Research Internship - LIP6 - Complex Networks

Robustness of Web of Trust Mechanisms

Laboratory: Laboratoire d'Informatique de Paris 6 (UMR 7606)
Team: Complex Networks (http://www.complexnetworks.fr/)
Supervisors: Nicolas Gensollen (nicolas.gensollen@lip6.fr)
Matthieu Latapy (matthieu.latapy@lip6.fr)

Motivation: Reputation systems are programs that allow users to rate each other in online communities in order to build trust through reputation. These systems are commonly used on E-commerce websites such as Ebay, or online advice communities such as Stack Exchange. A specific instance of a reputation system is a web of trust mechanism in which users of a given system are organized over a dynamical network. Nodes can enter or leave the network as users sign up or cancel their membership. Links, which specify the trust relationships between the nodes, can appear and disappear as these relationships are forged or broken.

We will focus here on a new cryptocurrency called $\tilde{G}1$ [1] [2] in which a web of trust mechanism is implemented to identify its members. In this cryptocurrency, the monetary growth is not related to mining (as it is the case for Bitcoin for example), but is shared evenly among the members. This makes $\tilde{G}1$ the first "libre" cryptocurrency [3]. In other words, each member of this system receives every day one share of the monetary growth as a *universal dividend.* For this reason, each member account has to match one, and only one, real living human being. Otherwise, anybody would be able to create multiple accounts and receive multiple dividends, which would have catastrophic consequences on the stability of the currency.

The proper identification of the members, and therefore, the integrity of the web of trust itself, are extremely important. To protect this system from Sybil attacks, some rules have been designed by the developers of $\tilde{G}1$ [4] [5]. Some of these rules are purely topological (for example, all members have to have at least five certifications at any time), while other rules are linked to the dynamics of the system (for example, certifications emitted by a member have to be separated by at least five days). These rules rely on preliminary work done by the core developers of $\tilde{G}1$, but additional studies are needed to investigate how they impact and protect the integrity of the web of trust.

Objectives of the internship: The internship aims at:

(i) - modeling and describing the $\tilde{G}1$ web of trust as a dynamical network in which nodes and links appear and disappear over time. Stream graph models [6] developed by the complex networks team could for example be used here.

(ii) - studying the robustness of generated and existing webs of trust against malicious attacks as well as the consequences of these attacks on the cryptocurrency itself (inflation, deflation...).

(iii) - proposing new sets of rules that better guarantee the integrity of the system.

Required skills: A good knowledge of one scientific programming language such as Python or Julia is required. Any experience or knowledge in graph theory, complex systems, modeling, or simulation of dynamical systems would be a plus. English.

References and useful links:

[1] https://monnaie-libre.fr/
[2] https://g1.duniter.fr//app/home
[3] https://trm.creationmonetaire.info/
[4] https://g1.duniter.fr//app/currency/lg
[5] https://duniter.org/en/deep-dive-into-the-web-of-trust/
[6] *Stream Graphs and Link Streams for the Modeling of Interactions over Time*, Matthieu Latapy, Tiphaine Viard and Clémence Magnien Social Networks Analysis and Mining, 8: 61, 2018