Prototype of Multi-Identifier System Based on Voting Consensus

XING Kaixuan[1], LI Hui[1], YIN Feng[1], MA Huajun[1], HOU Hanxu[2], XU Huanle[2],
Yunghsiang S. HAN[2], LIU Ji[1], and SUN Tao[3]

(1. Shenzhen Graduate School, Peking University, Shenzhen, Guangdong 518055, China;
2. School of Electrical Engineering and Intelligentization, Dongguan University of Technology, Dongguan, Guangdong 523808, China;
3. The Network and Information Center of Shenzhen University Town, Shenzhen, Guangdong 518055, China)

Abstract: With the rapid development of the Internet, the expansion of identifiers and data brings a huge challenge to the network system. However, the network resources such as Domain Name System (DNS) are monopolized by a single agency which brings a potential threat to cyberspace. The existing network architecture cannot fundamentally solve the problems of resource monopoly and low performance. Based on the blockchain, this paper designs and implements a new Multi-Identifier System (MIS), providing the analysis and management for different identifiers in the multi-identifier network. Our preliminary emulation results prove the correctness and efficiency of the algorithm. Besides, the prototype system of MIS has been tested on the real operators' network, realizing the function of co-governing, security supervision and data protection.

Keywords: blockchain; multi-identifier; co-governing

DOI: 10.12142/ZTECOM.202001003

http://kns.cnki.net/kcms/detail/34.1294.tn.20200318.0955.002.html, published online March 19, 2020

Manuscript received: 2019-12-16

Citation (IEEE Format): K. X. Xing, H. Li, F. Yin, et al., "Prototype of multi-identifier system based on voting consensus," *ZTE Communications*, vol. 18, no. 1, pp. 07 – 17, Mar. 2020. doi: 10.12142/ZTECOM.202001003.

1 Introduction

In nearly half a century, the Internet has experienced rapid development from simplicity to complexity. As the main carrier of cyberspace, the Internet plays a significant role in human life, social activity and even national security. However, serious problems such as resource exhaustion and poor business adaptability of the Internet network appear with the rapid development of big data and cloud computing. The semantic overload of IP address also reduces its scalability and mobility that further hinders security. In addition, under the existing system, the network resources such as Domain Name System (DNS) are monopolized by a single agency which brings a potential threat to cyberspace. Besides, malicious network users adopt a series of technical methods to hide individual IP address to escape the supervision and sanctions of the service provider. The content published by the malicious user is difficult to be discerned. These problems such as poor security and weak controllability under the traditional IP system need to be solved urgently.

To decentralize the management of the network architecture, blockchain [1] and other solutions [2] – [6] have recently been applied to build a future network realizing co-governing.

This work is supported by PCL Future Regional Network Facilities for Large-scale Experiments and Applications under Grant No. PCL2018KP001; Natural Science Foundation of China (NSFC) under Grant No. 61671001; Guangdong Province R&D Key Program under Grant No. 2019B010137001; National Keystone R&D Program of China under Grant No. 2017YFB0803204; Shenzhen Research Programs under Grant No. JSGG20170824095858416, JCYJ20190808155607340, and JCYJ20170306092030521; the Shenzhen Municipal Development and Reform Commission (Disciplinary Development Program for Data Science and Intelligent Computing).

Namecoin [7] and Blockstack [8] first applied blockchain to decentralize the management of the domain name system. However, in its underlying system based on public blockchain exists a bottleneck for its performance. To solve the problem, BENSHOOF et al. proposed an alternative solution of the DNS system based on blockchain and a distributed hash table named 3 [9], which provides solutions to current DNS vulnerabilities such as Distributed Denial of Service (DDoS) attacks. However, it risks leaking users' IP information and increases the difficulty of large-scale deployment. To mitigate the problem, the HyperPubSub system [10] uses the passive publish/subscribe receiving mode to reduce the traffic load and the delay caused by blockchain.

The above methods improve the performance of network and level of decentralization, respectively, but are unable to meet requirements [11] simultaneously. Our preliminary work proposed a new architecture: Multi-Identifier Network (MIN) [12] that constructs a network layer with parallel coexistence of multi-identifiers, including identity, content, geographic information and IP address. To solve the two major defects of the traditional network, we decentralize the identifier management by using consortium blockchain. This paper proposes a voting consensual-based multi-identifier management system Multi-Identifier System (MIS). MIS is a decentralized system composed of software and servers providing unified identifiers registration generation, classification, storage and management for identity, content, IP and other identifier spaces through the consortium blockchain Proof of Vote (PoV) [13]. Moreover, the MIS implements the digital signature to enhance security supervision and data protection.

The following chapter structures as follows. Section 2 introduces the MIN architecture. Section 3 describes the management system MIS and key technologies. Section 4 describes and analyzes the system flow of MIS, Section 5 shows the function realization and simulated verification of the prototype system, and Section 6 provides some concluding remarks and discusses ongoing and future research directions.

2 Architecture

2.1 Overview of Multi-Identifier Network

For the co-governing MIN, its decentralized management and large resolution capability enables a progressive transition from the existing network architecture to a new one.

MIN supports the coexistence of network identifiers including identity, content, geographic information and IP address. Identifiers in the network are identity-centric. All the resources are bound to the identity of their publishers. The architecture of MIN is shown in **Fig. 1**.

Fig. 2 shows the network hierarchy of MIN. It divides the whole network into hierarchical domains from top to bottom. The nodes in the top-level domain belong to the organizations of the major countries maintaining a consortium blockchain. The respective regional organizations govern the other domains. Among them, the registration and management mode of identifiers and the specific implementation details can vary. This low coupling guarantees the security of the network and enables the customization of each domain [13], [14].

The functions of a completed node in the network participate in the intra-domain management of users and the registration process of identifiers on the blockchain, as well as provide inter-translation and resolution services. In addition, there are supervisory nodes, individual users and enterprise users. Supervisory nodes are set up as the data access interfaces between the upper and lower domains. Each supervisory node has multiple identifiers.

The architecture of MIN includes a management plane and a data plane. The management plane supports traceable data signing and checking mechanism. The data plane provides the resolution for identity, content, geographic information and other identifiers. In addition, the data plane is responsible for packet forwarding and filtering. The reason for storing only the important data on-chain is to ensure efficiency, while all the information of the identifiers is stored off-chain.

2.2 Overview of Multi-Identifier System

The MIS we proposed in this paper is responsible for the generation and management of identifiers in the management plane. All user and publication resources are required to register their identifiers with the supervisory nodes. The supervisory nodes verify the identifier and reach a consensus through the consensus algorithm. It records the relevant attribution information and operation information on the blockchain to make the data in the whole network unified, tamper-resistant and traceable. All resources are required to register an identifier with a regulatory organization within the domain. Users can only access a resource in the network when its identifier has been approved by most organizations and successfully written on the blockchain. Meanwhile, the MIS uses a digital signature scheme that has the advantages of autonomy, uniqueness, security and traceability.

