New Mexico Research Spotlight Forum

10.17.2019 Grid Resiliency

Blockchain-Enabled Smart Grid: Resilient Data Exchange and Resource Orchestration

Michael Devetsikiotis, Professor and Chair

Department of Electrical & Computer Engineering

The University of New Mexico

mdevets@unm.edu

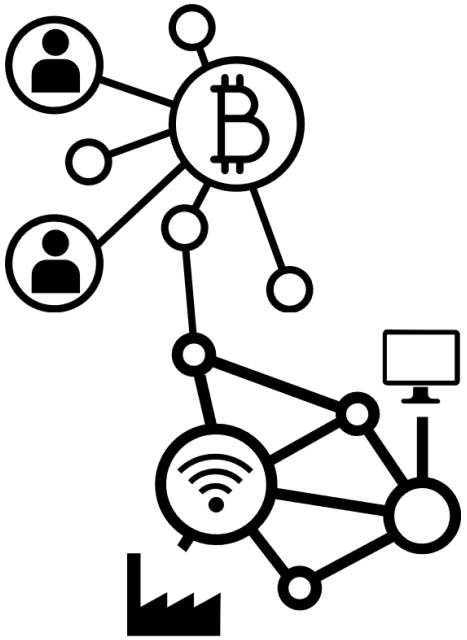
Sandia National Laboratories | Georgia Institute of Technology | ILLINOIS | PURDUE UNIVERSITY | THE UNIVERSITY OF TEXAS AT AUSTIN | THE UNIVERSITY OF NEW MEXICO | NM STATE UNIVERSITY | NEW MEXICO TECH SCIENCE • ENGINEERING • RESEARCH UNIVERSITY

SAND2019-13650 PE

RESEARCH BACKGROUND AND TOPICS

- Trained as an Electrical Engineer, BS, MS and PhD
  - Worked initially on telecommunications modeling
  - Later in high speed networks, ATM systems, tele-traffic
- My major interest is in Operations Research
  - Performance evaluation and rare-event simulation
  - "Cyber-physical" and "socio-technical" systems

- Smart Grid Communications
- Electric Vehicle Charging Infrastructures
- Smart Cities and Cyber-Physical Systems
- Blockchain Technology



INTERNET OF THINGS LABORATORY

- IoT Lab focus: Performance Modeling, Cyber-Physical & Socio-Technical systems
  - Modeling of Smart Grid Communications
  - Intelligent Electric Vehicle Charging
  - Intelligent IoT Enabled Cities and Location-based Services
  - Blockchains for IoT and Transactions in Smart Systems
  - Smart Infrastructure Resiliency and Public Safety Architectures
- Research group
  - Three PhD Students: Dimitris Sikeridis (UNM), Will Stout (Sandia), Kostas Christidis (Netflix)
  - Four Undergraduate Students: Isaac Carrasco, Andrew Gilbert, Santiago Martin Cejas, Kavin Kullama (UNM and Senior Design Projects)

GRID RESILIENCY - GROWING SECURITY CONCERNS

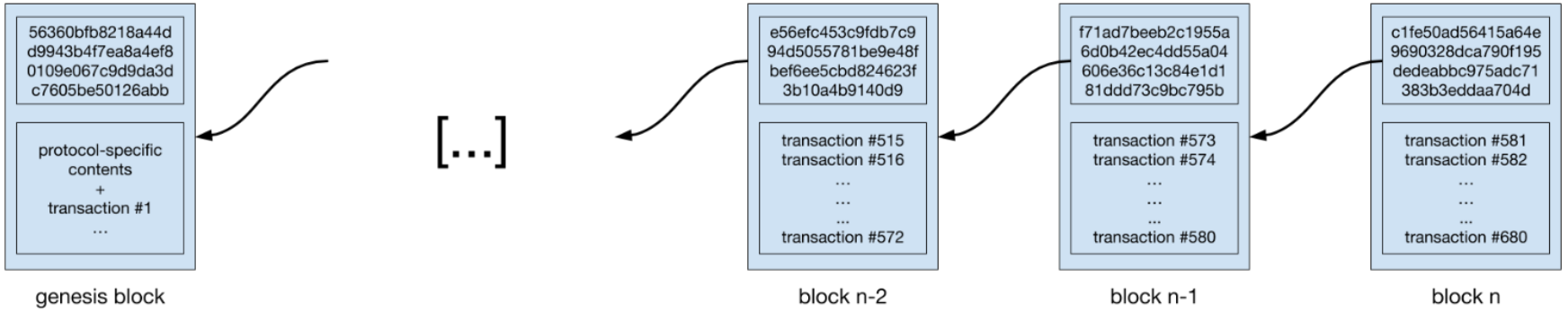
- Smart Grid joining the Internet → CPS Attacks expand exponentially
- Frequency of IoT-inspired attacks grows
  - Expanding number of Smart Grid equipment prone to corruption
  - Single point of failure
  - Identity Spoofing and Leaks in CPS and Smart Grid
  - Data integrity attacks
  - Seen in 2016 Mirai botnet attack with generation of Tbps of malicious traffic

