NATIONAL ENERGY TECHNOLOGY LABORATORY

# Project: Incorporating Blockchain/P2P Technology into an SDN-Enabled Cybersecurity System to Safeguard Fossil Fuel Power Generation Systems

Agreement Number: FE0031742

University of North Dakota
College of Engineering and Mines

August 27th, 2020.

# Project Description and Objectives

## Overview

- **This project aims to strengthen the security protection of software defined networking (SDN) for facilitating its deployment in fossil fuel power generating systems.**
  - The security protection solution makes use of the blockchain and the peer-to-peer (P2P) technologies.
  - This project is in response to Area of Interest 2 of DE-FOA-0001991.
  - AOI 2: "*investigate how cutting-edge network technologies such as blockchain may be leveraged and integrated into industrial monitoring and process control systems for optimized, cybersecure operation of electricity generating units.*"
- **This project aims to produce two deliverables:**
  - A cloud-based networking platform for prototyping and experimenting various designs of safeguarding the software-defined networks deployed in electric power systems.
  - A blockchain/P2P-based technology for detecting the compromised controllers in a software defined network.
    - The application will operate in the cloud-based networking platform.
- **The outcomes of this project will serve in**
  - Meeting the general security requirements of the electric power generating systems.
  - Mitigating the security risks targeting the vulnerabilities of SDN-enabled operational networks.

# Project Description and Objectives

## Strategic Alignment of Project to Fossil Energy Objectives

- **Serving for Meeting the General Security Requirements of Electric Power Systems**
  - Safe operations of power systems rely on the fundamental security mechanisms
    - Authentication, Authorization, and Anti-spoofing.
- **Serving for Facilitating the Deployment of SDN-Enabled Operational Networks**
  - Software Defined Network (SDN) technologies will be increasingly adopted to support data communications in electric power systems.
  - The Department of Energy had sponsored research projects on
    - Applying SDN technology to support the device-to-device communications;
    - Prototyping a dashboard application for providing the operators with a global view of the SDN-enabled operational networks.
- **Serving for Addressing the Threats Targeting the SDN-Enabled Operational Networks**
  - SDN paradigm faces new security threats and attacks.
  - Our project addresses the security risks targeting SDN technology and the protection solutions.

# Project Description and Objectives

## Technology Benchmarking

- This project aims to construct
  - A cloud-based networking platform which can be used for
    - Studying the threats targeting SDN-enabled operational networks deployed in electric power systems, and
    - Prototyping security protection solutions thwarting the attacks targeting the control plane, the forwarding plane, and the communications between the control plane and the forwarding plane.
  - A blockchain/P2P-based technology for detecting the compromised controllers in software defined networks.
- Industry/input or validation
  - This project is in collaboration with *Minnkota Power Cooperative.*
  - *Minnkota Power Cooperative* helps to facilitate decision-makings on the scientific and technical direction of the project and will be a user of the cloud-based networking platform.

# Project Description and Objectives

## Overview of Tasks

- This project basically progresses with respect to its originally planned timelines.
- There was about one-month delay when we spent extra time in deploying the cloud infrastructure.
- The pandemic has not affected our progress.
- After the cloud infrastructure and the software packages having been deployed in place, we think we will be able to accomplish the subsequent tasks according to our planned completion timelines.

| Task Description | Planned | | Achieved | |
|---|---|---|---|---|
| | Start Date | End Date | Start Date | End Date |
| Task 1.0 -- Update project management plan | 9/1/19 | 9/30/19 | 9/1/19 | 9/30/19 |
| Task 2.0 -- Demonstration of Sample Runs of an SDN System | 10/1/19 | 4/30/20 | 10/1/19 | |
| Subtask 2.1 -- Demonstration of Installation of Software on Controllers and Switches | 10/1/19 | 11/30/19 | 10/1/19 | 12/31/19 |
| Subtask 2.2 -- Demonstration of Traffic Flows Between SDN Switches | 12/1/19 | 1/30/20 | 12/1/19 | 2/28/20 |
| Subtask 2.3 -- Demonstration of Query for Rules | 2/1/20 | 2/28/20 | 2/1/20 | 3/31/20 |
| Subtask 2.4 -- Demonstration of Traffic Flow Handling Based on Rule Specifications | 3/1/20 | 4/30/20 | 3/1/20 | 5/30/20 |
| Task 3.0 -- Demonstration of a P2P Inquiry Platform in the SDN System | 5/1/20 | 4/30/21 | 5/1/20 | |
| Subtask 3.1 -- A Justification Report of the Choice of a P2P Open-Source Package | 5/1/20 | 5/30/20 | 5/1/20 | 6/15/20 |
| Subtask 3.2 -- Demonstration of Querying Rules from the P2P System | 6/1/20 | 11/30/20 | 6/1/20 | |
| Subtask 3.3 -- Making SDN Forwarding Switches to Query Rules from the Inquiry Platform | 12/1/20 | 4/30/21 | | |
| Task 4.0 -- Demonstration of Use Case of Identifying a Compromised Controller | 5/1/21 | 8/31/22 | | |
| Subtask 4.1 -- Demonstration of a Blockchain System Running on Top of a P2P System | 5/1/21 | 10/1/21 | | |
| Subtask 4.2 -- Demonstration of Replicated Rules in Blockchain System | 11/1/21 | 1/30/22 | | |
| Subtask 4.3 -- Demonstration of Storing Replicated Data Chunks in Blockchain System | 2/1/22 | 6/1/22 | | |
| Subtask 4.4 -- Demonstration of Identifying a Compromised Controller | 7/1/22 | 8/30/22 | | |

