been implemented to) track and even facilitate other transactions[7], such as:
  - Digital identity and intellectual property management
  - Digital voting
  - Smart contracts that execute without the need of a bank or broker
- See the FACTSheet on the Application of Blockchains[8] for details.

Blockchain technology is at a point in its development similar to the internet in the '80s or mobile devices in the '90s. There is good reason to predict that blockchain technology will be as disruptive in finance and commerce as these other technologies have been in communication, entertainment and commerce[9].

Sources

[1] "Blockchains: The great chain of being sure about things". The Economist, 31 October 2015
https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable

[2] "What is Blockchain Technology? A Step-by-Step Guide For Beginners". Blockgeeks
https://blockgeeks.com/guides/what-is-blockchain-technology

[3] "Explaining public-key cryptography to non-geeks". Panayotis Vryonis, Medium, 27 August 2013
https://medium.com/@vrypan/explaining-public-key-cryptography-to-non-geeks-f0994b3c2d5

[4] "Bitcoin: A Peer-to Peer Electronic Cash System". Satoshi Nakamoto, The Cryptography Mailing List, 31 October 2008
http://nakamotoinstitute.org/bitcoin

[5] "A Short History Of Bitcoin And Crypto Currency Everyone Should Read". Bernard Marr, Forbes, 6 Decebmer 2017
https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read

[6] "BITCOIN: A Primer for Policymakers". Jerry Brito and Andrea Castillo, Mercatus Center, George Mason University, 2013
https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf

[7] "5 Blockchain Applications That Are Shaping Your Future". Ameer Rosic, The Huffington Post, 6 December 2017
https://www.huffingtonpost.com/ameer-rosic-/5-blockchain-applications_b_13279010.html

[8] "The Applications and Risks of Blockchain technology". FACTS•MA, TBD
https://www.factsma.org/factsheets

[9] "A Brief History of Blockchain". Vinay Gupta, Harvard Business Review, 28 February 2017
https://hbr.org/2017/02/a-brief-history-of-blockchain

For more information see "Blockchain World". IEEE Spectrum, October 2017
https://spectrum.ieee.org/static/special-report-blockchain-world