JOURNAL OF MANAGEMENT INFORMATION SYSTEMS
2021, VOL. 38, NO. 2, 374–400
https://doi.org/10.1080/07421222.2021.1912926

Beyond the Block: A Novel Blockchain-Based Technical Model for Long-Term Care Insurance

Wenping Zhang [a], Chih-Ping Wei [b], Qiqi Jiang [c], Chih-Hung Peng [d], and J. Leon Zhao [e]

[a]School of Information, Renmin University of China, Beijing; [b]Department of Information Management, College of Management, National Taiwan University,Taiwan; [c]Department of Digitalization, Copenhagen Business School, Frederiksberg, Denmark; [d]Department of Management Information Systems, College of Commerce, National Chengchi University,"Taipei", Taiwan; [e]School of Management and Economics, Chinese University of Hong Kong (Shenzhen), Shenzhen, P.R.C

ABSTRACT

The insurance business is characterized by complicated transactional interrelationships among various stakeholders involved in insurance-related activities. Given this unique nature, the century-old challenge in the insurance industry is to effectively reduce transaction costs among the stakeholders while maintaining business privacy and trust. Although blockchain is a promising technology to mitigate this challenge, two technical issues, namely (1) inefficiency in data auditing and (2) difficulty in verifying encrypted data, are of strategic importance when applying blockchain to the insurance industry. To address these technical challenges, we propose an innovative blockchain-based technical model, InsurModel, in the context of newly initiated long-term care insurance in China. Specifically, we utilize cryptographical methods including "zero-knowledge-proof" to 1) represent business interdependence and 2) verify confidential business information without disclosure of specifics. We demonstrate the scalability and applicability of InsurModel and explore its strategic implications in constraining adverse behaviors of the stakeholders.

KEYWORDS

Long-term care insurance; blockchain application; business interdependence; zero-knowledge proof; transaction-cost economics; blockchain in insurance

Introduction

Blockchain technology has received enormous attention in the insurance industry in recent years and has rapidly become the frontier of business innovation. Insurance business is characterized by document-intensive workflows and complicated transactional interrelationships among a number of stakeholders (e.g., insured, insurer, hospitals, and nursing homes) involved in insurance-related activities (e.g., application, claim, and reimbursement). Given this nature of insurance business, the largest challenge is to effectively reduce transaction costs among the stakeholders while maintaining business privacy and trust. Many practitioners have suggested adopting blockchain technology to reduce the transaction costs [10, 30, 31]. More specifically, decentralized database, immutability, and transparency characterize the blockchain as a trusted transaction system, which can constrain the opportunistic behaviors and thereby reduce transaction costs [22]. Nevertheless, two

CONTACT Chih-Hung Peng chpeng@nccu.edu.tw No.64, Sec. 2, Zhi-Nan Rd., Wenshan District, Taipei City 116011, Taiwan (R.O.C.).

Supplemental data for this article can be accessed on the publisher's website.

technical challenges remain, constraining the application of blockchain in the insurance industry [6, 11, 19].

The first technical challenge is the inefficiency in auditing data submitted by different stakeholders. All stakeholders participating in the insurance industry frequently exchange insurance-related data. Data in blockchain are deposited as an independent point, and business interdependence information among the data is unavailable. For instance, an insured individual must submit his/her application file (denoted as Dp1), including the files (denoted as Dp2) from another agency, for reimbursement. In this case, Dp1 and Dp2 are interdependent because they are linked by the reimbursement procedure. However, existing blockchain techniques do not keep business interdependence information in a blockchain, though such information significantly enhances data traceability. Therefore, if any data tampering activity from either Dp1 or Dp2 or their collusion exists, identifying the tampering source in the existing blockchain is time-consuming and inefficient because the existing blockchain does not afford traceability. Consequently, such inefficiency in auditing data may induce stakeholders to perform opportunistic behaviors (i.e., economic actors' self-interest seeking and their calculated efforts to mislead or distort information), thereby increasing the transaction cost [45, 46]. Therefore, embedding business interdependence information into blockchain is beneficial because such implementation can enhance the traceability of blockchain, which eventually conduces to reducing the transaction cost.

Second, information is encrypted and stored in a blockchain; however, the encrypted information cannot be effectively verified through most protocols used in existing blockchain applications. Although information exchange among stakeholders in the insurance industry is beneficial, stakeholders are not obligated to grant permission to others to access encrypted information due to concerns regarding their business privacy. For example, insurance companies conduct background investigations on applicants (e.g., credit score of an applicant) by themselves and can share information with each other (e.g., whether the credit score of an applicant passes a threshold). However, insurance companies are less willing to share because other stakeholders may opportunistically misuse the shared customer data. An insurance company has the following two options to avoid or mitigate such potential opportunism. First, the insurance company can decline to share all its customer information, thus possibly terminating the information exchange among stakeholders. As a consequence, the focal insurance company cannot receive information from other parties as well, thereby increasing its cost because the insurance company must check all applications by itself. Second, the insurance company chooses to share its customer information with other stakeholders. However, the insurance company needs to put additional effort in its ex-post governance to the shared data, leading to additional cost. Hence, the transaction cost increases regardless of which option the insurance company chooses for managing opportunism. In this study, we focus on mitigating the transaction costs incurred by the second option. Therefore, a mechanism to verify the encrypted information containing business privacy without any privacy disclosure is needed.

The aforementioned challenges incur transaction costs associated with opportunism in authentication and verification. To address these challenges, we propose in this research a novel blockchain-based technical model, *InsurModel*, which is in collaboration with a Fortune 500 insurance company in China (referred to as "Tai-Chi Insurance"), for a specific insurance product, namely long-term care insurance

(hereinafter, LTCI, details are provided in § *The Long-Term Care Insurance [LTCI] Initiative in China*). In particular, InsurModel implements an embedded layer representing the business interdependence in the blockchain. A new protocol with zero-knowledge proof (ZKP) is also implemented in InsurModel. This protocol can verify whether the encrypted information (i.e., pricing information in our context) is within the specified range without any sensitive information disclosure.

The feasibility of the proposed approach is demonstrated through an in-depth applicability check. In particular, we conducted a series of interviews with insurance sales representatives, a data security manager (DSM), an IT manager (ITM), and a vice president (VP) of Tai-Chi Insurance. The interviews derive several strategic implications: First, InsurModel can constrain opportunistic behaviors among stakeholders and thus reduce transaction costs. Second, because of its scalability, InsurModel can be applied to other insurance products that are remarkably complicated and involve numerous stakeholders. Third, InsurModel facilitates cooperation among the stakeholders due to its business privacy protection.

In the remainder of this article, we first elaborate the research background, including the LTCI initiative in China, and the key challenges in the current practice in the next section. Subsequently, we present a comprehensive review of the related literature. Next, we detail the design of our proposed InsurModel with a scenario-based illustration and then describe the evaluation results and the applicability check of InsurModel. We conclude this study with the strategic implications of our proposed InsurModel and some future research directions in the last section.

Research Context

Long-Term Care Insurance (LTCI) Initiative in China

Long-term care involves a variety of services, which help fulfill the needs of people with chronic diseases or disabilities who cannot take care of themselves for a long period of time [17, 32]. LTCI, or similar insurance products, are designed and sold in many countries, such as the United States, the United Kingdom, Canada, and Germany. In contrast with conventional health or life insurance, LTCI is only used to pay for the costs associated with long-term care, such as Alzheimer's facilities, nursing homes, assisted living facilities, and adult day-care centers. Due to the commonwealth nature of LTCI, only qualified individuals are allowed to purchase this insurance.

The Chinese government initiated a national LTCI program in 2016. In this cooperative program, the government and qualified individuals respectively share 90 percent and 10 percent of the expense for a commercial LTCI. To reduce vicious competition among insurance companies and avoid potential monopoly, the government appointed only one insurance company as the leading role and other insurance companies as the distributing role in one city. That is, only one LTCI product, which is designed by the leading insurance company, is available in each city. To utilize the existing sales networks effectively, all insurance companies (including the leading company) in the city serve as the distributing insurance companies for selling LTCI. Accordingly, the government grants different authorities to the leading insurance company and distributing insurance companies. The leading insurance company is authorized to authenticate all claims and documents, such as medical

records or reimbursement applications, which are submitted by different parties, such as hospitals, nursing homes, financial institutions, and distributing insurance companies. Specifically, the government delegates the leading insurance company to serve a regulatory role in its city. Moreover, the insurance company that releases the LTCI product in a city is obligated to compensate all insured for the expenses associated with long-term care, even when the insured purchased the LTCI product from other distributing insurance companies. Hence, the leading insurance company has a high workload of authentication and verification.

In contrast to the leading insurance company, which takes governance and regulatory responsibilities in LTCI, the distributing insurance companies (including the leading insurance company) 1) sell the LTCI to qualified individuals and 2) collect and transfer the relevant files or documents from/to the other stakeholders. Thus, the distributing insurance companies are obliged to collect and authenticate all documentary claims from their LTCI clients (i.e., those who bought their LTCI products) and send such files to the local leading insurance company. In addition, a fixed amount of compensation per transaction is rewarded to the distributing insurance companies as a source of motivation. Moreover, the government (i.e., China Insurance Regulatory Commission) grants distributing insurance companies the right to price their LTCI products within a specific range autonomously. Therefore, the distributing insurance companies can sell the LTCI at their customized price as long as such price is within a specified and regulative range.

Challenges in the Chinese LTCI

A leading insurance company encounters several operational challenges associated with opportunism due to the business model of LTCI. The first challenge is related to data authentication and verification. As previously depicted, the leading insurance company is both the regulator and a seller in the LTCI business. As the regulator, the leading insurance company supervises the general operation of LTCI and authenticates the submitted claims and documents of the distributing insurance companies. By contrast, as a seller, the leading insurance company also competes with other distributing insurance companies for the market share. Such a dual role of the leading insurance company creates a trust concern for the distributing insurance companies, thereby inducing the opportunistic behaviors to seek for their self-interest. For example, the distributing insurance companies may passively cooperate with the leading insurance company in the LTCI practice. Elaborately, the distributing insurance companies may be reluctant to verify each part of a file or document submitted by or collected from the insured or other stakeholders in an adversarial or uncooperative stance conscientiously. This condition incurs additional transaction costs for the leading insurance company in either verification or future auditing, which is consequently prejudicial to the LTCI practice. Essentially, blockchain technology can only afford assurance for tamper-proof records. However, the insurance industry involves a large load of documentation and complex business interdependence among various stakeholders. Thus, designing a mechanism that can reduce transaction costs by promptly tracing the business interdependence of the documents deposited in the blockchain is crucial. This new mechanism can constrain the potential opportunism and thus eliminate the skepticism for both sides (i.e., leading insurance company versus distributing insurance companies).

