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

著者	WU Jun, DONG Mianxiong, OTA Kaoru, LI Jianhua, YANG Wu
journal or publication title	IEEE NETWORK
volume	34
number	1
page range	69-75
year	2020
URL	http://hdl.handle.net/10258/00010327

doi: info:doi/10.1109/MNET.001.1900179

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

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

Abstract— **Currently, Internet of Things (IoT) has become a 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 following challenges. Dynamic management and configuration of the consensuses in a blockchain are required due to the IoT applications have high dynamics. Moreover, a IoT node is usually reutilized by various applications in different blockchains, which leads 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, consensus function virtulization approach with application-aware work flow are proposed, which can abstract and manager various consensus resources. Next, a transfer learning based intelligent scheme is deigned 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 to enhance the flexibility and extendibility of blockchains in IoT.**

Index Terms—**Blockchain, internet of things (IoT), consensus, virtualization.**

I. 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 the Merkle tree. In addition, the transaction information is verified against the results of the data, such as the Merkle certificate. Moreover, a smart contract is an executable layer that is agreed in advance to the transaction and submitted to the blockchain by both parties. The blockchain can automatically execute smart contracts for the corresponding transactions. Due to the constraints of the resource in IoT, most of the current blockchains in IoT have constraints on the throughput of transactions. In fact, it is necessary to implement the cross-chain collaborations and interaction among different blockchains, especially in the era of Internet of Everything (IoE).

At the same time, Internet of Things (IoT) has been widely used in environment monitoring, intelligent transportation, e-health, Industry 4.0, etc. Blockchain enables trustless networks that provide secure peer-to-peer transactions in IoT without a trusted intermediary. In other word, the secure and unchangeable storage in blockchain guarantees the reliability and traceability of the data in IoT. Moreover, blockchain-based IoT eliminates singular points of failures in centralized networking structure of IoT. In IoT, some strong sensor node and networking interface module/node can be used to mine, which makes blockchain can be deployed at edge of the network and enhance the security of IoT. This has become a important development trend of blockchains. Please refer to following revision in the revised manuscript [2]. It is estimated that almost 50 billion devices will be interconnected by 2020, which makes the various IoT services grows very rapidly. The IoT users in "smart city" usually have dynamical requirements for one application. For instance, a doctor usually needs 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 is a must. Morevoer, a IoT node are usually reutilized by various applications, such as transportation control, weather forecast, 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, the low-complexity consensus mechanisms (e.g. proof-of-stake) are utilized to provide the low-latency industrial service. In trading systems of Industry 4.0, blockchain applications typically employ the proof-of-work (PoW) consensus mechanism to ensure trustworthy of transactions. If the Industry 4.0 node cannot switch between aforementioned differentiate

Jun Wu, Jianhua Li are with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, China.

Mianxiong Dong and Kaoru Ota are Department of Information and Electric Engineering, Muroran Institute of Technology, Muroran, Japan.

Wu Yang is with Information Security Research Center, Harbin Engineering University, Harbin, China.

