Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.036658
Article

Check for updates

A Blockchain-Based Trust Model for Supporting Collaborative Healthcare Data Management

Jiwon Jeon, Junho Kim, Mincheol Shin and Mucheol Kim*

Department of Computer Science and Engineering, Chung-Ang University, Seoul, 06911, Korea
*Corresponding Author: Mucheol Kim. Email: mucheol.kim@gmail.com
Received: 08 October 2022; Accepted: 13 January 2023

Abstract: The development of information technology allows the collaborative business process to be run across multiple enterprises in a larger market environment. However, while collaborative business expands the realm of businesses, it also causes various hazards in collaborative Interaction, such as data falsification, inconstancy, and misuse. To solve these issues, a blockchain-based collaborative business modeling approach was proposed and analyzed. However, the existing studies lack the blockchain risk problem-solving specification, and there is no verification technique to examine the process. Consequently, it is difficult to confirm the appropriateness of the approach. Thus, here, we propose and build a blockchain-based trust model to strengthen and verify the integrity and security of the collaborative business process; Integrity and security address the validity of collaborative interactions in terms of a trust, and we construct a blockchain pattern based on trust elements to meet the required the characteristics. Specifically, a trust model can be applied to the healthcare data-sharing process, and then the achievement of the trust-based safe data-sharing process can be proven. Our model can be used as a trust-building guidance tool or for integrity and security verification with the collaborative business process in a distributed environment with blockchain.

Keywords: Blockchain; business process; trust model; healthcare data-sharing; data science

1 Introduction

The business process is performed according to a set of complex rules that aim to integrate and synchronize the operation, such as transaction and management system, and support the ultimate goals of the process [1,2]. In a collaboration of multiple organizations, it is important to achieve an organic connection and integrity [3]. A collaborative business process improves the workflow among the related organizations, and it is important to set up a task model as well as analyze the mutual operation pattern in the collaboration [4].

Knowledge and information sharing are essential for successful task performance, including innovation, decision-making, and responses, in a company [5,6]. Data-sharing systems can efficiently

use the information by providing accessibility to the available data [7,8]. Safe data sharing requires, as a priority, data integrity and the participants' compliance with the collaboration rules, especially the rules related to data use and data use authority [9]. Nevertheless, even in the collaborative process, in which mutual trust among the participants is critical, there are risks of data falsification and illegal use, such as violation of privacy or infringement of personal information [10].

"Trust" has several different definitions (for example, confidentiality [11] and traceability [12]), and it is an important predictor variable that determines the success or failure of attaining collaborative goals [13]. In contrast, lack of trust increases uncertainty in task performance, and consequently harms the business operation (for example, data inconsistency [14], or fraudulent act of an intermediary [15]) [16–18]. As a result, in some recent cases of collaborative business processes, collaboration rules, and control mechanisms are developed to solve the issue of lacking trust [19,20].

Blockchain [21] is a peer-to-peer (P2P) type of distributed ledger technology. It provides data decentralization and integrity, and thereby supports the execution of collaborative business processes [22]. Specifically, blockchain's distributed ledger realizes decentralization, and its hash block structure guarantees data integrity and security in a mutual collaborative operation [23]. Smart contracts are programs stored on a blockchain that run when predetermined conditions are met, and then automatically execute the next process. Smart contract technology facilitates work automation and accurate performance of preconditioned process sequences [24,25]. Thus, the use of blockchain for improving the collaboration environment in a business process is increasing. Distributed collaboration through blockchain [26] and automation study [27] are some typical examples.

Data sharing promotes the use of knowledge and information, and therefore, provides research opportunities and advances business execution [28]. In the healthcare sector, data sharing becomes more widespread to upgrade the system as we move into the super-aged society. While the health data-sharing system increases data accessibility and availability, it also exhibits some risks, such as violation of privacy [29,30] and data falsification [31]. Therefore, it is critical to ensure data integrity through data encapsulation, as a countermeasure to violation of privacy, and reinforcement of trust in collaborators or data users in the sharing process.

