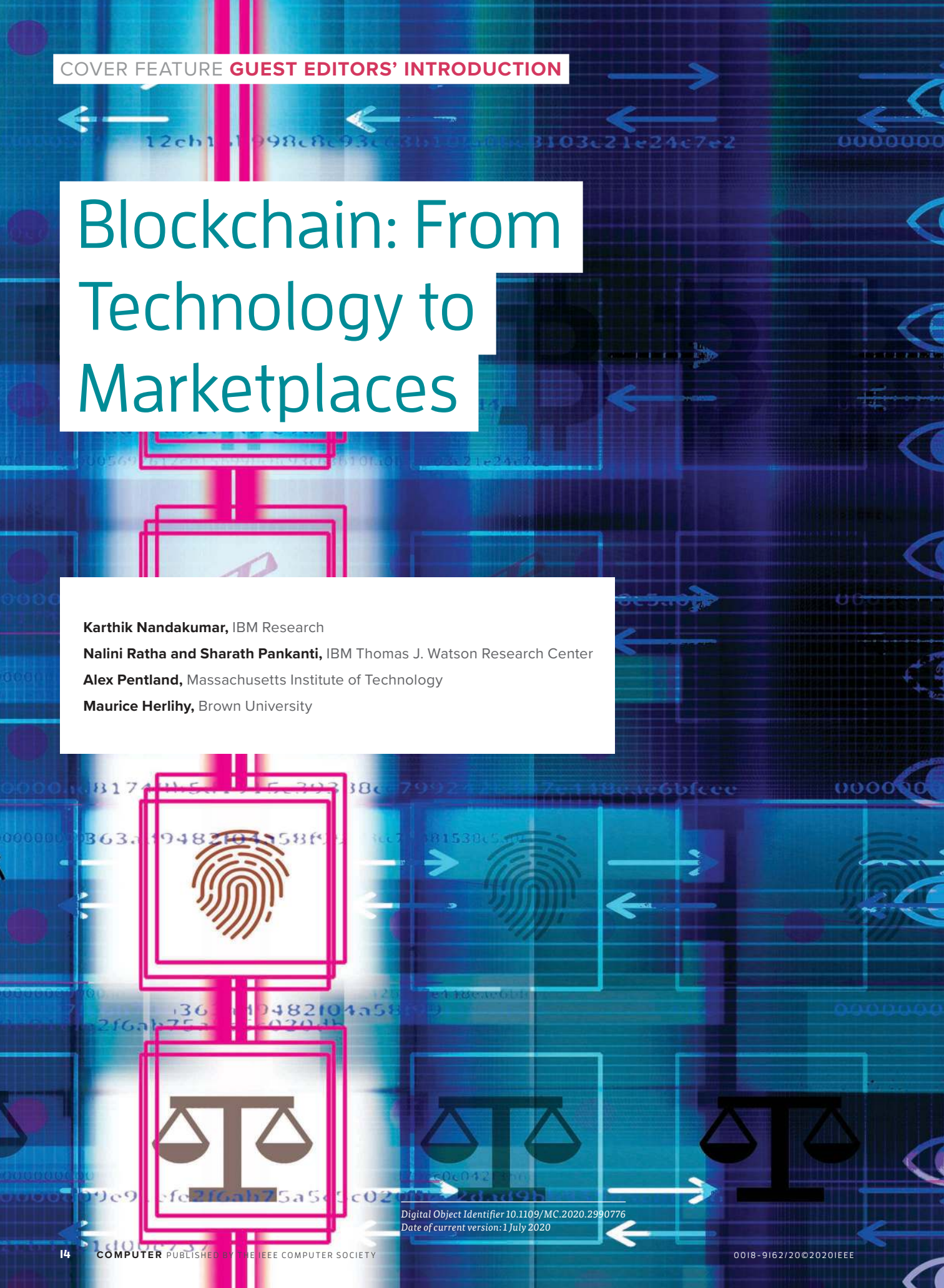
Blockchain: From Technology to Marketplaces

Karthik Nandakumar, IBM Research
Nalini Ratha and Sharath Pankanti, IBM Thomas J. Watson Research Center
Alex Pentland, Massachusetts Institute of Technology
Maurice Herlihy, Brown University



Digital Object Identifier 10.1109/MC.2020.2990776
Date of current version: 1 July 2020

0018-9162/20©2020IEEE

This theme issue provides a glimpse of the diverse research challenges in adopting blockchain technology into mainstream applications. The four articles focus on the following core issues: scalability, transparency versus privacy, standardization, ecosystem, and integration.

