A Blockchain-Oriented Distributed SDN-aware Architecture for a Scalable Smart City Network

Akram Hakiri[1][0000−0001−7151−5499], Bassem Sallemi[1,2][0000−0001−6869−3518], Fatma Ghandour[3][0000−0003−0757−6232], and Sadok Ben Yahia[2][0000−0001−8939−8948]

[1] University of Carthage, SYSCOM ENIT, ISSAT Mateur, Tunisia
[2] University of Tunis El Manar, Faculty of Sciences, Dept of Computer Sciences, Tunisia
[3] Planning Department, Tunisie Telecom, Les jardins du Lac II, Tunis, 1073, TN
akram.hakiri@enit.utm.tn, sellami.bassem@gmail.com,
fatma.ghandour@tunisietelecom.tn, sadok.benyahia@fst.rnu.tn

Abstract. The widespread growth of the Internet of Things (IoT) systems has motivated the need for trusted IoT transactions, where smart devices can be active participants that share their data with cloud-hosted applications. A compromised IoT device can be prone to vulnerable attacks and overwhelm the whole network with malicious traffic. Recently, Blockchain is being envisioned to enforce security and trustworthiness in diverse IoT environments, including transactive energy auctions, connected vehicles, and trusted healthcare systems. However, Blockchain experience slower latency and higher fees charged to process IoT transactions. It also could be cost ineffective, as it consumes substantially computing power and higher energy to process and validate IoT transactions. Additionally, the lack of IoT-focused consensus protocols makes it is difficult to coordinate distributed IoT systems to detect and destroy large-scale Botnets. To address these challenges, this paper presents the architectural 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. We also evaluate our solution against voting-based and lottery-based consensus algorithms.

Keywords: Blockchain · Distributed Ledger · Internet of Things · SDN/NFV · Ethereum · Security.

1 Introduction

The growing evolution of the Internet of Things (IoT) with tremendous growth in sensors and actuators motivated the need for trusted transactions due the transformation of IoT devices from smart sensing to being active participants that share their data with cloud-hosted applications. IoT systems encounter several security and privacy concerns to prevent unauthorized access to smart devices and to secure trust-less interactions between devices themselves and with service providers on the Internet [2]. A compromised IoT devise could be prone to Distributed Denial-of-Service (DDoS) attacks and 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. Current security models [15] 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 [17], 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 [7], guaranteeing fair payments in smart grids [13], Electric Vehicles [11], monitoring environment quality in smart city [10], and trusted healthcare systems [27]. Despite the promise, Blockchain can be cost ineffective [4] 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, scalability and decentralization is currently at odds as all IoT nodes need to store the entire blockchain transactions, state of account balances, contracts, and storage. As the number of connected IoT devices is forecast to grow to almost 31 billion in the next decade, scalability becomes an issue especially when it comes to process billions of transactions that are expected on these devices [8]. 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. Furthermore, since most IoT devices run over centralized resource-constrained platforms with low memory footprint and computation resources, storing big files inside IoT nodes becomes a concern as more computing infrastructure and financial investment in public blockchains will be needed. Thus, Blockchain was not widely adopted in resource constrained IoT systems.

Software Defined Network (SDN) [3] showed a significant promise in meeting IoT needs by offloading the computation to Fog infrastructures at the network edge. Aligned with SDN, Network Function Virtualization (NFV) [28] enables scaling IoT capabilities by allowing on-demand service orchestration and management. Scaling up IoT resources could be performed through Virtualized Network Functions (VNF), which in turn can be provisioned inside virtual appliances deployed on a generic hardware. In addition to improving the management of network flows in IoT systems, SDN allows better isolation of data flows and improves resiliency to failure for critical data. 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 [26]. That is, by combining Blockchain and SDN/NFV we can optimize the management of IoT flows in response to attacks. We can also enable sophisticated analysis of IoT transactions, improve security, and increase privacy based on global network awareness given by SDN controllers.

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. We also 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.

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 how SDN operates in blockchain-based IoT networks. Section 3 describes the architecture of our solution on empowering IoT systems with SDN and blockchain. Section 5 qualitatively evaluates the performance and the scalability. Section 6 provides concluding remarks describing potential future directions and open research problems in this realm.

2 Related Work

This section draws on the research directions on the convergence of blockchain and the Internet of Things (IoT), and empowering Blockchain-based IoT networks with SDN/NFV.

2.1 Blockchain Integration with IoT

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. [14] 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. [5] 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. [24] 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.

Ellul el al. [6] proposed the Alkyl Virtual Machine, where an Aryl blockchain agent acts as an interface between IoT network and Ethereum blockchain. The AlkylVM continue using the traditional energy intensive Proof-of-Work (PoW) consensus mechanism to validate all transactions on behalf of IoT devices and thereby offloads resource-constrained IoT devices from unnecessary computation. Novo [17] introduced a fully decentralized architecture for arbitrating the communication in permissioned IoT network. Instead of using multiple smart contracts, distributed miners add transaction records into the blockchain, then a single smart contract is used to mange consensuses in the entire network. However, transactions processing incurs long delays when a manager node to grant access to trusted nodes or deny access to particular resources in a device. An unauthorized attacker could gain access to restricted information before a manager could validate and secure transaction's data.

