Chapter 10

A Software Defined Blockchain-based Architecture for Scalable and Tamper-Resistant IoT-enabled Smart Cities

Akram Hakiri [1] *and Aniruddha Gokhale* [2]

The increasing reliance on smart city operations has motivated the need for trusted Internet of Things (IoT) transactions due to the transformation of IoT devices from smart sensing to being active participants that share their data with fog/edge computing services. Existing security models such as centralized cloud-hosted security infrastructures cannot address IoT's security and privacy concerns because of lack of resources and flexibility, which makes IoT devices susceptible to elevation of privileges, and distributed denial of service (DDoS). An attractive and more realistic alternative to address these challenges is the Blockchain, which uses a decentralized infrastructure for fighting DDoS attacks and eliminate the risk of a single point of failure. Blockchain serves as the backbone for diverse IoT applications, such as transactive energy auctions, self-driving cars, and trusted healthcare systems. Additionally, Software Defined Networking (SDN) allows the development of customized security policies and services in a dynamic, software-based fashion. Complementing SDN, Network Function Virtualization (NFV) enables scaling IoT capabilities by allowing on-demand service orchestration and management. By combining Blockchain and SDN/NFV we can optimize the flow management in response to attacks by enabling sophisticated analysis of IoT transactions and improving security and privacy based on global network awareness given by centralized SDN controllers. To that end, in this chapter, we introduce an SDN architecture for enforcing security of IoT transaction in the blockchain. We also introduce a novel Proof-of-Authority (PoA) consensus algorithm to report suspected IoT smart devices and report them under smart contract. We then introduce a distributed intrusion detection system as a manifestation of virtualized network functions (VNFs) in the fog computing environment , i.e. a Firewall-as-a-Service in SDN network, which takes care of malicious flows and enables DDoS detection and mitigation on-demand.

[1]University of Carthage, SYSCOM ENIT, ISSAT Mateur, Tunisia.
[2]Dept of EECS, Vanderbilt University, Nashville, TN, USA.

10.1 Introduction

Smart cities represent a rich and dynamic environment where multiple Internet of Things (IoT) sensors and actuators interconnect to each other to communicate and share their data. These IoT devices have motivated the need for trusted transactions due their transformation from smart sensing to being active participants that record and store their data in the cloud [1]. An additional trend reveals that smart city IoT devices should provide (i) on-demand basis resource allocation to support adaptive horizontal and vertical scaling of the network resources, (ii) flexible infrastructure virtualization that exploits in-network programmability capabilities to operate inside a Software Defined Network (SDN)-enabled virtualization platform and (iii) decentralized security appliances for addressing distributed denial of service (DDoS) attacks thereby paving the way to construct trustworthy smart city networks, and eliminating the risk of a single point of failure.

Software Defined Networking (SDN) shows significant promise in meeting smart cities needs by offloading the computation to geographically distributed Fog Computing infrastructures [2]. SDN enables developing and deploying flexible and programmable smart city Fog network infrastructures, and allows developing customized network control policies and services in a dynamic and software-based fashion. In addition to improving the management of the network flows in smart cities communication system, SDN allows better isolation of the data flows and improves resiliency to failure/attacks for critical data, by creating logical isolated network partitions overlaid on top of a smart cities physical network infrastructure. Complementing SDN is Network Function Virtualization (NFV), which enables scaling of the IoT capabilities by allowing on-demand service orchestration and management. NFV allows scaling up IoT resources through Virtualized Network Functions (VNF) provisioned in virtual appliances that are deployed on a generic and low-cost hardware.

Although SDN has been envisioned to optimize the flow management in response to attacks by enabling sophisticated analysis of IoT transactions, SDN itself can be vulnerable to several types of attacks. The SDN dataplane can be compromised by manipulating flow rules such that the flows can be diverted to a black hole route. Centralized SDN controllers suffer several security breaches because security is minimally specified in SDN specification, i.e. it does not specify any certificate format to ensure data integrity and protect devices against malicious traffic analysis, information disclosure, tampering, elevation of privileges, and denial of service. A malicious controller can create false flow table entries towards the neighboring SDN switches to gain complete control of the network. As the controller broadcasts OpenFlow discovery messages to all its connected devices, forged flow rules and flooding attacks can be propagated easily since the SDN routers lack sufficient intelligence to identify genuine flow rules from malicious ones. Thus, exploiting buffer overflow will allow attackers in controlling or crashing the forwarding process or modifying its internal variables. Furthermore, any unauthorized access to SDN networks will cause unauthorized modification of network control policies, configuration files and network topology, thereby increasing the impact of loss of integrity, service disrup-

tion and unavailability. The loss of trust in the centralized SDN wreaks havoc on their operation.

In summary, shifting towards SDN without taking all precaution into account opens up new attack vectors for hackers as SDN devices are API-based, i.e., the network topology is prone to attacks. The Southbound and Northbound APIs can be spoofed and defective or virulent SDN applications can be manipulated by unauthorized entities [2]. Therefore, SDN security involves sophisticated encryption mechanisms to enforce confidentiality, prevent hackers, recover packets from failure and ensure that malicious entities do not tamper with the controller configuration. Integrity is also mandatory for protecting network policies, configurations, and flow tables from intentional or unintentional tampering. Thus, any IoT SDN security mechanism should ensure that rogue devices are detected in a timely manner, vulnerabilities are rejected and the system has recovered from any potential fault.

A promising approach to address this problem is to leverage the blockchain technology, such as Bitcoin [3] and Ethereum [4] platforms, which has been increasing adopted in many financial [5] and government [6] sectors. Blockchain has moved data distribution from non-trusted transactions towards decentralized, cryptographically secure, and immutable ecosystem, without any centralized authority. Blockchain has also been the backbone for deploying decentralized ledgers in diverse IoT applications. For example, the integration of IoT with blockchains in smart grids enables scheduling energy resources, where machines can guarantee fair payments automatically [7] [8] [9]. Kang et al. [10] used blockchain to localize Peer-to-Peer electricity trading among Hybrid Electric Vehicles. Likewise, Ibba et al. [11] used a Blockchain to monitor environment quality in smart city. Biswas et al. [12] proposed a security framework that integrates the blockchain with smart devices to provide a secure communication platform in a smart city. Similarly, Lu et al [13] investigated IoT-blockchain to ensure traceability processes in supply chain management. Bocek et al. [14] leverage blockchain to assert data immutability and public accessibility of temperature records in the pharmaceutical supply-chain.

Despite the promise, Blockchain can be cost ineffective, as it consumes substantially computing power and higher energy required by miners [15] for creating trusted transactions [16]. 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. Scalability becomes an issue especially when it comes to processing billions of transactions expected to grow to almost 31 billion connected IoT devices in the next decade. 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 has not been widely adopted in resource-constrained IoT systems. Hence, it becomes hard to judge how well the Blockchain technology is able to meet IoT needs and requirements.