There are increasing attempts to employ collaborative business process and blockchain technology in the management of heterogeneous healthcare data to strengthen data integrity and security [32]. However, the existing studies are often focused on risk analysis and environmental improvement (i.e., solving integrity and security issues) [33,34]. In addition, intelligent communication technologies for providing network purposes [35,36] and services have been developed in response to the demand for process consistency and integrity. They have limitations in that they cannot guarantee trust and integrity against potential problems. Namely, it is difficult to verify the integrity and security appropriateness as they do not provide the sufficient specification of the trust reinforcement related to the risks in a mutual operation in the collaborative process. In contrast, blockchain enforces the integrity of consistency through the invariance and transparency of distributed books. Therefore, it is a technology suitable for the field of healthcare data sharing where demand for information processing and data encryption is active. Therefore, in this study, we specified the possible solutions to the risks in collaboration, especially the uncertainty of trust, and proposed a verification model by using blockchain from the perspective of trust.

This study was conducted to develop and demonstrate a blockchain pattern-based trust model to solve the uncertainty in the business process. Our contributions are as follows:

- To propose a blockchain pattern-based trust model for a collaborative business process.

- To strengthen data integrity and security by using the proposed blockchain pattern-based trust model.
- To verify the pattern-based trust model for a healthcare data management process under a distributed environment.

The paper is structured as follows: Section 2 explains the related works on the application of the blockchain-based business process; Section 3 elucidates the elements of trust and proposes a trust model methodology; Section 4 presents a healthcare data management process under distributed environments based on the trust model, and Section 5 indicates study outcomes and the direction of further studies in the future.

2 Related Work

Various studies have been conducted to identify and reflect the requirements of trust for improving the collaborative business process. Viriyasitavat et al. [37] examine a study on the relationship between workflow characteristics and trust attributes in the Business Process, and present requirements for achieving trust attributes such as integrity, security, and confidence in interactions. This requirement can be utilized to verify workflow trust properties. Gol Mohammadi et al. [38] reflect the trust requirements for Business Process Management and examine a BPM model that can improve the business process model.

Various investigations have also been conducted on the use of blockchain to improve the business process. Morkunas et al. [39] categorize the blockchain effects on a business model in eight directions. Integrates security and privacy as key factors that influence trust and action intentions, and proposes a blockchain user model. Mont et al. [40] investigate the pattern of blockchain-based application software system design. For this, the researchers have designed a business collaboration trust service on a hybrid architecture that combines centralized control and P2P components. Lu et al. [41] present a model-based method that designates a specific model for asset management and integration of business process and proposes a method to create a smart contract that automatically converts the established model of the business process to a smart contract programming language. Müller et al. [42] investigate the trust pattern of a blockchain corresponding to trust elements, but a more empirical study is still required.

Liu et al. [43] apply encryption to data transmission and examine blockchain-based healthcare data sharing and security systems. MedRec [44] establishes a distributed system for large-scale healthcare data management. MedBlock [45] has developed a platform in which patients can, by themselves, not only integrate, manage, and distribute their medical information, which is stored in different healthcare institutions but also decide the scope of information disclosure at their discretion.

3 Our Proposed Blockchain-Based Trust Model for the Collaborative Business Process

This paper proposes a blockchain pattern-based trust model, which strengthens data integrity and security in the collaborative business process. In this method, the trust elements are deduced from the risks in a business process and subsequently sorted as a pattern by using blockchain technology. A normalized pattern based-trust model is used to design the collaborative business process models and verify their trust levels. The proposed model enables to build reliable collaborative business processes by suppressing the potential risks of collaborative business processes.

