Application-Aware Consensus Management for Software-Defined Intelligent Blockchain in IoT

Jun Wu, Mianxiong Dong, Kaoru Ota, Jianhua Li, and Wu Yang

Abstract

Currently, IoT has become an important carrier of blockchains, which not only makes blockchain more ubiquitous but also improves the security of IoT. Consensus is the core component of blockchains with various forms, which raises the following challenges. Dynamic management and configuration of the consensuses in a blockchain are required because IoT applications have high dynamics. Moreover, an IoT node is usually reutilized by various applications in different blockchains, which means the IoT node should be switched frequently to cross consensuses in different blockchains. To address this, a software-defined blockchain architecture is proposed to realized the dynamic configurations for blockchains. Then a consensus function virtualization approach with application-aware work flow is proposed, which can abstract and manage various consensus resources. Next, a transfer-learning-based intelligent scheme is designed to implement the application-layer packet analysis and perform the efficient management of virtualized consensus resources. Experiment results indicate the feasibility of the proposed scheme. This work is significant in enhancing the flexibility and extendibility of blockchains in IoT.

Introduction

Nowadays, blockchain is regarded as a new form of distributed peer-to-peer encryption storage application, which provides a subversive innovation of networking and computing models [1]. It can be used widely in security and trust-critical environments, such as finance and industry. In the blockchain, the transaction party is the entity that actually records, deposits, and stores transaction information. The blocks packed by a node can be successfully verified by each node and added into the blockchain. Each block in the blockchain contains a large amount of transaction information, which is typically organized in a specific structure, such as a Merkle tree. In addition, the transaction information is verified against the results of the data, for example, by a Merkle certificate. Moreover, a smart contract is an executable layer that is agreed in advance of the transaction and submitted to the blockchain by both parties. The blockchain can automatically execute smart contracts for the corresponding transactions. Due to the resource constraints in the Internet of Things (IoT), most current blockchains in IoT have constraints on the throughput of transactions. In fact, it is necessary to implement cross-chain collaborations and interaction among different blockchains, especially in the era of the Internet of Everything (IoE).

At the same time, IoT has been widely used in environment monitoring, intelligent transportation, e-health, Industry 4.0, and so on. Blockchain enables trustless networks that provide secure peer-to-peer transactions in IoT without a trusted intermediary. In other words, the secure and unchangeable storage in blockchain guarantees the reliability and traceability of the data in IoT. Moreover, blockchain-based IoT eliminates single points of failure in the centralized networking structure of IoT. In IoT, some strong sensor nodes and networking interface modules/nodes can be used to mine, which means blockchain can be deployed at the edge of the network and enhance the security of IoT. This has become an important development trend in blockchains [2]. It is estimated that almost 50 billion devices will be interconnected by 2020, which means that the various IoT services are growing very rapidly. The IoT users in a smart city usually have dynamic requirements for one application. For instance, a doctor usually needs to change the monitoring and action applications of the e-health IoT when the diagnosis and treatment are provided to the patient. Thus, the applications of IoT have high dynamics. Therefore, dynamic management and configuration of the consensuses in a blockchain are imperative. Moreover, an IoT node is usually reutilized by various applications, such as transportation control, weather forecast, and environment monitoring. For example, the operations of the smart factory and trading are integrated seamlessly in Industry 4.0. Thus, a lot of nodes in Industry 4.0 cross the processes of smart factory and trading. In the smart factory, low-complexity consensus mechanisms (e.g., proof of stake, PoS) are utilized to provide low-latency industrial service. In the trading systems of Industry 4.0, blockchain applications typically employ the proof-of-work (PoW) consensus mechanism to ensure the trustworthiness of transactions. If an Industry 4.0 node cannot switch between the aforementioned different consensuses, it cannot be reutilized in both smart factory and trading. The drawback is that the processes of smart factory and trading cannot be integrated efficiently. Similarly, a camera at the roadside can be used by both intelligent transportation systems

Jun Wu, Jianhua Li are with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, China.
Mianxiong Dong (corresponding author) and Kaoru Ota are with Muroran Institute of Technology; Wu Yang is with Harbin Engineering University.