GRID RESILIENCY - RETHINKING SECURITY MODELS

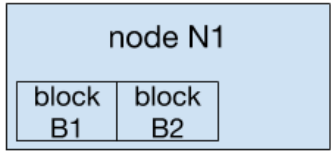
- Data Integrity → Need for a persistence layer that can not be tampered
- Identity Spoofing → Need for cryptographic verification of *all* activity
- SPoF/DDoS Attack Resiliency → Need for a Decentralized Architecture

GRID RESILIENCY - THE BLOCKCHAIN PARADIGM

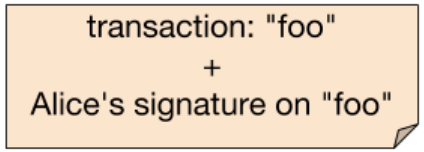
- Data Integrity → Need for a persistence layer that cannot be tampered with



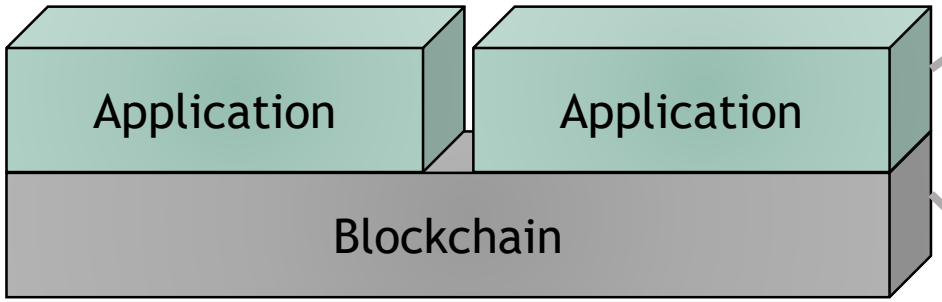
- A network of nodes:
  1. All holding the same copy of the blockchain
  2. Forming a peer-to-peer network



- A network of users:
  1. All holding private/public key pairs
  2. Writing to the blockchain via transactions



GRID RESILIENCY - LAYERED DESIGN



1. Smart Grid application records all activity to the blockchain
2. Authorization guaranteed by public key Infrastructure

1. All interactions managed by public keys
2. Thousands of nodes replicating the activity log
3. Activity log is tamper-evident

GRID RESILIENCY - RESOURCE ORCHESTRATION

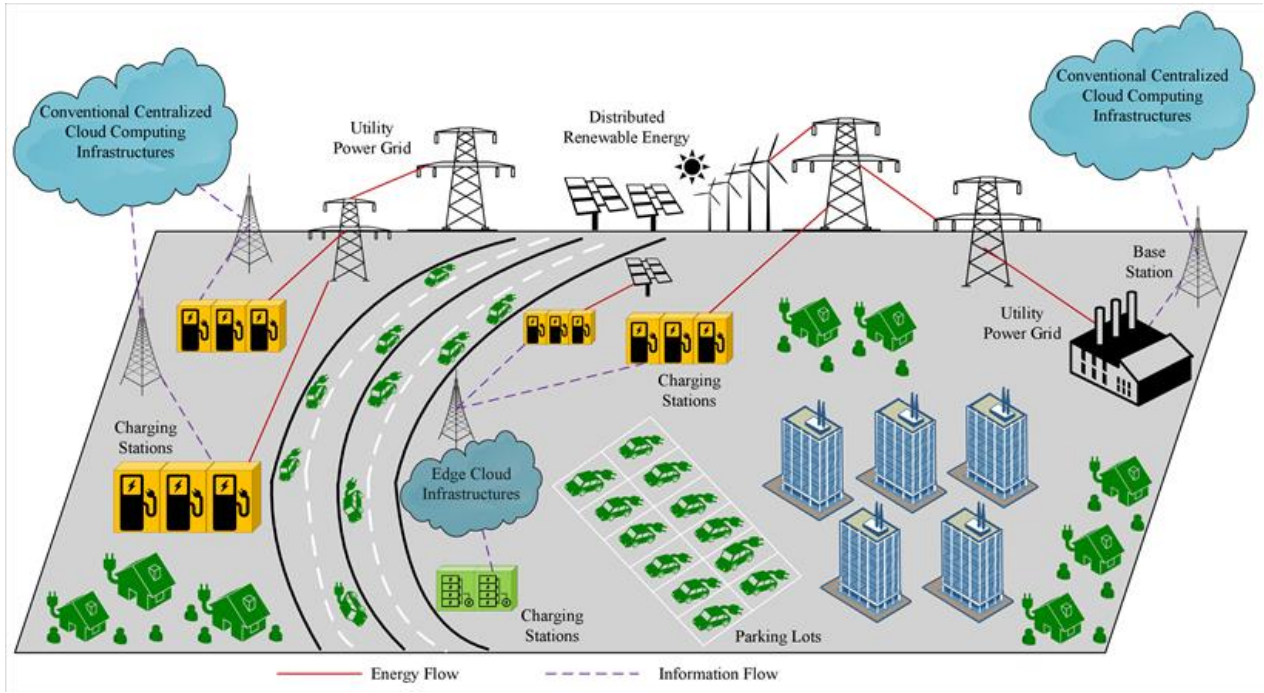
- A layer that can be used to coordinate resources.