2.2 Blockchain-based IoT networks with SDN/NFV

SDN and Blockchain have been merged to mitigate some issues such as flexibility, efficiency, availability, and security. Salahuddin et al. [21] argue that using SDN in blockchain-based IoT networks could enforce the security of IoT data against malicious traffic analysis. Kataoka [12] 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 [22] virtualized IoT resources by combining Blockchain and SDN to enforce permission-based communication during resource provisioning. Additionally, Steichen et al. [25] proposed ChainGuard framework atop of the Floodlight controller to filter and intercept illegitimate packets and prevent malicious behavior from vulnerable sources. Abbasi et al. [1] introduced the VeidBlock framework to generate verifiable identities based on blockchain over distributed SDN infrastructure.

Likewise, Qiu et al. [19] used Dueling Deep Q-Learning approach to achieve low cost, low latency and low-band intensive network computation and optimize the trust features and the throughput performance. Rodrigues et al. [20] proposed a Blockchain Signaling System (BSS) for whitelisting or blacklisting IP addresses across multi domains SDN network. Similarly, Hari et al. [9] proposed Internet Blockchain for securing Border Gateway routing Protocol (BGP) sessions and DNS transactions. Sharma et al [23] 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. Mendiboure et al. [16] introduced a SDN-based Application Trust Index (ATI) to enable authentication and control in Internet-of-Vehicule (IoV) during resources allocation process. The authors used the Proof-of-Elapsed Time (PoET) consensus algorithm for Hyperledger Sawtooth to prevent high resource utilization and high energy consumption. They used the PoET algorithm by following a fair lottery system to elect (with equal opportunities) SDN controllers for managing the certification process. Participating SDN controllers select random time to win the election and become manager nodes, and the winner controller should indeed completed certain waiting time. Despite the promise, PoET is susceptible to Sybil attacks, where a single attacker can forge multiple node identities to achieve the majority of 51% and take control over the IoT network. Additionally, PoET has the disadvantage to necessary rely on specializing SGX hardware (only available from Intel) which could be a barrier as it runs against the new paradigm of removal of trust in intermediaries.

2.3 Paper Contribution

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. Furthermore, rather than using energy intensive PoW as in [18] or the Sybil-vulnerable POET, we introduced a Proof-of-Authority (PoA) consensus algorithm to select a pre-qualified number of IoT nodes for validating transactions according to strict rules.

Compared to [25], we implemented a Blockchain Decentralized Application (DApp) as a SDN northbound network application to enforce trust on IoT transactions. The DApp can list and report suspicious IoT nodes and validate (or not) unknown blocks. Moreover, compared to permissioned Blockchain approach in [19], we employ state machine replications in a form of VNF appliances to deal with existing cloud-hosted Byzantine nodes, and enable DDoS detection and mitigation-on-demand. That is, in our architecture distributed SDN controllers are aligned with distributed blockchain nodes to avoid unified IoT vulnerability attacks and emphasis geographical distribution of Fog computing nodes and thereby latency reduction.

3 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.

3.1 System Design

Figure 1 illustrates the architectural overview of our proposed solution, which 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 are described in Figure 1. 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.

The latter implements distributed SDN controllers which are responsible for distributing security policies between Blockchain nodes and IoT network infrastructure. Thanks to the decentralized applications (DApps) 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. 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

