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.
‡CNRS, LAAS, UPS, 7 Avenue du colonel Roche, F-31400 Toulouse, France.
Corresponding author: akram.hakiri@enit.utm.tn

***Abstract*—In this paper we introduced the design of a novel Blockchain-based IoT network architecture that leverages Software Defined Network (SDN) and Network Function Virtualization (NFV) to secure IoT transactions. We developed an intrusion detection system in a form of Virtualized Network Functions (VNFs) that improves both the scalability and performance of IoT networks. We show how the design of our IoT-focused smart contract can prevent DAO induction attacks in distributed IoT network. We introduce a novel Proof-of-Authority (PoA) consensus algorithm to detect and report suspected IoT nodes and mitigate malicious traffic.**

***Index Terms*—Blockchain; Distributed Ledger; Internet of Things; SDN/NFV; Ethereum; Security.**

I. Introduction

Current security models [1] that empower the IoT communication, such as centralized cloud-based security infrastructures, cannot address the IoT's security and privacy concerns because of lacking resources and flexibility, which makes IoT devices susceptible to elevation of privileges, and spoofing attacks. An attractive and more realistic alternative is the Blockchain [2], which deploys a decentralized infrastructure for fighting DDoS attacks and eliminate the risk of a single point of failure. Blockchain has been seen as the backbone for diverse IoT applications, such as transactive energy auctions [3], guaranteeing fair payments in smart grids [4], Electric Vehicles [5], monitoring environment quality in smart city [6], and trusted healthcare systems [7]. Despite the promise, Blockchain can be cost ineffective [8] as it consumes substantially computation power required by miners to solve a mathematical puzzle known as Proof-of-Work (PoW) problem for creating trusted transactions. Besides, smart contracts come with many disadvantages when deployed in IoT networks. In particular, because smart contracts are immutable by design, upgrading their software code or patching security vulnerabilities becomes difficult and sometimes impossible.

Software Defined Network (SDN) [9] showed a significant promise in meeting IoT needs by offloading the computation to Fog infrastructures at the network edge. Specifically, SDN allows redirecting and balancing IoT flows in case of node or link failure, so that flows will be delivered to their destination while still meeting QoS requirements [10].

978-1-7281-8241-4/20/$31.00

In this paper, we introduce the design of a Blockchain-based architecture for enforcing the security of IoT transactions by implementing a SDN-aware Decentralized Application (DApp), which listen to mining nodes, reports suspicious IP addresses, and validate unknown packets. The architecture introduces a Proof-of-Authority (PoA) consensus algorithm that reveals suspected IoT smart devices and report them under smart contract.

The remainder of this paper is organized as follows: Section II highlights existing approaches to integrate Blockchain in SDN-enabled IoT systems and points out how SDN operates in blockchain-based IoT networks. Section III describes the architecture of our solution on empowering IoT systems with SDN and blockchain. Section V provides concluding remarks describing potential future directions and open research problems in this realm.

II. Related Work

Blockchain has opened up a wide range of possibilities for IoT era as it implements a control logic to manage the diverse information coming from various IoT devices to provide them with a secure communication platform in IoT key themes. For example, Machado et al. [11] introduced two consensus algorithms, i.e. Proof-of-Trust (PoT) and Proof-of-Luck (PoL), which use Fog nodes as a middle layer for integrating IoT devices with the cloud. Chen et al. [12] introduced Devify framework to build an interoperable trusted IoT networks in a decentralized fashion. The framework adopts the Web of Things ontology model to develop cloud-hosted Blockchain IoT applications. Similarly, Singh at al. [13] introduced a unique crypto ID called Trust Bit (TB) for decentralized intelligent vehicle (IV) communication. The authors created a reward system to store Trust bit details, and reward trusted IVs by distributing some TBs after successful and trusted inter-IVs communication.

Similarly, SDN and Blockchain have been merged to mitigate some issues such as flexibility, efficiency, availability, and security. Salahuddin et al. [14] argue that using SDN in blockchain-based IoT networks could enforce the security of IoT data against malicious traffic analysis. Kataoka [15] integrated SDN and blockchain to automate the process of doubting, verification and trusting of IoT web services to prevent them from attacks. Samaniego et al [16] virtualized

IoT resources by combining Blockchain and SDN to enforce permission-based communication during resource provisioning. Additionally, Steichen et al. [17] proposed ChainGuard framework atop of the Floodlight controller to filter and intercept illegitimate packets and prevent malicious behavior from vulnerable sources.