We surmise that by combining Blockchain and SDN/NFV, we can optimize the flow management in response to attacks by enabling sophisticated analysis of IoT transactions and improving security and privacy based on global network awareness

given by centralized SDN controllers [2]. We claim that we can enhance the scalability, flexibility and agility of IoT networks and enforce trust and resiliency in smart city infrastructure through 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. We further claim that our blockchain-enabled architecture enables new types of trustless interactions for empowering IoT communications and brings more transparency and performance by reducing deep packet inspection of SDN-enabled IoT traffic. That is, while individual IoT devices are not powerful enough to meet the IoT security needs, SDN/NFV can enforce their coordination in large-scale Botnets by dynamically provisioning Blockchain virtual functions for firewalling and mitigating malicious traffic, thereby allowing them to be a prepared for threats that can otherwise overwhelm even well-prepared defenses of critical services.

To that end, in this chapter we first provide a background on blockchain, and survey significant litterateur on how it operates in IoT networks, and discuss how SDN can be involved in Blockchain network. We then introduce our architecture on empowering smart city networks for interconnecting its various IoT systems with SDN and Blockchain. We propose a solution for enforcing security of Blockchain IoT transactions in form of virtualized network functions (VNFs) to take care of malicious flow and enable DDoS detection and mitigation on demand. We also introduce a novel Proof-of-Authority (PoA) consensus algorithm that helps in validating IoT transactions. We then present three use cases, one each from Internet of Vehicles, Energy Internet, and IoT Gateways, which will benefit from the proposed architecture. Finally, we discuss open challenging issues that should be addressed in the near future to support other technical requirements for improving advanced trusted smart cities networks and highlight potential future directions and open research problems in this realm.

10.2 Background and Literature Review

This section draws on three bodies of research: background on Blockchain technology, the convergence of blockchain and the Internet of Things (IoT), and securing SDN networks using Blockchain technology.

10.2.1 Overview of Blockchain Technology

Blockchain is the technology underlying Bitcoin cryptocurrency and is increasingly becoming a choice for decentralized resource management and transactions look up. Beyond its cryptocurrency use, Blockchain is a distributed and a decentralized ledger which stores records and transactions carried out between users since their setup, where each member can check the validity of the chain by itself. A distributed ledger is a shared pseudo-anonymous database fully replicated at multiple nodes or sites without any centralized third party authority. Information exchanged between nodes or sites are maintained in a doubly linked list of ordered blocks, where each block records one or multiple transactions between two parties efficiently and in a verifiable

and permanent way. Blocks use cryptographic validation to link together, i.e. each block references and identifies the previous block using a hashing function to form an unbroken chain. Once recorded, chained blocks are designed to be resistant to modification so that their data cannot be altered retroactively.

The chained data are synchronized globally so that any changes in the previous blocks requires changes in all the latter blocks. That is, while every one can see the data tagged with the sender address in the blockchain, no one can modify it, except by a node that can prove they are the owner via a private key. Multiple computer nodes compete to validate the newest block entries before the other nodes to gain a reward for doing so. The block validation system is designed to be immutable. That is to say, all transactions old and new are preserved forever with no ability to delete. Anyone on the network can browse via a designated website and see the ledger. This provides a way for all participants to have an up-to-date ledger that reflects the most recent transactions or changes. In this way, Blockchain establishes trust, which as we shall see helps facilitate transactions and brings many cost-saving efficiencies to all types of transactional interactions.

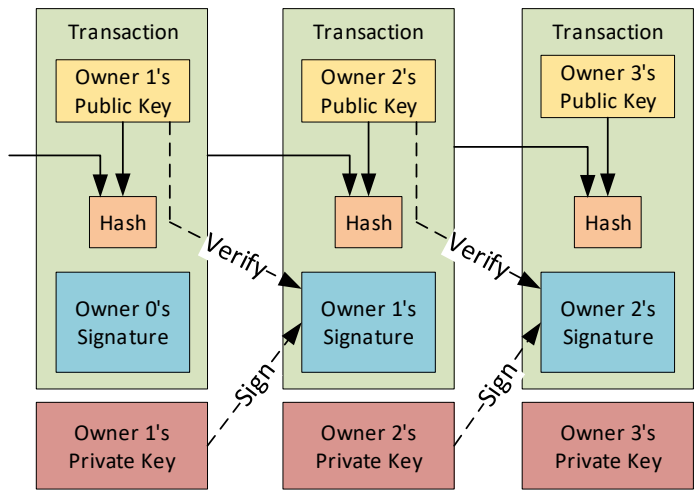


Figure 10.1: Structure of Blockchain

Figure 10.1 illustrates a typical Blockchain structure that consists of transaction data and hash values. Transaction data are used to store user records, while hash values store coded and secure information generated from the previous block. The first block which does not have a hash value to the previous block is called the genesis block. Furthermore, the blockchain is distributed because a complete copy lives on as many nodes as there are in the system. The blockchain is immutable because none of the transactions can be changed. The blockchain is pseudo-anonymous because the identity of those involved in the transaction is represented by an address key in the form of a random, i.e. hash string. Updating the blocks needs the agreements of most distributed nodes that use a specific decision protocol called the consensus algorithm,

such that if 51 percent of the nodes agree then trust of the chain is guaranteed. That is, the blockchain is validated by the miners who are compensated for building the next secure block.

Blockchain is secure by design and an example of a distributed computing system with high Byzantine fault tolerance. Decentralized consensus can therefore be achieved with a public blockchain. Like cloud computing implementations, different types or categories of blockchain have emerged. Analogous to the cloud, there are public blockchains that everyone can access and update, while private ones for just a limited group within an organization to be able to access and update, and a third kind, which is a consortium of blockchains that are used in collaboration with others.

Through the use of peer-to-peer networking approach, blockchain nodes can be managed autonomously. Their ledgers can be programmed to trigger transactions automatically and achieve large-scale systematic cooperation in an entirely distributed and decentralized manner. Blockchain transactions store users records, historical, information, and control data. Once executed locally at each participant node connected to the blockchain, these data are synchronized using a set of computer programs or protocols that govern the interaction between two or more nodes. Such protocols are called smart contracts and have the capacity to perform automation, reporting, and monitoring encrypted transaction. Smart contracts take diverse forms depending on the use case where they will be deployed [17] such as financial, notary, Game, wallet, library, etc. Smart contracts can also pave the way towards new business models and facilitate resource management of diverse IoT services [1]. As blockchain ledgers are still emerging, smart contracts take diverse forms.

The IoT-blockchain combination could realize trusted and secure communication model between non-trusted things. This can be considered and implemented as a ubiquitous IoT governance tool, capable of managing IoT interactions on a large scale and dismissing traditional centralized entities.

10.2.2 Convergence of Blockchain and IoT

Blockchain has opened up a wide range of possibilities for smart city 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 a smart city. For example, Cha et al. [18] developed a smart contract to enforce user's privacy by enabling a digital signature to ensure their authentication when connected to IoT gateway. Singh et al. [19] combined automotive and blockchain by introducing a unique crypto ID called Trust Bit (TB) for decentralized intelligent vehicle (IV) communication. The authors created a cloud-hosted reward system to store Trust bit details, reward IVs by distributing some TBs after successful inter-IV communication. Gupta et al. [20] proposed a security model for IoT atop a blockchain protocol layer and a blockchain application layer to ensure network security. The former encompasses the consensus and mining algorithms, while the latter holds the IoT security constructs.