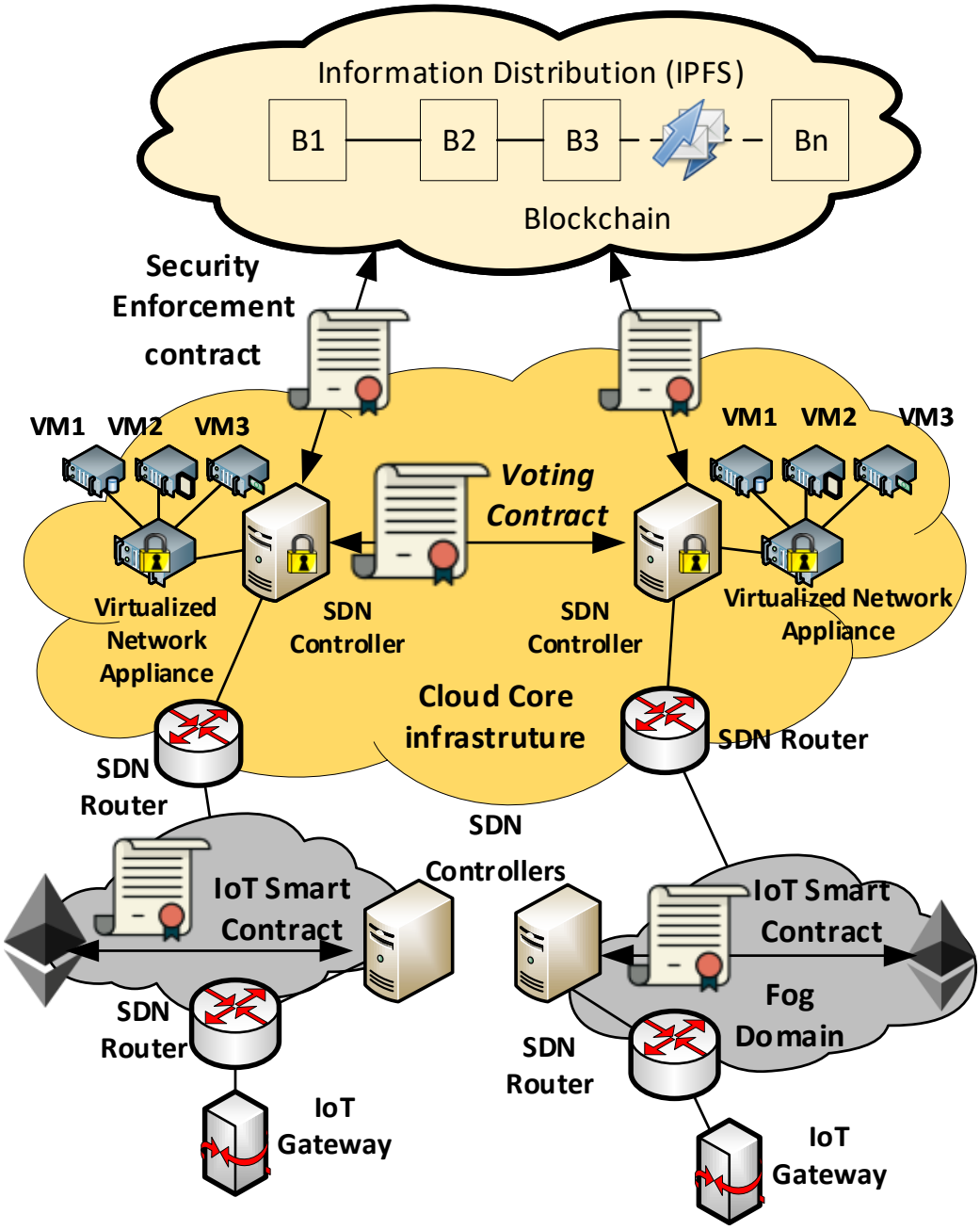

Fig. 1: Overview of the Blockchain-SDN IoT architecture.

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 validating unknown packets. Besides, intrusion detection VNFs (i.e. Firewall as a Service) are deployed inside Kubernetes clusters to take care of malicious flows and enables DDoS detection and mitigation-on-demand. The SDN controller triggers storing decisions to VNF instances to maintain reports about whitelisted and blacklisted IP addresses. The Kubernetes manager can dynamically scale up and down clus-

tered 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, which interface remote sensors and actuators. SDN controllers implement security policies to protect the underlying virtual routers and switches against eventual intrusion. As the SDN routers are directly connected to the blockchain, data are encrypted before being transmitted to remote participants.

3.2 Flow Management

Figure 2 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.

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. Finally, the access control module (will be discussed in Section 3.4) implements the functions for enforcing trust on transactions by listening to mining nodes and reporting suspicious IP addresses.

In the meanwhile, 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 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 will also sign and verify 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 distributed 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) [28]. On the other hand, the SDN controller network abstraction layer can enforce 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 Design

The smart contract is about 400 lines of Solidity code. Listing 1.1 illustrates only a snapshot of it. 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. Data structure "*struct SuspectBehavior*" in Listing 1.1 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

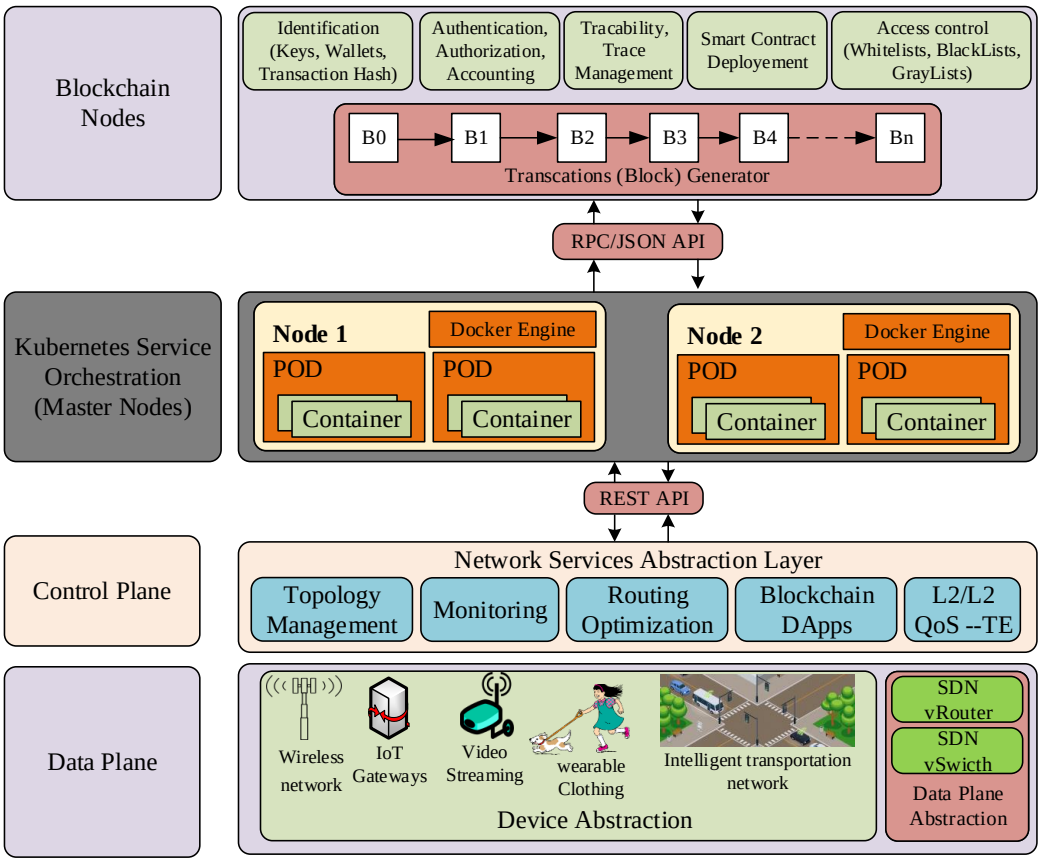

Fig. 2: Blockchain-SDN Applications Framework in Smart City Security.