Digital Object Identifier:
10.1109/MNET.001.1900179

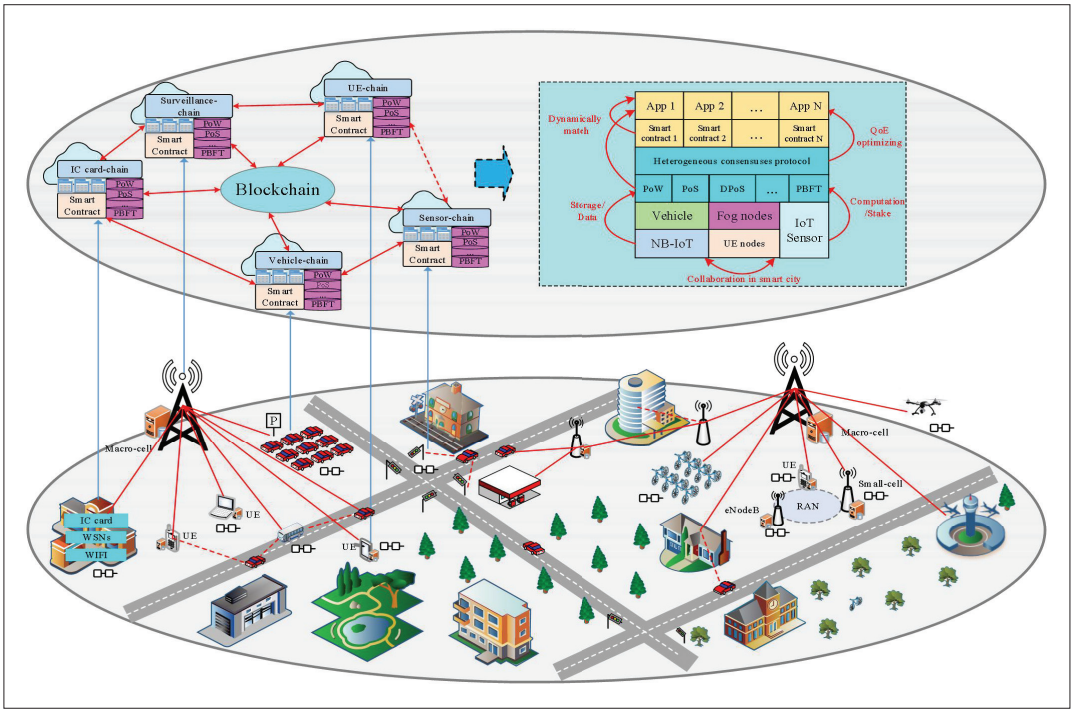


FIGURE 1. Scenario of dynamic management of blockchain in IoT.

(ITS) and security surveillance [3]. Therefore, when the IoT services are switched among different application systems, the requirements of the consensus are different. In other words, the consensuses of the blockchain in IoT should be switched dynamically to match the upper-layer applications. Thus, dynamic switching among heterogeneous consensuses of different applications should be provided. Based on the aforementioned motivation, a dynamic and intelligent management approach for blockchain is a must to provide application-aware capabilities for heterogeneous consensuses. The application scenario and motivation of this article are shown in Fig. 1.

On the other hand, software-defined networking (SDN) has been applied as a novel network architecture. In SDN, the network is decoupled into the control plane and data plane, which makes the underlying networks and components programmable [4, 5]. Meanwhile, an Industry Specification Group called European Telecommunications Standards Institute Network Function Virtualization (ETSI NFV) has specified the virtualization of network elements [6]. In ETSI NFV, the reference architecture of management and orchestration (MANO) is defined for resource scheduling for networks. The dynamic management capabilities of SDN and NFV provide the possibility to reconstruct the implementation architecture of blockchain in IoT. Currently, there are some existing works using blockchain to improve the security of SDN. However, a software-defined and virtualized function architecture of blockchain in IoT is still a open issue.

Based on the aforementioned challenges, this article proposes a software-defined blockchain architecture with consensus function virtualization capabilities, which can provide application-aware and intelligent management for consensuses in IoT. There are two contributions in the proposed architecture. First, to match the dynamic and differentiated applications in IoT, the proposed software-defined blockchain architecture provides a feasible approach to dynamically manage and control the blockchain resources. Second, the proposed consensus function virtualization and intelligent mangement methods can realize virtual consensus scheduling based on IoT application awareness.

The rest of the article is organized as follows. The following section analyzes related works. Following that, the analysis of blockchain and consensuses in IoT is presented. Then we give details of software-defined blockchain and consensus function virtualization. The application-aware intelligent scheduling scheme for virtual consensus functions is then given. Finally, we conclude this article.

Related Works

With the rapid development of IoT [7], the transactions at the edge of networks have become an important requirement in recent years [8]. For example, FiiiLab proposed the first mobile blockchain token, FiiiCoin, in 2018. It is an opportunity for an edge user to participate extensively in blockchain mining if IoT is used as the blockchain carrier.