Likewise, Yin et al. [21] proposed a blockchain-based architecture for Machine-to-Machine (M2M) communication in both public and private areas. They highlighted the efficiency of blockchain technology in expanding safety and security

M2M communication. All requests are embedded in a query packet that encompasses a digital signature for enforcing the security. The blockchain block embeds both the header and data information. The header contains hash value that relates to the next block, while the data contains information to identify the sending and receiving devices, the data payload, etc. Hahn et al. [22] introduces a smart contract that implements a transactive energy auction that operates without the need for a trusted entity's oversight.

Chen [23] introduced the Flowchain distributed ledger system over peer-to-peer IoT systems. Flowchain provides a secure, real-time data exchange model to enforce IoT privacy. Moreover, Chen introduced the Devify framework [24] to build an interoperable trusted IoT networks in a decentralized fashion. The framework adopts the Web of Things ontology standards-based model to simplify the development of cloud-hosted IoT applications, as well as mobile and resource-constrained IoT systems.

Daza et al. [25] introduced a discovery service called CONNECT to find things and services in IoT networks. CONNECT uses the hierarchical layered approach of blockchain to provide a seamless naming and discovery service for IoT. Conoscenti et al. [26] reviewed the integrity, anonymity and adaptability of blockchain to different IoT use cases and proposed a blockchain model to foster a decentralized and private-by-design IoT [27]. Xiong et al. [28] highlighted how blockchain could be used in mobile edge IoT architecture. Kshetri et al. [29] claim that blockchain could strengthen the IoT security by ensuring authentication, and access control management.

10.2.3 Blockchain Security over SDN

Kataoka [30] integrated SDN and blockchain to automate the process of doubting, verification and trusting IoT services to prevent them from attacks. A SDN controller receives information regarding trustable services and devices, and transforms them into flow rules that could be deployed to SDN switches at the network edge. Samaniego et al. [31] [32] considered using SDN to virtualize the IoT resources at the network edge in combination with blockchain to enforce permission-based communication during IoT resource provisioning. They evaluated their architecture inside Intel Edition Arduino platform. The approach considerably reduced the network latency and the throughput when blockchain is applied at the network edge. They also proved that it is possible to implement SDN-enabled blockchain inside resource-constrained devices, which could open the discussion on moving the computation to the network edge.

Rodrigues et al. [33] proposed DDoS mitigation across multiple network domains using blockchain Signaling System (BSS) [34]. The approach introduces smart contact's collaborative mechanism for Whitelisting or blacklisting IP addresses across multi domains SDN network. A SDN controller verifies the trusted IP lists to monitor and enforce the negotiation of intra-domain security policies. The authors introduced a SDN application that encompasses local SDN policies for retrieving and reporting blacklisted IP addresses as well as programming the OpenFlow flow table entries in SDN switches [35]. Abbasi et al. [36] introduced the VeidBlock

security framework to generate verifiable identities based on blockchain over distributed SDN infrastructure. Moreover, NFV is used to virtualize security functions such as firewall and load balancer and instantiate a LedgerVeidBlock. Subsequently, signed and timestamped ledger blocks are sent to the controller, which verifies and checks the freshness of the received requests. Once the verification is validated by the NFV orchestrator, i.e. the firewall, the controller extracts anonymous identities from VeidBlock and sends it to OpenFlow to establish the communication.

Sharma et al. [37] proposed a distributed cloud architecture based on blockchain that uses SDN controller as a fog node to program flow rules and provide secure and on-demand access to IoT systems at the network edge. They also proposed DistBlockNet [38] as a distributed secure, peer-to-peer SDN architecture for IoT using blockchain where IoT members could interact seamlessly without a trusted intermediary. DistBlockNet uses blockchain to update OpenFlow rules, security and verify OpenFlow table and flow rule tables, and download and install updated flow rules to the forwarding SDN/IoT devices.

Similarly, Salahuddin et al. [39] advocates that blockchain guarantee the security of IoT data in many smart healthcare applications and services by protecting patient information and other confidential medical records against malicious traffic analysis. Hari et al. [40] 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.

Steichen et al. [41] proposed ChainGuard which is a firewall SDN application atop the Floodlight controller to enforce blockchain security. ChainGuard filters the network traffic and intercepts illegitimate packets to mitigate flooding attacks and prevent malicious behavior from vulnerable sources. ChainGuard specifies three types of list: graylist are nodes that are not known to the SDN controller and could correspond either to whitelist which are legitimate node that can join that blockchain network, or blacklist which are illegitimate nodes prohibited from connecting to the blockchain. Additionally, Tselios et al. [2] argue that blockchain could improve security and privacy in SDN-enabled IoT networks by using distributed ledger transactions.

10.3 Architectural Design

This section delves into the details of our distributed SDN-enabled Blockchain architecture in IoT Fog network. It implements secure identification and authentication approach to support scalable, dynamic, and flexible IoT resource management. A logically distributed set of SDN controllers aligned with distributed blockchain and consensus algorithms can avoid coordinated vulnerability attacks and emphasize geographical distribution and latency reduction. To accommodate global service optimization, automotive security, authentication, and trust management in both distributed and decentralized IoT systems, the architecture addresses the anonymity of

credential access identification realized by IoT devices and provides a layered network approach by supplementing the SDN controllers with a consensus algorithm.

10.3.1 System Design

Figure 10.2 illustrates the architectural overview of our proposed solution. The architecture of our system comprises four different layers. At the top of Figure 10.2 is the blockchain application service layer, i.e. Decentralized applications (DAPPs) running autonomously. DAPPs are autonomous software programs running inside distributed SDN controller nodes to trigger the generation of transactions data from different IoT nodes. All transactions are cryptographically secured using hash functions and embedded inside a block of data. Then, consensus-driven decisions are made between DAPPs to validate the block generated by different IoT nodes. Once validated, blocks are immutable and their content will not be altered, modified or deleted during the process.

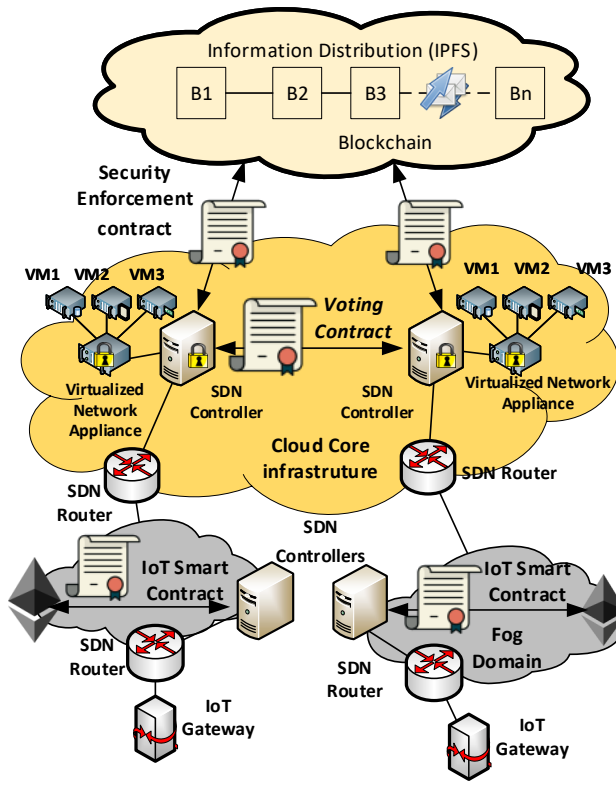


Figure 10.2: Overview of the Blockchain-SDN IoT architecture.