Unlike the aforementioned approaches, our solution delegates blacklisting and whitelisting IP addresses to Virtualized Network Functions (VNFs) instances inside Docker containers. The VNFs trustworthy maintain all reports about white-listed and black-listed IP addresses. VNF instances can be dynamically deployed to meet changing conditions and accommodate to higher traffic demand or more stringent service requirements.

III. Architecture Overview

This section delves into the architectural details that enable to support scalable, dynamic, and flexible resource management with our SDN-based framework, and presents the algorithms to perform tamper-resistant IoT-on-Blockchain communication in symbiosis with SDN.

A. System Design

The architectural overview of our proposed solution comprises four different layers. First, the peer-to-peer blockchain networking layer which use the InterPlanetary File System (IPFS) for storing and sharing data in a distributed file system. Blockchain nodes, i.e. miners and clients, use IPFS to interoperable with smart contracts and blockchain transactions.

Second, both the virtualization layer and the controller network service abstraction layer. The former provides a Blockchain on Kubernetes as an Infrastructure-as-code, where applications are maintained inside Docker containers across multiple physical hosts. It also provides many management features to facilitate the orchestration of VNFs. On the one hand, these virtual appliances host distributed blockchain client nodes in a form of lightweight containers (i.e. Pods), which communicate with the main Blockchain network and perform agreement-driven decisions between each other. On the other hand, they communicate with blockchain applications (i.e. DApps) using low level Application Binary Interface (ABI) calls over remote procedure call (RPC) API to interact with smart contracts. Smart contracts are self-executing contract objects that make it easy to interact with blockchain nodes to exchange data in a trusted, conflict-free manner. Thanks to JSON interface that converts contract agreements, i.e. ABI, into RPC calls without relying on a third party authority.

B. Flow Management

Figure 1 depicts the details of flow management through different layers. First, the Blockchain layer is composed of four modules: 1) the identification module manages the user/node access using the private and public keys. Indeed, IoT node addresses are inferred from their own public keys in the blockchain (i.e. a node address is the last 20 bytes string from the 32-byte string public key after dropping 12 of these bytes), which is also associated with node balances and used for sending and receiving transactions.

Furthermore, since each IoT node could have one or multiple accounts (i.e. called Externally Owned Account (EOA)), it should have different identification scenarios for each EOA. Therefore, the framework implements another module for the Authentication, Authorization and Accounting (AAA) with the Blockchain. Thus, an IoT node can access the infrastructure service using a given account for a given scenarios, and interact with the blockchain through API calls to reserve the required resources and execute the transactions. The authentication is based on identity to ensure impersonation prevention, protect the control and data planes against intrusion, and ensure that malicious attacks do not tamper with the controller configuration.

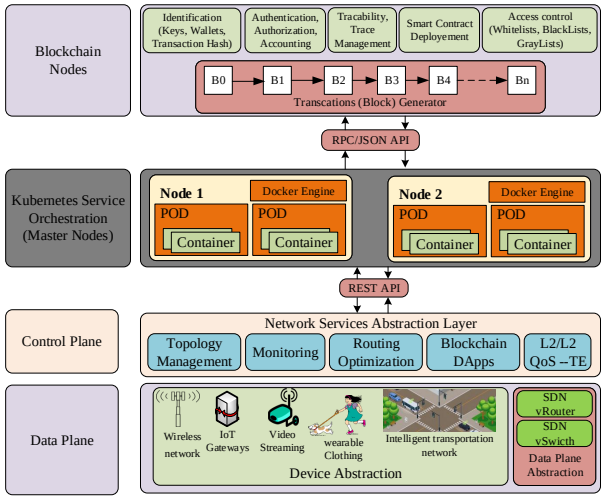

Fig. 1: Blockchain-SDN Applications Framework in Smart City Security.