The second challenge is related to protecting business privacy. The leading insurance company designs the LTCI product and also sets its price range in one city. As depicted in the last section, the China Insurance Regulatory Commission permits distributing insurance companies to set their selling price of this LTCI product within the specified range. Evidently, the selling price, which is an important business privacy issue for each insurance company, is nondisclosure information, even to the local regulator (i.e., the leading insurance company), because they are competitors in selling insurance products in the same city. The distributing insurance companies may perform opportunistic behaviors because they are compensated for each transaction. In particular, these distributing insurance companies may sell LTCI at a price below the lower bound of the specified price range to receive transaction rewards unethically. The detailed selling price is encrypted and deposited in the blockchain by the distributing insurance company. Thus, the leading insurance company, as the local regulator, should ensure that LTCI is sold within the specified price range despite no access to pricing information. Accordingly, a new method for price range proof with insufficient information is needed.

Review of Relevant Literature

The literature review is conducted on the basis of the challenges identified in the proceeding section. In particular, the following review mainly focuses on the overview of blockchain technology and its opportunity and implications for the insurance industry from the perspective of transaction cost economics.

Overview of Blockchain Technology

A blockchain was originally designed as a public ledger to support the transactions of the first-ever cryptocurrency (i.e., Bitcoin). This public ledger is a secure system that effectively resolves the double-spending problems without a third-party authenticator [29, 31] by jointly using a peer-to-peer (hereinafter P2P) network and various cryptographic protocols. Elaborately, a P2P network is neither a new phenomenon nor a new technology; it was developed to store and share files by a group of devices collectively [12]. To record cryptocurrency transactions, a secured P2P network was implemented to store a copy of the ledger across multiple anonymous devices. That is, each device in the P2P network serves as an anonymous node storing certain data, which characterizes the decentralization property of blockchain technology.

Although a P2P network overcomes the deficiencies of the client-server (C/S) architecture, the traditional P2P network remains vulnerable to establishing a trustworthy relationship among different anonymous nodes within the network [19]. Therefore, the data transacted in a blockchain and their respective storage information are encrypted, and any changes to transaction data require a majority consensus of the network nodes. Given such unique characteristics, a blockchain inherently guarantees that transaction data are processed in an immutable and transparent manner [49].

In addition to the high degree of security and efficiency, a blockchain, as a programmable artifact, exhibits considerable potential to support different business requirements. For example, financial institutions have attempted to design and implement blockchain-based smart contracts to mitigate information asymmetry and increase contractibility in an algorithmically automated and conflict-free manner [11]. Merchandisers have also

conducted a trial to use blockchain-based systems in governing and monitoring logistics and supply chains [27].

Several rudimental blockchain-based applications are also available in the extant literature. For example, Liang et al. [23] implemented blockchain to synchronize personal health data across different devices for mobile users and found that the blockchain-based solutions outperformed the traditional C/S architecture in terms of efficiency and security. Zheng et al. [50] proposed a prototype system for sharing health data by jointly using smart devices and a blockchain and then proved the viability of their proposed system. Zhou et al. [51] utilized blockchain technology to develop a decentralized database to store medical insurance records and evaluated the technical and economic performance of transactions. Chanson et al. [8] applied the design science approach to building a blockchain-based sensor data-protection system to prevent odometer fraud. Despite their contribution to blockchain applications, business relevance or economic rationale is not comprehensively expounded. Thus, research on synthesizing the technological and business aspects of blockchain in a real case is demanded to obtain the sociotechnical perspective for the IS discipline. In the next subsection, we will build upon the transaction cost economics and deliberate how this theory serves as a kernel theory to inform the construction of a blockchain-based artifact in the insurance industry.

Transaction Cost Economics and Blockchain in the Insurance Industry

Transaction cost economics (hereinafter TCE) posits a governance structure that achieves economic efficiency by minimizing transaction cost [45]. TCE pertains to "transaction" and "cost." The "transaction" refers to an exchange of information, goods, or services, while "cost" (namely "transaction cost") refers to the associated monetary or non-monetary values involved in such an exchange. Information and communication technology can reduce the imperfection in the economic system. Therefore, TCE has been widely applied to support the theoretical explanation of many topics in IS literature. For instance, the TCE offers a theoretical rationale to explain the variations in offshoring costs or transaction risks and their impacts in accomplishing projects of IT sourcing [14, 48]; digitalization can drastically reduce the transaction costs incurred from the supply chain by symmetrizing and integrating information between upstream vendors and downstream buyers [13, 15]; TCE also affords theoretical perspectives to explain why IT investment contributes to firm's IT capability, thereby informing the relevant IT strategies [3, 37, 44].

Despite its dominance as an explanatory theory, few studies in extant IS literature have used TCE as a kernel theory in design science research. Gregor and Hevner [20] argued that justificatory knowledge from any descriptive theory could be employed to inform artifact construction [20]. Any information exchange between the leading insurance company and a distributing insurance company can be understood as a "transaction" in the LTCI context, and the time and expense associated with such transaction is the "cost." Therefore, guided by the viewpoints proposed by Gregor and Hevner [20], we further delve into TCE and discuss how TCE can be referenced to design IT artifact in our case.

The central assumption of TCE is that economic actors are opportunistic. Opportunism refers to self-interest seeking actions with guileful behaviors, such as "incomplete or distorted disclosure of information and calculated efforts to mislead, distort, disguise,

obfuscate, or otherwise confuse" [46, p. 47]. Theoretically, an informationally complete contract [1] between contracting parties can prevent opportunism. However, due to the absence of a complete contract, each contracting party likely indulges in opportunism and seeks economic rents [47], incurring transaction costs. Thus, mitigating the opportunistic inclination of contracting parties is a valid approach to reduce transaction costs. One potential mitigation approach is to build trust between contracting parties [5, 9].

Blockchain allows contracting parties to develop their mutual trust and constrain their opportunistic behaviors. As previously depicted, because of its decentralized nature, blockchain does not depend on a third-party to establish trust among contracting parties but depends on immutable and transparent transactions as well as validated records. In other words, blockchain naturally builds up trust among all involved parties and constrains their potential opportunistic behaviors [39]. For example, in the insurance industry context, the decentralized ledger in a blockchain can constrain opportunistic behaviors, such as suspicious and duplicate claims, by logging each transaction record stored in multiple devices. Such decentralized repositories serve as verifiers for authenticating all historical files and documentations, consequently preventing opportunism among all concerned parties by technologically prohibiting corruption and tampering [43]. As suggested in TCE, constricting opportunism can effectively reduce the transaction cost.

There are two types of transaction cost in TCE: ex-ante and ex-post transaction cost. The former refers to the transaction cost incurred from setting up a contract (i.e., a trustworthy communication protocol among all stakeholders in the LTCI context), while the latter refers to the transaction cost used to monitor other contracting parties to assure contract fulfillment. The rudimental blockchain can alleviate opportunism resulting from distrust between/among contracting parties, thereby reducing the ex-ante transaction cost. However, opportunistic behaviors can still emerge from contracting parties, thus incurring the ex-post transaction cost. In our research context, the leading insurance company must validate all the transaction-related data from other stakeholders to detect insurance fraud. Although data manipulation or distortion is traceable in a blockchain, such traceability in an existing blockchain becomes inefficient when the complexity of business transactions and the number of contracting parties significantly increase. In this case, other stakeholders may exploit such inefficiency to conduct opportunistic behaviors, such as tampering or distorting data, because their opportunism may not be promptly traced. Accordingly, monitoring and managing such opportunism increases the ex-post transaction cost, which should be reduced with more efficient auditing or authentication. Therefore, it is essential and desirable to facilitate the efficient traceability of existing blockchain applications not only for the leading company in LTCI (i.e., our research context) but also for the general insurance industry.

The existing blockchain also allows contracting parties to protect their business privacy. In the LTCI context, the leading insurance company is required to verify submitted data by stakeholders. However, submitted data are encrypted in the blockchain environment. Therefore, effectively verifying encrypted data is difficult for the leading insurance company because the stakeholders are not obligated to grant permission to encrypted data. Without access to the encrypted data creates an opportunity for the stakeholders who attempt to conduct opportunistic behaviors. For example, a distributing insurance company may sell an LTCI product at a price lower than the specified price range and such pricing information as a business privacy of the distributing insurance company is encrypted in the

blockchain. The leading insurance company, as a regulator in LTCI, must govern the opportunistic utilization of the business privacy protection mechanism, which, in turn, incurs the ex-post transaction cost. Therefore, it is necessary to improve the functionality of existing blockchain applications, which allows one party to verify the business privacy of the other party and allows the other party to protect its business privacy.

To further mitigate the transaction costs, especially ex-post transaction costs, we propose a technical model to add on the existing blockchain technology. In particular, a new layer embedded in the blockchain is constructed to represent the business interdependence. This layer can facilitate traceability, which, in turn, reduces the transaction costs incurred by authentication or auditing. In addition, we apply a cryptographic method, namely ZKP, to verify the statement without disclosing complete information. This method protects business privacy while fulfilling the authentication requirement.

Design of InsurModel: A Technical Model for a Chinese LTCI

To address the challenges described in the previous section, our proposed blockchain-based technical model needs to achieve the following objectives. The first objective is to capture and represent the business interdependence among files or documents received from different LTCI stakeholders in the blockchain. The second objective is to allow the leading insurance company to perform the price range proof without requiring distributing insurance companies to reveal their selling prices. In addition to the two objectives, the proposed InsurModel should attain a high-level functional scalability and applicability.