Corresponding author: Mianxiong Dong, E-mail: mx.dong@csse.muroran-it.ac.jp

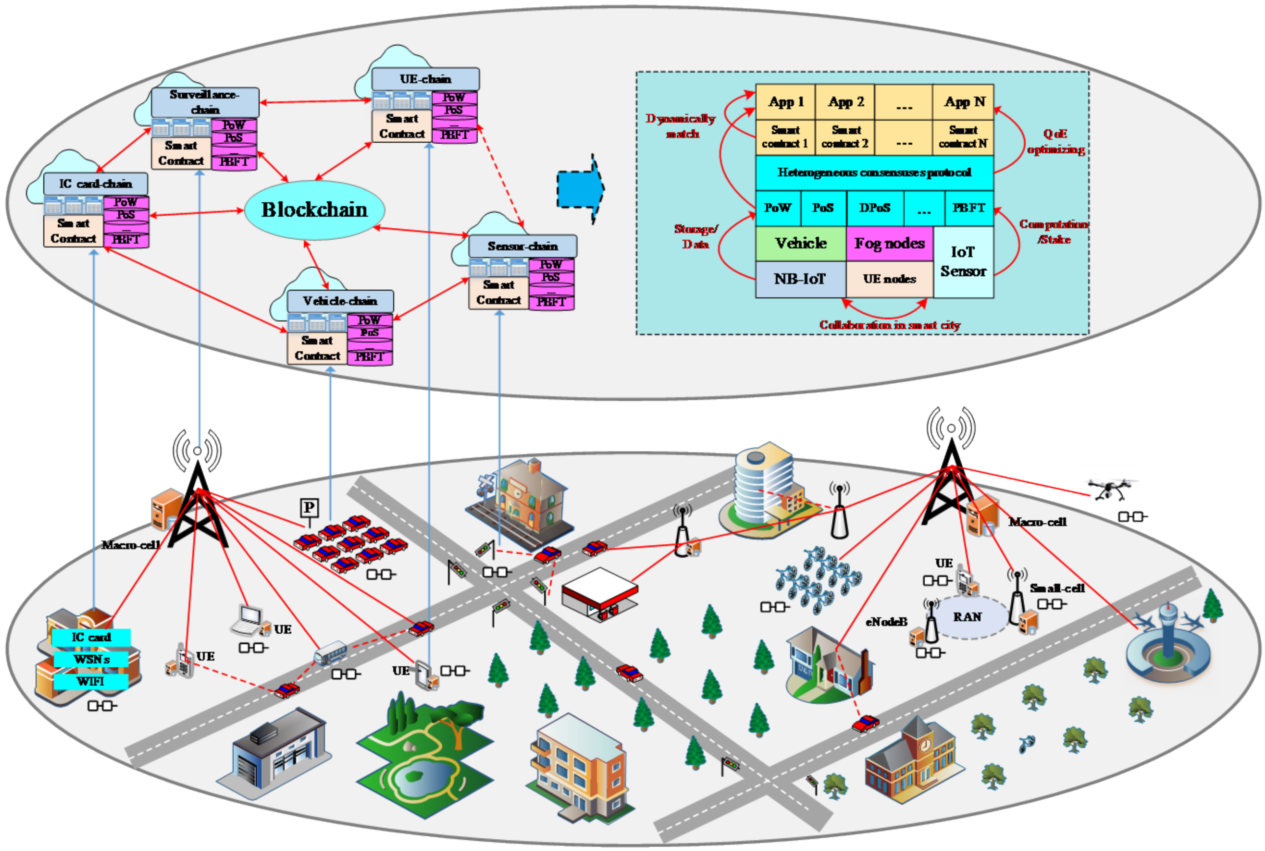


Fig. 1. Scenario of dynamic management of blockchain in IoT.

consensuses, it cannot be reutilized in both smart factory and trading. The drawback is that the processes of smart factory and trading cannot be are integrated efficiently. Similarly, a camera at the roadside can be used by both the intelligent transportation systems (ITS) and security surveillance [3]. Therefore, when the IoT services are switched among different application systems, the requirements of the consensus are differentiated. In other word, the consensuses of the blockchain in IoT should be switched dynamically to match the upper-layer applications. Thus the dynamic switch among heterogeneous consensuses of different applications should be provided. Based on aforementioned motivation, a dynamic and intelligent management approach for blockchain is a must, which can provide application-aware capabilities for heterogeneous consensuses. The application scenario and motivation of this paper are shown in Fig. 1.

On the other hand, software-defined networking (SDN) has been applied as the novel network architecture. In SDN, the network is decoupled into control plane and data plane, which makes the underlying networks and components programmable [4][5]. Meanwhile, an Industry Specification Group called ETSI Network Function Virtualization (ETSI NFV) has specified the virtualization of network elements [6]. In ETSI NFV, Reference Architecture by the Management and Orchestration (MANO) is defined for the resources 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 aforementioned challenges, this paper 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 manage and control dynamically 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 paper is organized as follows. Section II analyzes related works. In section III, the analysis of blockchain and consensuses in IoT is presented. Section IV gives the details of software-defined blockchain and consensus function virtualization. The application-aware intelligent scheduling scheme for virtual consensus functions is given in Section V. Finally, Section VI concludes this paper.

