MIS Quarterly Executive

Volume 18 | Issue 4 Article 3

12-3-2019

Special Issue Editorial: Delivering Business Value through Enterprise Blockchain Applications

Mary Lacity

Rajiv Sabherwal

Carsten Sørensen

Editors' Comments

Special Issue Editorial: Delivering Business Value through Enterprise Blockchain Applications

Editorial

This December 2019 Special Issue focuses on enterprise blockchain applications, particularly the strategic opportunities they create and the ways to overcome the management challenges that might arise. We foresee that the collection of papers in this issue, combined with two previous *MISQ Executive* articles[1] on enterprise blockchains, will not only inform practice, but also serve as insightful readings for business courses and research studies. In this editorial, we first provide a brief history of blockchains and an overview of blockchain fundamentals to enable the readers to better understand the six papers in the special issue. Then, we summarize the special issue articles and highlight the contributions each makes.

Brief history of blockchains

Public solutions. By now, most people are familiar with Bitcoin, the first live blockchain application. Satoshi Nakamoto launched Bitcoin in January 2009.[2] Bitcoin is a peer-to-peer payment application. It uses cryptography, computer algorithms, and behavioral incentives to verify, secure, and permanently store any transfers of value on a single ledger. This ledger is copied and distributed to all the active nodes in the network (about 10,000 nodes as of this writing). Bitcoin has its roots in Libertarian and Cypherpunk values, which aim to by-pass governments and large financial institutions. No one person, enterprise, or government owns or controls it. Many other like-minded blockchain networks were launched, such as Litecoin, Monero, Ethereum, and Zcash. These are all "public-permissionless" blockchain applications, indicating that anyone can transact in the network, and anyone can run validator nodes. To transact, users just need an application interface, such as a digital wallet. Anyone may run a validator node by downloading the source code and turning on the mining function; mining is an open competition to solve a cryptographic puzzle that incentivizes people to validate transactions and secure the network. For the first five years of its existence, traditional enterprises mostly ignored Bitcoin and the myriad of subsequent cryptocurrencies.

Enterprise Exploration. By 2014, however, enterprises were beginning to explore the strategic opportunities and threats posed by Bitcoin and related blockchain technologies. Enterprise efforts seeking to establish blockchains that comply with regulations differ significantly from those supporting "public-permissionless" blockchains. Enterprise blockchains are primarily adopting "private-permissioned" blockchains where joining the network is by invitation-only, and where the validation of transactions is done by the members. There is much preliminary work that needs to be done before enterprises can share a blockchain solution: Members have to define data models, rules, and network standards; members need to specify shared governance rules over intellectual property, financing the network, rights of membership, data ownership, and software update control; and members have to find incentives for key players to join their chosen ecosystems. Consortia began to emerge to coordinate efforts.

Enterprise Consortia. R3 is one of the first consortia of significance. R3 was launched by David Rutter in 2014 with nine large banks: Barclays, BBVA Francés, State Street, JP Morgan, Commonwealth Bank of Australia, Goldman Sachs, Royal Bank of Scotland, Credit Suisse and UBS. Next year, the Linux Foundation launched the Hyperledger Project in December of 2015. It aims to advance the application of enterprise-grade blockchains across industries.[3] The Jiangsu Huaxin blockchain Research Institute (JBI), owned and operated by the Chinese government, was founded in September of 2016 in Nanjing.

1 Lacity, Mary (2018) "Addressing Key Challenges to Making Enterprise blockchain Applications a Reality," MIS Quarterly Executive: 17(3), Article 3; Pedersen, Asger B.; Risius, Marten; and Beck, Roman (2019) "A Ten-Step Decision Path to Determine When to Use blockchain Technologies," *MIS Quarterly Executive*: 18(2), Article 3.

2 Nakamoto, S. (2008), "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf

3 The Linux Foundation (January 22 2016), The Hyperledger Project Charter, available at https://www.hyperledger.org/about/charter

B3i was founded in October 2016 in Zurich Switzerland to focus on blockchain standards for the insurance sector; The Enterprise Ethereum Alliance was launched in 2017 by Microsoft, Accenture, JP Morgan, BNY Mellon, CME Group, MasterCard, Santander, Wipro and 26 other enterprises. Members want an enterprise-grade blockchain based on the Ethereum protocol. The blockchain in Transportation Alliance (BiTA) was launched in 2017 to develop standards for the entire transportation industry. More recently, the Oil & Gas blockchain Consortium launched in 2019. There are nearly 103 blockchain consortia of significance.[4] These consortia are developing standards, building code bases, and or developing applications.

Enterprise Code Bases. In 2017, three significant code bases for enterprises were released as open source software. JP Morgan released Quorum, a permissioned version of Ethereum; R3 released Corda, a peer-to-peer code base aimed at enterprises that want strict data and transaction privacy; HyperLedger released Fabric—much of whose code was donated by IBM. Fabric is commonly used by enterprises, including IBM, WalMart, and Maersk. From these code bases, thousands of proof-of-concepts were built in sandboxes, across industries and geographies.[5]

Enterprise Solutions. By 2018, enterprises began moving blockchain applications into production. Examples include: TradeLens tracks shipping containers—it's long journey to fruition is the subject of the first article in the special issue; MediLedger—covered by the second paper in the special issue—verifies the authenticity of pharmaceutical returns in the U.S. supply chain; the IBM Food Trust traces food from farm and fishery to retail stores; WineChain tracks and authenticates wine bottles; and Microsoft uses a blockchain application to track royalty payments owed to Xbox application owners. While none of these applications are fully scaled yet, they demonstrate the possibilities of getting business value from blockchain technologies.[6]

Blockchain fundamentals

If enterprise blockchains are the answer, what is the question? From an enterprise perspective, the question is: How can we significantly improve the way we transact outside the boundaries of the firm? The best way to understand a blockchain application's potential business value is to compare it to the way partners most frequently trade today. We focus on two key attributes:

1. **Trusted Third Parties.** Before a blockchain application, parties rely on trusted third parties (TTPs) to establish trust and to mitigate counter-party risks in trading relationships. TTPs provide independent "truth attestations" such as notarizing signatures; verifying identity; verifying ownership; authenticating assets; preventing double spending; and attesting that agreements have been properly executed. TTPs provide these and many other vital services to facilitate trade; that is why they exist, why parties rely upon them, and why they are paid so well.

2. **Enterprise-level record keeping.** Before a blockchain, every party maintains its own systems of record. Specifically, each party maintains its own accounting system to post transactions on its own ledger. Each party benefits from controlling its own accounting system and ledger—each enterprise can swiftly and unilaterally execute decisions about accounting rules, transaction reversals, software upgrades, etc., within the boundaries of the firm.

Despite the benefits of (1) TTPs, and (2) enterprise-level record keeping, there are negative consequences, including:

- **Low transparency:** Enterprises typically only see the transactions entering or exiting the boundaries of the firm. In turn, low transaction visibility makes locating assets or ascertaining the status of transactions difficult.

4 ESI Intelligence (2019) "Solutions for blockchain Consortia," https://esg-intelligence.com/blockchain-consortia-analysis/

5 Lacity, M. (2018), "A Manager's Guide to blockchains for Business: From Knowing What to Knowing How", *SB Publishing*, Stratford-Upon-Avon.

6 Lacity, M., Steelman, Z., and Cronan, P. (2019), "Blockchain Governance: Insights for Enterprises", *University of Arkanas BCoE white paper* (BCoE 2019-02).

- **Mutability of records:** Once reconciled, there is nothing to prevent trading partners from modifying records after the fact; partners cannot be confident they are dealing with the same historical record of transactions through time.

- **Vendor opportunism:** The threat of "vendor opportunism"—the idea that vendors may pursue their self-interests with guile[7], may withhold information, or may not comply with the terms and conditions of the agreement—always exists. Both low transparency and mutability of records potentially enhance vendor opportunism. Therefore, trading partners spend a lot of resources monitoring agreements to make sure that trading partners are behaving as promised.

- **Slow settlement times:** With enterprise-level record keeping, every party has its own version of the truth that needs to be reconciled with trading partners. Reconciliations are expensive and time-consuming.

- **High transaction costs:** TTPs typically earn between two and 22 percent of the value of the transaction in fees.

- **High cybersecurity costs:** Each party spends significant resources protecting its IT perimeters against cybersecurity attacks. Large enterprises successfully fend off thousands of cybersecurity threats each day. However, a single security breach can cost an organization billions of dollars to protect or remedy.

Blockchain applications aim to improve all of these.

A blockchain application is software that is shared among ecosystem partners. Parties run the same software and maintain an identical copy of the digital ledger on independent ***nodes*** (e.g., host computers, each with a unique identifier) in the network.

Instead of TTPs, a blockchain application uses ***cryptography***—"a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it"[8]—and ***computer algorithms***—well-defined procedures so that a computer can execute a process—to perform truth attestations. For example, many blockchain applications rely on cryptographic private-public key pairs to verify asset ownership; whoever is in possession of the private key is assumed to be the legitimate owner of the asset.

The software examines all the newly submitted transactions using the rules of the network. Unverified transactions are rejected. Verified transactions are time stamped, sequenced, secured with unique cryptographic identifiers and added to the ledger. The first node that updates the ledger distributes the update to all authorized nodes. Once enough independent nodes accept the update, the network reaches ***consensus***; they all agree, "this is the record of truth". The transactions are forever locked in the ledger, a property known as ***immutability***. The nodes constantly chatter with each other to make sure no party tampers with the records after-the-fact. If anyone cheats, the other parties' nodes automatically ignore it.

To sum, a blockchain application is a shared application that uses cryptography and computer algorithms (instead of institutions) to establish trust in trade and stores them permanently on a single, immutable, distributed ledger.

For enterprises, the main benefits of sharing software and ledgers are:

- **Better transaction visibility:** Parties of an exchange can instantly determine the location of an asset or the status of a transaction by reading the ledger.

- **Immutability of records:** Every party can be confident they are always dealing with the same historical data, guaranteeing consistent data provenance across parties.

- **Lower vendor opportunism:** Rather than rely exclusively on paper contracts, verbal agreements or handshakes, parties can rely—at least in part—on computer algorithms (called **smart contracts**)

7 Williamson, O., (1991), "Comparative economic organization: the analysis of discrete structural alternatives," *Adm. Sci. Quart. 3*6 (2), 269–296.

8 https://searchsecurity.techtarget.com/definition/cryptography

that automatically execute the terms of agreements without oversight.

- **Faster settlement times:** Parties rely on one version of the truth, so there is no need for reconciliations; it's a confirm-before-commit process instead of post-then-confirm-later process. The transactions can settle in sub-second to sixty minutes, depending on which consensus algorithm is used in the blockchain application.
- **Lower transaction costs:** Fees are typically quite small, just enough to finance the blockchain application.
- **Better cybersecurity:** Blockchain applications still function properly even if a high percentage of nodes are faulty—or even malicious—enabling fault tolerance, resiliency and 100 percent availability. In theory, the only way to break a blockchain application is to commandeer more than 50 percent of the nodes.

Additionally, many organizations have worthwhile social missions like using blockchain technologies to bring financial services to the 1.7 billion people who lack access; protect the property rights of people with low economic status; protect the integrity of political elections; and enable self-sovereignty over one's identity and personal data.

Special issue papers

The first four papers appear in the December 2019 issue; The last two papers will be published in the March 2020 issue.

The first paper in the special issue, "How TradeLens Delivers Business Value with blockchain Technology" is by Thomas Jensen, Jonas Hedman, and Stefan Henningsson. The authors document the six-year journey of building what was to become TradeLens, an ecosystem blockchain-enabled platform to track shipping containers and related documents. Initially Maersk—the largest shipping-container company—started a series of digitization and innovation initiatives to reduce the administrative costs per shipping container. IBM—the U.S.-based multinational information technology company—also had started initiatives to digitize global trade documents. In 2016, IBM approached Maersk to propose a blockchain-based solution based on Hyperledger Fabric, the enterprise blockchain code base IBM built and then donated to the open source community. Maersk and IBM joined forces to develop, test and pilot blockchain technology-based prototypes. The partners went live with a commercial solution in 2018. However, to achieve business value across the international supply chain, competitors would need to join the blockchain platform. Maersk realized that it had to think differently about strategy; instead of using the platform to gain a competitive advantage, it needed to uplift the entire ecosystem comprising customers, partners, authorities and competitors. The governance model was changed to attract key players. Specifically, an advisory board that now includes Maersk's biggest competitors, such as the Mediterranean Shipping Company (MSC) and CMA CGM, was formed to provide transparency and input on the choices TradeLens makes. According Bridget van Kralingen, Senior VP for blockchain at IBM, TradeLens had tracked 500 million events on 20 million containers by 2019. TradeLens was adding between 25,000 to 30,000 documents a day.[9] The authors identified six key lessons:

1. Blockchains are ecosystem solutions that require organizations to think differently about strategy
2. Focus on the vision, not on the return on investment (ROI)
3. Blockchains are decentralized technical solutions to inter-organizational problems
4. Partnership trust precedes—and follows—blockchain trust
5. Let legitimacy and political feasibility guide the starting point
6. Governance models need to evolve as adoption expands

The second paper, "How an Enterprise Blockchain Application in the U.S. Pharmaceuticals Supply Chain is Saving Lives," is by Jens Mattke, Christian Maier, Axel Hund,

9 Bridget van Kralingen & Mike White at blockchain Revolution Global 2019, https://youtu.be/7crOWQnz9tw

and Tim Weitzel. The authors describe how U.S. pharmaceutical supply chain partners are working together via the MediLedger Project to comply with the U.S. Drug Supply Chain Security Act (DSCSA) of 2013. The purpose of the act is to better trace pharmaceuticals throughout the entire supply chain to prevent counterfeit drugs. Counterfeit drugs cause one million deaths globally and cost $200 billion for supply chain partners. The MediLedger Project was founded in 2017 by Chronicled, a U.S.-based supply chain-focused IT firm. So far, the MediLedger Project's working group members include McKesson; Pfizer; AmerisourceBergen; Cardinal Health; Genentech; Gilead; and Amgen. MediLedger's first service, called Product Verification, went live in 2019. The service looks up the correct manufacturer based on product item numbers stored on the blockchain and then sends a private message to the manufacturer to verify the legitimacy of a return, i.e. that the drug is not counterfeit or expired. The solution uses zero-knowledge proofs[10] to ensure data privacy while still demonstrating the authenticity of a transaction. The authors identified four key lessons:

1. Build governance through a benevolent dictator and 'consensus through collaboration'.
2. Instead of storing verified transactions on the shared distributed ledger, store proofs that the transactions were verified.
3. Use zero-knowledge proofs to verify product authenticity while preventing custody traceability.
4. Leverage blockchain application capabilities to fix some non-working information systems landscapes.

The third paper, "Building a Blockchain Application that Complies with the EU General Data Protection Regulation," is by Alexander Rieger, Florian Guggenmos, Jannik Lockl, Gilbert Fridgen, and Nils Urbach. This paper addresses one of the key concerns identified earlier, that data retirement policies seem incompatible with a blockchain's property of record immutability. Europe's General Data Protection Regulation (GDPR) was passed in 2016 and required compliance by 2018. Among its requirements, individuals covered by the act have rights over their personal data, including rights over data processing, rights to rectify errors, and rights of erasure of personal data. Germany's Federal Office for Migration and Refugees were certainly concerned with complying with GDPR when designing a blockchain-based solution to manage asylum applications. The use case was perfect for blockchain technology because different government agencies need to share and update records. To comply with GDPR in blockchain applications, the authors identified three governance options: "central authority", "shared responsibility", and "pseudonymization". With central authority, the network nominates a central authority to act as controller; rights to erasure are waived in a contract; if waivers later become void, the central controller must erase the data from the blockchain. In the best-case scenario, the central authority could submit counter transactions that makes the data semantically undecipherable. In the worst case, a central authority would manage the removal of data from its block and recalculate the hashes for all subsequent blocks. With "shared responsibility", these responsibilities are shared among network partners as defined in a contract. With "pseudonymization", data on the blockchain de-personalized and only people with offchain information can attribute the data on the blockchain to person. While this is the easiest to administer, there are concerns that meta-patterns in the data stored on the blockchain could revel personal data. Based on the case, the authors identified three lessons, with the caveat that they are not providing legal advice:

1. Avoid storing personal data on a blockchain; (store personal data offchain)
2. A blockchain solution that needs to process personal data should use a private and permissioned pseudonymization approach.

10 Zero knowledge proofs were developed in 1985 by Shafi Goldwasser, Charles Rackoff, and Silvio Micli in 1985. (https://blockonomi.com/zero-knowledge-proofs/). Zero knowledge proofs are a method for one party to verify possession of a piece of information to other parties without revealing the information. In blockchain applications, zero-knowledge proofs are used to guarantee that transactions are valid without revealing information about the sender, receiver, and/or transaction. Besides MediLedger, Zcash and EY's Nightfall use zero knowledge proofs in blockchain applications.

3. A blockchain solution that needs to coordinate cross-organizational workflows should use a private and permissioned pseudonymization approach with identifier mapping.

The fourth paper, "The worth of words: How technical white papers influence ICO[11] blockchain funding," is by Benjamin Barraza. We selected this paper on ICOs for inclusion in the MISQE special issue because startups play an important part in the global blockchain landscape. The author, using quantitative methods, examined 193 ICOs that occurred between 2015 and 2018 to see what factors influenced the amount of money raised during their initial fundraising periods. In his research, Barraza found that what fund-seekers write in their technical white papers is significantly related to the amount of money raised. Specifically, the more detailed white papers raised more money than the superficial ones. Although the results are not surprising in and of themselves, the author has a number of insights on what happened to the ICO model. Recently, the U.S. Security and Exchange Commission (SEC), as well as other regulatory bodies around the globe, now often view digital coins released in an ICO as securities. We present and discuss his ongoing research in the form of a conversation, allowing us to explore the history and changes in the market since he did his analysis. The author believes that managers have a lot to learn from the ICO market, including the following lessons:

1. The ICO bubble informs the framing of the next generation technologies; Firms like JP Morgan are beginning to launch their own coins, and managers need to understand the history of the space.

2. Two direct descendants from the ICO, the Initial Exchange Offering (IEO) and the Security Token Offering (STO) are increasingly being used;

3. Firms—especially those that are in the firing line of initiatives backed by smart VC funds—should begin to build dynamic capabilities in this space.

The fifth paper, "Building Together: Lessons Learned from a blockchain Consortium in the Car Ecosystem" is by Liudmila Zavolokina, Rafael Ziolkowski, Ingrid Bauer, and Gerhard Schwabe. This paper reports from a university-industry collaboration for the second-hand car industry. Ackerlof's famous 1970 article on "a market for lemons"[12] illustrating market dynamics when there is uncertainty of quality using the example of the second-hand car market. The cardossier project aims to provide information certainty and symmetry across the diversity of firms and individuals engaged in buying, selling, insuring, and registering used cars. The paper focuses on one of the key challenges for private permissioned blockchains — establishing a viable consortium of partners. In this case, the consortium represents an industry vertical with a representative from each element in the value-chain, rather than a consortium of similar companies seeking pre-competitive standardization. The consortium managed to resolve the inherent tensions arising from the different goals and interests of the participating firms. The paper offers three main lessons:

1. Blockchain encourages collaborations, but requires initial mutual trust, which could be facilitated through non-competing partners.

2. Blockchain can form the foundation for new ecosystem value-chains by providing a means to achieve standardization across firms.

3. Laws and regulations are key in blockchain projects. Working closely to align blockchain consortium governance and legal constraints is critical.

The sixth paper, "The Role of blockchain in Regulatory Technology: Lessons from Project Maison" is by Daniel Gozman, Jonathan Liebenau, and Tomaso Aste. This paper focuses on the use of blockchain technology for regulatory compliance. It draws upon Project Maison, a prototype blockchain developed in conjunction with two banks and the UK regulator, to discuss the benefits, risks, use cases, and governance

11 An Initial Coin Offering (ICO) is a funding model where a startup or blockchain project raise money by selling digital coins during a fundraising round.

12 Akerlof, George A. (1970). "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism". *Quarterly Journal of Economics*. The MIT Press. 84(3): pp. 488–500.

Table 1: Highlights of the Special Issue Papers Highlights of the Special Issue Papers

Paper	Case example	Benefits	Major Challenges	Recommendations
Jensen, Hedman, and Henningsson, (2019)	The TradeLens Project	• Reduce the administrative costs per shipping container • Better transparency across the supply chain	• Need to change the governance model to attract key players, including competitors	1. Blockchains require organizations to think differently about strategy. 2. Focus on the vision, not ROI. 3. Use blockchains as decentralized technical solutions to interorganizational problems. 4. Partnership trust and blockchain trust are intertwined. 5. Let legitimacy and political feasibility guide the starting point. 6. Governance models need to evolve as adoption expands.
Mattke, Maier, Hund, and Weitzel (2019)	The MediLedger Project	• Better trace pharmaceuticals throughout the entire supply chain to prevent counterfeit drugs	• Ensure data privacy while still demonstrating the authenticity of a transaction	1. Build governance through a benevolent dictator and 'consensus through collaboration'. 2. Instead of storing verified transactions on the shared distributed ledger, store proofs that the transactions were verified. 3. Use zero-knowledge proofs to verify product authenticity while preventing custody traceability. 4. Use blockchain application capabilities to fix some non-working IS landscapes.

Table 1: Highlights of the Special Issue Papers Highlights of the Special Issue Papers (continued)

Paper	Case example	Benefits	Major Challenges	Recommendations
Rieger, Guggenmos, Lockl, Fridgen, and Urbach (2019)	Germany's Federal Office for Migration and Refugees	• Enable different government agencies to share event logs. • Improve the exchange of information, consideration of security aspects, and the speed of asylum procedures.	• Concerns that meta-patterns in the data stored on the blockchain could allow identification of asylum applicants.	1. Avoid storing personal data on a blockchain; 2. A blockchain solution that needs to process personal data should use a private and permissioned pseudonymization approach. 3. A blockchain solution that needs to coordinate cross-organizational workflows should use a private and permissioned pseudonymization approach with identifier mapping
Barraza (2019)	Initial Coin Offerings (ICOs)	• Initially, ICOs provided a new way to fund blockchain projects and startups • New funding models evolved from ICOs that better inform investors	• Regulators charged with protecting investors increasingly deemed that ICOs were securities	1. The ICO bubble informs the framing of the next generation technologies, including firms launching their own coins. 2. Firms, especially those in the firing line of initiatives backed by smart venture-capital funds, should build dynamic capabilities in this space.
Zavolokina, Ziolkowski, Bauer, and Schwabe (2020)	The Cardossier Project (for second-hand car industry)	• Improve trust in the used car market	• Difficult to establish a viable consortium of partners in private permissioned blockchains • Need to resolve the tensions arising from the participating firms' different goals and interests.	1. Non-competing partners can facilitate initial mutual trust needed for blockchains. 2. Blockchain can form the foundation for new ecosystem value-chains by helping achieve standardization across firms. 3. Work closely to align blockchain consortium governance with legal and regulatory constraints.

Table 1: Highlights of the Special Issue Papers Highlights of the Special Issue Papers (continued)

Paper	Case example	Benefits	Major Challenges	Recommendations
Gozman, Liebenau, and Aste (2020)	Project Maison	• Enhanced data quality and standardized formatting • Improved governance, transparency, and accountability • Consistent interpretation and use of rules and obligations between regulators banks and other industry participants	• Reactive or proactive supervision • Custodianship of data • Discretion versus standardized practices • Monopolization of market infrastructures	1. Evaluate resource implications and interoperability capabilities 2. Evaluate cost reductions against loss of control of calculations and discretionary cases. 3. Revisit the need for a Blockchain solution. 4. Weigh potential efficiencies over the pain of implementing a new system 5. Manage conflicts over ownership of market infrastructures.

challenges, and offer five mitigation principles for realizing the benefits. The authors discuss how decentralized architectures, enabled by blockchain, can establish new and effective forms of compliance by enabling transparency, incentives and accountability while increasing standardization and automation. More specifically, they identify three potential benefits of Project Maison, enabled by R3's Corda blockchain platform: (1) enhanced data quality and standardize formatting; (2) improved governance, transparency and accountability; and (3) consistent interpretation and application of rules and obligations between regulators banks and other industry participants. The authors highlight governance challenges for enterprise blockchains, related to reactive or proactive supervision, custodianship of data, discretion versus standardized practices, and monopolization of market infrastructures. They argue that if the decentralized architecture is developed, controlled and owned by one or two key players, it would be an extremely unattractive proposition to other industry participants. They also offer five principles to mitigate the various challenges:

1. Evaluate resource implications and interoperability capabilities.
2. Evaluate cost reductions against loss of control of calculations and discretionary cases.
3. Revisit the need for a blockchain solution.
4. Weigh potential efficiencies over the pain of implementing a new system.
5. Manage conflicts over ownership of market infrastructures.

Conclusion

As discussed above, the six papers selected for this special issue provide a variety of examples of blockchain applications. Table 1 summarizes the examples used by each paper, as well as the benefits and challenges identified, and the recommendations offered.

As the papers show, blockchain applications promise enterprises a significant amount of business value, like transacting directly with trading partners, eliminating the need for reconciliations, instantly tracking assets, providing robust data provenance, settling

transactions quickly and cheaply and enabling a security model that is fault tolerant, resilient, and available.[13] However, the technology is still maturing, standards are still being established, and concerns over regulatory uncertainty still overshadows many c-suite discussions. Besides these ecosystem factors, enterprises are also challenged by the internal implications of blockchain applications, such as sharing control and data with competitors, allowing others to validate and store the enterprise's data, and data retirement policies that are incompatible with a blockchain's immutability of records. Thus, despite the promised business value, blockchain technology, like any other technology, poses new management challenges. Cumulatively, the six papers from this special issue help mangers think through, and overcome, many of these challenges. Each paper offers a set of recommendations, which should help future adopters of blockchain address such challenges and achieve benefits that come close to this technology's tremendous potential.

About the Special Issue Editors

Mary Lacity

Mary Lacity is Walton Professor of Information Systems and Director of the blockchain Center of Excellence in the Sam M. Walton College of Business at The University of Arkansas. She was previously Curators' Distinguished Professor at the University of Missouri-St. Louis. She has held visiting positions at MIT, the London School of Economics, Washington University, and Oxford University. She is a Certified Outsourcing Professional ® and Senior Editor for *MIS Quarterly Executive*. Her recent research focuses on improving business services using Robotic Process Automation (RPA), Cognitive Automation (CA), and blockchain technologies. She was inducted into the IAOP's Outsourcing Hall of Fame in 2014, one of only three academics to ever be inducted along with Peter Drucker and Leslie Willcocks. She has published 28 books, most recently, *A Manager's Guide to blockchains for Business*, SB Publishing, UK. Her publications have appeared in the *Harvard Business Review*, *Sloan Management Review*, *MIS Quarterly*, *MIS Quarterly Executive*, *IEEE Computer, Communications of the ACM*, and many other academic and practitioner outlets. Her work has been cited over 17,000 times; Her h-index is 55. She earned her Ph.D. in Business Administration at the University of Houston.

Rajiv Sabherwal

Rajiv Sabherwal is Distinguished Professor, Edwin and Karlee Bradberry Chair, and Department Chair of Information Systems at the Sam M. Walton College of Business, University of Arkansas. He investigates the processes associated with management of emergent information technologies and their impacts of on individuals and organizations. He has published in *Management Science*, *MIS Quarterly*, *Information Systems Research*, *Organization Science*, *MIS Quarterly Executive*, *California Management Review*, and other prestigious journals, and authored textbooks on business intelligence and knowledge management. He has served as: University of Missouri System Curators' Professor, Fulbright-Queen's School of Business Research Chair; Editor-in-Chief of IEEE Transactions on Engineering Management; Conference Co-chair for International Conference on Information Systems; and senior/guest editor for *MIS Quarterly*, *Information Systems Research*, and *Journal of AIS*. He received a Ph.D. in business administration from University of Pittsburgh, and Post-Graduate Diploma in Management from Indian Institute of Management, Calcutta. He is a Fellow of both IEEE and Association of Information Systems.

Carsten Sørensen

Carsten Sørensen is Reader (Associate Professor) in Digital Innovation within Department of Management at The London School of Economics and Political Science (carstensorensen.com). Carsten has since the 1980s researched digital innovation, for example innovating the digital enterprise through mobile technology (enterprisemobilitybook.com), and the innovation dynamics of mobile infrastructures and -platforms (digitalinfrastructures.org). He developed LSE's first blockchain course, an online course on cryptocurrency disruption. Carsten has published widely within Information Systems since 1989 (scholar.carstensorensen.com), for example in *MIS Quarterly*, *Information Systems*

13 Lacity, M. (2018), "A Manager's Guide to blockchains for Business", *Stratford-Upon-Avon SB Publishing*

Research, *Journal of Management Information Systems*, *Information Systems Journal*, *Journal of Information Technology*, *Information & Organization*, *The Information Society*, *Computer Supported Cooperative Work*, and *Scandinavian Journal of Information Systems*. This body of work has been cited over 5,000 times with a h-index of 35. Carsten also has extensive experience managing national, EU, and industry research projects with research grants totalling over £3 million. He has for a number of years been engaged in assisting and assessing digital start-ups and has for 25 years been actively engaged in academic consultant and executive education with a broad range of organisations – IMF, Microsoft, Google, PA Consulting, Huawei, Orange, Vodafone, Intel, GEMS, to name just a few. Most recently, he has contributed to a report with Gowling WLG on digital disruption.