Business Interdependence

Business Interdependence in LTCI

In the current practice, LTCI stakeholders store data in their relational databases. Application programming interface (API) calls are used to facilitate data exchange from these databases with disparate data schemas. However, such synchronization is neither effective nor trustworthy. Figure 1a illustrates communication among different relational databases with heterogeneous data schemas. Each organization has its own relational database with distinctive data schemas. Data communication and exchange among different organizations depend on API calls. Thus, the overall process is vulnerable because miscommunication may occur in either the intraorganizational process (solid arrow) or interorganizational communication (dashed arrow). For example, suppose T (square mark), as the leading insurance company, must receive two identical files from two organizations, namely A (rhombus mark) and X (another rhombus mark), for authentication. However, in the presence of inconsistent information in the two files, T cannot identify the reason causing such inconsistency because 1) A may opportunistically send different files to X and T or 2) X may tamper the file received from A and then sends the tampered file to T.

In contrast to the *Traditional Database Model* (Figure 1a), the blockchain technology deposits each encrypted piece of data in the blockchain, thereby assuring a tamper-proof record through decentralized storage. As Figure 1b illustrates, despite keeping the organization-specific databases, we create a blockchain as a new layer above all entities. After encrypting all relevant data into a series of irreversible strings (hash values, as will be detailed in § *Representation of Business Interdependence in Blockchain*), we deposit these

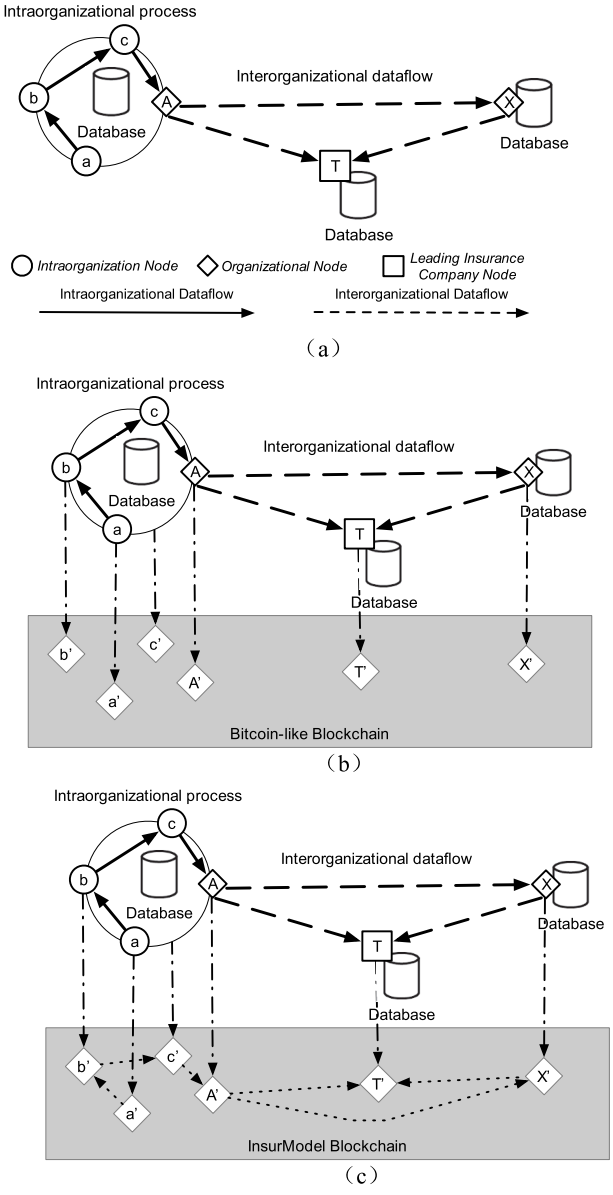


Figure 1. a) Overview of traditional database model; b) Overview of bitcoin-like blockchain model; c) Overview of our proposed InsurModel blockchain model.

strings in the blocks (the grey area). The blocks are linked with one another through a cryptographic hash and eventually form a chain [12], which assures the integrity of the previous block and is strengthened against tampering and revision.

However, the traditional blockchain-based model (i.e., the *Bitcoin-like Blockchain Model*) cannot efficiently address the traceability issue at the file level. Each transaction record in Bitcoin is independently stored, and the relationship among transaction records is missing. In our research context, each data point represents a file or claim uploaded by a stakeholder,

which should be interdependent with other files in accordance with different industrial logics. Thus, our proposed technical model (i.e., InsurModel) should provide decentralization and consider business interdependence. Figure 1c shows that the relationship (solid and dashed arrows) between different nodes is also cryptographically linked and cannot be revised or tampered with.

Representation of Business Interdependence in Blockchain

In contrast to the Bitcoin-like Blockchain Model, InsurModel essentially stores data and represents the entire business interdependence inside its blockchain. To do so, in addition to depositing the encrypted data into the blockchain, we apply a hash function, which is used to map data of arbitrary size to fixed-size values, to generate a Merkle tree[2] to encode business interdependence.

To better understand the representation of business interdependence in a blockchain, the key difference between the Bitcoin-like Blockchain Model and InsurModel is respectively illustrated in Figures 2a and 2b. Assume that business interdependence exists among three parties (i.e., A→B→C) (dash-dotted arrow in Figures 2a and 2b). In particular, File A, which is stored in the database of Party A (Database A), is used as input to construct File B1, which is stored in Database B (dashed arrow in Figures 2a and 2b). File B2 from Database B is used as input to construct File C1, which is stored in Database C (dashed arrow in Figures 2a and 2b). An intraorganizational dependence also exists within Party C, from Files C2 to C3 (dashed arrow in Figures 2a and 2b). The Bitcoin-like Blockchain Model only encrypts the data from each file and stores it as a point in the block, where each point is independent of each other as shown in Figure 2a. In the proposed InsurModel, in addition to data file encryption, a hash function is also used to construct a Merkle tree whose structure exhibits business interdependence, as Figure 2b shows. Specifically, similar to the Bitcoin-like Blockchain Model, data points are encrypted and stored in the blocks in the proposed InsurModel. Business interdependence is cryptographically represented as a tree-like structure by using a smart contract, a self-executing contract with the terms of the agreement between the two or more parties being directly written into the lines of code (A, B, and C in the example). The tree-like structure embedded into the blockchain is referred to as the InsurModel FileTree. In this regard, the data points encrypted from the files and the relationship across different parties are deposited and represented in the block.

To achieve the design in Figure 2b, two functions, namely a hash function (denoted by h(x)) and a digital signature function (denoted by s(X)), are used to compute the hash value of a particular file, where x refers to the file (e.g., File A, B1, or C2), and X refers to the party (e.g., A, B, or C). Thus, the hash value of File A, denoted by $\text{Hash\_Value}_{\text{File\_A}}$, can be expressed as:

$$Hash\_Value_{File\_A} = h(File\ A) + s(A)$$

.

Given only one file, File A, is found in Database A, we deposit $\text{Hash\_Value}_{\text{File\_A}}$ into the Merkle root of Party A, which is denoted by Root A. Subsequently, given that File A serves as the input for File B1, we append the hash value of File A to the end of the content in File B1 and then apply the hash function with the digital signature of B. Similarly, the hash value of File B1 can be calculated as follows.

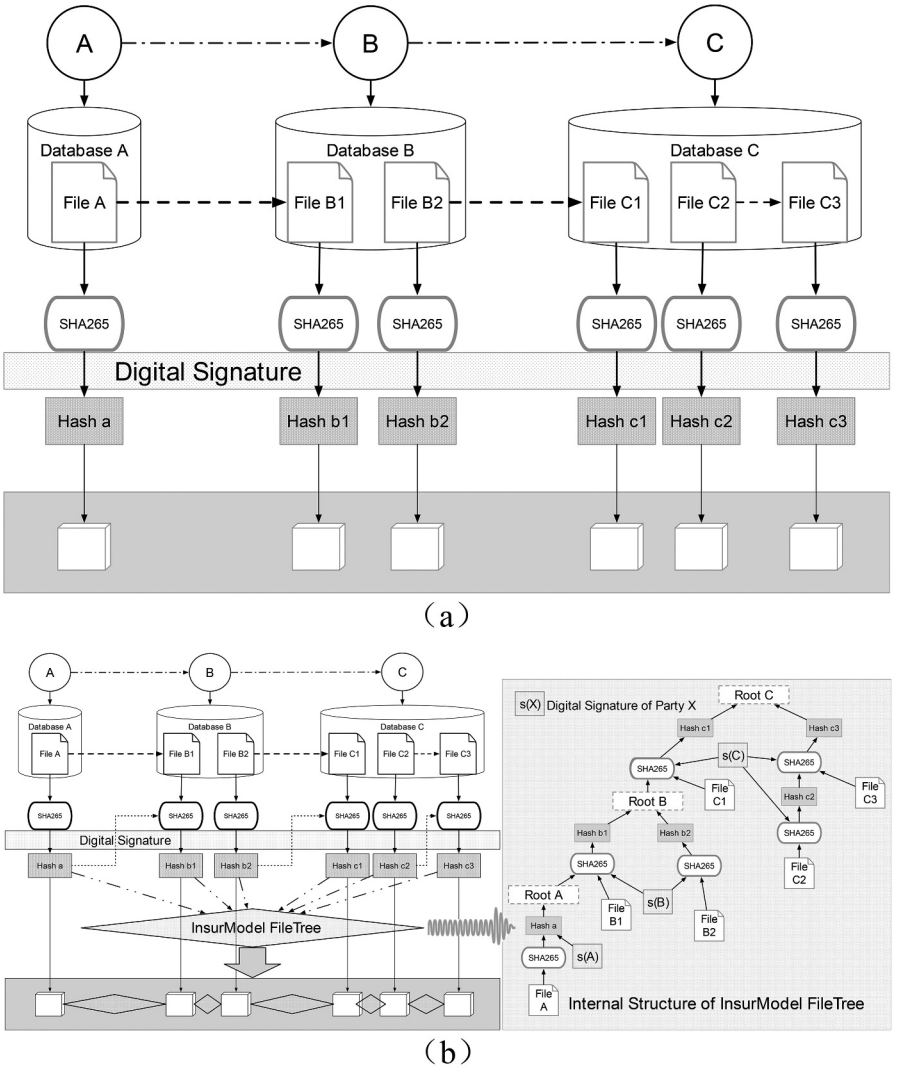


Figure 2. a) Workflow in bitcoin-like blockchain model; b) Workflow in InsurModel blockchain model.

$$Hash\_Value_{File\_B1} = h(File\ B1 + Hash\_Value_{File\_A}) + s(B)$$

.

