GUEST EDITORS' INTRODUCTION: Blockchain and Cyber-Physical Systems

An Braeken, *Member, IEEE,* Madhusanka Liyanage, *Member, IEEE,* Salil S. Kanhere, *Senior Member, IEEE,* and Sudhir Dixit, *Life Fellow, IEEE*

Abstract

Distributed ledger technologies like Blockchain inherent features such as consensus algorithms, distributed data storage and secure protocols which can be used to increase the robustness and reliability of cyber-physical systems. Thus, this special issue will elaborate on the opportunities, challenges and solutions to be offered by combining blockchain and Cyber-Physical Systems for different application domains.

Index Terms

Internet of Things, Cyber-physical Systems, Blockchain, Distributed Ledger Technologies

I. Main Content

The steam engine, electricity and digital economy all have made revolutionary changes in the world economy. Nowadays, utilizing sensor data from machinery can make similar impact in manufacturing, transportation, energy and health sectors. Performing big data analysis, switching to preventive maintenance and service-oriented production can boost efficiency, and even 1% reduction in costs in major sectors of economy could provide dramatic results. Cyber-physical systems (CPS) combine physical objects or systems with integrated computing facilities and data storage. Such CPSs can be interconnected in networks, within which they can exchange and share data and information with other objects and systems. For instance, CPS such as the Industrial Internet brings together the advances of two transformative revolutions. On the one hand, there are the myriad machines, facilities, fleets and networks that arose from the Industrial Revolution, and on the other hand the more recent powerful advances in computing, information and communication systems brought to the force by the Internet Revolution. According to [1] the global CPS market worldwide was valued at 60.50 Billion in 2018 dollars and is predicted to grow with a compound annual growth rate (CAGR) of 9.3% for the next ten years.

The Internet-of-things (IoT) in general is making a rapid progress in the Internet by providing connectivity to consumer devices such as toasters to enable their remote monitoring and integrated smart-home solutions. On the industrial side, such approach is referred to as Machine-to-machine or Machine-type Communication, which is supported in the latest ETSI standards. The Internet economics presently revolves around mining user data and providing targeted advertisement by giant companies including Google and Facebook. In fact, the best minds in network applications are focusing on creating the best algorithms to overcome advertisement blocking software and to sell something to the users.

Blockchain is another promising technology in ICT domain. For many researchers, the Blockchain technology has been seen as one of the most important innovations since the Internet and even of this century. A recent Gartner study estimates that blockchain will add $3.1 trillion in business value by 2030 [2]. Blockchain is a decentralized digital database (ledger) which stores the transactions committed by users. The authenticity of such transactions is verified by the connected community (miners) before adding them to the ledger. Thus, blockchain employs a distributed trust model by eliminating third party centralized trust model. In the blockchain, each block bundles an array of transaction records and the cryptographic chain links. Blockchain, like any other database, is technically prone to forgery. Such alterations are possible, if someone takes control of more than fifty one percent of miners and alter all of the transaction records within a very short period of time. However, this scenario is nearly impossible due to the distributed core architecture and the computational heavy mathematical puzzle, which is extensive and unreachable to solve, with current computing infrastructure.

One of the main major shortcomings in CPS and also more general IoT systems is the current centralized architecture models which will struggle to scale up to meet the demands of future CPSs. To solve such issues, the decentralized and consensus-driven distributed ledger technology like Blockchain and the combination of cryptographic processes behind it can offer an intriguing alternative. The combination of CPS/IoT and Blockchain will disrupt existing processes across a variety of industries, including manufacturing, agriculture, banking, transportation, shipping, energy, the financial sector and healthcare. However, it is still in its infancy. Moreover, the combination with CPS/IoT still requires essential insights with respect to concrete application domains, scalability, privacy issues, performance, and potential financial benefits.