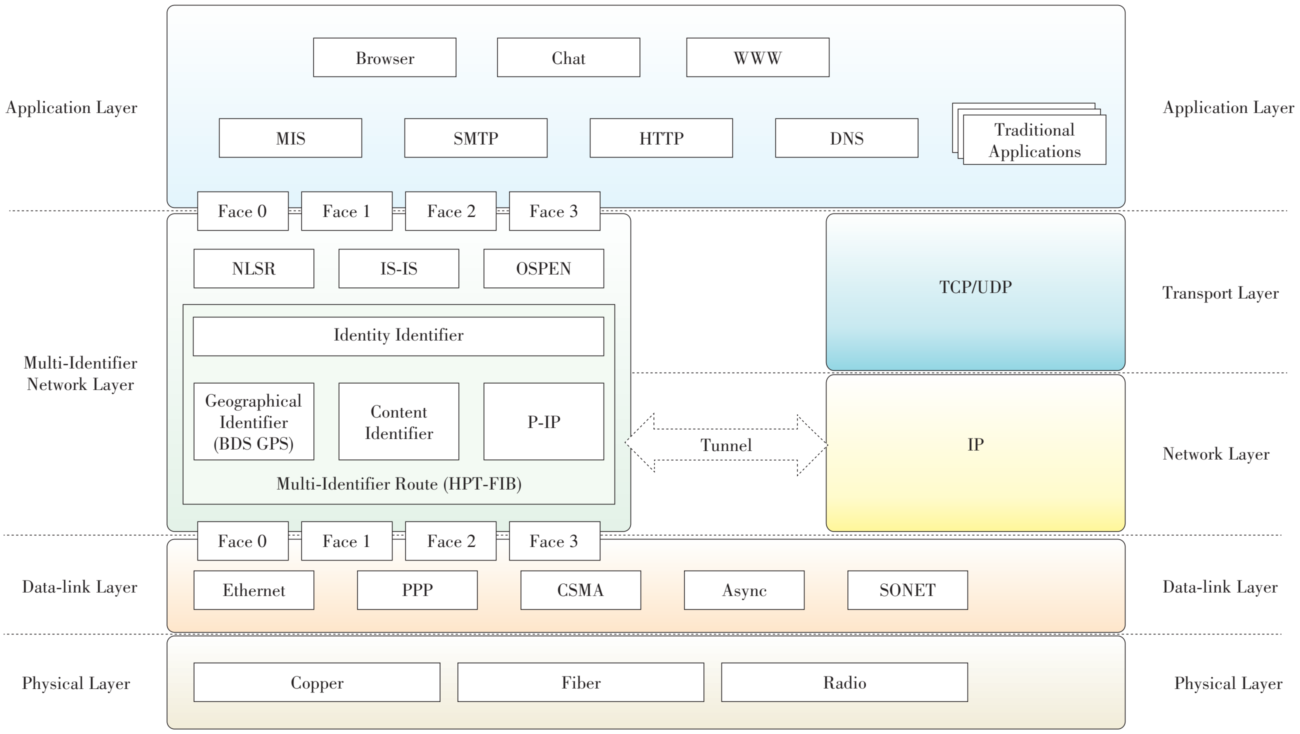
1) Autonomy.

The registration of identifiers is based on decentralized blockchain technology. The user independently defines the application for registration prefix on the premise of legal non-repetition. Besides, the registration and management rules are open, and there is no centralized control organization.

2) Uniqueness.

Real identity information such as biological information and ID number is registered to generate prefix to ensure uniqueness. Meanwhile, each user can use a prefix to identify the published resources, so that the users can identify and obtain the resource accurately.

3) Security and traceability.



BDS: Beidou Navigation Satellite System
CSMA: Carrier Sense Multiple Access
DNS: Domain Name System
FIB: Forwarding Interest Base
GPS: Global Positioning System
HPT: Hash Table And Prefix Tree
HTTP: Hypertext Transfer Protocol
IP: Internet Protocol
IS-IS: Intermediate System-to-intermediate System
MIS: Multi-Identifier System
NLSR: Named-Data Link State Routing Protocol
OSPF: Open Shortest Path First
OSPFN:Ospf Based Routing Protocol For Named Data Networking
PPP: Point To Point Protocol
SMTP: Simple Mail Transfer Protocol
SONET: Synchronous Optical Network
TCP: Transmission Control Protoco
UDP: User Datagram Protocol
WWW: World Wide Web

▲Figure 1. The architecture of Multi-Identifier Network.

The prefix name must be registered and generated with real ID information to ensure that the identity of the content publisher is authentic and reliable. In addition, registration is successful only when an identity has been approved by most institutions and successfully written into the blockchain. Users who have successfully registered must use prefixes to publish content identification, and resource-publishing operations need to add user signature information. After receiving the request for publishing resources, blockchain verifies the user through signature to ensure that the resources published in the network space are safe and reliability. At the same time, the prefix name of content realizes network supervision by tracing resources to publishers.

MIS manages users' behaviors of publishing and access permission. The blockchain undeniably records illegal actions as well. Therefore, MIS keeps the cyberspace in an orderly and secure state that will direct Internet traffic to the post-IP multi-identifier network.

