Towards a Blockchain-SDN Architecture for Secure and Trustworthy 5G Massive IoT Networks

Akram Hakiri
ISSAT Mateur, SYSCOM-ENIT
University of Carthage
Carthage, Tunis, Tunisia
akram.hakiri@enit.utm.tn

Behnam Dezfouli
Internet of Things Research Lab
Santa Clara University
Santa Clara, CA, USA
bdezfouli@scu.edu

ABSTRACT

The emerging 5G mobile network is a prominent technology for addressing networking related challenges of Internet of Things (IoT). The forthcoming 5G is expected to allow low-power massive IoT devices to produce high volumes of data that can be transmitted over ultra-reliable, low-latency wireless communication services. However, IoT systems encounter several security and privacy issues to prevent unauthorized access to IoT nodes. To address these challenges, this paper introduces a novel blockchain-based architecture that leverages Software Defined Network (SDN) and Network Function Virtualization (NFV) for securing IoT transactions. A novel security appliance is introduced in a form of Virtualized Network Functions (VNFs) for improving the scalability and performance of IoT networks. Then, we introduce a novel consensus algorithm to detect and report suspected IoT nodes and mitigate malicious traffic. We evaluate and compare our proposed solution against three well-known consensus algorithms, i.e., Proof of Work (PoW), Proof of Elapsed Time (PoET), and Proof of Stake (PoS). We demonstrate that the proposed solution provides substantially lower latency and higher throughput as well as trustworthy IoT communication.

CCS CONCEPTS

• **Networks** → **Programmable networks**; *Security protocols*; *Network privacy and anonymity*; • **Security and privacy** → *Intrusion detection systems*; *Distributed systems security*.

KEYWORDS

SDN; NFV; IoT; Blockchain; Security; Trust and Confidence.

ACM Reference Format:
Akram Hakiri and Behnam Dezfouli. 2021. Towards a Blockchain-SDN Architecture for Secure and Trustworthy 5G Massive IoT Networks. In *Proceedings of the 2021 ACM International Workshop on Software Defined Networks & Network Function Virtualization Security (SDN-NFV Sec'21), April 28, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3445968.3452090

SDN-NFV Sec'21, April 28, 2021, Virtual Event, USA

ACM ISBN 978-1-4503-8318-9/21/04…$15.00
https://doi.org/10.1145/3445968.3452090

1 INTRODUCTION

The emerging 5G mobile broadband network significantly enhances Internet of Things (IoT) connectivity [6]. Millions of battery-powered IoT devices such as smart cameras, environmental monitoring sensors, and smart meters are deployed to serve diverse scenarios such as smart cities, autonomous farming, and smart manufacturing; and these applications require delivering high volumes of data over ultra-reliable, low-latency wireless communication services [14]. The forthcoming Ultra-Wide Band (UWB) 5G employs millimeter-wave (mmWave) signals at frequencies of about 28 GHz and 39GHz. This frequency band facilitates meeting the demands for low-latency, high energy-efficiency, high connection density, and high-speed IoT traffic [7] and enables the deployment of IoT to grow unencumbered in the lower end of the frequency spectrum [8] in the Narrowband Internet of Things (NB-IoT) . However, 5G-enabled massive IoT suffers a variety of security and privacy concerns [40], which hinders the reliability of involved massive IoT devices [34]. Current 5G security models that empower the IoT systems exploit the wireless channel properties [37] to enhance communication security through appropriate coding and signal processing. A compromised IoT device could be prone to Distributed Denial-of-Service (DDoS) attacks and overwhelm IoT network with malicious traffic. Malignant IoT nodes can join the massive IoT network at any time and overwhelm their resources with malicious traffic to make their services unavailable.

Blockchain has opened up a wide range of possibilities for IoT era [31], by managing diverse data coming from various IoT devices and provide them with a secure communication platform in various key scenarios. Blockchain deploys a decentralized security infrastructure for coping against DDoS attacks and eliminating the risks pertaining to relying on a single point of failure [22]. Despite the promise, blockchain can be cost ineffective [5] for massive IoT. For example, Lei et al. introduced the Groupchain [15] framework to support Fog-enabled IoT services on public blockchain. Nonetheless, this approach requires computing resources far beyond the reach of resource-constrained IoT devices, thereby preventing the full adoption of distributed consensus protocols in IoT systems. Zhaofeng et al. [44] introduced a decentralized trust management and secure usage control scheme of IoT big data. However, it consumes a substantial computation power required by miners to solve a mathematical puzzle known as Proof-of-Work (PoW) problem for creating trusted transactions. Furthermore, scalability and decentralization becomes at odds as massive IoT nodes need to store the entire blockchain transactions, state of account balances, contracts, and storage [12].

Software Defined Networking (SDN) [4] and Network Function Virtualization (NFV) [42] showed a significant promise in meeting massive IoT needs by offloading the computation to fog infrastructures close to edge devices and scaling IoT capabilities by allowing on-demand service orchestration and management. In addition to improving the management of network flows in massive IoT systems, SDN allows better isolation of data flows and improves resiliency to failures for critical data [21]. 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 [41].

By enabling sophisticated analysis of IoT transactions and improving security and privacy based on the global network awareness provided by SDN controllers, we surmise that combining blockchain and SDN/NFV can be leveraged to optimize flow management in response to attacks. With this method, we enhance the scalability, flexibility and agility of massive IoT networks using SDN/NFV and enforce trust and resiliency using blockchain. SDN controllers can distribute security policies between the blockchain nodes and IoT network. They can also enforce security and trust between IoT gateways and their local sensors as well as among distributed gateways. Also, our blockchain-enabled architecture enables new types of trust-less interactions for empowering massive IoT communication and brings more transparency and performance by reducing deep packet inspection of IoT traffic.

