IEEE Global Information Infrastructure Networking Symposium (GIIS) 2020
October 28th to 30th, 2020

A Blockchain Architecture for SDN-enabled Tamper-Resistant IoT Networks

Akram Hakiri*, Bassem Sellami**, Sadok Ben Yahia**, and Pascal Berthou***

University of Carthage, SYSCOM ENIT, ISSAT Mateur, Tunisia.*
University of Tunis El Manar, Faculty of Sciences, Dept of Computer Sciences (LIPAH).**
LAAS-CNRS Laboratory, Toulouse-France. ***

Outline

- Introduction
- Problem and research challenges
- Requirements
- Solution approach
- Performance evaluation
- Conclusion

What is this Research About?

- Create secure and distributed Blockchain-enabled IoT transactions while reducing resources computation and latency.

- Focusing on resolving a specific challenge of providing an integrated Blockchain-SDN IoT architecture with the help of Network Function Virtualizations (NFV).

Problem: IoT Security and Privacy Trust Framework (1/2)

- Distributed Denial-of-Service (DDoS) can overwhelm IoT network with malicious traffic
  - Malignant IoT nodes can join the network at any time and overwhelm their resources with malicious traffic to make their services unavailable
- Unauthorized access to IoT devices
  - There is a need to secure trustless interactions between IoT devices themselves and with service providers on the Internet

Problem: IoT Security and Privacy Trust Framework (2/2)

- Centralized cloud-based security appliances and infrastructures cannot address IoT's security and privacy concerns
  - Because of lacking resources and flexibility, IoT devices are susceptible to elevation of privileges, and spoofing attacks.
- More advanced, distributed, and IoT "infrastructure-less" approach is required to enhance IoT devices and services security

Solution requirements

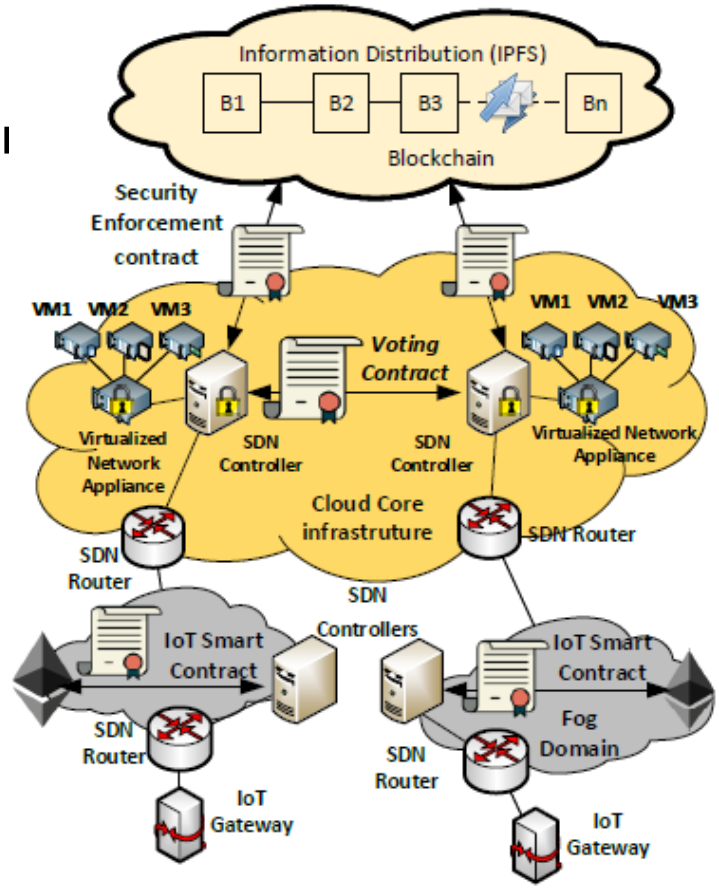
- We need an framework that can
  - Distribute IoT communication over centralized SDN network support
  - Secure IoT transactions against blockchain smart contract recursive calls
  - Prevent DDoS attacks in a distributed IoT network.
    - Detect, remove, and report suspected IoT nodes and mitigate malicious traffic

Solution Approach

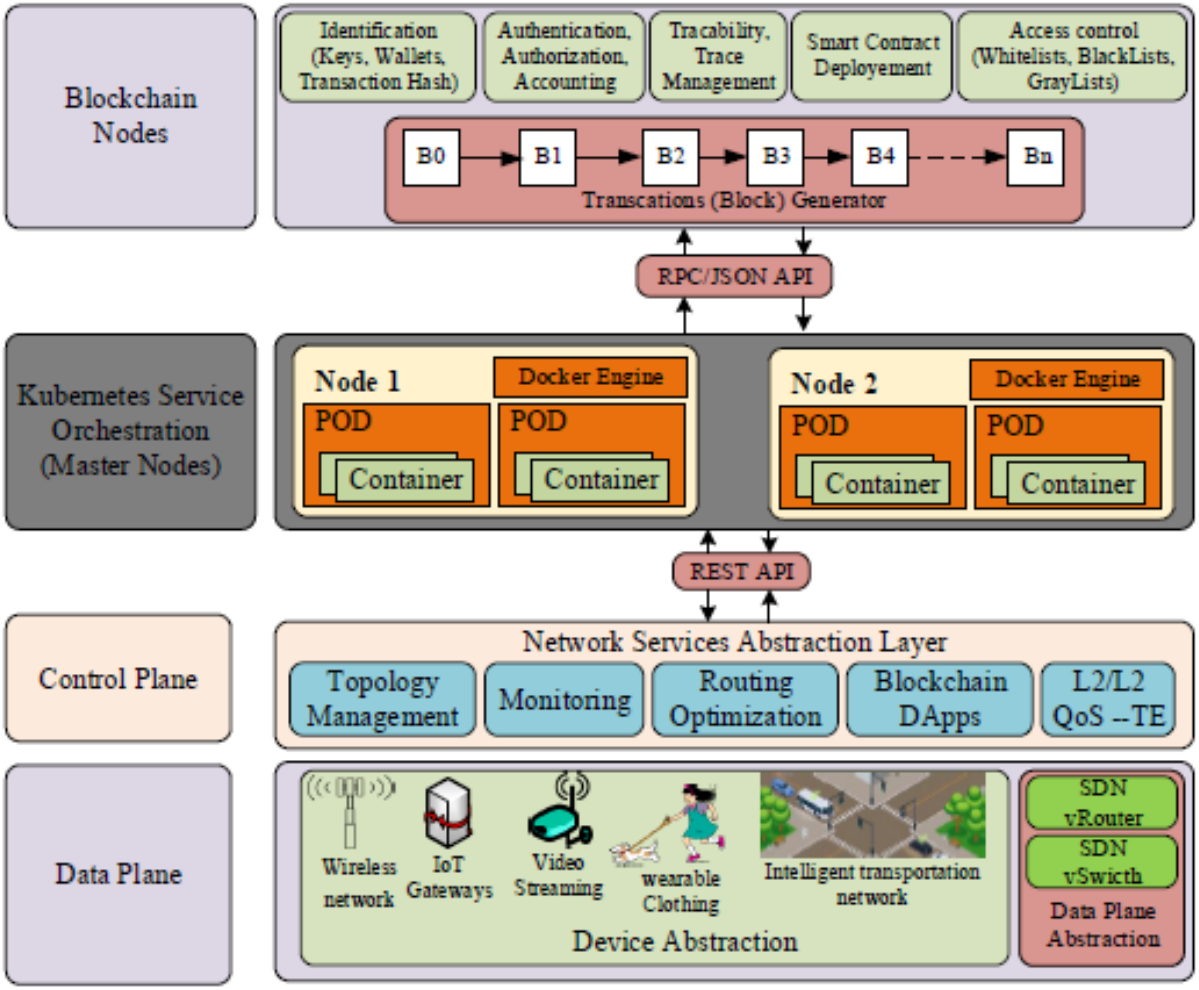
- Implementing a SDN-aware Decentralized Application (DApp),
  - which listen to mining nodes, reports suspicious IP addresses, and validate unknown packets.
- Introduces a Proof-of-Authority (PoA) consensus algorithm
  - that reveals suspected IoT smart devices and report them under smart contract
- Developed an intrusion detection system
  - in a form of virtualized network functions (VNFs) to eliminate malicious flow and enable DDoS detection and mitigation on-Demand

Our solution: Blockchain-SDN based IoT architecture (1/4)

- The peer-to-peer blockchain networking layer :
  - use the Interplanetary File System (IPFS) for storing and sharing data in a distributed file system
- The controller network service abstraction layer:
  - For distributing security policies between Blockchain nodes and IoT network infrastructure
- The virtualization layer :
  - facilitate VNFs orchestration across multiple physical hosts.
- The data plane abstraction layer :
  - SDN vrouters for the abstraction device layer



Our solution: Blockchain-SDN Applications Framework (2/4)



Our solution: Smart Contract Design (3/4)

- Any detected misbehavior is reported not only based on its MAC and IP addresses
  - Detect suspected behavior and report
  - Distribute trusted lists of IoT devices
  - Check the validity of IoT devices connected over the blockchain
- Identify every abnormal behavior in the network
  - Isolate from sending blockchain traffic from the Blacklisted nodes

Our solution: Proof-of-Authority Consensus (PoA) (4/4)

- Mining nodes are elected based on their QoS parameters:
  - higher bandwidth link, lower latency, CPU, Memory, etc,
- Group of authority nodes are pre-approved validators to verify transactions and build blocks
  - we ensure that nodes wishing to become authorities and validators should disclose their identity
- Validating IoT transactions relies on a mining rotation schema
  - to fairly distribute the responsibility of block creation among authorities

Performance Evaluation: PoA VS PBFT and PoET

- PoA performs three (03) times better latency against PBFT and PoET.
- PoA approach helps in reducing
  - the necessary power energy to maintain the network
  - the dependency of using high-performance hardware to validate blocks
- In PoA network consistency
  - is not well defined and supported
  - does not depend on the network size

Conclusion

- SDN/NFV combined with Blockchain to
  - enable dynamic on-demand transparency and security to IoT transactions.
- Meet the various scalability and performance
  - through the use of micro-services on lightweight Kubernetes
- We introduce a Proof of Authority (PoA) consensus mechanism
  - to pre-select IoT leaders as authorities to
    - validate their transactions
    - and verify the accuracy of blocks exchanged

Future work

- Enhance IoT transactions to be more structured, abundant and complete from their creation to their finish,
- Make them more suitable for in-blockchain big data analytics using advanced Graph Neural Networks (GNN)

Thank you for your attention

- Questions & Answers