Fig. 1 displays the composition of a trust model proposed in this study. The model is comprised of the risks of the collaborative business process, trust concern, and uncertainty, which are identified

as trust elements, as well as the blockchain technology corresponding to such elements. A blockchain-based trust pattern is deduced that can respond to the elements of influence for preventing the manifestation of risks in the mutual operation of the collaborative business process.

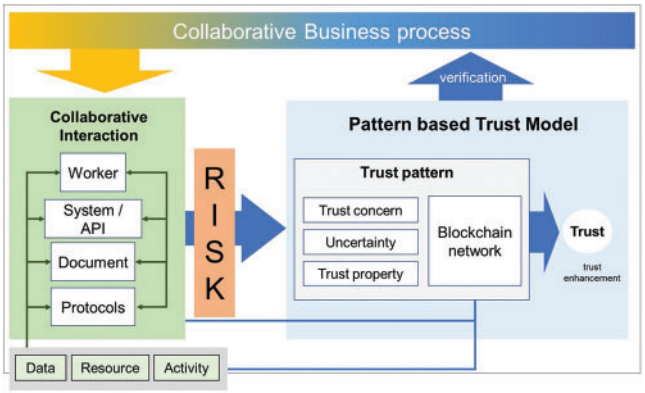

Figure 1: Blockchain pattern-based trust model

3.1 Concept of Trust in the Collaborative Business Process

In this study, we approached the collaborative business process from the perspective of trust to improve the process to achieve the targeted goals more accurately. Further, we define the concept of trust in a collaborative scheme for trust-building and identify the elements of trust that affect the process.

3.1.1 Definitions of Trust in the Collaborative Business Process

Previous approaches have addressed potential risks (data falsification, validity of requirements) that occur in the collaborative process by ensuring the integrity of the workflow. Accordingly, we propose a blockchain based trust model which supports a robust collaborative process from integrity and security issues. Trust is approached as workflow integrity for collaboration [46]. Integrity is judged by assessing whether the workflow progress and related resources match the process design. In the collaborative business process, integrity is required in five collaborative interactions (Table 1). These are categorized by some key factors, such as the main users who interact with one another in the collaborative process, more specifically, the interactive operation between the collaborators as well as between the collaborators and the information system, and tasks, such as documentation, business protocol, and updates [47].

Definition 1. Trust is the integrity of a workflow for collaboration

Table 1: Interactive operation in the collaborative business process

	Collaborative interaction	Description
Main users	Interaction between the collaborators	Communication such as question and answer, between the participants in the course of the collaborators' task performance

(Continued)

Table 1: Continued

	Collaborative interaction	Description
	Interaction between the collaborators and the information system	Data sharing between the information system used by the collaborators
Task	Documentation	Documentation through data input by collaborators and management of shared documents
	Business protocol	Adequate procedure and activities to attain the collaboration goals
	Updates	Updates for addition or changes of information during the collaboration work

In addition, in this study, we categorized the requirements of integrity in the interaction according to six attributes, namely, integrity, transparency, traceability, availability, validity, and fault tolerance. In detail, first, the shared data and resources should be the same or consistent between all the collaborators. Second, the interaction between the collaborators and the shared resources should be transparent [48]. Third, an immutable audit log, which traces the responsible source of illegal data reproduction and workflow-related issues, should be guaranteed. Fourth, any collaborators should be able to access the shared information [49]. Fifth, the collaboration should be carried out by a certain business process protocol [50]. Finally, updates should be continuously made, even in the case of risks, while maintaining the availability and integrity of the resources. The attributes presented in this study are applied to verify the trust model (Trust property in Subsection 3.1.2) in the collaborative business process model.

