# Master Degree Thesis Proposals
# Research Group on
# Blockchain and Social Networking
# Reference: Laura Ricci (laura.ricci@di.unipi.it)
# May 2020

This document presents a set of topics for Master Thesis related to research areas I am currently investigating with my research group. If you are interested, you can contact me **by e-mail (laura.ricci@unipi.it), to fix a Skype/Meet call.**

# Blockchain: Research Topics

**Thesis 1**
**Title: Analysis of the topology of the Lightning Network**

**Thesis description and goals:** Actually, this thesis is of a **complex network analysis.** Scalability has historically been a major drawback of Blockchain protocols. In fact, one of the main critiques to cryptocurrencies, such as Bitcoin, has always been their modest transaction throughput, insufficient for real world global applications. As such, much research has been dedicated to the study of alternatives and improvements to increase transaction throughput. One of such proposals is the Lightning network protocol. The lightning network is a P2P network of payment side channels opened by users. It allows any two users on the network to exchange value among a path of mutually untrusted channels. Since its inception in January 2018 the network has seen a considerable growth, as well as the appearance of big channel hubs. In fact, each channel has a fee to be used, and central nodes make a profit by keeping their channels funded and usable by peers on the periphery. Aim of this thesis is to build a **network prober,** capable of reconstructing the entire network topology from a single input point. This means creating a channel towards two periphery nodes on the LN and to find all possible paths between them iteratively to cover all connected components. Such prober will be used to perform:

- a connectivity analysis of the network
- a temporal study of the network
- a dynamic stability analysis of the network.

The probing may be performed mostly through available tools that operate through flexible RPC Lighning Network APIs.

**Thesis 2**
**Thesis title: Lightning Network Routing Protocols**

**Thesis description and goals:** The aim of this thesis is to investigate **new payment routing algorithms** for the Lightning Network. The design goal for these algorithms is to ensure that routes can be found as quickly as possible. This may be accomplished by enabling each node to proactively gather information about the Lightning Network topology and by defining the routing problem as a min cost flow problem, which to be solved in a distributed setting. The definition of the algorithm should consider:

- privacy issues
- enhancing the algorithm by exploiting the social behaviour of the nodes
- channels balance techniques

This thesis is oriented **to network routing, at application level.**

**Thesis 3**
**Investigating the Algorand Blockchain**

**Thesis description and goals:** Algorand is a truly democratic and efficient way to implement a public ledger. Unlike prior implementations based on proof of work, it requires a negligible amount of computation, and generates a transaction history that will not "fork" with overwhelming high probability. Algorand is based on a novel and super fast message-passing- based Byzantine agreement.
This thesis will investigate the Algorand eco-system, by studying the consensus algorithm and by exploiting the Algorand (see API at https://developer.algorand.org/docs/reference/sdks/) to investigate the Algorand echo-system.

# Blockchains: Practical Applications

**Thesis 1**

**Distributed Ledger Technologies for Digital Rights Management (DLT4DRM)**

**Thesis type:** master's degree (6 months)

**Thesis description and goals:** Blockchain technologies allow registering digital works with a decentralized Intellectual Property protection approach, increasing the visibility and availability of information about content ownership and copyright. The goal of this thesis is to develop a blockchain-enabled digital rights management (DRM) platform allowing to:

- Enlist the content that users want to upload to make it available to others, while maintaining its copyright, or simply registering themselves as the authors of it.
- Reward the creation and curation of content.
- Automate Copyrights negotiation through the implementation of smart contracts that allow local configurations of terms of use for IP, and direct interactions between the interested parties.
- Create an innovative DRM model enabled by blockchain technology for trusted timestamping, keeping an immutable record of copyrighted work and smart contracts to manage sales automatically.

During the thesis the student, supported by a tutor, will be able to:

- Understand the state-of-the-art of digital rights management topic and properly articulate research questions.
- Understand the state-of-the-art and the principles of Distributed Ledger Technologies.
- Learn how to leverage trusted timestamping, to securely keep track of the creation and modification time of a digital artifact and hash functions, to generate content fingerprint so that an author can obtain a unique.
- Learn how to develop smart contract and tokenization mechanisms.

Prerequisites:

- Basic knowledge of Distributed Ledger Technologies
- Good programming skills (Javascript, Solidity, GoLang, HTML/CSS, C++, Node.js)
- Fluency in written/spoken English
- Good independence and problem-solving attitude

**Thesis 2**

**Distributed Ledger Technologies for Digital Handshaking (DLT4DH)**

**Thesis type:** master's degree (6 months)

**Thesis description and goals:** The thesis will focus on the study, the design and the implementation of a Digital Handshake Proof-of-Concept (PoC) based on Blockchain technologies to provide a secure, fast and reliable way to manage contracts and agreements between small providers/sellers and their customers. Such a system will allow two users, who might be two artisans or an artisan and her/his customer, to virtually agree on simple contract terms. The work will be divided in the following phases: (i) analysis of the state of the art of existing solutions for digital handshake; (ii) configuration of Hyperledger Fabric and EOSIO blockchain platform; (iii) smart contract development; (iv) creation of incentive mechanism based on tokenization design practice; (v) development of a simple web interface for final users.
During the thesis the student, supported by a tutor, will be able to:

- Understand the state-of-the-art of digital handshake topic and properly articulate research questions.
- Understand the state-of-the-art and the principles of Distributed Ledger Technologies.
- Learn how to configure and use blockchain permissioned and permissionless technologies.
- Learn how to develop smart contract and tokenization mechanisms.

