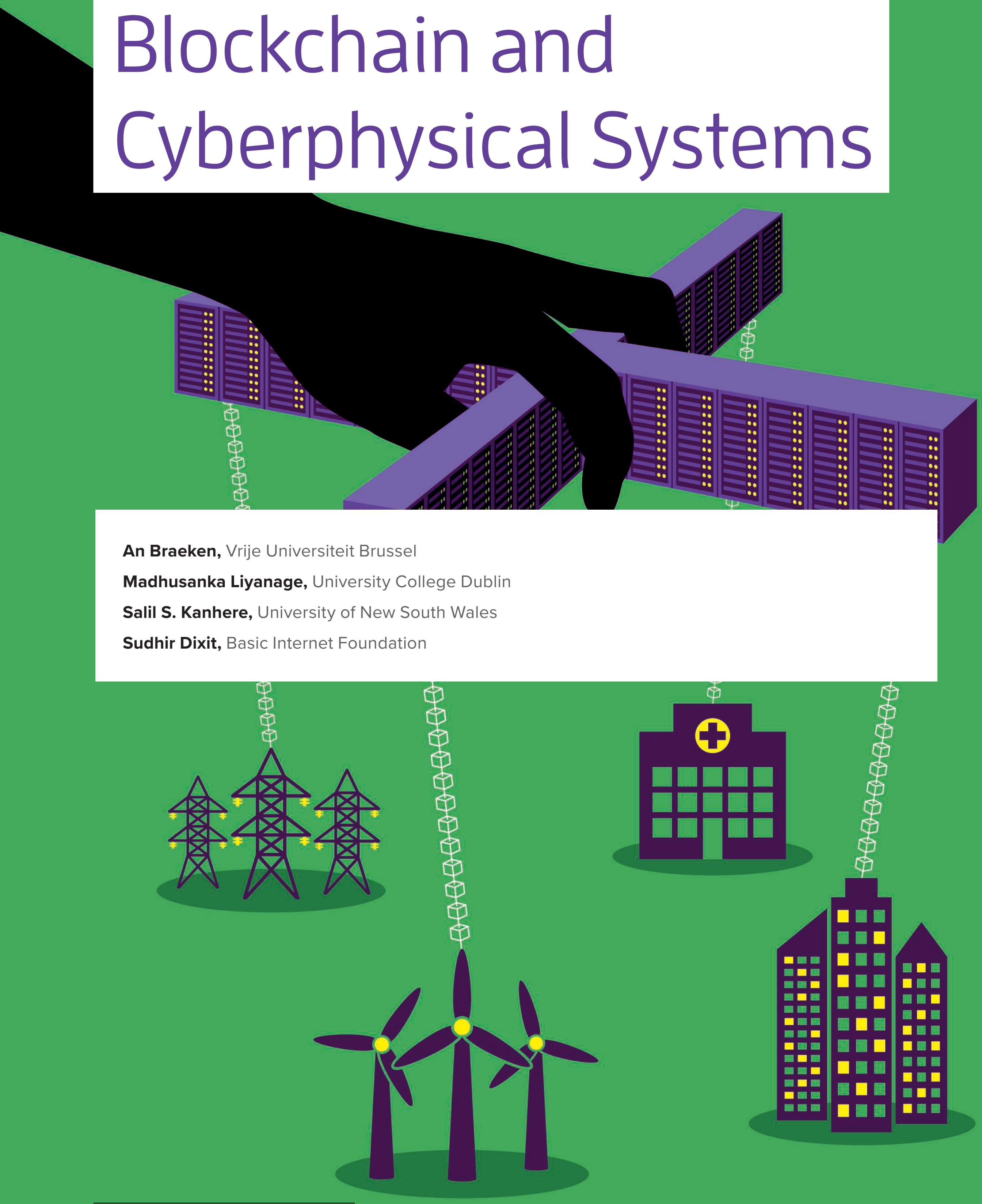
Blockchain and Cyberphysical Systems



An Braeken, Vrije Universiteit Brussel

Madhusanka Liyanage, University College Dublin

Salil S. Kanhere, University of New South Wales

Sudhir Dixit, Basic Internet Foundation

Digital Object Identifier 10.1109/MC.2020.3005112
Date of current version: 4 September 2020

This theme issue will elaborate on the opportunities, challenges, and solutions to be offered by combining blockchain and cyberphysical systems for different application domains.

