Cryptographic Algorithms and Protocols for Distributed Ledgers

Sergey M. Avdoshin, Kirill I. Kupriyanov
*National Research University Higher School of Economics (HSE), Faculty of Computer Science,
School of Software Engineering,
3 Kochnovsky pass., 125319, Moscow, Russia

***Abstract*—The Blockchain technology is typically associated with Bitcoin, because it was the first system which has been distributed using the Blockchain technology. As the technologies evolved, the number of various blockchains with different kinds of applications had been drastically risen. A huge amount of blockchains can be explained by various cryptographic algorithms and protocols usage in them. It brought a problem of the absence of systematically gathered and structured information about cryptographic algorithms and protocols in existing distributed ledgers. The main objective of this work is to generalise all known common cryptographic algorithms and protocols, which are being used nowadays. The algorithms used in blockchains are going to be classified by common metrics: time complexity, space complexity, and the resistance to hacking. It is also intended to bring a programming library, where analyzed algorithms and protocols are gathered in one place. The library would serve as a toolbox for developers when creating a personal distributed ledger. Structured information and an accompanying programming toolbox will preliminary cause positive effect on approaching extension in this area.**

***Index Terms*—blockchain; bitcoin; distributed ledger; DLT; cryptography; classification; python**

I. Introduction

Recent years have witnessed a growing academic interest to cryptocurrencies, blockchains and distributed ledgers$^{section\ II}$. The past ten years have shown that the advance in the field of studying distributed ledgers and cryptocurrencies is enormous compared to any other field in the past. One of the results of the growing interest is thousands of researches carried out by scientists and individuals. These researches initiated the creation of hundreds cryptocurrencies and other uses of distributed ledgers. Some cryptocurrencies repeat each other in the form of algorithms (hashing, crypto-) and protocols used, but their spectrum is vast. Relatively little research has been carried out on the algorithms used, and even less on protocols. The generalisability of many published research on this issue is problematic. While most websites provide non-scientific explanations, there several studies, mainly [1], and [2] that provide some aggregation of information on algorithms and protocols in distributed ledgers. However, if consider the research in [1], firstly, a number of technical and essential questions remain about the classification of algorithms and protocols for distributed ledgers, and secondly, it had only been carried in 2014, which makes the information in it obsolete. New algorithms, modern applications of old algorithms, new cryptocurrencies and their protocols are being released every year, and nowadays there is a lot of possibilities to expand that area. This prospective work is designed to investigate the usage of modern algorithms and protocols in distributed ledgers and to make their up-to-date classification. The aim is to extend the existent classification with new algorithms and protocols, focusing on the broad scope of technologies and not on their number. According to plan, our detailed classification should reflect actual condition in the field of distributed ledgers. One more important point of the project is to collect all described implemented algorithms or code them if they have not been done yet in a complete library for free usage. This library will serve as a "toolbox" for a programmer who wants to build cryptoledger combining known algorithms and protocols from the developed library.

II. Technical Aspects

A definition of a distributed ledger, as well as the difference between distributed ledgers and blockchains must be given. A blockchain differs from a traditional spreadsheet or from another ledger in case of being a decentralized, distributed ledger, stored in a distributed databases of network devices. People refer to it as "distributed" because no single entity manages a distributed ledger system on its own. The ledger is distributed across a network of computers, also known as "nodes", and each involved party has an access to the ledger. This access allows all parties to receive real-time status updates on transactions which occur within the network of nodes.

Each record of a transaction in a blockchain is represented by a timestamped "block". Whenever a new block is generated on a blockchain, the system appends this block to the previous block using this blockchains unique algorithm. The visual result of the process is one of a "chain" of blocks. Hence the term "blockchain".

Not all distributed ledgers are blockchains. There are types of distributed ledgers, which represent DAGs (Directed Acyclic Graphs), or some other company-related data structure rather than the chain of blocks. But the majority of distributed ledgers serve to the purpose of maintaining the viability of cryptocurrencies. It does not mean that every Distributed Ledgers Technology is used for creating cryptocurrencies. Some of them are being used for different purposes, which are not covered in this paper.

III. Problem Statement

The importance of creating a comprehensive classification of cryptographic algorithms and protocols for distributed ledgers has recently been recognized by the industry. However, the existing classification is expired, and there are no any comprehensive study on them in the online sources. It may cause difficult for a user, who wants to work with distributed ledgers (e.g. cryptocurrencies), problems to overcome. A target user in terms of this research is a user, who is concerned about security and cryptography and who desires to reveal and understand algorithms are being used in the technology which is going to be encountered. If an actor wants to know what cryptographic algorithms and protocols is included when buying a cryptocurrency, it might be difficult to find that out and to compare the chosen one to other cryptocurrencies' algorithms and protocols. These are the possible consequences of modern tendency for websites to be consumer-oriented and provide only crisp and eye-appealing information. A major problem with this approach is that selling a content pretends to be the primary goal whereas the information delivery fades into the background. Consequently, it takes a long time for average user to find out an underlying algorithms in a particular distributed ledger.

Limitations of modern online "blockchain creators" is another problem for a target user. Platforms, which are to deliver (e.g. "cryptocurrency creation" service), on average provide up to 3 algorithms and even less protocols. In fact, in certain cases they do not provide user the ability to choose any preferred protocol. Taking that into account a target user will not be able to choose algorithms and protocol for his/her own ledger from the whole variety. The limitations that those services put on the user are problematic.