Currently, some existing works focus on the management approaches of blockchains. To resolve the problem of energy-aware resource management in cloud data centers, a robust decentralized resource management framework was proposed; the energy consumed by the request scheduler can be saved for blockchain-based cloud data centers [1]. Moreover, distributed-ledger-based consuming identity management was proposed [9]. However, dynamic management studies for blockchains are rare, especially for blockchains in IoT. Dynamic distributed storage was proposed for blockchains, in which secret key sharing, private key encryption,

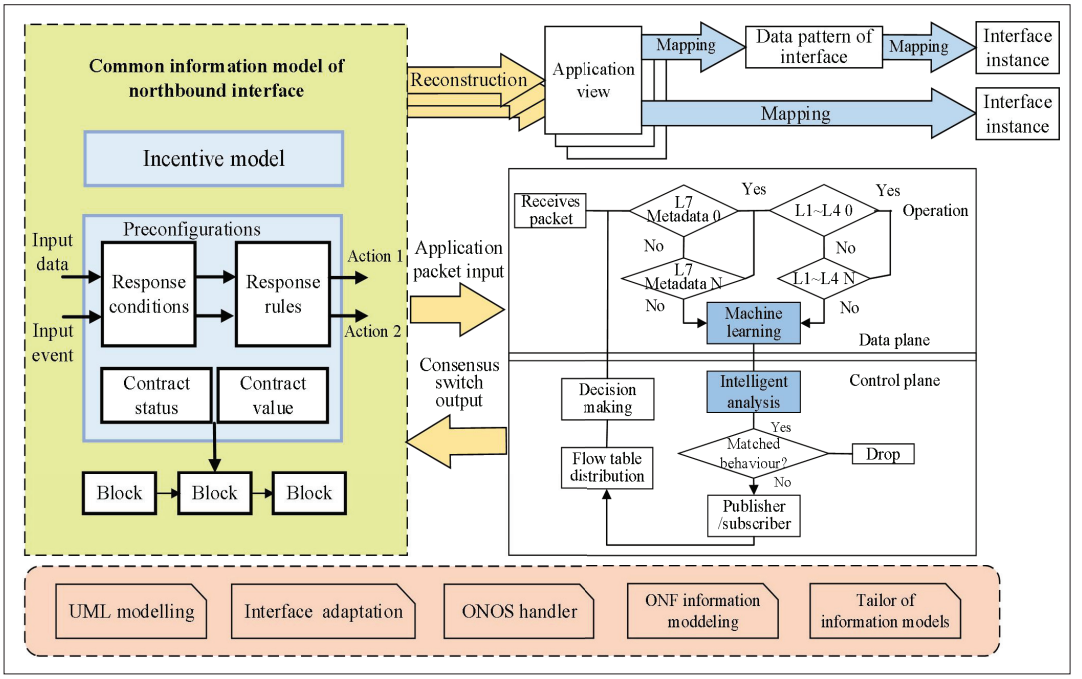


FIGURE 2. Work flow of application-aware consensus.

and distributed storage were integrated to design a coding scheme. In this scheme, each node just stores a part of each transaction; thereby, storage cost was reduced. In addition, a virtualization approach was proposed for distributed ledger technology [10]. The aforementioned works only consider the storage and distributed ledger management for common blockchains. Dynamic management and configuration of blockchain in IoT are still open issues.

Analysis of Blockchain and Consensuses in IoT

The consensus layer refers to the set of algorithms running in the blockchain peer-to-peer network to achieve consistency. In fact, there are various consensuses of blockchain that can be used in different IoT applications. PoW is a kind of consensus on the amount of computation, which calculates a nonce value related to cryptographic security. It is related to solving the mining problem in local IoT setup or domain. PoS can be implemented based on the IoT users' own privilege to determine who can construct the next block in the blockchain. For an IoT node with higher privilege, the probability of constructing the next block is higher. Practical Byzantine Fault Tolerance (PBFT) is essentially a state-machine-based copy replication algorithm. It can model the IoT service as a state machine and replicate copies on different nodes. There are also some other novel consensus methods to verify that certain concepts or theories model real applications. For example, proof of concept (PoC) has attracted a lot of attention. Specifically, in the transaction, PoC refers to partial solutions involving a small number of users to verify whether a system satisfies certain requirements.

Based on the aforementioned analysis, the design principles of various consensus schemes are differentiated, which are also the important differences among various blockchain applications. Because the aim of IoT is to connect everything in the world, it is very necessary to provide an application-aware consensus management approach for blockchain in IoT, which is also the motivation of this article.

Software-Defined Blockchain and Consensus Function Virtualization Architecture in IoT

Architecture of Software-Defined Blockchain

To provide application-aware capabilities for blockchain in IoT, we reconstruct the blockchain architecture based on SDN technologies. It is necessary to control network operation in the control plane. First, an IoT network commonly consists of many heterogeneous devices and various communication modes. Since different switches should be built independently for every pair of devices and communication modes, existing switch technologies have limited scalability and robustness in handling more than two devices or communication models without the SDN control plane. Second, the control plane supports unprofessional IoT users in configuring network resources accurately and efficiently. Third, the SDN control plane will be beneficial to achieve fine-grained network monitoring and traffic control.