- Agents can lease resources programmatically by exhibiting properly signed requests
- Blockchain-connected rule engines authoritatively allow/prevent access

- Examples of resource orchestration in Smart Grid:
  - Coordination of prosumers in local energy markets for peak saving and resource optimization
  - Data and Setting exchange in critical smart grid infrastructures

BLOCKCHAINS IN TRANSACTIVE ENERGY SYSTEMS

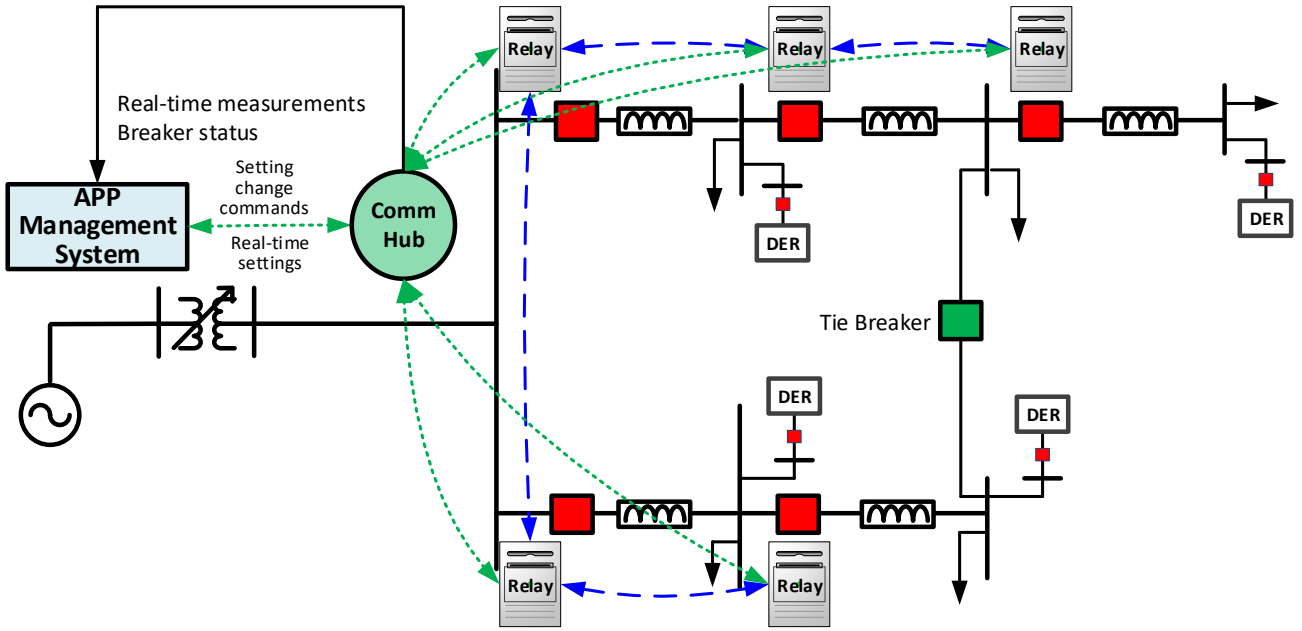
- Local energy markets are emerging
- Blockchains form a unified automatic billing layer that directly connects producers to consumers
- Achieve interoperability and standardization among all parties



K. Christidis, Y. Wang, D. Sikeridis, M. Devetsikiotis, "Blockchain-based local energy markets: implications of data and governance models on performance", work in progress

