Cryptographic Algorithms and Protocols for Distributed Ledgers

Student: Kirill I. Kupriyanov
Supervisor: Sergey M. Avdoshin
Higher School of Economics, FCS SSE

NATIONAL RESEARCH
UNIVERSITY

March 20, 2019

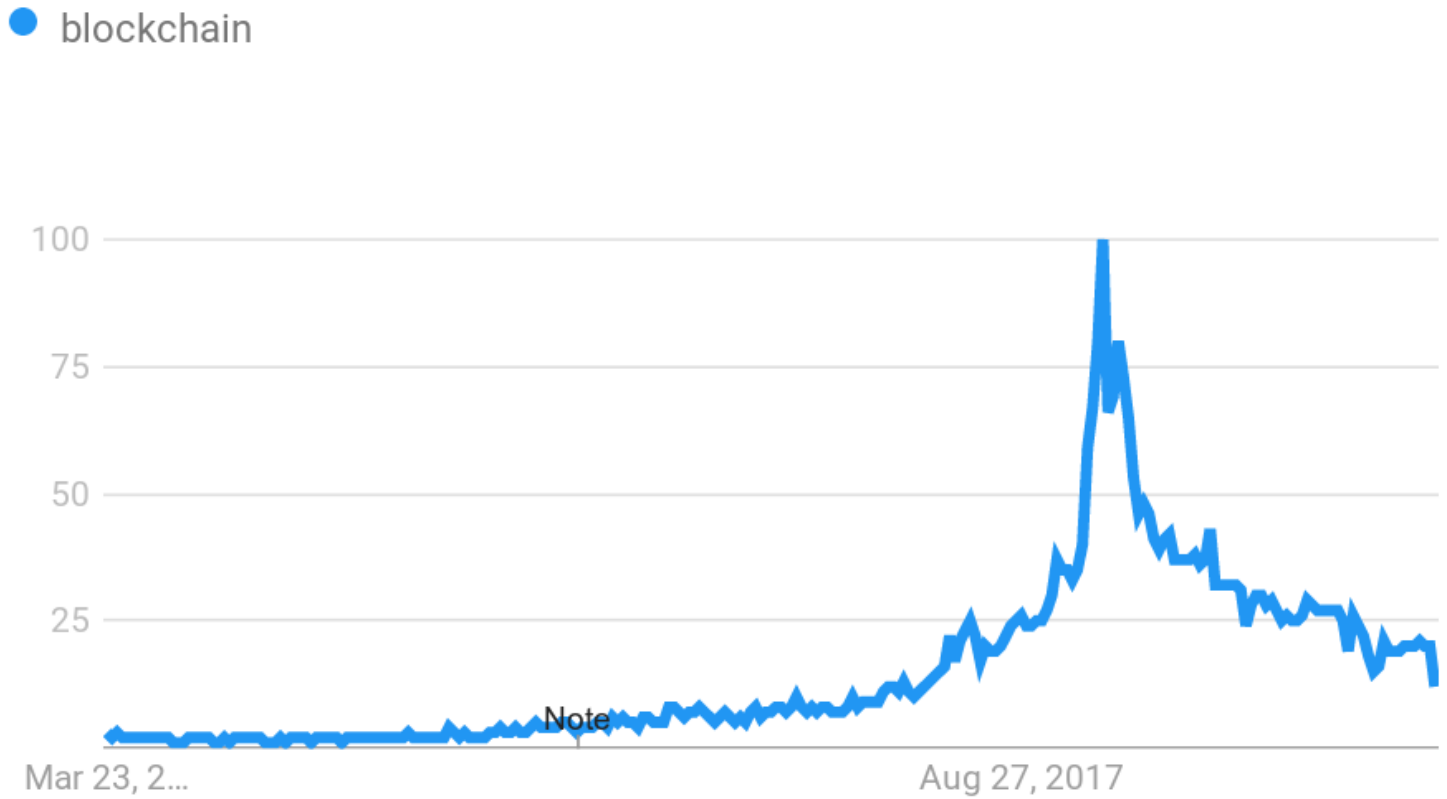
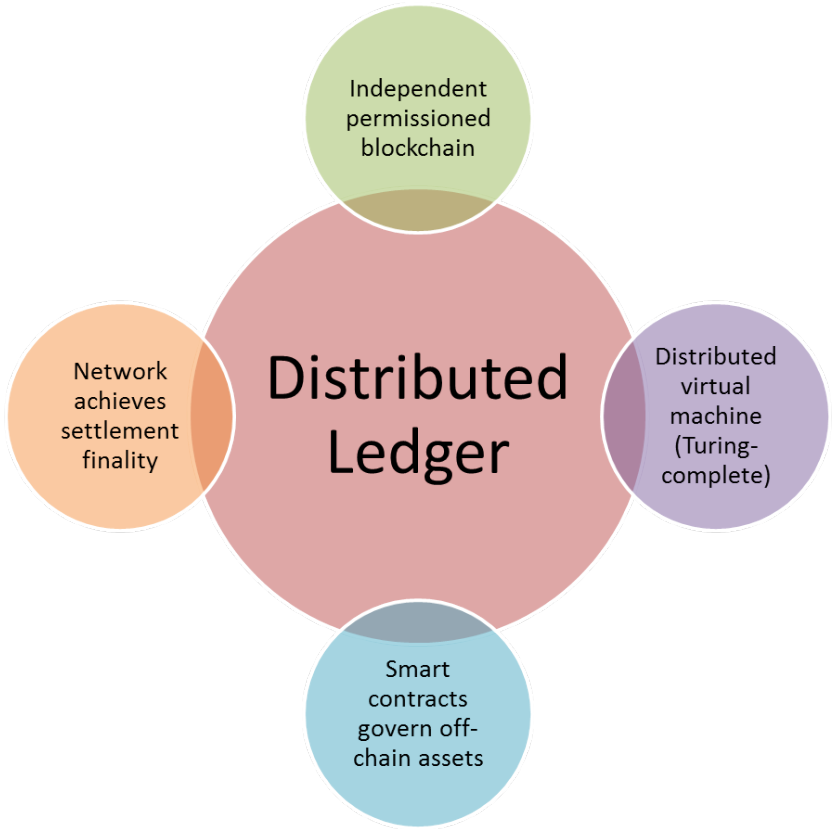