# Project Description and Objectives

## Current Status of Project

- This project started in September 1st, 2019 for a 3 years duration.
- This project is still in the construction stage, and there is no available comparison with known benchmark.
- There is no major change in the project goals/objectives.
- We have made some changes in the actual implementation of the tasks.
  - We have decided to construct the originally proposed testbed in the form of a cloud-based networking platform.
  - We have decided to adopt the proof-of-reputation consensus model for detecting the compromised network controllers in SDN networks.

# Project Update

## Accomplishments

- Deployment of a cloud infrastructure running across 3 servers
  - Hardware: 3 high-end Dell servers (Model PowerEdge R540).
  - Software: Proxmox Virtual Environment (PVE) and OpenStack.
- Deployment of an Openflow-based SDN environment
  - Data plane: *mininet* is used to emulate OpenvSwitch (OVS) switches
  - Control plane: *Open Network Operating System (ONOS)* is used to emulate an OVS controller.
  - Running Openflow networks in the cloud environment.
- Design of the architecture of a blockchain/P2P-based framework for supporting prototyping security protection mechanisms safeguarding the Openflow SDN networks.
- There are no published papers yet.

# Project Update

## Project Results (1)

### The Data Center

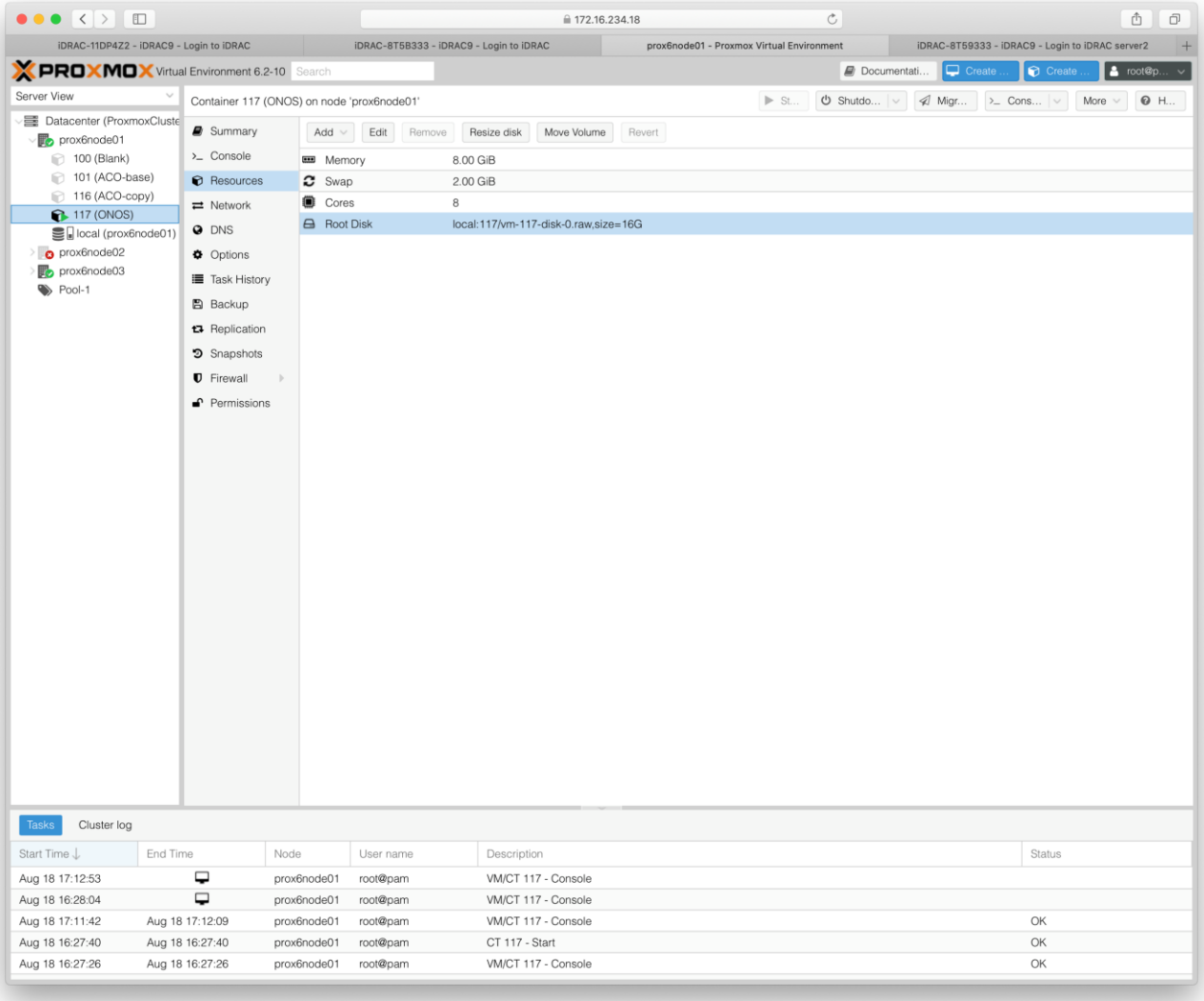
- Running across 3 Dell servers
  - Interconnected to form a single data center.
  - The cloud management software runs across the interconnected cluster of servers.
  - The data center can be smoothly scaled upward or downward.
  - The current data center on 3 servers is shown on the right.
- Remotely Powering Up and Powering Down
  - Facilitates us for keeping working in the project without interruptions caused by the pandemic.