II. Related Works

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

Current, some existing works focus on the management approaches of blockchains. To resolve the problem of energy-aware resource management in cloud datacenters, a robust decentralized resource management framework was proposed and the energy consumed by the request scheduler can be saved for blockchain-based cloud datacenters [1]. Moreover, a distributed ledger technology based consuming identity management was proposed [9]. However, the dynamic management studies for blockchains are rare, especially for blockchains in IoT. A dynamic distributed storage was proposed for blockchains, in which secret key sharing, private key encryption, 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]. Aforementioned works just consider the storage and distributed ledger management for common blockchians. Dynamic management and configurations of blockchain in IoT is still an open issue.

III. 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 which can be used in different IoT applications. Poof of Work (PoW) is a kind of consensus of 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. Proof of Stake (PoS) can be implemented based on the IoT users' own privilege to determine who can construct the next block in the blockchain. For the IoT node with higher privilege, the probability of constructing next block is higher. The 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 replicates copies on different nodes. There are also some other novel consensuses to verify that certain concepts or theories to model real applications. For example, the proof of concept (PoC) has attracted a lot of attentions. Specially, in the transaction, PoC refers to partial solutions involving a small number of users to verify whether a system satisfies certain requirements.

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

IV. Software-Defined Blockchain And Consensus Function Virtualization Architecture In Iot

A. *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 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, exiting switch technologies have limited scalability and robustness in handling more than two devices or communication models without SDN control plane. Second, control plane supports unprofessional IoT users configure network resources accurately and efficiently. Third, 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 provide the virtual functions of the blockchain resources in IoT, which is controlled and scheduled by the blockchain control layer. Moreover, the IoT application configuration layer provide the differentiated application aware information for the blockchain control layer. First, in the blockchain NFVI layer, hetegeneous consensuses are virtualized as various Virtual Network Functions (VNFs), such as PoW_VNF, PoS_VNF, PoC_VNF, etc. All the VNFs can be configured by the NFV Orchestrator, which can orchestrate the consensuses based on the applications. The consensus VNFs are in charged by a VNF manager. In addition, the resources of data layer of the blockchain, including blockchain data, chain structure, digital signature, hash function Merkle tree and aysmmetric encryption, are virtualized through virtualisation 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, flow tables are deployed in SDN controller. The VNF discovery component provides the capabilities of search blockchain and network VNF, which are suitable for the applications. When a new VNF is presented in the blockhain system, VNF registration component managers 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. Blockchain abstraction component is used to provide the abstract and formal model of blockchain related resources. Other traditional components are also involved in SDN controller, including flow table, VNFs of networking control and abstraction. Third, in the IoT application configuration layer, the important proposals in SDN controller, smart contract and incentives are embedded in northbound interface, which interacts with IoT applications.

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

Smart contract is a modular of blockchain, which is registered when the blockchain is deployed. To ensure the reliability of smart contract, data related to a specific smart contract (e.g., inputs, outputs, smart contract codes, etc) will be audited the blockchain nodes. Basically, in the proposed architecture, the smart contract is decoupled independently from the consensuses.

B. *Work Flow of Application-Aware Consensus*

Current blockchain in IoT still regards the system as a set of devices rather than a holistic resources. Moreover, the IoT system cannot monitor the application-layer behaviours for the dynamical 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 is 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 get a packet, the matching implementation will be started based on flow table. The packet will be sent to the SDN controller, in case that there is no contain Layer-7 (L7) metadata matching reasonable flow table. Next, DPI based application-aware module will inspect the packet. Intelligent packet analysis provides intelligent consensus configuration for the software-defind blockchain, in which machine learning will be used as the analysis algorithm.

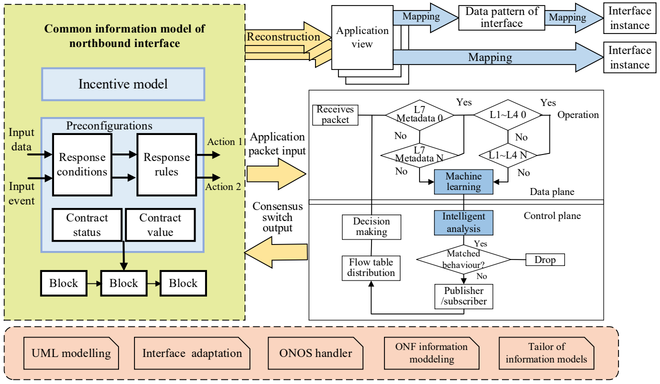


Fig. 2. Work flow of application-aware consensus.

