Guest Editors' Introduction

Distributed Ledger Technologies

Fred Douglis
Perspecta Labs

Angelos Stavrou
George Mason University

Distributed Ledger Technologies (DLT), of which blockchain is a popular example, are increasingly becoming a popular means to maintain transactional integrity and achieve consensus among competing parties in many modern distributed data exchanges. Indeed, a Gartner survey estimates that by 2020, DLT and blockchain will support the global movement and tracking of $2 trillion of goods and services annually.[1] Unlike centralized files and databases, distributed ledgers rely on peering nodes to record, share, and synchronize transactions and data in their individually maintained local ledgers. In the case of blockchain, information is organized into blocks that are securely and transparently chained together. These blocks become immutable global knowledge among all peers using consensus algorithms to achieve data synchronization. The "append-only, globally accepted" transactions supported by blockchain technologies have given rise to both opportunities and challenges compared to traditional data storage systems.

One of the challenges faced by current information sharing systems, and a key concept that makes DLT appealing is the support for the creation of large scale systems from nodes and components that do not trust each other. Being able to reach consensus and share a commonly verifiable ledger is a very powerful primitive, which is already being considered for data sharing applications in energy, pharmaceuticals, and many other domains. A brief by World Bank[2] mentions that blockchain and DLT are the building block of "Internet of value," and enable recording of interactions and transfer "value" in a peer-to-peer fashion, without a need for a centrally coordinating entity. In this context, ownership and control of the data are central and *"value"* can take many forms to include any data record that represents a transaction of ownership of assets. Examples of DLT enabling value-based data sharing include money, securities, land titles, wireless spectrum, and other forms of data associated ownership. DLT is also useful for controlling access to information, such as identity and health records.

Of course, like any other technology, DLT have limitations, too: many researchers have pointed out security and privacy challenges with the use of consensus algorithms and their dependence on the persistence and control of individual peers. These limitations have given rise to different blockchain designs spanning from public/permissionless to private/permissioned and logic-oriented to transaction-oriented approaches utilizing different consensus algorithms.[3] Overall, it seems that DLT have the potential to be disruptive and impactful in many use cases. DLT are not meant to be a sweeping replacement for traditional databases and storage solutions but rather a powerful and targeted option to be deployed only in certain use cases.

Digital Object Identifier 10.1109/MIC.2020.3002415
Date of current version 21 July 2020.

Published by the IEEE Computer Society

IN THIS ISSUE

There are two articles in this DLT issue that show how distributed ledgers can be used to share critical information in a secure and auditable manner across multiple participating entities. Moreover, the sharing of information takes place among parties that might have competing business incentives and availability of resources. Finally, the articles demonstrate the ability of DLT to apply regulatory requirements and maintain globally agreed audit trails without a centralized trusted authority.

The first article, titled "Distributed Ledgers for Spectrum Authorization," is authored by Cigdem Sengul and demonstrates how DLT can create business incentives for wireless spectrum owners to open their spectrum for sharing among multiple cross-industry stakeholders. This use case exemplifies the strengths of DLT to act as a precise and transparent interorganizational record-keeping medium. Through the use of smart contracts, spectrum can be traded between participants allowing for security and privacy while maintaining auditability on demand. The article goes into more technical details on the governance, protocols, network, and data operations of a DLT-based spectrum authorization system discussing both the challenges and limitations of existing and DLT systems.

The second article examines the use of DLT as a means for sharing cybersecurity information including security vulnerabilities and cybersecurity readiness. Furthermore, DLT can be employed to authenticate security certifications between collaborating entities with different requirements. Indeed, in the article titled "An Interledger Blockchain Platform for Cross-border Management of Cybersecurity Information," José Luis Hernández-Ramos and his colleagues discussed how blockchain approaches foster cooperation and ensure transparency and immutability of the cybersecurity information. Again, the use of DLT is applied to ensure distributed trust, transparency, and accountability, whereas at the same time achieving scalability, performance, and interoperability on a global scale.

REFERENCES

1. Dec. 2018. [Online]. Available: https://www.gartner.com/document/3895043.
2. Apr. 2018. [Online]. Available: https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt
3. W. Wang *et al.*, "A survey on consensus mechanisms and mining strategy management in blockchain networks." *IEEE Access*, vol. 7, pp. 22328–22370, Jan. 2019. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8629877

Fred Douglis is a chief research scientist with Perspecta Labs, where he works on applied research in the areas of high-performance computing, network optimization, blockchain, and security. He received the M.S. and Ph.D. degrees from U.C. Berkeley, CA, USA, and the B.S. degree from Yale University, CT, USA, all in computer science. He is a member of the IEEE Computer Society Board of Governors. He was an editor-in-chief of *IEEE Internet Computing* from 2007 to 2010, and has been on its editorial board since 1999. He is also on the editorial boards of IEEE Transactions on Computers and *ACM Transactions on Storage*. He formed the IEEE-CS Technical Committee on the Internet, chairing it from 1997–2000, and previously chaired the TC on Operating Systems from 1996–1998. He is a Fellow of the IEEE. Contact him at f.douglis@computer.org.

Angelos Stavrou is a professor with the Computer Science Department, George Mason University, VA, USA, and a founder of Kryptowire LLC, a Virginia-based mobile security company. His current research interests include security and reliability for distributed systems, security principles for virtualization, and anonymity with a focus on building and deploying large-scale systems. He received the M.Sc. degree in electrical engineering, and the M.Phil. and Ph.D. degrees, with distinction, in computer science, from Columbia University, New York, NY, USA. His team is the recipient of the DHS Cyber Security Division's "Significant Government Impact Award" in 2017 and "Bang for the Buck Award" in 2019. In 2013, he became the recipient of the IEEE Reliability Society Engineer of the Year award. He is a NIST guest researcher, a member of the ACM and USENIX. He is a Senior Member of the IEEE. Contact him at astavrou@gmu.edu.