# Project Update

## Project Results (2)

**The PVE cloud infrastructure**

- Running across 3 Dell servers
- Remotely accessible from anywhere.
- Many virtual machines (VMs) and containers can be configured to run in the cloud.
  - The OVS switches and ONOS controllers are encapsulated in VMs or containers.
  - A network topology is split into multiple VMs or containers.
  - A network experiment is executed by making the membership VMs and containers to run concurrently.
- Easy-to-use user interface for configuring the VMs and containers. (as shown on the right)

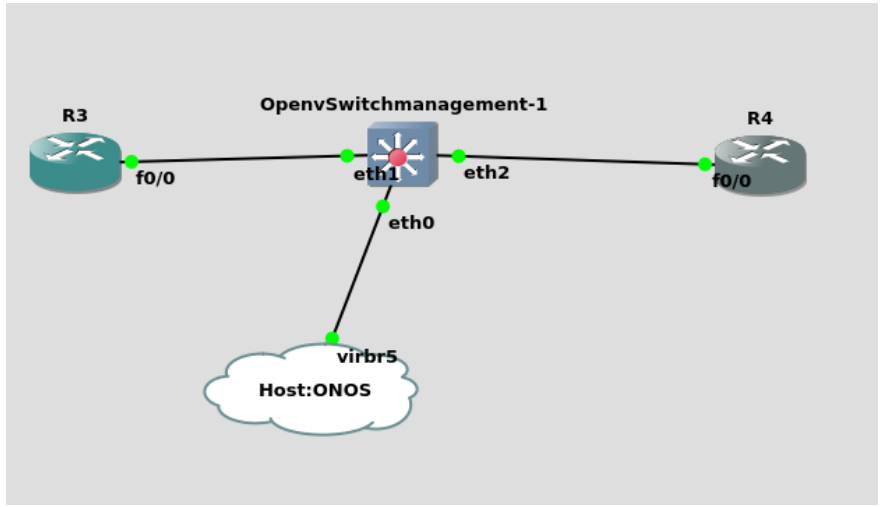


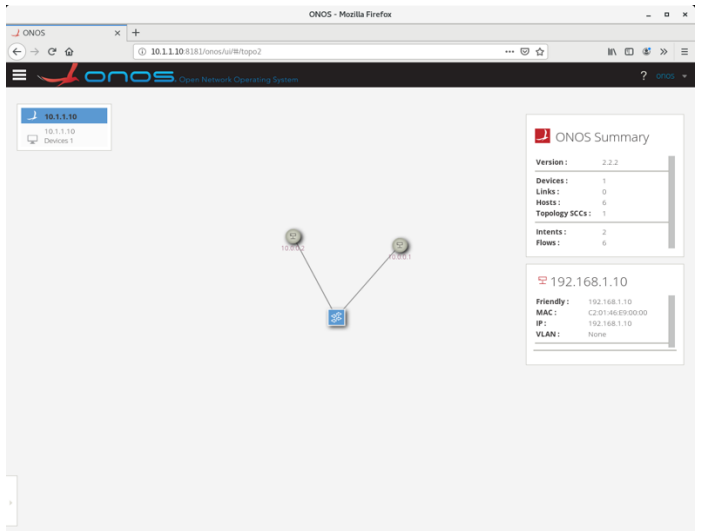
# Project Update

## Project Results (3)

### The Openflow-based SDN networks

- *mininet* is used to emulate OVS switches.
- ONOS is used to emulate an OVS controller.
- Network topology can be viewed through ONOS user interface. (shown below)