3 Key Technologies for MIS

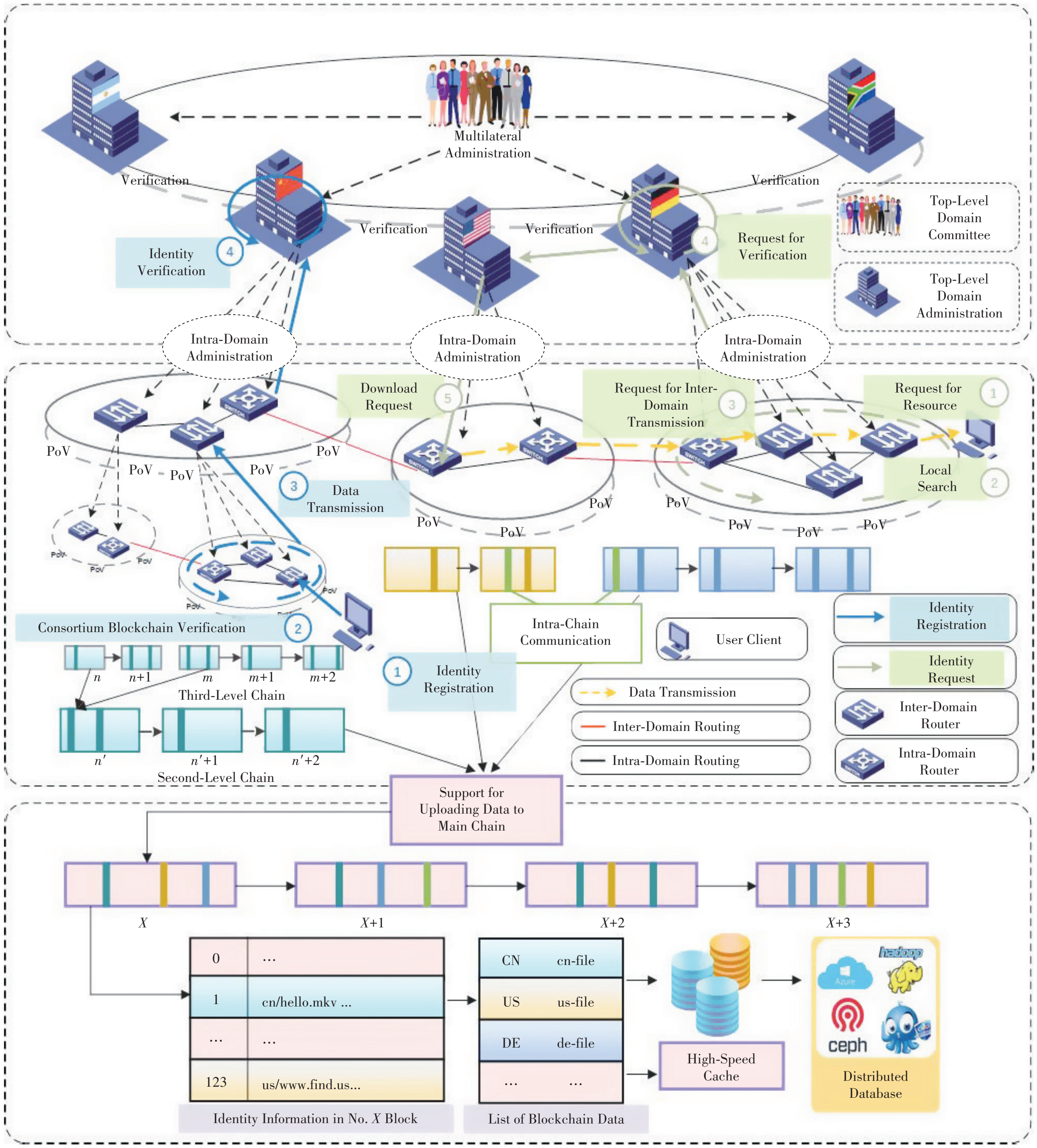
3.1 High-Performance Consensus Algorithm

The MIS system realizes the unified management of identifiers based on the improved PoV consortium blockchain consensus [13], a non-forking consensus algorithm for consortium blockchain. The core lies in the separation of voting rights and butler rights. The butler nodes work in a joint effort to conduct decentralized arbitration according to the votes of the commissioner nodes.

The PoV consensus divides the blockchain nodes into four characters: the commissioner, butler, butler candidate, and ordinary user. Each node has its own public-private key pair and digital certificate based on its identity and account number.

1) Commissioner.

The commissioners come from different regions or institutions maintaining a consortium blockchain together. Commissioners have the right to recommend, vote and evaluate the but-



PoV: Proof of Vote

▲**Figure 2. Multi-Identifier Network management architecture and operation flow.**

lers. They also have the obligation to verify and forward blocks and transactions. A block generated in the blockchain network will be sent to all commissioners for verification. When a block receives at least 51% of the votes, the block will be marked as valid and be added to the blockchain. The result of the voting can represent the will of all the commissioners.

2) Butler.

The butler is responsible for generating blocks in the current consensus round. The number of butlers is limited. A butler gathers transaction information from the network, packs them into a block, and signs the block. At the end of the term, the commissioner votes on the butler candidate to produce the next butler nodes. Besides, a node can be a commissioner and a butler at the same time.

3) Butler candidate.

As the number of butlers is limited, a butler comes from butler candidates by election and all commissioners vote candidates. If a candidate is lost in the election, he can stay online and wait for the next election

4) Ordinary user.

Ordinary users are responsible for processing block distribution and message forwarding if not being authorized. They can join or exit the network anytime without being authorized and their behaviors can be arbitrary.

There are two types of message voting in PoV for the transactions of identifiers and election: verification vote and confidence vote.

1) Vote for block generation.

The butler processes transactions to generate a block then sends it to all commissioners. A commissioner will encrypt the block header and return the signature to the butler if it agrees to produce the block.

2) Vote for confidence.

In the last duty cycle of the term, the commissioner sends signed voting transactions to the butler. After collecting and counting the ballot tickets, the butler generates a special block with election results and related records. Then the butler sends this block to all the commissioners for validation

3.2 Privacy Protection and Identity Management Solution

There are effective solutions to privacy protection in blockchain, but it is unable to achieve effective management of the participating nodes' identity and tracking of their behaviors. This is unacceptable in the MIS where there is a need to manage the behavior of participants.

The MIS provides privacy protection by applying identity management.

Nodes in the domain can be divided into three characters: the ordinary node, butler node and commissioner node according to their different missions. One node can concurrently act as more than one characters (**Fig. 3**). The ordinary nodes in green color have the right-to-know and the right-to-propose but cannot participate in the consensus process. The butler nodes own the rights to the generate blocks. The commissioner nodes have the right to verify the block; they can recommend, verify and evaluate the butler node and participate in consensus on the upper level. The commissioner nodes of the lower domain also act as a character in the upper domain.

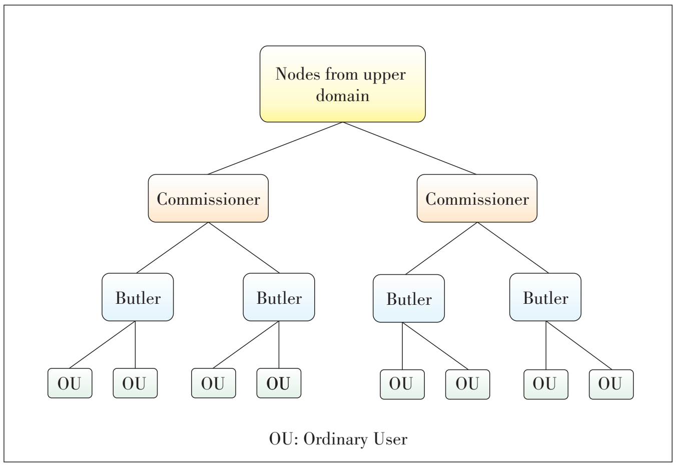
A hierarchical group/ring signature mechanism is used in the MIS due to the different node division. The node signatures in the network form a tree structure, and each parent node regards a group of subordinate nodes as its leaf nodes. The superior signature is generated by the combination of the subordinate signatures. The superior signature contains all the subordinate signature information. The verification of the superior signature also includes the verification of the tree with the signature as the root. Similar to normal group/ring signature requirements, no third party can trace the identity of the signer who has produced the signature with obtained signature and verified the public key. In addition, the security of the hierarchical group signature scheme requires that the group administrator can only trace the signer's leaf nodes' identity, while he/she cannot open the signatures generated by other groups' members. The group administrator of the parent node can quickly locate the problem group and identify the corresponding malicious users by establishing a group relationship between nodes of different levels and characters.

The following specific signature process is shown in **Fig. 4**.