3.1.2 Summary of the Concept of Trust Elements

In this section, we organize both the threat and enhancing trust elements and analyze them to establish the integrity of the collaborative business process. (Table 2) Fig. 2 shows the relationship between the threats and enhancing elements of the collaborative business process. Here, threats imply a concrete factor that threatens the integrity of the collaboration in the business process, and they are categorized into Trust Concern, Trust Issue, and Risk, based on Gol Mohammadi et al. [38]. In detail, the definition of Trust Issue for this study is an abstract concern about the possibility of Risk occurrence, and Trust Concern is a concrete medium of Risk occurrence. Risk implies that a Trust Issue can become an actual danger. Among these, Risk should be resolved to prevent its actual occurrence or manifestation. Trust Property is an enhancing element that directly affects trust-building by imposing a compulsory nature on the characteristics of integrity.

Table 2: Theorem of the elements of trust and description

Element of trust	Theorem	Description
Trust	Be certain	Guarantee of integrity in collaborative workflow

(Continued)

Table 2: Continued

Element of trust	Theorem	Description
Uncertainty	Unable to be certain	Uncertainty in the collaboration of business process
Trust Issue	Abstract concern (Psychological concerns)	Concern about the occurrence of risk threats in the collaboration of business process
Trust concern	Medium of risk occurrence	Medium of trust issues, such as resources management and flow, activity, and data
Risk	Risks arising from uncertainty	Major hazard elements that threaten the integrity of collaboration, such as violation of privacy and data falsification
Trust property	Trust attribute that creates a positive effect on trust building against risk (subsection 3.1.1)	Elements that create positive impacts on trust building, against risk, such as integrity, transparency, traceability, availability, validity, and fault tolerance
Trust enhancing	Enhancement of trust	Trust building through trust enhancement. For trust enhancement, uncertainty should be resolved and the conditions of trust property should be satisfied.

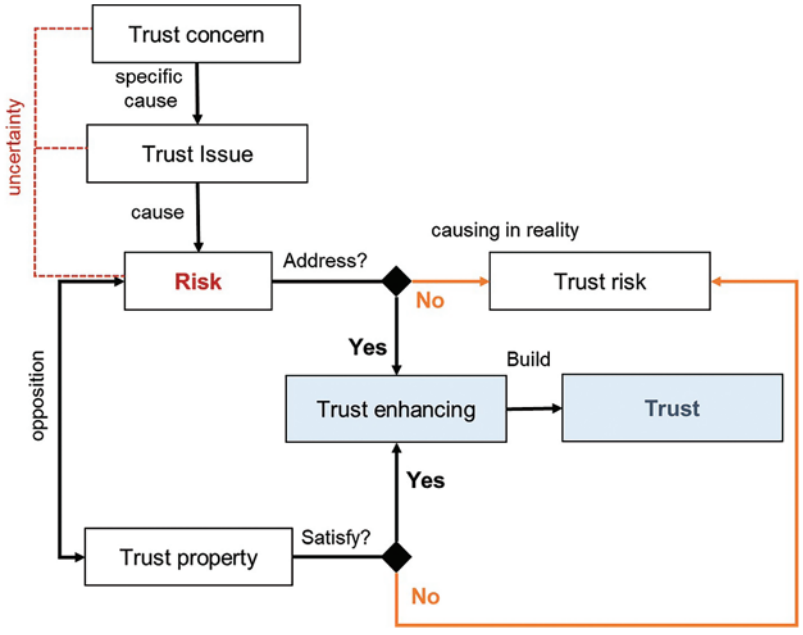

Figure 2: Relation between trust threat and trust enhancing elements, and enhancement of trust

3.1.3 Identification of Trust Elements in the Collaborative Business Process

The next step after categorizing the risks that may occur in a collaborative business process is to identify the elements that affect the risks. Our analysis is limited to only the risks that threaten the achievement of collaboration goals. Risks are categorized according to the cases of "Business Process Risk Classification [17]," and normalized by analyzing the trust elements from the location where the risk occurs, as shown in Table 3.