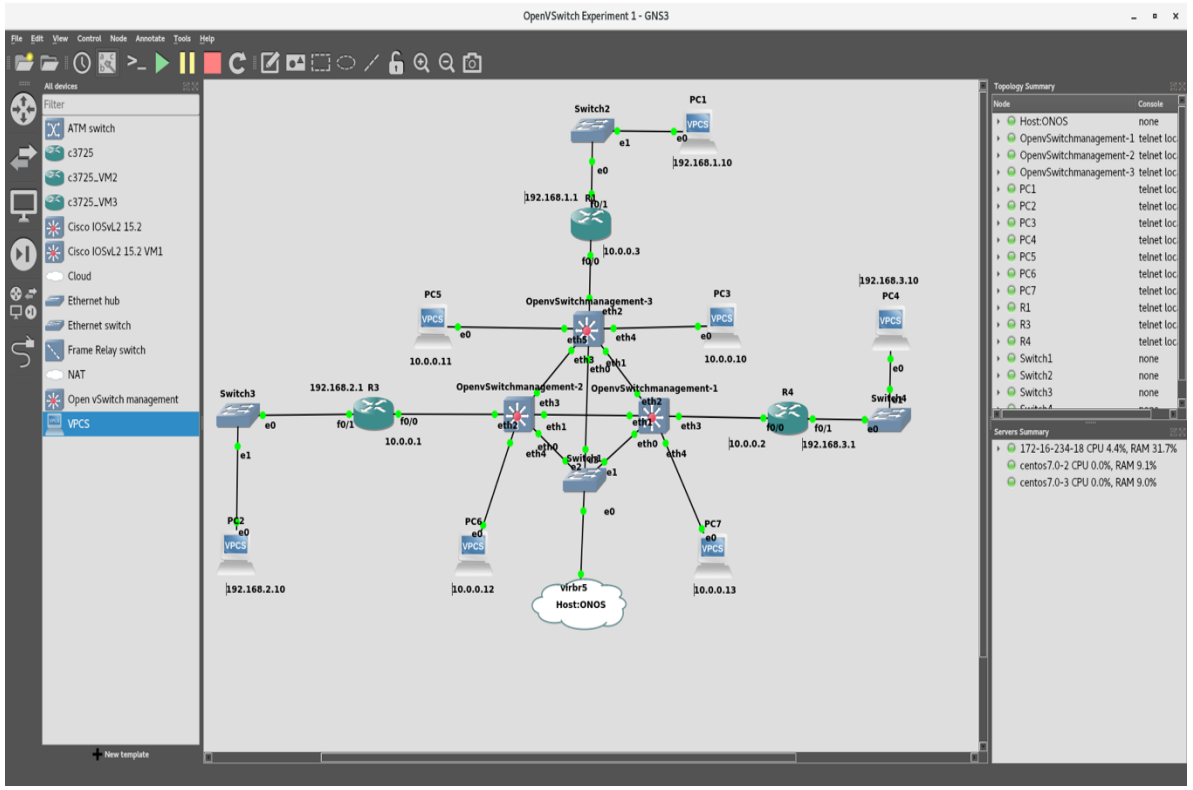



# Project Update

## Project Results (4)

**Realistic networks with conventional network switches and SDN-enabled network devices**

- A realistic network topology can consist of conventional network devices and SDN-enabled network devices.
- Both types of network devices can be configured to inter-operate in the same network environment
- Using Graphical Network Simulator version 3 (GNS3) to emulate a network environment consisting both types of network devices. (as shown on the right)