An Braeken is with Industrial Engineering Department (INDI), Vrije Universiteit Brussel, Belgium. Email: an.braeken@vub.be

Madhusanka Liyanage is with the School of Computer Science, University College Dublin, Ireland and the Center for Wireless Communications, University of Oulu, Finland. e-mail:madhusanka@ucd.ie

Salil Kanhare is with the School of Computer Engineering, University of New South Wales, Sydney, Australia. e-mail:salil.kanhere@unsw.edu.au

Sudhir Dixit is with Basic Internet Foundation, USA. e-mail:sudhir.dixit@ieee.org

Manuscript received April 19, 2005; revised August 26, 2015.

A. General Challenges in CPS and IoT

More specific for the new cyber-physical systems like the Industrial internet in new applications, due to their popularity, new requirements are created such as high security, enhanced scalability, optimal utilization of network resources, efficient energy management, and low operational cost. Specifically, the increasing number of connected and heterogeneous devices together with a large set of new services will result in the increasing capacity requirements for the CPSs. Thus, accommodating the secure connectivity for this expected traffic growth is an imminent requirement of future CPSs. Although the existing secure communication architectures are able to provide a sufficient level of security, they are suffering from limitations such as limited scalability, over utilization of network resources and high operational cost, mainly due to the complex and static security management procedures organized in a centralized architecture.

In addition, due to this centralized architecture in IoT and CPS, the data is often stored in isolated data silos, making data analysis more difficult and slowing down data research. Moreover, a complete trust is needed in cloud and application providers since there is a lack of control possibilities by the user over how the data is shared and collected. In particular, for IoT devices collecting highly personal data like health related parameters, this presents a major privacy issue.

Furthermore, CPS/IoT has a vast ecosystem. The capabilities of IoT devices are largely heterogeneous. In addition, it supports a wide variety of different communication technologies, different software stacks, different operating systems and different topologies. Also, CPS/IoT network are highly dynamic due to sleep modes in IoT devices. As a results, it is challenging to maintain a coherent service platform. Different stakeholders have to work together to enable proper operation of the network.

B. What are the features in Blockchain and how these features will solve above general challenges

Blockchain will offer a rich set of features such as decentralization, immutability, distrubuted trust, enhanced security, faster settlements, smart contracts, digital currency and minting which can be used to solve these challenges. Blockchain will enable IoT devices/CPSs to send data to private blockchain ledgers for inclusion in shared transactions with tamper-resistant records. The distributed replication of Blockchain enables vertical industries and various CPS data users to access and supply IoT data without the need for central control and management. All stakeholders in the CPS ecosystem can verify each transaction, preventing disputes and ensuring each user is held accountable for their individual roles in the overall transaction. Thus, the development of such a secure and dependable model for each piece of the CPS ecosystem can serve as an intriguing alternative to the traditional client/server transaction model.

Blockchain based smart contacts, i.e. a piece of auto executable code upon meeting the predefined conditions, can be used to automate many CPS related processes such as IoT data sharing, device ownership transfer, new user registration, security certificate deployment and revocation etc. A minting process allows to use digital currency instead of fiat currency. It helps to settle the transactions fast and without involvement of a third party moderator. Moreover, a digital currency allows to create digital market place to trade resources in many CPSs such as smart grids, transport systems, logistic networks, etc [3].

The exploitation of blockchain in the domain of CPS enables distributed security since its combination with cryptographic processes behind it, offers an intriguing alternative to the centralized security. Because blockchain is built for decentralized control, a security scheme based on it should be more scalable than a traditional one. Furthermore, blockchain's strong protections against data tampering would help prevent a rogue device from disrupting a home, factory or transportation system by relaying misleading information. Thus, the blockchain technology holds the potential to securely unlock the business and operational value of CPSs to support common tasks, such as sensing, processing, storing information, and communicating.

Clear advantages and opportunities have been already identified in the combination of blockchain and CPS for different application domains. First, in supply chain management, several issues like detection of the source of infection, food fraud, illegal production and food recall, require a transparent, decentralized and robust tracebility scheme for monitoring the origin of raw materials, the quality of the products measured by IoT sensors, the handover actions between different players, etc. Blockchain CPS based technology enables a perfect answer to these questions, as being demonstrated in [4]. Second, another very important application domain in which CPS is already strongly integrated and blockchain technology can offer strong added value is in Industrial IoT (IIoT). Here, blockchain will enable support to the reliability challenge and offer possibilities to integrate automation and accountability via a reputation and trust based framework [5]. Many more examples exist in different application domains, like e-health, vehicular networks, smart grids, etc.

