



## Master Thesis: SOTA-Report on different Blockchain Protocols

### Context:

The reputed disruptive Blockchain technology gained more and more attention in the recent years. From the starting point, the Peer-to-Peer electronic cash service 'Bitcoin' in 2008, a variety of different siblings emerged. Some of them tackle new detected issues of the Bitcoin-protocol [1] and some other Blockchains address different application use areas. Certainly, Ethereum [2] was another massive milestone in Distributed Ledger Technology with the turing-complete programmability of Smart Contracts.

### Problem Statement:

The explosive amount of research spent from several groups all over the world have led to an actual jungle of various Blockchain protocols. In addition to the steep learning curve coming with Blockchain Technology, novices are confronted with a scattered literature structure. A big advance was the publication of a taxonomy of Blockchain Technologies [4]. The authors have classified the terms and functionalities of many Blockchain protocols. This provides a very useful overview of the current strategies addressed in the protocols. However, special attention was given to the abstract building blocks of Blockchains and not on fully describe the single protocols which is central to this master thesis.

### Task:

An initial step is to fully understand the basic functioning of Blockchain Technology. A good starting point are the two "big" protocols Bitcoin [5] and Ethereum [6]. Depending on the own preferences, some might prefer to start with the taxonomy [4] and read the specific protocols afterwards.

Having a good overview of Blockchain technology, the student can start with digging deep into the heap of protocols. The references list of [4] will help to find some of them. The student must read the specifications of the protocols which can be found either by using literature databases (Google Scholar etc.) or search engines using keywords like "[PROTOCOL NAME] white paper" or "[PROTOCOL NAME] yellow paper". Some papers are also hosted within the protocol's GitHub repositories. While reading the different specifications, the student will classify the protocols by various categories. These categories might come from [4], but there will be a need of extending them, e.g. storage format: Bitcoin -> Blockchain, IOTA -> Directed Acyclic Graph, ...

The student is free to extend the possible categories. They can also be of practical nature, e.g. the set up of the network can be under investigation or the usability or the expressive power of the programming languages.

## Goal:

The goal of the thesis is a complete overview of many Blockchain protocols. The overview can be presented in tabular form, or in the form of taxonomies, ontologies, UML diagrams, Database schemas, ... The student must decide on the best fitting form. With the help of the thesis, other people must immediately be able to answer questions like "What protocols have unlimited-deterministic asset supply management?" (The question should be clear after reading [4]) or "Show me a complete overview of the protocol 'Dogecoin'". For the latter question, also a small Web-application is thinkable, where the findings in the master thesis builds the database and the user-interface shows the information of the protocols.

The thesis is evaluated on the extent in terms of number of protocols which are investigated, as well as the extent of the categories in which the protocols are classified. On top, the scientific methods will affect the grading and the knowledge gain of the student during the thesis. The usability, i.e. how easy someone can retrieve information on protocols (cf. the questions in the paragraph above) will heavily affect the overall rating. As stated, this can be done by a web application or appropriate presentations in the written thesis.

## References

[1] <https://bitcoin.org/bitcoin.pdf>

[2] <https://ethereum.github.io/yellowpaper/paper.pdf>

[4] Paolo Tasca: A Taxonomy of Blockchain Technologies: Principles of Identification and Classification

[5] Andreas Antonopoulos: Mastering Bitcoin

[6] Andreas Antonopoulos: Mastering Ethereum