Hyperconnected Network: A Decentralized Trusted Computing and Networking Paradigm

Hao Yin, Dongchao Guo, Kai Wang, Zexun Jiang, Yongqiang Lyu, and Ju Xing

Abstract

With the development of the Internet of Things, a complex CPS system has emerged and is becoming a promising information infrastructure. In the CPS system, the loss of control over user data has become a very serious challenge, making it difficult to protect privacy, boost innovation, and guarantee data sovereignty. In this article, we propose HyperNet, a novel decentralized trusted computing and networking paradigm, to meet the challenge of loss of control over data. HyperNet is composed of the intelligent PDC, which is considered as the digital clone of a human individual; the decentralized trusted connection between any entities based on blockchain as well as smart contract; and the UDI platform, enabling secure digital object management and an identifier-driven routing mechanism. HyperNet has the capability of protecting data sovereignty, and has the potential to transform the current communication-based information system to the future data-oriented information society.

Introduction

The Internet of Things (IoT) conducts the integration of cyber, physical, and social (CPS) systems [1], which accelerates the transformation from the Internet to an information society. However, the coupling of user data and applications in current service mechanisms has introduced many challenges in data protection and application innovation [2]. Specifically, users have to move data to service providers in exchange for services and applications. Service providers, featuring high concentrations of computation and storage resources, treat the management of these data as their own business and prevent data sharing with any other entities. In this case, users have totally lost control over their data, which leads to several critical problems, summarized as follows.

Risk in Privacy Preservation

The coupling of data and applications means that data has to be provided to applications of various service providers. One service provider could exchange privacy data it holds with another service provider for the purpose of business without notifying the user. Unfortunately, as pointed out by de Montjoye from MIT Media Lab [3], the user can do nothing to prevent data leakage because of the separation of data ownership and management. In addition, the user may lose confidence in the adoption of Internet services for fear of privacy leakage.

Hampering Innovations

Internet giants monopolize a vast majority of the service provisioning market share. These giants have privilege to collect user data and hold data exclusively. As a result, they have definite advantages over new businesses, which depend on data mining to provide better services. This fact creates a technological barrier for new entrants without data, which leads to high technological innovation cost.

Challenge in Government Capability

Confronted with data monopolization, the government cannot play its part in tackling many social affairs such as protecting the data sovereignty of citizens. Also, it is hard for the government to conduct the data-driven decision making. In contrast, those giants could provide some public services that should be offered by the government and thus hold increasing influence on social affairs. Recent examples are Apple's refusal to unlock the iPhone of a suspect for the FBI and Alibaba's credit score applicable for a Japanese visa application.

The history of information technology indicates that substantial innovation is usually boosted by breaking the bottleneck of closed systems. Let us have a look back into the history of information technology, as shown in Fig. 1. In the 1970s, the emergence of the PC composed of standardized components decoupled the hardware and software components of the computer. This ended the monopoly of the mainframe computer (e.g., IBM360) on the computer market. The introduction of the concept of software-defined networking (SDN) decouples the data plane and the control plane of the Internet. Thus, the integrated and closed networking system is separated by SDN into an open system of loosely interdependent components in which innovations are made simultaneously at different levels. In a CPS system, it is expected that a novel technology will be proposed to deal with the data monopolization. Unfortunately, it is difficult for the contemporary computing and networking paradigms such as cloud computing to tackle data monopolization. These paradigms usually rely heavily on data centers that hold huge storage and computation capabilities and provide services to entities in a centralized way [4]. Consequently, the

Digital Object Identifier:
10.1109/MNET.2018.1700172

The authors are with Tsinghua University.

0890-8044/18/$25.00 © 2018 IEEE

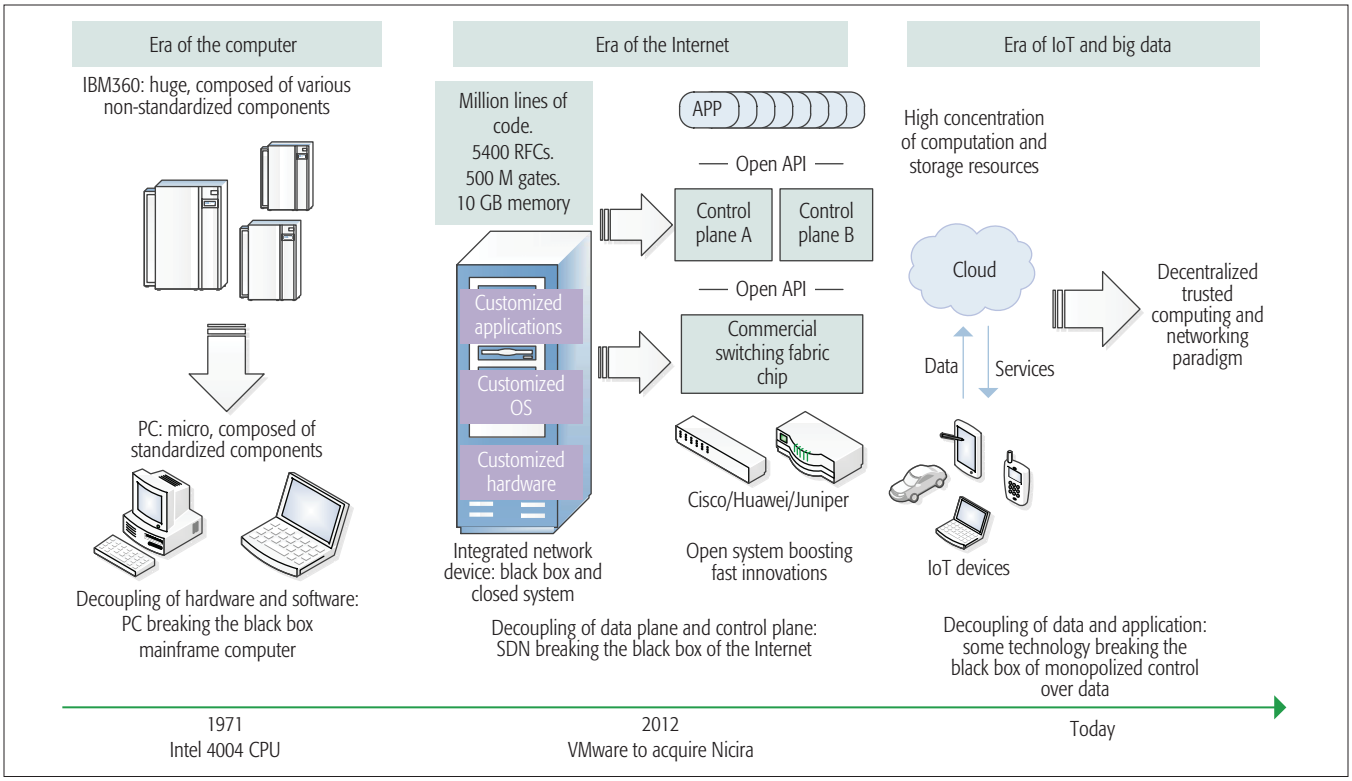

FIGURE 1. A history of information technology.

loss of control over data is inevitable. However, the rapid development of edge computing [5, 6], mobile crowdsourcing [7], and blockchain implies a return of the decentralized computing and networking paradigm, which inspires a novel paradigm to tackle data monopolization in the CPS system.

In this article, we propose a novel decentralized trusted computing and networking paradigm, named the hyperconnected network (HyperNet), to guarantee data sovereignty and to achieve trusted connections within the untrusted networking environment. The rest of this article is organized as follows. The following section elaborates the architecture of HyperNet in detail and presents a typical use scenario. The final section concludes our work and illustrates some open issues for future study.

Hyperconnected Network

The design philosophy behind HyperNet is the transformation from the contemporary communication-based Internet to the future computation-storage-centric information infrastructure. Specifically, the Internet features the end-to-end principle where service providers and users reside in the end nodes of the network with intermediary nodes such as routers playing a key role. The Internet, designed according to this principle, is capable of efficiently sharing data while causing the coupling of data and applications. In contrast, HyperNet is a data-oriented architecture, featuring the private data center (PDC) as the basic networking element, interactions between PDCs following smart contracts, and secure data object management enabled by the universal data object identifier (UDI) platform.

Previous research reported that a new architecture could survive only if it provides different functionality than the incumbent [8]. Thus, HyperNet tends to succeed in surviving because of the exclusive functionalities (e.g., trusted connection) it provides that are different from the Internet. Since HyperNet provides more general services such as PDC and UDI, the center of the protocol stack of the future information infrastructure will move from the networking layer to a higher level, according to the viewpoint of previous research [8]. In other words, HyperNet has the potential to become the center of the future information infrastructure.

System Architecture

Recent advances in computing and networking technologies enable a fundamental transformation of information infrastructure from Internet to HyperNet, as shown in Fig. 2. Specifically, HyperNet is a computation- and storage-centric architecture, while the Internet is a communication-centric architecture. The PDC, featuring control over user data and concentration of computation and storage resources, becomes the basic element of HyperNet architecture. Any kind of interaction between PDCs is forced to follow certain agreed rules indicated by a smart contract to achieve trusted connection. The management and routing of data object are conducted by the UDI.

As shown in Fig. 2, HyperNet is composed of the following components:

- The intelligent PDC
- The decentralized trusted connection between any entities based on blockchain [9] as well as smart contract [10, 11]
- The UDI platform

As a novel computing and networking paradigm, HyperNet has the capability of protecting data

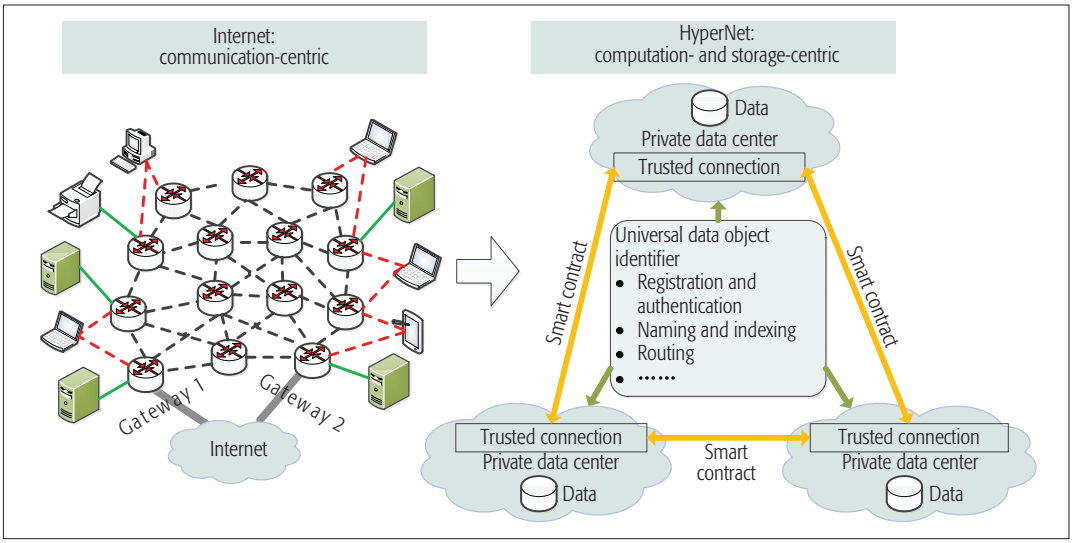

FIGURE 2. Transformation of the design philosophy of information infrastructure.

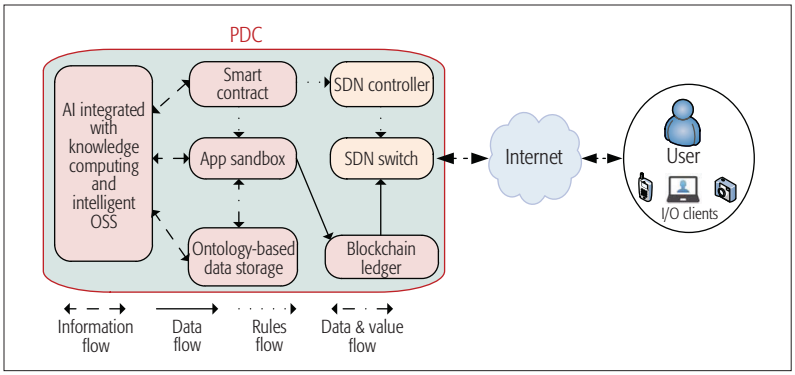

FIGURE 3. Typical structure of a PDC.

sovereignty and building up the future information infrastructure for CPS systems. The introduction of the PDC gives users control over their data. Users are capable of choosing which applications use their data instead of totally giving up data control to service providers. Interactions between PDCs or PDCs and service providers operate following the rules negotiated and regulated by smart contracts. Since the interaction process recorded in blockchain is auditable and unchangeable, any data abuse or leakage is not likely to happen. The UDI platform is aimed at storing, indexing, and routing data objects in a decentralized trusted way. This helps to decouple data from applications. To sum up, HyperNet enables not only the control over data in PDCs but also the data sharing between entities in the CPS system. Also, HyperNet is a computing paradigm that is not only compatible with current applications in the Internet but also capable of running well designed applications in PDCs.

Major Components

The functional components of HyperNet will be elaborated in detail in this subsection.

Private Data Center: The PDC, which is among the most important components of the HyperNet, can be considered as the container for the digital clone of a human individual in the real world. A PDC safely stores all the data of information (e.g., personal biological features, social relationships, network activities) on every HyperNet user, and provides a secure environment where applications can run under effective supervision and intelligent operation support.

Different from the current data usage model of the Internet, a PDC has its own key individual features. On one hand, data is the private property of its HyperNet user and stored in the user's own PDC rather than on application servers. A PDC acts as an intelligent private data coffer, where data can be stored in its secure zone or its free zone, facilitating users to protect and have control over their data while sharing some data freely. Requesting data within a PDC is controlled by access control strategies of the PDC owner with the help of SDN technology; meanwhile, usage of data is supervised by the artificial intelligence (AI) component to enable smart services as well as automatic operation support. On the other hand, compared to the current service model of the Internet, where applications isolate their users' data, the data of every HyperNet user is decoupled from its application, which enables users to share their data selectively and seamlessly with any set of applications or any set of other users, without constraints from application providers. In other words, with the help of a PDC, every HyperNet user can freely choose which applications access data or which users interact with data, and easily monitor the behavior of every running application inside.

The typical structure of a PDC, shown in Fig. 3, is elaborated as follows. The AI component, which integrates knowledge computing and the intelligent operation support system (OSS), is responsible for governing and organizing functional components of a PDC to run as a whole. Specifically, the AI component can act as a virtual personal assistant, aiming to create an accurate user profile and performing promising services. In other words, the AI component acts as the brain of the PDC, which helps to not only make high-level decisions in response to complicated actions regulated by smart contracts, but also transform the high-level logics of the decisions into network-level rules used by SDN compo-

nents. Following the corresponding rules, the app sandbox component creates a virtual environment with high security to prevent potential malicious application behavior. Apps are decoupled from raw data in the sense that they run on the virtual environment and can only interact with the ontology-based data storage and management component. In other words, the data of every HyperNet user is decoupled from applications and stored physically within the corresponding PDC, which enables the PDC owners in charge of the data sovereignty as data cannot be shared unless the owner of the PDC allows it. The ontology-based data storage and management component implements a network of concepts derived from raw data and provides rich information at the conceptual level to the AI component to help make decisions. Perhaps more importantly, the ontology-based data storage and management component exchanges data and value with the sandbox component. In this sense, a PDC not only implements a privacy preserving mechanism, but also constitutes the basic element of the network of value. Data flow going outside a PDC will be recorded by the trusted blockchain ledger. The network-level actions of a data flow are regulated by an SDN switch following rules from an SDN controller. A PDC can be accessed by typical I/O clients (e.g., PC, smartphone, tablet) of its owner, which makes it possible for HyperNet users to access their own PDCs anytime and anywhere. In addition, requests from outside of the PDC should be controlled by SDN rules, which are produced by compiling the corresponding smart contract between PDCs.

Trusted Connection: Trusted connection aims to guarantee consistent and credible behaviors among users, institutions, and even infrastructures. Considering the expressivity, universality, and flexibility of a smart contract, it can be used as the first citizen in the context of trusted connection. All the behaviors among different entities are derived and constrained by contracts. Instead of putting effort into the underlying design of control logics, entities can just focus on their contracts with others. For example, interactions between PDCs are well controlled via a trusted connection mechanism that benefits from contract-driven style and SDN capabilities. As shown in Fig. 4, regulations on all the interactions between PDCs are predefined in the form of smart contracts. The smart contracts are recorded in blockchains for the purpose of credibility and traceability. A PDC controller (PDCC) hooks onto the chain to supervise the states of the smart contracts and generate policies according to them. Besides, the SDN is leveraged to have a global view of multi-domain networks, including link states and traffic conditions. Policy enforcement can be done either in the devices on the path or in the ingress routers (i.e., source routing style). When one PDC is ready to share its data, it first makes a request to the PDCC. Once the PDCC receives the request, which triggers predefined conditions, it will enforce the precompiled policies.

With the help of the mechanisms described above, HyperNet achieves trusted connection, where user data can be used in a more secure and fine-grained way.

Decentralized Digital Object Routing: In the CPS system, there are many data-related critical issues. How to identify a specific piece of data is the most important one. Specifically, an identity system capable of identifying the source, the version, the ownership, and many other attributes of data is essential. Only if an efficient and secure data object identity system is proposed first is it possible to manage and exchange data objects between different entities. The second critical issue is to propose a universal data management system that can be extended at a low cost. The last issue is how to prevent data leakage while supporting free data sharing for academic or commercial purposes.

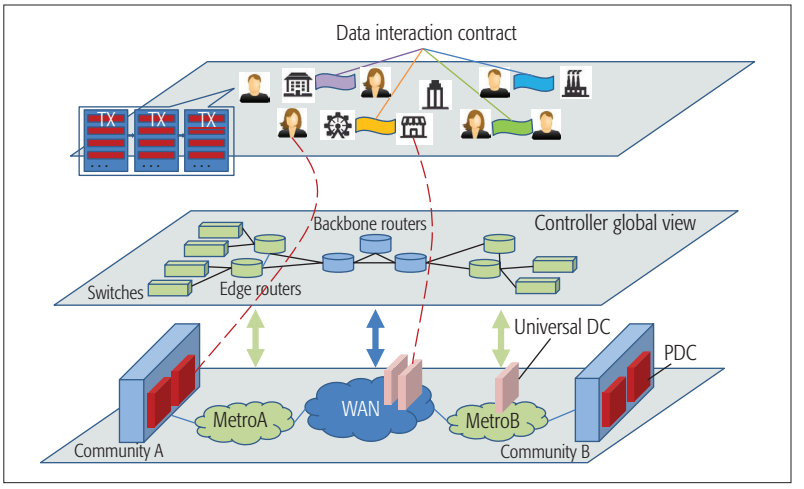

FIGURE 4. Trusted connection between PDCs.

The UDI technique is essential to the digital object management and routing mechanism. A UDI technique such as Handle System [12] is aimed at assigning, managing, and resolving persistent identifiers for data objects. The identifier of a data object is associated with some pieces of meta-data. A piece of meta-data usually includes attributes such as the index, the type, and the payload. For example, the attribute of type could be "Location" such as Uniform Resource Locator (URL). The attribute of payload stores the URL address of the corresponding piece of data. Distinct from the changeable and unreliable URL, UDI uses a persistent digital object identifier and provides a permanent identification mechanism to identify and manage a digital object. Moreover, UDI provides users with the metadata associated with digital objects and the relationships between objects. UDI is usually implemented in a centralized way like DNS [12]. By means of blockchain technology, it is possible to implement a decentralized UDI platform. This platform could assign, manage, and resolve persistent identifiers for any digital objects in a decentralized way.