Table 3: Elements of trust deduced from the risks of the collaborative business process

Risk	Element of trust	Content	Trust property
Data risk	Trust concern	Ethics of the participants, and resources	Integrity, transparency
	Risk	Falsification and modulation	
	Uncertainty	Falsification and modulation of the resources	
Organizational data risk	Trust concern	Ethics of the central organization, and records	Integrity, transparency
	Risk	Falsification and modulation	
	Uncertainty	Falsification and modulation of the records	
Goal risk	Trust concern	Workflow	Validity
	Risk	Failure to meet the conditions	
	Uncertainty	Workflow invalidity	
Structural risk	Trust concern	Events	Continuity, sustainability
	Risk	Uncertain sequence, and invalidity of workflow	
	Uncertainty	Unable to guarantee the sequence	
Technology risk	Trust concern	Collaborative network	Fault tolerance, integrity, availability

Data risk burdens the process execution by damaging the data integrity. It arises from the ethical behaviors of the collaborators and the resource data as a medium. Because unreliable collaborators, inside or outside the collaboration scheme, may falsify or alter the data with malicious intent during the data input stage depending on their ethics, there is uncertainty about data falsification. Moreover, data falsification or modulation may take place in the course of data transmission due to an outside attack. Therefore, to eliminate uncertainty, the integrity of resources should be guaranteed. In addition, transparency, which allows us to tracing of the detailed trail of the collaborator's performance, is required to force the integrity of the collaborators. This point is elucidated in more detail in the following description of organizational data risk.

Organizational data risk causes a threat to the performance of the collaboration and affects the outcome of the collaboration workflow. More specifically, there are risks of falsification or modulation, or loss of workflow records, such as transaction records, by central managers. In other words, records' integrity is vulnerable as the records are usually subject to improper management by central managers. Therefore, it is imperative to assure a proper management structure that can monitor and administer the business records transparently.

Goal risk affects the achievement of collaboration goals or workflow. Where there is a goal risk, task performance outcomes do not match the collaboration goals, while the collaborative workflow is used as a medium. This is because the un-normalized tasks cause confusion in the workflow due to the discrepancies in the collaborators' understanding and views, and thus make it difficult for the collaborators to be certain about the performance of the business process subject to the set conditions. Therefore, to ensure the validity of the workflow, normalization, and verification of the validity of such normalization is essential.

Structural risk affects the validity of the process design. Uncertainty of the sequences in the process events harms the process itself, implying that the workflow sequence should be designed to activate the following workflow fluidly, subject to set conditions. Contrarily, un-normalized workflow sequences do not guarantee the continuity of the workflow.

Technology risk harms system availability by causing uncertainties in network availability. Examples of technology risk include network interruption or loss of backup data due to a cyber-attack or error in the physical environment. To mitigate this risk, companies are forced to have several backup servers; nevertheless, the integrity of the backup data is still not guaranteed. Elimination of technology risks requires a sophisticated recoverability of the data or fault-free data, as well as a fault tolerance of the network.

3.2 Blockchain Pattern-Based Trust Model

In this section, we propose a pattern-based trust model that normalizes the blockchain interaction corresponding to the trust elements (Subsection 3.1.3). The pattern in the trust model applies blockchain to the risk factors to prevent the risks in the collaborative business process, and thus strengthen the data integrity and security. The proposed pattern treats the risks occurring in the collaboration, without considering security factors in blockchain technology, such as the re-entrance of smart contracts. A detailed examination of the pattern is presented in Subsection 4.3. Fig. 3 displays a blockchain pattern applied to the collaborative business process. In this stage, uncertainty is resolved by the application of the blockchain pattern to the risk occurrence point, and the trust model incorporates the elements of trust into the pattern and verifies the collaborative business process. Verification of the blockchain pattern-based trust model is explained in Section 4, together with the construction of the model.