information contained in the OpenFlow packet headers to create a wide network view including topology state and transactions meta-data.

```
1
2  pragma solidity >=0.4.16 <0.7.0;
3  contract SDIoTDefender
4  {
5  //
6  struct Report {
7    uint expirationdate;
8    IPAddress sourceIp;
9    IPAddress destinationIp;
10 }
11
12 struct SuspectBehavior {
13   address subject; //subject who performed the misbehavior;
14   address object; //
15   string res; //
16   string action; // (e.g., "read", "write", "execute") of the
         misbehavior
17   string misbehavior; //misbehavior
18   uint time; //time of the Misbehavior occured
19   uint penalty; //penalty (number of minitues blocked);
```

```
  string suspectIP;
  string suspectMAC;
}

struct IoT_Gateway {
  string          Gateway_IP;
  string          Gateway_MAC;
  string          mask;
  string[]        Gateway_Apps;
  string          deliveryMode;//anycast, unicast, multicast
  bytes32         _hash;
}

function deleteIoT_Gateway() ownerOnly returns (bool success)
{
  delete IoT_Gateway[key];
}
}
```

Listing 1.1: Smart contract for detecting malicious IoT devices

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. The *function deleteIoT_Gateway() ownerOnly returns (bool success)* in Listing 1.1 is called when overwhelmed node should be removed the whole network. Whitelisted nodes are users or devices whose behavior is normal, and they could continue delivering their content as they belong to the blockchain.

3.4 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.

Second, by relying on a group of authority nodes that are pre-approved validators to verify transactions and build blocks, we ensure that nodes wishing to become authorities and validators should 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. Figure 3 depicts the block creation and validation using POA mechanism. The time is divided into steps, each of which has an authority elected as mining leader. In this example, there are 3 authorities with id 1, 2 and 3. The leader of the first step is node 1, then 2, and 3. The leader of a step s is the authority identified by the id $l = SmodN$; where S is the number of steps, and N is the number of authority nodes.

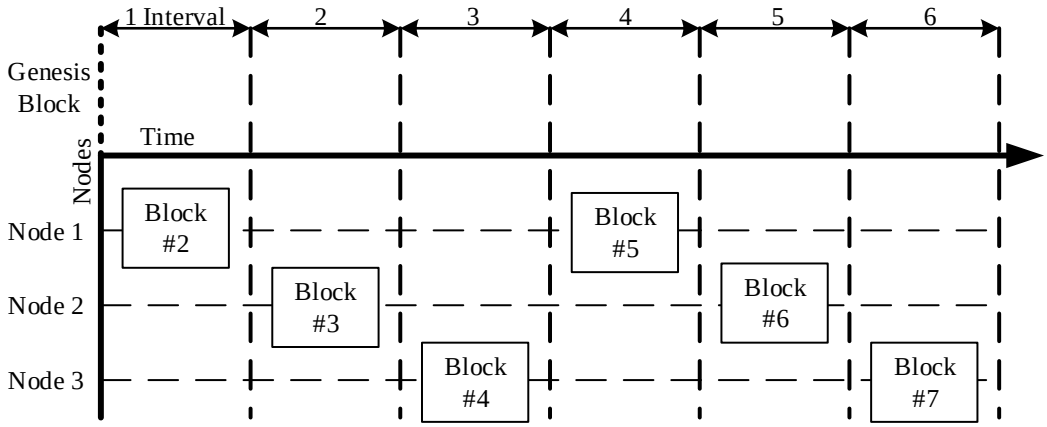

Fig. 3: Block creation in PoA Consensus Algorithm

Third, validating IoT transactions relies on a mining rotation schema to fairly distribute the responsibility of block creation among authorities. Authorities are assumed to be asynchronous and all of them are allowed to propose blocks in each computation step. The current step is calculated based on a formula that combines the block number and the number of authorities. To prevent an authority from monopolizing the network resources (e.g. 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 Use case

4.1 Blockchain-SDN enabled Internet of Vehicles

Figure 4 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. IoV is envisaged to improve the safety of vehicles and are foreseen to use 5G mobile networks to push their performance and capabilities to their extremes.

As shown in Figure 4, 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.

