A Lightweight Machine-learning Framework for Enhancing Security in IoT Blockchain Networks

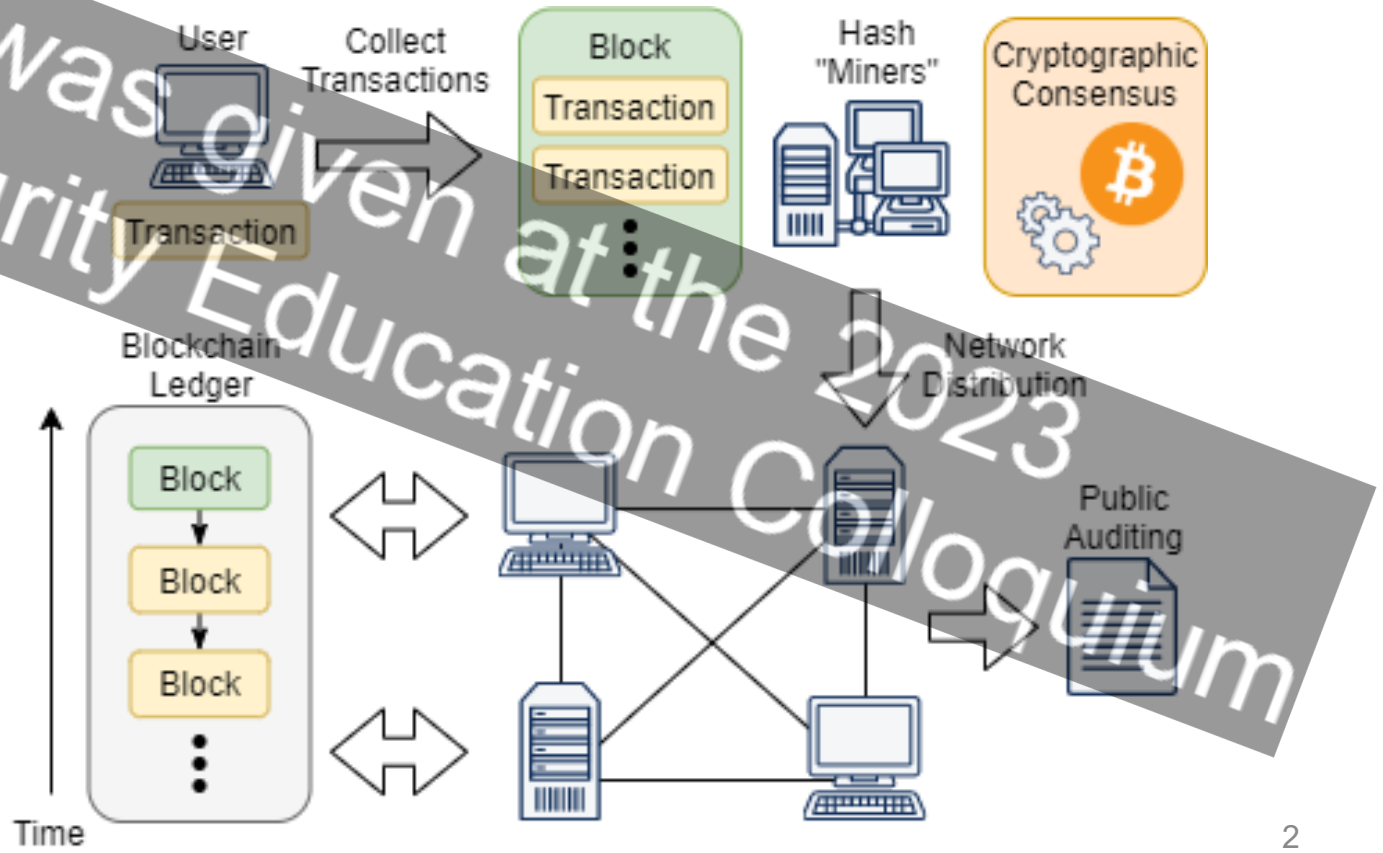
Charles Rawlins

Academic Advisor: Jagannathan Sarangapani

MISSOURI S&T

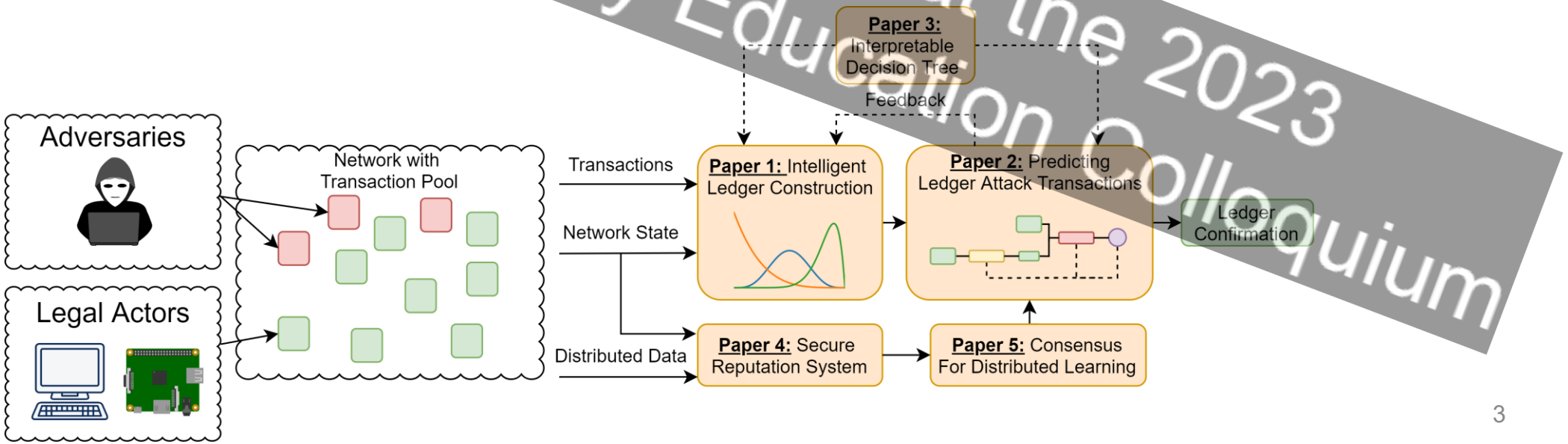
Challenges with Blockchain and IoT

- A blockchain is a decentralized network for recording arbitrary data in a transaction format with strong fault tolerance, implemented typically for full-powered workstations
- Overall goal of dissertation is empowering lightweight mobile IoT devices to execute full blockchain protocol without reliance on full-powered servers
- Main features:
  - An auditable ledger
  - Block queue for collecting transactions
  - A consensus algorithm appending ledger data
  - Cryptography securing data in a linked list
- Challenges
  - Computationally-intense
  - Inefficient consensus
  - Large storage requirement



Our Approach

- Propose an approach to validate transactions in IoT blockchain networks with machine-learning
  - *Can blockchain data attacks/conflicts be predicted from previous experience?*
- Applying lightweight distributed machine-learning is not trivial
- Introducing prediction to this environment adds additional challenges, addressed with our work
  - Evasion attacks (input manipulation), imbalanced/poisoned learning, Byzantine nodes, etc.
- The application with this approach is to allow limited IoT nodes to execute a blockchain network securely and independently in a mobile environment
- Primarily compared against the IOTA protocol for experimentation



Recent Progress and Outcomes

- Each paper has been tested in both a controlled and realistic testbed based on the IOTA ledger protocol
- Remaining paper to be submitted will focus on computational efficiency
  - Implementing gradient-descent alternatives with auditable fuzzy decision trees
  - Will replace deep networks in other papers
- Development of this scheme will empower IoT device participation in blockchain protocols and advance blockchain technology towards the use of machine-learning in next generations
  - Focused this effort on detecting fraud in transactions, but could be used in other data domains, like files or sensor data