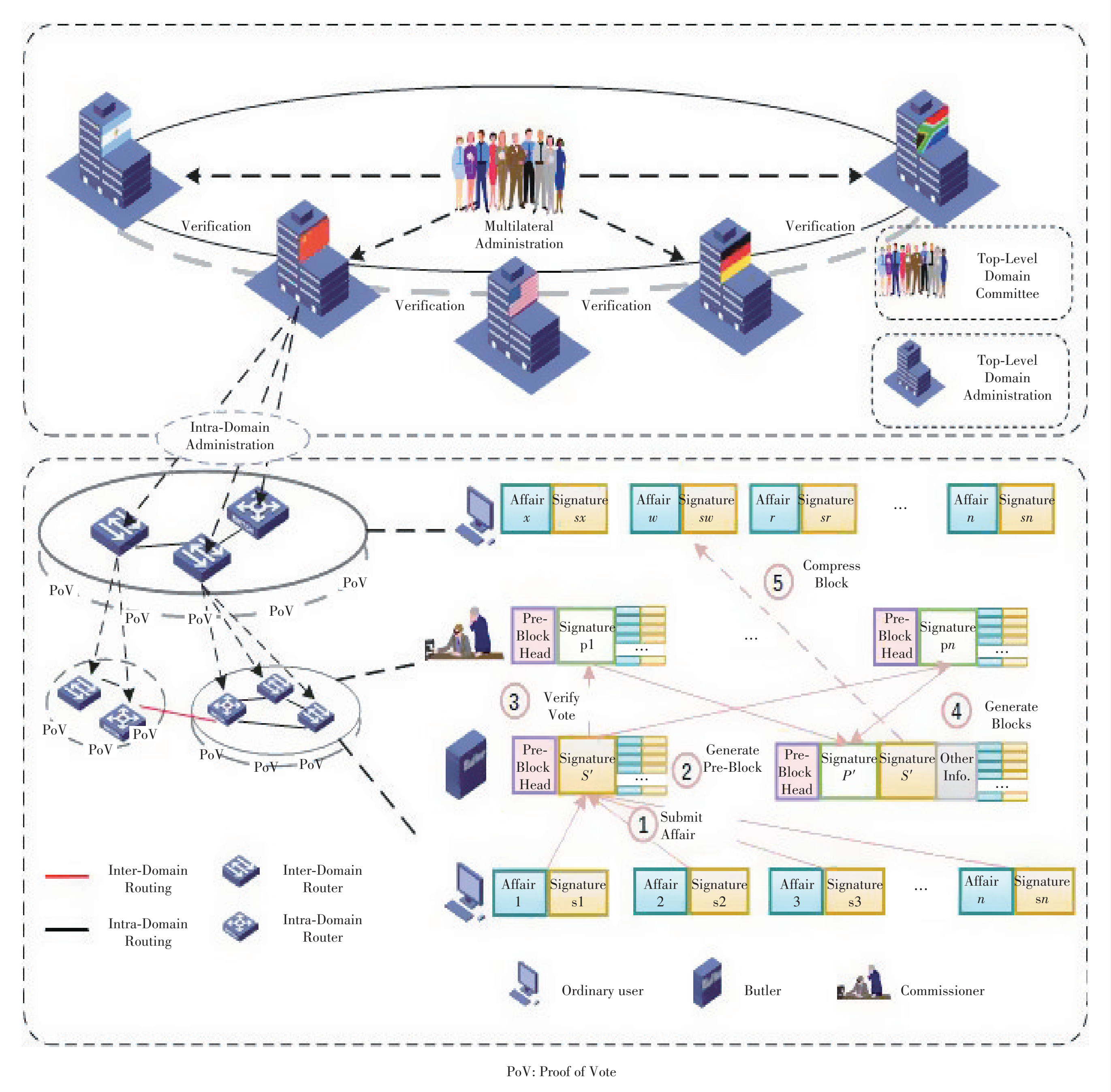
1) An ordinary node in the underlying domain produces a transaction and a signature S. It also receives intra-domain transactions, verifies the correctness of the transaction content and signature, and forwards the transaction to other nodes in the domain if correct. The butler nodes listen on intra-domain transactions and place valid transactions into the transaction pool.

2) The butler nodes periodically take some transactions out of the transaction pool and then encapsulates them into pre-blocks. The pre-blocks group with the ordinary nodes it belonged to generate a new parent group signature S'. S' and the pre-block are sent to all the commissioner nodes and other butler nodes in the domain. Once receiving the new parent group signature S' and the pre-block, the other butler nodes save them.

3) After the commissioner node receives the pre-block, they verify the transaction and butler signature in the pre-block. If it agrees to the generation of this block, it sends back its relat-



▲**Figure 3. Relationship among characters.**



▲**Figure 4. The specific signature processes.**

able ring signature P and timestamp to the butler node.

4) Before the deadline of generating a block, if the number of the commissioners' signatures and time stamps that the butler has received is more than the default value, the butler will generate a new superior ring signature and add it to the head of the pre-block to generate a block. This block will be broadcasted to all domains with block body and signature S'. Otherwise, if the number is no more than the default value or timeout, there will be no block generated in this consensus cycle. The default value can be set in different scenarios.

5) After receiving the block, the commissioner node verifies its signature S' and P', and then removes the transaction contained in the valid block from the transaction pool. If the commissioner nodes are not in the top-level domain, extract the block as a transaction, generate a new superior group signature S'' according to the attached butler signature S', and submit the transaction as an ordinary node of the previous domain. The other superior nodes continue to verify the signa-

ture. Only if the block is in the top-level domain and the number of commissioner nodes is greater than the default value, it will enter the legal state and have the final confirmation.

According to the characteristics of the hierarchical signature scheme, the MIS uses different data structures for block and pre-block (**Tables 1** and **2**).

The multi-identifier management and privacy protection mechanism based on digital signature is the key technology to ensure the security and reliability of the transaction of the consortium chain.

4 Implementation of MIS

1) User registration.

Every blockchain node in the MIS runs a service thread that is used to process requests sent by clients and provide corresponding services. **Fig. 5** describes the full process of user registration including request reception, verification and user registration information saving on the blockchain. User registration involves the communication between clients and blockchain nodes by embedding the user registration into the consensus of blockchain. The commission nodes verify and reach consensus so as to achieve the co-governing function.

The main function of the user client is to generate a pair of public and private keys for the user according to his/her identity. The two keys will be bound and then uploaded to the blockchain. At the same time, the user who publishes the resource will apply for a content name prefix when registering, thus realizing the binding of content identifier and public key. The users who have successfully registered can publish resources using the content name prefix produced through registration. The resource publishing needs to add the user private key information.

When a new user registers for using the network, MIS will require the user to submit the information such as prefix and real identity shown in **Table 3**. According to different security requirements, MIS can dynamically adjust the biometric information recognition strategy. For now, the prototype achieves the function for collecting fingerprint, facial and human iris information.