Figure 1. Interest of search quere “blockchain” over time, Google Trends; March 19, 2019

OUTLINE

STUDY AREA

- Distributed ledgers
- Cryptography
- Programming



Swanson, T., The Distributed Ledger Landscape, Jun 27, 2015

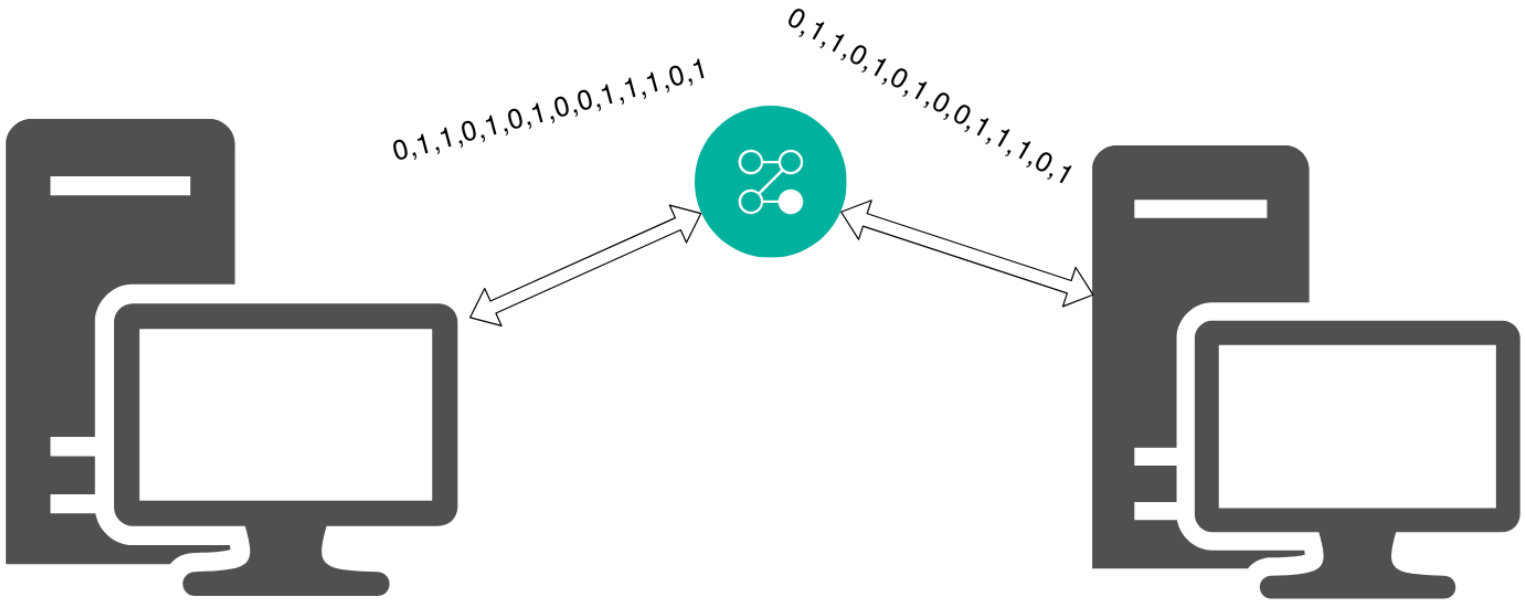
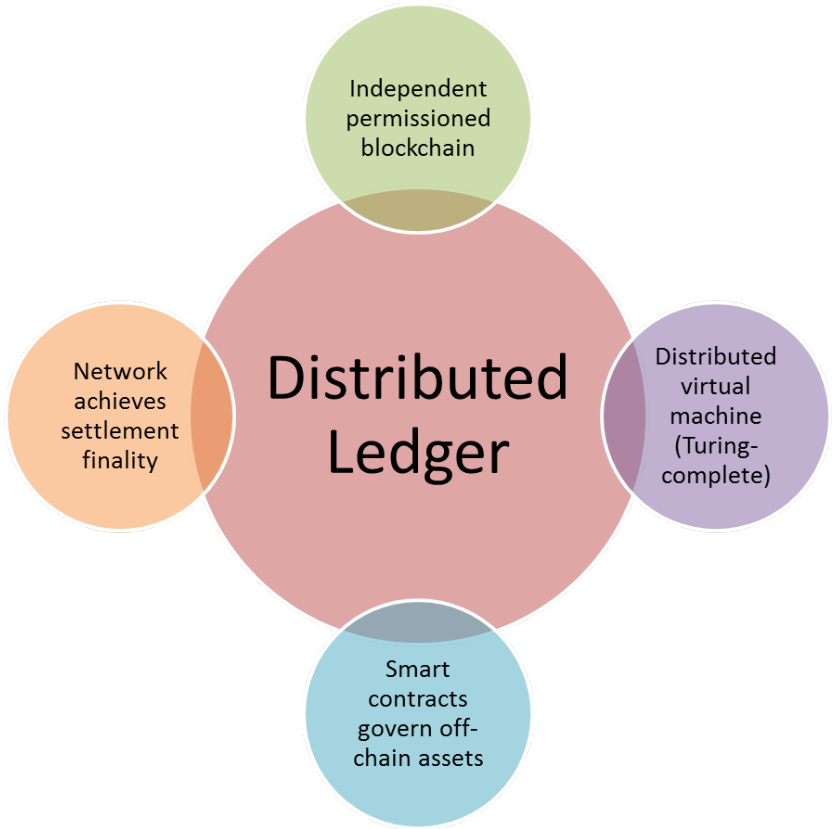


