Business Horizons (2019) 62, 35—45

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

Blockchain technology for enhancing supply chain resilience

Hokey Min

College of Business Administration, Bowling Green State University, Bowling Green, OH 43403, U.S.A.

KEYWORDS
Blockchain technology;
Supply chain risk management;
Cryptocurrency;
Blockchain architecture;
Supply chain resilience

Abstract With the soaring value of bitcoin and frenzy over cryptocurrency, the blockchain technology that sparked the bitcoin revolution has received heightened attention from both practitioners and academics. Blockchain technology often causes controversies surrounding its application potential and business ramifications. The blockchain is a peer-to-peer network of information technology that keeps records of digital asset transactions using distributed ledgers that are free from control by intermediaries such as banks and governments. Thus, it can mitigate risks associated with intermediaries' interventions, including hacking, compromised privacy, vulnerability to political turmoil, costly compliance with government rules and regulation, instability of financial institutions, and contractual disputes. This article unlocks the mystique of blockchain technology and discusses ways to leverage blockchain technology to enhance supply chain resilience in times of increased risks and uncertainty.

1. Blockchain: It is time to get up to speed

According to CoinDesk (2017)—which has traced prices from digital currency exchanges including Bitfinex, Bitstamp, Coinbase, and itBit for the last decade—the price per bitcoin hit an all-time high of $17,872.56 on December 15, 2017. As of September 2017, the total market value of all digital currencies surpassed $135 billion (Hackett, 2017a). Although the skyrocketing price tag of a bitcoin may not reflect its true currency value, an astonishing rise in its price for a relatively short period of time drew a frenzy of interest from many investors worldwide. As the interest in bitcoin continues to grow, the blockchain technology (BT) that powers the cryptocurrency concept and underlying technology has become the center of attention in the business community. For example, Juniper Research (Holden, 2017) revealed that 39% of approximately

E-mail address: hmin@bgsu.edu

https://doi.org/10.1016/j.bushor.2018.08.012
0007-6813/

400 company founders, executives, managers, and information technology (IT) specialists it surveyed either considered deploying or were in the process of deploying BT. BT started to gain traction from a growing number of supply chain executives. The recent Eyefortransport (2017) report indicated that nearly 62% of supply chain executives surveyed claimed to have engaged with BT. Overall, the business value-add of a blockchain is expected to grow to more than $176 billion by 2025 and exceed $3.1 trillion by 2030 (Gartner, 2017).

Despite this rosy outlook, many firms are still either skeptical about blockchain's face value or unfamiliar with its inner workings and application potential. Although 88% of surveyed marketers valued the potential of BT to disrupt current practices in a positive way, a mere 15% felt they could explain that technology to their clients (Annalect, 2017). Similarly, 62% of the supply chain professionals surveyed by Infosys Consulting did not know what to expect from BT (Langley, 2017). Since unfamiliarity and misunderstanding can derail the successful applications of BT, there is a growing need to explain it.

BT is a peer-to-peer (P2P) network of IT that keeps records of digital asset transactions using distributed ledgers in lieu of traditional databases that are centrally controlled by intermediaries such as banks, credit agencies, governments, and accountants. BT's decentralized, open, and cryptographic nature engenders trust and thus brings unprecedented security benefits. Hacking attacks that commonly impact large centralized intermediaries like banks would be nearly impossible as blockchain can keep track of all transactions. If someone wanted to hack into a particular block in a blockchain, a hacker would not only need to hack into that specific block but also all the preceding blocks in the entire history of that blockchain. As such, BT provides a way to securely create a tamper-proof log of business activities and transactions (Fallahpour, Shirmohammadi, Semsarzadeh, & Zhao, 2014; Lemieux, 2016). To further enhance the security of a blockchain, blockchain networks can be private with restricted membership similar to an intranet, restricting access to those networks in lieu of making them public.

The acceptance of BT as a tool to enhance security benefits and revolutionize supply chain practices would take a considerable amount of time until its benefit potential is fully realized and backed by many success stories. To speed up the BT application process, we need to understand how BT typically works. Figure 1 demonstrates the inner workings of BT. As Figure 1 illustrates, no one owns a blockchain; no one can delete a block from the chain and anyone can add to it. As such, the blockchain allows anyone to transfer his/her assets—including intangible assets—without the risk of hacking and building silos that limit interactions among trading partners.

In addition to the security benefit, BT can bring a multitude of managerial benefits to everyday business practices (Maruti Techlab, 2017; Takahashi, 2017), including:

- Reduced transaction costs/time resulting from better-preserved blockchain platforms that do not necessitate third-party involvement;
- Visibility improvement across the supply chain, a result of increased transparency gained via open ledgers that any person can see; and
- Improved connectivity among trading partners through the integration of digital and physical worlds (Maruti Techlab, 2017; Takahashi, 2017), which includes a shared visibility of transactions and information flows across the supply chain.

