Master thesis : Vivisecting Blockchain P2P Networks

Auteur : Ben Mariem, Sami
Promoteur(s) : Donnet, Benoît
Faculté : Faculté des Sciences appliquées
Diplôme : Master : ingénieur civil en informatique, à finalité spécialisée en "computer systems security"
Année académique : 2018-2019
URI/URL : http://hdl.handle.net/2268.2/6791

UNIVERSITY OF LIEGE

Abstract

University of Liege
Faculty of Applied Science

Master in Civil Computer Science Engineering
Professional focus on Computer Systems and Security

Vivisecting Blockchain P2P Networks

by Sami BEN MARIEM

"**A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution**"
(Satoshi Nakamoto, 2009, p. 1)

The idea behind this statement has been the key motivation for the development of the *"crypto-currencies"*. Indeed, those digital currencies rely on a recent implementation of an immutable and distributed ledger -i.e, the *Blockchain* - to allow transactions to take place in a distributed and decentralised manner without the need for any central authority. Blockchains are typically managed by peer-to-peer networks, which provide the support and substrate to the so-called *distributed ledger*, a replicated, shared and synchronised data structure, geographically spread across multiple nodes. Indeed, peer-to-peer networks allow the system to disseminate information among its peers while keeping it as much decentralised as possible.

In this paper, the network side of the blockchain technology will be studied, by characterising its topology and main properties from a purely network measurements-based approach. This will be done by analysing the most relevant cryptocurrency network : the *Bitcoin peer-to-peer network*.
First, the Blockchain technology as well as one of its most famous implementation -i.e., the Bitcoin - will be presented from a theoretical point of view, using well-known notions of Cryptography and Distributed Systems. Then, the methodology used for characterising the entities of the bitcoin network as well a passive measurements-based approach to unveil the topology of blockchain P2P network will be described. Finally, a characterisation of the bitcoin entities will be given through the combined analysis of multiple snapshots of the Bitcoin network as well as by using other publicly available data sources. As it is shown and discuss, many key ideas and methods are likely to be reusable in various other fields using the blockchain technology. Therefore, the impact of this thesis reaches far beyond the Bitcoin technology itself.

Among other relevant findings, it is shown that *(i)* the size of the BTC network has remained almost constant during the last 12 months – since the major BTC price drop in early 2018, *(ii)* most of the BTC P2P network resides in US and EU countries, and *(iii)* despite this western network locality, most of the mining activity and corresponding revenue is controlled by major mining pools located in China.

Remark: Several results that are presented in this thesis have been previously presented in the paper : *"Vivisecting Blockchain P2P Networks: Unveiling the Bitcoin IP Network"*