Figure 2. Transmitting bytes from one source to another, FOSS; Mar 19, 2019

STUDY AREA

- Distributed ledgers
- Cryptography
- Programming



Swanson, T., The Distributed Ledger Landscape, Jun 27, 2015

DEFINITIONS

- Distributed Ledger
- Blockchain
- Cryptocurrency

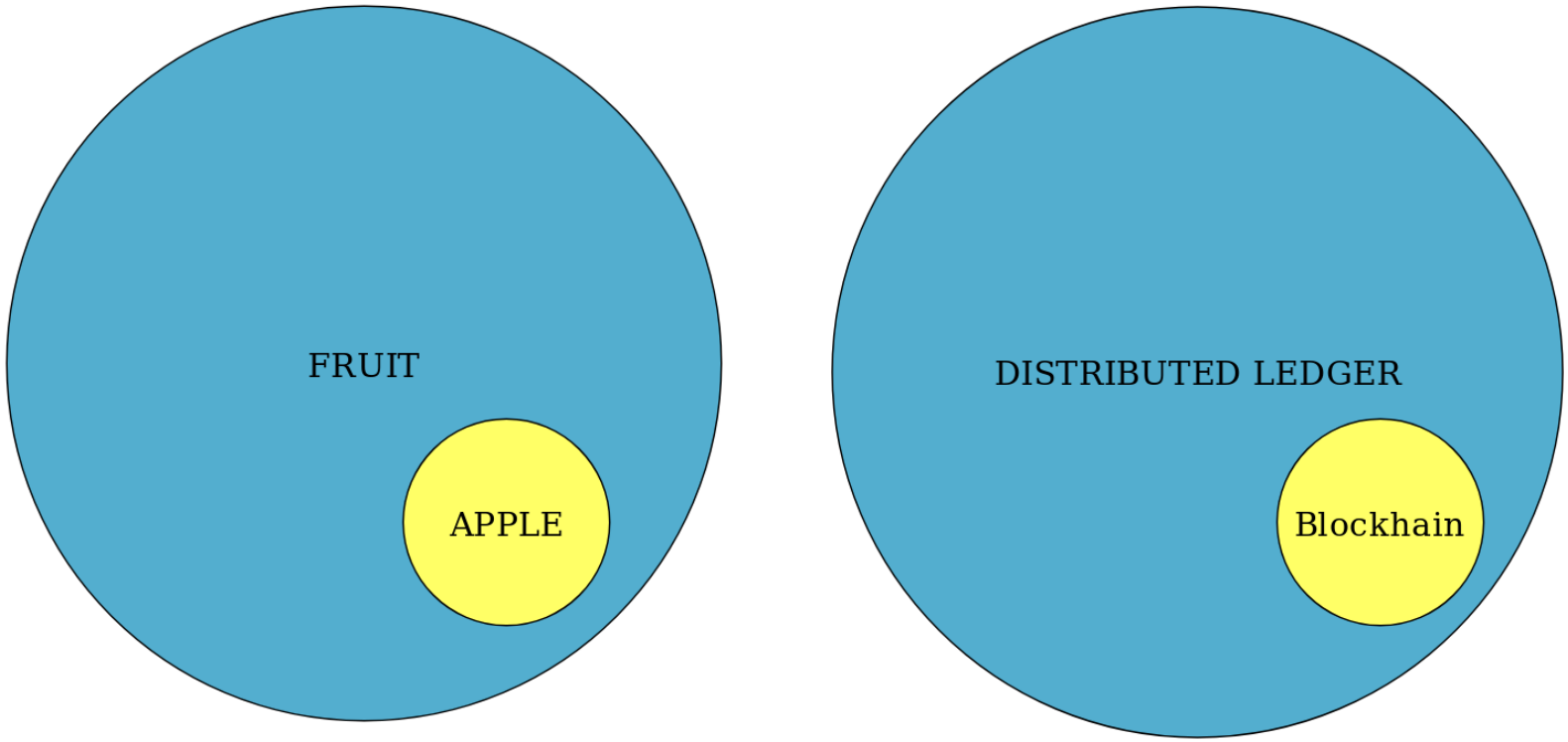


Figure 3. Comparing blockchains to fruits, FOSS, Mar, 19, 2019

