future internet

MDPI

Editorial

Cyber-Physical Systems: Prospects, Challenges and Role in Software-Defined Networking and Blockchains

Uttam Ghosh [1,*], Deepak Tosh [2], Nawab Muhammad Faseeh Qureshi [3], Ali Kashif Bashir [4], Al-Sakib Khan Pathan [5,*] and Zhaolong Ning [6]

[1] Department of Computer Science and Data Science, Meharry Medical College, 1003 DB Todd Blvd., Nashville, TN 37208, USA
[2] Department of Computer Science, University of Texas at El Paso, 500 W. University Ave, El Paso, TX 79968, USA
[3] Department of Computer Education, Sungkyunkwan University, Seoul 03063, Republic of Korea
[4] Department of Computing and Mathematics, Manchester Metropolitan University, Manchester M15 6BH, UK
[5] Department of Computer Science and Engineering, United International University, Dhaka 1212, Bangladesh
[6] School of Software, Dalian University of Technology, Dalian 116620, China
* Correspondence: ghosh.uttam@ieee.org (U.G.); sakib.pathan@gmail.com (A.-S.K.P.)

check for updates

Citation: Ghosh, U.; Tosh, D.; Qureshi, N.M.F.; Bashir, A.K.; Pathan, A.-S.K.; Ning, Z. Cyber-Physical Systems: Prospects, Challenges and Role in Software-Defined Networking and Blockchains. *Future Internet* **2022**, *14*, 382. https://doi.org/10.3390/fi14120382

Received: 28 November 2022
Accepted: 9 December 2022
Published: 18 December 2022

In recent years, cyber-physical systems (CPSs) have gained a lot of attention from academia, industry and government agencies, considered to be the world's third wave of information technology, following computers and the internet. Software-defined networking (SDN) is an emerging technology that can be integrated with CPS to provide scalable, reliable, secure and efficient communication in heterogeneous infrastructures. The increasing importance of blockchain technology has clearly emerged, offering security solutions in various domains, including CPS. Given today's direction of cyber technologies, the goals of CPS, its challenges and the role of SDN and blockchains in CPS need to be identified. Therefore, this Special Issue aimed to invite researchers from academia, industry and government agencies to focus on bringing awareness to security challenges and attacks on the surface of modern cyber-physical systems, and to construct innovative solutions with the help of cutting-edge technologies, such as SDN and blockchains.

We especially sought submissions concerning blockchain-based security solutions of critical infrastructures, secure and resilient system architectures, protocols and applications for softwarized CPS environments and SDN capabilities in critical infrastructures, as well as key challenges facing the software-defined CPS of the future. In response, we received a considerable number of submissions, resulting in a total of seven papers being finally accepted. Here, we summarized the contributions of the authors, hailing from various parts of the globe.

In the paper "*Pulverization in Cyber-Physical Systems: Engineering the Self-Organizing Logic Separated from Deployment*", Roberto Casadei et al. [1] introduce a novel model for self-organizing CPSs that foster the "pulverization" of the structure and execution of global system behaviors, which they define as the ability to decompose macrolevel components and activity into microlevel ones. Additionally, they try to ensure deployment independence, which is the ability to move components and activities with different deployment targets. They validated their approach in a simulation case of pollution-aware household heat monitoring and control systems.

In the paper "*A MILP Model for a Byzantine Fault Tolerant Blockchain Consensus*", Vitor Nazário Coelho et al. [2] propose a MILP (mixed-integer linear programming) model that behaves similar to a very strong Byzantine adversary, capable of exploring many types of issues in consensus algorithms, including arbitrary network delays and generating intentional failures in an exact manner. The core idea of the paper is an exact adversarial model that explores current limitations for practical blockchain consensus applications, such as dBFT (delegated Byzantine fault tolerance), based on the idea that it can also be extended to other decentralized ledger technologies.