Additionally, Blockchain distributed ledgers, coupled with consensus mechanisms, can guarantee the preservation of trustworthy data. Figure 4 shows two consecutive steps and how current leader and authorities allowed proposing blocks change. There are $N = 8$ authorities (i.e. RSU1 to

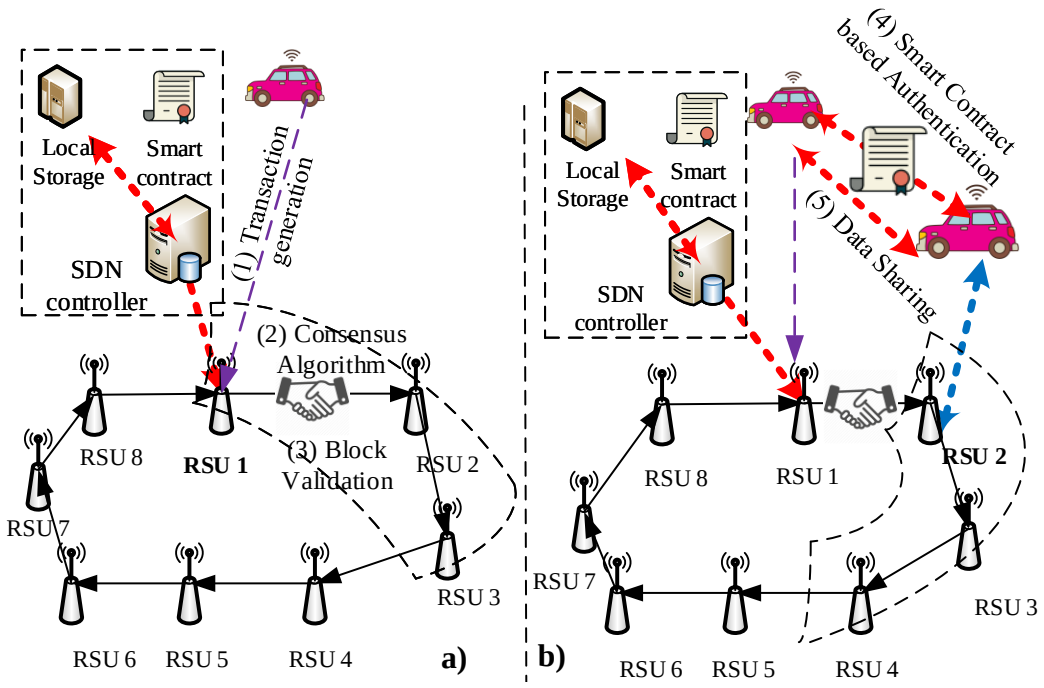

Fig. 4: Secure message dissemination in SDN-enabled VANET

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 4). In the first time step in Figure 4(a), RSU1 is the leader while RSU2 and RSU3 are allowed to propose blocks. Next, in next time step as depicted in Figure 4(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.

Besides, as VANETs becomes more open, connected vehicles will encounter several security and privacy concerns. Since VANETs do not rely on a third-party security server, malicious nodes from the network or compromised OnBoard Units (OBU) can cause security vulnerabilities, such as jamming, eavesdropping, and tampering, and overwhelm the network with malicious traffic. In this context, Blockchain distributed ledgers, coupled with consensus mechanisms, can guarantee the preservation of trustworthy data.

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. We can rethink of using consensus algorithm like the practical Byzantine Fault Tolerance (PBFT), where

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, Blockchains can handle blocks concurrently with SDN to ensure and efficient, agile and flexible network management while preventing malicious activities.

4.2 Improving Security between IoT Gateways

Blockchain can improve SDN-enabled IoT gateways in a dynamic fashion. First, adopting distributed ledgers can enforce the trust in IoT networks by enabling security mechanisms between IoT gateways and IoT services distributed among Fog nodes at the network edge. Figure 5 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.

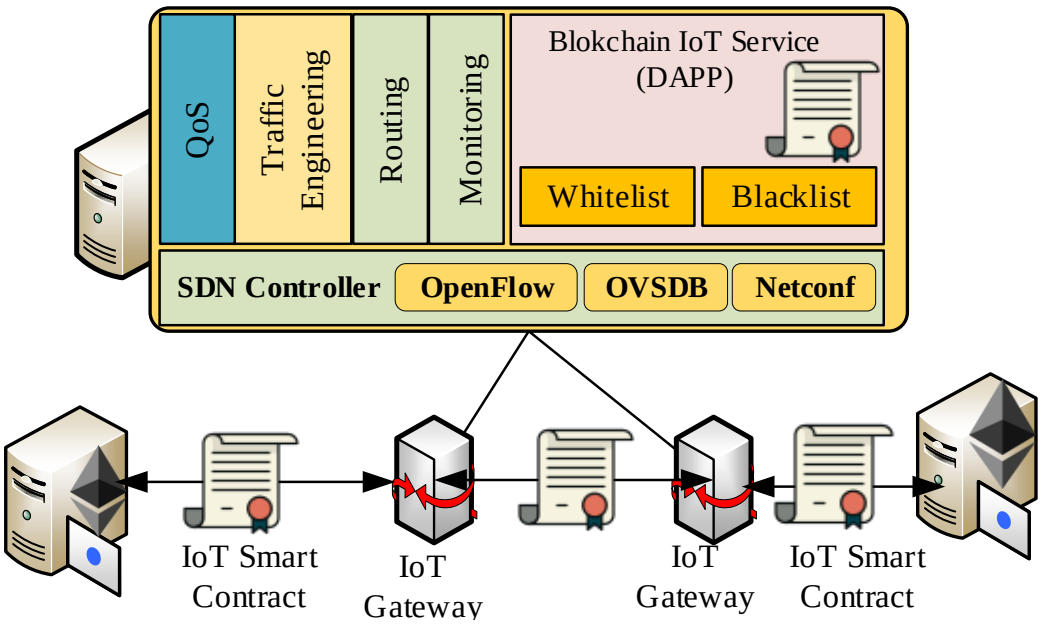

Fig. 5: Ensuring Security and Interoperability between IoT Gateways.