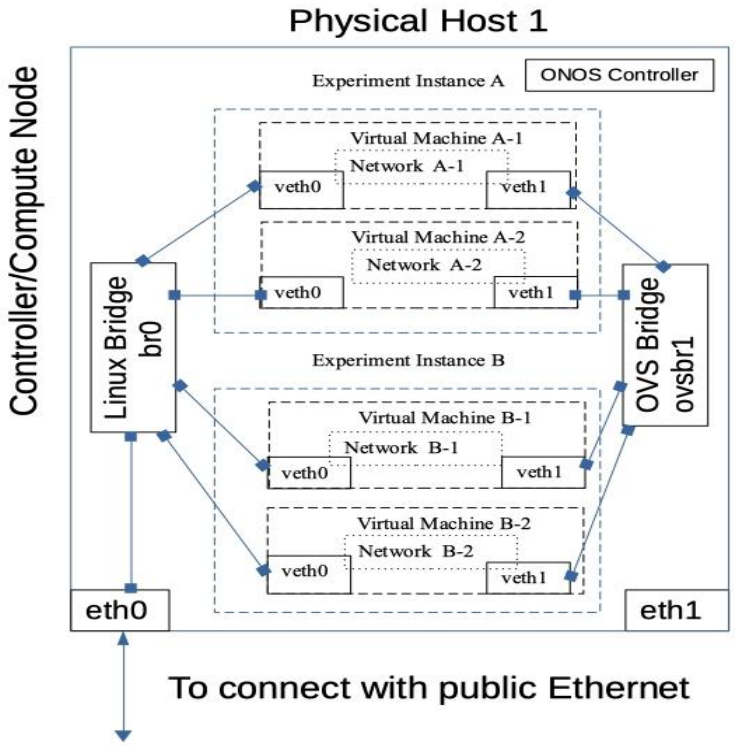


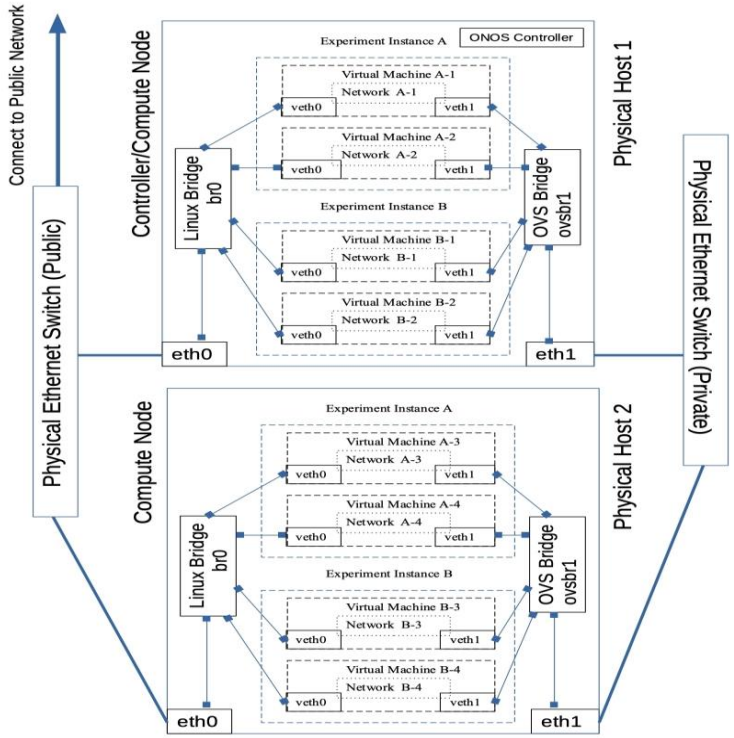
# Project Update

## Project Results (5)

**Concurrent executions of multiple network experiments on the cloud infrastructure**

- Concurrent execution of multiple experiments on a single physical host. (shown on the left)
- One network experiment can span across multiple physical hosts. (shown on the right)
- Concurrent execution of multiple experiments across multiple physical hosts. (shown on the right)



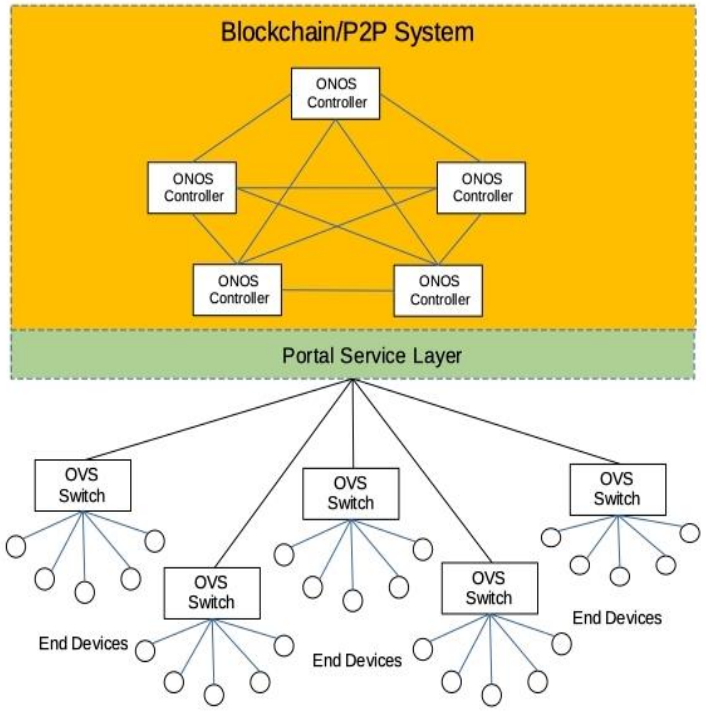



# Project Update

## Project Results (6)

### The architecture of a blockchain/P2P framework supporting research on safeguarding SDN networks

- The Portal Service Layer
  - The intermediary between the Openflow-based SDN data plane and the control plane.
  - Serving for high availability of the control plane and for preventing the dominated control on OVS switches by a single OVS controller.
- The Blockchain/P2P System
  - Maintaining a distributed consensus among a group of OVS controllers.
  - The distributed consensus serves to define the expected behavior that all uncompromised network devices are expected to follow.
  - Deviations from the consensus is identified as compromises.
  - Compromised devices need to be quickly excluded from the operations of an SDN network.