In particular, in this paper, we introduce the design of a blockchain-based architecture for enforcing the security of massive IoT transactions by implementing a SDN-aware Decentralized Application (DApp), which listens to mining nodes, reports suspicious IP addresses, and verifies unknown packets. The architecture introduces an election process based on the Proof-of-Authority (PoA) consensus mechanism [2] that identifies suspected IoT smart devices and reports them under smart contract. We also developed an intrusion detection system in a form of virtualized network functions (VNFs) inside Kubernetes virtual testbed to eliminate malicious flow and enable DDoS detection and mitigation on demand. Our solution approach offers lower latency and higher throughput compared against PoW and PoS consensus algorithms lower latency and higher throughput

The remainder of this paper is organized as follows: Section 2 highlights existing approaches to integrate blockchain in SDN-enabled IoT systems and points out the unique features of our design to offer a scalable micro-service architecture for easier massive IoT network deployment and monitoring. Section 3 describes the architecture of our solution on empowering massive IoT systems with SDN/NFV and blockchain. Section 4 presents quantitative evaluation of performance and scalability. Section 5 concludes the paper and highlights potential future directions.

2 RELATED WORK

Since SDN and NFV are being nested into 5G mobile backbone to enable network softwarization and slicing, blockchain becomes a promising paradigm to address the challenges pertaining to transparency, immutability, data encryption, confidentiality, integrity, and availability to network infrastructure [36]. Additionally, Guo et al. [10] introduced Deep Reinforcement Learning (DRL) approach to construct the trusted and auto-adjust service function chain (SFC) orchestration architecture and improve resource allocation in SDN/NFV infrastructure. Likewise, Qiu et al. [26] proposed dueling deep Q-learning approach based on blockchain decentralized protocol to implement consensus among multiple controllers under complex industrial environments. Okon et al. [23] proposed a unified SDN and blockchain architecture to enhance wireless spectrum management of mobile network operators (MNOs).

Similarly, Gao et al. [9] enhanced the performance of Vehicular Ad-Hoc Networks (VANETs) by incorporating SDN into decentralized blockchain infrastructure in order to track malicious activities in the network. Singh et al. [35] developed a deep-learning-based blockchain to improve SDN reliability and extend the control plane beyond its centralized ecosystem, thus avoiding a single point of failure. Based on voting-based consensus mechanism, the authors proposed to use the blockchain to identify anomalous switch requests and verify and certify trustworthy SDN switches using zero-knowledge proof.

Likewise, Liu et al. [16] developed an access control system for IoT on consortium blockchain. Benedict et al. [3] proposed serverless blockchain-enabled IoT architecture for monitoring environment quality in smart city. However, these approaches relies on centralized cloud-hosted security infrastructures to deploy authentication and privacy-preserving schemes. Lu et al. [17] proposed a SDN-based energy Internet distributed energy-trading scheme supported by blockchain. Their design offered a reasonable match of the transaction objects and allowed meeting security and privacy needs in smart grids. Misra et al. [20] extended IoT security by implementing an encrypted networked clock mechanism to synchronize IoT devices with their fog network within a private Ethereum blockchain. Hamdaoui et al. [11] implemented a decentralized protocol for enabling secure authentication, registration, and management for participatory IoT devices. The proposed scheme offers fast discovery of IoT resources and secure instantiation of IoT networks-on-demand. Houda et al. [1] introduced a SDN-based framework, called Cochain-SC, for intra-domain and inter-domain DDoS mitigation. Cochain-SC relies on Ethereum's smart contracts to facilitate the collaboration among SDN-based large-scale domains and achieves a high accuracy in detecting illegitimate flows.

Luo et al. [18] proposed to improve the scalability and the flexibility of SDN-based industrial IoT by integrating decentralized blockchain into multi-SDN distributed control plane to handle a large amount of data generated by industrial devices. The authors proposed partially observable Markov decision process (POMDP) and a deep reinforcement learning (DRL) approach to optimize the system energy efficiency, we adaptively allocate computational resources and the batch size of the block. Medhane et al. [19] described a blockchain-based framework that leverages edge-cloud and SDN to support prominent features like continuous confidentiality, authentication, and robustness. A thread detection layer is implemented at the cloud side servers to reduce the overhead of SDN-enabled IoT gateways at the edge layer.

Yan et al. [39] proposed replacing traditional blockchain hash and cryptographic functions with specialized hardware component to attest that the running code was set up correctly in a protected

environment. Nevertheless, breaking a single piece of trusted hardware enables the attacker to always win the lottery. Second, because smart contracts are immutable by design, upgrading their software code or patching security vulnerabilities becomes difficult and sometimes impossible. Rahman et al. [28] proposed a Blockchain-SDN architecture managing a safe and secure data transfer in smart building system. Rahman et al. [27] used SDN/NFV and blockchain in symbiosis to offer a reliable condominium communication in smart building networks. The claimed their framework, called DistB-Condo, can robust, and secured platform to meet safety, confidentiality, flexibility, efficiency, and availability requirements needed by IoT networks.

Rodrigues et al. [30] [29] proposed a DDoS mitigation across multiple network domains using blockchain Signaling System (BSS). The authors envisioned smart contact's collaborative mechanism for whitelisting or blacklisting IP addresses across multi domains SDN network. The BSS framework stores the security reports directly in the contract itself. However, storing reports could grow expensive at scale since the cost of the data entry scales linearly with the number of reports stored by the contract, i.e. gas fees is scared resource in blockchain. Additionally, Blockchain disincentives the storage of large data because each node needs to keep track of a whole blockchain by downloading it. Besides, Hari et al. [13] proposed Internet Blockchain for securing Border Gateway routing Protocol (BGP) sessions and DNS transactions without using a Public Key Infrastructure (PKI). Internet Blockchain allows scaling up the core network to enable a large number of transactions for BGP advertisements and offers a tamper resistant DNS infrastructure. Furthermore, Sharma et al [32] proposed the DistBlockNet framework to update OpenFlow rules, verify security of flow rule entries, and install updated flow rules to the forwarding SDN-aware IoT devices. However, such a solution is also prone to connectivity issues and does not take full advantage of the decentralization and immutability of the blockchain.

