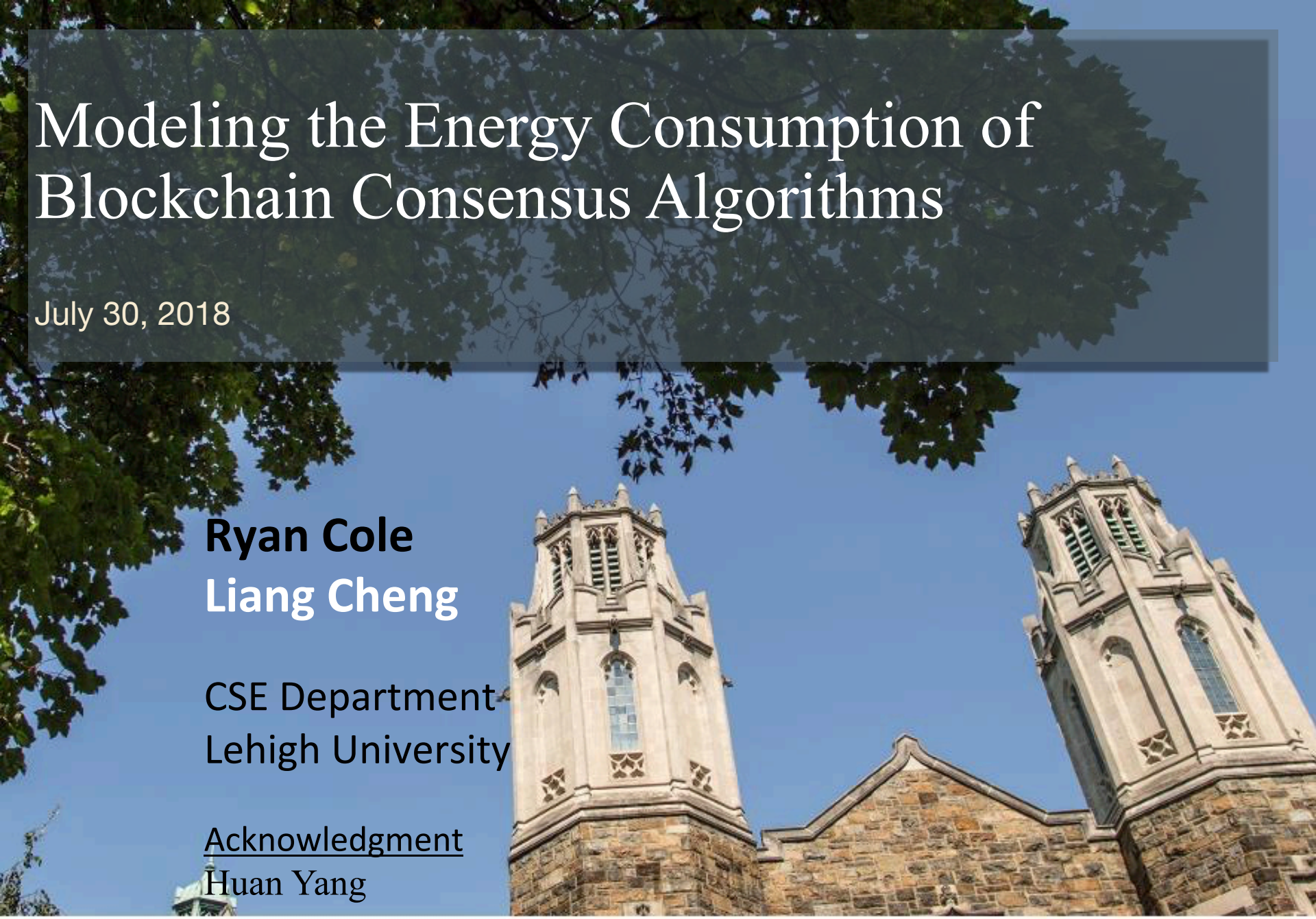
Modeling the Energy Consumption of Blockchain Consensus Algorithms

July 30, 2018



Ryan Cole
Liang Cheng

CSE Department
Lehigh University

Acknowledgment
Huan Yang

Background

Blockchain for Internet of Things Applications

- Smart cities / communities
- Smart transportation systems

Advantages

- Distributed trust via data immutability
- Resilient system by distributed data storage

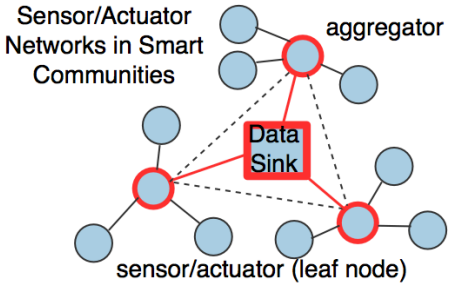
Research Problem

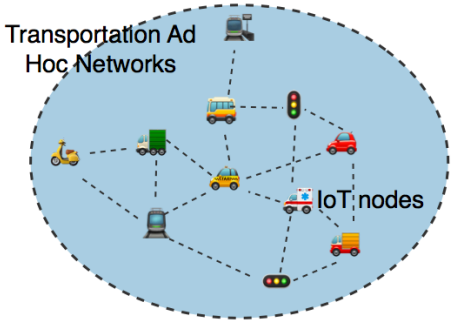
Energy Consumption Issues of using Blockchain for IoT Applications