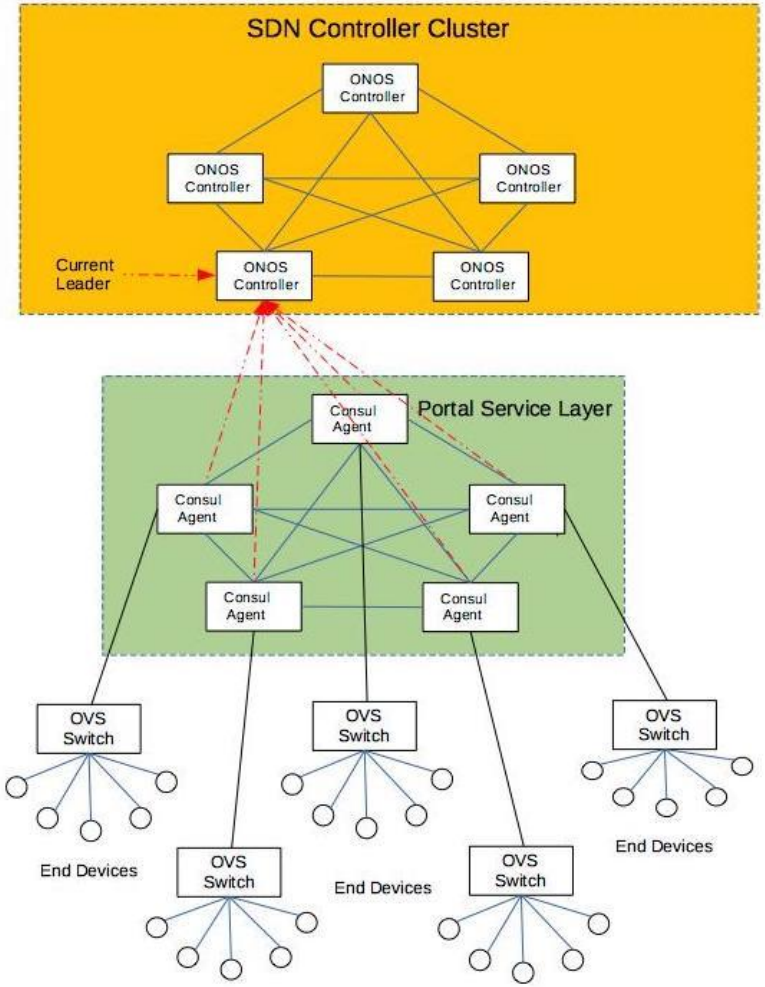


# Project Update

## Project Results (7)

**The structure of the portal service layer**

- The portal service layer is a group of fully-connected Consul agents.
- The Consul agents are used to forward messages between the SDN data plane and the control plane.
  - An OVS switch is connected to a fixed Consul agent.
  - Every Consul agent forwards messages sent from an OVS switch to the currently active OVS controller.
  - The messages sent from the active OVS controller to the OVS switches are also relayed by the portal service layer.
- Determination of an active SDN controller
  - The currently active OVS controller is determined by the Blockchain/P2P system.
  - The Blockchain/P2P system registers the currently active OVS controller to the portal service layer.