In particular, the prefix information follows the naming rules for hierarchical network domains. In addition, the system creates a table as shown in **Table 4** to store the successfully registered user information on the blockchain.

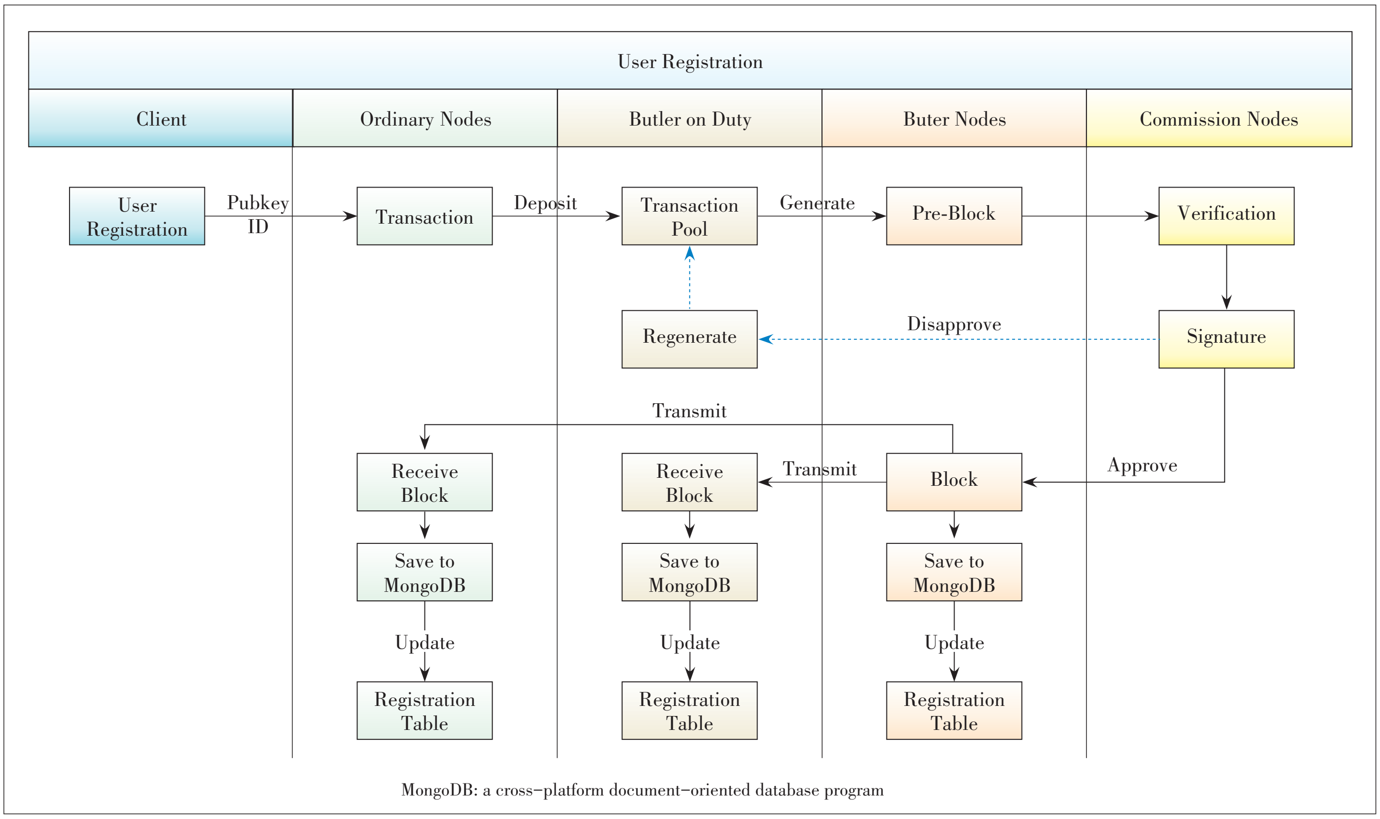
MIS generates a certificate for users once it receives and saves such an application. Then user identity and prefix binding process are completed. All the resources published by, for example, Jason will be located in /Jason. The certificate con-

▼**Table 1. Data structure for block**

Block		
Final-Header		Body
Pre-Header	Contain all property of Pre-Header	$\{tx\} = \begin{Bmatrix} tx_0, \\ tx_1, \\ \cdots, \\ tx_i \end{Bmatrix}$
pre_header_ring_sign $\{\langle C\_time, C\_sign \rangle\}$	The Commissioner node returns the superior ring signature *C_time* is processor timestamp *C_sign* is the commissioner signature of *Pre−header* and *C_time*	
R	Random function obtained using the RandomNum algorithm that determines the butler number for the next block.	
M	The times of cycle to generate a block	
Time	Time of current block	

▼**Table 2. Data structure for pre-block**

Pre-Block		
Pre-Header		Body
Hash	Unique ID of block, Hash the SHA-256	$\{tx\} = \begin{Bmatrix} tx_0, \\ tx_1, \\ \cdots, \\ tx_i \end{Bmatrix}$
Pre-Header	Hash Value of previous block	
Height (h)	The height of current block	
Height *_LastSpecial* *(hs)*	The height of special block next to the current block Especially when $h = hs$, the block is a special block Special block generated every B_w Usually $h - hs \leqslant B_w$	
M	The times of cycle to generate a block	
Puk *(addr)*	Encapsulate the public key of the butler of the current block; used to prove the accounting attribution of the current block	
Merkle_Root	Used to verify primitiveness and authenticity of all transactions	
…	Custom properties section	



▲Figure 5. User registration flow.

tains the user information and will be located under /Jason/cer. Other users who request for /Jason resources will first verify the certification under the /Jason/cer to check whether legal or not. Besides, the user information determines the access permission so as to achieve specific management functions underlying different scenarios.

2) User inquiry.

The user inquiry process consists of receiving the client's query user request, querying the user information from the user information table and returning it to the client. MIS system supports two types of queries: querying the corresponding user information through the user public key and querying all user information.

3) Resource publishing.

The content in the network also follows the rules of prefix names. **Fig. 6** shows the full process of resource publishing. When a user applies to publish content on the network, the published resource will be signed and submitted to the blockchain node for the consensus process. Specifically, the blockchain node that receives the request encapsulates the request in an ordinary transaction, and then several nodes verify and vote on this transaction. If the consensus is agreed, the inter-translated information will be stored in the table shown in **Table 5**.

4) Resource inquiry.