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.

5 Performance Evaluation

In this Section, we discuss performance analysis based on the the consensus algorithm in term of message exchanging. Specifically, we consider two key properties, i.e. the performance and scalability, to determine the effectiveness and fitness of the consensus algorithm. The performance refers to transaction latency and throughput, i.e. a transaction is not considered valid until it is committed out to the blockchain. The performance is bounded by a combination of block interval (i.e. time between publishing subsequent blocks) and block size. These parameters establish an upper bound on transaction throughput.

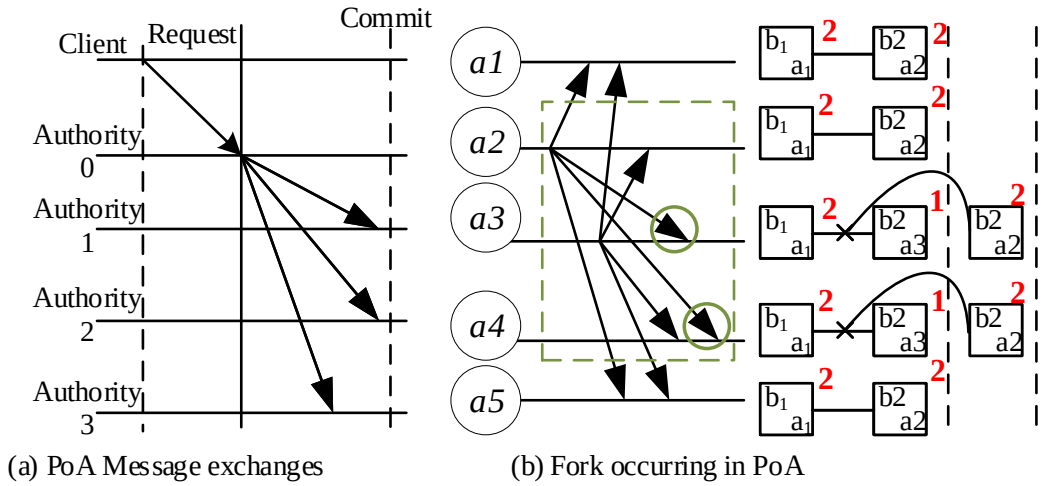

Fig. 6: Latency during Message Exchange in PoA

Figure 6a) shows the message exchange at each step, where each leader node broadcasts a block to all other authorities, which in turn commit it to the blockchain. There is a particular case depicted in Figure 6b), where a leader node a_2 broadcasts a new block b_1 and another no-leader authority node a_3 broadcasts also another block b_2. The first new created block b_1 precedes the block b_2 and reaches nodes a_1 and a_5 before b_2. However, b_2 reaches nodes a_3 and a_4 before they receive the first created block b_1. As depicted on the right side of Figure 6b), a fork operation is performed by each authority node to detect every received new block, and reference it as a previously reacted block not at disposal of the authority.

Compared to voting-based consensus (e.g. PBFT and PoW) as shown in Figure 7 and lottery-based style of consensus algorithms (e.g PoET) as shown in Figure 8, PoA requires less message exchanges and hence performs better transaction's throughput. As illustrated in Figure 6, in PoA each block proposal requires one round for leader to send the proposed block to all other authorities. The block is committed at once, hence the latency in terms of message rounds is 1. Compared to other consensus algorithms, as depicted in Figure 7, PBFT requires three message rounds to commit a block, while PoET needs more than three message rounds as illustrated in Figure 8 to validate a block. Hence, PoA performs better transaction's throughput.