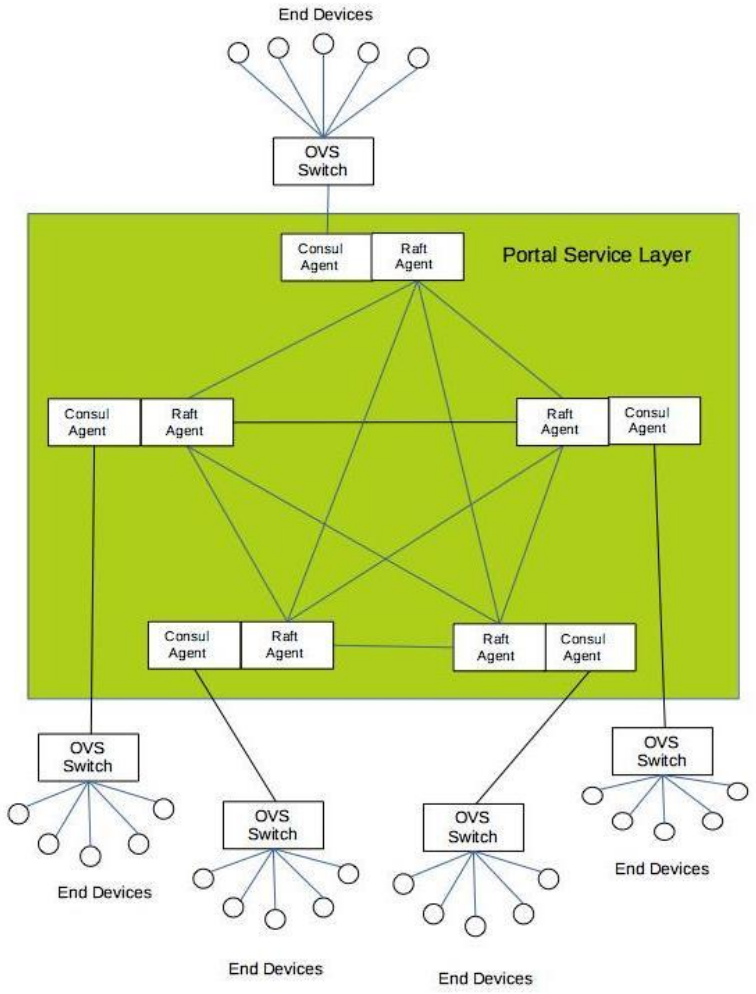


# Project Update

## Project Results (8)

## Consensus in the portal service layer

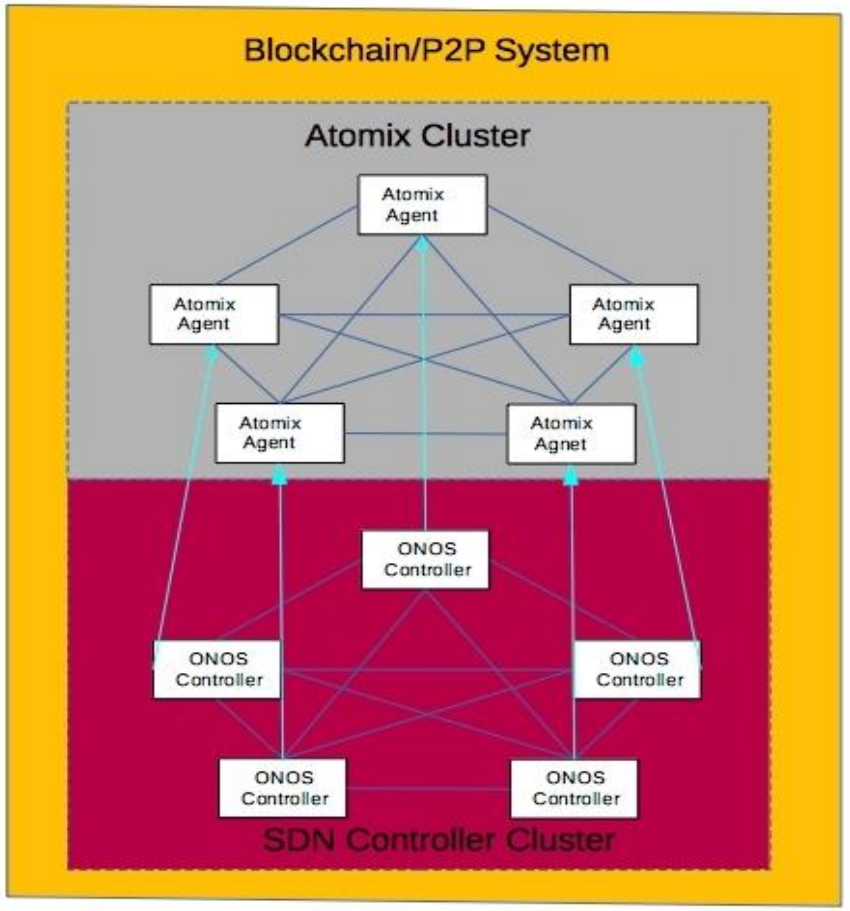
- A consensus is maintained among the Consul agents by running a Raft protocol.
- A leader Consul agent is elected under the Raft protocol.
- Elections are held periodically.
- The leader Consul agent takes the charge of informing other Consul agents about the identity of the currently active OVS controller.



## Project Results (9)

# The Structure of the Blockchain/P2P system

- The Blockchain/P2P system consists of a cluster of ONOS controllers and a cluster of Atomix agents.
- The cluster of Atomix agents forms a distributed data storage which is shared among the ONOS controllers.