The resource inquiry function receives the client's identifier query request. The request inquires about the real address

▼Table 3. An example of the user application table

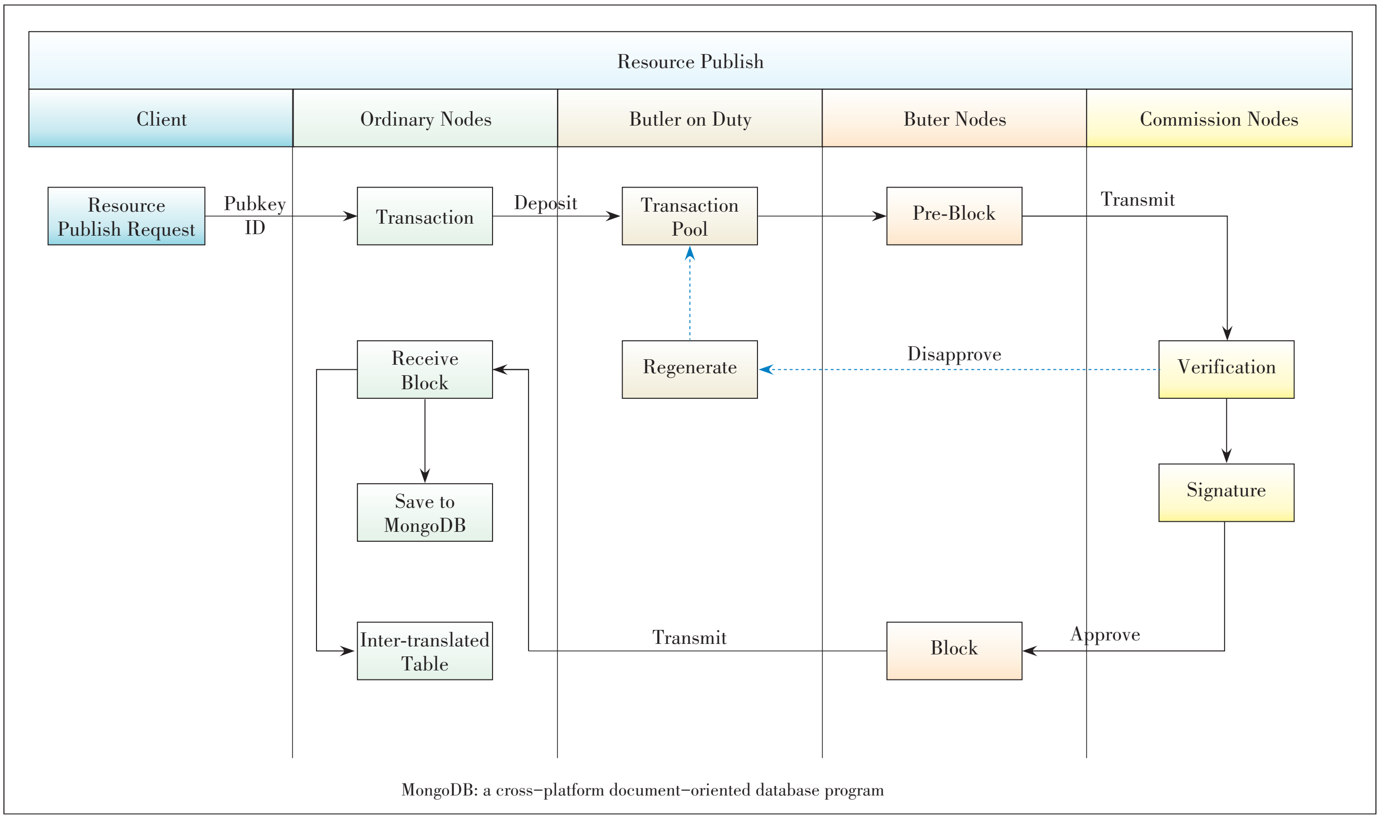
Registration Prefix	/Jason
Name	Jason
Valid ID	E77669818
Public key	54cd12s4d6g9mj
Biometric information	fs283n2n812b59u0sk42
Phone	9876070

▼Table 4. User information table

Key	Value	Description
Pub_KEY	String	Pub key of user
Prefix	String	Identifier prefix
Level	Int	User permission level
Real_msg	String	Real ID
Timestamp	Double	Time

▼Table 5. Content in inter-translation table

Key	Value	Description
Identifier	String	Resource
RealAdd	String	Real Address
Pub_KEY	String	Public Key
Hash	String	Hash Value
Timestamp	Double	Time stamp



MongoDB: a cross-platform document-oriented database program

▲**Figure 6. Resource publication flow.**

corresponding to the inter-translation information table. Similar to the user inquiry, MIS supports two types of queries: querying data by content identity and querying data by the resource publisher's public key.

5 Evaluation

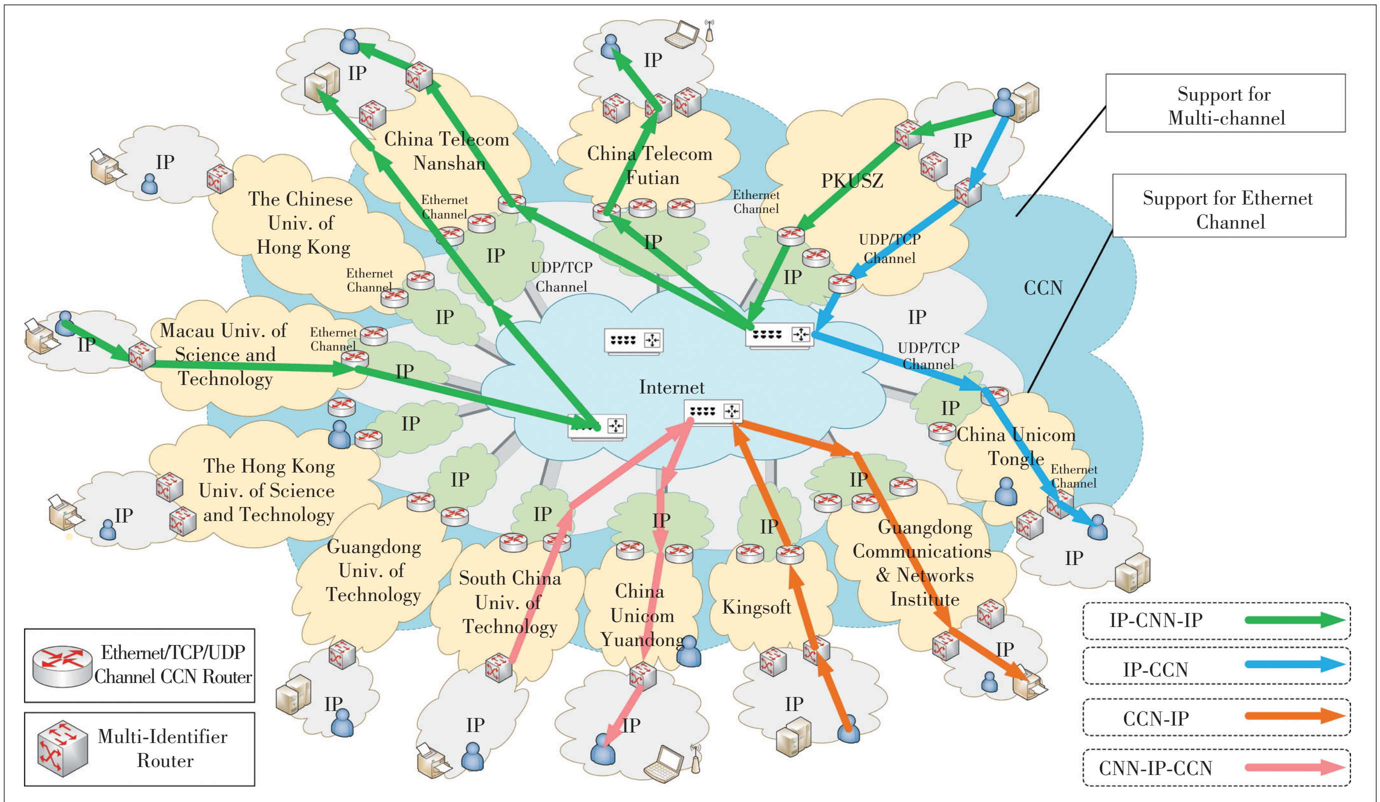
We develop a prototype system for MIS and deploy it on a real carrier-level operators' network consisting of the Chinese mainland and China's Hong Kong and Macao special administrative regions, as shown in **Fig. 7**. The system has realized the binding mechanism of user content and private key signature, as well as the blockchain function module and application function module. The system contains the user client and administrator client.