Additionally, a web resource can change its content as many times as needed, which makes it hard for blockchain users to keep track of updates and to verify whether the content of the web page is still the same as it was when the entry into the blockchain was created. To overcome these limitations the authors proposed a hybrid blockchain model [33] where the core network holds mining nodes with higher computation power for creating blocks and verifying PoW; and the edge network contains the SDN controllers and lightweight Blockchain nodes (i.e. which do not support mining service) to acheive higher availability and realize ease deployment of smart city networks.

Xie et al. [38] designed a blockchain-based security framework for SDN-enabled vehicular IoT services. They implemented an intelligent transportation system that relies on cloud servers to detect malicious vehicular nodes and perform real-time video reporting and trust management on vehicular messages. Pourvahab et al. [24] presented a cloud-hosted digital forensic architecture using SDN and blockchain to protect their data from unauthorized users. At the core of this architecture is a Secure-Ring-Verification-based Authentication (SRVA) scheme to generate keys using the Harmony Search Optimization (HSO) algorithm. Encryption is performed in cloud servers using Sensitivity-Aware Deep Elliptic Curve Cryptography (SA-DECC) algorithm. Pourvahab et al. [25] introduced a forensics architecture in SDN-IoT that establishes the Chain of Custody (CoC) in blockchain. The CoC migrates SDN packets from malicious SDN routers to nearby switches. The packets disobeying flow rules are discarded. Sharma et al. [33] proposed a novel blockchain-based distributed cloud architecture with a SDN-enabled controller fog nodes at the edge of the network to meet the required design principles.

Unlike the aforementioned approaches, our solution delegates blacklisting and whitelisting IP addresses to VNFs instances, which we implemented in a form of micro-services inside Kubernetes-based Docker containers. These VNFs micro-services are dynamically deployed to meet changing conditions, accommodate to higher traffic demand or more stringent service requirements, and report white-listed and black-listed IP addresses. Furthermore, instead of using computationally-intensive puzzle and energy intensive PoW, we introduce an election process based on the Proof-of-Authority (PoA) consensus algorithm to select a pre-qualified number of IoT nodes for validating transactions according to strict rules. Additionally, we implemented a Blockchain Decentralized Application (DApp), as a SDN northbound network application, to enforce trust of IoT transactions. Moreover, we employ state-machine replications with the VNF appliances to deal with existing cloud-hosted Byzantine nodes, enable DDoS detection and mitigation-on-demand. That is, our architecture of distributed SDN controllers is aligned with distributed blockchain nodes to avoid unified IoT vulnerability attacks of fog computing nodes to achieve latency reduction.

3 SYSTEM MODEL

This section delves into the architectural overview of our blockchain-SDN framework for flexible, tamper-resistant resource management of massive IoT communication.

3.1 Overview of the Blockchain-SDN enabled Architecture

The system design of our proposed framework is described in Figure 1, which comprises four different layers.

The first layer is the blockchain networking layer, which allows storing and sharing data in a distributed file system (i.e. IPFS). Blockchain validating nodes, i.e., nodes *B1, B2, etc.* in Figure 1, relay to each others to maintain a copy of every IoT transactions' blocks and check (approve or reject blocks) and confirm the transactions against the consensus rules (cf. Section 3.4). Specifically, each validating node acts as service provider in the platform, where each node interacts with other nodes in the blockchain through a distributed smart Service Level Agreement (SLA) to guarantee the trustworthiness of involved IoT transactions. Trusted transactions are executed using consistent distributed agreements in a conflict-free manner, without the need for a central arbitration authority. Thus, the integration of a SLA into blockchain smart contract makes it possible to verify that the delivered service fulfills the required Quality of Service (QoS).

The second layer involves both the virtualization layer and the controller network service abstraction layer. The blockchain virtualization is performed using Kubernetes micro-services deployed through an Infrastructure as code (IaC). Virtualized appliances are

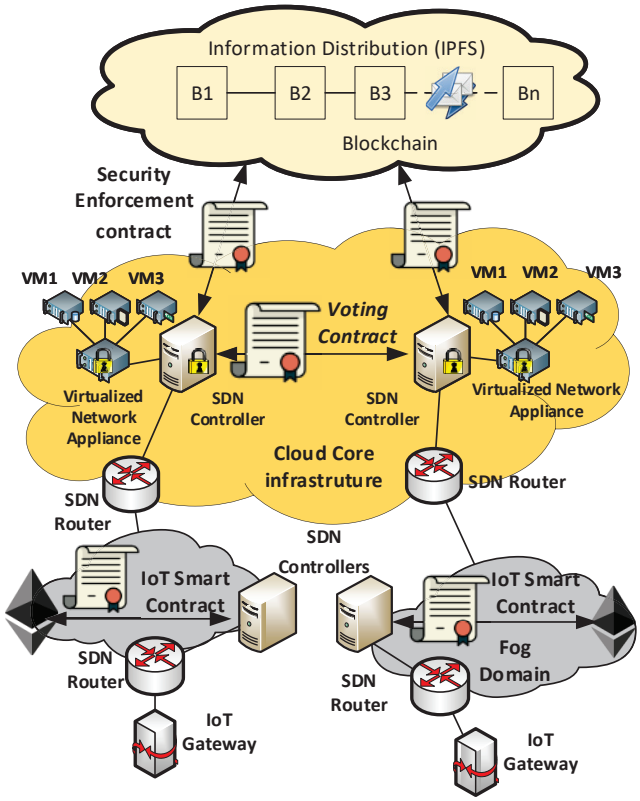

Figure 1: Overview of the Blockchain-SDN IoT architecture.

deployed inside small execution units called pods, which maintain lightweight Docker containers. On the one hand, virtual appliances host distributed ledger nodes and communicate with the main blockchain network and perform agreement-driven decisions between each other. These appliances are running across multiple physical hosts to offer agile management features and facilitate the orchestration of VNFs. On the other hand, virtual appliances communicate with blockchain-SDN applications (i.e., DApps) using low-level Application Binary Interface (ABI) calls over Remote Procedure Call (RPC) to interact with smart contracts. The contract object is converted into json interface where all the contract calls are converted into low-level ABI calls over RPC.