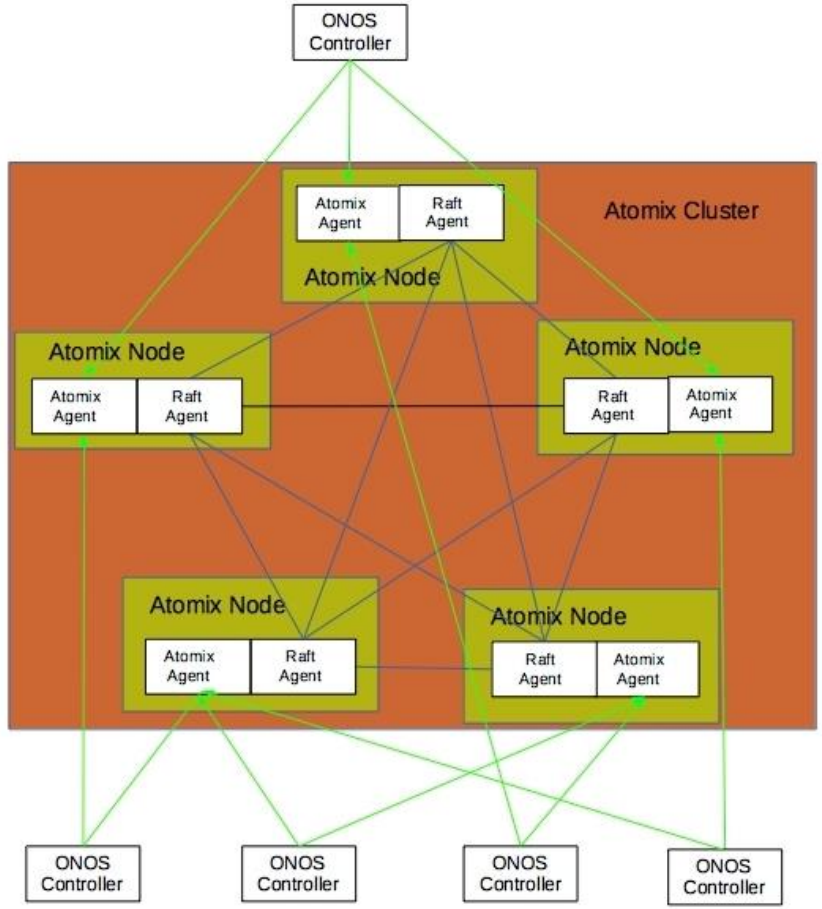


# Project Update

## Project Results (10)

### Consensus in the Blockchain/P2P system

- Consensus has been made a heavy use in the Blockchain/P2P system.
- Multiple instances of consensus are maintained in the cluster of Atomix agents under the Raft protocol.
- One instance of consensus is maintained for dynamically elect an active ONOS controller in the cluster of ONOS controllers.
  - The newly elected active ONOS controller is registered to the current leader Consul agent in the portal service layer.
- Consensus is also used to maintain a peer-to-peer system.
  - The data stored in the cluster of Atomix agents are split into multiple data sets.
  - Each data set is replicated in the cluster of Atomix agents.
  - A consensus is maintained for each data set under the Raft protocol.
  - Each Atomix agent becomes a peer.
  - A distributed indexing structure is maintained among the Atomix agents to route among the peers.
- A blockchain system operates on top of the P2P system.



# Project Update

## Technological Challenges

- Programming the Raft agents to make them to maintain the various types of consensus.
  - The Raft protocol is difficult to be used correctly.
  - Some algorithmic designs and the associated theoretical analysis are needed to construct the desired consensus.
- Correctly constructing the P2P system
  - Dynamically managing the data sets in the P2P system.
  - Maintaining the consensus for each data set.
  - Constructing an indexing structure for routing among different data sets.
  - Both theoretical analysis and system construction are needed.
- Constructing proof-of-reputation consensus model in the blockchain system
  - A solid theoretical analysis is required.

# Project Update

## Next Steps in Accomplishing Project Goals/Objectives

- We have already established a solid framework to support the next stage of the construction of the cloud-based networking platform.
- We have also had a better understanding on the roadmap for furthering our project after having searched into the literature and the state-of-the-arts of the research areas related to our project.
    - We have performed a good documentation on the literature and the existing methods.
    - We still need to creatively develop our own solution methods to meet our needs in this project.
- We need to make the algorithmic designs and analysis needed in the later stage of this project to happen earlier while we are still constructing the basic system support in the current stage.
    - It is a very challenging task to conduct the theoretical analysis on the proof-of-reputation consensus model in the existence of *Byzantine* participants.

# Concluding Remarks

- This project aims to strengthen the security protection of software defined networking (SDN) by making use of the blockchain and the peer-to-peer (P2P) technologies.
- This project aims to produce two deliverables:
  - A cloud-based networking platform for prototyping and experimenting various designs of safeguarding the software-defined networks deployed in electric power systems.
  - A blockchain/P2P-based technology for detecting the compromised controllers in a software defined network.
- The outcomes of this project will serve for
  - Meeting the general security requirements of the electric power generation systems, and
  - Mitigating the security risks targeting the vulnerabilities of SDN-enabled cybersecurity protection systems.
- Next steps and technical challenges
    - To develop the blockchain/P2P system.
    - The major technical challenges are the solid theoretical study of the proof-of-reputation consensus model.