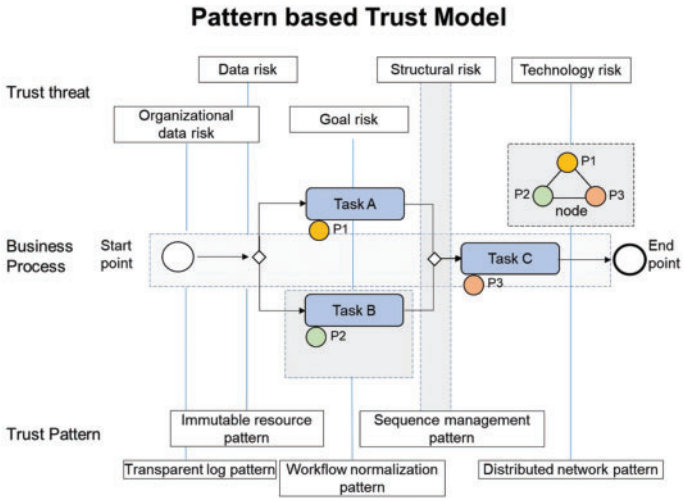

Figure 3: Trust pattern to enhance trust in the collaborative business process

4 Empirical Analysis

We realized a blockchain pattern-based trust model as a healthcare data-sharing process in distributed environments, and subsequently verified the integrity and enhanced security of the process.

4.1 Environmental Setup

The environments to set up the blockchain network are as follows. First, Ethereum, a public blockchain, is used to increase the level of decentralization in the blockchain platform, and Proof of Authority (PoA) is adopted as the consensus algorithm to realize the ID verification function for user privacy. A PoA algorithm is a consensus algorithm that gives block generation authority to some nodes that are reliable and is used for public blockchain that requires privacy protection.

Blockchain Platform Ethereum 2.0

Consensus Algorithm Proof of Authority

4.2 Implementation

Our trust model applies blockchain to a healthcare data-sharing process under distributed environments [51], and thus verifies the integrity and security enhancement of the process. The resulting process is a collaborative business process that shares the data in distributed research environments based on the blockchain. This process ensures the mutual application of data-sharing by integrating the healthcare data structure. The trust model prepares the basis of information protection through data encapsulation structure and encryption. Guarantee of data integrity as well as an irreversible and immutable block suppresses the risks that may manifest inside the healthcare data sharing system, such as falsification or modulation of data while ensuring a safe data sharing network. In addition, the model verifies the integrity and security enhancement by comparing the blockchain patterns. Our model has a trust-guaranteed process for transactions occurring in data-sharing collaboration as follows. First, trust in integrity is secured through healthcare data verification transactions through blockchain. Transactions that occur during data-sharing are transparently disclosed when logged to a block to secure trust. It also ensures the identity of the peer in charge because the creator of the

shared block can be tracked. In addition, it was implemented to ensure trust in the validity of the collaboration contract because the transaction is executed based on the pre-consulted collaboration contract.

By building a trust model-applied collaborative business process, we propose the following research question and verify the appropriateness of the contribution of this study.

Rq1. What are the differences between the blockchain pattern-based trust model and the existing business processes?

In traditional business processes, all the tasks are executed in a centralized order and thus are suitable for a single organization. Contrarily, our trust model adopts distributed architecture of blockchain and thus enables multiple parties and organizations to collaborate for common goals. Moreover, an immutable hash block enables safe data sharing and provides integral and transparent data. In the existing business processes, reliance on a third party is seeking to mediate the execution of workflow between related organizations. In contrast to this process, our model does not require reliance on third parties for integrity as it builds the distributed nodes and smart contracts and realizes decentralization and disintermediation. The healthcare data sharing process in the web environment has potential risks in terms of security and integrity. In addition, the on-chain blockchain healthcare data sharing process faced limitations in block size and caused a lot of loads on the network. Accordingly, we solved the limitation of on-chain block size by distributing healthcare data stored off-chain through a web interface and encrypted on-chain blocks to ensure security and integrity.

Rq2. Why is blockchain necessary for the collaborative business process?