The distributed SDN controllers are responsible for distributing security policies among blockchain nodes and IoT network infrastructure. This is achieved by the blockchain decentralized applications (running inside these controllers), which trigger the generation of transactions' data from different IoT nodes. All transactions are cryptographically secured using hash functions and embedded inside blocks of data. Because massive IoT devices can join and leave the SDN network in a dynamic fashion, they use asymmetric authentication to sign a JSON token. These tokens are then passed to the SDN controller as the proof of identity of the IoT device. Then, consensus-driven decisions are made between DApps to validate blocks generated by different IoT nodes. Once validated, blocks are immutable and their content will not be altered, modified or deleted during the process.

Furthermore, the SDN control plane in Figure 1 encompasses softwarized agile, flexible, and communication layer that translates blockchain decisions (i.e., transactions and blocks validations) into flow rules to program the underlying SDN routers according to the application requirements. Specifically, the controller listens to the incoming IoT traffic and reports suspicious IP addresses before verifying unknown packets. Besides, intrusion detection VNFs (i.e., Firewall as a Service) are deployed inside Kubernetes clusters to take care of malicious flows and enable on-demand DDoS detection and mitigation. The SDN controller triggers storing decisions to VNF instances to maintain reports about white-listed and blacklisted IP addresses. Routing SDN packets among these VNF components is completely managed and controlled by the SDN controller using the *pipework* and the *overlay* mode of Open vSwitch software router. The former allows connecting multiple containers in arbitrarily complex scenarios. The later provides a form of private IP addresses that are only valid internally. Each IP address P identifies a service deployment in a separate chain, so that the SDN controller can program the flow table with the required flow entries F_P to define the following component $B = F_P(A)$ in the chain for which the traffic will be forwarded. The controller creates, for each flow entry F_P, the forwarding table entries that match received packets against the forwarding ports A they should follow with P as the destination address. The Kubernetes manager can dynamically scale up and down clustered VNFs to meet changing conditions and accommodate higher traffic demand or more stringent service requirements.

Finally, the data plane abstraction layer in Figure 1 contains both SDN virtual routers and switches as well as the abstraction device layer. It gathers sensing data from IoT gateways that connect remote sensors and actuators. SDN controllers implement security policies to protect the underlying virtual routers and switches against eventual intrusions. As the SDN routers are directly connected to the blockchain, data are encrypted before being transmitted to remote participants.

3.2 Blockchain as a Service

Figure 2 depicts the details of flow management through different layers. First, the blockchain layer is composed of four modules. The identification module manages user/node access using private and public keys. Indeed, IoT node addresses are inferred from their own public keys in the blockchain after parsing their tokens, which is also associated with node balances and used for sending and receiving transactions. Furthermore, since each IoT node can have one or multiple accounts each with different token/keys, it should have different identification scenarios for each account. Therefore, the framework implements another module for the Authentication, Authorization and Accounting (AAA) within the blockchain. An IoT node can access the infrastructure service using a given account for given scenarios, interact with the blockchain through API calls, reserve the required resources and execute the transactions. The authentication is based on asymmetric cryptography to ensure impersonation prevention, protect the control and data planes against intrusion, and ensure that malicious attacks do not tamper with the controller configuration. 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. Finally, the access control module holds the functions for enforcing trust on transactions by listening to mining nodes and reporting suspicious IP addresses.

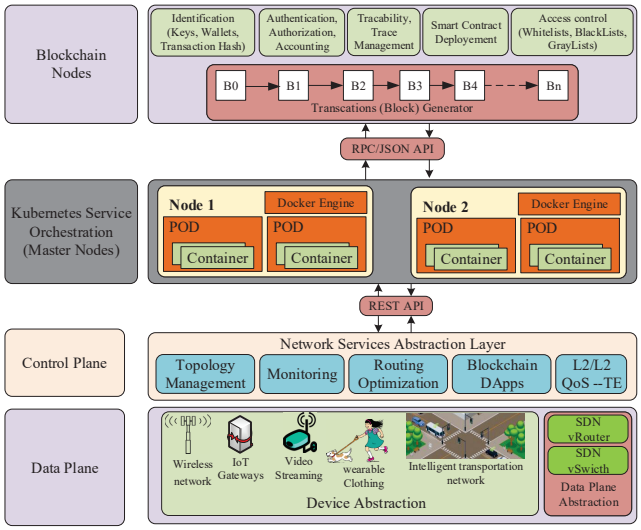

Figure 2: Blockchain-SDN Applications Framework in Smart City Security.

Kubernetes orchestration layer allows creating a set of network functions that can be deployed into software packages, assembled and chained to create the services required by massive IoT nodes. It also coordinates and orchestrates the virtual appliances (i.e., containers) either when predefined resource limits are being reached or after receiving trigger events from the underlying SDN controller. The latter also signs and verifies IoT transactions across distributed IoT nodes in which data could be signed and verified in near real-time. Leveraging SDN/NFV enforces the coordination of massive IoT nodes and increases their performance by creating a modular architecture in which virtual miners can be hosted inside a NFV platform such as the Open Platform for NFV (OPNFV) [42]. On the other hand, the SDN controller network abstraction layer enforces the security policies and configuration of the data plane by protecting flow table rules inside virtual SDN routers from intentional or unintentional tampering.