Prerequisites:

- Basic knowledge of Distributed Ledger Technologies
- Good programming skills (Javascript, Solidity, GoLang, HTML/CSS, C++, Node.js)
- Fluent in written/spoken English
- Good independence and problem-solving attitude

**Thesis 3**

**CONDAC: Condos as DACs**

**Thesis type**: masters' degree (6 months)

**Thesis description and goals**: the thesis will focus on the design, implementation and simulation of the mechanisms of a Decentralized Autonomous Community (DAC) aiming at digitalizing condominium administration processes. The goal is to demonstrate that the application of DLTs to a traditional process, such as administration of condominiums, can have a relevant impact on levels of efficiency, transparency and trust.
In the first month, the problem will be investigated and potential issues will be identified. Innovative DLT-basd services (voting, delegation, tokenization, assets digitalization and exchange, etc.) will be analysed and applied to evaluate the feasibility of the solution and its capacity to deliver valuable outcomes.
During the next 5 months, a Proof-Of-Concept (PoC) will be implemented by exploiting a delegated proof-of-stake infrastructure, smart contracts and tokenization to develop an ad hoc solution. EOS will be the reference blockchain architecture that will be used to implement the solution.

Prerequisites:

- Good knowledge of Distributed Ledger Technologies foundations
- Solid programming skills (Solidity, Javascript, HTML/CSS, C++, Node.js)
- Good knowledge of Linux OS
- Fluent in written/spoken English
- Good independence and problem-solving attitude

# Complex Network Analysis

## Thesis 1
### Distributed Community Detection

The study of complex networks, such as social networks, can uncover hidden properties which are not clear in the first place. In particular, community detection was one of the most investigated problems and was proven to be successful in containing the spread of viruses, as a method for link prediction, or to profile users. In centralised scenarios, a lot of effort was put in the field and currently, community detection algorithms can be classified in global or local. Global approaches focus their attention in trying to detect communities according to some properties of the whole network, such as trying to minimize conductance of a partition or maximise the modularity of the partition. On the other hand, local approaches try to detect the community structure by exploiting local information, such as the local clustering coefficient. There are several issues concerning the research of local community detection. Several local community detection algorithms use the ego network structure to model the local information of a node. In this thesis, the student will tackle the problem without restricting to the ego network of the users, but instead create a **community structure that is network-wide**. The added challenge is to design the algorithm in a completely decentralized fashion so that the nodes organise themselves and reach a consensus on the community structure. Finally, we also plan to include many self-* properties, such as self-organising, self-healing, and so on.

## Thesis 2
### Facebook Group analysis

During the last years, the way people communicate over social media platforms is changing and even platforms are constantly evolving to increase the meaningfulness and the quality of the interactions among users. For instance, Facebook recently puts a lot of effort in improving the user experience in the groups by adding new reactions and roles, while on the other hand Steemit, the most successful Blockchain Online Social Media, recently introduced the "communities", which is the first equivalent mechanism on a decentralized platform. The way these so-called Online Social Groups work is pretty unique compared to the rest of the common social networking platforms, indeed they are usually themed, and adopt a broadcast-like way of communication. These groups are themed because they usually revolve around specific themes, such as music, and all users in the group tend to share the same broad

view or opinion, or usually, the groups gather people sharing something, such as the living place. Moreover, the communication model does not revolve anymore around a specific user, but around the group itself in a broadcast fashion. Users do not need to explicitly connect to each other to start interacting, but rather they just need to be part of the group, so anyone, with just one request, can enter in contact with potentially million other users, rather than having to search for them one by one and send a request each. The importance of these groups is becoming crucial on social platforms, indeed users started using their private wall as a personal diary, but they use social groups to socialize with other people. Indeed, the need for studying and understanding better how the new social model affects how people interact with each other on social groups. Aim of the thesis is to find potentially active groups among the Facebook groups and write a scraper to download some raw data about users' interactions. The data is very rich, because not only the textual part is available, but also the "roles" in the group and the reactions to each contribution can be retrieved. After a relevant dataset is gathered, a set of analyses can be performed on the dataset, such as the detection of Dunbar Circles, the detection of interaction communities or the prediction of future interactions.

**Thesis 3**
**Distributed Analysis**

The world dramatically changed with the rise of Artificial Intelligence, which became seamlessly part of everyone's life. It is widely known which are the limits of machine learning approaches; the two most important ones are the need of a sufficient amount of data and the means to store them, and the need for a machine powerful enough to develop a good model. These big challenges often impose restrictions on the scenarios in which they can be applied. Indeed, in peer-to-peer systems, it is a very hard task to use such a tool without having external support, such as a cloud resource. Trying to adapt these tools to truly p2p systems was an object of research and some results were already achieved. In this thesis, we want to test the feasibility of completely distributed approaches either by applying ensemble learning techniques or distributing the data over the nodes. Of paramount importance is to evaluate the loss of quality, in case of simplified models or reduced/imbalanced data available to nodes. Finally, we are interested in techniques to cope with the loss of accuracy of the models, such as Continual Learning, and model merging techniques.