Similarly, the traceability module offers the ability to trace the entire lifestyle of a transaction, from its originating node to every processing on the blockchain infrastructure. The smart contract deployment module allows the interaction between contract functions and IoT nodes from their creation to their deployment.

C. Smart Contract Design

The smart contract is about 400 lines of Solidity code. Any detected misbehavior is reported not only based on its MAC and IP addresses, but also on the IP addresses of the impacted IoT nodes. For example, a spoofing attacker can read, write, or execute actions in the network. A Data structure "*struct SuspectBehavior*" is used to detect suspected behavior and report, i.e. Data structure "*struct Report*", it to the SDN controller. This latter can now distribute trusted lists of IoT devices. A blockchain validator is introduced to check the validity of IoT devices connected over the blockchain. The validator parses the OpenFlow messages to identify the source and destination of incoming traffic. The SDN controller uses the information contained in the OpenFlow packet headers

to create a wide network view including topology state and transactions meta-data.

By expecting and parsing every OpenFlow packet exchanged between the IoT devices and the network, the SDN controller can identify every abnormal behavior in the network. That is, if an attacker wants to take control of any IoT device, the changes of device ownership in the network will be visible in the topology viewer module within the SDN controller. This method allows the SDN control plane to distinguish two types of lists, i.e. blacklisted devices and whitelisted ones. Blacklisted nodes are suspicious users whose behavior is abnormal (i.e. representatives of malicious attack or unexpected behavior) so the controller should isolate them from sending traffic on the blockchain.

D. Consensus Algorithm

We rely to the Proof-of-Authority (PoA) consensus algorithm to select a set of N trusted nodes called the authorities. To enforce the network security, the PoA selects a pre-qualified number of IoT nodes for validating transactions according to strict rules. First, nodes are elected based on their QoS parameters, i.e. higher bandwidth link, lower latency, and higher hardware resources performance (CPU, Memory, link quality). These nodes can themselves elect a limited number of leaders which have a set of authorities to maintain and keep the network working. By leveraging the identity of pre-selected nodes, our framework gives more importance to a node's reputation rather than the computation power in Bitcoin Proof-of-Work approaches or digital assets owned by nodes in Ethereum PoS (Proof-of-Stake). The advantages of this approach are twofold: first, it helps in keeping the decentralization more efficient while requiring less computational power.

IV. Use Case

A. Blockchain-SDN enabled Internet of Vehicles

Figure 2 depicts a scenario of The Internet of Vehicles (IoV), where distributed networks interconnect various IoT systems, such as connected cars, pedestrians, roads, and parking systems. As shown in Figure 2, SDN can solve the issues related to frequent node topology changes, high node mobility, and dynamic topology changes caused by cooperative nodes communication. Specifically, SDN controllers can exploit information obtained from Road Side Units (RSUs) to find optimal paths to connected vehicles and route messages across shortest paths within the VANET. SDN can also extend RSU coverage by coordinating their communication with other RSUs and with neighbor wireless access points. The SDN controller will collect routing information from the VANET nodes to create a global view map of the connected vehicles and handle various topological changes in the VANET. Furthermore, combined with NFV, the controller will significantly improve scalability, performance and Quality of Service (QoS). Specifically, SDN/NFV enable generation of flow rules to support dynamic resource allocation, network slides isolation and orchestration, and mobility management. RSUs will parse SDN packets received from the controller layer to decide the actions to perform for packet forwarding either to connected vehicles or push them down to other RSUs.