BLOCKCHAINS IN DISTRIBUTION PROTECTION SYSTEMS (1/3)

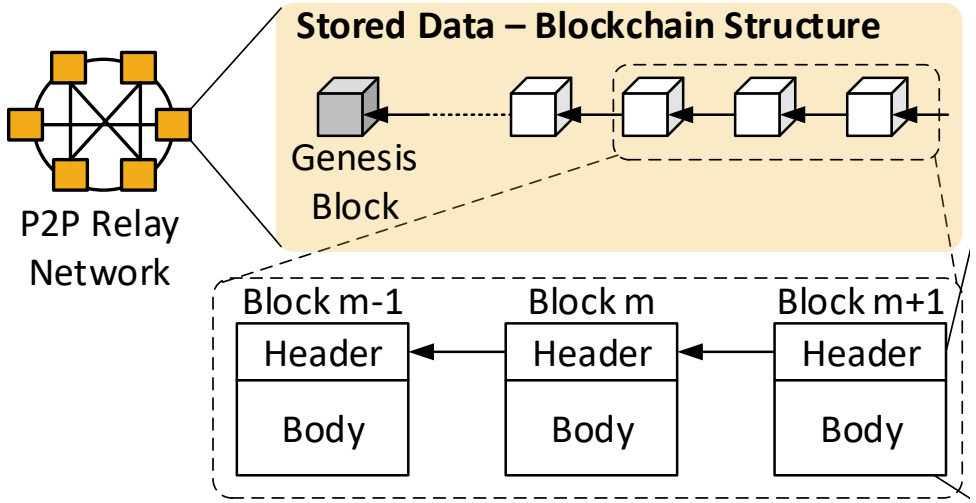
- Distribution protection systems
- Physical components coupled with communication-enabled intelligence
- Deploy a blockchain-based network for data collection and settings dissemination
  - Integrity of grid measurement streams
  - Immutability of control signals and record keeping of firmware updates

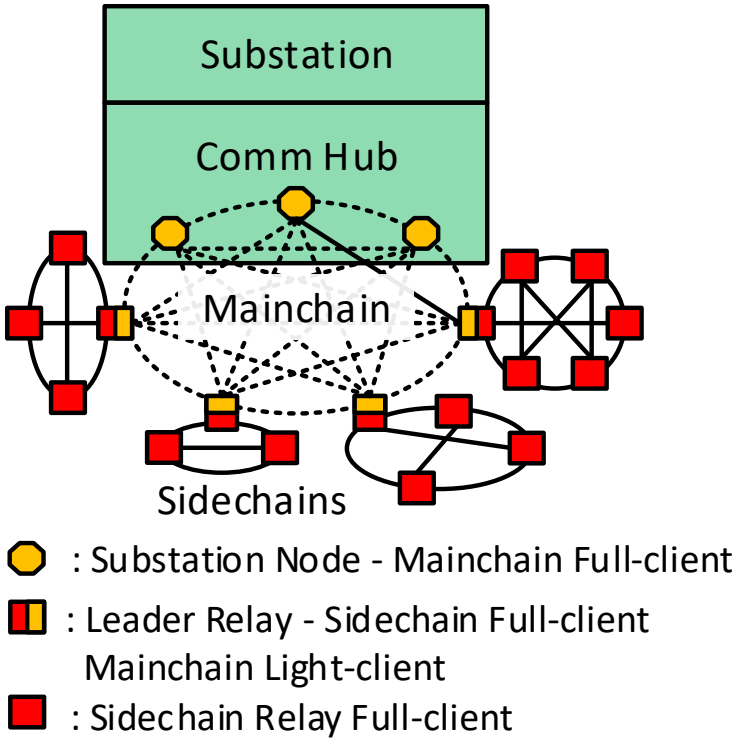


D. Sikeridis, A. Bidram, M. Devetsikiotis, M. Reno, "A Blockchain-Based Mechanism for Secure Data Exchange in Smart Grid Protection Systems", IEEE Consumer Communications & Networking Conference 2020, to appear

BLOCKCHAINS IN DISTRIBUTION PROTECTION SYSTEMS (2/3)

- P2P Relay Network Architecture
- Each Relay is a Blockchain Node
- Improve data exchange performance with a layered design
  - Creation of Sidechains of Neighboring Relays with a single Leader Relay
  - A Mainchain connects all the Sidechains with the Substation

