IN THIS ISSUE

In this issue, we return to a topic that was central to several *Computer* issues in 2020: distributed ledger technology and blockchain.

In the article "A Taxonomy for Distributed Ledger Analytics," the authors argue that, with increasing transaction volumes and the proliferation of decentralized applications based on smart contracts, the need for a deeper understanding of distributed ledger technology arises. They offer the idea of distributed ledger analytics (DLA). The authors also outline a taxonomy for DLA and propose that most analyses currently rely on transaction data but that the extended focus areas on governance, smart contracts, and value analytics each offer their own opportunities for future research.

In "A Novel Reputation System for Mobile App Stores Using Blockchain," the authors suggest that thousands of mobile applications may be accompanied by an increase in malware that is detected only after infecting users or when this problem is reported back to the store. They offer a potential solution that would be to leverage such reports across all mobile ecosystems, creating a reputation system for both consumers and app developers. This article presents a scalable blockchain-based solution for reputation management to provide the necessary requirements while still being cost-effective.

In the last article, "A Secure and Flexible FPGA-Based Blockchain System for the IIoT," the authors assert that blockchain is a promising solution for Industry 4.0 because of its security and scalability. However, they contend that it is not straightforward to apply blockchain to the Industrial Internet of Things (IIoT) because of endpoint security. They also propose a secure and flexible field-programmable gate array (FPGA)-based blockchain system for IIoTs. In their proposed architecture, the secret key generation, sensor data monitoring, and transaction generation are conducted inside the FPGA in an isolated manner. Because only restricted access to the FPGA is allowed, adversaries who have the root privilege still cannot trick the system with illegal or fake transaction generation.

Digital Object Identifier 10.1109/MC.2021.3052614
Date of current version: 11 February 2021

—Jeffrey Voas, Editor in Chief

information, they may lose. How? For example, consumers may lose out on the benefits when a company delivers advertisements that provide discounts. If they share too much, problems such as identity theft can easily occur.

Whether user data are protected depends greatly on the stakeholders' (for example, consumers, advertisers, and social media platforms) valuation of such data. Data privacy regulations generally consider two types of consequences: 1) allocative (the total amount advertisers are willing to pay for consumers' data) and 2) distributional (how the amount spent on data is distributed across social media platforms and to consumers).

When personal data privacy is weak, allocative and distributional effects more likely benefit social media providers. The real issue that underlies the privacy debate concerns consumers' lack of ability to control their personal information. The distributional effects of data privacy laws favor social media platforms if they can share user data with advertisers deceptively or without permission and face no penalty.

While little regulatory attention has been paid to this issue in terms of the monetary value of personal data, governments are beginning to take personal data privacy a bit more seriously. Why? Some nations now perceive new national security threats when their citizens are being improperly monitored by foreign governments.

Finally, you, as a generator of data, may unknowingly create various forms of value, including

DISCLAIMER

The authors are completely responsible for the content in this article. The opinions expressed here are their own.