# P2P Systems and Blockchains Thesis Proposals May 2021

## 1) Simulate payment routing strategies on the Lightning Network

**Keywords** Routing design and simulation - Lighting Network

**Context** The Lightning Network is a P2P overlay built on top of Bitcoin. The goal is to enable transactions that are not restricted by the Bitcoin mining, which takes about 15 minutes to create a block, and generally 1 hour to confirm a transaction. Currently, the Lightning Network consists of 20K nodes and 45K channels (edges) (https://1ml.com/), even though the number might change depending on the source. A node can pay another node exploiting a multi-hop payment, where the intermediate nodes forward some coins from the sender to the receiver, but retaining a small fee. To improve privacy, the Lightning Network payment utilize Onion routing, like Tor, therefore the payment path is source routed, i.e. is chosen by the sender.

**Goal** The goal of this thesis is to evaluate and compare multiple source routing algorithms, and simulate them. This problem has the following constraints: the Lightning Network can be seen as a weighted graph, where each channel has a balance (weight), but the balance is in reality an upper bound of the payment capability of a node, that is potentially unknown; an intermediate node has to be online to carry on the payment; each intermediate node applies a fee; and more.

**Outline** The thesis would follow these steps:

1. Study and identify the source routing algorithm present in the Lightning Network;

2. Given a snapshot of a Lightning Network, that will be provided to the student, implement a few routing algorithms;

    - Possibly, exploit the identity of known nodes that act as hubs in the algorithm's choices;

3. Simulate the routing algorithms on multiple snapshots and interpret the results.

### References and related work

- A beginner guide to the Lightning Network

- A Cryptoeconomic Traffic Analysis of Bitcoin's Lightning Network and their simulator
- Flare: An Approach to Routingin Lightning Network

## 2) Analysis of the Ethereum ERC20 token ecosystem

**Keywords** Data gathering, preprocessing, and analysis - Ethereum - Token ERC20

**Context** Ethereum Decentralized Applications (DApp) have become very popular, especially applications involving custom sub-currencies, also known as tokens. The Ethereum community proposed the ERC20 standard, so that each token could be implemented equally, following a common interface. As a consequence, it is possible to query the Ethereum blockchain to find all the transactions and smart contracts related to any ERC20 token. One approach would be looking for the specific ERC20 events emitted by the smart contracts.

**Goal** The goal of this thesis is to study the ecosystem of the Ethereum ERC20 tokens, analyzing the transactions. In particular, the analysis should answer to the following questions:

- Does the token economy have a particular pattern, common to most of the tokens?
  - for example, does typically exist a big hub/token exchange and many addresses owning a small amount?
- Are tokens exchanged frequently? How many times an address transfers a token?
  - build the transaction graph to find payment paths between the addresses, or find if there exist interesting patterns, either static or temporal;
- Are the token economies very similar to each other?
  - for example, token1 and token2 do have the same behavior? Such as, a big hub and all transactions go mostly through the hub, etc.
- Optionally, associate the findings of the most popular ERC20 tokens with other usage statistics that can be retrieved online.

Other questions might arise during the development of the thesis.

**Outline** The thesis would follow these steps:

1. Download and sync the Ethereum blockchain;
2. Query the blocks, and create a dataset composed by the transactions involving only ERC20 tokens;
3. Explore and analyse the dataset to answer the questions. The analysis could involve the application of advanced analysis tools such as temporal series and unsupervised classification methods.

### References and related work

- Ethereum ERC20 standard
- Measuring Ethereum-Based ERC20 Token Networks
- Traveling the token world: A graph analysis of Ethereum ERC20 token ecosystem

# 3) Enhancing the EOS.IO Access Control ecosystem

### Context

The EOS.IO [1] software introduces a new generation of blockchain architecture designed to work on Delegated Proof of Stake (DPOS) consensus algorithm. It provides the basic building blocks for developing enterprise Decentralized Applications (DApps), such as, accounts, authentication, databases, and asynchronous communication. A smart contract in EOS.IO is a C++ program that can be executed on the blockchain as a trusted computation and this execution takes part of the immutable history of the blockchain. The EOS.IO software provides a simple role-based permission management [2] system that gives to users high-level control on who can execute actions over another smart contract.

**Goal** The goal of this thesis is to enhance the role-based permission management system provided by EOS.IO. In particular, this work involves the definition and development of a general-purpose tool for managing permissions of DApps. The tool must support at least a common and basic form of access control (such as, hierarchical groups and multiple permissions).

**Outline** The thesis would follow these steps:

1. Study the reference EOS.IO blockchain platform and learn its permission management system;
2. Identify a suitable access control pattern to be integrated;
3. Design the tool and implement it on the EOS.IO in order to evaluate its performance;

### References and related work

1. https://developers.eos.io/
2. https://medium.com/leclevietnam/understanding-eos-permission-ee60dcfec8ad
3. De Capitani, Sara Foresti, and Pierangela Samarati. "Authorization and access control." Security, Privacy, and Trust in Modern Data Management. Springer, Berlin, Heidelberg, 2007. 39-53.

## 4) Credentials Management System for a Self-Soverign Identity ecosystem

**Context** Self-Soverign Identity, (SSI), [1] is recent paradigm which helps individuals in managing their digital identity autonomously. Indeed, in contrast to centralized identity management systems where a service provider creates, maintains, and manages identity information of individuals, the SSI allows individuals to create Decentralized Identifiers [2] (DID) which can be issued to the different service providers. The individuals can prove control over their DIDs, without relying on any other parties, and can create one or more assertions about a subject. Such assertions are known as Verifiable Credentials [3] because they can be cryptographically verified by any individual and they cannot be tampered from other users without visible damage.

**Goal** The main purpose of this thesis is to design and develop a system entity that acts as a source of Verifiable Credentials by using reference libraries. The system allows an individual to upload one or more Verifiable Credential Presentations containing information derived from the original verifiable credentials (and it can be synthesized by using zero-knowledge proofs for example). Presentations are protected against tampering and they can be shared with verifiers.

**Outline** The thesis would follow these steps:

1. Study and learn the reference libraries used to deal with Decentralized Identifiers and Verifiable Credential;
2. Identify the key requirements of the system by exploiting reference use cases and design the system;
3. Implement and test the system in order to evaluate its performance.

### References and related work

1. Mühle, Alexander, et al. ”A survey on essential components of a self-sovereign identity.” Computer Science Review 30 (2018): 80-86.
2. https://www.w3.org/TR/did-core/
3. https://www.w3.org/TR/vc-data-model/