The main function of the user client is to generate a pair of public and private keys for the user and upload the user ID and public key to the blockchain so that the user ID is bound to the public key. Details are shown in **Fig. 8**. At the same time, the users who publish resources will apply for a content name prefix when registering, achieving the binding of content identifier and public key. The users who have successfully registered can publish content using the content name prefix applied during registration. The resource publishing operation needs to add the user's private key signature information. After the blockchain receives the request to publish the resource, it verifies the user rights through the signature. The signature also binds the user identity to the published content identifier, so as used for the inter-translation of the identity when routing.

The main function of the administrator client of blockchain includes the real-time display of the running state of nodes, querying of blockchain data and configuration of blockchain nodes. Blockchain nodes store the identifier data, the user information stored in the form of transactions in each block. Each registration and publication generate a consensus for the whole network. The consensus is reflected in the number of transactions in the administrator interface that is shown in **Fig. 9**.

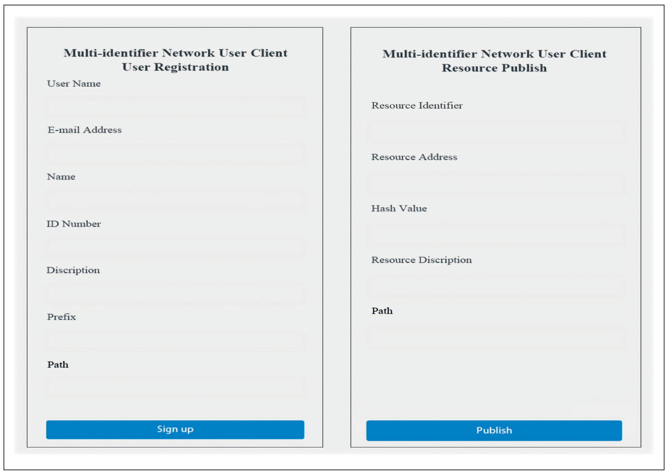
We deployed PoV and Practical Byzantine Fault Tolerance (PBFT) in a distributed environment and measured their throughput Transaction Per Second (TPS) separately. The experimental environment included five servers connected to the same router, each with 128 Gigabytes of memory and an Intel Xeon Silver 4116 processor. The PoV butler node was set to generate six PoV blocks, including five common blocks and one special block, within one service cycle. The theoretical calculation and experimental test results are shown in **Table 6**.

The results show that the performance trends of the two algorithms are consistent with the theoretical values. When the number of nodes is more than 100, the TPS of PoV declines slowly, and the rate of decline is slower than PBFT. Com-


IP
China Telecom Nanshan
China Telecom Futian
PKUSZ
Support for Multi-channel
Support for Ethernet Channel
CCN
The Chinese Univ. of Hong Kong
Ethernet Channel
UDP/TCP Channel
Macau Univ. of Science and Technology
Internet
China Unicom Tongle
The Hong Kong Univ. of Science and Technology
Guangdong Univ. of Technology
South China Univ. of Technology
China Unicom Yuandong
Kingsoft
Guangdong Communications & Networks Institute
Ethernet/TCP/UDP Channel CCN Router
Multi-Identifier Router
IP-CNN-IP
IP-CCN
CCN-IP
CNN-IP-CCN

CCN: Content Centric Network
IP: Internet Protocol
PKUSZ: Peking University Shenzhen Graduate School
TCP: Transmission Control Protocol
UDP: User Datagram Protocol

▲Figure 7. The proposed prototype system for multi-identifier System.


Multi-identifier Network User Client
User Registration

User Name

E-mail Address

Name

ID Number

Discription

Prefix

Path

Sign up

Multi-identifier Network User Client
Resource Publish

Resource Identifier

Resource Address

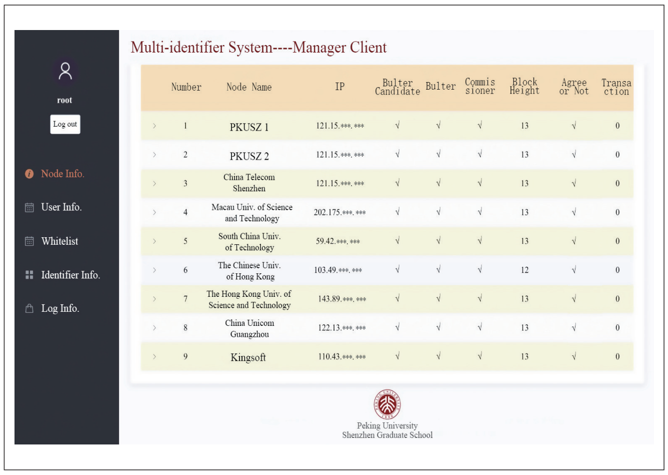
Hash Value

Resource Discription

Path

Publish

▲Figure 8. Interfaces of user registration and resource publishing.



Multi-identifier System----Manager Client

	Number	Node Name	IP	Bulter Candidate	Bulter	Commis sioner	Block Height	Agree or Not	Transa ction
›	1	PKUSZ 1	121.15.***.***	√	√	√	13	√	0
›	2	PKUSZ 2	121.15.***.***	√	√	√	13	√	0
›	3	China Telecom Shenzhen	121.15.***.***	√	√	√	13	√	0
›	4	Macau Univ. of Science and Technology	202.175.***.***	√	√	√	13	√	0
›	5	South China Univ. of Technology	59.42.***.***	√	√	√	13	√	0
›	6	The Chinese Univ. of Hong Kong	103.49.***.***	√	√	√	12	√	0
›	7	The Hong Kong Univ. of Science and Technology	143.89.***.***	√	√	√	13	√	0
›	8	China Unicom Guangzhou	122.13.***.***	√	√	√	13	√	0
›	9	Kingsoft	110.43.***.***	√	√	√	13	√	0

Peking University
Shenzhen Graduate School

▲Figure 9. Status information of blockchain.

pared with the traditional PBFT algorithm, PoV has better scalability. This is because the PoV consensus two-phase commit communication complexity is only $O(n)$, which is only affected by the number of commission nodes. In terms of performance, the PoV consensus only needs one block to achieve tamper-proof transaction confirmation, with better performance and lower energy consumption than the public chain.