In the preceding formula, business interdependence between A and B (i.e., File A as input for File B1) is included in the hash function. Iteratively, we can construct a Merkle tree to represent business interdependence based on the file-level relationship. Given that the hash value is unique from the same algorithm (in our case, we adopt SHA256, a type of Secure Hash Algorithm), because each file's hash value is calculated by the hash value of its backward file and its digital signature, when any tampering occurs, we can explicitly identify the source of tampering. For example, a set of unique hash values were stored in the Merkle tree in Figure 2b when the original data were first inputted. The initial hash values can be

used as the reference benchmark to examine whether tampering occurs in the subsequent rounds. If no tampering occurs, the hash value in each Merkle root (i.e., Root A, B, or C) should be consistent with the initial hash value. However, when multiple parties tamper with File B2, the source of tampering can be traced by comparing the hash values with those in the reference by "leaf." The first inconsistent hash value can eventually be identified from File B. Accordingly, we can determine the respective tampering source, namely File B, and the party performing opportunistic behavior, namely B. Thus, the use of a Merkle tree to represent business interdependence can improve the efficiency of data search and verification, particularly for handling data involving large amounts of parties, and consequently mitigate the transaction cost. We will report empirical evidences in § *System Evaluation*.

Price Range Proof

As described in § *Challenges in the Chinese LTCI*, a distributing insurance company may strategically commit fraud against the government by selling LTCI below the lowest price allowed. To address such a dilemma between business privacy and the demand for verification, we implement the ZKP protocol in InsurModel. The ZKP enables one party, referred to as the verifier in the ZKP literature, to verify particular information possessed by another party (called the prover) without revealing the information itself [4].

In the LTCI context, ZKP serves as an important mechanism to facilitate the leading insurance company to verify whether an unethical reward has been received by a distributing insurance company. Given that pricing information has been anonymized by the hash function, the leading insurance company cannot determine the real selling price of a distributing insurance company. The ZKP of range is used to prove whether a secret value lies within a given range without revealing the exact value. The given range in the LTCI context is the price range set by the leading insurance company, and the secret value is the LTCI selling price of a particular distributing insurance company. We illustrate the business logics of price range proof in Figure 3.

To understand how ZKP is implemented in the LTCI context, we further elaborate the mechanism of ZKP and its application in this context. Similar to any modern cryptographical protocols, ZKP is established on a commitment schema. The commitment schema is a cryptographic primitive that allows an individual to commit to a secret message m by creating a commitment c. Such a commitment can be disclosed at a later time. On the basis of Morais et al. [28], we define a commitment scheme as follows.

Definition 1. A commitment scheme is

(1) $c = \text{Commit}(m, r)$, where m and r denote a secret and randomness, respectively. The commitment value c, which is calculated from the commit algorithm, encloses the secret m. Furthermore, no alternative, which is denoted by m' and r', from the commitment value c meets the condition that $\text{Commit}(m', r') = \text{Commit}(m, r)$.

(2) An open algorithm, which is denoted by $b = \text{Open}(c, m, r)$, is available. This algorithm returns a TRUE value only when the returned value from the commit algorithm, $\text{Commit}(m, r)$, is consistent with the given value c.

Two security properties (i.e., hiding and binding properties) are presented in the preceding definition. The hiding property indicates that no one can learn what exactly the committed message m is from commitment c, while the binding property indicates that commitment c is exclusively associated with message m.

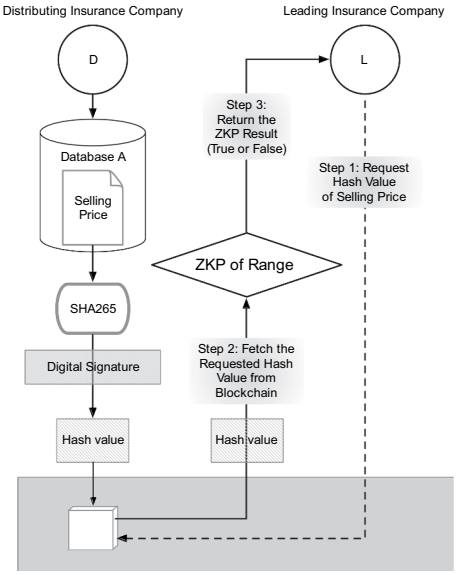


Figure 3. Business logics of price range proof in InsurModel.

In our study, we adopt the Pedersen commitment [34], which is one of the most popular commitment schemas. Mathematically, let $\mathbb{Z}_p$ denote the group of secrets with prime order p, and the commitment is defined as $c = \text{Commit}(m, r) = g^m h^r$. In this closed formula, g and h are two random public generators, m refers to a secret message, and r denotes randomness.

The ZKP of range can be explained through a decomposition process. A secret δ (e.g., the selling price of a distributing insurance company) can be decomposed into a base u format as follows:

$$\delta = \sum_{j=0}^{l} \delta_j u^j$$

.

Thus, to proof that $\delta \in [0, u^l)$, we need to verify that each δ_j satisfies $\delta_j \in [0, u)$. Then, by conducting ZKP of range for any proofing ranges $[a, b)$, we need to verify that $\delta \in [a, a + u^l)$ and $\delta \in [\text{b} - u^l, b)$, namely the respective proofs of $\delta - a \in [0, u^l)$ and $\delta - b + u^l \in [0, u^l)$. That is, to complete the proof of a specific range $[a, b)$, we need to apply the algorithms given in Table A1 in the Online Supplemental Appendix I twice to prove that $\delta - a \in [0, u^l)$ and $\delta - b + u^l \in [0, u^l)$, respectively.

Supposing the suggested price range of LTCI is between 200 and 300 Chinese Yuan, we need to verify whether the selling price δ is within this range (200, 300). First, we construct a range $(0, u^l)$ that contains the given range (200, 300) with the minimal values of u and l. Hence, the value of u and l are 7 and 3, respectively. Thus, the selling price δ can only be proven to be within the given range (200, 300) by meeting the following conditions: $0 \leq \delta$ −200 <343 (namely, $0 \leq \delta - a < u^l$) and $0 \leq \delta$+43 <343 (namely, $0 \leq \delta - b + u^l < u^l$).

As previously stated, two parties are involved in the LTCI context: the leading insurance company (verifier) and a distributing insurance company (prover). The leading insurance company, as the local regulator, should verify whether the distributing insurance company is selling LTCI within the price range without requiring the distributing insurance company to reveal the true selling price. Suppose the price range is from a to b, where $0 < a < b$. The proof can be conducted and completed by applying the algorithmic procedures presented in Table A1 in the Online Supplemental Appendix I. After executing the algorithms, the leading insurance company can obtain a Boolean value (true or false) as a return. The "True" value means that the distributing insurance company sold the LTCI product within the specified price range.

Scalable Implementation: A Scenario-Based Illustration

It is noted that we have not intended to replace existing systems that have been already used in different stakeholders. As depicted in § *Challenges in the Chinese LTCI*, a new universal layer (i.e., the InsurModel blockchain) is built on top of these systems to attain functional scalability. Thus, we construct a middle layer to attain communication between existing systems and the InsurModel blockchain (referred to as the *InsurModel-Layer*), which consists of two components. The first component is used to communicate with its local database(s) through API calls. The second component is designed to 1) convert existing data (either fetched from a local database or newly inputted data) to an encrypted string and write it onto the InsurModel blockchain, 2) execute a smart contract to transform business interdependence to a Merkle tree and store it in the InsurModel FileTree, 3) query the encrypted string stored in the InsurModel blockchain, and 4) conduct the price range proof when necessary. To attain connectivity scalability, we package InsurModel as a software development kit (SDK) and enable all involved LTCI stakeholders to install this kit in their local environments. An overview of the InsurModel architecture, including business relationship and dataflow, is illustrated with an exemplar scenario in Figure 4 to demonstrate how InsurModel works.

In this exemplar scenario, we only include four prominent stakeholders in LTCI: a person applying for LTCI (denoted as *applicant)*, a nursing home (denoted as *NHO*), an LTCI distributing insurance company (denoted as *DIO*), and an LTCI leading insurance company (denoted as *LIO*). In this scenario, a person submits his/her document package to a DIO to purchase an LTCI product. Figure 4 shows that the entire process comprises 16 main steps. Each step is elaborated in Table A2 in the Online Supplemental Appendix I.

Although the exemplar scenario only has four stakeholders, the proposed InsurModel is scalable from functional and connectivity perspectives. As previously stated, any organization can install InsurModel locally and set up a connection with the InsurModel blockchain using the InsurModel SDK. The querying task is implemented through a Merkle tree, which significantly improves querying and authentication efficiency. The performance of this task is systematically evaluated and presented in the next section.

System Evaluation

The proposed InsurModel is evaluated in two steps. First, a series of computational experiments were conducted to prove the technological advancement of InsurModel.