3.3 Smart Contract

Similar any other regular transaction generated by massive IoT devices, smart contracts must be validated by distributed nodes. However, smart contracts have a specific built-in account in the blockchain without any private key. They are stored and managed as special transactions that can be used to interact with DApps. Algorithm 1 illustrates the contract deployment to provide a trustworthy mechanism to secure IoT transactions.

Algorithm 1 describes how the SDN controller can enforce trust of the network using function *setFlowRulesTurstList* in line 2. Any

Algorithm 1: Deploy the Smart Contract.

Input: Contract Address & ABI
Output: List of available nodes
`// Deploys contract`
1 getInstance(class ContractInterface)
2 deployContract(ABI, contractAddress)
`// Retreive IoT application by token`
3 nodes ← mycontract(nodeAddress).getAllApps()
4 **for** *i* ← *1* **to** *length(nodes)* **do**
`// Get nodes' details`
5 nodesDetails ← mycontract(getAppsDetails(nodes[i])
`// generate a list of application details`
6 ListApps[apps[i]] ← nodesDetails
`// Sending maching packets to SDN controller`
7 **for** *j* ← *1* **to** *len*(*ListApps*) **do**
8 setFlowRulesTurstList(ListApps[apps[i]])
`// Receive SDN controller messages`
9 devices ← getAllDevices()
10 **for** *i* ← *1* **to** *len* (*devices*) **do**
`// Get IoT device info`
11 deviceInfo ← mycontract(getIoTDevDetails(devices[i]))
`// Get service layer details`
12 appDevInfo ←
mycontract(getIoTDevApps(detailsIoTDev[1]))
`// List IoT devices by their Apps`
13 listDevs[devices[i]] ← (IP, MAC, Apps)
14 **for** *k* ← *1* **to** *length(listDevs)* **do**
15 tmp ← ListApps[k]
portsDev.Append(tmp["appProtocol"]-
"tmp["appPort"])

detected misbehavior is reported not only based on its MAC and IP addresses, but also by identifying the business application impacted by possible intrusion. A blockchain validator is introduced to check the validity of IoT devices connected over the blockchain. The validator parses 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 global 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 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.

Algorithm 2 shows how the SDN control plane distinguishes two types of lists, i.e., blacklist and whitelist. The blacklist includes suspicious IoT devices with abnormal behaviour, i.e., representatives of malicious attack or unexpected behavior. The controller uses this list to isolate these devices from sending traffic to the blockchain. The function *servergateway()* is called when an overwhelmed node

Algorithm 2: Blacklisting and Whitelisting of IoT nodes

Input: List IoT devices by Apps
Output: Update trusted IoT apps by protocol:ports

```
// Update list of protocol:ports
results ← list(portsDev) ;
if length(results) ≠ 0 then
    for i ← 1 to length(results) do
        keys ← results[i] ;
        for k ← 1to length(ListApps) do
            p ← ListApps[k] ;
            if key["appPort"] = p[1] then
                // Port added
                file.write(p[1] + "," + key["time"]") ;
for i ← 1 length(ListDevs) do
    src_mac ← ListDevs[i] ;
    src_ip ← key['IP'] ;
    myapp ← key['myApp'] ;
    Assert(key in ListDevs) ;
    for i ← 1 to length(myapp) do
        // Reputation preprocessor to whitelist
           trusted IoT nodes
        if myapp[i] in ListApps then
            dst_ip ← ListApps[myapp[i]]['appIPaddr'];
            dst_port ← ListApps[myapp[i]]['appPort'];
            proto ← ListApps[myapp[i]]['appProtocol'];
            source ← ListMAc[key]['dpid'] -
              ListMAc[key]['dpid'] ;
            dest ← servergateway;
            // Create SDN topology graph
            create_graph (source, servergateway, src_mac,
              scr_ip, dst_ip, dst_port, proto)
```

must be removed the network. The whitelist includes users or devices whose behavior is normal and can continue delivering their content as they belong to the blockchain. As shown in line 21 of Algorithm 2, the SDN controller continuously updates the list of whitelisted nodes and establishes a topology graph, which displays a topology of discovered trustworthy IoT nodes.

3.4 Consensus Agreement

We rely on the Proof-of-Authority (PoA) consensus algorithm to select a set of N trusted nodes called the authorities. To enforce 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). At each time step, these pre-selected nodes use a rotating algorithm to elect a leader node who propagates the current block.

Figure 3 illustrates the rotating algorithm where an IoT device (circle *0* in sub-figure c)) send a commit message to the blockchain. At the first time step *t1*, node ***a1*** is elected as a leader where nodes ***a2*** and ***a3*** can propose blocks but are not leaders. In the next time step *t2*, node ***a2*** becomes the leader and nodes ***a3*** and ***a4***. Node ***a1*** becomes in a waiting state and it cannot propose new block until the node ***a7*** becomes a leader. This rotating algorithm helps in keeping the decentralization more efficient while requiring less computational power.