C. What are the technical and societal challenges related to Blockchain CPS integration

The usage of distributed ledger technology for CPS/IoT is not straightforward and contains inherent particularities. First of all, the regular consensus mechanisms like proof of work are often too complex in a CPS/IoT based application and lead to a too high delay and too low throughput, which is unacceptable for many applications. Also, the typical Blockchain applications require incentives for mining, which is not directly present in a CPS based use case. Therefore, dedicated distributed ledger technologies and architectures taking into account the realtime nature of many CPS applications and the constrained character of the IoT devices, still offering sufficient scalability, is an important research direction.

From a theoretical point of view, using mathematical modelling, it can be proven that distributed ledger technologies offer very strong security. Although, history has shown that this statement is not at all true in practice. Between beginning of 2017

and 2019, hackers, both lonely opportunistic ones and sophisticated cybercrime organizations have stolen more than 2 billion dollars of cryptocurrencies [6], which only reflects the publicly revealed data and is probably even much higher in reality. Few of the attacks are due to implementation bugs on the platforms, which consist of very complex code and thus are easily prone to small subtle leaks. Consequently, special attention should be paid to that when developing own dedicated application specific Blockchain CPS systems. However, most of the hacks are on the transactions, exploiting the 51% rule attack leading to double spends, which is currently inherently available in most platforms relying on the proof of work consensus for transaction verification. While this attack is very costly on popular blockchains like Bitcoin, it becomes much more attractive on the more than 1500 other smaller cryptocurrencies on the market. Moreover, a promising dedicated distributed ledger platform especially dealing with scalability issues present in IoT applications, called Tangle, is even more vulnerable and only requires a control of 34% by the attacker. Another recently very popular type of attack is on the exploitation of bugs in smart contracts. In particular, for Blockchain CPS systems, several dedicated smart contracts need to be developed in order to offer application specific features to its users. These bugs are very difficult to fix as already executed transactions cannot be easily reversed. In order to overcome all these types of blockchain hacking, several companies have started to offer auditing services to detect mal behavior and suspicious transactions using artificial intelligence mechanisms. Also formal verification proofs have been developed to identify errors or potential vulnerabilities in both platform and smart contract.

Finally, one of the major barriers for effective adoption of blockchain based technology in the future is to increase the acceptance rate with both developers as consumers and broad audience. Despite the well known advantages that the technology can offer with respect to automation, transparency of the processes, privacy protection and independence of banks or other third parties, only a limited amount of people and companies are currently exploiting its usage. This is not only due to lack of knowledge and understanding of the principles behind it, but also mainly due to lack of trust in the underlying technology caused by the news with regular reports on cybercrime against blockchain based platforms. A potential solution to overcome this barrier is to issue certificates to blockchain solutions or platforms, which have undergone a thorough audit based on some transparent criteria. In addition, insurance companies can define specific insurances to offer assistance in case of fraud.

II. In this Issue

This issue has selected five papers, three dealing with blockchain based industrial IoT applications and two papers dealing with energy based systems.

O. Bouachir, M. Aloqaily, L. Tesng, A. Boukerche, Blockchain and fog computing for cyber-physical systems: case of smart industry

Bouachir et al. discuss the integration of blockchain technology in a fog-based architecture for industrial IoT. Besides the many advantages like reduced latency, availability and increased security that can be offered, several opportunities but also challenges have been identified for this type of architecture.

J. Pennkamp, R. Matzutt, S.S. Kanhere, J. Hiller, K. Wehrle, The road to accountable and dependable manufacturing

Automatisation of manufacturing processes mandate high levels of security, privacy, accountability and verifiability. Research in such accountable and dependable manufacturing is structured into three layers, related to blockchain inherent challenges, scenario-driven challenges and socio-economic challenges. It is explained how blockchain can play a major role in this.