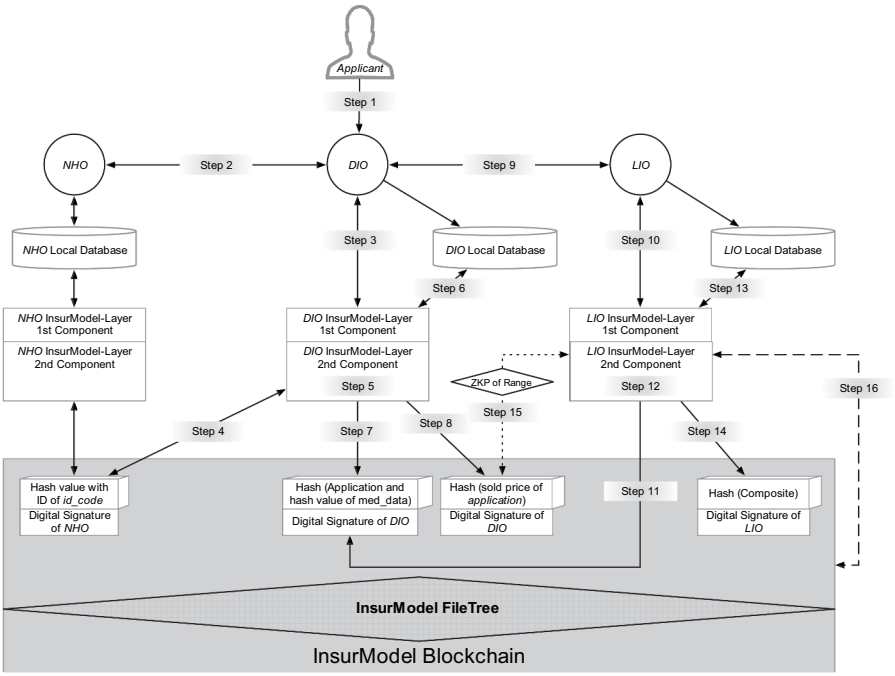


Figure 4. Scalable implementation of InsurModel.

Specifically, we assess 1) the extent to which the transaction cost can be reduced by manifesting business interdependence in the blockchain and 2) the viability of the ZKP of range. Second, we conducted the applicability check by using the focus group method and in-depth interviews, empirically demonstrating the practical and strategic implications of our proposed InsurModel.

Performance Evaluation through Computational Experiments

In our first computational experiment, we designed a scenario-based task and recorded the time spent on task completion across three different technical models—that is, the Traditional Database Model (existing model), Bitcoin-like Blockchain Model (traditional blockchain model), and InsurModel (our purposed model), over various numbers of business nodes (manifesting connectivity scalability). The experiment scenario is related to a data tampering case involving LTCI. Figure 5 depicts a simplified business process that involves *N* parties as nodes in the flowchart. Each node represents a stakeholder (e.g., a nursing home, a hospital, a distributing agent insurance company, or a leading insurance company) in the LTCI setting. The overall process starts with a file submission by Node 1, which sends a transaction file to the next node(s) for further processing. After a series of steps, the transaction file is eventually received by its intended receiver (i.e., Node N). Any intermediate node can tamper with or revise this transaction file and send the tampered file to the subsequent node due to the long trajectory of the entire process. For example, a nursing home files an insurance reimbursement claim with a face value of 1,500 Chinese Yuan and sends this

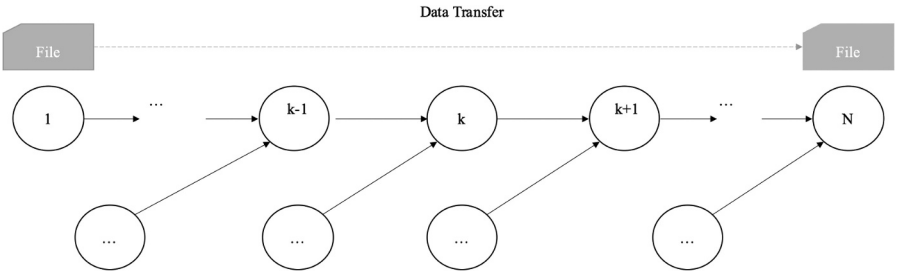


Figure 5. Illustration of experimental scenario.

file to the distributing insurance company of the insured. The distributing insurance company tampers with the file to change the face value to 15,000 Chinese Yuan. Ultimately, the distributing insurance company defrauds 13,500 Chinese Yuan from this reimbursement. Given that multiple parties could have processed the tampered file before it reaches its final receiver, efficiently and accurately identifying a fraud can reduce the transaction cost. This fraud scenario is simulated with different numbers of intermediate nodes across three types of models, the settings and results of which are presented as follows.

This task aims to identify the source of tampering and fraud. This experiment has two players: a fraudster and a detective. The task of the fraud is to select a business node randomly, tamper with the file at this node, and send the tampered file to the subsequent node(s). The detective aims to identify the source of the first tampering activity. The general procedures used by the detective to identify the tampering vary across the three models due to the difference in their designs, as depicted in Figures 1a-c.

We conducted the evaluation experiment for the Traditional Database Model in a local network to avoid any network delay. Meanwhile, we set up the Bitcoin-like Blockchain Model and InsurModel in the Hyperledger Fabric, which is an enterprise-grade permissioned blockchain infrastructure [2, 7, 41]. Table A3 in the Online Supplemental Appendix I lists the hardware information of our experimental server.

The experiment condition is the number of deployed business nodes in the network, which ranges from 5 to 110. Such a range was selected after consulting a senior manager of our research partner (i.e., Tai-Chi Insurance). Each node represents an organization that connects to the blockchain for LTCI. The upper limit, which is 110 nodes, was suggested as the scenario for megacities, such as Beijing or Shanghai. Assume that each business node processes the same amounts of files with the same size (i.e., 1 kilobyte, KB). The tests were run for 10,000 rounds for each model with a particular number of nodes. The multiple rounds can avoid hardware-specific bias (e.g., increasing temperature in the CPU or network delay).

In practice, completing the tasks involves two steps, namely fetching the relevant data and comparing their consistency. In the Traditional Database Model, each node has its own database. As previously indicated, communication between databases depends on the API calls. Data transmission for any intermediate node has two mandatory steps: 1) saving the data in the local database and 2) sending the copy to the next node. To identify the source of fraud, the detective must collect the copies of all the circulated files and compare their

differences between each consecutive pair. In the traditional Bitcoin-like Blockchain Model, relationships among different nodes are unavailable. Thus, the data points stored in a blockchain are independent of one another. The nodes encrypt their data with the respective hash values and deposit such hash values into the blockchain. Furthermore, in the Bitcoin-like Blockchain Model, business interdependence among different nodes is predetermined in a smart contract, in which the identity of each node (e.g., a digital signature) is stored in the same order as the business process. The detective applies the same strategy used in the Traditional Database Model to identify the source of fraud. The only difference between the two models is that the detective compares any difference in hash values instead of the original files between each consecutive pair. As depicted in § *Business Interdependence*, a tree-like structure is constructed in InsurModel to store business interdependence. The value of the root hash changes (Root A, B, or C in Figure 2b) as soon as tampering occurs in the data. The detective can promptly identify the source of the fraud by 1) determining whether the hash value at each "leaf" is consistent with its self-computed hash value and 2) finding the first inconsistent source. In these experimental tasks, data fetching consumes time as well as network traffic, whereas verification only consumes time. Accordingly, we recorded 1) the time spent on data fetching and verification and 2) the traffic volume consumed in data fetching for each round of task completion. Table 1 presents the mean value and standard deviation of every 10,000 rounds with the same number of business nodes and then illustrates the respective trend.

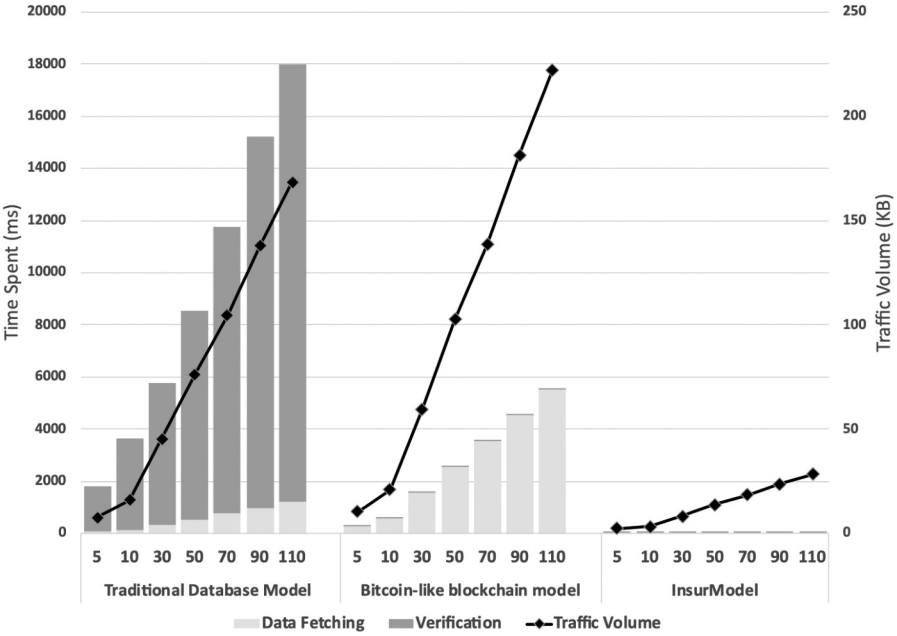
Table 1 shows that InsurModel fetches data considerably faster than the Traditional Database and the Bitcoin-like Blockchain Models. Such outperformance exponentially amplifies with the increase in the number of business nodes (i.e., from 5 to 110). Regarding network traffic volume, InsurModel also consumes substantially less than the two other models in terms of data fetching. Such results provide strong evidence that InsurModel can significantly reduce the transaction cost. Notably, the Bitcoin-like Blockchain Model consumes more time and network traffic than those of the Traditional Database Model because the blockchain usually consumes more resources than the SQL database in data fetching. In our case, every fetch in either the Bitcoin-like Blockchain Model or InsurModel takes around 50 ms and consumes 2-3 KB traffic volume. Such activities in the SQL database only need 10 ms and 1.5 KB of traffic volume on average.

The difference in task completion time across the three models is due to the varying extent of search complexity [25]. As discussed earlier, the Traditional Database and the Bitcoin-like Blockchain Models use a linear search algorithm (i.e., consistency comparison between each two consecutive business nodes). The search complexity function can be expressed as O(N), where N is the total number of business nodes. However, the data structure in InsurModel can be analogically viewed as a binary tree, wherein search complexity can be expressed as O(logN). Thus, InsurModel should be faster than the traditional blockchain model. In short, the Traditional Database Model or the Bitcoin-like Blockchain Model needs to continue fetching and verifying data along with the number of accessed business nodes. However, InsurModel can fetch all the required data (i.e., a series of hash values) through a single visit.