As shown in Fig. 2, there are three layers in the proposed architecture. The blockchain network function virtualization infrastructure (NFVI) layer provides the virtual functions of the blockchain resources in IoT, which are controlled and scheduled by the blockchain control layer. Moreover, the IoT application configuration layer provides the differentiated application-aware information for the blockchain control layer. First, in the blockchain NFVI layer, heterogeneous consensuses are virtualized as various virtual network functions (VNFs), including PoW_VNF, PoS_VNF, PoC_VNF, and so on. All the VNFs can be configured by the NFV Orchestrator, which can orchestrate the consensuses based on the applications. The consensus VNFs are under the charge of a VNF

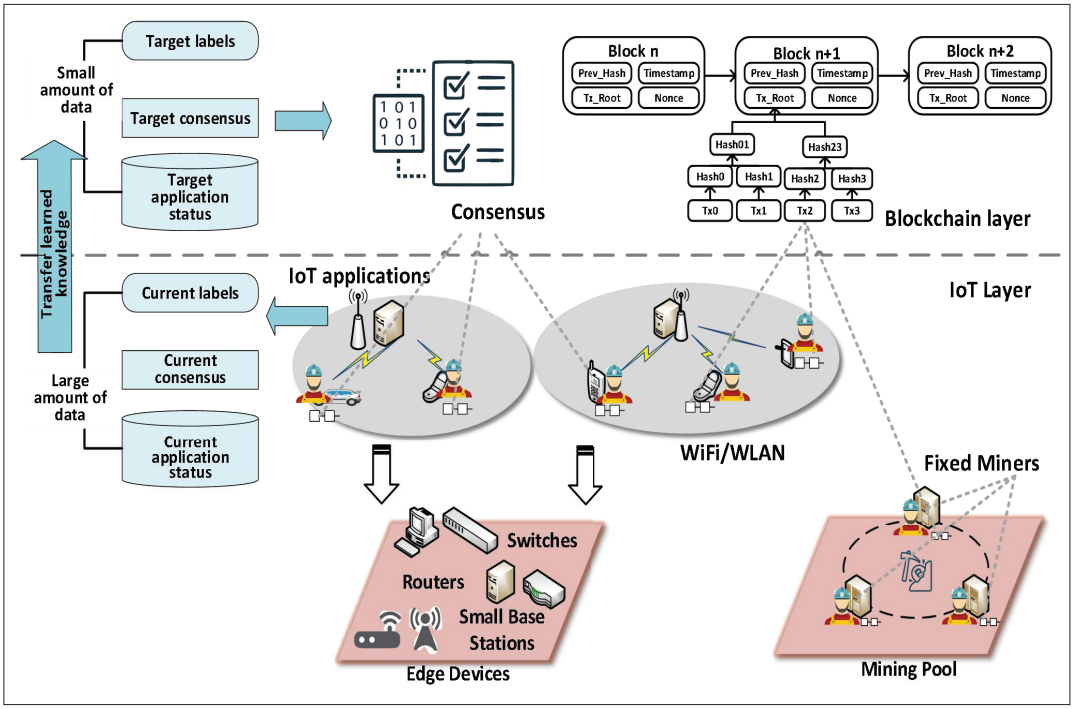


FIGURE 3. Intelligent management scheme for software-defined blockchain.

manager. In addition, the resources of the data layer of the blockchain, including blockchain data, chain structure, digital signature, hash function Merkle tree, and aysmmetric encryption, are virtualized through the virtualization layer. Second, in the blockchain control layer, the consensus and common IoT control capabilities are implemented in the SDN controller. Besides, the components of blockchain abstraction, VNF discovery, VNF registration, VNF selection, and flow tables are deployed in the SDN controller. The VNF discovery component provides the capabilities of blockchain search and network VNF, which are suitable for the applications. When a new VNF is presented in the blockchain system, a VNF registration component manages the information of the VNF, which means this VNF is registered. The function description, source, cost, and required hardware/software are the typical information of VNF registration. The blockchain abstraction component is used to provide the abstract and formal model of blockchain-related resources. Other traditional components are also involved in an SDN controller, including flow table, and VNFs of networking control and abstraction. Third, in the IoT application configuration layer, the important proposals in the SDN controller, smart contract, and incentives are embedded in the northbound interface, which interacts with IoT applications.

The proposed architecture is centralized in the SDN controller, which is also a node in the IoT domain. The decentralized consensus_VNFs are deployed in blockchains in IoT.

A smart contract is a module of blockchain, which is registered when the blockchain is deployed. To ensure the reliability of a smart contract, data related to a specific smart contract (inputs, outputs, smart contract codes, etc.) will be audited by the blockchain nodes. Basically, in the proposed architecture, the smart contract is decoupled independent of the consensuses.