Secondly, both the virtualization layer and the controller network service abstraction layer are described in Figure 10.2. The virtualization layer provides a

Blockchain on Kubernetes in the form of Infrastructure-as-code. Kubernetes platform helps in managing applications in the form of containers across multiple physical hosts. Additionally, it also provides many managements features to facilitate the orchestration of virtualized network functions. In particular, several distributed blockchain nodes can be hosted inside these containers and perform agreement-driven decisions between each other. They also communicate with DAPPs using low level ABI calls over 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. Application Binary Interface (ABI), into RPC calls without relying on a third party authority.

Furthermore, the SDN control plane encompasses softwarized agile, flexible, and communication layer that translates the Blockchain decisions into flow rules to program the underlying network infrastructure according to the application requirements. The controller can listen to the blockchain and report suspicious IP addresses before validating known packets. It allows deploying a virtualized intrusion detection system inside the Kubernetes cluster in the form of virtualized network functions (VNFs), i.e. a Firewall as a Service in SDN OpenFlow-based network, which takes care of malicious flows and enables DDoS detection and mitigation-on-demand. The SDN controller can trigger storing decisions to VNF instances to maintain all the reports about whitelisted and blacklisted IP addresses. The Kubernetes manager can dynamically scale up and down to meet changing conditions and accommodate higher traffic demand or more stringent service requirements.

The last layer is the data plane abstraction layer, which contains both the SDN virtual routers and switches as well as the abstraction device layer which communicate using interfaces to IoT gateways with remote sensors and actuators. Additionally, the SDN controller implements security policies to protect the underlying virtual routers and switches against eventual intrusion. As the SDN routers are directly connected to the blockchain, data should be encrypted before its transmission to remote participants.

10.3.2 Flow Management

Figure 10.3 depicts the details of the layered framework. First, the DAPPs layer is composed of four modules: 1) the identification module, which manages the user/node access using the private and public keys. Indeed, from the public key is inferred the IoT node address in the blockchain (i.e. the 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 the node balance and used for sending and receiving transactions. The wallet is used to store the node balance of tokens (i.e. ERC20 tokens) used to pay the transaction fees.

Each blockchain node could have one or multiple accounts, called Externally Owned Account (EOA), where each node should have different identification scenarios for each EOA. Therefore, the framework implements another module for the Authentication, Authorization and Accounting (AAA) with the Blockchain so that nodes can access the infrastructure service through the API calls to reserve the re-

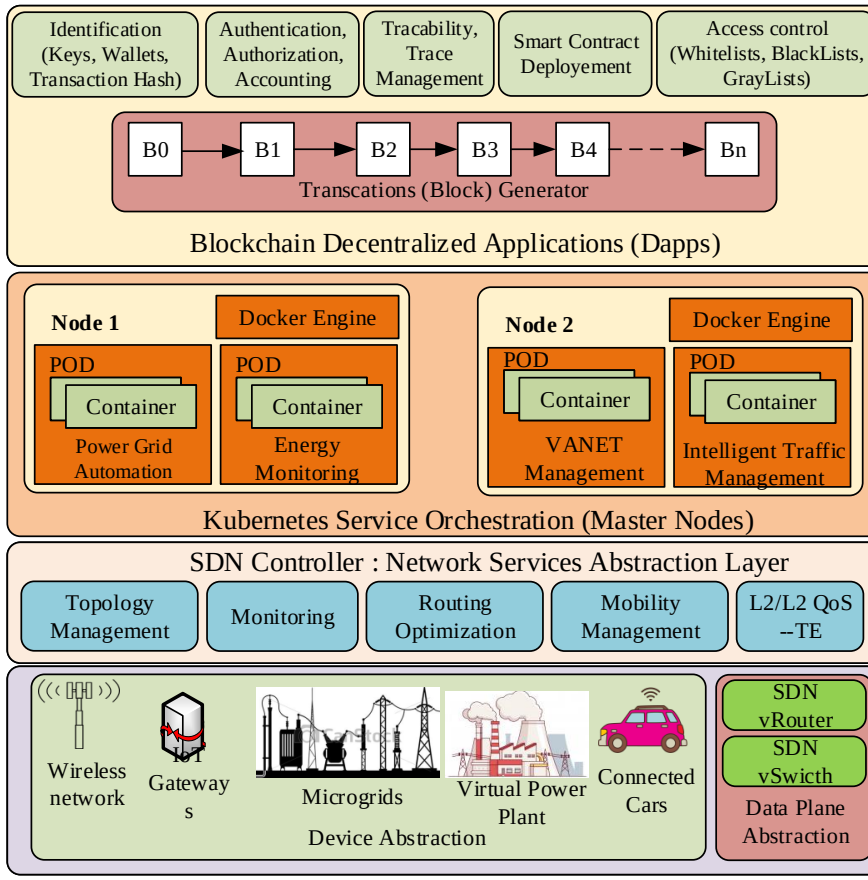


Figure 10.3: Blockchain-SDN Applications Framework in Smart City Security.

quired 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 the transaction, from its originating node to every processing on the blockchain infrastructure. The smart contract deployment module, which will be discussed in Section 10.3.3, allows the interaction with the contract from its creation to its deployment. Finally, the access control module, which will be discussed in Section 10.3.4, implements the functions for enforcing trust on transactions by listening to mining nodes and reporting suspicious IP addresses.

Likewise, the 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 the 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). 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.

10.3.3 Smart Contract design

The smart contract is a software program stored on the Blockchain infrastructure, which needs to be validated by distributed blockchain nodes like any other regular transaction generated by IoT devices. 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. For example, our approach uses the Ethereum Blockchain platform to build the smart contract in the Solidity language as shown in Listing 10.1, which are then compiled into "*bytecode*", read and executed over a portable execution environment called the "*Ethereum virtual machine*" (EVM).

```
1
2  pragma solidity >=0.4.16 <0.7.0;
3  contract SmartCityContract
4  {
5  address public owner;
6  IPAddress ipBoundary;
7  Lifeliness currentState;
8  Lifeliness constant defaultState = Lifeliness.sensing;
9
10 struct Report {
11 uint expirationdate;
12 IPAddress sourceIp;
13 IPAddress destinationIp;
14 }
15
16 struct SuspectBehavior {
17 address subject; //subject who performed the misbehavior;
18 address object; //
19 string res; //
20 string action; //action (e.g., "read", "write", "execute") of the
       misbehavior
21 string misbehavior; //misbehavior
22 uint time; //time of the Misbehavior occured
23 uint penalty; //penalty (number of minitues blocked);
24 string suspectIP;
25 string suspectMAC;
26 }
27 }
```

Listing 10.1: Smart contract for detecting malicious IoT devices

As shown in Listing 10.1, our approach allows trusting the IoT nodes based on their MAC and IP addresses, and their interaction with other IoT services. The smart contract is about 400 lines of Solidity code. Listing 10.1 illustrates only a snapshot of it. A data structure (*struct SuspectBehavior*) inside the blockchain smart contract is used to detect suspected behavior and report (*struct Report*) it to the SDN controller. This latter can now distribute trusted lists of IoT devices. A blockchain validator is introduced to check the validity of IoT devices connected over the blockchain. The validator parses the OpenFlow messages to identify the source and destination of incoming traffic. The SDN controller uses the information contained in the OpenFlow packet headers to create a wide network view including topology state and transactions meta-data.

