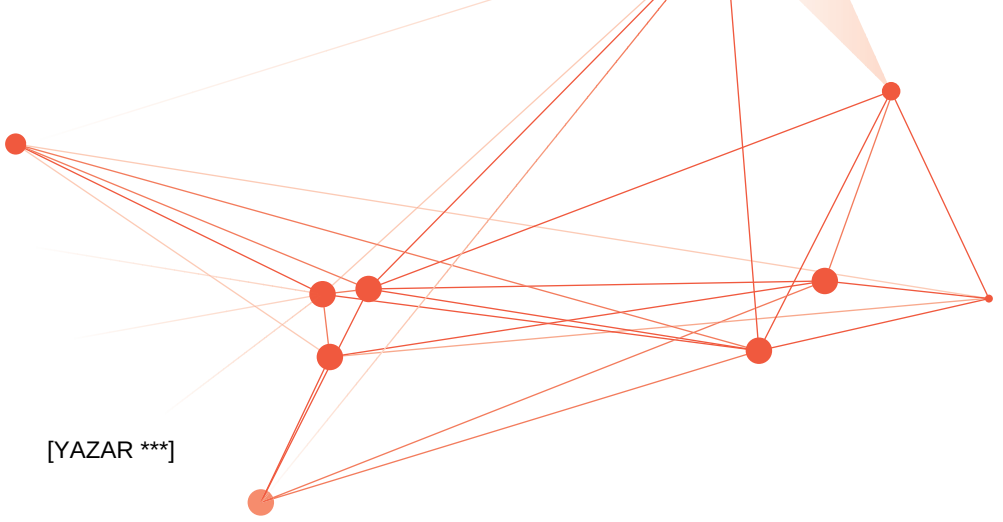
[YAZAR***]

in Finance

0018-9162/17/$33.00 © 2017 IEEE



[YAZAR ***] [KURUM ***] [YAZAR ***]
,
[YAZAR ***] [YAZAR ***]
, R3
[YAZAR ***]
, Blockseer

*The banking and financial-services industry has taken notice of [YAZAR ***]'s many advantages. This special issue explores its unlikely origins, tremendous impact, implementation challenges, and enormous potential.*

Blockchain technology promises to be hugely disruptive and empowering in both public and private sector computing applications. As a way to order transactions in a distributed ledger, blockchains offer a record of consensus with a cryptographic audit trail that can be maintained and validated by multiple nodes. It lets contracting parties dynamically track assets and agreements using a common protocol, thus streamlining and even completely collapsing many in-house and third-party verification processes.

Originally conceived as the basis of cryptocurrencies, aspects of [YAZAR ***] [YAZAR ***] have far-reaching potential in many other areas. To understand this potential, it is important to distinguish two core blockchain components: distributed-ledger technology (DLT) and smart contracts.

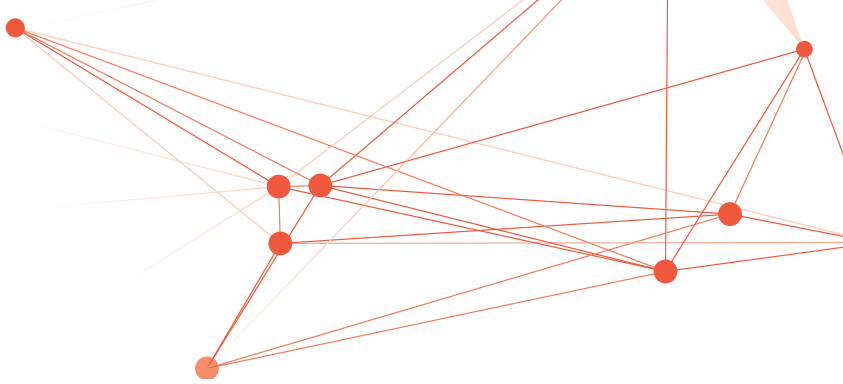
A *distributed ledger* is a decentralized, shared, replicated, and synchronized record of transactions between contracting parties secured by cryptographic sealing. Unlike a distributed database, nodes of a distributed ledger cannot trust other nodes and so must independently verify transactions before applying them. Distributed ledgers are divided into two broad classes: those that seek to minimize the role of trusted and identifiable third parties, and those that explicitly rely on identifiable third parties for some subset of the system's properties. Not all distributed ledgers are blockchains, but all blockchains are distributed ledgers.

A *smart contract* constitutes the rules that participants have collectively agreed upon to govern the evolution of "facts" in the distributed ledger. Such smart contracts can be computer programs that attempt to ensure that all transactions comply with the underlying legal agreements and that the records managed by DLT are authoritative with respect to the existence, status, and evolution of the underlying legal agreements they represent. When paired with a blockchain that records changes of asset ownership, a smart contract can serve as a wrapper for a transaction that automatically moves value and executes the contract's terms. Smart contracts also have the potential to automate laws and statutes, which could significantly improve government services' efficiency and transparency.

BLOCKCHAIN BASICS

In simple terms, the technology handles blocks—uniquely identified, linked transaction records—in a chain. A blockchain is a continuously growing, distributed, shared ledger of such blocks, which are sealed cryptographically with a digital fingerprint generated by a hashing function. Each block is "chained" to the previous one by referring to its hash value. The computers, or nodes, that connect to the blockchain verify that a transaction is valid per the rules of the governing logic—namely, the smart contract. The defining characteristic of many blockchain platforms is the confirmation process by which new records are added to the ledger.

Blockchain systems possess a number of attractive attributes for the banking and financial-services markets. Such systems are *resilient* and can operate as decentralized networks that do not require a central server and do not have a single point of failure. Because they operate using distributed open source protocols, they have *integrity* and do not need to trust a third party to execute transactions. Public blockchain



JOIN OUR ROUNDTABLE DISCUSSION

As part of this special issue of *Computer*, Tim Swanson of R3 chaired a roundtable with blockchain experts. Swanson discusses the trajectory of [YAZAR ***] [KURUM ***] with an expert panel featuring Sarah Meiklejohn, [YAZAR ***] London (UCL); Andrew Miller, University of Illinois at Urbana–Champaign; Elaine Shi, Cornell University; Angela Walch, St. Mary's University School of Law and UCL; and Zooko Wilcox-O'Hearn, Zcash. Join us at youtu.be/wPFxKnlu1bA to listen to a discussion of the essential issues, including privacy, security, and the technology's future impact.

systems are also inherently *transparent*, because all changes are visible by all parties. The blockchain functionality also allows applications and users to operate with a high degree of confidence because transactions are *unchangeable*—they cannot be reversed or resequenced. In general, blockchain systems are uniquely able to ensure that contracting parties all have accurate and identical records.

IN THIS ISSUE

In the banking and financial-services domain, [YAZAR ***] can simplify business processes while creating safe, trustworthy records of agreements and transactions. The five articles in this special issue of *Computer* describe numerous facets of the technology's potential impact.

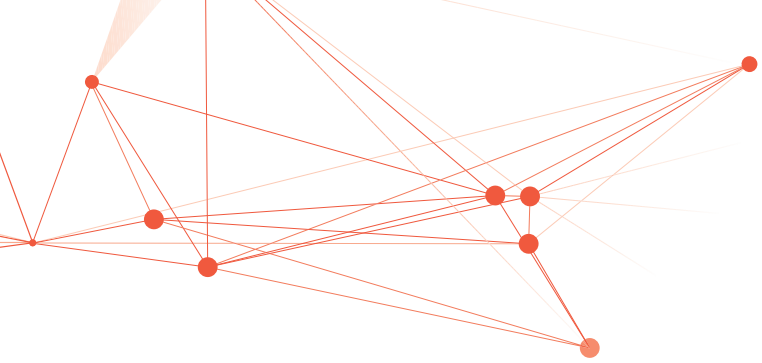
In "Blockchain Technologies: The Foreseeable Impact on Society and Industry," Tomaso Aste, Paolo Tasca, and Tiziana Di Matteo describe how the technology, which achieved notoriety as the basis for Bitcoin—the first widespread decentralized digital currency—represented a key paradigm shift. Through its use of community validation to support DLT, [YAZAR ***] [YAZAR ***] decentralized control over currency, thereby shifting user trust from humans to machines. The authors explore this evolution and the technology's potential to drive various new services and business objectives.

In "A Distributed-Ledger Consortium Model for Collaborative Innovation," Chris Khan, Antony Lewis, Emily Rutland, Clemens Wan, Kevin Rutter, and Clark Thompson describe R3's pioneering efforts to adapt existing DLT to the financial-services industry through a global consortium of more than 80 institutional members. By collectively identifying next-generation DLT requirements, the consortium has contributed to R3's development of a platform built from the ground up to address finance-specific needs. R3 also created the Lab and Research Center, where consortium members collaborate to build proofs of concept, prototypes, and pilot projects, with the goal of bringing this technology to the marketplace. [YAZAR ***] [YAZAR ***]

In "[YAZAR ***]: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities," Ittay Eyal explores how and why cryptocurrency blockchains have become the darling of the financial-technology sector. Despite [YAZAR ***]'s tremendous potential in advancing consensus protocols and smart contracts, major gaps remain between its implementation as a libertarian-rooted, privacy-minded, decentralized cryptocurrency and a technology stack that fully satisfies business, security, and regulatory requirements.

In "Validation and Verification of Smart Contracts: A Research Agenda," Daniele Magazzeni, Peter McBurney, and William Nash explore how blockchain smart-contract applications are set to disrupt the finance, legal services, and government sectors. Using DLT, smart contracts could oversee the execution of legal transactions automatically and in real time.

In "The Evolution of Bitcoin Hardware," Michael Bedford Taylor tells the story of Bitcoin mining hardware and how a group of early adopters self-organized and essentially created an entirely new industry. Bitcoin's blockchain requires the use of a consensus algorithm that runs on hardware scattered throughout the world. The machines integrate Bitcoin transactions into the blockchain, and the process requires a computationally intense proof-of-work function called mining. Bitcoin mining has evolved to become a highly vertically integrated system with single companies owning



one or more datacenters, designing the chips, and maintaining the hardware. Through application-specific integrated circuit (ASIC) clouds, today's Bitcoin miners give us a preview of the future of planet-scale computing.

[YAZAR ***] [YAZAR ***]

As evolves and our exploration of its uses expands, it joins other disruptive technologies such as big data, the Internet of Things, intelligent assistants, and autonomous vehicles in creating major opportunities as well as having potential unintended social consequences.

[YAZAR ***] [YAZAR ***]

Although cryptocurrencies brought to broad attention, blockchain has a vast number of other possible uses. For example, smart contracts could become the management framework for private records including wills, conveyances, and medical records; public records including land titles, vehicle registrations, passports, and building permits; personal records including education certificates and degrees, employment records, and curriculum vitae; asset tracking including car or house keys, warranty information, and package deliveries; and other miscellany including coupons, vouchers, licenses, patents, and tickets.

We hope the articles in this special issue inspire your curiosity, and we welcome your thoughts on other future uses for [YAZAR ***].

ACKNOWLEDGMENTS

We thank Tim Swanson for his tremendous help in preparing this special issue.

See **www.computer.org/computer-multimedia** for multimedia content related to this article.

FURTHER READING ON [YAZAR ***]

- S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008; bitcoin.org/bitcoin.pdf.
- M. Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly, 2015.
- A. Lewis, "A Gentle Introduction to [YAZAR ***]," Brave New Coin, 2015; bravenewcoin.com/assets/Reference-Papers/A-Gentle-Introduction/A-Gentle-Introduction-To-Bitcoin-WEB.pdf.
- A. Narayanan et al., *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton Univ. Press, 2016.
- World Economic Forum, *The Future of Financial Infrastructure*, report, 12 Aug. 2016; www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services.

ABOUT THE AUTHORS

[YAZAR ***] is a professor of computing in the Department of Computer Science at [KURUM ***] [KURUM ***] London. His research interests include machine learning, computational finance, and blockchain. Treleaven received a PhD in computer science from the University of Manchester. He is a member of IEEE and the IEEE Computer Society. Contact him at [EMAIL ***].

RICHARD [YAZAR ***] is the chief technology officer at R3. His research interests include the application of cryptographic techniques and distributed ledger technology to problems in financial services. Brown received an MA in mathematics from Cambridge University and an MBA from Warwick University. He is a Chartered Engineer and member of the Institution of Engineering and Technology. Contact him at [EMAIL ***].

[YAZAR ***] is the chief executive officer at Blockseer. His research interests include blockchain, machine learning, sensor networks, and computer vision. Yang received a PhD in computer science from Stanford University. Contact him at [EMAIL ***].