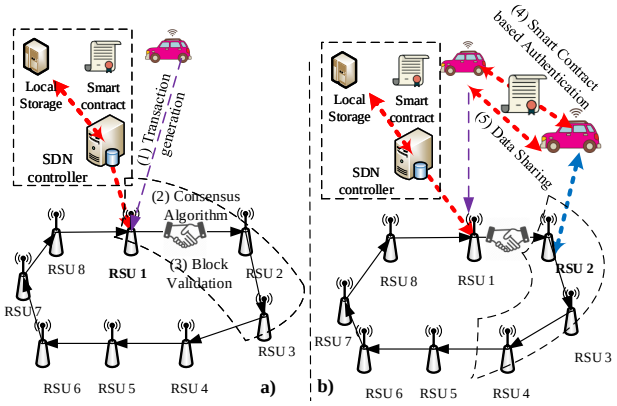

Fig. 2: Secure message dissemination in SDN-enabled VANET

Additionally, Blockchain distributed ledgers, coupled with consensus mechanisms, can guarantee the preservation of trustworthy data. Figure 2 shows two consecutive steps and how current leader and authorities allowed proposing blocks change. There are $N = 8$ authorities (i.e. RSU1 to RSU8), hence $N - (N/2 + 1) = 3$ authorities allowed to propose a block at each step, with one of them acting as leader (the bold node in Figure 2). In the first time step in Figure 2(a), RSU1 is the leader while RSU2 and RSU3 are allowed to propose blocks. Next, in next time step as depicted in Figure 2(b), RSU1 is not allowed anymore to propose a block (it was in the previous step, so it has to wait $(N/2) + 1$ steps), while RSU4 is now authorized to propose a new block and RSU2 is the current leader.

The combination SDN and Blockchain can effectively and efficiently manage and control operations of VANET systems. Blockchain distributed ledgers record transactions generated in VANET nodes and maintain these records in transparent, immutable and secure infrastructure. RSUs nodes can be pre-selected to create blocks and perform lightweight mining. For example, a voting process can be established between these pre-qualified nodes to validate transactions and verify the correctness of exchanged blocks. Various messages exchanged between RSUs can be recorded as evidence the trustworthiness of received data. In such an approach, falsified transactions can be easily detected by the shortlisted cluster of VANET nodes and decisions can be provided to sender nodes to report any detected intrusion. Thus, Blockchain can handle blocks concurrently with SDN to ensure an efficient, agile and flexible network management while preventing malicious activities.

B. Improving Security between IoT Gateways

Figure 3 shows how IoT gateways can be connected to our SDN controller using our developed Blockchain IoT service layer. The SDN controller implements a Python-based decentralized application that integrates with Ethereum Web3 API to filter the traffic and detect suspicious IoT nodes. It provides a collaborative mechanism for whitelisting or blacklisting

suspicious IoT gateway IP addresses. Our approach delegates storing blacklisted and white listed IP addresses to VNFs. VNF instances can be dynamically deployed to meet changing conditions and accommodate to higher traffic demand or more stringent service requirements.

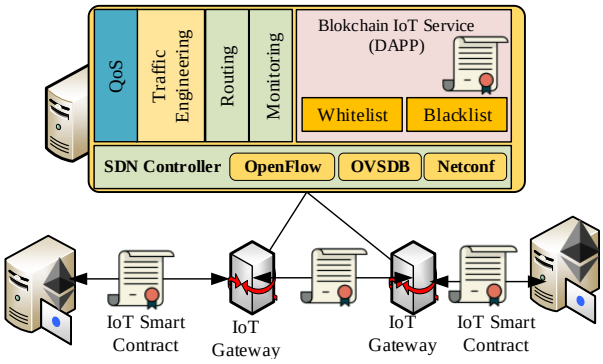

Fig. 3: Ensuring Security and Interoperability between IoT Gateways.

That is, our approach enhances scalability, flexibility, agility, resiliency, and dynamic resource management and enforces trust on the IoT-on-the-blockchain network. Additionally, it enables new types of trust-less interactions for empowering IoT communications and brings more transparency and performance by reducing deep packet inspection of SDN-enabled IoT traffic. Thus, while individual IoT devices need not be powerful to meet IoT security needs, combing the on-demand service orchestration offered by SDN/NFV and security capability offered by Blockchain, we can enforce their coordination in destroying large-scale Botnets. Blockchain security functions can be deployed as container-based virtual appliances for firewalling and mitigating malicious traffic, thereby allowing them to be prepared for threats that can overwhelm well-prepared defenses of critical services.

V. Conclusion

In this paper, we present a novel IoT architecture that combines SDN/NFV and Blockchain to enable dynamic on-demand transparency and security to IoT transactions. Our approach uses lightweight Kubernetes containers to meet various needs of scalability and performance that govern IoT communication. Additionally, we introduced a Proof-of-Authority (PoA) consensus mechanism to preselect IoT leaders as authorities to validate their transactions and verify the correctness of exchanged blocks. Thus, falsified transactions can be detected and eliminated from the network. Thanks to our blockchain-based decentralized application that detects malicious nodes, blacklists them and trigger remote orders to the SDN controller to delete them from the network.