By expecting and parsing every OpenFlow packet exchanged between the IoT devices and the network, the SDN controller can identify every abnormal behavior in the network. That is, if an attacker wants to take control of any IoT device, the changes of the 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. The former are the 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 latter are users or devices whose behavior is normal, and they could continue delivering their content as they belong to the blockchain.

10.3.4 Consensus Algorithm

The proposed framework introduces a Proof-of-Authority (PoA) consensus concept for IP addresses and reports them under smart contracts. The PoA consensus algorithm 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 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, the framework gives more importance to a node's reputation rather than digital assets owned by nodes in traditional PoW (Proof-of-Work) and 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, 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. In order to keep the network more efficient and trusted, the number of validator 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.

10.4 Use Cases

This section describes three use cases that can use our proposed architecture in three different applications, including SDN-enabled Internet of Vehicles (IoV) environment.

10.4.1 Blockchain-SDN enabled Internet of Vehicles

The Internet of Vehicles (IoV) is a distributed network that interconnects various IoT systems, such as connected cars, pedestrians, roads, and parking systems. It allows them to exchange their information more efficiently with infrastructures using Vehicular Ad Hoc Networks (VANETs) to improve the safety of vehicles and are foreseen to use 5G mobile networks to push their performance and capabilities to their extremes [42] [43] [44].

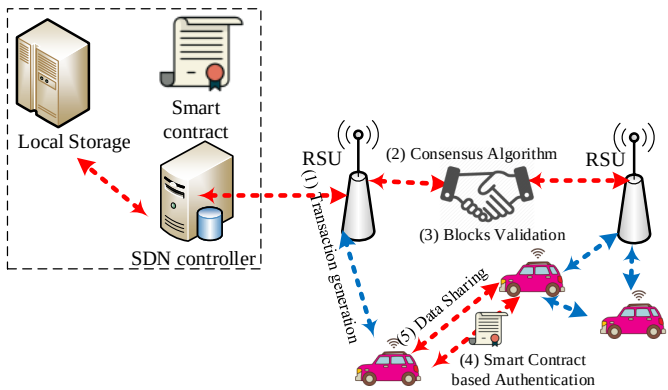


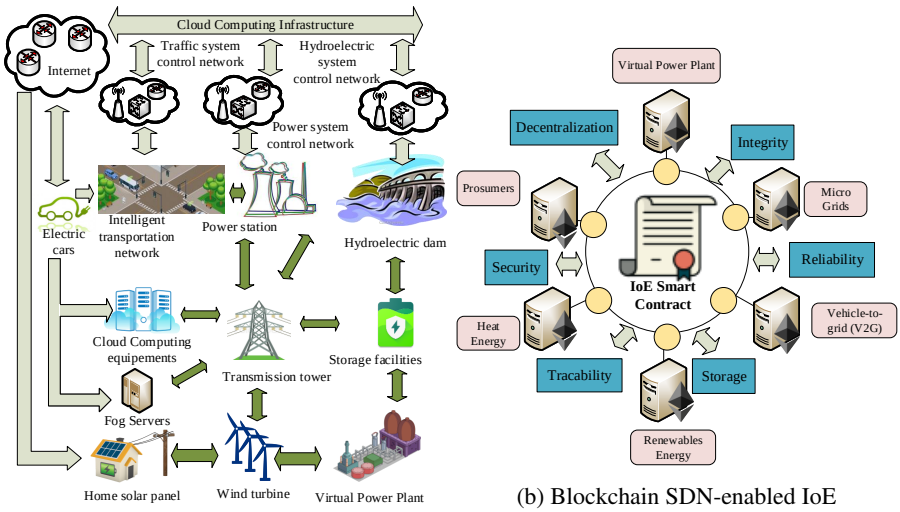
Figure 10.4: Secure message dissemination in SDN-enabled VANET

As shown in Figure 10.4, 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 the connected vehicles or push them down to other RSUs.
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 [45].
The combination SDN and Blockchain can effectively and efficiently manage and control operations of VANET systems [43]. 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 preselected 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 [46].

10.4.2 When Blockchain and SDN meet Internet of Energy (IoE)

Internet of Energy (IoE) [47] has recently received significant attention from energy manufacturers and producers to reduce fossil energy and address environmental pollution concerns [48]. At its core, IoE is a peer-to-peer, distributed, interconnected, open and intelligent network architecture for upgrading and automating electricity infrastructure, including renewable energy, energy harvesting devices, micro-grids, and Virtual Power Plant (VPP). In particular, VPP is a cloud native network architecture that embraces message brokers, network virtualization, and sensors softwarization to aggregate the capacities of heterogeneous distributed energy resources.
Figure 10.5 depicts the current traditional Internet of Energy model (i.e. Figure 10.5a) and Blockchain-enabled model supported by our approach (i.e. Figure 10.5b). Our approach can be perceived to have tremendous potential to meet flexibility, security, resiliency, and flow isolation requirements of the Internet of Energy network [49]. The computer nodes in Figure 10.5b describe distributed ledgers that mediate data dissemination between Internet of Energy stakeholders [50]. For example, in virtual power plans these ledgers hold a SDN control layer to offer fast flow rerouting and low latency capabilities, build resilient network communication, and abstract and integrate the distributed utility resources. Similar to mobile cellular operators, this approach enables supporting different virtual energy operators



(a) Traditional Virtual Power Plant

(b) Blockchain SDN-enabled IoE

Figure 10.5: Internet of Energy: Traditional Model vs Blockchain-enabled Model

and service providers that same physical infrastructure but implement their own operations and businesses independently. The decentralized aspect of Blockchain fits perfectly in this universal vision of IoE by enabling the participation of connected and distributed electricity infrastructures in validating transactions [51]. That is, Blockchain perfectly addresses not only the challenging issues of energy trading in the above use case, but also satisfies data integrity and ensures data security and privacy-preservation.

10.4.3 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 10.6 shows how IoT gateways can be connected to a controller built in the Blockchain IoT service layer. The SDN controller provides a collaborative mechanism for whitelisting or blacklisting suspicious IoT gateway IP addresses. Our approach delegates storing blacklisted and white listed IP addresses to Virtualized Network Functions (VNFs) instances inside lightweight containers for trustworthiness by maintaining all the reports (i.e. about white-listed and black-listed IP addresses). Those VNF instances can be dynamically deployed to meet changing conditions and accommodate to higher traffic demand or more stringent service requirements.

