Prezentation text

Introduction

Good afternoon, everyone. My name is Kirill Kupriyanov and today's topic is my research proposal for the thesis Cryptographic Algorithms and Protocols for Distributed Ledgers. This theme is strongly related to cryptographic algorithms, cryptocurrencies and a blockchain. PAUSE 2 SEC.

Google trends pic

In recent years the popularity of blockchain has been decreasing steadily, which can be seen on the line graph presented. There is no comparison between the spike in 2017 and today's numbers. Still, it remains a (relatively) frequent topic of discussion. Today, scientists focus mainly on the upcoming events: overflow of blocks number, higher fees, expanding and popularizing knowledge of cryptocurrencies in public. That is why we expect to see another burst of interest and attention in the near future. That is why we chose this theme, outline of which will be introduced now.

Outline

Firstly, the study area we are working with, and technichal terms that may be needed to fully get the content will be introduced. PAUSE 2 SEC. In the main part important ideas and concepts will be listed. And finally, we will be able to dicuss questions that might appear during the presentation. Let's move to the next part.

Study area

The theme of the research is bound to cutting edge areas. Although cryptography is a science which has been evolving throughout humanity's history, now, when most it's methos are known and studied, the interesting part is applications of this study area.

Cryptobytes

It applies to every field of Computer Science, because Computer Science is all about transmitting bytes from one source to another, security of this process is vital.

Study area

In the scope of the research the majority of the work will be studying, analyzing and classifying things, and programming job will also take place. The Distributed Ledger is the most important part, which should firstly be defined.

Definitions

There is a subtle difference between a blockchain and distributed ledger.

Apple slide

A blockchain is a type of distributed ledger. Much like an apple is a type of fruit. Apple is a fruit, and a Blockchain is a Ditstributed Ledger. This is a common confusion, which arises because in most papers the term "Blockchain" was introduced before "Distributed Ledger". The sudden surge of popularity had the term "Blockchain" turn into a generic term. Furthermore, it became so generic that most people belive that all cryptocurrencies are blockchains. This leads to the next

confusion.

Blockchain and cryptocurrencies

Blockchain is just one of the bases for building a cryptocurrency. On the other side, people invented cryptocurrencies which are based on another type of a distributed ledger called DAGs (Directed Accyclic Graphs) – it is a complex mathematical data structure, concepts of which are not covered in this presentation. So, which cryptocurrencies are blockchains, and which are DAGs?

Blockchain vs DAGs

It is important that there are more types of Distributed Ledgers, and more types of cryptocurrencies, and only some of them are presented on the slide. NAME OR NOT??? Let's move to the next part of presentation.

Problems

We detected a few problems in the field. The first problem is that the classification of all types of algorithms and protocols in Distributed Ledgers is outdated. Users who want to want to know how a particular distributed ledger is built, face the need in the fresh classification.

Outdated classification

Many new cryptocurrencies added, protocols used, and algorithms applied. Because this classification was designed in 2014, there is a vast area of upgrading this scheme.

Problems

The second problem is lack of technical information. The majority of websites regarding these technologies are consumer oriented, they do not provide important technichal details, which hardens the search of how a particular ledger is implemented.
The third problem is lack of affordable solutions being able to build a ledger from scratch, in educational or commercial purposes.
We aim to solve all these problems using the following methods.

Methodology of problem 1

They exactly match the problems. Outdated classification is solved by analyzing, classifying and structurizing information from trusted sources.

Methodology of problem 2

The second problem will be tackeled by building a structured, robust, easy to acces, and holding all needed without unnecessary information in one place, wiki, like a github, or notabug wiki.
The final problem will be solved by producing a Python library, which will contain all revied algorithms and protocols, and will be published to PyPi and will be available to everyone in world. The library should be easy to use, well documented and have a wiki page on github or notabug. This is the last method, and it is time to conclude the expected results.

Expected results

In the end of the research and programming work it is expected that all problems are solved using the stated methods. We expect to have an updated classification for 2019 and a well-documented

code and wiki. The text has to be written in affordable language without unnecessary information. This will help people to rapidly find technical info on any algorithm or protocol used in a particular Distributed Ledger. Let us move to the final.

References

The references which were used during the preparation are available on the slide.

Questions

Now there will be some time for us to discuss questions and unclear moments, if any. And if we will not succeed to cover all of them, please do not hesitate contacting us via these contacts.

Thnaks for attentions

Thanks.