C. *Principal 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 dynamical configuration of application-aware bolockchain 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, virtual machine (VM), etc. Because the implementation of docker in sensors has been proven, the consensus function virtualization is realized based docker technology, which is an open source container engine. The independent implementation environment are provided based on sandbox mechanism.

V. Application-Aware Intelligent Management For Virtual Consensus Functions

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

Machine learning and cognitive model are feasible to be used 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 feasible approach to implement the intelligent analysis and provide the results to the dynamic consensuses management and selection. Because there are different distributions between the test and training data in application environments of blockchain in IoT, a lot of traditional machine learning schemes cannot be applied directly.

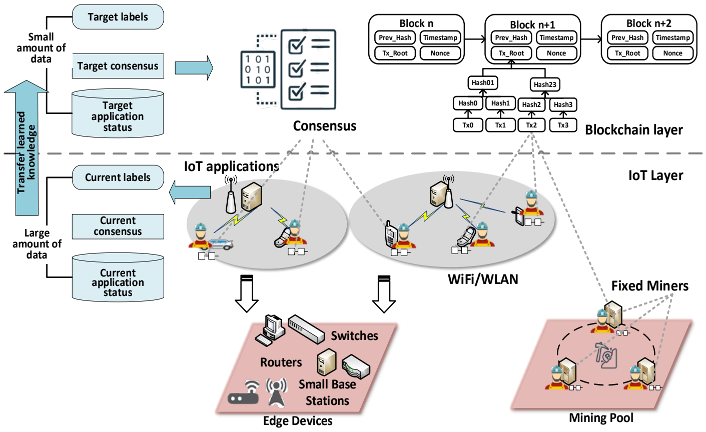


Fig. 3. Intelligent management scheme for software-defined blockchain.

To resolve aforementioned problem, transfer learning [13] is introduced and adapted to realized 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 as 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, there are just a small part of the current packets with the same distribution of the historical packet data of IoT applications. Therefore, the accurate classification and analysis cannot be implemented and enough training packet data are needed for IoT application packets. In the blockchain application environments in IoT, transfer learning based intelligent management approach constructs and store 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 consensus. TrAdaBoost [14] based transfer learning is used in the proposed scheme. The learning frame is a promotion of traditional AdaBoost algorithm, which is used to improve the classification accuracy of a weak classifier. Assumes 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 pre-trained model is established for current consenssus. The key principle here is to leverage the pre-trained model's weighted layers to extract features but not to change the weights of the model's layers during training with further IoT applicatoin 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 the suitable virtual consensus functions. Thus the consensus can be configured dynamically.

VI. Evaluations

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

A. Experimental Setup

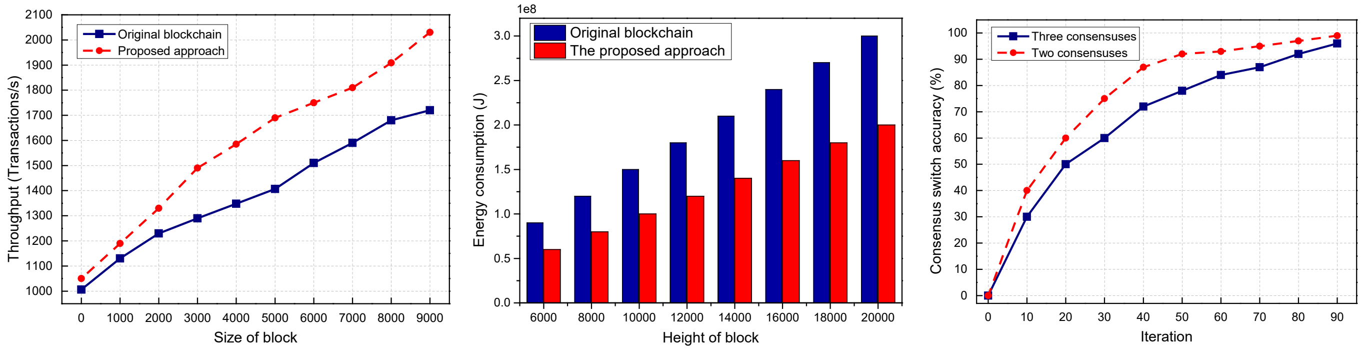
Some simulations and experiments approaches for blcokchain based IoT can be referred[15]. The experimental environment includes three parts: sensor networks in IoT, SDN controller and IoT clients.