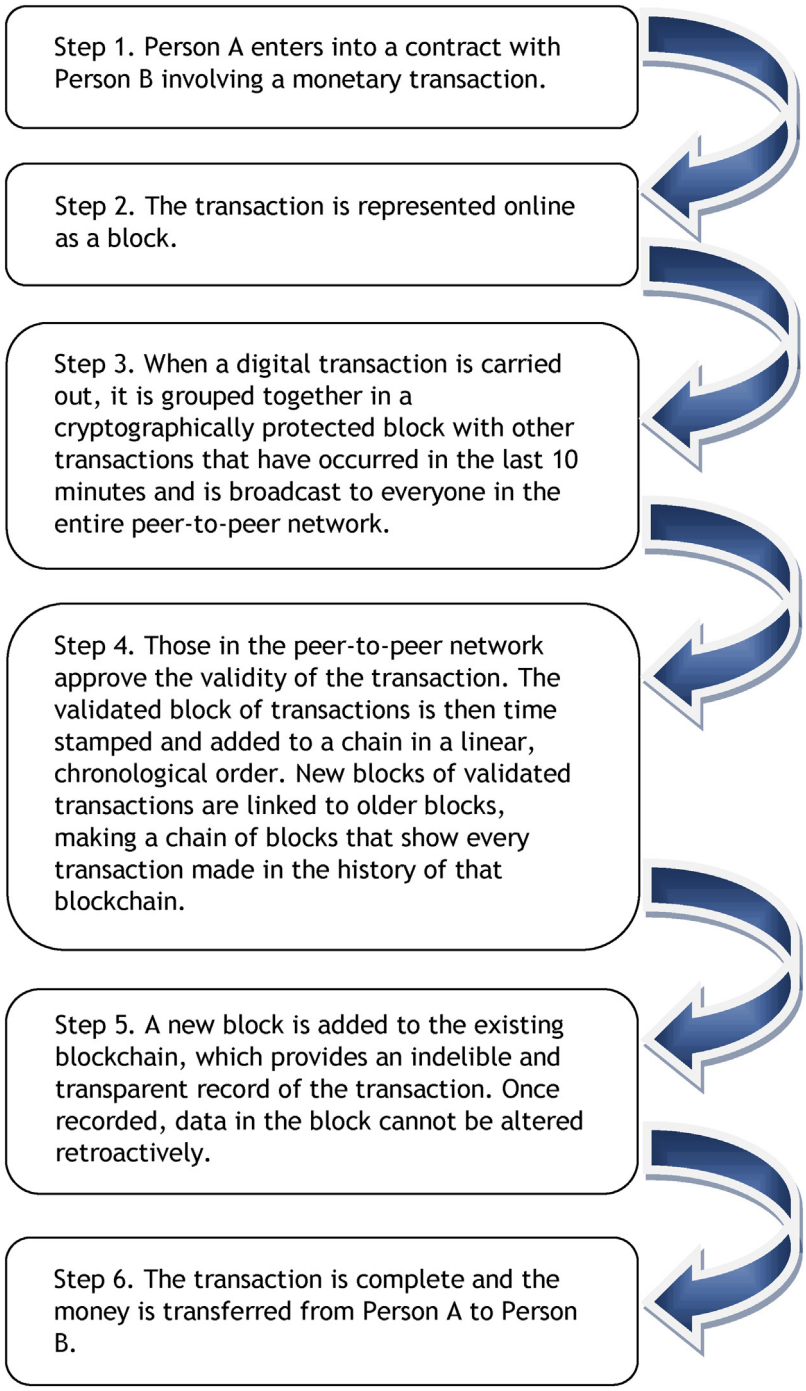
With the aid of technologies such as electronic data interchange (EDI), extensible markup language (XML), and application programming interface (API), BT can facilitate faster, auditable interactions and the exchange of immutable data among supply chain partners (IBM, 2017).

Despite these potential benefits, BT can pose a number of implementation challenges such as a lack of organizational readiness or technical expertise/infrastructure, issues with scalability, and limited financial resources for BT investment. As such, there is an urgent need for developing managerial strategies to help firms overcome those challenges while fully exploiting the benefits of BT. Unfortunately, a vast majority of blockchain research focused on bitcoin systems and anecdotal studies of potential blockchain applications, including smart contracts, financial services, and licensing (e.g., Crosby, Pattanayak, Verma, & Kalyanaraman, 2016; Mainelli & Smith, 2015; Raval, 2016; Tapscott & Tapscott, 2016; Underwood, 2016; Yli-Huumo, Ko, Choi, Park, & Smolander, 2016). Considering these research gaps and the overall scarcity of blockchain research, in this article I present a blockchain architecture and propose potential remedies for overcoming blockchain challenges. I also offer ways managers can exploit BT to improve supply chain resilience from a security perspective. In addition, I identify and investigate contextual variables that may influence a firm's decision to adopt BT.

2. Blockchain architecture

Since a blockchain is a decentralized mesh network of computers linked to each other rather than

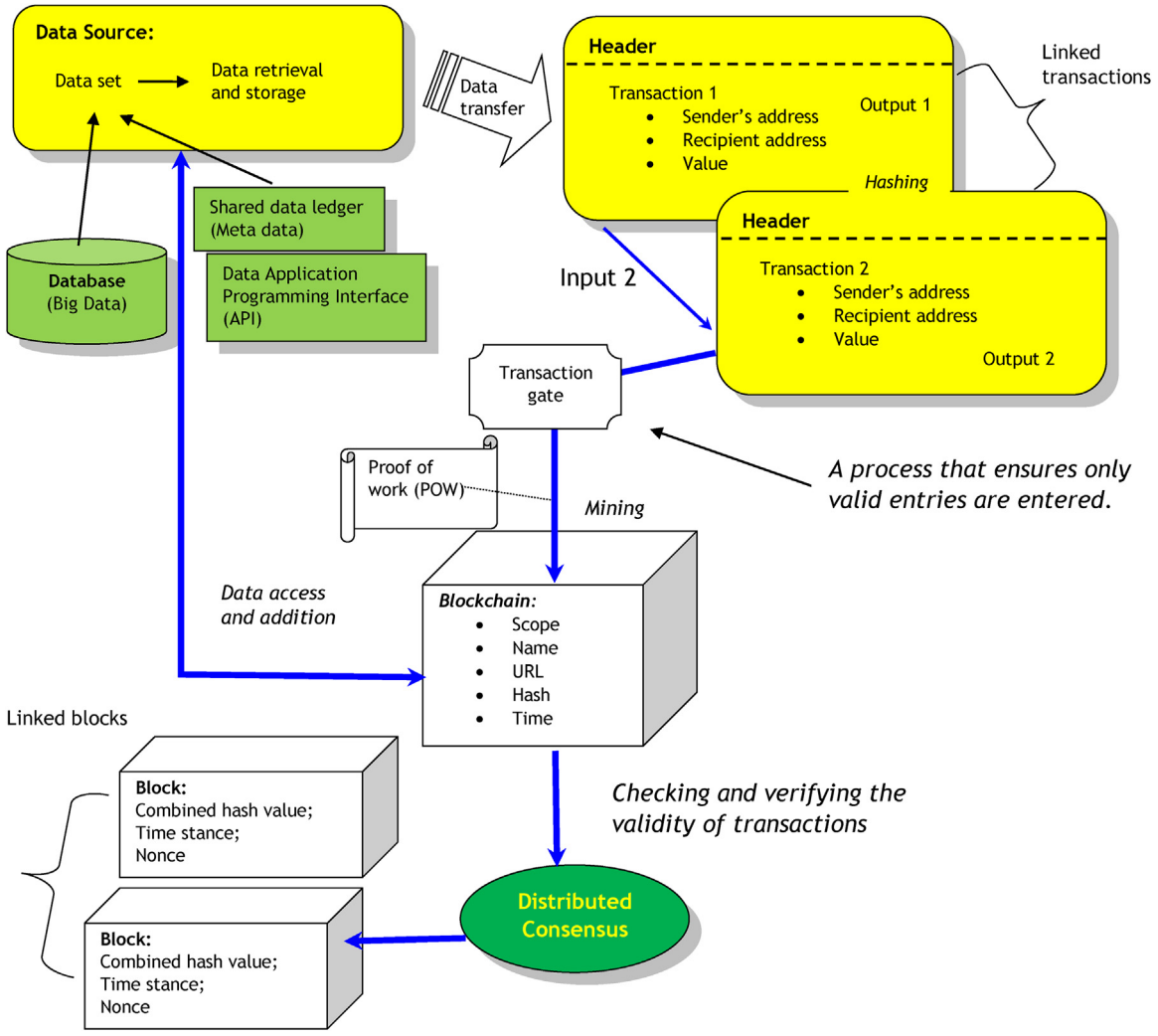
Figure 1. Basic inner workings of blockchain technology



through a central server, there are a number of layers that govern blockchain operations and create the protocols for BT applications. With this in mind, as displayed in Figure 2, I present a blockchain architecture that consists of five modules:

1. *Data source module*, which helps create a blockchain in shared, distributed databases (i.e., ledgers). Unlike traditional databases, these do not use the client-server network controlled by a designated central authority. As such, in providing access to the databases, there is no need for the authentication of a user's credentials by the central authority, which is often subject to hacking and tampering. Instead, all participants in the P2P network verify new additions to the

Figure 2. A basic architecture of the blockchain technology



blockchain based on consensus, making it more difficult to tamper with data. In other words, every user is ensured that that data he/she is retrieving is uncorrupted and unaltered as soon as it is recorded. In this module, data can only be written and read through queries and retrievals as opposed to being read, updated, and deleted.

2. *Transaction module*, which allows for the validation of a transaction and writing of a new transaction. A transaction is a transfer of value between the seller and the buyer and thus changes the state of data contained in the block. While past entries in the block should always remain the same, a new entry can change the state of the data in the past entries (Ray, 2017). This module begins with a transaction agreement between the buyer and the seller. After reaching that agreement, this transaction is broadcast to the P2P network and *miners* (i.e., computers on that P2P network) collect that transaction and process the block with rewards. Once verified, the miners will disseminate the new, unalterable block to the entire P2P network. In this module, an input is a reference to an output from a previous transaction (e.g., Output 1 in Figure 2). Multiple inputs are often listed in a transaction. All of the new transaction's input (e.g., Input 2 in Figure 2) values are added up. Herein, the total value of inputs must be equal to or exceed the total value of outputs.

3. *Block creation module*, which records transaction data permanently in a file called a block. If a block is linked to preexisting blocks and then organized into a linear sequence over time, the blockchain is created. However, it should be noted that a new block cannot be submitted and added to the P2P

network without mining (i.e., the process of adding transaction records to the public distributed ledger of past transactions by solving difficult mathematical puzzles).

4. *Consensus module*, which confirms and validates transactions using the proof of work, proof of stakes, or Byzantine fault tolerance consensus algorithm. This module is crucial in maintaining the sanctity of the transaction data recorded on the blockchain and safeguarding the transaction and block order. As such, this module involves the optimal selection of a consensus mechanism that avoids the corruption of data recorded on the blockchain.

5. *Connection and interface module*, which facilitates web interfaces among users—including ones without coding, technical, or legal skills—while synchronizing and integrating all the IT platforms, software (e.g., bitcoin wallets), and algorithms needed for blockchain applications. This module should help provide real-time information about contractual status and transaction tracking using mobile devices. This module also facilitates the integration among different companies or industries that can communicate with each other and share digital assets with each other seamlessly. As such, interoperability enhanced by this module makes it possible to build more partnerships among different companies and drive greater business value with shared blockchain solutions.

As discussed above, the collaborative supply chain partnership is an important prerequisite to the successful establishment of the BT architecture. The collaborative partnership, however, cannot be formed without sharing common strategic goals (e.g., risk mitigation) and collectively banding resources (e.g., IT investment funds) among the partners. In addition, all partners across the supply chain need to share transaction data that may contain proprietary and sensitive information. This begs the question: Who should be the focal company in the P2P network and who are the trustworthy partners? Herein, the focal company refers to a channel captain that owns abundant resources and thus has a bargaining power over other actors such as its suppliers and distributors in the supply chain. Leveraging its bountiful resources and bargaining power, the focal company can lead the BT initiative and help its trading partners embrace BT. In other words, the focal company is considered a facilitator for establishing the BT architecture and aiding its supply chain partners in exploiting BT. The typical profile of the focal company may be a large multinational firm (MNF) that owns a network of manufacturing and/or distribution facilities supported by a well-established IT infrastructure and staff. The MNFs that fit into this profile include Walmart, Dell, Sony, Samsung, Apple, Unilever, Nestlé, Ford, Toyota, Hyundai, and other *Fortune* 500 companies. In addition to the focal company, trustworthy partners (e.g., certified suppliers) can play an important role in the P2P network by creating or adding to a block in the blockchain.

3. Blockchain applications to supply chain security

A supply chain often intersects business functions and national boundaries with an extensive network of trading partners. These interactions increase the vulnerability of the supply chain and can lead to its disruption. To reduce such vulnerabilities, supply chain professionals need to identify potential weak links and assess their level of risk. Generally, the risk assessment includes the following steps:

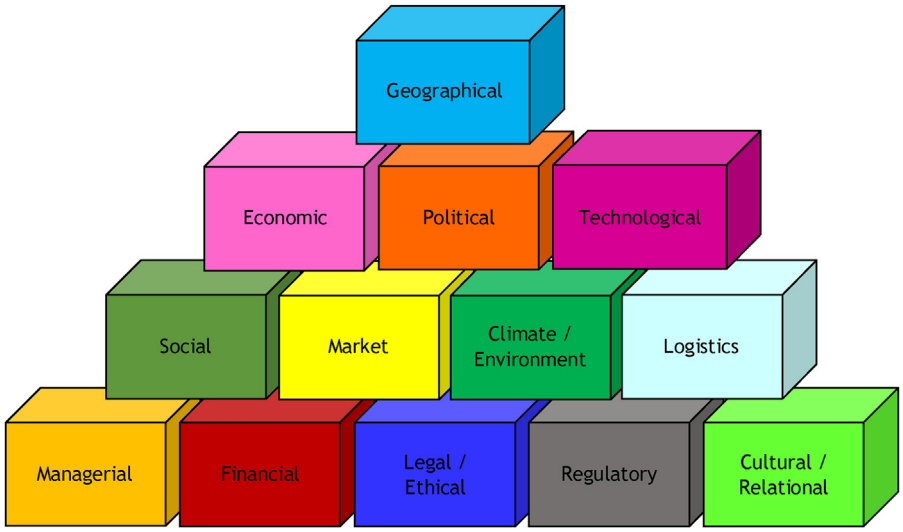
1. *Identify trading or supply chain partners*. These partners may form dots (or nodes) in the supply chain network and represent parties that can create supply chain contracts.

2. *Create the supply chain or process map that shows a transaction and its related information flows*. Mapping these flows (e.g., cargo, container, capital, documents) provides clues to the potential chokepoints (i.e., weakest links) and the degree of exposure to risks and threats, including cyberattacks. Figure 3 shows many sources of supply chain risks.

3. *Categorize and assess vulnerabilities*. Depending on the estimation of risks, those risks should be classified into different categories (e.g., high, medium, low risk) or their risk levels should be calculated with a probability if possible (C-TPAT Training Seminar, 2010).

4. *Develop action or contingency plans for risk mitigation*. Based on the level of security risks and vulnerability assessed by the previous step, appropriate risk mitigation remedies should be developed with deadlines or timetables. In particular, timetables should be set for the establishment of specific action plans, assignment of responsibilities for detailed subplans, outlines of the implementation process, and the delineation of expected outcomes. For example, by adopting

Figure 3. Various sources of supply chain risks



a radio frequency identification (RFID) system that can spot the risks of potential security breaches and can capture the data regarding vehicle movement (e.g., port entry/exit) automatically, security personnel or cargo inspectors can match the captured data to the preregistered/documented data (e.g., shipping documents, manifests). Then, they can identify suspicious data trends (e.g., points of origin from high-terror risk countries) in the incoming cargo for red flags (Min & Shin, 2012). As such, port security can be beefed up with the early detection of abnormalities that often cause security failures.

5. *Implement a system for controlling and monitoring risk mitigation efforts*. Every plan should be evaluated for its efficiency and impacts on security enhancement. Also, it is necessary to check and see if such a plan is on schedule or reaches the designated milestone for continuous monitoring and assurance of the progress. This step includes the development of relevant performance metrics.

Though it is rarely utilized, BT can play a significant role in the steps above; it can be used to prevent security breaches while strengthening supply chain connectivity. BT is hack-resistant, tamper-proof, and immutable due to its distributed ledger and network verification process. BT also offers automatic traceability, since append-only distributed databases of transaction records can be shared across the entire P2P network and those historical records remain forever with permanent footprints. Furthermore, as Figure 4 shows, a blockchain comprised of nodes and arcs can be embedded in the typical supply chain structure comprised of nodes and arcs and thus can be utilized to capture both organizational and network risks associated with the supply chain.

Considering application potentials of BT for managing supply chain risks, it is important to identify specific supply chain activities for which risk can be reduced and then come up with viable remedies for enhancing supply chain resilience. These remedies should comply with the following underlying principles for enhancing supply chain resilience.

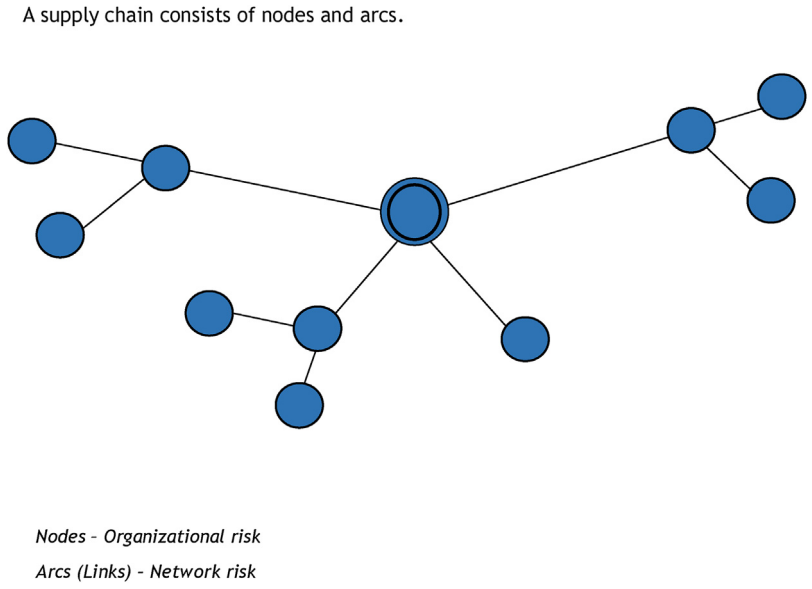
1. *Prevent risk occurrence*. Identify risk sources to avoid risk. For example, avoid shipping routes with high sea piracy or avoid seaports susceptible to frequent bottlenecks and labor strikes.

2. *Reduce the impact of supply chain disruptions*. Consider buffering with additional safety stock, hedging against fuel price hikes for transportation carriers, and risk transfer through insurance coverage.

3. *Improve the flexibility for coping with supply chain disruptions*. Enhance the quick-response capability by shortening recovery time from unexpected events such as disasters or shifting sources of supply close to manufacturing plants (e.g., shifting from offshoring to reshoring or near sourcing).

4. *Change bad habits built by a business-as-usual attitude*. Since complacency or organizational resistance can stifle an innovative idea for managing supply chain risks, supply chain professionals should be open-minded about emerging concepts such as BT. Bad habits of conventional

Figure 4. The supply chain structure with two types of potential risks



risk management often originate from a set of preconceived notions and assumptions that market behaviors are always rational, forecasts are reliable, random events are rare, and buffering is the most effective way to handle risk. This conventional type of risk management rests upon remedies intended for mitigating tangible, visible risks such as terrorism, theft/pilferage, accidents, and natural disasters. These remedies tend to be more reactive (i.e., passive) than proactive and thus focus on damage control after the fact. Many companies that rely on conventional risk management are exposed to invisible risks such as cyberattacks, computer hacking, counterfeiting, miscommunication, credit failures, and contract frauds. Under the many watchful eyes of the P2P network, BT helps reduce hidden, invisible risks that cannot be easily detected by a limited number of participants (e.g., seller, buyer, financial institution) in typical business transactions or supply chain activities. In other words, BT enables its adopter to exploit multiple layered security measures. Figure 5 compares and contrasts conventional risk management principles and BT-enabled risk management principles.

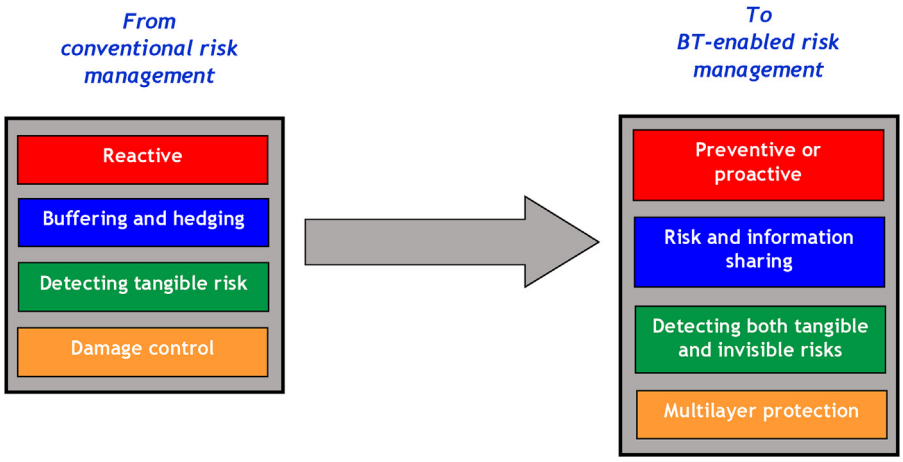
With the above principles in mind, we will elaborate on specific supply chain areas of applications for BT in Sections 3.1.—3.4.

3.1. Smart contracts

One of the first steps that triggers supply chain activities is contract formation. As such, contractual disputes resulting from fraud, misunderstanding, and performance failures can not only destroy the supply chain partnership but also disrupt supply chain activities with prolonged time for resolution. One of the plausible ideas that was put forward recently is to form a *smart contract*, which is a computer protocol intended to facilitate, verify, or enforce contractual obligations by embedding contractual clauses (e.g., collateral, bonding, delineation of property rights) in the computer system and then automating contract execution (Szabo, 1997). Thus, smart contracts not only define the rules and penalties around a contractual agreement in the same way that a traditional contract does, but they also enforce those obligations automatically. Smart contracts are self-verifying and self-executing agreements that can automate the contract lifecycle to improve compliance, mitigate risk, and increase efficiencies across the enterprise (Icertis, 2017).

In a smart contract, a contract can be converted to computer codes and then stored and replicated on the computer system and supervised by the network of computers that run the blockchain. In particular, smart contracts can help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman (Blockgeeks, 2017). As a result, transaction time and costs will be reduced, since smart contracts can execute themselves. Also, by incorporating the Internet of Things (IoT) into the blockchain, contractual fraud will be easily detected and prevented. Furthermore, the integrity of asset transfer made by the contract will be improved with the shared database confirmed by

Figure 5. Evolution from conventional risk management to BT-enabled risk management

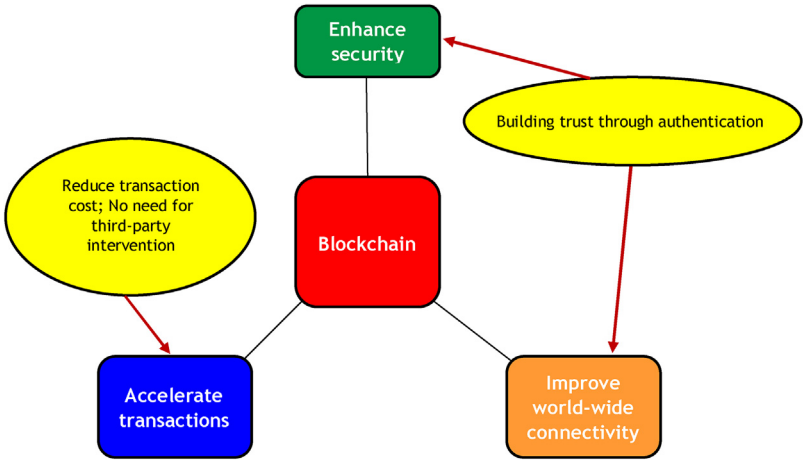


many network participants and the enhanced security of a contract as shown in Figure 6.

3.2. Asset tracking

Once assets—both tangible and intangible—are listed on the blockchain, their ownership is immutable unless the owner verifies a change. The immutable and paperless ledger in the blockchain cannot be altered and thus ownership history cannot be fabricated. In addition, BT operates as a complete and publicly viewable ledger that permanently tracks and records all the supply chain-related activities for a particular asset. BT allows its user to trace all the way back to the origin of an asset. As such, blockchain not only prevents the transaction of fake or counterfeit assets, but it also makes it easier to track goods as they move and change hands in the supply chain. Indeed, the U.S. Department of the Treasury plans to track and monitor the movement of physical assets in real time as they are transferred from one party to another throughout the supply chain process using digital records of asset transfers stored on the blockchain (Higgins, 2017). Likewise, the BT can be utilized to track shipments in global logistics operations. The shipment (i.e., asset) tracking capability of BT can reduce the risk of loss and damage during transit. For example, Maersk, the Danish shipping giant, recently completed a 20-week blockchain proof of concept trial to track its cargo. BT's reliance on cryptographic signatures makes it difficult for anyone to tamper with shipping labels or misplace shipments during transit, all while simplifying global trade with added trust and transparency across the supply chain (Green, 2017; Hackett, 2017b).

Figure 6. Convergence of the blockchain with the Internet of Things



3.3. Secure and error-free order fulfillment

With paperless and easy-to-access customer records, BT can expedite order fulfillment processes throughout the supply chain by quickly confirming customer credit history, checking inventory status, verifying finances, notifying order/shipment status, and offering transparency throughout the entire order fulfillment process as highlighted with circles in Figure 7. By automating the circled order fulfillment steps with accuracy and security, BT will not only reduce order fulfillment errors but also speed up the order fulfillment process. In addition, since the blockchain ledger is open and can be seen by any P2P network participant (e.g., both the buyer and the seller), blockchain transparency will increase visibility of the order fulfillment process and thus reduce the risk of fulfillment error.

3.4. Cybersecurity

Cybercrime has been on the rise for the past decade (CBS, 2015; Statista, 2016). The growing threat of cybercrime can cripple supply chain activities in the stretched supply chain network. Despite countless efforts (e.g., antivirus or malware software, password protection, threat alerts) to deal with such a threat, the risk of cybercrime has never been abated. Another viable solution may be the use of BT, which can remove the risk of a single point of failure with its end-to-end encryption, visibility, and privacy. The immutable nature of a blockchain and the fact that every computer on the P2P network is continually verifying the information stored on it makes BT an excellent tool for mitigating the risk of cybercrime and hacking. In particular, the secure nature of BT makes it useful for accounting and payment audits (e.g., freight payment audits, international payment audits) because BT ensures the integrity of transaction records and no one—not even the record owner—can alter accounting records once they are locked in the blockchain.

4. Managerial challenges of the blockchain

In the previous section, we learned about the various managerial benefits of BT, including reduced transaction fees, public transparency, asset integrity, fraud detection and prevention, P2P connectivity, improved order fulfillment, and increased trust among supply chain partners. However, BT is not without its potential shortcomings and implementation challenges due in part to its revolutionary concept and its sheer complexity. Some of those challenges are displayed in Figure 8. The most pressing among these challenges are scalability, interoperability, and government regulatory issues. In a blockchain, every node needs to process and validate every single transaction, so the blockchain by its nature requires enormous computing power and high bandwidth internet connection, which is not easy to build with the current technology. If such a challenge forces the blockchain to centralize its validation process, it may defeat its original purpose. In addition, given the various platforms that BT can use, finding the optimal combinations of different platforms that are interoperable and compatible with each other would not be easy.

Since BT relies on the distributed ledger that can bypass the interference of a government, the government may increase pressure on BT users through various forms of regulations and legal restrictions and thus may hamper the usefulness of BT for

Figure 7. Part of order fulfillment steps where BT can fit in

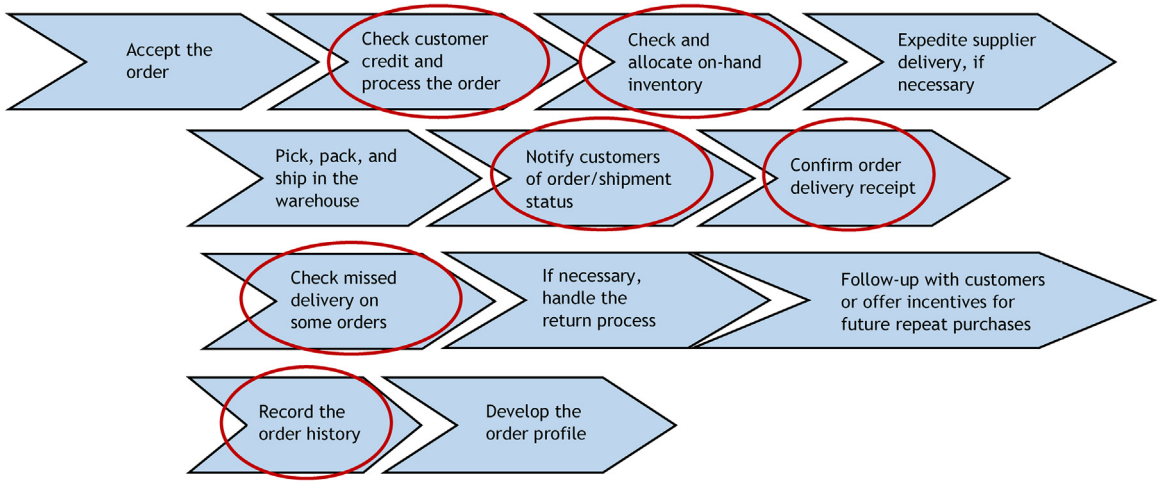
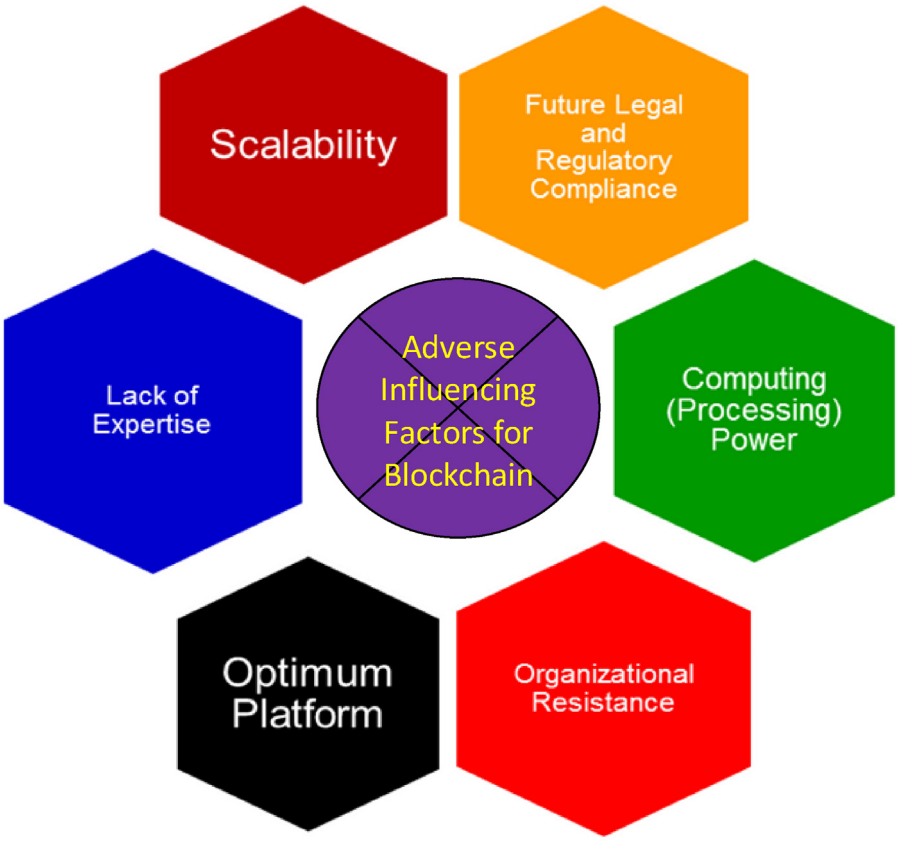


Figure 8. Potential challenges of blockchain technology



ensuring the integrity and privacy of transactions and asset transfers. For example, despite the petition made by the Korea Blockchain Industry Promotion Association, the Korean government is reportedly looking to cooperate with authorities in China and Japan to regulate or ban cryptocurrency exchanges powered by BT (De, 2018). Ironically, added privacy can make it harder for law enforcement officers to figure out who controls a digital wallet, which increases its vulnerability to potential scammers' plots to steal digital currencies recorded on the blockchain (Hackett, 2017a).

5. Concluding remarks and future research directions

In this article, I conceptualize the emerging BT and identify specific application areas of BT to supply chain operations from risk management/security perspectives. It is one of the first attempts to design an architecture of BT for revolutionizing supply chain practices and provide some rationales for its usefulness in enhancing supply chain resilience. Given the paucity of BT-related research and the relative newness of BT concepts that many are still unfamiliar with, this article establishes the conceptual framework of BT in business terms. This article can be extended to include and document real-world cases of BT applications while assessing the impact of contextual variables such as the industry sector, firm size, the size of IT staff and budget, and organizational readiness on the decision to adopt BT.

Similar to the studies of the technology adoption model (TAM) in the IT literature (e.g., Ashraf, Thongpapanl, & Auh, 2014; Cooper & Zmud, 1990; Davis, 1989; Maruping, Bala, Venkatesh, & Brown, 2017; Mathieson, 1991; Oliveira & Martins, 2011), future research will need to extend the scope of this study in order to examine the direction of causality between these variables and the BT adoption decision through cross-cultural and/or longitudinal studies. In addition, future research should investigate the potential impact of other contextual variables such as industry trends, peer pressures, government intervention, and the extent of top management support of the firm's BT adoption decision. Another promising research agenda may include the assessment of synergistic effects of BT on supply chain resilience when it is integrated with business analytics, cloud computing, robotics, and/or artificial intelligence (AI) tools (Min, 2016).

References

Annalect. (2017, October 12). *Blockchain pulls marketing into uncharted territory.* Available at https://www.annalect.com/blockchain-pulls-marketing-into-uncharted-territory/

Ashraf, A. R., Thongpapanl, N., & Auh, S. (2014). The application of the technology acceptance model under different cultural contexts: The case of online shopping adoption. *Journal of International Marketing, 22*(3), 68–93.

Blockgeeks. (2017). *Smart contracts: The blockchain technology that will replace lawyers*. Available at https://blockgeeks.com/guides/smart-contracts/

CBS. (2015, March 3). *These cybercrime statistics will make you think twice about your password: Where's the CSI cyber team when you need them?* Available at http://www.cbs.com/shows/csi-cyber/news/1003888/these-cybercrime-statistics-will-make-you-think-twice-about-your-password-where-s-the-csi-cyber-team-when-you-need-them-/

CoinDesk. (2017). *Bitcoin (USD) price*. Available at https://www.coindesk.com/price/

Cooper, R. B., & Zmud, R. W. (1990). Information technology implementation research: A technological diffusion approach. *Management Science, 36*(2), 123–139.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation, 2*, 6–10.

C-TPAT Training Seminar. (2010). *C-TPAT 5 step risk assessment process guide*. Washington, DC: U.S. Customs and Border Protection.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–339.

De, N. (2018, January 9). Report: South Korea eyes joint crypto regulations with China, Japan. *Coindesk*. Available at https://www.coindesk.com/report-south-korea-eyes-joint-crypto-regulations-with-china-japan/

Eyefortransport (2017). *2017 supply chain trends recap*. Morganville, NJ: EH Publishing Inc.

Fallahpour, M., Shirmohammadi, S., Semsarzadeh, M., & Zhao, J. (2014). Tampering detection in compressed digital video using watermarking. *IEEE Transactions on Instrumentation and Measurement, 63*(5), 1057–1072.

Gartner. (2017, March 2). *Forecast: Blockchain business value, worldwide, 2017–2030*. Stamford, CT: Gartner.

Green, A. (2017, November 9). Will blockchain accelerate trade flows? *Financial Times*. Available at https://www.ft.com/content/a36399fa-a927-11e7-ab66-21cc87a2edde

Hackett, R. (2017a). Blockchain mania. *Fortune, 178*(3), 44–59.

Hackett, R. (2017b, September 6). Maersk and Microsoft rested a blockchain for shipping insurance. *Fortune*. Available at http://fortune.com/2017/09/05/maersk-blockchain-insurance/

Higgins, S. (2017, October 3). The US Treasury is testing distributed ledger asset tracking. *Coindesk*. Available at https://www.coindesk.com/us-treasury-testing-distributed-ledger-asset-tracking/

Holden, W. (2017, September 25). Survey: Enterprise interest in blockchain is heating up. *Juniper Research*. Available at https://venturebeat.com/2017/09/25/survey-shows-enterprise-interest-in-blockchain-is-heating-up/

IBM. (2017). *The benefits of blockchain to supply chain networks*. Somers, NY: IBM Corporation.

Icertis. (2017). *Smart contracts are transforming the way we do business*. Available at https://www.icertis.com/resource/smart-contracts-are-transforming-the-way-we-do-business-featuring-gartner-research/

Langley, C. J. (2017). *The 2018 22nd annual third-party logistics (3PL) study.* Paolo Alto, CA: Infosys Consulting.

Lemieux, V. L. (2016). Trusting records: Is blockchain technology the answer? *Records Management Journal, 26*(2), 110–139.

Mainelli, M., & Smith, M. (2015). Sharing ledgers for sharing economies: An exploration of mutual distributed ledgers (aka blockchain technology). *The Journal of Financial Perspectives, 3*(3), 38–69.

Maruping, L. M., Bala, H., Venkatesh, V., & Brown, S. A. (2017). Going beyond intention: Integrating behavioral expectation into the unified theory of acceptance and use of technology. *Journal of the Association for Information Science and Technology, 68*(3), 623–637.

Maruti Techlab. (2017). *What is blockchain and understand its key benefits*. Available at https://www.marutitech.com/blockchain-benefits/

Mathieson, K. (1991). Predicting user intentions: Comparing the technology acceptance model with the theory of planned behavior. *Information Systems Research, 2*(3), 173–191.

Min, H. (2016). *Global business analytics models: Concepts and applications in predictive, healthcare, supply chain, and finance analytics*. Saddle River, NJ: Pearson Education.

Min, H., & Shin, S. S. (2012). The use of radio frequency identification technology for managing the global supply chain: An exploratory study of the Korean logistics industry. *International Journal of Logistics Systems and Management, 13*(3), 269–286.

Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *The Electronic Journal Information Systems Evaluation, 14*(1), 110–121.

Raval, S. (2016). *Decentralized applications: Harnessing Bitcoin's blockchain technology.* Sebastopol, CA: O'Reilly Media, Inc.

Ray, S. (2017, November 5). Blockchains versus traditional databases. *Hacker Noon*. Available at https://hackernoon.com/blockchains-versus-traditional-databases-c1a728159f79

Statista. (2016). *Statistics and market data on cyber crime*. Available at https://www.statista.com/markets/424/topic/1065/cyber-crime/

Szabo, N. (1997, December 15). Formalizing and securing relationships on public networks. *First Monday, 2*(9). Available at http://ojphi.org/ojs/index.php/fm/article/view/548/469

Takahashi, R. (2017, August). How can creative industries benefit from blockchain? *McKinsey & Company.* Available at https://www.mckinsey.com/industries/media-and-entertainment/our-insights/how-can-creative-industries-benefit-from-blockchain

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world*. New York, NY: Penguin.

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM, 59*(11), 15–17.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? A systematic review. *PLoS One*, *11*(10), e0163477 (Online publication).