Trust and trust management lie at the heart of today's increasingly decentralized economy. In the past, trust has been enabled through a central authority. Blockchain, in all its variations, is emerging as a foundational technology that allows mutually untrusting parties to reach consensus on a shared digital history without a (central) trusted party. At the core of a blockchain application is a distributed immutable data store, and that is managed through smart contracts. Although blockchain is best known as the underlying core infrastructure of cryptocurrencies, it has many promising applications in other application domains, such as identity management, discovering critical obstacles in a complex supply chain, detecting money laundering and other financial crimes, identifying fake content, and better diagnoses of diseases (see Figure 1).

Several early adopters of blockchain are already reaping business benefits[1] by building solutions centered on trust, openness, and privacy. However, realizing the full potential of blockchain will require a significant level of fundamental advances in science and technology, major changes in business processes to create the right enabling environment, as well as innovative ideas to facilitate the integration of blockchain into real-world applications. This theme issue provides a glimpse of the diverse research challenges in adopting the technology into mainstream applications. Specifically, the four articles in this issue

FIGURE 1. Sample applications of blockchain. A wide variety of applications could significantly benefit from leveraging blockchain infrastructure,[3] which can address issues related to trust, governance, privacy, auditability, and provenance. Blockchain typically acts as a seamless distributed infrastructure that manages how (human or automated) agents as well as organizations interact with data sources/digital assets and physical assets under their control. Four broad classes of blockchain applications are illustrated. 1) Decentralized identity management could alleviate identity theft incidents[4] by prudently using various identifiers including biometrics. 2) Blockchain-based integrity and provenance can alleviate problems related to fake news[5] and other forms of disinformation. 3) Immutable audit trails made possible by blockchain could potentially enable a trusted marketplace for assets and insights.[6] 4) Increasingly adversarial cybersecurity incidents[7] could be addressed by auditable distributed ledgers.

focus on a mix of the following five core issues:

1. *Scalability*: One of the limitations of existing blockchain technologies is their inability to scale up to real-world, high-throughput applications without compromising on decentralization.
2. *Transparency versus privacy*: Another seemingly insurmountable issue is the tradeoff between transparency and privacy that is often encountered in blockchain applications.
3. *Standardization*: In a large family of applications, replacing a conventional centralized infrastructure with a blockchain infrastructure is not possible without standardizing the underlying data formats and interfaces.
4. *Ecosystem*: The efficacy of blockchain is maximized when the entire ecosystem of inter-related different applications could provide significantly better service by overhauling its consistent blockchain-compliant interfaces. Practitioners are recognizing that building an ecosystem is the most critical (and complex) effort for sustaining the benefits of blockchain infrastructure, and we increasingly are hearing the term minimal viable ecosystem in the context of blockchain infrastructures.[2]
5. *Integration*: Two distinct threads of evolution are emerging in the context of integrating blockchain into applications. The first approach can be referred to as transitioning, which involves improving an application by gracefully transitioning from a conventional method with blockchain innovation so both can coexist in the transitional period. The second method is disruptive, which starts with recognizing a gap in a conventional application and bridging the limitation by replacing the conventional method with blockchain.

IN THIS ISSUE

In "Blockchain Architecture for Auditing Automation and Trust Building in Public Markets," Cao et al. showcase how blockchain can enable the automated auditing of transactions as they occur by leveraging the strengths offered by the technology, such as immutability, load balancing, and differential access. This article also proposes a mechanism for privacy-preserving information exchange and highlights some of the scalability issues with existing blockchain protocols. Although their research exclusively focuses on auditing applications, the authors correctly note that similar advantages can be reaped by other applications by appropriately replacing their centralized infrastructures with blockchain.