As shown in Fig. 5, the decentralized UDI platform allocates identifiers to data objects of a CPS system and manages the data object in a universal way. The decentralized UDI platform helps to build up an ID-driven network where the resolution and the routing are based on identifier rather than on conventional IP address. Besides, an evolutionary secure system, acting as a trusted computing environment, is proposed, where data from outside PDCs can be securely used for commercial or academic purposes. A blockchain-based

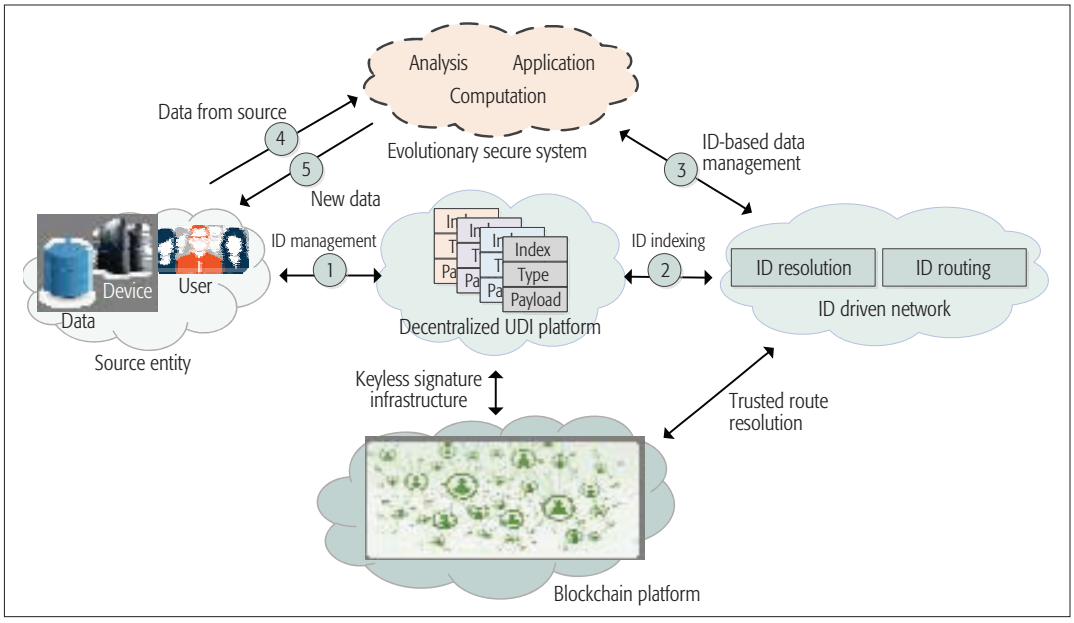

FIGURE 5. Architecture of HyperNet enabling secure data management and UDI-driven data object routing.

Our future research will focus on the collaborative mechanisms between different kinds of blockchains to improve the performance of HyperNet. For example, replacing public blockchains by consortium blockchains helps lower interaction delay.

digital signature system such as keyless signature infrastructure (KSI) [13] is introduced in the architecture to help the UDI platform construct a highly efficient decentralized authentication mechanism for protecting the integrity of digital data. According to the UDI of data, it is possible to efficiently collect the set of data requested by an application. Then each piece of data from this requested set will be located from the source entity and sent to the application in the evolutionary secure system. Finally, the new data generated by the application will be identified by the UDI platform and given back to the source entity.

There are advantages of decentralized digital object management and routing. User data is managed in a decentralized way, which means no service provider can control data. Only if the service provider is entitled to control over a piece of data of a user could it use the piece of data. The usage process is carried out under the corresponding smart contract. Thus, the abuse of data or data leakage is not likely to happen.

Use Scenario

HyperNet will enable a great number of applications. In this subsection, we take the social communication application as an example.

As shown in Fig. 6, if Alice wants to invite Bob to have dinner at 18:00 on September 15, 2017, she may access her PDC via an I/O client (e.g., mobile phone), write this message in her PDC, and then send it to Bob via email.

When Bob's PDC receives Alice's email, it analyzes the invitation information in this email and then decomposes it into several types of data (e.g., time, address, event, relationship). After that, the AI component within Bob's PDC starts to exploit the data to deduce some further information that may be helpful to Bob. For example, based on the data exploited from Alice's email, AI in Bob's PDC may give an actual picture of the dinner place to Bob, suggestions for Bob on when and how to get to a dinner address, and some more attractive suggestions such as the dressing style depending on the dinner occasion. The information from both Alice's email and the AI suggestions will be integrated to a new data, named "Dinner Event" stored in Bob's PDC, and then push this data to Bob's I/O client to notify Bob of this event. Since the data in the PDC is decoupled from applications, the data can be pushed to Bob's client in various ways. For example, it can be carried by a WeChat message, or an email, or any other applications that can show this event.

The "Dinner Event" data can be sent from Bob to different HyperNet users according to different smart contracts between them, via an SDN controlled networking environment. Different smart contracts of HyperNet users can be negotiated in advance based on different rules. For example, if the smart contracts between Bob and others are based on the strength of social relationships, the data shared to the PDC of Bob's wife may include everything of the "Dinner Event" (e.g., the dinner time, dinner address, dinner topic, the relationship between Bob and Alice, the time when Bob is coming home), while the data shared to the PDC of Bob's driver may only include the dinner time and dinner address. In addition, if Bob wants to post this dinner event to a public cloud (e.g., his Facebook), the only data he needs to share may be a picture of the dinner place.

Conclusion And Open Issues

In order to meet the challenge of the loss of control over data, we propose a novel decentralized trusted computing and networking paradigm, named HyperNet, to guarantee data control by users themselves instead of application providers, and achieve an information society where trusted connections can be enabled within untrusted

networking environments. The major components of HyperNet include the intelligent PDC, which is considered as the digital clone of a human individual, the trusted connection between any entities based on blockchain and smart contracts, and the secure universal digital object management and routing platform. HyperNet has many advantages that help change not only the computing paradigm in the era of IoT but also the future network architecture substantially. In the HyperNet framework, users are entitled to control their data located in the related PDC where data is decoupled from applications. Any interaction process between PDCs follows rules regulated by smart contracts. This means that a service provider cannot use the data for any purpose irrelevant to providing the promised services. Furthermore, HyperNet helps to build up a UDI-driven network that is capable of indexing and routing data in a universal way.

Our future research will focus on the collaborative mechanisms between different kinds of blockchains to improve the performance of HyperNet. For example, replacing public blockchains by consortium blockchains helps lower interaction delay.

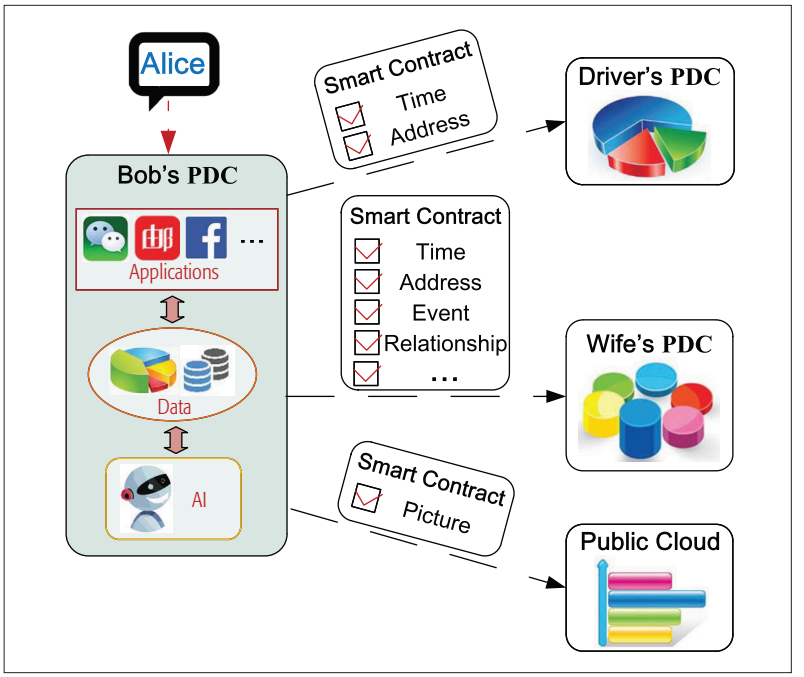

FIGURE 6. A social communication scenario in HyperNet.