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 com-

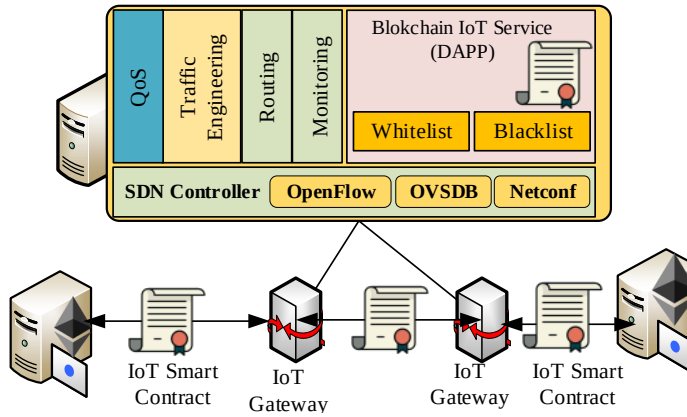


Figure 10.6: Ensuring Security and Interoperability between IoT Gateways.

munications 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 the IoT security needs, combing the on-demand service orchestration offered by SDN/NFV and security capability offered by Blockchain, 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 a prepared for threats that can overwhelm well-prepared defenses of critical services.

10.5 Open Challenges and Directions for Future Work

Blockchain is a nascent technology that comes with a set of complex and open issues that should be addressed to develop infrastructure, agreements and safety mechanisms to overcome them. This section delves into the key technical and government challenges, and discusses some initial solutions to address them. These issues then become the key directions for conducting future research.

10.5.1 Scalability issues

Despite the fact that Blockchain provides high-performance, transparent, immutable, and cryptographically verifiable transactions, scalability is still a significant issue to support low-latency communication in ultra-dense IoT systems [52]. Indeed, current Blockchain platforms may take seconds (e.g. Ethereum) or minutes (e.g. Bitcoin) for a transaction to be included in a block [53]. The main reason for this slow speed is that every block validation and every computation should be performed at every Blockchain node in the network, which increases the computational power and the transaction confirmation time of the entire network to the processing capability of a single node. Smart city devices, such as Fog servers and IoT gateways have limited processing, memory, and computation capabilities and currently cannot be used as

miners to process consensus algorithms. On the other hand, for large amounts of transfer, it is recommended to wait more time (about an hour) to confirm the transaction and verify its integrity because it must outweigh the cost of a double spend attack, while the same processing takes seconds at most with IoT gateways.

10.5.2 Power Consumption

As Blockchain miners should solve proof-of-work (PoW) puzzle to ensure IoT transactions integrity and validity, they consume substantial computing power and use massive amounts of energy for running both hardware and cooling systems. Some recent estimates showed that some Bitcoin miners consume around 61.4 TWh, which is equivalent to 1.5% of electricity consumed in the US, and all these costs are paid with fiat money. It was also estimated that validating and sharing one Bitcoin transaction requires the same amount of electricity for powering 1.57 American households for one day, which imposes more pressure on the digital currency value, especially if we know that all blockchain nodes spend their resources with no benefit other than mining, as they compete for useless proof-of-work effort in the hopes of a reward. Besides, as the mining hardware generates a lot of heat, it may overheat the machines, reduce their efficiency and even damage them. Thus, it becomes important to invest in submersion cooling where mining chips could be submerged in a cooling liquid that circulates to dissipate heat. Immersion cooling could help in packing more chips in the same mining hardware, i.e., packing more processing power and memory in the same physical space to increase the mining potential. Some other approaches tend to use under-the-sea cooling to develop self-sufficient underwater mining data centers.

10.5.3 Storage

Blockchain nodes typically store transitions and blocks in text and meta-data files, where the size of block depends on the synchronization mode activated at each involved participant node. For example, for a IoT node using the "*fast sync*" mode in Ethereum a complete copy of the Blockchain size is closer to 50 GB and this amount tends to grow by 14 GB each year. Although reducing the block size could improve storage, it however could impact their scalability as bigger blocks are as blockchain is more efficiently accessed.
Therefore, there is an urgent need to rethink innovative compression algorithms to make blockchain storage scalable perhaps by inspiring approaches from modern big data and data-intensive science advances. Another promising approach could be by improving data accessibility through the use of novel and advanced APIs that facilitate automated calls and notification, to notify user applications every time transactions or blocks are created on the network.

10.5.4 Privacy Leakage

Double spending 51% attack could become a security issue in blockchain as one mining entity could grab control of the overall blockchain. This issue stems from the

fact that centralizing the mining power into only few large mining pools who control the majority of the transaction recording. Another important security issue concerns the vulnerability of smart contracts themselves. A Smart contract is an autonomous software code running across distributed nodes that agree to its content. Attackers can unleash a malicious intermediate contract and invoke it repeatedly to perform memory-intensive work, thereby dramatically slowing down the overall blockchain network. This could happen when smart contracts are poorly designed and suffer from reinjection vulnerability, e.g., they were designed without rollback in mind so that the stolen amount is not recoverable.
A possible alternative to overcome this limitation would be to make the design of smart contracts more difficult for bugs to appear. This will need a formal verifiable language and model checking tools for exploring all possible states and transitions in the smart contract models, which in turn requires domain-specific abstraction techniques to perform formal verification.

10.6 Potential Future Research Opportunities

10.6.1 Off-chaining Models

To meet the scalability needs of future IoT networks using blockchain, off-chaining computations could be a promising approach. Computationally heavy tasks such as state transition functions are executed on Off-chain Nodes while only the state's outcomes are stored on the blockchain. Heavy computation can be delegated to another layer on top of the blockchain that performs heavy, compute-intensive work thereby using the blockchain resources effectively. Off-chaining computation could be centralized, distributed across a group of nodes or outsourced in a side-chain. In order to succeed in such an approach, IoT nodes will not only retrieve the results and the proof of correctness for the outsourced operations, but also IoT devices will be able to verify the proof of correctness themselves without consuming substantial computing power. Off-chaining model can help to scale up public main chain while limiting and isolating any damages to the private side chain to prevent the main chain from any dramatic damage.

10.6.2 Data Analytics

Big data analytics have been successfully applied to various smart city themes such as air quality, smart transportation, energy internet, and climate pattern analysis [54]. It also has been the successful driving force behind the evolution of various artificial intelligence, data mining, machine learning and statistical analysis-based solutions in smart cities [55]. Smart city big data are stored in siloes within different IoT infrastructure including IoT gateways, Fog computing servers, and cloud computing. Integrating Big data with Blockchain can transform the smart city environment by ensuring data integrity and supporting data auditability without the need for centralized third party auditors (TPAs) [56]. Additionally, when big data meets blockchain, it could help in tracking IoT transactions by creating incentive systems in the form of IoT node managers that delve into the interactions between IoT devices to uncover

hidden interaction patterns among them. Specifically, Big data could reshape the data structure in smart city services as it covers a huge amount of data gathered from climate monitoring tools, intelligent transportation systems, connected self-driving vehicles, thereby making more predictable decisions.
Furthermore, combining Blockchain and big data will 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. In particular, it avoids data fragmentation as all involved parties in IoT transactions have 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. For example, BigchainDB [3] is an open source distributed storage system that builds on top of Big Data for deploying a decentralized Blockchain to avoid any hard limit on the transaction size. This is extremely extremely interesting for smart cities to disseminate trained machine learning models and statistical analysis solutions to all involved parties. Similarly, Amazon Quantum Ledger Database (QLDB) [4] builds on top of a new type of fully managed ledger database to provide complete and cryptographically verifiable history of IoT transactions, which provides multiple smart city stakeholders with full data lineage within a centralized and trusted entity.

