This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2021-8674C

Resilient Blockchain-Based Machine Learning

Presenter: Caleb Carter (56291)

Mentor: Ashley Mayle (6534)

Manager: Susan Gardner (5629)

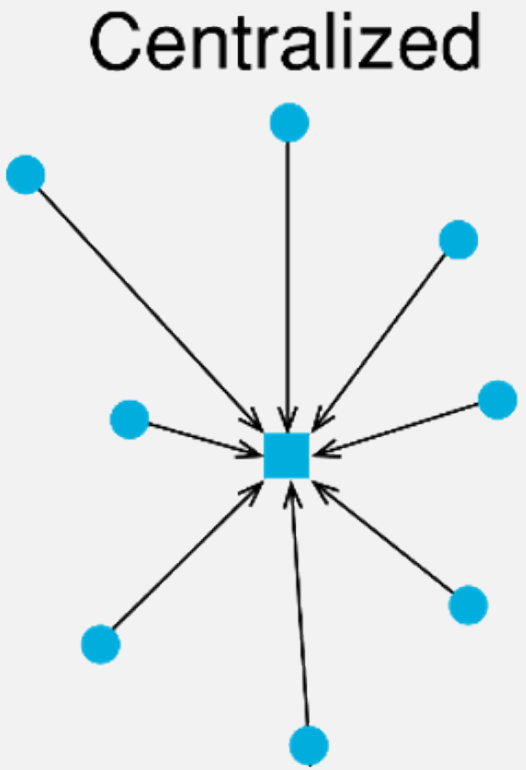
July, 27th 2021; Student Intern Symposium

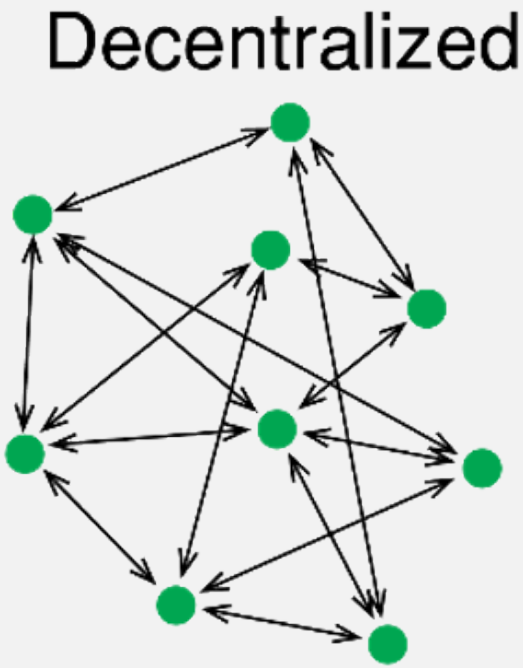
U.S. DEPARTMENT OF ENERGY NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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.

Project Overview

- Decentralized security concepts are on the rise
- Centralized edge computing techniques may contain a single point of failure
  - This means the entire system can fail from a the central node malfunctioning
- Working an LDRD exploring security focused machine learning algorithms on a blockchain
  - This presents less options for a single point of failure attack
  - Attackers will need majority control of the system to affect network communication
  - Increases resilience of whole system





Distributed Ledger Technology - Overview

- Distributed ledger technology (DLT) allows for Byzantine fault-tolerant decentralized computing
  - Each time a node sends data to another, all nodes in the system will receive this value and a majority will need to agree before adding this data to its ledger or reject it

- End result is a system that only permits data into its ledger that has been approved by the majority

Objectives

- Work with private-permission blockchains using MultiChain
  - Implemented custom filters on private blockchain that apply to all or specified transactions
  - Applied custom permissions to nodes in blockchain
    - Admin nodes can grant or revoke permissions from user nodes
    - Admin nodes can also issue new assets for transaction exchange

Conclusion

- By implementing security focused machine learning algorithms on a blockchain, our system will be less vulnerable to total failure, and still have the power to process data on multiple nodes
- Our next steps are to implement MultiChain in FireWheel

Questions?

Thank you