C.T.B. Garrocho, M.C. Silva, C.F.M. da Cavalcanti, R.A.R. Oliveira, Real-time systems implications in blockchain-based vertical integration of Industry 4.0

In this paper, Garrocho et al. analyse a real scenario via a proof of concept in a blockchain based industrial process automatisation system and showed several limitations regarding time, variation and loss of blocks, which is unacceptable due to the high reliability requirements in this type of settings. In future, it will be studied if blockchain better suits for applications to support auditing and the implementation of business/process roles.

F.S. Ali, M. Aloqaily, O. Alfandi, O. Ozkasap, Cyberphysical blockchain-enabled peer-to-peer energy trading

Ali et al. propose three blockchain based peer-to-peer energy trading models. They explain how the usage of blockchain technology allows to overcome several technical challenges and market barriers. For instance, the blockchain based approaches avoid single point of failure, support heterogeneity, increase trust between trustless parties, and allow payments via cryptocurrencies or energy coins instead of bank/visa transactions. Still several open issues are identified.

S. Eisele, C. Barreto, A. Bubey, X. Koutsoukos, T. Eghtesad, A. Laszka, A. Mavridou, Blockchains for transactive energy systems: opportunities, challenges and approaches

Eisele et al. present a blockchain based transactive energy system (TRANSAX). By defining external solvers in the consensus algorithm, also constrained prosumer IoT devices can participate in the market and a high reliability is obtained. Privacy is enabled due to the use of tradeable and mixable energy assets.

III. Conclusion

A lot of research is going to concrete dedicated blockchain based applications, each solving particular issues present in its domain. It will be interesting to see if generic solutions can be proposed in future, applicable to a multitude of application domains with only small adaptations.

REFERENCES

[1] C. Research, "Component (hardware, software, services); deployment (on premise, cloud); vertical (aerospace and defense, automotive, energy and utility, healthcare, manufacturing, consumer electronics, others)) — growth, future prospects and competitive analysis, 2019–2027," *Report code 59919-09-19*, 2019.

[2] B. Granetto, R. Kandaswamy, J.-D. Lovelock, and M. Reynolds, "Forecast: Blockchain business value, worldwide, 2017-2030," *Gartner G00325744*, 2017.

[3] A. Suliman, Z. Husain, M. Abououf, M. Alblooshi, and K. Salah, "Monetization of iot data using smart contracts," *IET Networks*, vol. 8, no. 1, pp. 32–37, 2018.

[4] K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration," 2017.

[5] S. Malik, V. Dedeoglu, S. Kanhere, and R. Jurdak, "Trustchain: Trust management in blockchain and iot supported supply chains," *IEEE International Conference on Blockchain*, 2019.

[6] M. Orcutt, "Blockchain/smart contracts, once hailed as unhackable, blockchains are now getting hacked, an open block revealing digital coins within ms tech, mit technology review," *https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/*, 2019.

Prof: An Braeken is a Professor at the Vrije Universiteit Brussel (VUB). Her research interests include the development, analysis and evaluation of privacy and security issues in wireless networks, IoT, CPSs, 5G networks, etc.

Asst. Prof. Madhusanka Liyanage is currently an Ad Astra Fellow/Assistant Professor at University College Dublin, Ireland and an adjunct professor at the Centre for Wireless Communications, University of Oulu, Oulu, Finland. His research interests are SDN, IoT, Block Chain, mobile and virtual network security.

Prof. Salil S. Kanhere is a Professor in the School of Computer Science and Engineering at UNSW Sydney, Australia. His research interests include Internet of Things, pervasive computing, blockchain, cybersecurity and applied machine learning.

Dr. Sudhir Dixit is a Co-Founder Evangelist of Basic Internet at the Basic Internet Foundation in Norway and heads its San Francisco office. His research interests are mobile communications, virtualization, SDN, network slicing, and bridging the digital divide globally.