The steam engine, electricity, and the digital economy all have made revolutionary changes in the world's economy. Nowadays, utilizing sensor data from machinery can make a similar impact in the manufacturing, transportation, energy, and health sectors. Performing big data analysis, switching to preventive maintenance, and service-oriented production can boost efficiency—even a 1% reduction in costs in major sectors of the economy could provide dramatic results. cyberphysical systems (CPSs) 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, a CPS like the Industrial Internet of Things (IIoT) 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 Credence Research,[1] the global CPS market worldwide was valued at US$60.50 billion in 2018 and is predicted to grow with a compound annual growth rate of 9.3% for the next 10 years.

The Internet of Things (IoT) in general is making rapid progress by providing connectivity to consumer devices, such as toasters, to enable their remote monitoring and integrated smart-home solutions. On the industrial side, such an approach is referred to as machine-to-machine or machine-type communication, which is supported in the latest standards of the European Telecommunications Standards Institute. Internet economics presently revolves around mining user data and providing targeted advertisements 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 sell something to the users.

Blockchain is another promising technology in the information and communications technology domain. For many researchers, 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 US$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 a third-party centralized trust model. In the blockchain, each block bundles an array of transaction records and their cryptographic chain links. Blockchain, like any other database, is technically prone to forgery. Such alterations are possible if someone takes control of more than 51% of the miners and alters 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 computationally heavy mathematical puzzle, which is extensive and unreachable to solve, with current computing infrastructure.

One of the major shortcomings in a CPS and 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, 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 CPSs/IoT and blockchains will disrupt existing processes across a variety of industries, including manufacturing, agriculture, banking, transportation, shipping, energy, the financial sector, and health care. However, it is still in its infancy. Moreover, the combination with CPSs/IoT still requires essential insights with respect to concrete application domains, scalability, privacy issues, performance, and potential financial benefits.

GENERAL CHALLENGES IN CPS AND IoT

More specific for the new CPSs like the IIoT is that new requirements are created in new applications, due to their popularity. These include 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 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 the IoT and CPSs, the data are 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 are shared and collected. In particular, for IoT devices collecting highly personal data, such as health-related parameters, this presents a major privacy issue.

Furthermore, the 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, software stacks, operating systems, and topologies. Also, CPS/IoT networks are highly dynamic due to sleep modes in IoT devices. As a result, it is challenging to maintain a coherent service platform. Different stakeholders have to work together to enable proper operation of the network.

The features in blockchain to solve these general challenges

Blockchain will offer a rich set of features, such as decentralization, immutability, distributed 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 all users 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 (for example, 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, and so on. A minting process allows the use of digital currency instead of fiat currency. It helps to settle the transactions quickly and without the involvement of a third-party moderator. Moreover, a digital currency allows the creation of a digital marketplace to trade resources in many CPSs, such as smart grids, transport systems, logistic networks, and so on.[3]

The exploitation of blockchain in the domain of CPSs enables distributed security since the cryptographic processes behind it offer an intriguing alternative to 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, 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 already been identified in the combination of blockchain and CPSs for different application domains. First, in supply chain management, several issues, such as the detection of the source of infection, food fraud, illegal production, and food recall, require a transparent, decentralized, and robust traceability scheme for monitoring the origin of raw materials, the quality of the products measured by IoT sensors, the handover actions between different players, and so on. Blockchain CPS-based technology enables a perfect answer to these questions, as demonstrated in Korpela et al.[4] Second, another very important application domain in which a CPS is already strongly integrated and blockchain technology can offer strong added value is in 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, and so on.

Technical and societal challenges related to blockchain CPS integration

The use of distributed ledger technology for a 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 are not directly present in a CPS-based use case. Therefore, dedicated distributed ledger technologies and architectures that account for the real-time nature of many CPS applications and the constrained character of the IoT devices, while still offering sufficient scalability, are important research directions.

From a theoretical point of view, it can be proven, by using mathematical modeling, that distributed ledger technologies offer very strong security, although history has shown that this statement is not at all true in practice. Between the beginning of 2017 and 2019, hackers (both lonely opportunistic ones and sophisticated cybercrime organizations) have stolen more than US$2 billion dollars of cryptocurrencies,[6] a figure that 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 dedicated applications of specific blockchain CPSs. 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 1,500 other smaller cryptocurrencies on the market. Moreover, a promising dedicated distributed ledger platform called *Tangle*, which deals especially with scalability issues present in IoT applications, is even more vulnerable and only requires a control of 34% by the attacker. Another recent and very popular type of attack is on the exploitation of bugs in smart contracts. In particular, for blockchain CPSs, several dedicated smart contracts need to be developed to offer application-specific features to its users. These bugs are very difficult to fix, as already executed transactions cannot be easily reversed. To overcome all of these types of blockchain hacking, several companies have started to offer auditing services to detect mal behavior and suspicious transactions using artificial intelligence mechanisms. Formal verification proofs also have been developed to identify errors or potential vulnerabilities in both platforms and smart contracts.