In addition, the verification time in the blockchain-enabled model, either the Bitcoin-like Blockchain Model or InsurModel, is considerably lower than that in the Traditional Database Model. The primary reason is that the verification in the Traditional Database Model is by comparing the original files, whereas the blockchain-enabled models verify data

Table 1. Performance on experimental task completion.

# of Business Nodes	Traditional Database Model			Bitcoin-like Blockchain Model			InsurModel		
	Data Fetching		Verification	Data Fetching		Verification	Data Fetching		Verification
	Time (ms)	Traffic Volume (kb)	Time (ms)	Time (ms)	Traffic Volume (kb)	Time (ms)	Time (ms)	Traffic Volume (kb)	Time (ms)
5	56.02 (1.89)	7.50 (0.25)	1764.01 (58.51)	288.97 (9.59)	10.50 (0.35)	0.29 (0.01)	49.982 (1.67)	2.40 (0.08)	0.28 (0.01)
10	108.96 (3.64)	16.00 (0.53)	3520.11 (116.88)	552.93 (18.66)	21.00 (0.70)	0.32 (0.01)	50.00 (1.67)	3.20 (0.11)	0.3 (0.01)
30	332.01 (11.08)	45.50 (1.51)	5450.47 (180.25)	1548.04 (51.90)	59.50 (2.01)	0.39 (0.01)	50.99 (1.71)	8.30 (0.28)	0.33 (0.01)
50	548.94 (18.31)	76.20 (2.54)	7991.08 (266.32)	2546.47 (84.92)	102.70 (3.39)	0.46 (0.02)	50.99 (1.70)	13.70 (0.46)	0.35 (0.01)
70	769.83 (25.55)	104.30 (3.49)	10975.65 (363.18)	3549.77 (119.99)	138.40 (4.63)	0.52 (0.02)	51.99 (1.72)	18.40 (0.61)	0.37 (0.01)
90	990.61 (33.30)	137.80 (4.54)	14222.85 (480.54)	4547.14 (152.16)	181.3 (6.04)	0.58 (0.02)	52.01 (1.73)	23.60 (0.80)	0.39 (0.01)
110	1209.30 (40.32)	168.40 (5.49)	16758.44 (553.75)	5546.25 (185.13)	222.1 (7.45)	0.64 (0.02)	52.02 (1.71)	28.50 (0.97)	0.40 (0.01)



consistency using hash values. As a result, the latter consumes minimal computational resources. Despite a marginal difference, InsurModel theoretically verifies the files faster than the Bitcoin-like Blockchain Model when the number of deployed business nodes increases. To statistically test whether InsurModel is more efficient than its counterparts, we conducted a series of *t*-tests to compare the means of the two groups across different number of nodes. The statistical tests confirm the observation in Table 1. Overall, InsurModel is significantly more efficient than either the Bitcoin-like Blockchain Model

or the Traditional Database Model in identifying the tampering source in our experiment, thereby increasing the efficiency in traceability.

In the second experiment, we assessed the viability of the ZKP of range in the LTCI context. As discussed in § *Price Range Proof*, the leading insurance company can apply the algorithms presented in Table A1 in the Online Supplemental Appendix I to verify whether a distributing insurance company prices the LTCI product within a specified price range without requiring the distributing insurance company to disclose the selling price. In response, we simulated 5,000 random numbers as the hypothetical selling prices and applied the ZKP of range to verify whether each simulated value is within a hypothetical price range (i.e., from 200 to 300 Chinese Yuan). Each round of ZKP of range encompasses the following three steps: initialization, proof, and verification. We recorded the time spent on each step across 5,000 rounds of verification. Figure 6 (stacked area chart) plots the relationship between the accumulated time spent on each step and the number of verification rounds. The linear relationship suggests that the execution of price range proof programs does not slow down with the increasing number of tasks. This result also manifests the robust scalability of our proposed method.

Applicability Check

In addition to technological advantages, it is crucial to examine whether our proposed InsurModel affords importance, accessibility, and suitability for practitioners [16, 38]. We then conducted an applicability check to address the practical and strategic implications. The applicability check is also conducive to avoid Type III errors [36] by verifying the meaningfulness of our research.

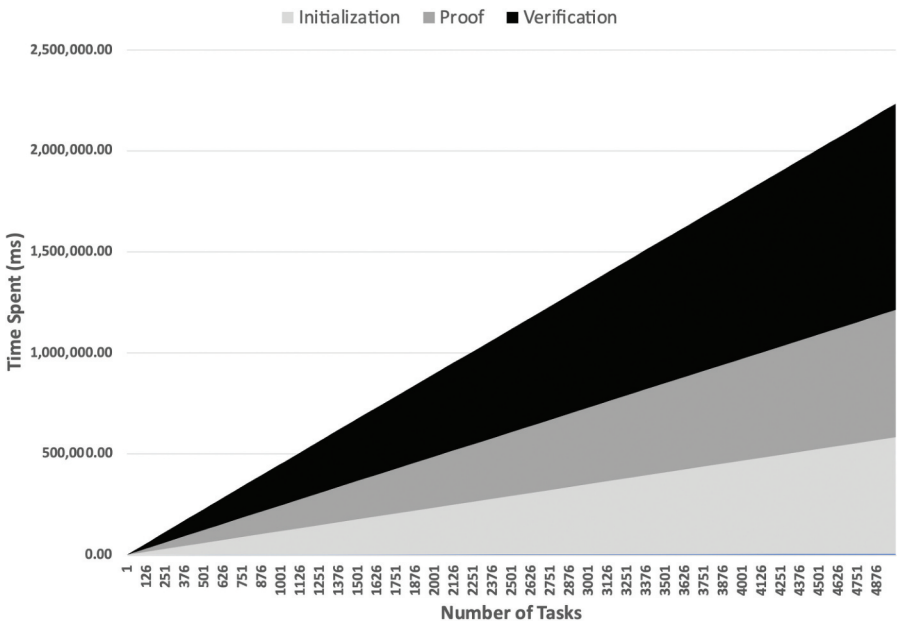


Figure 6. Performance of price range proof.

Our applicability check includes focus group discussion and in-depth interviews. All participants are employees of Tai-Chi Insurance, including insurance sales representatives, a DSM, an ITM, and a VP. The focus group comprises three insurance sales representatives, who will be involved in the LTCI business and directly interact with insurance systems equipped with InsurModel. Thus, this group can contribute insights from the perspectives of users. We also carried out in-depth interviews with employees holding management positions (i.e., the DSM, ITM, and VP at Tai-Chi Insurance), who are all deeply involved in the LTCI business. Given that our proposed InsurModel has been approved by Tai-Chi Insurance, the managers can provide additional insights into the role of InsurModel in future business and strategic planning at Tai-Chi Insurance. Detailed procedures and exemplar quotes are presented in the Online Supplemental Appendix II due to the page limitation.

The focus group discussion revealed the importance and necessity of a universal system across different stakeholders; such a system can contribute to streamlining daily routines for insurance sales representatives. In addition, the representatives expressed a strongly positive attitude to the traceability feature in blockchain and InsurModel. Because insurance claims involve a number of procedures and each procedure generates several files, it is very time-consuming to validate each of these files. When there is any misalignment or inconsistency across the files, the representatives need to spend even more time identifying the misalignment. The traceability function can help the representatives promptly identify the problematic file(s) and source(s) of liability.

A DSM, ITM, and VP at the Tai-Chi Insurance Group were interviewed independently to understand the strategic implications of our proposed InsurModel. The DSM and ITM stated the implications from a technical perspective, but the VP provided insights into the landscape of organizational strategy. First, the DSM and ITM placed considerable interests in reducing opportunistic behaviors and transaction costs from the anti-fraud auditing. The DSM and ITM also recognized that the blockchain can already contribute to such reduction through immutability and traceability. However, InsurModel, which manifests business interdependence, can further strengthen traceability, thus receiving high praise. The DSM and ITM further emphasized the importance of our ZKP in contributing to the cooperation among different stakeholders in terms of data exchange. Nonetheless, such a practice can only be adopted under the assurance of data security. In this regard, a cryptographical solution should be added to the existing blockchain technology. The ZKP for price range validation is regarded as a good attempt at this moment.

Second, the VP stated that digitalization is a long-term business strategy of the company. The adoption of blockchain for all insurance products will create a competitive advantage for Tai-Chi Insurance over its competitors because the use of blockchain can significantly improve the efficiency and traceability. Compared with LTCI, some other insurance products at Tai-Chi Insurance involve substantially more contracting stakeholders and more complicated business processes. Therefore, the InsurModel initiative for LTCI is treated as a pilot test. The promising results in the scalability of InsurModel will facilitate its future implementation in other insurance products.

Last but not least, the VP commented on our proposed InsurModel from the perspective of organizational strategy. The extent to which LTCI will be successful depends on the willingness of other distributing insurance companies to cooperate with Tai-Chi Insurance (i.e., the leading insurance company). The competition between Tai-Chi Insurance and

other distributing insurance companies is highly intense because they are competitors for a similar customer pool. Because of this intense competition, it is likely that the other distributing insurance companies are reluctant to share their data with Tai-Chi Insurance. However, due to its business privacy protection, InsurModel facilitates such cooperation.

Overall, InsurModel is believed to be an important and useful add-on to complement the existing blockchain technology. In particular, opportunism is constrained, thereby reducing the transaction costs in terms of the improved traceability feature. Moreover, since there is no change to the front-end interface, both Tai-Chi and other stakeholders can rapidly deploy InsurModel into their existing systems. That is, InsurModel affords high accessibility for potential adopters. Finally, InsurModel, as a blockchain-based solution, aligns with the general strategy of Tai-Chi Insurance Group, affording the suitability. Collectively, the applicability check confirms the relevance of our proposed InsurModel. More specifically, InsurModel not only increases productivity and efficiency by streamlining the transaction processes but also paves the way for future implementation of the blockchain strategy for Tai-Chi Insurance.

Concluding Remarks

In this study, we designed, developed, and evaluated a blockchain-based technical model, InsurModel, for a new LTCI initiative in China. Our study affords three primary contributions. First, following the design science paradigm by Gregor and Hevner [20], we deploy transaction cost economics (TCE) as a kernel theory to inform IT artifact construction and its strategic implications. Despite its prevalence in the IS literature, TCE has been rarely applied in design science research. Previous literature has argued the pivotal role of blockchain in mitigating transaction costs [1, 40], but there has been scant research that demonstrated this effect in a specific business setting. Thus, we attempt to fill this research gap by utilizing TCE in innovative blockchain design and application in the insurance industry. More specifically, blockchain, as a decentralized and immutable database, enables efficient and transparent transactions, which constitute a transactional environment with enhanced institutional trust [39]. The TCE literature shows that the establishment of trust among contracting parties constrains the respective opportunism, thereby reducing transaction costs and increasing economic efficiency. Therefore, the extant literature has theorized that blockchain technology is an effective governance proposition to complement TCE [39, 40]. However, although it is clear that blockchain contributes to constraining opportunism and reducing the overall transaction costs, how to reduce the ex-post transaction cost further has not been clearly demonstrated in the literature. In response, InsurModel is designed with two primary features, that is, representation of business interdependence in blockchain and utilization of the ZKP protocol to reduce the ex-post transaction cost for the LTCI initiative. Our computational experiments reveal that the representation of business interdependence can significantly strengthen traceability, thereby reducing the cost of auditing. In theory, the proposed design can significantly reduce the cost of auditing by saving considerable human resources and increasing the auditing accuracy. As stated by the data security manager (DSM), "We have to allocate a lot of human resources in auditing for anti-fraud procedures (at present) . . . If the blockchain (with your design) can extend to all of our (insurance) business (in Tai-Chi Group), the current large team can be downsized to a much smaller one (in terms of headcounts)." In addition, the deployment of ZKP into

blockchain contributes to reducing the ex-post transaction cost by mitigating the dilemma of business privacy and authentication integrity. Such a cryptographic method can help verify and authenticate the encrypted data without disclosing the real value. In the LTCI context, the leading insurance company can apply the ZKP protocol to attain a specific business goal, such as the proof of price range without disclosing the real selling prices of distributing insurance companies. Meanwhile, the business privacy (e.g., the real selling prices) of the distributing insurance companies is also protected to avoid opportunistic use by the leading insurance company. As indicated by the IT manager (ITM) at Tai-Chi Insurance, "We (Tai-Chi and other insurance companies) are competitors. The mutual trust is not very high among us. But we still need to cooperate to comply with the regulations from China Insurance Regulatory Commission . . . The ZKP for validating the price range in LTCI is a good start . . . " Collectively, our research findings expand the literature that blockchain technology accounts for the reduction in transaction costs because this technology establishes a trusted transaction environment. Moreover, we apply TCE as a kernel theory in design science research. Our proposed InsurModel can further reduce the ex-post transaction cost by facilitating traceability and authenticating the required information without disclosure.

Second, the proposed InsurModel achieves necessary scalability in terms of scalable implementation and the number of connected business nodes. The scalable implementation can increase the accessibility of InsurModel to a large number of users without disrupting their routine operations. Users are reluctant to switch to a new technology or system if they perceive significant differences between the extant and the new one. Thus, InsurModel is packaged as an SDK that can be set up by the stakeholders in their back ends only, thus alleviating the individual reluctance to use the new information system or infrastructure. As stated by the ITM at Tai-Chi Insurance, "I used to be reluctant to implement a new system or application because of the uncertainty. You never know whether people are willing to use it or not. Therefore, we prefer to keep the front end (interface) but make radical change at the back end (infrastructure or design)." More importantly, our computational experiments suggest that the performance of InsurModel does not deteriorate rapidly with the increasing number of connected business nodes and workload, which is far better than the performance of the Traditional Database and Bitcoin-like Blockchain Models. In other words, the proposed design assures the efficiency of the authentication and verification despite the presence of additional connected devices or infrastructures. This finding provides an important strategic implication for organizations that plan to implement blockchain technology to a large landscape of the market, including Tai-Chi Insurance. For example, Tai-Chi Insurance is planning to implement InsurModel in a third-tier city with around 5,000 insured and many organizational stakeholders. Our experimental results on scalability suggest that InsurModel can also run efficiently in first-tier cities, such as Beijing or Shanghai. As commented by the VP, " . . . The scalability (in blockchain application) is what we really want to examine, because other insurance products may involve more entities if we apply the blockchain to all other business in the future." Overall, the proposed scalable design affords accessibility to a large number of concurrent users or business nodes but does not sacrifice the effectiveness of functionality, thereby establishing an exemplar model for the future design of blockchain applications.

Third, our proposed InsurModel provides significant implications for organizations promoting a data-sharing strategy. Data are the new fuel in the digital economy.

However, many companies keep their data as closed silos, which hinder the process of gleaning data and developing deep and actionable insights from the data. Therefore, recent literature has encouraged organizations to share data and facilitate cooperation [26, 33]. Although some organizations have attempted to enable the authenticated API requests for data sharing, such an API-based sharing mechanism has its drawbacks in data security because the unauthorized third party can intercept the data in transit [42]. In addition, it is difficult to prevent the secondary usage of data retrieved from the API requests [21]. Accordingly, many organizations are still reluctant to share their data with others in the present API-based sharing mechanism. The emergence of blockchain technology has shed light upon data sharing due to its transparent governance structure and advanced encryption. However, the encrypted data carry the challenge of utilizing the shared data. Therefore, it is necessary for organizations to master a new method to utilize the shared data in an encrypted format, thereby eliminating/mitigating the cost from data transactions. In our proposed InsurModel, the ZKP is integrated into the blockchain to prove the price range without disclosing the real selling prices of distributing instance companies. The implication can yet inspire future research from different disciplines despite the technical solution. For instance, future research can extend prior literature to explore the data-sharing strategy supported by blockchain-related technology [18, 52]. Moreover, future research can also integrate more advanced cryptographical technology, such as ZKP of membership, homomorphic encryption, and neural cryptography, with blockchain, thereby exploring additional means of data cooperation. As the VP stated in the interview, "We (Tai-Chi) want to become a leader (in insurance industry) to leverage the blockchain technology to facilitate more data exchange in the future."

Although InsurModel was designed for the LTCI context, its ideas (i.e., representation of business interdependence and ZKP) can be generalized to not only other insurance products but also other industrial sectors. Future studies are urged to explore additional application scenarios to expand the generalizability of our proposed design. For example, the logistics industry has a high demand for traceability, namely registering and identifying a goods from its origin (production site) to its final destination [35]. Thus, our proposed design (i.e., representing business interdependence in blockchain) can be adopted and extended by the logistic industry to enhance traceability. In addition, blockchain technology can possibly transform health care operations. Our proposed design of the integration between blockchain and ZKP contributes to compromising the debate between privacy protection and data verification in health care. Take the example of a blockchain-based Covid-19 contract tracing app [24], in which the ZKP can allow users to check whether they were in close contact with a confirmed patient without disclosing his/her identity. Last, but not least, evidence from the applicability check supports the pivotal role of blockchain and the proposed InsurModel in improving individual productivity and efficiency. We urge future studies to collect additional evidences and statistically validate the effectiveness of blockchain function in the organizational context.

SSI

Notes

1. A complete contract refers to an agreement where the contracting parties can specify their respective rights and duties for every possible future state of the world. Particularly, the terms of the contract have no gaps.
2. The concept of Merkle tree is briefly introduced and illustrated in the Online Supplemental Appendix I.

Acknowledgements

We would like to thank Wei Zhu and Jinjun Tang for their technical support.

Funding

This work was partially supported by the National Natural Science Foundation of China (Grant Nos. 71801217, 71702133, 72072087, 72031001, and 71932002); Hong Kong ITF Fund (No. GHP/142/18GD); the Shenzhen Special Fund for Strategic Emerging Industries Development (Grant No.: JCYJ20170818100156260); and a University Development Fund in CUHKSZ.

ORCID

Wenping Zhang http://orcid.org/0000-0002-0183-4504
Chih-Ping Wei http://orcid.org/0000-0003-4150-3926
Qiqi Jiang http://orcid.org/0000-0002-1876-715X
Chih-Hung Peng http://orcid.org/0000-0002-7101-7999
J. Leon Zhao http://orcid.org/0000-0002-0624-0254

References

1. Ahluwalia, S.; Mahto, R. V.; and Guerrero, M. Blockchain technology and startup financing: A transaction cost economics perspective. *Technological Forecasting and Social Change*, *151* (2020), 119854.
2. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; Muralidharan, S.; Murthy, C.; Nguyen, B.; Sethi, M.; Singh, G.; Smith, K.; Sorniotti, A.; Stathakopoulou, C.; Vukolić, M.; Cocco, S. W.; and Yellick, J. Hyperledger fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference*. New York: Association for Computing Machinery, April 2018, pp. 1–15.
3. Bardhan, I.; Whitaker, J.; and Mithas, S. Information technology, production process outsourcing, and manufacturing plant performance. *Journal of Management Information Systems*, *23*, 2(2006),13–40.
4. Blum, M.; Feldman, P.; Oded Goldreich; and Micali, S. Non-interactive zero-knowledge and its applications. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*. New York: Association for Computing Machinery, 2019, pp. 329–349.
5. Bromiley, P.; and Harris, J. Trust, transaction cost economics, and mechanisms. *Handbook of Trust Research*, Northampton, MA, USA. Edward Elgar 2006, pp.124–143.
6. Busquets, J.; Rodon, J.; and Wareham, J. Adaptability in smart business networks: An exploratory case in the insurance industry. *Decision Support Systems*, *47*, 4(2009),287–296.

7. Cachin, C. Architecture of the hyperledger blockchain fabric. In *Proceedings of Workshop on Distributed Cryptocurrencies and Consensus Ledgers*. Chicago: Association for Computing Machinery, July 2016, Vol. 310, pp. 4.
8. Chanson, M.; Bogner, A.; Bilgeri, D.; Fleisch, E.; and Wortmann, F. Privacy-preserving data certification in the internet of things: Leveraging blockchain technology to protect sensor data. *Journal of the Association for Information Systems*, *20*, 9(2019), 10.
9. Chiles, T. H.; and McMackin, J. F. Integrating variable risk preferences, trust, and transaction cost economics. *Academy of Management Review*, *21*, 1(1996),73–99.
10. Cohn, A.; West, T.; and Parker, C. Smart after all: Blockchain, smart contracts, parametric insurance, and smart energy grids. *Georgetown Law Technology Review*,*1*,2,(2017),273–304.
11. Cong, L. W.; and He, Z. Blockchain disruption and smart contracts. *The Review of Financial Studies*, *32*, 5(2019),1754–1797.
12. Crosby, M.; Pattanayak, P.; Verma, S.; and Kalyanaraman, V. Blockchain technology: Beyond bitcoin. *Applied Innovation Review*, June, 5(2016), 6–19.
13. Dedrick, J.; Xu, S. X.; and Zhu, K. X. How does information technology shape supply-chain structure? Evidence on the number of suppliers. *Journal of Management Information Systems*, *25*, 2(2008),41–72.
14. Dibbern, J.; Winkler, J. K.; and Heinzl, A. Explaining variations in client extra costs between software projects offshored to India. *MIS Quarterly*, *32*, 2(2008),333–366.
15. Dong, S.; Xu, S. X.; and Zhu, K. X. Information technology in supply chains: The value of IT-enabled resources under competition. *Information Systems Research*, *20*, 1(2009),18–32.
16. Dong, W.; Liao, S.; and Zhang, Z. Leveraging financial social media data for corporate fraud detection. *Journal of Management Information Systems*, *35*, 2(2018),461–487.
17. Francesca, C.; Ana, L. N.; Jérôme, M.; and Frits, T. *OECD Health Policy Studies Help Wanted? Providing and Paying for Long-term Care: Providing and Paying for Long-term Care*. OECD Publishing, Paris, 2011.
18. Galbreth, M. R.; March, S. T.; Scudder, G. D.; and Shor, M. A game-theoretic model of e-marketplace participation growth. *Journal of Management Information Systems*, *22*, 1 (2005),295–319.
19. Gostin, L. O. National health information privacy: Regulations under the health insurance portability and accountability Act. *Journal of the American Medical Association*, *285*, 23 (2001),3015–3021.
20. Gregor, S.; and Hevner, A. R. Positioning and presenting design science research for maximum impact. *MIS Quarterly*, *37*, 2(2013),337–355.
21. Hussain, F.; Hussain, R.; Noye, B.; and Sharieh, S. Enterprise API security and GDPR compliance: Design and implementation perspective. *IT Professional*, *22*, 5(2020),81–89.
22. Iansiti, M.; and Lakhani, K. The truth about blockchain. *Harvard Business Review*, January-February *95*, 1(2017),118–127.
23. Liang, X.; Zhao, J.; Shetty, S.; Liu, J.; and Li, D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In *Proceedings of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*. Montreal: IEEE, 2017, pp. 1–5. https://doi.org/10.1109/PIMRC.2017.8292361
24. Liu, J. K.; Au, M. H.; Yuen, T. H.; Zuo, C.; Wang, J.; Sakzad, A.; Luo, X.; and Li, L. Privacy-preserving COVID-19 contact tracing app: A zero-knowledge proof approach. *IACR Cryptol. ePrint Arch.*, 2020, 528.
25. Mehlhorn, K. *Data Structures and Algorithms 1: Sorting and Searching (Vol. 1)*. Berlin: Springer Science & Business Media, 2013.
26. Mello, M. M.; Lieou, V.; and Goodman, S. N. Clinical trial participants' views of the risks and benefits of data sharing. *New England Journal of Medicine*, *378*, 23(2018),2202–2211.
27. Min, H. Blockchain technology for enhancing supply chain resilience. *Business Horizons*, *62*, 1 (2019),35–45.
28. Morais, E.; Koens, T.; Van Wijk, C.; and Koren, A. A survey on zero knowledge range proofs and applications. *SN Applied Sciences*, *1*, 8 (2019), 946.

29. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Manubot, 2019. Accessed on 2020.10.15
30. Nath, I. Data exchange platform to fight insurance fraud on blockchain. In *Proceedings of 2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)*. Barcelona: IEEE, December 2016, pp. 821–825.
31. Nofer, M.; Gomber, P.; Hinz, O.; and Schiereck, D. Blockchain. *Business & Information Systems Engineering*, *59*, 3(2017),183–187.
32. Norton, E. C. Long-term care*Handbook of Health Economics*, *1*(2000), 955–994.
33. Parra-Moyano, J.; Schmedders, K.; and Pentland, A. Shared data: Backbone of a new knowledge economy. In *Building the New Economy*. Retrieved from https://wip.mitpress.mit.edu/pub/yvy3qigg, April 30, 2020
34. Pedersen, T. P. Non-interactive and information-theoretic secure verifiable secret sharing. In *Proceedings of Annual International Cryptology Conference*. Berlin: Springer, 1992, pp. 129–140.
35. Pournader, M.; Shi, Y.; Seuring, S.; and Koh, S. L. Blockchain applications in supply chains, transport and logistics: A systematic review of the literature. *International Journal of Production Research*, *58*, 7(2020),2063–2081.
36. Rai, A. Editor's comments: Avoiding type III errors: Formulating IS research problems that matter. *MIS Quarterly*, *41*, 2(2017),iii–vii.
37. Rai, A.; Arikan, I.; Pye, J.; and Tiwana, A. Fit and misfit of plural sourcing strategies and it-enabled process integration capabilities: Consequences of firm performance in the U.S. electric utility industry. *MIS Quarterly*, *39*, 4(2015),865–886.
38. Rosemann, M.; and Vessey, I. Toward improving the relevance of information systems research to practice: The role of applicability checks, *MIS Quarterly*, *32*, 1(2008),1–22.
39. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; and Shen, L. Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*, 7 (2019),2117–2135.
40. Schmidt, C. G.; and Wagner, S. M. Blockchain and supply chain relations: A transaction cost theory perspective. *Journal of Purchasing and Supply Management*, *25*, 4(2019), 100552.
41. Sousa, J.; Bessani, A.; and Vukolic, M. A Byzantine Fault-tolerant ordering service for the hyperledger fabric blockchain platform. In *Proceedings of the 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. Luxembourg City: IEEE, June 2018, pp. 51–58.
42. Suzic, B. User-centered security management of API-based data integration Workflows. In *Proceedings of NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium*. Istanbul: IEEE, April 2016, pp. 1233–1238.
43. Tian, F. A supply chain traceability system for food safety based on HACCP, blockchain & internet of things. In *Proceedings of 2017 International Conference on Service Systems and Service Management*. Dalian: IEEE, June 2017, pp. 1–6.
44. Whitaker, J.; Mithas, S.; and Krishnan, M. S. Organizational learning and capabilities for onshore and offshore business process outsourcing. *Journal of Management Information Systems*, *27*, 3(2010),11–42.
45. Williamson, O. *Markets and Hierarchies: Analysis and Antitrust Implications*. New York: Free Press, 1975.
46. Williamson, O. *The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting*. New York: Free Press, 1985.
47. Williamson, O. The lens of contract: Private ordering. *American Economic Review*, *92*, 2 (2002),438–443.
48. Wonseok, O. H.; Gallivan, M. J.; and Kim, J. W. The market's perception of the transactional risks of information technology outsourcing announcements. *Journal of Management Information Systems*, *22*, 4(2006),271–303.
49. Yli-Huumo, J.; Ko, D., Choi, S.; Park, S.; and Smolander, K. Where is current research on blockchain technology?—A systematic review. *PLoS One*, *11*, 10(2016), e0163477. https://doi.org/10.1371/journal.pone.0163477

50. Zheng, X.; Sun, S.; Mukkamala, R. R.; Vatrapu, R.; and Ordieres-Meré, J. Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies. *Journal of Medical Internet Research*, *21*, 6(2019), e13583.
51. Zhou, L.; Wang, L.; and Sun, Y. Mistore: A blockchain-based medical insurance storage system. *Journal of Medical Systems*, *42*, 8(2018),1–17.
52. Zhu, K. Information transparency of business-to-business electronic markets: A game-theoretic analysis. *Management Science*, *50*, 5(2004),670–685.

About the Authors

Wenping Zhang is an assistant professor at the School of Information, Renmin University, China. He received his Ph.D. in information systems from City University of Hong Kong. Dr. Zhang's research interests include machine learning, deep learning, interpretable AI, and business analytics. His work has been published in *INFORMS Journal on Computing, Production and Operations Management, Decision Support Systems*, and other venues.

Chih-Ping Wei is a distinguished professor of Department of Information Management at National Taiwan University. He received his Ph.D. in Management Information Systems from the University of Arizona. Dr. Wei's research interests include data analytics and business intelligence, text mining and natural language understanding, patent analysis and mining, and health informatics. His papers have appeared in *Journal of Management Information Systems, European Journal of Information Systems, Decision Sciences, Decision Support Systems, Information & Management, IEEE Transactions on Engineering Management*, and many other journals.

Qiqi Jiang is an associate professor in the Department of Digitalization at Copenhagen Business School. He received his Ph.D. in Information Systems from City University of Hong Kong. Dr. Jiang's research interests include governance of open-source software development, digital economy, and gamification. His work has been published or forthcoming in *Journal of Management Information Systems, MIS Quarterly, Journal of the Association for Information Systems, Journal of Strategic Information Systems* and other journals.

Chih-Hung Peng is an assistant professor of Management Information Systems at National Chengchi University, Taiwan. He received his Ph.D. in Information Technology Management from the Georgia Institute of Technology. Dr. Peng's research interests include team decision-making, social media, e-commerce, and organizational innovation. His research work has appeared in *Information Systems Research, Journal of the Association for Information Systems, IEEE Transactions on Engineering Management*, and other venues.

J. Leon Zhao is a Presidential Chair Professor of Information Systems, School of Management and Economics, Chinese University of Hong Kong at Shenzhen. He holds a Ph.D. in Business Administration (Information Systems) from Haas School of Business, the University of California at Berkeley. Dr. Zhao's research focuses on blockchain, business intelligence, and FinTech.