10.6.3 Artificial Intelligence

In light of recent advances in blockchain technology, Artificial intelligence (AI) could help in solving some challenging issues in blockchain, such as energy consumption, scalability, security, privacy, efficiency, and mining. DeepMind AI has been proven to be very efficient in optimizing energy consumption as it consistently achieved a 40 percent reduction in the amount of energy used for cooling in Google data center. We believe that similar results could be achieved with blockchain as well. AI could also help in producing decentralized intelligence (either on-chain for basic information or off-chain in case of extra attachments) by introducing decentralized learning system such as federated learning and supporting sharding techniques to make the system more efficient.

10.6.4 Smart Contracts

Smart contracts are software code where bugs could exist and may be vulnerable to malicious activity. The DAO contract suffers from the reinjection vulnerability which was exploited by hackers to withdraw existing funds repeatedly. Therefore, smart contract performance analysis is very important as it will reveal the limitation and show the potential vulnerabilities that may occur. Thus, formal verification of smart contracts is important to detect any irregularities in its design and behavior. Model-Checking approaches [57], formally verifiable language [58], and formal verification tools [59] are necessary to verify that the smart contract implementation

[3]https://github.com/bigchaindb/bigchaindb
[4]https://aws.amazon.com/qldb/

complies with its specification, verify its security properties, formalize it by a set of temporal logic propositions [60].

10.7 Conclusion

Blockchain is emerging as a technological breakthrough to address security, privacy and data distribution in many smart cities key themes, such as energy internet, virtual power plan, and vehicular networks. Diverse consensus algorithms are being under investigation by the research community to increase the use of distributed ledgers in IoT systems. In this chapter, we presented a Blockchain architecture for supporting SDN-enabled IoT communication in smart cities. The symbiotic relationship between SDN and Blockchain brings more transparency and security to IoT transactions and enforces scalability and performance of the whole network. By enabling dynamic and on-demand resource provisioning through the use of lightweight virtualized appliances, our approach can meet the requirements of various needs of future smart city networks. We argue that Blockchain is still at its early stages, and soon we should expect an explosive growth of novel solutions that will emphasize providing functional and architectural design approaches to extend its use to healthcare industry, specifically given that the global COVID-19 pandemic, which started toward the end of 2019, has revealed several limitations of our global supply chains. Furthermore, Blockchain is foreseen one of the most disruptive technologies to address most of the current limitations and facilitate the functional standards of 6G, by enabling massive connectivity, improving privacy-preserving, and decentralizing mobile front-haul in 6G cellular network architecture.

Acknowledgments

This work was funded in part by the Tunisian Ministry of Higher Education and Scientific Research (MES) under the Young Researchers Incentive Program (19PEGC09-04) and the United States National Science Foundation (NSF) CNS US Ignite 1531079. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of MES or NSF.

References

[1] Christidis K, Devetsikiotis M. Blockchains And Smart Contracts For The Internet Of Things. IEEE Access. 2016;4:2292–2303.

[2] Tselios C, Politis I, Kotsopoulos S. Enhancing Sdn Security For Iot-related Deployments Through Blockchain. In: 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN); 2017. p. 303–308.

[3] Judmayer A, Stifter N, Krombholz K, et al. Blocks And Chains:introduction To Bitcoin, Cryptocurrencies, And Their Consensus Mechanisms; 2017.

[4] Dannen C. Introducing Ethereum And Solidity: Foundations Of Cryptocurrency And Blockchain Programming For Beginners. 1st ed. Berkely, CA, USA: Apress; 2017.

[5] Eyal I. Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams To Finance And Banking Realities. Computer. 2017;50(9):38–49.

[6] Nordrum A. Govern By Blockchain Dubai Wants One Platform To Rule Them All, While Illinois Will Try Anything. IEEE Spectrum. 2017 Oct;54(10):54–55.

[7] Sabounchi M, Wei J. Towards Resilient Networked Microgrids: Blockchain-enabled Peer-to-peer Electricity Trading Mechanism. In: 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2); 2017. p. 1–5.

[8] Kim G, Park J, Ryou J. A Study On Utilization Of Blockchain For Electricity Trading In Microgrid. In: 2018 IEEE International Conference on Big Data and Smart Computing (BigComp); 2018. p. 743–746.

[9] Lundqvist T, de Blanche A, Andersson HRH. Thing-to-thing Electricity Micro Payments Using Blockchain Technology. In: 2017 Global Internet of Things Summit (GIoTS); 2017. p. 1–6.

[10] Kang J, Yu R, Huang X, et al. Enabling Localized Peer-to-peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains. IEEE Transactions on Industrial Informatics. 2017 Dec;13(6):3154–3164.

[11] Ibba S, Pinna A, Seu M, et al. Citysense: Blockchain-oriented Smart Cities. In: Proceedings of the XP2017 Scientific Workshops. XP '17. Cologne, Germany; 2017. p. 12:1–12:5.

[12] Biswas K, Muthukkumarasamy V. Securing Smart Cities Using Blockchain Technology. In: 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS); 2016. p. 1392–1393.

[13] Lu Z, Sun C, Cheng J, et al. SDN-Enabled Communication Network Framework for Energy Internet. Journal of Computer Networks and Communications. 2017 Jun;2017:8213854.

[14] Bocek T, Rodrigues BB, Strasser T, et al. Blockchains Everywhere - A Use-case Of Blockchains In The Pharma Supply-chain. In: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM); 2017. p. 772–777.

[15] Polyzos GC, Fotiou N. Blockchain-assisted Information Distribution For The Internet Of Things. In: 2017 IEEE International Conference on Information Reuse and Integration (IRI); 2017. p. 75–78.

[16] Buccafurri F, Lax G, Nicolazzo S, et al. Overcoming Limits Of Blockchain For IoT Applications. In: Proceedings of the 12th International Conference on Availability, Reliability and Security. ARES '17; 2017. p. 26:1–26:6.

[17] Bartoletti M, Pompianu L. An Empirical Analysis Of Smart Contracts: Platforms, Applications, And Design Patterns. In: Financial Cryptography Workshops; 2017. .

[18] Cha SC, Chen JF, Su C, et al. A Blockchain Connected Gateway For Ble-based Devices In The Internet Of Things. IEEE Access. 2018;p. 1–1.

[19] 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); 2018. p. 62–67.