Work Flow of Application-Aware Consensus

Current blockchain in IoT still regards the system as a set of devices rather than a holistic resource. Moreover, the IoT system cannot monitor the application-layer behaviors for the dynamic configurations. In the proposed architecture, smart contract and incentives are encapsulated into the northbound interface for IoT applications. The northbound interface is modeled based on common information model (CIM). The principle and work flow of application-aware consensus are shown in Fig. 3. Here, deep packet inspection (DPI) is used to get the information of the IoT application layer from the packets. When the OpenFlow switch of software-defined blockchain gets a packet, the matching implementation will be started based on the flow table. The packet will be sent to the SDN controllerif there is no layer 7 (L7) metadata matching a reasonable flow table. Next, a DPI-based application-aware module will inspect the packet. Intelligent packet analysis provides intelligent consensus configuration for the software-defined blockchain, in which machine learning will be used as the analysis algorithm.

Principle of Consensus Function Virtualization

Based on the virtualization technology, the function of the consensuses can be divided into several functional components, which are implemented in software mode instead of hardware mode. In fact, virtualized consensus functions provide the approach to integrate and schedule applications, processes, and infrastructure software.

Consensus function virtualization is proposed to accelerate the dynamic configuration of application-aware blockchain services, which consolidates blockchain device types into unified resources to take advantage of simpler open blockchain elements.

Some existing implementation technologies can be used as the container of the consensus function virtualization, such as docker and virtual machine (VM). Because the implementation of docker in sensors has been proven, the consensus function virtualization is realized based on docker technology, which is an open source container engine. The independent implementation environment is provided based on a sandbox mechanism.

Application-Aware Intelligent Management for Virtual Consensus Functions

In the software-defined blockchain architecture, the dynamic management of consensuses is a key issue. As for the aforementioned work flow of IoT application-aware consensus, the intelligent analysis component supports inspection of application-layer packets. The intelligent management scheme should provide intelligent analysis of the IoT application packets so that the application behaviors can be obtained based on the unknown and dynamic IoT application packets. After getting the application behaviors and types information, related consensus type information can be obtained. Moreover, the consensus information can be analyzed dynamically based on intelligent management. Intelligent orchestration of the virtual functions of consensuses is based on the analysis results.

Machine learning and cognitive models are feasible for use in blockchain and novel networks [11, 12]. To achieve intelligent control and scheduling capabilities for the virtual functions of blockchain in IoT, machine learning can be a useful approach to implementing intelligent analysis and providing the results to dynamic consensus management and selection. Because there are different distributions between the test and training data in application environments of blockchain in IoT, many traditional machine learning schemes cannot be applied directly.

To resolve this problem, transfer learning [13] is introduced and adapted to realize the intelligent management of application-aware software-defined blockchain. The intelligent management scheme is shown in Fig. 3. We propose the application-aware intelligent management scheme with the following principle. First, the historical application-layer packets of IoT are collected as the basic training data. However, because of the high dynamics of IoT, only a small part of the current packets have the same distribution as the historical packet data of IoT applications. Therefore, accurate classification and analysis cannot be implemented; enough training packet data are needed for IoT application packets. In the blockchain application environments in IoT, a transfer-learning-based intelligent management approach constructs and stores the knowledge gained while getting the learning model of a kind of consensus and applying it to establish a different but related model for other consensuses. TrAdaBoost-based transfer learning [14] is used in the proposed scheme. The learning frame is a promotion of the traditional AdaBoost algorithm, which is used to improve the classification accuracy of a weak classifier. We assume that the IoT application packet data of the current consensus and the target consensus application are distributed differently. Due to the difference of the distribution among the IoT application packet data, some data in the current consensus application may be beneficial to the learning of target consensus, while some data may disturb the learning of target consensus. The pretrained model is established for current consensus. The key principle here is to leverage the pretrained model's weighted layers to extract features but not to change the weights of the model's layers during training with further IoT application data for the next consensus. The proposed scheme can adapt the weight of the current consensus application data by repeated iterations to reduce the impact of harmful data and increase the impact of helpful data on target learning.

According to the results from the transfer-learning-based application-layer packet analysis, intelligent management can be realized. Furthermore, the proposed scheme can switch to suitable virtual consensus functions. Thus, the consensus can be configured dynamically.

Evaluations

In this section, we evaluate the performance of the proposed application-aware consensus management for software-defined blockchains in IoT.

Experimental Setup

Some simulations and experiment approaches for blockchain-based IoT can be found in[15]. The experimental environment includes three parts: sensor networks in IoT, SDN controller, and IoT clients.

For the IoT client module, we use the Django framework to visualize IoT sensor data and operations. We build a web interface to display the data collected by the SDN controller and its sensors. The site interface is also used to switch a sensor by the user. The site is responsible for interacting with the database and IoT applications. On one hand, the site interface receives data from the SDN controller and sends control commands to the SDN controller. There is a database storing all the data from the IoT applications and their corresponding consensuses. After authentication, the alive blockchain SDN controller and its attributes can be used. The IoT user can get the information on the number of sensors in IoT operation, the application types of the sensors, and the states of the sensors. In addition, there is the output of each sensor and the attributes of each sensor, and here we can switch each sensor in IoT. This flexible interface provides the interaction approach between the use and the lower-layer blockchain SDN controller and sensors.

We use a Raspberry Pi 3 Model B+ as the implementation device for the blockchain in IoT, in which NFV of blockchain is implemented. The Raspberry Pi 3 Model B+ is the final revision in the Raspberry Pi 3 range. The system-on-chip (SoC) architecture is Cortex-A53 (ARMv8) 64-bit, which is embedded in a BCM2837B0 mainboard. The Raspberry Pi 3 Model B+ is also equipped with 1.4 GHz CPU and 1 GB LPDDR2 SDRAM. In addition, it supports 2.4 GHz and 5 GHz IEEE 802.11.b/g/n/ac wireless LAN and Bluetooth 4.2. In the experiment, 2.4 GHz IEEE 802.11n is used for the wireless links to organize the network of blockchain in IoT. For the operation system, we use Centos because it is more stable and reliable than Raspbian. In the proposed architecture, the SDN con-

troller needs to be networked with the underlying sensor networks in IoT, so it needs to support the access points of IEEE 802.11n. We use adapted Simple Network Management Protocol (SNMP) as the monitoring interface of the proposed software-defined blockchain architecture. Here, adapted NET-SNMP is used, which is an open source SNMP protocol implementation. It also contains all relevant implementations of Trap. As the monitoring interface, NET-SNMP includes the SNMP utility set and the full SNMP development library, which can provide the interaction between IoT applications and SDN controllers. It not only provides management tools, but also provides some development and configuration tools. These tools are generally provided by scripts in Perl language including mib2c and net-snmp-config.

Each virtualized infrastructure manager of the blockchain is connected to the sensors, where the extension board of the sensors in IoT include the 40-pin interface on Raspberry Pi. The sensor extension board is a customized printed circuit board for our blockchain testbed. Various sensors with different manufacturers, interfaces, and data formats are supported in the testbed. Devices with the inter-integrated circuit (I2C) interface include 1602 liquid crystal display (LCD), accelerometer, barometer, and analog-digital converter (ADC). With ADC, a series of analog sensors can be accessed in our system. Devices with a general-purpose input/output (GPIO) interface include buttons, light-emitting diode (LED), buzzers, relays, infrared sensors, and so on.

We use several routers to build the experimental IoT environments. The SDN controllers are connected to each other. The blockchain virtualized infrastructure manager is only connected to the corresponding SDN controller, while one controller can connect multiple virtualized infrastructure managers. We use the Python programming on the CentOS system to realize TCP communication by socket and wireless communication by pybluez. Next, network communication is implemented by Python sturct according to the standardized protocol of IoT, which is IEEE 21451. In addition, the virtualized infrastructure manager uses real-time sensors, GPIO, and a sensor library in python to collect data such as temperature, humidity, atmospheric pressure, and acceleration, and returns these data to the SDN controller based on the SNMP protocol.

To enable the IoT client side to obtain information about the blockchain virtualized infrastructure manager and its connected sensors through the SNMP interface, we first develop NET-SNMP on both the client and the SDN controller. Then we adapt the management information base (MIB) in NET-SNMP. We have expanded four bits based on the original oid .1.3.6.1.4.1.21451. The first bit corresponds to the ID of each blockchain virtualized infrastructure manager device that is connected to the SDN controller device. This allows the client to accurately find the desired virtualized infrastructure manager device. Then the following three bits correspond to the value of the virtualized infrastructure manager itself, including the state of the CPU and memory (CPU and memory size, real-time occupancy, etc.). Real-time properties of the blockchain network are also included, such as latency, bandwidth, traffic, and network connection status. Moreover, various transducer electronic data sheet (TEDS) formats are implemented, such as Meta TEDS, PHY TEDS, and sensor channel TEDS. The three-bit extension starting with "1" corresponds to the switching state and the output value of the connected sensors in IoT. We use such rules to enable clients to get the data accurately.

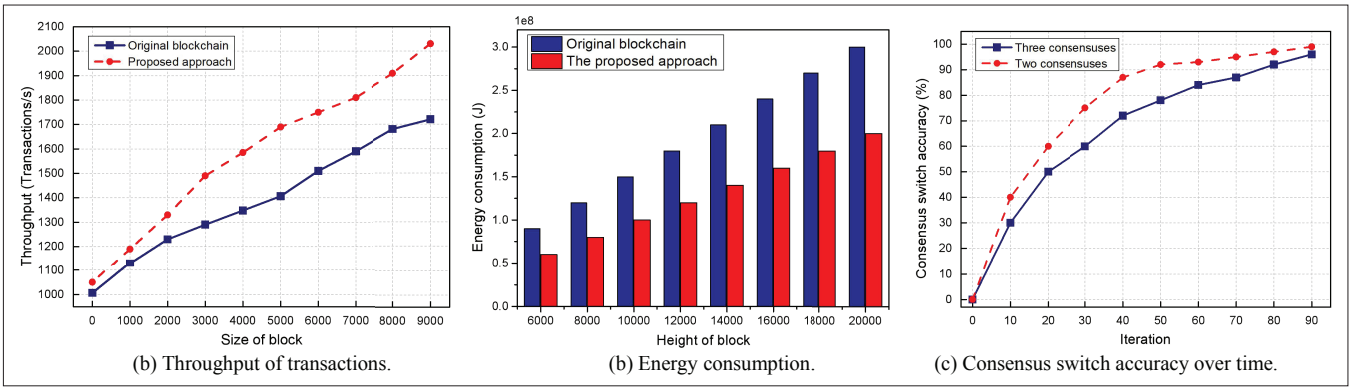
Twenty nodes are deployed, and a laptop is used as the SDN controller. The controller consists of 16 Intel® Xeon® E5620 CPUs (2.40 GHz), a bandwidth capacity of 1000 Mb/s, 16 GB memory, and 500 GB disk. In addition, an S12700 SDN switch is used. Both flow tables and transfer learning are deployed in the SDN controller. Three kinds of consensus cases are deployed — PoW, PoS, and PBFT — to evaluate the management of differentiated blockchains. PoW, PoS, and PBFT correspond to the trading, sensing, and data exchange applications in IoT. PoW is used as the initial consensus. The virtual function of PoW will be switched to other consensuses based on the intelligent analysis results.

In addition, we deploy the traffic measurement modular, sFlow, in the SDN controller and collect the throughput of the network. To measure the energy consumption in Joules of every node, we deploy a hardware energy measurement device, Juwei U96, for each Raspberry Pi 3 Model B+ node.

Experiment Results

Because IoT is resource-restrained network, energy consumption and communication resources are very important issues. The transaction load capability and energy are the main concerns that impact the performance of the blockchain in IoT. To perform the evaluation, these two factors are tested.

The comparison of the throughput of transactions is shown in Fig. 4a, where we take the sizes of blocks as the horizontal coordinates and transaction throughput as the vertical coordinate. Transaction throughput is calculated by the number of transactions per second. The size of the blocks means the number of transactions per block. Because of the application-aware capabilities introduced by software-defined blockchain architecture, the throughput of the proposed approach is higher than that of original blockchain. Moreover, the energy consumption of the proposed approach and traditional blockchain architecture are shown in Fig. 4b. Due to the consensus function virtualization and intelligent management of the resources, the energy consumption of the proposed approach is much lower than that of the original blockchain architecture with solidified consensus. The proposed approach satisfies the energy efficiency requirements of the resource-constrained IoT. The transfer-learning-based consensus switch accuracy over time is shown in Fig. 4c. The accuracy increases when the number of iterations of transfer learning increases. Moreover, after 80 iterations, the accuracy of both the cases of two and three consensuses exceed 90 percent. Basically, the change of the consensus algorithm will enhance the energy and resource consumption of the IoT node. However, the efficiency of blockchain implementation can be improved.



(b) Throughput of transactions. (b) Energy consumption. (c) Consensus switch accuracy over time.

FIGURE 4. Experimental results.

Conclusion

In the era of IoE, current static management of the consensuses in blockchains cannot provide application-aware and intelligent configuration capabilities for differentiated IoT services. Flexible and intelligent consensus management is a must for blockchain in IoT. To resolve this problem, this article proposes application-aware consensus management for software-defined intelligent blockchain in IoT. After analyzing the dynamic management requirements of differentiated consensuses, the architecture of software-defined blockchain is designed. Then the work flow of application-aware consensus and the mechanism of consensus function virtualization are proposed. To provide intelligent scheduling of the virtualized consensus resources, transfer learning is introduced to implement the application-layer packets analysis and provide the feedback to consensus switches. This work provides a novel roadmap for dynamic and intelligent management for blockchains in IoT.

This work implements transfer learning at the SDN controller based on a centralized model. To optimize the performance of the virtualized consensus resources in a decentralized approach, future works will aim to adapt edge artificial-intelligence-technology-based intelligent management for blockchain in IoT.