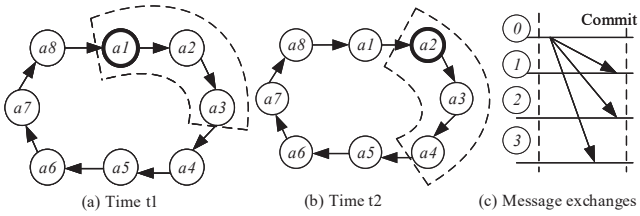

Figure 3: Election Process of Validating IoT Nodes

Second, by relying on a group of pre-approved authority nodes to validate IoT transactions, we make sure that nodes wishing to become leaders should voluntarily disclose their identity. A dedicated data-store is used to keep the list of pre-approved nodes, and new active nodes who wish to join the group of authorities, should comply with series of rules to be considered trustworthy, i.e., should be elected by at least 51% of existing ones. Third, validating IoT transactions rely on a mining rotation schema to fairly distribute the responsibility of block creation among authorities. All IoT validating nodes are asynchronous and all of them are allowed to propose blocks in each computation step. The current step is calculated based on an equation that combines the block number and the number of authorities. To prevent an authority from monopolizing the network resources, i.e., proposing a block when it is not allowed, each authority node is only allowed to propose a block every *'N/2 + 1'* blocks. That is, at any point of time a maximum number of *'N – (N/2 + 1)'* authorities allowed to propose a block. If an authority node acts maliciously it can be voted out and removed by other nodes from the list of legitimate authorities if a majority is reached.

4 RESULTS

We consider two key performance metrics: *transactions latency* and *transaction throughput*, to determine the effectiveness and fitness of the proposed approach. We implemented a prototype including 20 nodes that act as blockchain miners, where each node runs our leader election consensus algorithm. Then we compared our solution against three well-known consensus algorithms [43], i.e., Proof of Work (PoW), Proof of Elapsed Time (PoET), and Proof of Stake (PoS). The POW consensus algorithm involves solving cryptographically hard mathematical puzzles by using miners computational resources. PoS avoids using complex and unnecessary calculations used by the PoW. Instead of miners, there are validators that their own resources as pledge to become candidates to create and validate blocks. The PoET is a random leader election consensus introduced by Intel in which a separate random timer that operates independently at every node to spread the chances of winning equally across network participants. This randomization gives every single node the same chance of likely to be the winner.

We evaluate transactions latency by assessing the time between publishing an IoT transaction until its commitment and validation by validating nodes. We evaluate transaction throughput as the rate of committing valid transactions per second. In terms of transaction's latency, i.e., the time between submitting a transaction t by a participating node and its commit of a block including t by a leader node, our election-based IoT node validation process shows lower latency compared to other consensus algorithms. Because our approach relies on PoA, which is a communication-oriented consensus mechanism that does not involve extensive computation, it assumes bounded latency expressed in terms of time steps. Our approach achieves an average latency of 30ms for validating an IoT transaction, compared to the 600ms delay achieved by PoW, and 12 seconds by PoS. The PoET algorithm commits a transaction within 25 seconds and needs additional 10 seconds to validate it.

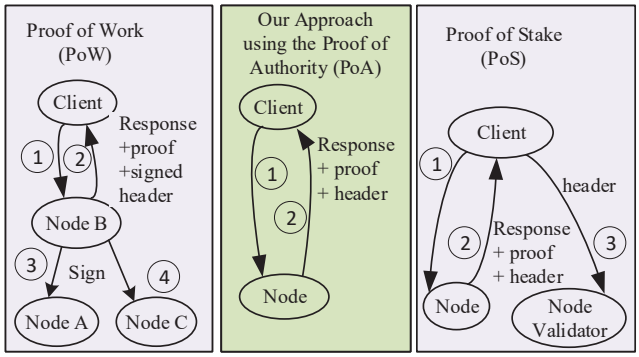

Figure 4: Transaction's Flow For our prototype using the three approaches.

Figure 4 depicts the transactions' flow in our solution and compares it to PoW and PoS. In our approach, each block proposal requires only one round for leader to validate the transaction and send the confirmation to all other authority nodes. The block is committed at once, hence the latency in terms of message rounds is one. Thus, our approach requires less message exchanges and hence shows a higher throughput. The PoW consensus algorithm, requires four message rounds to commit a block, which means that before a new IoT transaction block is confirmed, it should be verified and approved by most network nodes. Additionally, in PoW all unverified IoT transactions are put together in a poll, then all miners work to check that those transactions are legitimate by solving a complex mathematical puzzle. Thus, the PoW consensus algorithm is the most reliable and secure among the three algorithms. However, it has scalability issues because the block size is very small to sustain thousands of transactions, which limits the throughput performance of PoW.

Similarly, PoS already tackle the main scalability issues that PoW faces. PoS requires less message exchange to validate a block, i.e. there are three message exchange rounds per IoT transaction as shown in Figure 4. However, this difference is not significant. PoS fails to solve the performance problem since it needs to save a full copy of the ledger, which means that IoT devices should use far more memory than is currently expected from IoT devices.

Finally, the lottery-based style of consensus algorithms (i.e., PoET) needs five message rounds (i.e., Request, Commit, Fork, Resolve, and Consistency) to validate a block. Therefore, our approach based on PoA consensus mechanism archives higher transaction throughput compared to the other algorithms.

5 CONCLUSION

In this paper, we proposed a distributed blockchain-based SDN architecture for secure and tamper-resistant massive IoT settings. We introduced blockchain-based secure micro-services in a form of VNFs for improving both the scalability and performance of massive IoT networks. We show how the design of our IoT-focused smart contract can prevent distributed attacks. Additionally, an election process based on Proof-of-Authority (PoA) consensus mechanism is established between these validating nodes to validate transactions, verify the correctness of exchanged blocks, and perform lightweight mining. Our results confirm our claims that the solution we propose can readily be used to detect and eliminate falsified IoT transactions. Using the PoA consensus protocol, our mining IoT blocks offer 66% lower-latency compared against PoW and PoS consensus algorithms. In the future, we plan to demonstrate a systematic approach to improve SDN-blockchain with Federated Machine Learning and solve the issue of data ownership and privacy.