For 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 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 the one hand, the site interface receive data from SDN controller and send control commands to 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 their attributes can be used. The IoT user can get the information of 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, the attributes of each sensor, and here we can switch each sensor in IoT. This flexible interface provide the interaction approach between the use and the lower-layer blockchain SDN controller and sensors.

We use Raspberry Pi 3 Model B+ as the implementation devices 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 rang. The SoC architecture is Cortex-A53 (ARMv8) 64-bit, which is embedded in BCM2837B0 mainboard. And Raspberry Pi 3 Model B+ is also equipped with 1.4GHz CPU and 1GB LPDDR2 SDRAM. Besides, it also supports 2.4GHz and 5GHz IEEE 802.11.b/g/n/ac wireless LAN and Bluetooth 4.2. In the experiment, 2.4GHz IEEE 802.11n is used as the wireless links to organize the network of blockchain in IoT. For the operation system,we use the Centos because it is more stable and reliable than Raspbian. In the proposed architecture, SDN controller 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, adapted 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 include mib2c, net-snmp-config.

Each virtualised 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. 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 test-bed. Devices with Inter-Integrated Circuit (I2C) interface includes 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 General Purpose Input Output (GPIO) interface includes button, light-emitting diode (LED), buzzer, relay, infrared sensor etc.

We use several routers to build the experimental IoT environments. The SDN controllers are connected to each other. The blockchain virtualised infrastructure manager is only connected to the corresponding SDN controller while



(a) Throughput of transactions.

(b) Energy consumption.

(c) Consensus switch accuracy over time.

Fig. 4. Experimental results.

one controller can connect multiple virtualised infrastructure managers. We uses 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 virtualised infrastructure manager uses real-time sensors, general-purpose input/output (GPIO), and a sensor library in python, to collect data such as temperature, humidity, atmospheric pressure, and acceleration, and returns these data to SDN controller based on the SNMP protocol.

To enable the IoT client side to obtain information about the blockchain virtualised 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 with the ID of each blockchain virtualised infrastructure manager device which is connected to the SDN controller device. This allows the client to accurately find the desired virtualised infrastructure manager device. Then the following three bits is correspond with the value of the virtualised infrastructure manager itself, including the state of the CPU and memory (e. g. 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 Sheets (TEDS) formats are implemented, such as Meta TEDS, PHY TEDS, sensor channel TEDS. The three-bit extension starting with ".1" is 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(R) Xeon(R) E5620 CPU (2.40 GHz), a bandwidth capacity of 1000 Mbps, 16 G memory and 500 G disk. In addition, S12700 SDN switch is used. Both flow tables and transfer learning are deployed in SDN controller. three kinds of consensus cases are deployed, which are PoW, PoS and PBFT, to evaluate the management of differentiated blockchains. PoW, PoS and PBFT are corresponding with the trading, sensing and data exchange applications in IoT. PoW is used as the intial 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.

B. *Experiment Results*

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

The comparisons of the throughput of transactions is shown in Fig. 4(a), where we take the size of block 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 for 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 traditonal blockchain architecture are shown in Fig. 4(b). 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 resources-restrained IoT. The Transfer learning based consensus switch accuracy over time is shown in Fig. 4(c). The accuracy increase when the number of iteration of transfer learning are increase. Moreover, after 80 iterations, the accuracy of both the cases of two and three consensus exceed 90%. Basically, the change of the consensus algorithm will somehow enhance the energy and resource consumption of the IoT node. However, the efficiency of blockchain implementation can be improved.