Acknowledgment

This work is supported by the National Natural Science Foundation of China (Grant no. 61972255 and 61831007), and partially supported by the JSPS KAKENHI Grant Numbers JP16K00117 and JP19K20250, and the KDDI Foundation.

References

[1] C. Xu, K. Wang and M. Guo, "Intelligent Resource Management in Blockchain-Based Cloud Datacenters," *IEEE Cloud Computing*, vol. 4, no. 6, 2017, pp. 50–59.
[2] K. Zhang *et al.*, "Edge Intelligence and Blockchain Empowered 5G Beyond for Industrial Internet of Things," *IEEE Network*, to be published
[3] H. Liu, Y. Zhang, and T. Yang, "Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing," *IEEE Network*, vol. 32, no. 3, May/June 2018, pp. 78-83.
[4] J. Wu *et al.*, "Big Data Analysis-Based Secure Cluster Management for Optimized Control Plane in Software-Defined Networks," *IEEE Trans. Network and Service Management*, vol. 15, no. 1, 2018, pp. 27–38.
[5] S. Luo *et al.*, "A Security Assessment Mechanism for Software-Defined Networking-Based Mobile Networks," *MDPI Sensors J.*, vol.15, no.12, 2015, pp 31,843–58.
[6] B. Jaeger, "Security Orchestrator: Introducing a Security Orchestrator in the Context of the ETSI NFV Reference Architecture," *Proc. 2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, 2015.
[7] Y. Gu *et al.*, "Joint Radio and Computational Resource Allocation in IoT Fog Computing," *IEEE Trans. Vehic. Tech.*, vol. 67, no. 8, 2018, pp. 7475–84.
[8] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?" *IT Professional*, vol. 19, no. 4, 2017, pp. 68–72.
[9] P. Dunphy and F. A. P. Petitcolas, "A First Look at Identity Management Schemes on the Blockchain," *IEEE Security & Privacy*, vol. 16, no. 4, 2018.
[10] F. R. Yu *et al.*, "Virtualization for Distributed Ledger Technology (vDLT)," *IEEE Access*, vol. 6, 2018, pp. 25,019–28.
[11] Y. Dai *et al.*, "Blockchain and Deep Reinforcement Learning Empowered Intelligent 5G Beyond," *IEEE Network*, vol. 33, no. 3, May/June 2019, pp. 10–17.
[12] J. Wu *et al.*, "Fog Computing Enabled Cognitive Network Function Virtualization for Information-Centric Future Internet," *IEEE Commun. Mag.*, vol. 57, no. 7, July 2019, pp. 48–54.
[13] V. Jayaram *et al.*, "Transfer Learning in Brain-Computer Interfaces," *IEEE Computational Intelligence Mag.*, vol. 11, no. 1, 2016, pp. 20–31.
[14] W. Dai *et al.*, "Boosting for Transfer Learning," *Proc. 24th Int'l. Conf. Machine Learning*, Corvalis, OR, 2007.
[15] B. Hamdaoui, N. Zorba, and A. Rayes, "Participatory IoT Networks-on-Demand for Safe, Reliable and Responsive Urban Cities," *IEEE Blockchain Technical Briefs*, 2019.

Biographies

Jun Wu received his Ph.D. degree in information and telecommunication studies from Waseda University, Japan, in 2011. He was a postdoctoral researcher with the Research Institute for Secure Systems, National Institute of Advanced Industrial Science and Technology (AIST), Japan, from 2011 to 2012. He was a researcher with the Global Information and Telecommunication Institute, Waseda University, from 2011 to 2013. He is a visiting researcher at the Muroran Institute of Technology, Japan, from January to February 2019. He is currently an associate professor of the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, China.

Mianxiong Dong received B.S., M.S., and Ph.D. degrees in computer science and engineering from the University of Aizu, Japan. He is currently the vice president and a professor of Muroran Institute of Technology, Japan. He serves as an Editor for *IEEE Communications Surveys & Tutorials*, *IEEE Network*, and *IEEE Wireless Communications Letters*.

Kaoru Ota received her M.S. degree in computer science from Oklahoma State University in 2008, and her B.S. and Ph.D. degrees in computer science and engineering from the University of Aizu in 2006 and 2012, respectively. She is currently an associate professor with the Department of Information and Electronic Engineering, Muroran Institute of Technologyn. She serves as an Editor for *IEEE Communications Letters*.

Jianhua Li got his B.S., M.S., and Ph.D. degrees from Shanghai Jiao Tong University in 1986, 1991, and 1998, respectively. He is currently a professor/Ph.D. supervisor in the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University. He got the Second Prize of the National Technology Progress Award of China in 2005.

Wu Yang received his Ph.D. degree in computer system architecture specialty from the Computer Science and Technology School, Harbin Institute of Technology. He is currently a professor and a doctoral supervisor at Harbin Engineering University.