Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Prof. Laurent Vanbever
Networked Systems Group

Protecting Blockchain Applications with Programmable Networks

Project thesis proposal

Any application that uses the blockchain technology is to some extend vulnerable to routing attacks. An AS-level adversary can prevent nodes from reaching each other thus preventing them from exchanging updates on the distributed ledger. Even the most successful crypto-currency, namely Bitcoin [3] has been proven to be vulnerable to network attacks [2].

Fortunately, we found it is feasible to build a relay network that protects the bitcoin system and potentially any application on top of the blockchain from routing attacks. Such a relay network is composed of nodes (relays) that are strategically located in the Internet such that connectivity among relays cannot be diverged using BGP hijacking. The relay network also needs to guarantee continuous exchange of information among any number of nodes that are connected to at least one of the relays.

While promising, such an architecture relies on few nodes. As such, the BTC system (or any distributed system using the relays) becomes more centralized and thus more vulnerable to DDoS attacks. To shield against this attack vector as well as to allow fast on-line anomaly detection we propose the use of programmable hardware instead of traditional servers for implementing the relays. Programmable hardware [1] is capable of satisfying orders of magnitude more requests than a regular sever.

Thus, the goal of this project is to design and implement a protocol to enable a scalable communication between the programmable network device that will act as a relay node and an extended bitcoin client.

Requirements

- Excellent programming skills.
- C++ Knowledge.

Contact

- Maria Apostolaki, apmaria@ethz.ch
- Prof. Dr. Laurent Vanbever, lvanbever@ethz.ch

Tentative schedule

Week 1 Week 2	• Familiarize with the routing attacks • Familiarize with concepts of the Bitcoin code base
Week 3 Week 4 Week 5	• Design the Bitcoin client API. • Implement extension of the Bitcoin client to communicate with a switch and send requests.
Week 6 Week 7	• Design the switch API. • P4 implementation of the switch API that will answer queries or will direct them to a Master client.
Week 8 Week 9 Week 10	• Build a testbed of a Tofino Switch connected to thousands of Bitcoin clients. • Measure the throughput.
Week 11 Week 12	• Write report

References

[1] P. Bosshart, D. Daly, G. Gibb, M. Izzard, N. McKeown, J. Rexford, C. Schlesinger, D. Talayco, A. Vahdat, G. Varghese, and D. Walker. P4: Programming protocol-independent packet processors. *SIGCOMM Comput. Commun. Rev.*, 44(3):87–95, July 2014.

[2] A. Maria, Z. Aviv, and V. Laurent. Hijacking bitcoin: Routing attacks on cryptocurrencies. In *Security and Privacy (SP), 2017 IEEE Symposium on*. IEEE, 2017.

[3] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf.