Software is envisioned to play an unprecedented dominant role in future communication paradigms, with user-defined applications capable of not only communicating with, but also controlling some features of the underlying communication infrastructure in a secure and trustworthy manner. This (re)volutionary trend toward virtualized and “softwarized” networks enable Internet-based service users and providers, as well as the related stakeholders, to take advantage of resource abstractions and to adopt a programmatic approach to service deployment. In a “game-changing” scenario, a user’s needs can be decoupled and expressed independently of the specific underlying implementable technology, but yet the requested service must meet the expected mutual trustiness and security levels. This trend opens a number of disruptive solutions that can change the Internet as we know it.

Distributed ledger technologies including Blockchain, a digital, decentralized platform that records and verifies transactions (ledgers) and contracts in a secure manner, is a game-changer for enabling truly distributed transaction-based venues, including identity, Internet, financial, government, health, supply-chain, and other technology services. One of the first and most popular Blockchain application, Bitcoin, has showcased immense fortune in this technology, which is now widely considered as a viable example for many applications that go beyond the concept of digital currency to build on consensus-driven trust, immutability and decentralized nature provided by distributed ledger technology.

Identity theft presents a serious problem that impacts the integrity of on-line interactions. The reliance on user name and password has serious implications on fraud and the bottom line of financial transactions. Current identity management schemes that rely on knowledge-based authentication for performing Know-Your-Customer (KYC) operations are inadequate for performing online identity vetting. Furthermore, the approval of data protection laws, such as the General Data Protection Regulation (GDPR), will have a direct impact on the way identity data is treated by relying parties. In this regard, the emergence of distributed ledger technology has the potential of replacing old style identity federation schemes into modern dynamic ones based on the ability to access public keys on the ledger. This is also driving the potential adoption of new platforms for online digital identity, such as Sovereign Identity (http://www.sovrin.org).

Intent-based networking is another disruptive approach, since it allows users to request network services using only terms and languages that are known and relevant to them-selves, specifying “what” they want to achieve and not “how.” Such a high level of abstraction enables a complete decoupling of the service description from the technology-specific mechanisms required to deploy it, facilitating interoperability and provider-independence, and thus promoting an open and healthy Internet service economy.

Development of relevant and open standards for Distributed Ledger, Intent-based applications, as well as other related paradigms, will play a major role in favor of global interoperability, faster adoption, and market penetration. Some initiatives from relevant Standards Development Organizations (SDOs) are already in progress, including the ITU-T Focus Group on Application of Distributed Ledger Technology, ISO/TC 307 Blockchain and Distributed Ledger Technologies, IEEE P2418 Standard for the Framework of Blockchain Use in IoT, IEEE P1916.1 Standard for Software Defined Networking and Network Function Virtualization Performance, and ONF Intent NBI–Definition and Principles.

This special issue features six articles addressing major issues concerned with evolving standardization processes and underlying technologies in the context of Blockchain for different application domains, showing how distributed ledger technologies can be so disruptive that they can change the Internet as we know it. The article titled “Blockchain Standard: Can We Reach Consensus?” by Gramoli and Staples offers an overview of current standardization initiatives on Blockchain and distributed ledger technologies, including projects from ISO, ITU, W3C, IEEE, IETF, and other Standards Developing Organizations (SDOs). The authors focus on the need for a common terminology, and discuss some of the most important elements of a possible functional architecture: consensus, security and ownership. They finally argue that any standard development should be conceived with a high level of flexibility to cope with the fast evolution pace of Blockchain and distributed ledger technologies.

In the article titled “Blockchain Based Decentralized Cloud/Fog Solutions: Standards, Challenges and Opportunities,” Uriarte and De Nicola present an overview of smart contracts and Blockchain solutions that enable completely decentralized cloud/fog deployments, i.e., without any intermediary. In particular, the authors compare the Golem, iExec, and SONM projects: first they highlight the main common architectural aspects, then they analyze the specific technological differences and discuss the most relevant challenges. Finally, they provide an overview of existing standardization efforts and suggest new opportunities to foster interoperability.
The article titled “Blockchain-based Decentralized Applications for Multiple Administrative Domain Networking” by Rosa and Rothenberg investigates the vision, supported by working experiments, on how blockchain-based decentralized applications make it possible to take advantage of smart contracts for lifecycle management of end-to-end network service slices across multiple administrative domains. The authors define a number of operational phases for the deployment of a generalized network service in multi-administrative domains, including also a noteworthy “intent” stage to define network service requirements among different providers. They also present a proof-of-concept implementation of a multi-domain service orchestrator and discuss potential standardization opportunities.

In the article titled “Exploiting the IoT Potential of Blockchain in the IEEE P1931.1 ROOF Standard,” Meloni et al. discuss how Blockchain technology can facilitate the implementation of decentralized, semi-autonomous, and trusted Internet of Things (IoT) platforms and services, guaranteeing secured data exchange as well as tamper-proof record keeping. In particular, the authors present the architectural framework and the use of Blockchain technology proposed by the IEEE 1931.1 working group, which is currently defining a standard for technical and functional interoperability of federated IoT systems for Real-time Onsite Operations Facilitation (ROOF). They also provide an outlook of current open issues and future improvements needed for a successful deployment.

