Bento: Bringing Network Function Virtualization to Tor

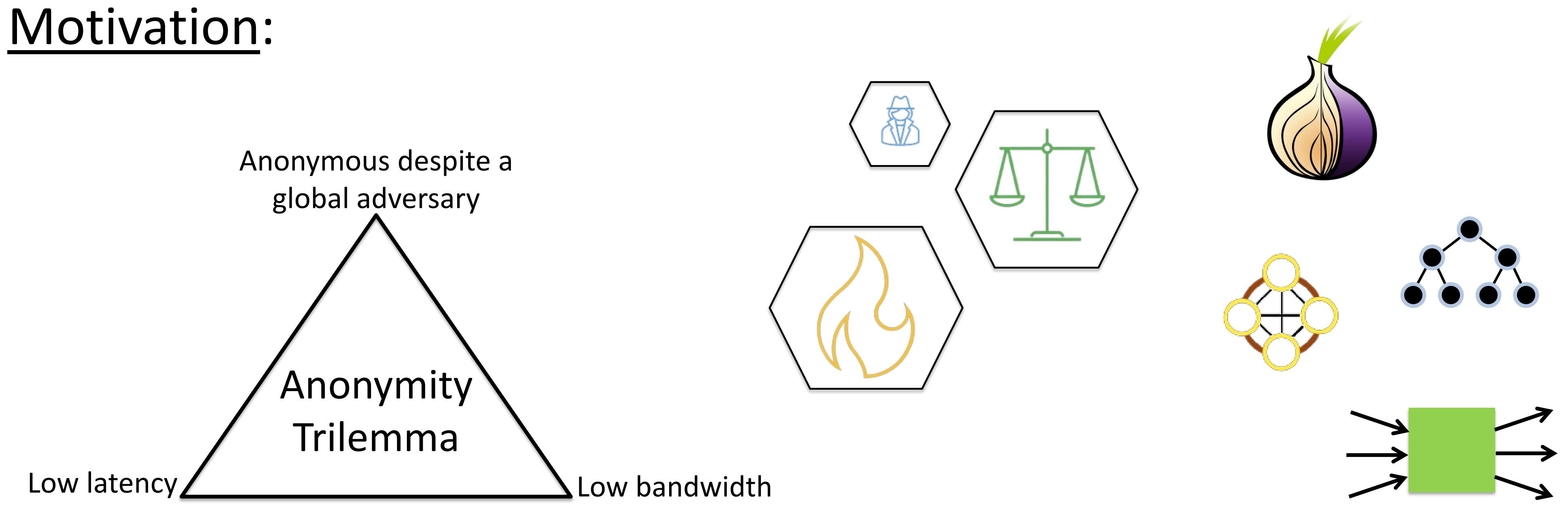
Christina Garman, Purdue University and Dave Levin, University of Maryland

https://bento.cs.umd.edu/

Tor is a powerful and important tool for providing anonymity and censorship resistance to users around the world. Yet it is surprisingly difficult to deploy new services in Tor—it is largely relegated to proxies and hidden services—or to nimbly react to new forms of attack. Conversely, "non-anonymous" Internet services are thriving like never before because of recent advances in programmable networks, such as Network Function Virtualization (NFV) which provides programmable in-network middleboxes.