Using blockchain, we developed a set of patterns that enhances the integrity of the collaborative business process and proposed a trust model based on the patterns. In this process, data integrity takes priority in the interaction between the collaborators that are distributed and unreliable. Blockchain has advantages in ensuring integrity through hash encryption, immutable block, and distributed ledger structure, which, in turn, guarantees data consistency in not only collaboration messages, but also the system and API data among the users. Another advantage is security through integral data comparison, which defeats any on- and off-chain data falsification or modification. At the same time, there exist some concerns related to the inflexibility of blockchain, implying that this technology, due to the immutable characteristics of the block, does not allow correction or erasure of data. To prevent such a problem, we applied a validity test in the course of creating the blocking process (moreover, any logical issue of the data can be resolved only through the user's verification).

4.3 Case Study-Verification of Blockchain Pattern-Based Trust Model

We apply the collaborative business process to a public blockchain and carry out trust verification. The application scope of the model is limited to the data-based interacting workflow as defined in the definition of trust in the collaboration business process (Subsection 3.1.1) (our model does not consider the integrity of external data or environments, such as off-chain data or oral contracts).

Method of Verification

The trust model analyzes and verifies the collaborative business process as follows:

1. To recognize a collaborative interaction in the collaborative business process (subsection 3.1.1) and find out potential risk.
2. To analyze and identify the elements of trust that affect the risk at the collaborative interaction point.

3. To identify the elements of trust in the pattern and apply blockchain technology with a model-pattern matching approach.
4. If the elements of trust and the pattern match, then the integrity of relevant collaborative interaction is verified.

The model verifies collaboration trust in an interaction between collaborators, interaction between collaborators and the information system, information records, business protocol, and data updates. By ensuring transparency, traceability, availability, validity, and fault tolerance, through the trust pattern, the integrity enhancement in the collaborative process can be also verified.

Verification of Pattern-based Trust Model for Collaborative Interaction

This section verifies the uncertainty resolution in the trust model-applied healthcare data-sharing process of distributed environments (Fig. 4). The trust pattern of the model is used as the verification index of the model-pattern matching approach (Subsection 3.3.2) and compared with the healthcare data management process of distributed environments (Subsection 4.2).

Table 4 presents the key technical characteristics of the blockchain applied to the trust pattern.

Each trust pattern is specified by the following attributes:

- Name of the pattern
- Trust concern: Threat occurrence point
- Uncertainty: Characteristics of risk occurrence from trust concern
- Blockchain technology: Characteristics of blockchain technology responding to trust concern and uncertainty
- Trust property: An essential element to enhance trust in a collaborative business process

Table 4: Blockchain characteristics in the trust pattern

Blockchain attribute	Description
Distributed ledger	Synchronization, and copy of shared ledger according to the agreement of blockchain network participants
Block hash	Hash encryption of a block transaction
	Blockchain uses the SHA-256 hash function
Block structure	Block header–version, nonce value, timestamp, previous block hash, and transaction hash
	Block body–cryptographic hash that collects transaction information
	It creates a new block that has the previous block hash value and connects the block in a chain
Smart contract	Program code developed to execute certain contract conditions in blockchain
Consensus algorithm	An agreed algorithm to synchronize the distributed ledger