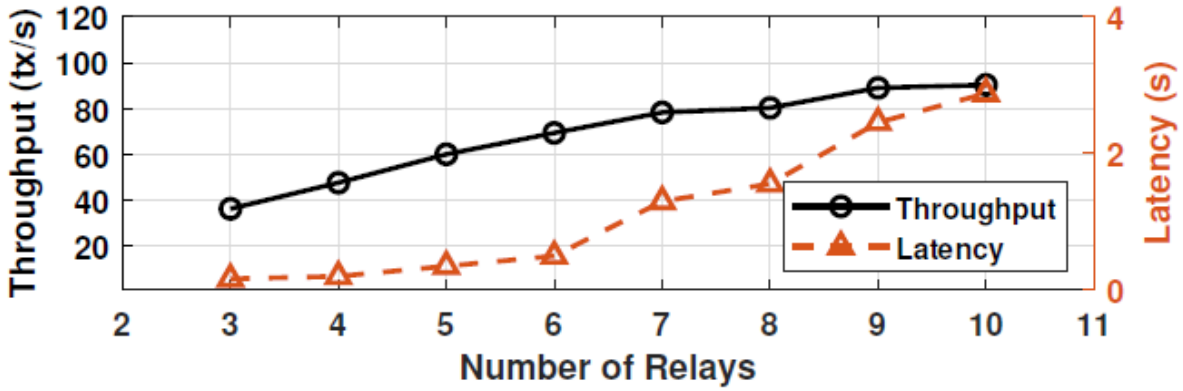




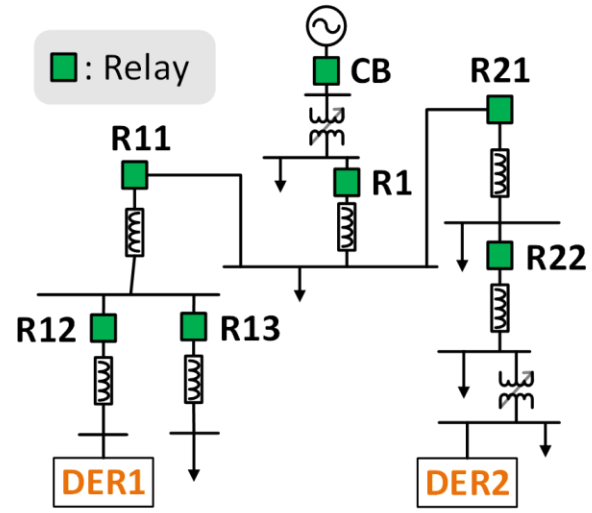
BLOCKCHAINS IN DISTRIBUTION PROTECTION SYSTEMS (3/3)

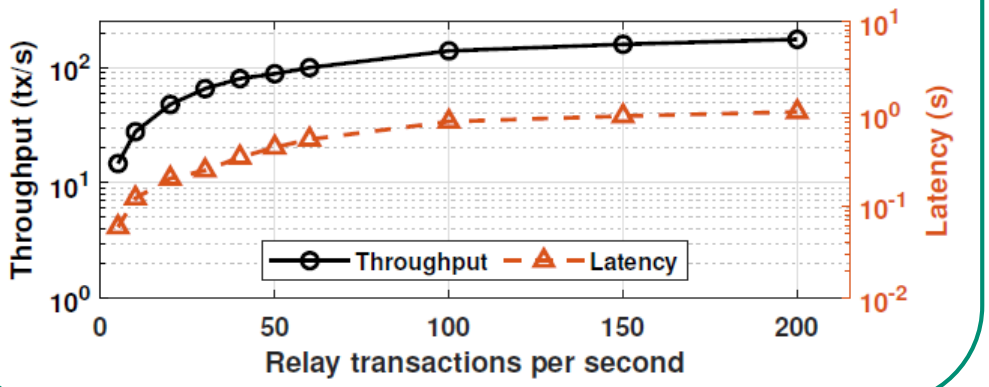
- Simulations with distribution circuit
- Each relay is simulated on a separate virtual node
  - Two Sidechains: {R11, R12, R13, DER1}, {R1, R21, R22, DER2}
  - One Mainchain: {CB, R11, R1}

- Impact of sidechain size for a fixed transaction rate



- Transaction throughput and latency for simulated circuit





FUNDING SOURCES

- Supported by the National Science Foundation under the New Mexico SMART Grid Center - EPSCoR cooperative agreement Grant OIA-1757207.

RESEARCH NEEDS

- Collaborate on more realistic, real-life security and resiliency scenarios.
- Benefit from real-life use cases, equipment, and data sets.
- Implement demos, testbeds and showcases.
- Resiliency, and similar quantities can benefit from precise, more actionable definitions.
- Great potential inside New Mexico, rural areas, Pueblos: partnerships needed!

Thank you!