In summary, there is a need for a better understanding of a cryptoledger infrastructure and a structured approach in identifying and collecting the majority of cryptographic algorithms and protocols that are being used widely today. The following research questions need to be considered:

- What are the typical cryptographic algorithms found in various distributed ledgers;
- What are the typical cryptographic protocols found in various distributed ledgers;
- How to classify these algorithms for easier understanding and representing;
- What are the current industry practices as well as research advancements in each algorithm and protocol addressed;
- How to unify the knowledge gathered about cryptographic algorithms and protocols into one neat place;
- How to gather implemented algorithms and protocols into a programming library, which will be easy to use for creating own cryptoledger purpose?

IV. Objectives

An initial objective of the project was to identify, analyze and classify the broad scope of cryptographic algorithms and protocols in distributed ledgers. The main aspect of the objective is the broad scope of algorithms and protocols itself, not the quantity of distributed ledgers analyzed. It means that (e.g. some cryptocurrencies) may not be reviewd if algorithms and protocols they use have already been classified. This goal also includes the implementation of the programming library with algorithms and protocols for creating own cryptoledger. Particularly, the study has the following sub-objectives:

- To provide a comprehensive review of cryptographic algorithms found in various distributed ledgers;
- To provide a comprehensive review of cryptographic protocols found in various distributed ledgers;
- To develop a robust classification method for easier understanding and representing;
- To review current industry practices and researches in regards to cryptographic algorithms and protocols in distributed ledgers;
- To outline a unification method for working with all gathered information on the topic;
- To outline a programming method, language and methodology for providing the library with algorithms and protocols reviewed.

The result of this study will be valuable to the industry practitioners (our target users^{III}) as well as researchers. The data gathered will be concise, comprehensive, structured and easy to read. The program library is supposed to be a complete toolbox for creating own cryptoledger, choosing from a variety of gathered implemented algorithms and protocols.

V. Preliminary Literature Preview

Previous research [1] has established "current ctyptoprotocol infrastructure". By 2014, it was a complete and comprehensive diagram, showing all algorithms and protocols used in most popular distributed ledgers up to that time. The analysis is also well-structured, but generalisable. What is missing from the past study is a comprehensive and structured approach in determining algorithms and protocols for cryptoledgers analyzed. However, this study is the closest study to the topic discussed, and can be a great point for taking-off with this research. The whitepapers for such technologies as [3], [5], [6], [8], [7], and [4] will surely be used thruought conducting the research. The value of these monographies consists of the following facts:

- Whitepapers usually reveal algorithms and protocols used in a particular distributed ledger;
- Whitepapers usually point out the source code of algorithms and protocols, or even entire ledger.

VI. Methodology

The primary research method for this study is the literature review and benchmark analysis. Identification and classification of cryptographic algorithms and protocols in distributed ledgers is the first and the main step for reaching the aim of this work. This study will review various types of distributed ledgers, such as cryptocurrencies, and investigate their characteristics firstly. Then, based on the understanding of the underlying structure of every analyzed ledger, a list of all known algorithms and protocols will be produced. In the third stage of this work, the new classification will be developed. Finally, the programming part, where the implementations of gathered cryptographic algorithms and protocols will be assembled into a one complete library, will be done. This library will be a toolbox for users who want to build a specified cryptoledger. The library should be written in Python version

3.6.5 and published in a remote PyPI repository. It should also be installable using "pip" utility with optional "extra-url" argument. This study will be conducted between November 2018 and March 2019.

VII. Conclusion

The anticipated results of this research may potentially show that structured body of knowledge of cryptographic algorithms and protocols in distributed ledgers as well as the library, containing all the algorithms analyzed, may be useful for people who want to build own cryptoledger. People, who is interested in how certain cryptoledgers are implemented, will also benefet from this systematic research.

Looking ahead, published results will give public the ability to have an in-depth view on rapid and dinamically-moving area in modern technology. As well as the presented thesis, the pythonic library may potentially cause ripe business development of small legal entities. Concluding the above, it could be said, that the completed objective can make a huge effect on modern approaches for distributed ledgers.

References

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

[2] 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.

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

[4] Schwartz, D., Youngs,N., Britto, A., *The Ripple Protocol Consensus Algorithm*, 2014. [ebook] Available at: https://ripple.com/files/ripple_consensus_whitepaper.pdf [Accessed 9 Feb. 2019].

[5] The IOTA Foundation, *IOTA whitepaper*, 2016. [ebook] Available at: http://iotatoken.com/IOTA_Whitepaper.pdf [Accessed 9 Feb. 2019].

[6] Poon, J., Buterin, V., *Plasma: Scalable Autonomous Smart Contracts*, 2017. [ebook] Available at: https://plasma.io/plasma.pdf [Accessed 9 Feb. 2019].

[7] Sunerock, J. *Blackpaper*, 2019. [ebook] Available at: https://vergecurrency.com/static/blackpaper/verge-blackpaper-v5.0.pdf, 5th ed., [Accessed 9 Feb. 2019].

[8] TKEY DMCC, *TKEYCOIN TECHNICAL DESIGN DOCUMENTATION*, 2018. [ebook] Available at: https://tkeycoin.com/docs/whitepaper/whitepaper.pdf, [Accessed 9 Feb. 2019].

Word count: 1654w. ______________________________