6 Conclusions

A future network should be decentralized, secure and compatible with the existing IP-based network. In this paper, we propose a multi-identifier system that constructs a network layer with a parallel coexistence of multiple identifiers, including identity, content, geographic information, and IP address. MIS provides the generation, management, and resolution ser-

▼**Table 6. Comparison between PBFT and PoV**

The Number of Nodes		10	50	100	150	200	250
PoV	Theoretical Results	11 669	2 277	1 105	715	521	406
	Experiment Results	8 408	1 686	848	552	381	314
	Uniformization	0.7205	0.7404	0.7674	0.772	0.7312	0.77
PBFT	Theoretical Results	11 457	1 427	330	116	52	27
	Experiment Results	8 305	1 083	257	84	40	20
	Uniformization	0.7249	0.7589	0.7788	0.7241	0.7692	0.7407
Ratio	Theoretical Results	1.02	1.6	3.35	6.16	10.02	15.04
	Experiment Results	1.01	1.56	3.3	6.57	9.52	15.7

PBFT: Practical Byzantine Fault Toleranc
PoV: Proof of Vote

vices of identifiers and uses consortium blockchain to enable decentralized management. MIS also implements data privacy protection. The test results based on the prototype system show that the network has excellent performance and can support real-world applications after further development.

References

[1] NAKAMOTO S, BITCOIN A. A Peer-to-Peer Electronic Cash System [EB/OL]. (2008) [2019-12-25]. https://bitcoin. org/bitcoin.pdf

[2] CACHIN C. Architecture of the Hyperledger Blockchain Fabric [C]//Workshop on Distributed Cryptocurrencies and Consensus Ledgers. Chicago, USA, 2016, 310: 4

[3] CASTRO M, LISKOV B. Practical Byzantine Fault Tolerance [C]//OSDI. New Orleans, USA, 1999: 173 – 186

[4] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol [C]//Proc. Annual International Cryptology Conference. Cham, Switzerland: Springer International Publishing, 2017: 357 – 388. DOI:10.1007/978-3-319-63688-7_12

[5] KING S, NADAL S. PPcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake [EB/OL]. (2012-08-19) [2019-12-26]. https://decred.org/research/king2012.pdf

[6] SCHWARTZ D, YOUNGS N, BRITTO A. The Ripple Protocol Consensus Algorithm [J]. Ripple Labs Inc White Paper, 2014: 1 – 8

[7] LOIBL A, NAAB J. Namecoin. Namecoin. Info [EB/OL]. (2014) [2019-12-26]. https://Namecoin.info

[8] ALI M, NELSON J, SHEA R, et al. Blockstack: A Global Naming and Storage System Secured by Blockchains [C]//Annual Technical Conference. Denver, USA, 2016: 181 – 194

[9] BENSHOOF B, ROSEN A, BOURGEOIS A G, et al. Distributed Decentralized Domain Name Service [C]//IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW). Chicago, USA: IEEE, 2016: 1279 – 1287.DOI:10.1109/ipdpsw.2016.109

[10] ZUPAN N, ZHANG K W, JACOBSEN H A. Hyperpubsub: a Decentralized, Permissioned, Publish/Subscribe Service Using Blockchains [C]//Proc. 18th ACM/IFIP/USENIX Middleware Conference: Posters and Demos. New York, USA: ACM, 2017: 15 – 16.DOI: 10.1145/3155016.3155018

[11] WU H Q. Reflections on the Reform of Network Architecture [J]. ZTE Technology Journal, 2019, 25(01): 2 – 4. DOI: 10.12142/ZTETJ.201901001

[12] LI H, WU J, XING K, et al. The Prototype and Testing Report of Multilateral and Multi-mode Identification Domain Management System [J]. Scientia Sinica Informationis, 2019, 49(09): 1186 – 1204. DOI: 10.1360/N112019-00070

[13] LI H, LI K, CHEN Y, et al. Determining Consensus in a Decentralized Domain Name System: US Patent App. 15/997,710 [P]. 2018

[14] LI H, WANG X, LIN Z, et al. Systems and Methods for Managing Top-Level Domain Names Using Consortium Blockchain: US10178069B2 [P]. 2019

Biographies

XING Kaixuan is a postgraduate student of Shenzhen Graduate School, Peking University, China. His research interests include new architectures and new generations of information communication technology.

LI Hui (lih64@pkusz.edu.cn) received the B.Eng. and M.S. degrees in information engineering from Tsinghua University, China in 1986 and 1989, and Ph.D. degree in information engineering from The Chinese University of Hong Kong, China in 2000. He is currently a professor with Peking University, China. His research interests include future network architecture, cyberspace security, and blockchain technology.

YIN Feng is a postgraduate student of Shenzhen Graduate School, Peking University, China. His research interests include blockchain technology and network security.

MA Huajun is a postgraduate student of Shenzhen Graduate School, Peking University, China. His research interests include network security and distributed system technology.

HOU Hanxu received the B.Eng. degree in information security from Xidian University, China in 2010 and Ph.D. degrees in information engineering from The Chinese University of Hong Kong, China in 2015 and from the School of Electronic and Computer Engineering, Peking University, China. He is now an assistant professor with the School of Electrical Engineering & Intelligentization, Dongguan University of Technology, China. His research interests include erasure coding and coding for distributed storage systems.

XU Huanle received the B.Sc. (Eng.) degree from the Department of Information Engineering, Shanghai Jiao Tong University, China in 2012 and Ph.D. degree from the Department of Information Engineering, The Chinese University of Hong Kong, China in 2016. His primary research interests focus on job scheduling and resource allocation in cloud computing, decentralized social net-works, parallel graph algorithms and machine learning. He is also interested in designing wonderful algorithms for real applications and practical systems using mathematical tools.

Yunghsiang S. HAN received his Ph.D. degree from the School of Computer and Information Science, Syracuse University, USA in 1993. Now he is with School of Electrical Engineering & Intelligentization, Dongguan University of Technology, China. He has also been a chair professor at Taipei University, China since February 2015. His research interests are in error-control coding, wireless networks, and security. Dr. HAN was a winner of the 1994 Syracuse University Doctoral Prize and a Fellow of IEEE. One of his papers won the prestigious 2013 ACM CCS Test-of-Time Award in cybersecurity.

LIU Ji is the director of the Information Office at Shenzhen Graduate School, Peking University. His research interest is new network architecture.

SUN Tao is the director of The Network Information Center of Shenzhen University Town. His research interests include blockchain and cyberspace security.