In their paper "*Challenges of PBFT-Inspired Consensus for Blockchain and Enhancements over Neo dBFT*", Igor M. Coelho et al. [3] explore variants of PBFT (practical Byzantine fault tolerance)-inspired consensus for blockchain, focusing on the dBFT consensus of the Neo blockchain. They discuss various challenges and possible enhancements to mechanisms in this domain. In their paper "*Improving Transaction Speed and Scalability of Blockchain Systems via Parallel Proof of Work*", Shihab Shahriar Hazari and Qusay H. Mahmoud [4] propose a method to improve the transaction speed and scalability of *permissionless* blockchain networks driven by proof-of-work (PoW) consensus mechanisms. The proposed method introduces a parallel PoW, in which all miners can together solve the puzzle by taking part in the competition. With the implementation and evaluation of the concept, the authors showed promising results.

A hybrid consensus algorithm based on a modified PoP (proof-of-probability) and DPoS (delegated proof of stake) is proposed in "*Hybrid Consensus Algorithm Based on Modified Proof-of-Probability and DPoS*" by Baocheng Wang et al. [5] Their system combines the advantages of the two consensus algorithms by adopting two different consensus algorithms for block generation and verification. In their work "*Blockchain and Fog Based Architecture for Internet of Everything in Smart Cities*", Parminder Singh et al. [6] design a framework named BFAN (Blockchain and Fog-based Architecture Network), to deploy Internet of Everything (IoE) applications in the smart city securely and optimally. BFAN architecture can reduce the fog node's average power consumption and make them scalable, and ensure that communication and computation are efficient. The major contributions of the proposed BFAN architecture include an energy-efficient platform for *thing-aware* wired/wireless TCP/IP connection, intra-primary communication in fog computing and security with Blockchain.

Finally, Abdelrahman Abuarqoub [7] contributed a review paper titled, "*A Review of the Control Plane Scalability Approaches in Software Defined Networking*", which explores different SDN (software-defined networking) controller scalability issues and topology-based and mechanism-based approaches, also discussing how they attempt to solve the scalability challenges. The author elaborates on the promising research trends and challenges, as well as some insights into relevant research issues.

We hope that the papers prove to be beneficial for the research community and provide them some insights into ongoing works in relevant fields.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Casadei, R.; Pianini, D.; Placuzzi, A.; Viroli, M.; Weyns, D. Pulverization in Cyber-Physical Systems: Engineering the Self-Organizing Logic Separated from Deployment. *Future Internet* **2020**, *12*, 203. [CrossRef]
2. Coelho, V.N.; Araújo, R.P.; Santos, H.G.; Qiang, W.Y.; Coelho, I.M. A MILP Model for a Byzantine Fault Tolerant Blockchain Consensus. *Future Internet* **2020**, *12*, 185. [CrossRef]
3. Coelho, I.M.; Coelho, V.N.; Araujo, R.P.; Qiang, W.Y.; Rhodes, B.D. Challenges of PBFT-Inspired Consensus for Blockchain and Enhancements over Neo dBFT. *Future Internet* **2020**, *12*, 129. [CrossRef]
4. Hazari, S.S.; Mahmoud, Q.H. Improving Transaction Speed and Scalability of Blockchain Systems via Parallel Proof of Work. *Future Internet* **2020**, *12*, 125. [CrossRef]
5. Wang, B.; Li, Z.; Li, H. Hybrid Consensus Algorithm Based on Modified Proof-of-Probability and DPoS. *Future Internet* **2020**, *12*, 122. [CrossRef]
6. Singh, P.; Nayyar, A.; Kaur, A.; Ghosh, U. Blockchain and Fog Based Architecture for Internet of Everything in Smart Cities. *Future Internet* **2020**, *12*, 61. [CrossRef]
7. Abuarqoub, A. A Review of the Control Plane Scalability Approaches in Software Defined Networking. *Future Internet* **2020**, *12*, 49. [CrossRef]