The Center for Cyber Defenders

Expanding computer security knowledge

Watching the Watchers

Detecting Fraud on Bitcoin's Lightning Network

Michael Rausch, University of Illinois at Urbana-Champaign

Project Mentor: Dr. Nicholas Pattengale, Org. 5824

SAND2018-7746D

Problem Statement:

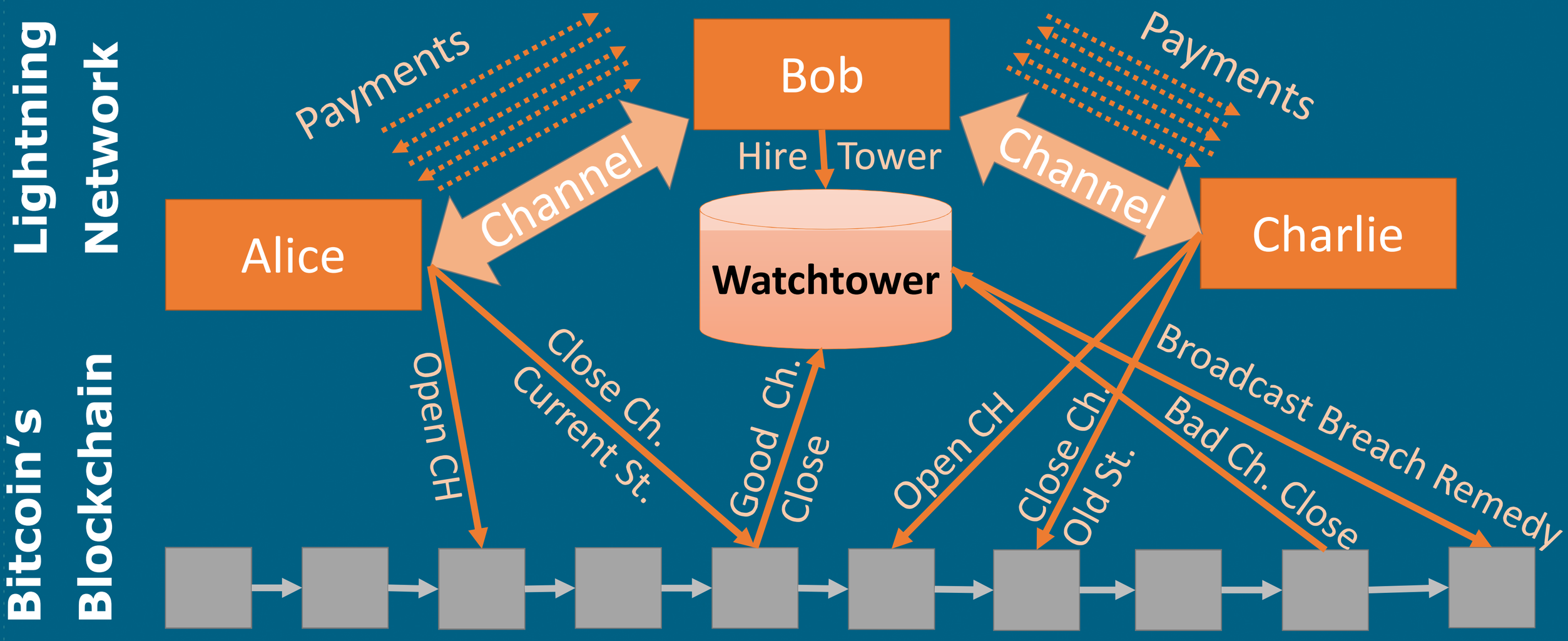
Bitcoin processes a mere 7 transactions per second (tps), compared to Visa's 45,000 tps. The Lightning Network (LN) is a proposed scaling solution. LN consists of payment channels (Alice routes a payment to Charlie through Bob) that use Bitcoin's blockchain as a trust anchor. Numerous fast, cheap, & secure transactions only require two bitcoin transactions. Watchtowers are a mechanism to help prevent fraud in the LN. The security properties of watchtowers are not yet well understood.

Objectives & Approach:

We investigate the security properties & effectiveness of LN watchtowers by constructing

- A threat model (including attacks),
- A user model (using real-world data)
- Multiple watchtower models, including incentive schemes and different configurations

We test the effectiveness of different watchtower configurations by running actual LN software in realistic emulation environments. This approach produces results better postured for validation.



Impact and Benefits: Our experimentation and analysis will

1) inform watchtower construction/incentivization for security,
2) inform user best practices for minimizing risk of LN fraud, and
3) inform cybersecurity analysts on protection/mitigation strategy

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration