Anonimle■tirilmi■ Makale - yeni

COVER FEATURE GUEST EDITORS’ INTRODUCTION

Blockchain Technology

in [KURUM ***]

14

C O M P U T E R P U B L I S H E D B Y T H E I E E E C O M P U T E R S O C I E T Y

0 0 1 8 - 9 1 6 2 / 1 7 / $ 3 3 . 0 0 © 2 0 1 7 I E E E

Philip Treleaven, [KURUM ***]

Richard Gendal Brown, R3

Danny Yang, Blockseer

The banking and financial-services industry has taken

notice of blockchain technology’s many advantages. This

special issue explores its unlikely origins, tremendous impact,

implementation challenges, and enormous potential.

Blockchain technology prom-

ises 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 blockchain technology have far-reaching potential in many other areas. To understand this potential, it is important to distinguish two core blockchain components: distributed-ledger technology ([KURUM ***]) 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 [KURUM ***] 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. [KURUM ***] contracts also have the potential to automate laws and statutes, which could significantly improve government services' efficiency and transparency.

BLOCKCHAIN B[KURUM ***]S

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 systems are also inherently transparent, because all changes are vis-

GUEST EDITORS' INTRODUCTION

JOIN OUR ROUNDTABLE DISCUSSION

A s part of this special issue of [KURUM ***], Tim Swanson of R3 chaired a roundtable with blockchain experts. Swanson discusses the trajectory of blockchain technology with an expert panel featuring Sarah Meiklejohn, [KURUM ***] ([KURUM ***]); Andrew Miller, [KURUM ***]; Elaine Shi, [KURUM ***]; Angela Walch, [KURUM ***] and [KURUM ***]; 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.

ible 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.

the banking and

IN THIS ISSUE

In

financial-

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

In

“Blockchain Technologies:
The Foreseeable Impact on [KURUM ***]
and Industry,” [KURUM ***], 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 para-
digm shift. Through its use of com-
munity validation to support [KURUM ***],
blockchain
technology decentral-
ized control over currency, thereby
shifting user trust from humans to
machines. The authors explore this
evolution and the technology’s poten-
tial to drive various new services and
business objectives.

In “A Distributed-Ledger Consor-
tium Model for Collaborative Innova-
tion,” Chris Khan, Antony Lewis, Emily

Rutland, Clemens Wan, Kevin Rutter,
and Clark Thompson describe R3's
pioneering efforts to adapt existing
[KURUM ***] to the financial-services industry
through a global consortium of more
than 80 institutional members. By col-
lectively identifying next-generation
[KURUM ***] 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.

In

"Blockchain

Technology:
Transforming Libertarian Cryptocur-

rency Dreams to [KURUM ***] and Bank-
ing [KURUM ***],” Ittay Eyal explores
how and why cryptocurrency block-
chains have become the darling of the
financial technology sector. Despite
blockchain technology’s tremendous
potential
in advancing consensus
protocols and smart contracts, major
gaps remain between its implemen-
tation as a libertarian-rooted, privacy-
minded, decentralized cryptocurrency
and a technology stack that fully sat-
isfies business, security, and regula-
tory requirements.

In “Validation and Verification of
[KURUM ***] Contracts: A Research Agenda,”
Daniele Magazzeni, Peter McBurney,
and William Nash explore how block-
chain smart-contract applications are
set to disrupt the finance, legal ser-
vices, and government sectors. Using
[KURUM ***], 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 ([KURUM ***]) clouds, today's Bitcoin miners give us a preview of the future of planet-scale computing.

FURTHER READING ON BLOCKCHAIN TECHNOLOGY

blockchain

As technology 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.

Although cryptocurrencies brought blockchain technology 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 blockchain technology.

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.

» 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 Blockchain Technology,” 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, [KURUM ***] 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

[KURUM ***] is a professor of computing in [KURUM ***] of Com-

puter [KURUM ***] at [KURUM ***]. His research interests include

machine learning, computational finance, and blockchain. Treleaven received

a PhD in computer science from [KURUM ***]. He is a member

of [KURUM ***] and the [KURUM ***] [KURUM ***] [KURUM ***]. Contact him at [EMAIL ***].

RICHARD GENDAL BROWN 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 [KURUM ***] and an MBA from [KURUM ***].

He is a Chartered Engineer and member of [KURUM ***] and

Technology. Contact him at [EMAIL ***].

DANNY YANG 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 [KURUM ***]. Contact him

at [EMAIL ***].