"PharmaCrypt: Blockchain for Critical Pharmaceutical Industry to Counterfeit Drugs," by Saxena et al., focuses on the problem of counterfeit drugs by first reviewing its widespread existence and the lack of solutions that can effectively ensure that both patients and dispensaries are made aware of the provenance of the drug. Their proposed solution describes a means of overhauling one of the most effective conventional centralized solutions based on radio-frequency identification (RFID) technology and thus enabling a smooth transition to blockchain. They realistically conclude that their prototype is merely a new beginning toward an eventual solution, which requires building a viable ecosystem.

The article "Blockchain for Video Streaming: Opportunities, Challenges, and Open Issues," by Barman et al., presents the role of blockchain technology in video streaming applications. The key message of this article is that a lack of standardization is critically debilitating the adoption of blockchain for media streaming. The authors propose a conceptual, unifying framework and interface for video streaming applications and observe the need for researchers to address several key technical challenges, such as scalability and privacy. They also stress the importance of appropriate business models to bring the technology to the marketplace successfully.

In the last feature article, "Blockchain for E-Health-Care Systems: Easier Said Than Done," Biswas et al. give the readers a glimpse of the complexity of implementing a blockchain solution in the real world. The authors observe that health care is delivered through an ecosystem of closely connected networks of related interoperable services. Hence, the blockchain solutions implemented by individual health service providers must also be interoperable, which requires standards and new protocols for trade and consensus management. Another critical requirement in e-healthcare systems is the privacy of patient data. The authors conclude that to make a blockchain-based health-care solution a long-term success, it is critical to precisely capture and address its plethora of requirements.

ABOUT THE AUTHORS

KARTHIK NANDAKUMAR is a research staff member at IBM Research, Singapore. His research interests include blockchain, computer vision, statistical pattern recognition, biometric authentication, image processing, and machine learning. Nandakumar received a Ph.D. in computer science from Michigan State University. He is a senior associate editor for *IEEE Transactions on Information Forensics and Security* and an associate editor for *Pattern Recognition*. He has received a number of awards including the Best Paper Award from *Pattern Recognition* (2005), Best Scientific Paper Award (Biometrics Track) at ICPR 2008, and the 2010 IEEE Signal Processing Society Young Author Best Paper Award. He is a Senior Member of the IEEE. Contact him at nkarthik@sg.ibm.com.

NALINI RATHA is a research staff member in artificial intelligence (AI) research at the IBM Thomas J. Watson Research Center. His areas of interest include computer vision, AI, biometrics and fairness, and trust in AI. Ratha received a Ph.D. in computer science from Michigan State University, East Lansing. He received the IEEE Biometrics Council Leadership Award in 2019. He has cochaired several workshops on the topics of blockchain, biometrics, fairness, and trust in AI and coedited several special issues of IEEE publications. He is a Fellow of the IEEE and International Association of Pattern Recognition and an Association for Computing Machinery distinguished scientist. Contact him at ratha@us.ibm.com.

SHARATH PANKANTI is a research staff member in the Artificial Intelligence (AI) Department at the IBM Thomas J. Watson Research Center. His research interests focus on building scalable, fair, and trusted computer vision applications and their performance evaluation. Pankanti received a Ph.D. in computer science from Michigan State University. He has coedited theme issues of *Computer* on the topics of biometrics and cognitive computing, and he also cochaired workshops on the topics of blockchain, video summarization, fairness, and data efficiency. He is a Fellow of the IEEE, IAPR, OSA, and SPIE. Contact him at sharat@us.ibm.com.

ALEX PENTLAND directs the Massachusetts Institute of Technology (MIT), Cambridge, Connection Science and helped create and direct the MIT Media Lab and the Media Lab Asia in India. He is one of the world's most cited computational scientists, serves on the board of the UN Foundation's Global Partnership for Sustainable Development Data, co-led the World Economic Forum discussion in Davos, Switzerland, that led to the European Union privacy regulation General Data Protection Regulation, and was central in forging the transparency and accountability mechanisms in the UN's Sustainable Development Goals. He is a member of the U.S. National Academies, and his most recent books are *Building the New Economy* (MIT Press), *Trusted Data* (MIT Press), and *Social Physics* (Penguin). He is a Member of the IEEE. Contact him at sandy@media.mit.edu.

MAURICE HERLIHY is the An Wang Professor of Computer Science at Brown University. Herlihy received a Ph.D. in computer science from the Massachusetts Institute of Technology. He is the recipient of the 2003 Dijkstra Prize in Distributed Computing, the 2004 Gödel Prize in theoretical computer science, the 2008 ISCA Influential Paper Award, the 2012 Edsger W. Dijkstra Prize, and the 2013 Wallace McDowell Award. He received a 2012 Fulbright Distinguished Chair in the Natural Sciences and Engineering Lecturing Fellowship, and he is fellow of the Association for Computing Machinery, National Academy of Inventors, National Academy of Engineering, and National Academy of Arts and Sciences. Contact him at mph@cs.brown.edu.

These four articles show that overcoming challenges such as scalability and privacy require core scientific and technological advancements in areas like distributed computing and cryptography. For challenges such as standardization and ecosystem building, a herculean effort at consensus building among a diverse set of stakeholders is required. These advances will enable the transformation of blockchain from a niche technology for cryptocurrencies into a general-purpose technology capable of achieving unprecedented levels of transparency, accountability, and intelligence in the way we do business. We hope that this issue of *Computer* will serve as a valuable resource for the research community. Finally, we enjoyed guest editing this issue and would like to thank the reviewers for their time in shepherding these articles through the review process. Please feel free to contact us if you have any questions.

ACKNOWLEDGMENTS

Karthik Nandakumar, Nalini Ratha, and Sharath Pankanti would like to thank the members of the IBM Blockchain community for their support.

A HERCULEAN EFFORT AT CONSENSUS BUILDING AMONG A DIVERSE SET OF STAKEHOLDERS IS REQUIRED.

REFERENCES

1. "Forward together: Three ways blockchain explorers chart a new direction," IBM, Armonk, NY, May 2017. [Online]. Available: https://www.ibm.com/services/insights/c-suite-study/blockchain
2. E. Abebe et al., "Enabling enterprise blockchain interoperability with trusted data transfer (industry track)," in *Proc. 20th Int. Middleware Conf. Industrial Track*, Dec. 2019, pp. 29–35. doi: 10.1145/3366626.3368129.
3. D. D. F. Maesa and P. Mori, "Blockchain 3.0 applications survey," *J. Parallel Distrib. Comput.*, vol. 138, pp. 99–114, Apr. 2020. doi: 10.1016/j.jpdc.2019.12.019.
4. H. Weisbaum, "More than 1 million children were victims of ID theft last year," *NBC News*, June 21, 2018. [Online]. Available: https://www.nbcnews.com/business/consumer/more-1-million-children-were-victims-id-theft-last-year-n885351
5. F. Davey-Attlee and I. Soares, "Fake news," CNN. Accessed on: May 14, 2020. [Online]. Available: https://money.cnn.com/interactive/media/the-macedonia-story/
6. G. Singh and J. Levi, "MiPasa project and IBM Blockchain team on open data platform to support Covid-19 response," IBM, Armonk, NY, Mar. 27, 2020. [Online]. Available: https://www.ibm.com/blogs/blockchain/2020/03/mipasa-project-and-ibm-blockchain-team-on-open-data-platform-to-support-covid-19-response/
7. G. Belani, "5 cybersecurity threats to be aware of in 2020," IEEE Computer Society, Washington, D.C. Accessed on: May 14, 2020. [Online]. Available: https://www.computer.org/publications/tech-news/trends/5-cybersecurity-threats-to-be-aware-of-in-2020