[20] Gupta Y, Shorey R, Kulkarni D, et al. The Applicability Of Blockchain In The Internet Of Things. In: 2018 10th International Conference on Communication Systems Networks (COMSNETS); 2018. p. 561–564.

[21] Yin S, Bao J, Zhang Y, et al. M2m Security Technology Of Cps Based On Blockchains. Symmetry. 2017;9(9).

[22] Hahn A, Singh R, Liu CC, et al. Smart Contract-based Campus Demonstration Of Decentralized Transactive Energy Auctions. In: 2017 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT); 2017. p. 1–5.

[23] Chen J. Flowchain: A Distributed Ledger Designed For Peer-to-peer IoT Networks And Real-time Data Transactions. In: In proceedings of the 2nd International Workshop on Linked Data and Distributed Ledgers; 2017. .

[24] 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; 2017. .

[25] Daza V, Pietro RD, Klimek I, et al. Connect: Contextual Name Discovery For Blockchain-based Services In The Iot. In: 2017 IEEE International Conference on Communications (ICC); 2017. p. 1–6.

[26] Conoscenti M, Vetrò A, Martin JCD. Blockchain For The Internet Of Things: A Systematic Literature Review. In: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA); 2016. p. 1–6.

[27] Conoscenti M, Vetrò A, Martin JCD. Peer To Peer For Privacy And Decentralization In The Internet Of Things. In: 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C); 2017. p. 288–290.

[28] Xiong Z, Zhang Y, Niyato D, et al. When Mobile Blockchain Meets Edge Computing; 2017. .

[29] Kshetri N. Blockchain's Roles In Strengthening Cybersecurity And Protecting Privacy. Telecommunications Policy. 2017;41(10):1027–1038.

[30] Kataoka K, Gangwar S, Podili P. Trust List: Internet-wide And Distributed Iot Traffic Management Using Blockchain And Sdn. In: 2018 IEEE 4th World Forum on Internet of Things (WF-IoT); 2018. p. 296–301.

[31] Samaniego M, Deters R. Blockchain As A Service For IoT. In: 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData); 2016. p. 433–436.

[32] 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. BDAW '16; 2016. p. 58:1–58:9.

[33] Rodrigues BB, Bocek T, Lareida A, et al. A Blockchain-based Architecture For Collaborative Ddos Mitigation With Smart Contracts. In: AIMS; 2017. .

[34] Basnet SR, Shakya S. BSS: Blockchain security over software defined network. In: 2017 International Conference on Computing, Communication and Automation (ICCCA); 2017. p. 720–725.

[35] Rodrigues B, Bocek T, Stiller B. Enabling A Cooperative, Multi-domain Ddos Defense By A Blockchain Signaling System (bloss); 2017. .

[36] Abbasi AG, 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. UCC '17 Companion; 2017. p. 173–179.

[37] Sharma V, You I, Palmieri F, et al. Secure And Energy-efficient Handover In Fog Networks Using Blockchain-based DMM. IEEE Communications Magazine. 2018 May;56(5):22–31.

[38] Sharma PK, Singh S, Jeong YS, et al. Distblocknet: A Distributed Blockchains-based Secure Sdn Architecture For Iot Networks. IEEE Communications Magazine. 2017;55(9):78–85.

[39] Salahuddin MA, Al-Fuqaha A, Guizani M, et al. Softwarization Of Internet Of Things Infrastructure For Secure And Smart Healthcare. Computer. 2017;50(7):74–79.

[40] Hari A, Lakshman TV. 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. Atlanta, GA, USA; 2016. p. 204–210.

[41] 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); 2017. p. 1–8.

[42] Chen H, Zhao T, Li C, et al. Green Internet of Vehicles: Architecture, Enabling Technologies, and Applications. IEEE Access. 2019;7:179185–179198.

[43] Gao J, Obour Agyekum KO, Sifah EB, et al. A Blockchain-SDN-Enabled Internet of Vehicles Environment for Fog Computing and 5G Networks. IEEE Internet of Things Journal. 2020;7(5):4278–4291.

[44] Yang Y, Hua K. Emerging Technologies for 5G-Enabled Vehicular Networks. IEEE Access. 2019;7:181117–181141.

[45] Ma Z, Zhu L, Yu R. A Novel Framework of Vehicle Ad-Hoc Networks Based on Virtualization and Distributed Ledger Technology. In: Proceedings of the 9th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications; 2019. p. 39–47.

[46] Xie L, Ding Y, Yang H, et al. Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs. IEEE Access. 2019;7:56656–56666.

[47] CAO Y, LI Q, TAN Y, et al. A comprehensive review of Energy Internet: basic concept, operation and planning methods, and research prospects. Journal of Modern Power Systems and Clean Energy. 2018 May;6(3):399–411.

[48] Mahmud K, Khan B, Ravishankar J, et al. An internet of energy framework with distributed energy resources, prosumers and small-scale virtual power plants: An overview. Renewable and Sustainable Energy Reviews. 2020;127:109840. Available from: http://www.sciencedirect.com/science/article/pii/S1364032120301349.

[49] Lu X, Shi L, Chen Z, et al. Blockchain-Based Distributed Energy Trading in Energy Internet: An SDN Approach. IEEE Access. 2019;7:173817–173826.

[50] Rehmani MH, Davy A, Jennings B, et al. Software Defined Networks-Based Smart Grid Communication: A Comprehensive Survey. IEEE Communications Surveys Tutorials. 2019;21(3):2637–2670.

[51] Mollah MB, Zhao J, Niyato D, et al. Blockchain for Future Smart Grid: A Comprehensive Survey. IEEE Internet of Things Journal. 2020;p. 1–1.

[52] Reyna A, Martín C, Chen J, et al. On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems. 2018;88:173 – 190.

[53] Yasaweerasinghelage R, Staples M, Weber I. Predicting Latency of Blockchain-Based Systems Using Architectural Modelling and Simulation. In: 2017 IEEE International Conference on Software Architecture (ICSA); 2017. p. 253–256.

[54] Soomro K, Bhutta MNM, Khan Z, et al. Smart city big data analytics: An advanced review. WIREs Data Mining and Knowledge Discovery;9(5):e1319.

[55] Al Nuaimi E, Al Neyadi MNAJJ Hind. Applications of big data to smart cities. Journal of Internet Services and Applications. 2015 December;6(25):1–15.

[56] Yu H, Yang Z, Sinnott RO. Decentralized Big Data Auditing for Smart City Environments Leveraging Blockchain Technology. IEEE Access. 2019;7:6288–6296.

[57] Osterland T, Rose T. Model checking smart contracts for Ethereum. Pervasive and Mobile Computing. 2020;63:101129.

[58] Antonino P, Roscoe AW. Formalising and verifying smart contracts with Solidifier: a bounded model checker for Solidity. ArXiv. 2020;abs/2002.02710.

[59] Frank JC, Aschermann C, Holz T. ETHBMC: A Bounded Model Checker for Smart Contracts; 2020. .

[60] Yoo J, Jung Y, Shin D, et al. Formal Modeling and Verification of a Federated Byzantine Agreement Algorithm for Blockchain Platforms. In: 2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE); 2019. p. 11–21.