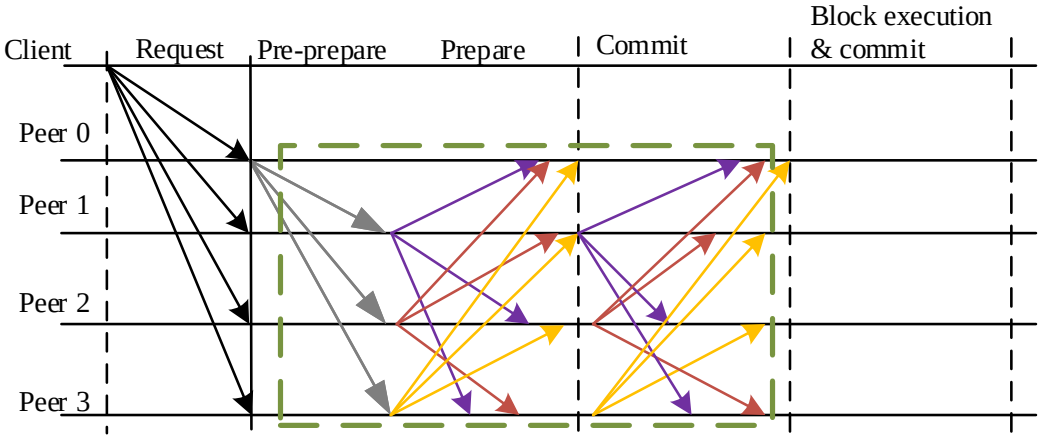

Fig. 7: Latency during Message Exchange in voting-based PBFT

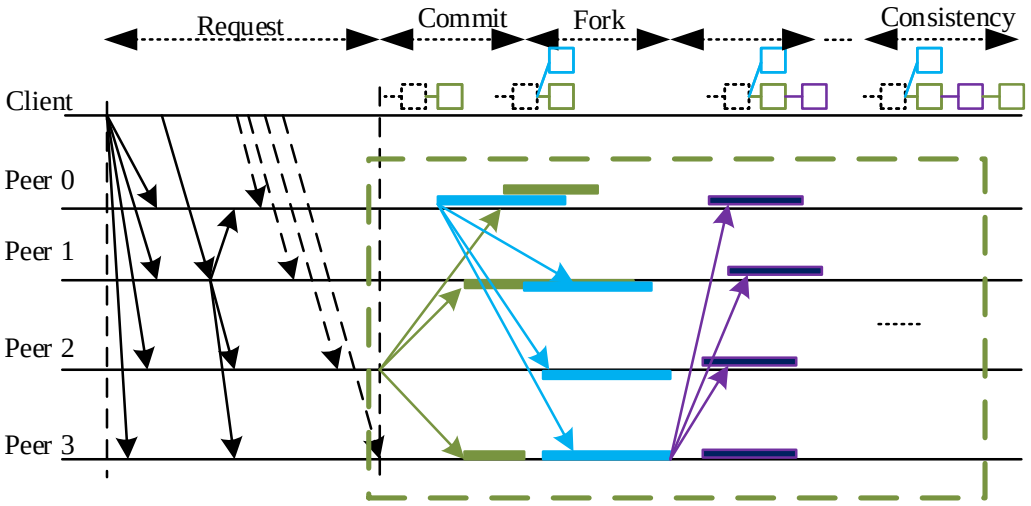

Fig. 8: Latency for Message Exchange in lottery-based PoET

Similarly, in terms of latency of a transaction t, i.e the time between the submission of a transaction t by a participating node and its commit of a block including t by a leader node, PoA performs better latency compared to other consensus algorithms. PoA is communication oriented consensus mechanism, that does not involve relevant computation and it assumes bounded latency expressed in terms of time steps, rather than CPU-bound (e.g. PoW) or digital asset bound (e.g. PoS). PoW algorithm performs and average latency is 10 minutes in Bitcoin blockchain and average latency of 12 seconds in Ethereum blockchain.

The scalability refers to the ability of the blockchain network to improve or degrade the workload as the number of nodes increases or decreases. In PoA consensus, in order to keep the network more efficient and trusted, the number of validators nodes should be kept small, i.e. 5 or 7 for small scale network and up to 25 validators for a large-scale one. Thus, the PoA approach helps in reducing the necessary power energy to maintain the network and reduce the dependency of using high-performance hardware to validate blocks. Finally, consistency requires realistic synchronous network model where all nodes are synchronized. In PoW network, consistency does not depend on the network size. In contrast to other voting-based and lottery-based styles of consensus algo-

rithms, consistency means that more computing power to solve a mathematical puzzle are available for new nodes attempting to publish blocks. Compared to PBFT algorithms, the design of PoA sacrifices consistency (forking can happen by the GHOST protocol) for better availability (faster block committal).

6 Conclusion

In this paper, we introduced a novel architecture that brings network softwarization and virtualzation to the blockchain nodes, to enable dynamic and on-demand service orchestration and improve security, and privacy-preservation in order to meet various requirements of scalability, performance, seamless distribution, and transparency. Besides, we proposed a novel consensus algorithm based on the proof of authority that delivers fast transactions, by increasing the speed at which the authorities validate transactions. Thus, malicious transactions can be detected, signaled, and removed from the network. A decentralized application (DApp) detects malicious IoT nodes and trigger remote miner to invalidated IoT transactions by blacklisting their originating IP addresses. Our solution can be used in various scenarios and use cases such The Internet of Vehicles (IoV), securing IoT gateways, and audit traceability, thereby reinventing the Blockchain.

Since Blockchain is a nascent technology, we argue that processing billions of transactions in few seconds will be a challenging issue for scenarios like Internet of Vehicles and smart cities. We believe that combining Blockchain Big Data Analytics, and Deep Reinforcement Learning could change the way how smart city data can be consumed, which means data will be more structured, abundant and complete, making it more suitable for analytics. Our future research directions will focus on how these technologies can avoid data fragmentation, how to involve all these parties in IoT transactions to provide access to the same data and share the same and complete overview of these transactions from their creation to their finish, without needing access to multiple siloed systems, while at the same time each involved party can manage and control its own data without any third party authority or centralized repository.

Acknowledgments

This work was partially funded by the Tunisian Ministry of Higher Education and Scientific Research (MESR) 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 MESR.