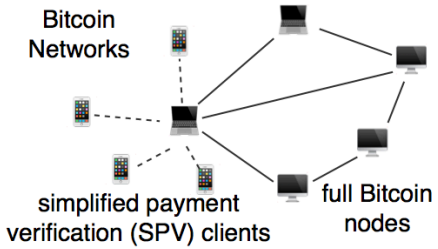
- Hundreds or even thousands of non-leaf nodes and/or ad hoc nodes

Criticisms of blockchain technologies, particularly Proof-of-Work-based systems

- Digiconomist estimates that a single Bitcoin transaction uses over 800 kilowatt hour







Our Approach

Collecting real-world data and modeling the energy consumption of both PoW and non-proof-of-work coins and associated consensus algorithms

- The size of the network
- The number of messages sent per transaction
- The computing cost of such a consensus protocol

Variable	Meaning
c	Energy used to communicate between nodes
e	Energy for a machine to validate a transaction
f	Average transaction fee
h	Network hashrate
o	Average confirmation time for a transaction
t	Number of transactions in the last 24 hours
v	Energy to validate a transaction locally (Stellar)

Consensus Algorithms

Proof of Work

- The original blockchain consensus algorithm

Ripple Protocol Consensus Algorithm

- A customized solution to the Byzantine Generals Problem

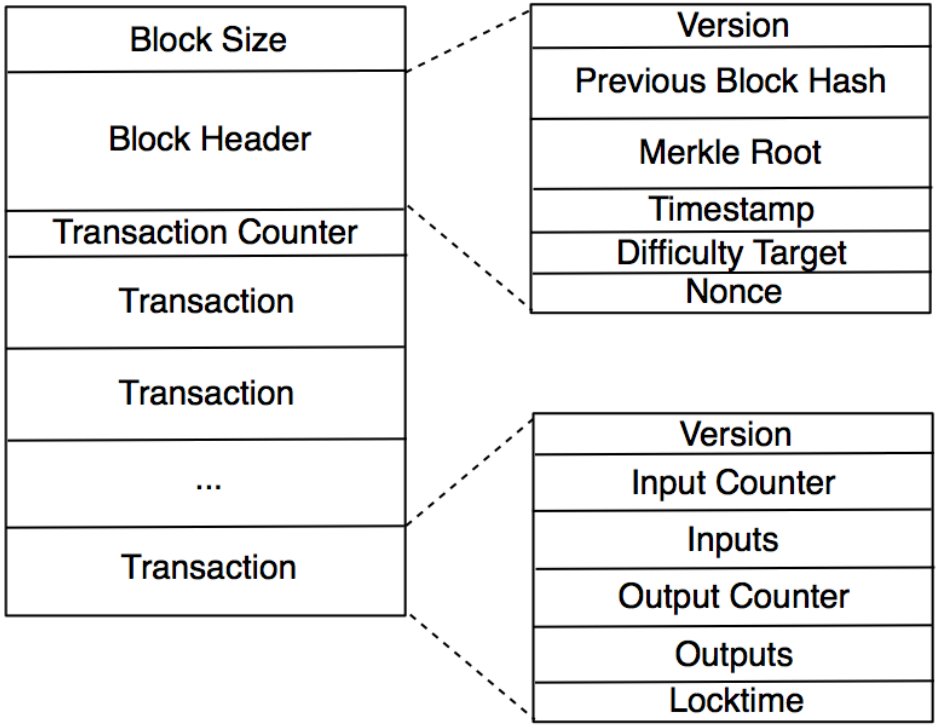
Stellar Consensus Protocol

- Federated Byzantine Agreement (FBA) using open membership and quorum slices

PoW

Proof of Work

- Full nodes must solve a complex mathematical puzzle in order to be able to verify a group of transactions included in a block
- In order to mine a block, a full-node miner must guess a nonce for the block
- Once a block is mined the miner node will broadcast the block to the network for its validation by the rest of the network



RPCA

Ripple Protocol Consensus Algorithm

- Ripple divides voting into rounds
- Initially, each node collects all transactions that it has seen that have not yet been applied and then publishes them in what is known as a "candidate set".
- Each node collects the candidate sets and votes on the validity of the transactions.
- All transactions that receive more than a certain percentage of "yes" votes proceed to the next round, if applicable.
- In the final round, at least 80% of the nodes must vote yes on each transaction for it to be verified.
- After this round, all transactions that have reached this threshold are added to the public ledger.