The article titled “ApproxBC: Blockchain Design Alternatives for Approximation-Tolerant Resource-Constrained Applications” by Vairam et al. investigates possible design alternatives to the current Blockchain technologies, in order to reduce the requirements in terms of computational power and storage capacity. In particular, the authors present two design variants: the first one uses Hash-tables instead of Merkle-trees to store the fingerprint of accepted transactions; the second one uses a novel data structure called e-BF that combines the space and computational efficiency of Bloom filters with the usability of hash-tables. The authors argue that the proposed ApproxBC solutions can be configured to provide a level of security that is acceptable for a certain class of applications in resource-constrained environments, including as relevant examples vehicle insurance and power utility management.

Finally, in the article titled “Blockchain Based DNS and PKI Solutions,” Adiguzel and Karaaslan discuss how to implement decentralized Domain Name System (DNS) and Public Key Infrastructure (PKI) solutions based on Blockchain technologies. The authors provide a classification of Blockchain-based DNS and PKI implementations according to the offered services. They highlight advantages and feasibility aspects of those implementations, reporting also from practical experience. Finally, they address the vision of a “decentralized Internet.”

We would like to thank all the authors for their valuable contributions to this Feature Topic, and the reviewers for their voluntary effort and constructive feedback to the authors.

Biographies

HESHEM ELBAKOURY (Heshem.Elbakoury@huawei.com) is an industry veteran with extensive background and expertise in information technology, and enterprise, carrier networks and broadband access networks. He is a principal architect at Futurewei Technologies Inc., focusing on advanced technology research and standards in Access and Network Research Labs. His research involves different technologies such as next generation Internet, intent-based networking, ultra-low latency and time sensitive networking, SDN/NFV, cloud and mobile edge computing, Blockchain, autonomic networking, and distributed cable access architectures. As a chief systems architect, Mr. Elbakoury has led the architecture, design and development of several very successful switching/routing, security, broadband access, data center, and carrier Ethernet products. He is a capable leader who demonstrated the ability to set a technological vision, and build and energize engineering teams to deliver on a common vision and goals. He has served as a keynote speaker and participated in panels at several conferences around the globe. He has been active in different standard groups, including IEEE 802, IETF, MEF, SCTE, and OF. He was an editor of IEEE 1904.1 (SPoD), he is the vice chair of IEEE 1916.1, and served as the editor for several CableLabs standards and Technical Reports. He has several publications and patents in the field of networking, and he holds an M.S.C. degree from Waterloo University, ONT, Canada.

MOHAMMAD ASAD REHMAN CHAUDHRY (masadch@ieee.org) is a seasoned professional and thought-leader with extensive experience in leading multidisciplinary projects in Information and Communication Technologies. He received a Ph.D. in electrical and computer engineering from Texas A&M University, Texas, USA. He currently spearheads projects in SDN/NFV ecosystems, Blockchain, Big Data systems, data centers networks, and system optimization. An Executive Director with Soptimizer, his experience spans several industries, and academia. He is the Chair of IEEE Standards Group P1916.1, where he leads development of the standards for software-defined networking and network function virtualization performance. Some of his previous roles include the High Performance and Exascale Systems Team with IBM Research, a research fellow with Hamilton Institute, University of Toronto, a network scientist with RCUA for DARPA System F6, an assistant director of the Huawei-LET Technology Joint Telecom Center, and a faculty member of the Electrical Engineering Department at the University of Calgary, and the University of Engineering and Technology. He is one of the most cited authors in the areas of coding, a paradigm focused on improving system “success rate” as it is also a coinventor of spate coding, a paradigm focused on optimizing Big Data platforms. He has served as a chair, keynote, and lead-panelist for several distinct conferences, workshops and symposia in command area’s of networking, security, and entrepreneurship. He also holds editorial roles for major journals. He has received the Fulbright Fellowship, Presidential Scholarship, Ontario Graduate Scholarship, and Texas A&M Class Star Award.

WALTER CERRONI (SM) (walter.cerroni@unibo.it) is a tenured assistant professor of communication networks at the University of Bologna, Italy. In 1999 he was a visitor researcher at the Alcatel Corporate Research Center, Dallas, TX, USA. From 2003 to 2005 he worked as a research associate at the Italian National Inter-University Consortium for Telecommunications (CNI). In 2008 he was on short leave as a visiting assistant professor at the School of Information Sciences, University of Pittsburgh, PA, USA. His most recent research interests include: definition, implementation, and performance evaluation of intent-based northbound interfaces for programmable SDN/NFV infrastructures; design, implementation, and performance evaluation of virtual network function chaining in cloud computing platforms (e.g. OpenStack); modeling and design of inter-data and intra-data center interconnection networks for cloud computing infrastructures; and design of programmable, software-defined hybrid optical network architectures. He has contributed to several national and international research projects. He is currently serving as an associate technical editor for IEEE Communications Magazine and an associate editor for IEEE Communications Letters. Recently, he cochaired two IEEE ICC/Globecom symposia, four workshops on SDN/NFV-related topics, and has served as Publication Co-Chair for IEEE NetSoft 2017 and IEEE NFV-SDN 2017.

HAIWU HE (Haiwu.he@ericsson.com) is a senior security advisor in the areas of identity management, mobile devices and authentication at Aetna Global Information Security. He has extensive experience in identity and access management. He has worked with many standard organizations on developing next generation authentication technologies. His current focus is on decentralized identity management using distributed ledger technology. He holds a Ph.D. in computer engineering from Louisiana State University. In his more than 25 years in the software and security industry, he has been a professor of computer science, an application developer, data compression and encryption systems architect, security and compliance consultant, author and inventor of numerous security algorithms and articles.