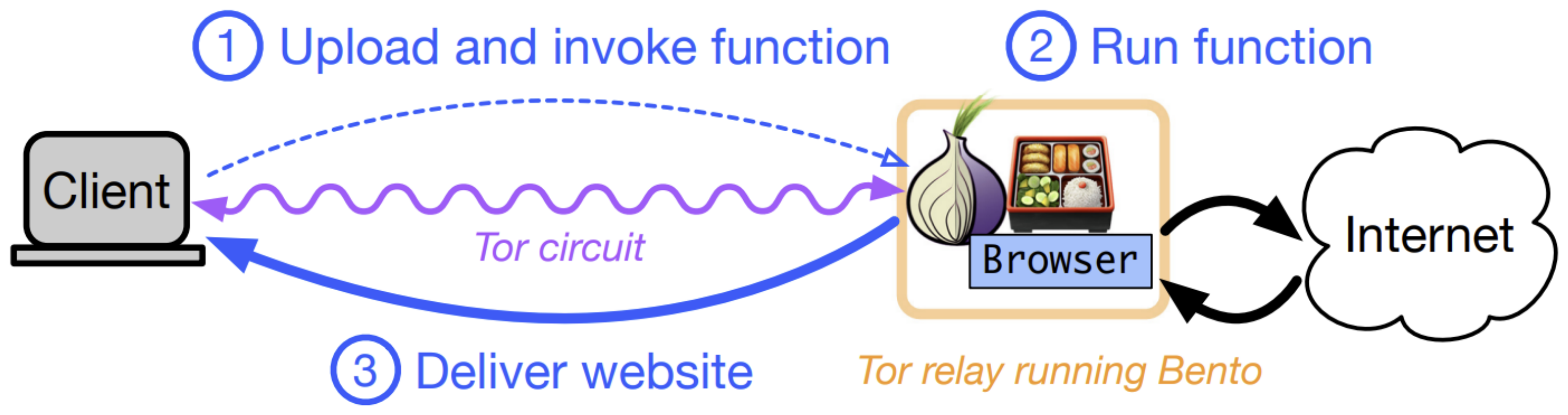
Bento seeks to close this gap by introducing programmable middleboxes into the Tor network. In this architecture, users can install and run sophisticated "functions" on willing Tor routers, further improving anonymity, resilience to attack, performance of hidden services, and more. We present the design of an architecture, Bento, that protects middlebox nodes from the functions they run—and protects the functions from the middleboxes they run on. Bento does not require modifications to Tor and can run on the live Tor network. With Bento, we can significantly extend the capabilities of Tor to meet users' anonymity needs and nimbly react to new threats.

Motivation:



While all three properties above may not be simultaneously achievable for all users, we argue that a more programmable anonymity network can let users choose the precise set of trade-offs they want, when they want them.

Example Application:

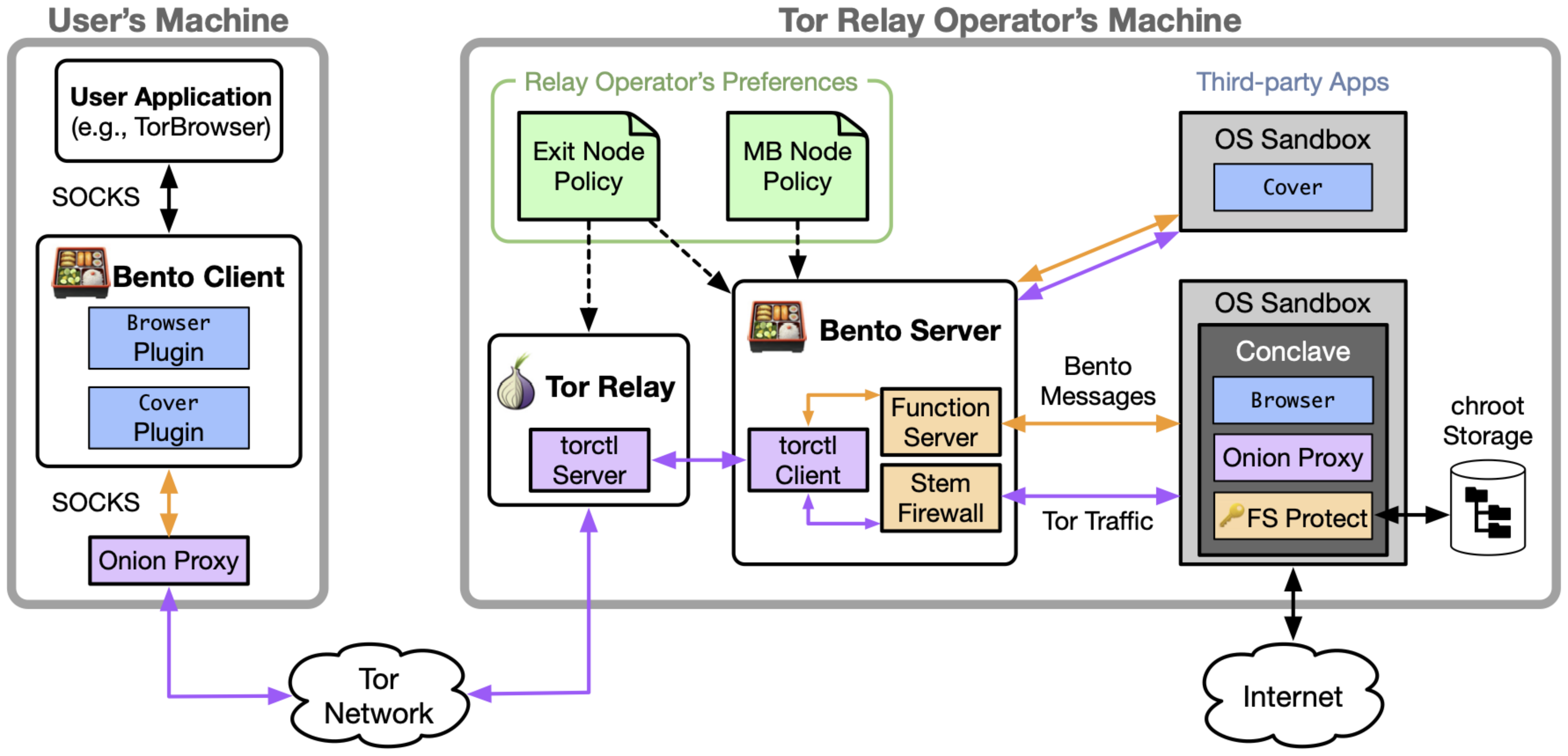


Overview of installing, and executing a Browser "function" that runs on an exit node, downloads a given URL, and delivers it, padded to some threshold number of bytes. To an attacker sniffing the client's link, it appears the client uploads a small amount and then downloads a large amount.

Bento Overview:

Design Goals and Challenges:

- Expressiveness
- Protect functions from middleboxes
- Protect middleboxes from functions
- No Harm to Underlying Tor
- No Extensions to Tor



Key Components:

- Functions
- Bento server
- Containers (conclaves)
- Middlebox node policies

Broader Impact:

The goal of this work is to show that programmable anonymity networks are useful, possible, and challenging, yet attainable. The applications that we have explored suggest that even a small amount of programmability would significantly improve the speed at which new techniques can be rolled out into the Tor network.

There remain many interesting and important problems that must be solved in order to achieve programmable anonymity networks. We view this work as merely the first step, and we hope that it engenders a lively discussion among the anonymity community as well as application developers who wish to expand the offerings possible on anonymity networks.

Our artifact-evaluated Bento source code can be found at: https://github.com/breakerspace/bento

And our artifact-evaluated source code for conclaves can be found at: https://github.com/smherwig/phoenix/

This project has funded a number of undergraduate students in their first research experiences, some of which have since gone on to graduate school; masters students; and multiple PhD students.

Video Link and Relevant Papers:

https://www.cs.purdue.edu/homes/clg/SaTCPoster.html

Stephen Herwig, Christina Garman, Dave Levin. "Achieving Keyless CDNs with Conclaves". In USENIX Security, 2020.

Michael Reininger, Arushi Arora, Stephen Herwig, Nicholas Francino, Jayson Hurst, Christina Garman, Dave Levin. "Bento: Safely Bringing Network Function Virtualization to Tor". In ACM SIGCOMM, 2021.