SCP

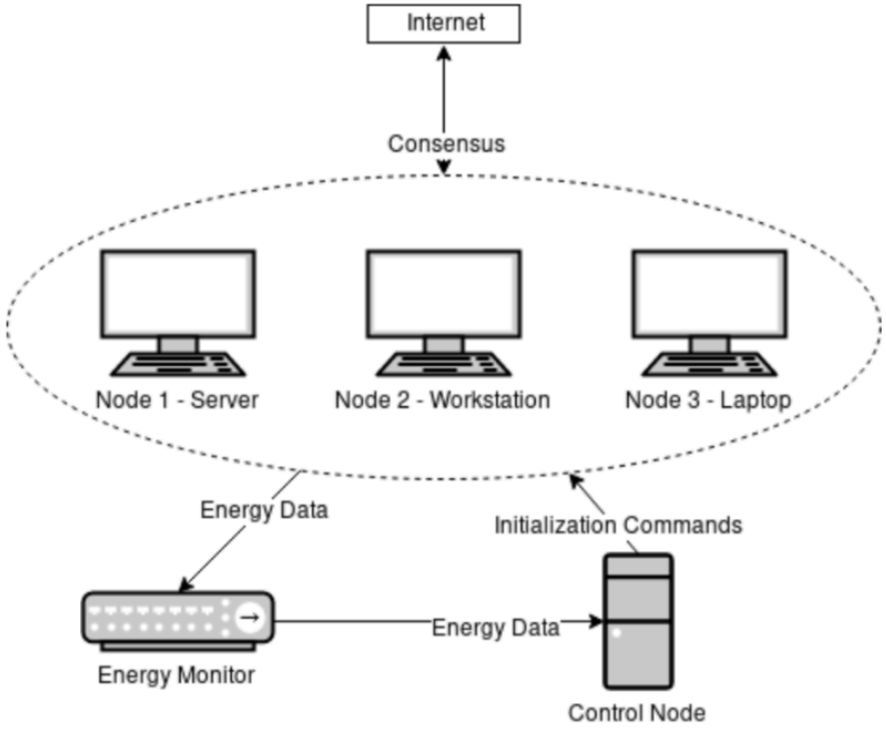
Stellar Consensus Protocol

- A quorum is a set of nodes sufficient to reach an agreement.
- Stellar also utilizes quorum slices, which is a subset of a quorum that can convince another node of agreement.
- Each node decides upon a group of nodes that it trusts, which forms the node's quorum slice.
- There are two conditions for a node to accept a transaction
  - the node must have never accepted a conflicting transaction;
  - a large enough portion of the node's quorum slice must also vote for or claim to accept the transaction.

Data Collection

Online Data Scraping

- Proof-of-work coins from cryptocurrency statistics available online, including Bitcoin, Ethereum, Litecoin, Monero, and Vertcoin.
- For each coin, we collected daily data on the number of transactions, the difficulty, hashrate, mining profitability, and price.
- Using Digiconomist formula to estimate each coin's daily energy usage



Testbed

- RPCA &SCP; energy consumption measured by Yokogawa power meter

Modelling Results (1)

PoW

- LASSO (Least Absolute Shrinkage and Selection Operator) regression model
- Estimates the energy usage of a cryptocurrency in kilowatt hours with 92% accuracy

$$e = 8.987e^{-12}\boldsymbol{h} + 1.041e^{7}\boldsymbol{f} + 15.02\boldsymbol{t} + -1.375e^{4}\boldsymbol{o}$$

Variable	Meaning
$\boldsymbol{c}$	Energy used to communicate between nodes
$\boldsymbol{e}$	Energy for a machine to validate a transaction
$\boldsymbol{f}$	Average transaction fee
$\boldsymbol{h}$	Network hashrate
$\boldsymbol{o}$	Average confirmation time for a transaction
$\boldsymbol{t}$	Number of transactions in the last 24 hours
$\boldsymbol{v}$	Energy to validate a transaction locally (Stellar)

Modelling Results (2)

Ripple Protocol Consensus Algorithm

$$e = n * t * 5.05e - 4$$

Stellar Consensus Protocol

$$e = n * t * 1.914e^{-6}$$

Variable	Meaning
c	Energy used to communicate between nodes
e	Energy for a machine to validate a transaction
f	Average transaction fee
h	Network hashrate
o	Average confirmation time for a transaction
t	Number of transactions in the last 24 hours
v	Energy to validate a transaction locally (Stellar)

Conclusion and Future Work

Linear regression models provide reference estimations of the energy consumption impact in designing blockchains for IoT systems

Future research

- Impact of sharding blockchain networks on energy consumption
- Trade-offs between the energy usage and the transaction time on large-scale blockchains

Nonlinear models