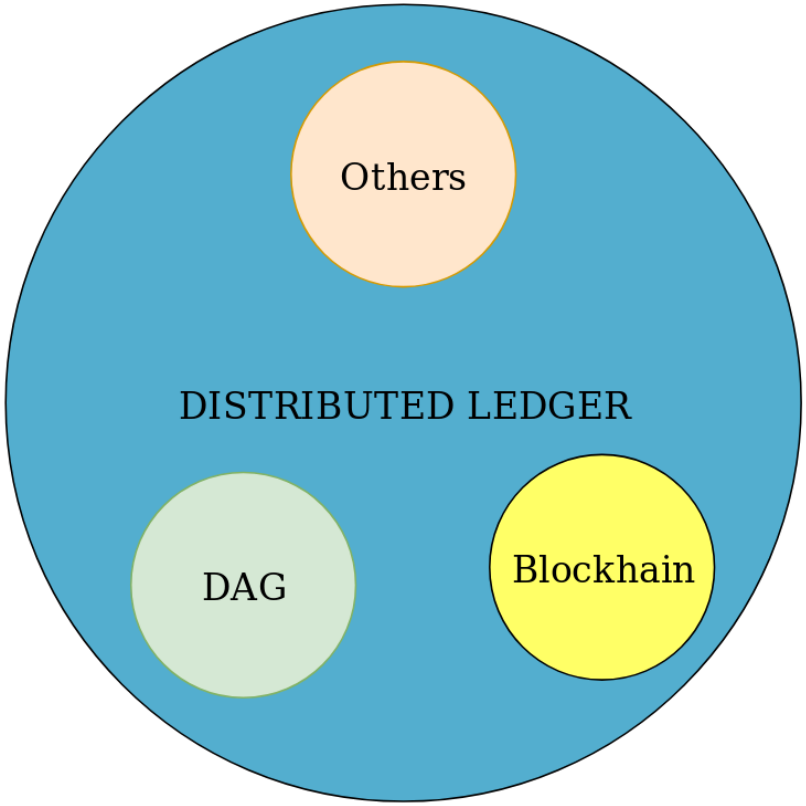


Figure 4. Components of DLT, FOSS, Mar, 19, 2019

EXAMPLES

- Bitcoin
- Litecoin
- Namecoin
- Etherium
- Monero
- Dash
- Ripple
- ...

- IOTA
- Byteball
- NANO
- ...

PROBLEMS

- Outdated existing classification
- Lack of technical information
- Unsuitable blockchain creator programms