ACKNOWLEDGMENTS

This work was funded by the NGI Explorers Program under the Horizon 2020 Research and Innovation Framework (H2020), Grant Agreement number: 825183, Call identifier: H2020-ICT-31-2018. 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 NGI or H2020.

REFERENCES

[1] Z. Abou El Houda, A. S. Hafid, and L. Khoukhi. 2019. Cochain-SC: An Intra- and Inter-Domain Ddos Mitigation Scheme Based on Blockchain Using SDN and Smart Contract. *IEEE Access* 7 (2019), 98893–98907.

[2] N. A. Asad, M. T. Elahi, A. A. Hasan, and M. A. Yousuf. 2020. Permission-Based Blockchain with Proof of Authority for Secured Healthcare Data Sharing. In *2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT)*. IEEE, New York, NY, USA, 35–40.

[3] S. Benedict. 2020. Serverless Blockchain-Enabled Architecture for IoT Societal Applications. *IEEE Transactions on Computational Social Systems* 7, 5 (Oct 2020), 1146–1158.

[4] S. Bera, S. Misra, and A. V. Vasilakos. 2017. Software-Defined Networking for Internet of Things: A Survey. *IEEE Internet of Things Journal* 4, 6 (Dec. 2017), 1994–2008.

[5] Francesco Buccafurri, Gianluca Lax, Serena Nicolazzo, and Antonino Nocera. 2017. Overcoming Limits Of Blockchain For IoT Applications. In *Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES '17)*. Association for Computing Machinery, New York, NY, USA, Article 26, 6 pages.

[6] L. Chettri and R. Bera. 2020. A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems. *IEEE Internet of Things Journal* 7, 1 (2020), 16–32.

[7] I. B. F. de Almeida, L. L. Mendes, J. J. P. C. Rodrigues, and M. A. A. da Cruz. 2019. 5G Waveforms for IoT Applications. *IEEE Communications Surveys Tutorials* 21, 3 (2019), 2554–2567.

[8] J. Ding, M. Nemati, C. Ranaweera, and J. Choi. 2020. IoT Connectivity Technologies and Applications: A Survey. *IEEE Access* 8 (2020), 67646–67673.

[9] J. Gao, K. O. Obour Agyekum, E. B. Sifah, K. N. Acheampong, Q. Xia, X. Du, M. Guizani, and H. Xia. 2020. A Blockchain-SDN-Enabled Internet of Vehicles Environment for Fog Computing and 5G Networks. *IEEE Internet of Things Journal* 7, 5 (May 2020), 4278–4291.

[10] S. Guo, Y. Dai, S. Xu, X. Qiu, and F. Qi. 2020. Trusted Cloud-Edge Network Resource Management: DRL-Driven Service Function Chain Orchestration for IoT. *IEEE Internet of Things Journal* 7, 7 (July 2020), 6010–6022.

[11] B. Hamdaoui, M. Alkalbani, A. Rayes, and N. Zorba. 2020. IoTShare: A Blockchain-Enabled IoT Resource Sharing On-Demand Protocol for Smart City Situation-Awareness Applications. *IEEE Internet of Things Journal* 7, 10 (Oct 2020), 10548–10561.

[12] R. Han, V. Gramoli, and X. Xu. 2018. Evaluating Blockchains For IoT. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, New York, NY, USA, 1–5.

[13] Adiseshu Hari and T. V. Lakshman. 2016. The Internet Blockchain: A Distributed, Tamper-Resistant Transaction Framework for the Internet. In *Proceedings of the 15th ACM Workshop on Hot Topics in Networks (HotNets '16)*. Association for Computing Machinery, Atlanta, GA, USA, 204–210.

[14] H. Hejazi, H. Rajab, T. Cinkler, and L. Lengyel. 2018. Survey of platforms for massive IoT. In *2018 IEEE International Conference on Future IoT Technologies (Future IoT)*. IEEE, New York, NY, USA, 1–8.

[15] K. Lei, M. Du, J. Huang, and T. Jin. 2020. Groupchain: Towards a Scalable Public Blockchain in Fog Computing of IoT Services Computing. *IEEE Transactions on Services Computing* 13, 2 (March 2020), 252–262.

[16] H. Liu, D. Han, and D. Li. 2020. Fabric-iot: A Blockchain-Based Access Control System in IoT. *IEEE Access* 8 (2020), 18207–18218.

[17] X. Lu, L. Shi, Z. Chen, X. Fan, Z. Guan, X. Du, and M. Guizani. 2019. Blockchain-Based Distributed Energy Trading in Energy Internet: An SDN Approach. *IEEE Access* 7 (2019), 173817–173826.

[18] J. Luo, Q. Chen, F. R. Yu, and L. Tang. 2020. Blockchain-Enabled Software-Defined Industrial Internet of Things With Deep Reinforcement Learning. *IEEE Internet of Things Journal* 7, 6 (June 2020), 5466–5480.

[19] D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad, and J. Wang. 2020. Blockchain-Enabled Distributed Security Framework for Next-Generation IoT: An Edge Cloud and Software-Defined Network-Integrated Approach. *IEEE Internet of Things Journal* 7, 7 (July 2020), 6143–6149.

[20] S. Misra, A. Mukherjee, A. Roy, N. Saurabh, Y. Rahulamathavan, and M. Rajarajan. 2021. Blockchain at the Edge: Performance of Resource-Constrained IoT Networks. *IEEE Transactions on Parallel and Distributed Systems* 32, 1 (Jan 2021), 174–183.

[21] Vaishnavi Moorthy, Revathi Venkataraman, and T. Rama Rao. 2020. Security and privacy attacks during data communication in Software Defined Mobile Clouds. *Computer Communications* 153 (2020), 515–526.

[22] O. Novo. 2018. Blockchain Meets IoT: An Architecture For Scalable Access Management In IoT. *IEEE Internet of Things Journal* 5, 2 (April 2018), 1184–1195.