Acknowledgment

We would like to thank the anonymous reviewers for their comments and suggestions. This work was funded in part by the National Key Research and Development Program under Grant No. 2016YFB1000102, in part by the National Natural Science Foundation of China under Grant No. 61672318, No. 61631013, and No. 61702439, and in part by the QUALCOMM university sponsored program.

References

[1] A. Al-Fuqaha *et al.*, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 4, June 2015, pp. 2347–76.
[2] T. Chajed *et al.*, "Amber: Decoupling User Data from Web Applications," *Proc. 15th USENIX Conf. Hot Topics in Operating Systems*, Kartause Ittingen, Switzerland, May 18–20, 2015, pp. 19–24.
[3] Y. A. de Montjoye *et al.*, "openPDS: Protecting the Privacy of Metadata through SafeAnswers," *PLoS ONE*, vol. 9, no. 7, July 2014, pp. 1–9.
[4] Y. Zhang *et al.*, "A Survey on Emerging Computing Paradigms for Big Data," *Chinese J. Electron.*, vol. 26, no. 1, Jan. 2017, pp. 1–12.
[5] Y. Mao *et al.*, "Mobile Edge Computing: Survey and Research Outlook," *IEEE Commun. Surveys & Tutorials*, 2017; arXiv:1701.01090.
[6] J. Ren *et al.*, "Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing," *IEEE Network*, vol. 31, no. 5, Sept./Oct. 2017, pp. 96–105.
[7] J. Ren *et al.*, "Exploiting Mobile Crowdsourcing for Pervasive Cloud Services: Challenges and Solutions," *IEEE Commun. Mag.*, vol. 53, no. 3, Mar. 2015, pp. 98–105.
[8] S. Akhshabi and C. Dovrolis, "The Evolution of Layered Protocol Stacks Leads to an Hourglass-Shaped Architecture," *SIGCOMM Comp. Commun. Rev.*, vol. 41, no. 4, Aug. 2011, pp. 206–17.
[9] J. Bonneau *et al.*, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," *2015 IEEE Symp. Security and Privacy*, May 2015, San Jose, CA, pp. 104–21.
[10] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, May 2016, pp. 2292–2303.
[11] A. Kosba *et al.*, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," *2016 IEEE Symp. Security and Privacy*, May 2016, San Jose, CA, pp. 839–58.
[12] CNRI, Technical Manual, Handle.Net, v. 8, Nov. 2015; http://www.handle.net/tech_manual.html
[13] A. Buldas, A. Kroonmaa, and R. Laanoja, "Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees," *Secure IT Systems*, Springer, 2013, pp. 313–20.

Biographies

HAO YIN (h-yin@tsinghua.edu.cn) is a professor in the Research Institute of Information Technology (RIIT) at Tsinghua University. His research interests span broad aspects of multimedia networks, future networks, and big-data-driven network science and engineering. Some of his research results have been widely used in industry and adopted by industry standards. He has published over 100 papers in refereed journals and conferences.

DONGCHAO GUO (dongchaoguo@mail.tsinghua.edu.cn) received his Ph.D. degree in signal and information processing from Beijing Jiaotong University (BJTU), China, in 2014. Currently, he is a postdoctoral researcher at RIIT, Tsinghua University. His research interests include complex networks and content distribution networks.

KAI WANG (wangkai.phd@outlook.com) received his B.S. degree in electronic science and technology and his Ph.D. degree in communication and information systems from BJTU in July 2009 and June 2014, respectively. Now he works as a postdoctoral research fellow at RIIT, Tsinghua University. Before he joined Tsinghua University, he was an assistant professor at Yantai University from December 2015 to June 2017, and an engineer in the 41st Institute of China Electronics Technology Group Corporation from July 2014 to December 2015. His research interest is in architectures and protocols of data communication networks.

ZEXUN JIANG is a Ph.D. student at RIIT, Tsinghua University. His research interests focus on network measurement and information retrieval.

YONGQIANG LYU received his Ph.D. degree in computer software and theory from Tsinghua University in 2006. Currently, he is an associate professor at RIIT, Tsinghua University. His research interest focuses on usability and security of human-machine fusion systems.

JU XING is a Ph.D. student at RIIT, Tsinghua University. His research interests focus on network architecture and network security.