Future directions will focus on how IoT transactions will be more structured, abundant and complete from their creation to their finish, to make them more suitable for in-blockchain big data analytics using advanced Graph Neural Networks (GNN).

Acknowledgments

This work was partially funded by the Tunisian Ministry of Higher Education and Scientific Research (MES) under the Young Researchers Incentive Program (19PEJC09-04). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of MES.

References

[1] P. Massonet, L. Deru, A. Achour, S. Dupont, A. Levin, and M. Villari, "End-to-end security architecture for federated cloud and iot networks," in *2017 IEEE International Conference on Smart Computing (SMARTCOMP)*, 2017, pp. 1–6.

[2] O. Novo, "Blockchain Meets IoT: An Architecture For Scalable Access Management In IoT," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.

[3] A. Hahn, R. Singh, C. C. Liu, and S. Chen, "Smart Contract-based Campus Demonstration Of Decentralized Transactive Energy Auctions," in *2017 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Apr. 2017, pp. 1–5.

[4] T. Lundqvist, A. de Blanche, and H. R. H. Andersson, "Thing-to-thing Electricity Micro Payments Using Blockchain Technology," in *2017 Global Internet of Things Summit (GIoTS)*, Jun. 2017, pp. 1–6.

[5] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling Localized Peer-to-peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[6] S. Ibba, A. Pinna, M. Seu, and F. E. Pani, "Citysense: Blockchain-oriented Smart Cities," in *Proceedings of the XP2017 Scientific Workshops*, ser. XP '17, Cologne, Germany, 2017, pp. 12:1–12:5.

[7] P. Zhang, M. A. Walker, J. White, D. C. Schmidt, and G. Lenz, "Metrics For Assessing Blockchain-based Healthcare Decentralized Apps," in *2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Oct. 2017, pp. 1–4.

[8] F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera, "Overcoming Limits Of Blockchain For IoT Applications," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ser. ARES '17, 2017, pp. 26:1–26:6.

[9] S. Bera, S. Misra, and A. V. Vasilakos, "Software-defined networking for internet of things: A survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1994–2008, Dec. 2017.

[10] C. Zhang, G. Hu, G. Chen, A. K. Sangaiah, P. Zhang, X. Yan, and W. Jiang, "Towards a sdn-based integrated architecture for mitigating ip spoofing attack," *IEEE Access*, vol. 6, pp. 64–77, 2018.

[11] C. Machado and A. A. M. Fröhlich, "Iot data integrity verification for cyber-physical systems using blockchain," in *2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC)*, May 2018, pp. 83–90.

[12] J. Chen, "Devify: Decentralized Internet Of Things Software Framework For A Peer-to-peer And Interoperable Iot Device," in *In proceedings of the Workshop on Advances in IoT Architecture and Systems*, Jun. 2017.

[13] M. Singh and S. Kim, "Trust Bit: Reward-based Intelligent Vehicle Commination Using Blockchain Paper," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Feb. 2018, pp. 62–67.

[14] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, and F. Sallabi, "Softwarization Of Internet Of Things Infrastructure For Secure And Smart Healthcare," *Computer*, vol. 50, no. 7, pp. 74–79, 2017.

[15] K. Kataoka, S. Gangwar, and P. Podili, "Trust List: Internet-wide And Distributed Iot Traffic Management Using Blockchain And Sdn," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Feb. 2018, pp. 296–301.

[16] M. Samaniego and R. Deters, "Using Blockchain To Push Software-defined Iot Components Onto Edge Hosts," in *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies*, ser. BDAW '16, 2016, pp. 58:1–58:9.

[17] M. Steichen, S. Hommes, and R. State, "Chainguard : A firewall for blockchain applications using sdn with openflow," in *2017 Principles, Systems and Applications of IP Telecommunications (IPTComm)*, Sep. 2017, pp. 1–8.