[23] A. A. Okon, I. Elgendi, O. S. Sholiyi, J. M. H. Elmirghani, A. Jamalipour, and K. Munasinghe. 2020. Blockchain and SDN Architecture for Spectrum Management in Cellular Networks. *IEEE Access* 8 (2020), 94415–94428.

[24] M. Pourvahab and G. Ekbatanifard. 2019. Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology. *IEEE Access* 7 (2019), 153349–153364.

[25] M. Pourvahab and G. Ekbatanifard. 2019. An Efficient Forensics Architecture in Software-Defined Networking-IoT Using Blockchain Technology. *IEEE Access* 7 (2019), 99573–99588.

[26] C. Qiu, F. R. Yu, H. Yao, C. Jiang, F. Xu, and C. Zhao. 2019. Blockchain-Based Software-Defined Industrial Internet of Things: A Dueling Deep Q -Learning Approach. *IEEE Internet of Things Journal* 6, 3 (June 2019), 4627–4639.

[27] A. Rahman, M. J. Islam, Z. Rahman, M. M. Reza, A. Anwar, M. A. P. Mahmud, M. K. Nasir, and R. M. Noor. 2020. DistB-Condo: Distributed Blockchain-Based IoT-SDN Model for Smart Condominium. *IEEE Access* 8 (2020), 209594–209609.

[28] A. Rahman, M. K. Nasir, Z. Rahman, A. Mosavi, S. S., and B. Minaei-Bidgoli. 2020. DistBlockBuilding: A Distributed Blockchain-Based SDN-IoT Network for Smart Building Management. *IEEE Access* 8 (2020), 140008–140018.

[29] Bruno Rodrigues, Thomas Bocek, and Burkhard Stiller. 2017. Enabling A Cooperative, Multi-domain Ddos Defense By A Blockchain Signaling System (bloss). In *42nd IEEE Conference on Local Computer Networks 2017*. IEEE, Singapore, 1 – 3.

[30] Bruno Bastos Rodrigues, Thomas Bocek, Andri Lareida, David Hausheer, Sina Rafati, and Burkhard Stiller. 2017. A Blockchain-based Architecture For Collaborative Ddos Mitigation With Smart Contracts. In *AIMS*. Springer, Zurich, Switzerland, 33– 46.

[31] R. Sekaran, R. Patan, A. Raveendran, F. Al-Turjman, M. Ramachandran, and L. Mostarda. 2020. Survival Study on Blockchain Based 6G-Enabled Mobile Edge Computation for IoT Automation. *IEEE Access* 8 (2020), 143453–143463.

[32] P. K. Sharma, M. Y. Chen, and J. H. Park. 2017. A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture For Iot. *IEEE Access* PP, 99 (2017), 1–1.

[33] V. Sharma, I. You, F. Palmieri, D. N. K. Jayakody, and J. Li. 2018. Secure And Energy-efficient Handover In Fog Networks Using Blockchain-based DMM. *IEEE Communications Magazine* 56, 5 (May 2018), 22–31.

[34] Sabrina Sicari, Alessandra Rizzardi, and Alberto Coen-Porisini. 2020. 5G In the internet of things era: An overview on security and privacy challenges. *Computer Networks* 179 (2020), 107345.

[35] M. Singh, G. S. Aujla, A. Singh, N. Kumar, and S. Garg. 2021. Deep-Learning-Based Blockchain Framework for Secure Software-Defined Industrial Networks. *IEEE Transactions on Industrial Informatics* 17, 1 (Jan 2021), 606–616.

[36] M. Tahir, M. H. Habaebi, M. Dabbagh, A. Mughees, A. Ahad, and K. I. Ahmed. 2020. A Review on Application of Blockchain in 5G and Beyond Networks: Taxonomy, Field-Trials, Challenges and Opportunities. *IEEE Access* 8 (2020), 115876–115904.

[37] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao. 2018. A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead. *IEEE Journal on Selected Areas in Communications* 36, 4 (2018), 679–695.

[38] L. Xie, Y. Ding, H. Yang, and X. Wang. 2019. Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs. *IEEE Access* 7 (2019), 56656–56666.

[39] W. Yan, N. Zhang, L. L. Njilla, and X. Zhang. 2020. PCBChain: Lightweight Reconfigurable Blockchain Primitives for Secure IoT Applications. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 28, 10 (Oct 2020), 2196–2209.

[40] R. Yugha and S. Chithra. 2020. A survey on technologies and security protocols: Reference for future generation IoT. *Journal of Network and Computer Applications* 169 (2020), 102763.

[41] C. Zhang, G. Hu, G. Chen, A. K. Sangaiah, P. Zhang, X. Yan, and W. Jiang. 2018. Towards a SDN-Based Integrated Architecture for Mitigating IP Spoofing Attack. *IEEE Access* 6 (2018), 64–77.

[42] T. Zhang, H. Qiu, L. Linguaglossa, W. Cerroni, and P. Giaccone. 2020. NFV Platforms: Taxonomy, Design Choices and Future Challenges. *IEEE Transactions on Network and Service Management* 1, 1 (2020), 1–1.

[43] Wenbing Zhao, Shunkun Yang, and Xiong Luo. 2019. On Consensus in Public Blockchains. In *Proceedings of the 2019 International Conference on Blockchain Technology* (Honolulu, HI, USA) *(ICBCT 2019)*. Association for Computing Machinery, New York, NY, USA, 1–5.

[44] M. Zhaofeng, W. Lingyun, W. Xiaochang, W. Zhen, and Z. Weizhe. 2020. Blockchain-Enabled Decentralized Trust Management and Secure Usage Control of IoT Big Data. *IEEE Internet of Things Journal* 7, 5 (May 2020), 4000–4015.