VII. 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. The flexible and intelligent consensus management is a must for blockchain in IoT. To resolve this problem, this paper proposed an 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 was designed. Then the work flow of application-aware consensus and the mechanism of consensus function virtualization were proposed. To provide the intelligent scheduling for the virtualized consensus resources, transfer learning was introduced to implement the application-layer packets analysis and provide the feedback to consensus switches. This work provide a novel roadmap for dynamic and intelligent management for blockchains in IoT.

This work implement 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 National Natural Science Foundation of China (Grant No. 61972255 and 61831007) and partially supported by the JSPS KAKENHI Grant Number JP16K00117, JP19K20250 and 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, pp. 50-59, 2017.

[2] K. Zhang, Y. Zhu, S. Maharjan, and Y. Zhang, "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, pp. 78-83, 2018.

[4] J. Wu, M. Dong, K. Ota, J. Li, Z. Guan, "Big Data Analysis-Based Secure Cluster Management for Optimized Control Plane in Software-Defined Networks," IEEE Transactions on Network and Service Management, vol. 15, no. 1, pp. 27-38, 2018.

[5] S. Luo, M. Dong, K. Ota, J. Wu, J. Li, "A Security Assessment Mechanism for Software-Defined Networking-Based Mobile Networks," MDPI Sensors Journal, vol.15, no.12, pp 31843-31858, 2015.

[6] B. Jaeger, "Security Orchestrator: Introducing a Security Orchestrator in the Context of the ETSI NFV Reference Architecture," In Proc. 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 2015.

[7] Y. Gu, Z. Chang, M. Pan, L. Song and Z. Han, "Joint Radio and Computational Resource Allocation in IoT Fog Computing," IEEE Transactions on Vehicular Technology, vol. 67, no. 8, pp. 7475-7484, 2018.

[8] N. Kshetri, "Can blockchain strengthen the Internet of Things?," IT Professional, vol. 19, no. 4, pp. 68-72, 2017.

[9] P. Dunphy, 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, J. Liu, Y. He, P. Si, and Y. Zhang, "Virtualization for Distributed Ledger Technology (vDLT)," IEEE Acess, vol. 6, pp. 25019-25028, 2018.

[11] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He and Y. Zhang, "Blockchain and Deep Reinforcement Learning Empowered Intelligent 5G Beyond", IEEE Network, vol.33, no.3, pp. 10-17, 2019.

[12] J. Wu, M. Dong, K. Ota, J. Li, W. Yang and M. Wang, "Fog Computing enabled Cognitive Network Function Virtualization for Information-Centric Future Internet," IEEE Communications Magazine, vol. 57, no. 7, pp. 48‑54，2019.

[13] V. Jayaram, M. Alamgir, Y. Altun, B. Scholkopf, and M. Grosse-Wentrup, "Transfer Learning in Brain-Computer Interfaces," IEEE Computational Intelligence Magazine, vol. 11, no. 1, pp. 20-31, 2016.

[14] W. Dai, Q. Yang, G. Xue, and Y. Yu, "Boosting for Transfer Learning," in Proc. 24th international conference on Machine learning (ICML 2007), Corvalis, Oregon, USA, 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 the Ph.D. degree in information and telecommunication studies from Waseda University, Japan, in 2011. He was a Post-Doctoral 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, Japan, from 2011 to 2013. He is a visiting researcher of Muroran Institute of Technology, Japan, from Jan. 2019 to Feb. 2019. He is currently an associate professor of School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, China.

Mianxiong Dong received B.S., M.S. and Ph.D.in Computer Science and Engineering from The University of Aizu, Japan. He is currently the Vice President and Professor of Muroran Institute of Technology, Japan. Dr. Dong serves as an Editor for IEEE Communications Surveys and Tutorials, IEEE Network, IEEE Wireless Communications Letters.

Kaoru Ota was born in Aizu Wakamatsu, Japan. She received M.S. degree in Computer Science from Oklahoma State University, USA in 2008, B.S. and Ph.D. degrees in Computer Science and Engineering from The University of Aizu, Japan in 2006, 2012, respectively. She is currently an Associate Professor with Department of Information and Electronic Engineering, Muroran Institute of Technology, Japan. She serves as an editor for IEEE Communications Letter.

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

Wu Yang received the 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 with Harbin Engineering University.