# Cryptographic Algorithms and Protocols for Distributed Ledgers

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



March 20, 2019



NTRODUCTION 1 of 18

METHODOLOGY

EXPECTED RESULTS

0

INTRODUCTION

BACKGROUND

blockchain

PROBLEMS

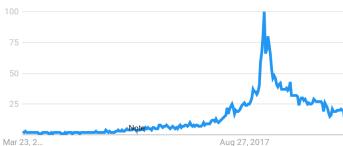


Figure 1. Interest of search quere "blockchain" over time, Google Trends; March 19, 2019

References

QUESTIONS

Introduction 2 of 18

 Introduction
 Background
 Problems
 Methodology
 Expected results
 References
 Questions

 0000000
 000
 0
 0
 0
 0

# OUTLINE

Introduction

BACKGROUND

Study area Definitions

PROBLEMS

Modern problems and questions

METHODOLOGY

Theoretical and practical approaches

EXPECTED RESULTS

Concluding above

REFERENCES

Sources and literature used

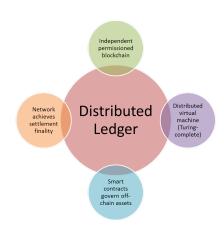
QUESTIONS



NTRODUCTION 3 of 18

#### STUDY AREA

- ► Distributed ledgers
- Cryptography
- ► Programming



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



BACKGROUND 4 of 18

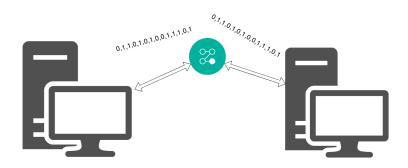
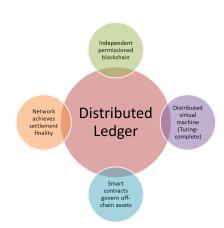


Figure 2. Transmitting bytes from one source to another, FOSS; Mar 19, 2019

BACKGROUND 5 of 18

#### STUDY AREA

- ► Distributed ledgers
- Cryptography
- ► Programming



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



BACKGROUND 6 of 18

## **DEFINITIONS**

- ► Distributed Ledger
- ► Blockchain
- ► Cryptocurrency



BACKGROUND



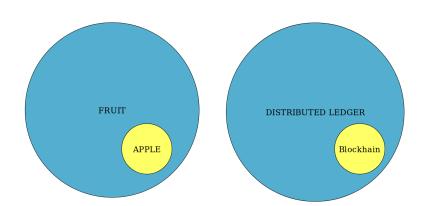


Figure 3. Comparing blockchains to fruits, FOSS, Mar, 19, 2019

BACKGROUND 8 of 18

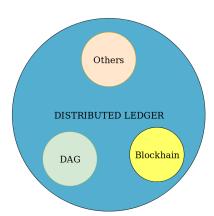


Figure 4. Components of DLT, FOSS, Mar, 19, 2019

BACKGROUND 9 of 18

# **EXAMPLES**

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

- ► IOTA
- ► Byteball
  - ► NANO
  - \_

#### **PROBLEMS**

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

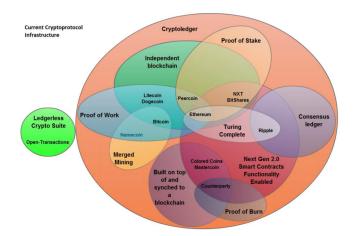


Figure 5. Swanson, T., The Great Wall of Numbers, 2014

Problems 12 of 18

#### **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

METHODOLOGY

#### **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]

METHODOLOGY

EXPECTED RESULTS

# QUESTIONS

INTRODUCTION

Any questions?

BACKGROUND

PROBLEMS



REFERENCES

QUESTIONS

#### THANK YOU FOR ATTENTION

#### Contacts

Kirill I. Kupriyanov *mephisto@openmail.cc* 

Sergey M. Avdoshin *savdoshin@hse.ru*