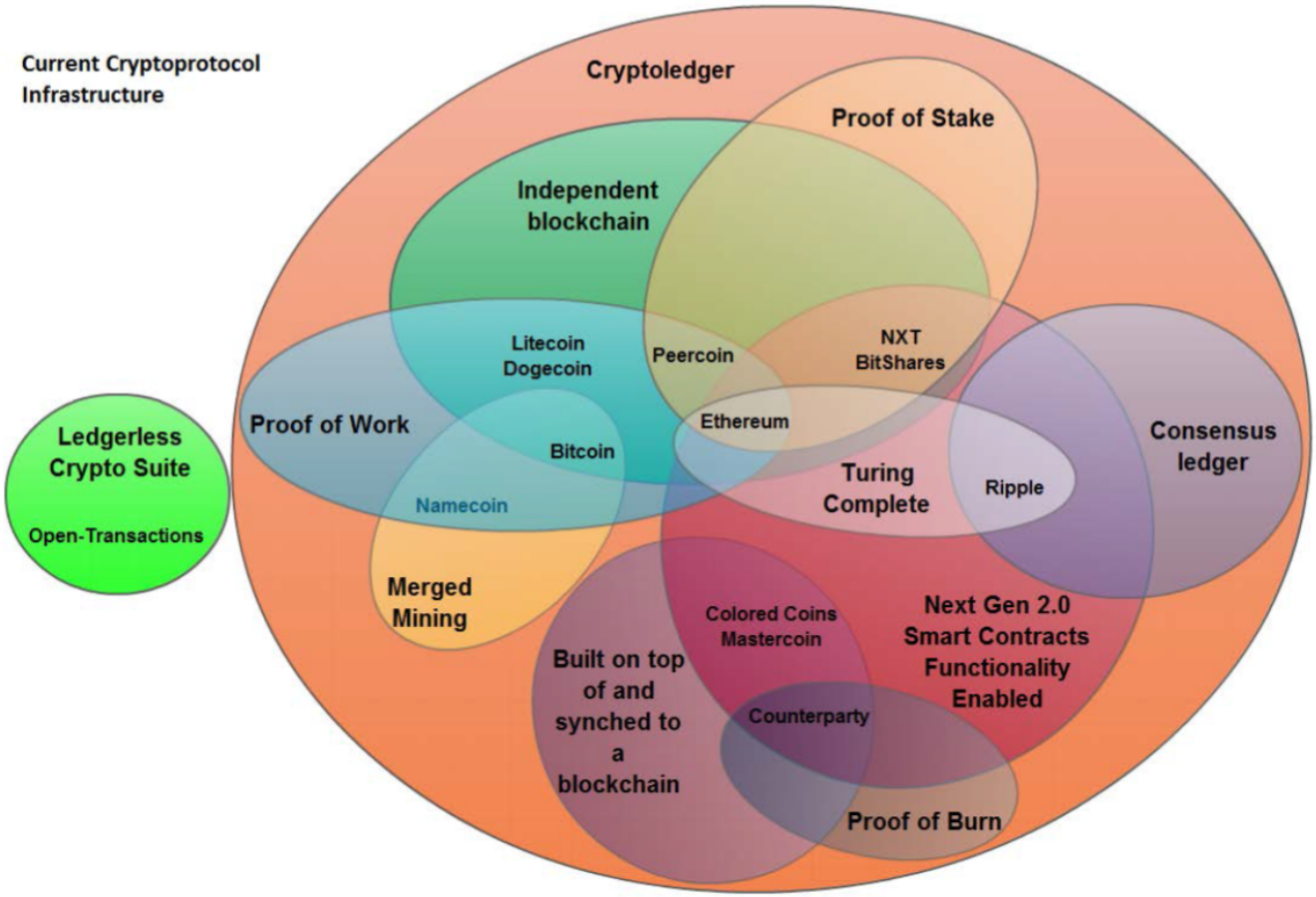


Figure 5. Swanson, T., The Great Wall of Numbers, 2014

PROBLEMS

- Outdated existing classification
- Lack of technical information
- Unsuitable blockchain creator programms

METHODOLOGY

- Literature review
- Benchmark analysis, publishing to wiki
- Free Python v. 3.6.5 library

EXPECTED RESULTS

- Structured body of knowledge is helpful
- Research provides an in-depth view
- Python library is used by target users

SOURCES AND LITERATURE USED


Swanson, T., *Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management.*, 2014, pp.44-47


T. Swanson, "The Distributed Ledger Landscape", Slideshare.net, 2019. [Online]. Available: https://www.slideshare.net/MrCollectrix/the-distributed-ledger-landscape. [Accessed: 19- Mar- 2019]


Xu, Xiwei & Weber, Ingo & Staples, Mark & Zhu, Liming & Bosch, Jan & Bass, Len & Pautasso, Cesare & Rimba, Paul. *A Taxonomy of Blockchain-Based Systems for Architecture Design.*, 2017, 10.1109/ICSA.2017.33, pp. 4-6


Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2014. [ebook] Available at: `https://bitcoin.org/bitcoin.pdf` [Accessed 9 Feb. 2019]


"Google Trends", Google Trends, 2019. [Online]. Available: https://trends.google.com/trends/. [Accessed: 19- Mar- 2019]

QUESTIONS

Any questions?

THANK YOU FOR ATTENTION

Contacts

Kirill I. Kupriyanov
mephisto@openmail.cc

Sergey M. Avdoshin
savdoshin@hse.ru