Finally, one of the major barriers for the effective adoption of blockchain-based technology in the future is to increase the acceptance rate with both developers as consumers and a broad audience. Despite the well-known advantages that the technology can offer with respect to automation, transparency of processes, privacy protection, and independence of banks or other third parties, only a limited number of people and companies is 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 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 help in case of fraud.

IN THIS ISSUE

This issue has selected four articles, two dealing with blockchain-based IIoT applications and two dealing with energy-based systems. In "Blockchain and Fog Computing for Cyberphysical Systems: The Case of Smart Industry," Bouachir et al. discuss the integration of blockchain technology in a fog-based architecture for IIoT. Besides the many advantages that can be offered, such as reduced latency, availability, and increased security, several opportunities and also challenges have been identified for this type of architecture.

Automatization 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's inherent, scenario-driven, and socio-economic challenges.

In "Real-Time Systems Implications in the Blockchain-Based Vertical Integration of Industry 4.0," Garrocho et al. analyze a real scenario via a proof of concept in a blockchain-based, industrial process automatization 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. If blockchain is better suited for applications to support auditing and the implementation of business/process roles will be looked at in future studies.

Ali et al. propose three blockchain-based, peer-to-peer energy trading models in "Cyberphysical Blockchain-Enabled Peer-to-Peer Energy Trading." They explain how the usage of blockchain technology can 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.

In “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, constrained prosumer IoT devices can also participate in the market and a high reliability is obtained. Privacy is enabled due to the use of tradeable and mixable energy assets.

Considerable research is being directed toward 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 the future, applicable to a multitude of application domains with only small adaptations.

REFERENCES

1. “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,” Credence Research, 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, Stamford, CT, G00325744, 2017.
3. A. Suliman, Z. Husain, M. Abououf, M. Alblooshi, and K. Salah, “Monetization of IoT data using smart contracts,” *IET Netw.*, vol. 8, no. 1, pp. 32–37, 2018. doi: 10.1049/iet-net.2018.5026.
4. K. Korpela, J. Hallikas, and T. Dahlberg, “Digital supply chain transformation toward blockchain integration,” in *Proc. Hawaii Int. Conf. System Sciences (HICSS)*, 2017, pp. 1–10. doi: 10.24251/HICSS.2017.506.
5. S. Malik, V. Dedeoglu, S. Kanhere, and R. Jurdak, “Trustchain: Trust management in blockchain and IoT supported supply chains,” in *Proc. IEEE Int. Conf. Blockchain*, 2019, pp. 184–193. doi: 10.1109/Blockchain.2019.00032.
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*, Feb. 19, 2019. [Online]. Available: https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/

ABOUT THE AUTHORS

AN BRAEKEN is a professor in the Industrial Engineering Department of the Vrije Universiteit Brussel, Brussels, Belgium. Her research interests include the development, analysis, and evaluation of privacy and security issues in wireless networks, the Internet of Things, cyberphysical systems, 5G networks, and so forth. She is a Member of IEEE. Contact her at an.braeken@vub.be.

MADHUSANKA LIYANAGE is an Ad Astra Fellow/assistant professor in the School of Computer Science, University College Dublin, Ireland and an adjunct professor at the Center for Wireless Communications, University of Oulu, Finland. His research interests include software-defined networking, the Internet of Things, blockchain, and mobile and virtual network security. He is a Member of IEEE. Contact him at madhusanka@ucd.ie.

SALIL S. KANHERE is a professor in the School of Computer Science and Engineering at the University of New South Wales, Sydney, Australia. His research interests include the Internet of Things, pervasive computing, blockchain, cybersecurity, and applied machine learning. He is a Member of IEEE. Contact him at salil.kanhere@unsw.edu.au.

SUDHIR DIXIT is a cofounder evangelist of basic Internet at the Basic Internet Foundation in Norway and heads its San Francisco office. His research interests include mobile communications, virtualization, software-defined networking, network slicing, and bridging the digital divide globally. He is a Life Fellow of IEEE. Contact him at sudhir.dixit@ieee.org.