References

1. Abbasi, A.G., Khan, Z.: Veidblock: Verifiable Identity Using Blockchain And Ledger In A Software Defined Network. In: Companion Proceedings of the10th International Conference on Utility and Cloud Computing. pp. 173–179. UCC '17 Companion (2017)
2. Ali, M.S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., Rehmani, M.H.: Applications of blockchains in the internet of things: A comprehensive survey. IEEE Communications Surveys Tutorials pp. 1–1 (2018)
3. Bera, S., Misra, S., Vasilakos, A.V.: Software-defined networking for internet of things: A survey. IEEE Internet of Things Journal **4**(6), 1994–2008 (Dec 2017)
4. Buccafurri, F., Lax, G., Nicolazzo, S., Nocera, A.: Overcoming Limits Of Blockchain For IoT Applications. In: Proceedings of the 12th International Conference on Availability, Reliability and Security. pp. 26:1–26:6. ARES '17 (2017)
5. Chen, J.: 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)

6. Ellul, J., Pace, G.J.: Alkylvm: A Virtual Machine For Smart Contract Blockchain Connected Internet Of Things. In: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). pp. 1–4 (Feb 2018)
7. Hahn, A., Singh, R., Liu, C.C., Chen, S.: Smart Contract-based Campus Demonstration Of Decentralized Transactive Energy Auctions. In: 2017 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT). pp. 1–5 (Apr 2017)
8. Han, R., Gramoli, V., Xu, X.: Evaluating Blockchains For Iot. In: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). pp. 1–5 (Feb 2018)
9. Hari, A., Lakshman, T.V.: The internet blockchain: A distributed, tamper-resistant transaction framework for the internet. In: Proceedings of the 15th ACM Workshop on Hot Topics in Networks. pp. 204–210. HotNets '16, Atlanta, GA, USA (2016)
10. Ibba, S., Pinna, A., Seu, M., Pani, F.E.: Citysense: Blockchain-oriented Smart Cities. In: Proceedings of the XP2017 Scientific Workshops. pp. 1–5. XP '17 (2017)
11. Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., Hossain, E.: Enabling Localized Peer-to-peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains. IEEE Transactions on Industrial Informatics **13**(6), 3154–3164 (Dec 2017)
12. Kataoka, K., Gangwar, S., Podili, P.: Trust List: Internet-wide And Distributed Iot Traffic Management Using Blockchain And Sdn. In: IEEE 4th World Forum on Internet of Things (WF-IoT). pp. 296–301 (2018)
13. Lundqvist, T., de Blanche, A., Andersson, H.R.H.: Thing-to-thing Electricity Micro Payments Using Blockchain Technology. In: 2017 Global Internet of Things Summit (GIoTS). pp. 1–6 (Jun 2017)
14. Machado, C., Fröhlich, A.A.M.: Iot data integrity verification for cyber-physical systems using blockchain. In: 2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC). pp. 83–90 (May 2018)
15. Massonet, P., Deru, L., Achour, A., Dupont, S., Levin, A., Villari, M.: End-to-end security architecture for federated cloud and iot networks. In: 2017 IEEE International Conference on Smart Computing (SMARTCOMP). pp. 1–6 (2017)
16. Mendiboure, L., Chalouf, M.A., Krief, F.: Towards a blockchain-based sd-iov for applications authentication and trust management. In: Internet of Vehicles. Technologies and Services Towards Smart City. pp. 265–277. Springer International Publishing (2018)
17. Novo, O.: Blockchain Meets IoT: An Architecture For Scalable Access Management In IoT. IEEE Internet of Things Journal **5**(2), 1184–1195 (Apr 2018)
18. Pradip Kumar Sharma and Jong Hyuk Park: Blockchain based hybrid network architecture for the smart city. Future Generation Computer Systems **86**, 650–655 (2018)
19. Qiu, C., Yu, F.R., Yao, H., Jiang, C., Xu, F., Zhao, C.: Blockchain-based software-defined industrial internet of things: A dueling deep q-learning approach. IEEE Internet of Things Journal pp. 1–1 (2018)
20. Rodrigues, B.B., Bocek, T., Lareida, A., Hausheer, D., Rafati, S., Stiller, B.: A Blockchain-based Architecture For Collaborative Ddos Mitigation With Smart Contracts. In: AIMS (2017)
21. Salahuddin, M.A., Al-Fuqaha, A., Guizani, M., Shuaib, K., Sallabi, F.: Softwarization Of Internet Of Things Infrastructure For Secure And Smart Healthcare. Computer **50**(7), 74–79 (2017)
22. Samaniego, M., Deters, R.: Using Blockchain To Push Software-defined Iot Components Onto Edge Hosts. In: Proceedings of the International Conference on Big Data and Advanced Wireless Technologies. pp. 58:1–58:9. BDAW '16 (2016)
23. Sharma, P.K., Singh, S., Jeong, Y.S., Park, J.H.: Distblocknet: A Distributed Blockchains-based Secure Sdn Architecture For Iot Networks. IEEE Communications Magazine **55**(9), 78–85 (2017)
24. Singh, M., Kim, S.: Trust Bit: Reward-based Intelligent Vehicle Commination Using Blockchain Paper. In: 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). pp. 62–67 (Feb 2018)
25. Steichen, M., Hommes, S., State, R.: Chainguard : A firewall for blockchain applications using sdn with openflow. In: 2017 Principles, Systems and Applications of IP Telecommunications (IPTComm). pp. 1–8 (Sep 2017)
26. Zhang, C., Hu, G., Chen, G., Sangaiah, A.K., Zhang, P., Yan, X., Jiang, W.: Towards a sdn-based integrated architecture for mitigating ip spoofing attack. IEEE Access **6**, 64–77 (2018)
27. Zhang, P., Walker, M.A., White, J., Schmidt, D.C., Lenz, G.: Metrics For Assessing Blockchain-based Healthcare Decentralized Apps. In: 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom). pp. 1–4 (Oct 2017)
28. Zhang, T.: Nfv platform design: A survey. arXiv: Networking and Internet Architecture (2020)