Proposals for Master Degree Thesis
Research Group on
Blockchain and Social Networking
Reference: Laura Ricci
May 2019

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), or during the question time, on thursday, 15.00-18.00.

Research Area: blockchain technology

1. *A Blockchain based framework for Citypost*

   Citypost S.p.A, born in 2000 in Pisa, works in the area of postal services and, with its franchising Sailpost, counts 140 main agencies and a large number of offices. This makes it the most important postal franchising operator in Italy.

   From 2017, Citypost starts to give services of delivery of small parcels for Amazon e Groupon. The services offered by Citypost involve several actors: brokers for package flows to assign to shippers on the basis of the good characteristics; fullfillment and logistic operators; dropshipping operators which offer web portals hosting Web products and so on.

   In this scenario, each package, before arriving at the final destination, can be managed by a set of actors, each one offering a part of the service or a part of the path toward the destination. All operators must report a feedback towards the seller and the buyer must control the advancement of the packet toward the destination. The goal of this thesis is to analyze the tracking scenario in the area of postal logistics of Sailpost, and to check the benefits of the adoption of the blockchain technology. A proof of concept tracking system for Sailpost will be implemented by exploiting a permissoned blockchain of the Hyperledger family.

2. *Digital Assets: safekeeping and management of the private keys*

   The diffusion of digital assets is continously growing: it starts with the cryptocurrencies (e.g., Bitcoin), it continues in the financial fields with the ICO/STO and, in the last times, it regards the redefinition of trational currencies as digital assets (stablecoin with JP Morgan and Facebook).

   Even if this brings to new interesting scenarios, it introduces novel problems, like that of the sefekeeping and management of the privete keys. Loss, thefts and legacy are real life scenarios that must be faced for the real introduction of digital assets.

This thesis is a joint proposal of my group and of the CONIO company, and regards the analysis of systems for the key decomposition (e.g., Shamir's Secret Sharing and multi-key signatures), with the goal of developing systems, based on trustless frameworks which reduce the risks related to the management of the private keys, offering, at the same time, ease of use in the real life.

Some references that introduce the problem of key management:

- *Fast Multiparty Threshold ECDSA with Fast Trustless Setup* (Rosario Gennaro, Steven Goldfeder) `https://eprint.iacr.org/2019/114.pdf`.
- *Fast Secure Multiparty ECDSA with Practical Distributed Key Generation and Applications to Cryptocurrency Custody* (Yehuda Lindell, Ariel Nof, Samuel Ranellucci) `https://eprint.iacr.org/2018/987.pdf`
- Video: `https://www.youtube.com/watch?v=Qv4-vh-KJ1s`

3. *Investigating Stable Coins*

   The diffusion of digital assets is continously growing: it has started with the cryptocurrencies (e.g., Bitcoin), and currently the traditional currency have been redefined in the digital world (i.e., Stablecoin projects like JP Morgan e Facebook).

   The aim of this thesis is to analyze a set of existing stablecoin present on private blockchains and the different protocols for the distributed consensus (e.g., Proof of Authority, Paxos, Raft), and then to implement novel solutions characterized by good characteristics of scalability, efficiency and resilience. The thesis will be developed in the framework of a collaboration between my group and the CONIO company.

Research Area: Social Networks

1. *Trust in Social networks through Ant Algorithms*

   In social networks, users share their experience, relations, views, etc. It is very important to provide trust mechanism to establish a trust relationship between users and the source of information and the consumers of the information on the social network. Trust prediction has become one of the most important tools for finding and identifying the potential trust relationship between any online communities. Such a reliable source of information of the users in the community would be recommended to other targets and online communities. In the literature, several trust models have been proposed, but the propblem of trust definition and propagation is still a complex one. This thesis will investigate models of trust for social networks and a class of algorithms, i.e. ant algorithms, which can be used to propagate trust. The thesis will be developed within the Europen Project *HELIOS: A Context-aware Distributed Social Networking Framework*, in collaboration with the *Trinity College of Dublin*.

2. *Privacy policies in Social Networks: a blockchain based approach*

   In the last years, several distributed online social networks have been proposed, like Diaspora, Mastodon and some blockchian based social networks, like Steemit and Peepeth. An interesting class of proposals are those where social data are not stored on the blockchian and the blockchain is exploited to check the control policies for accessing social data of the users. The thesis will investigate which type of access control (attribute based, role based, history based) is more suitable for the scenario of social networks and will implement a solution integrating a distributed file system like IPFS (`https://en.wikipedia.org/wiki/InterPlanetary_File_System)`, with a blockchain-based access control system.

3. *Link prediction and Social Network Analysis on Multilayer Networks* During the last years, the user have started to exploit more and more social networks, so fragmenting information in their profile into different social networks. A new model of multiple social network has gained interest, the multilayer social network model. This thesis will investigate this new model and how the classical algorithms, like those for link prediction, have to be re-adaptedto these model. The thesis will be developed within the H2020 Europen Project *HELIOS: A Context-aware Distributed Social Networking Framework*.