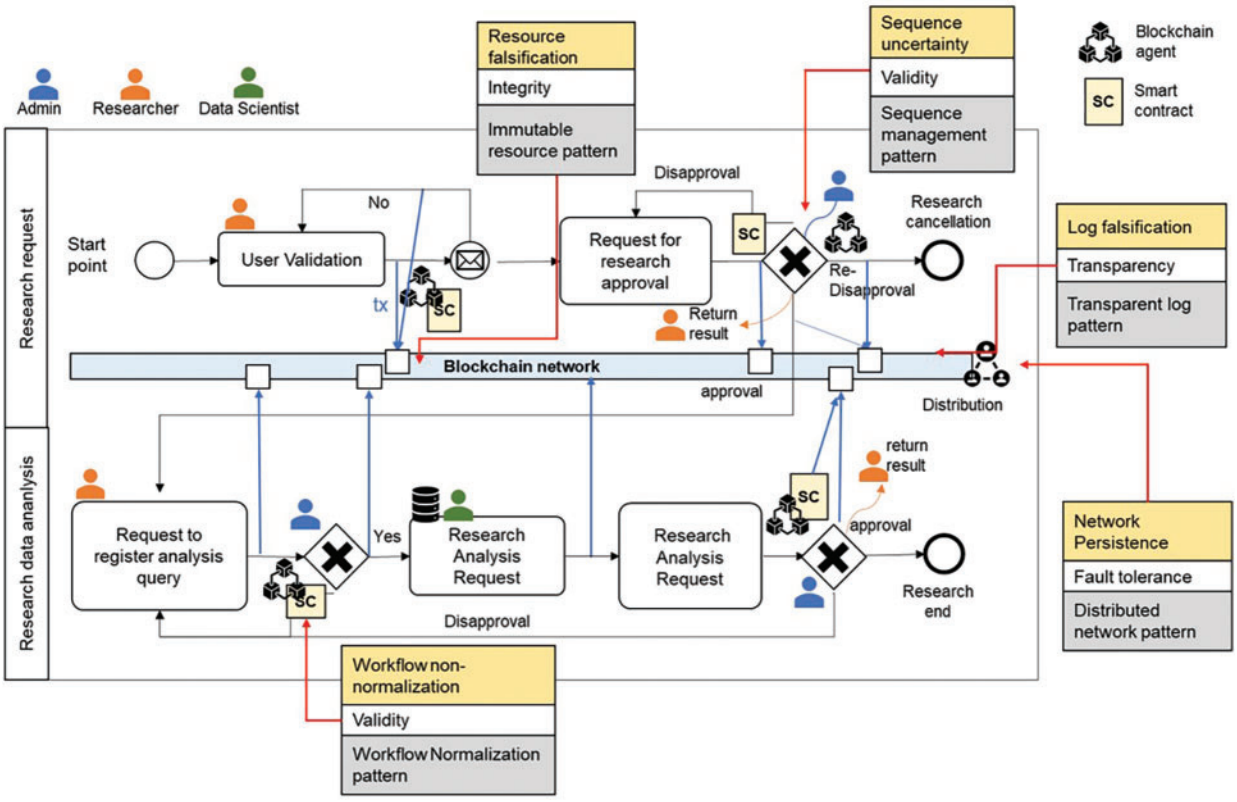

Figure 4: Trust model-applied healthcare data management process under distributed environments (yellow box indicates trust concern, the white box indicates trust property, and the grey box indicates trust pattern)

4.3.1 Immutable Resource Pattern

The immutable resource pattern embeds the blockchain hash, immutable block, and distributed ledger into the trust elements of data risk. Trust concern is identified by the collaborators' ethical actions and shared resources, and uncertainty is identified by the falsification of resources and data. By applying the hash encryption block and distributed ledger technology of the blockchain, the risk of data falsification is eliminated. The hash function converts all the transactions inside the process, such as message exchanges between software, API data transmission and reception, resource sharing, and interaction between collaborators, with an SHA-256 hash algorithm and stores them in a block. Block satisfies the integrity elements (Trust property) because mutual integrity is proven by the hash of the linked block. Moreover, participants' ethics require falsification monitoring, because it relies on the ethics of the collaborators completely. Further, ethics is essential, because the blockchain cannot ensure the integrity of the off-chain data that are not on the blocks; however, it can ensure the integrity of the on-chain data. Therefore, data falsification can be identified by motoring through the distributed ledger and follow-up management is available thereby. Further, accordingly, the uncertainty of falsification of resources and ethical trust can be resolved by using a cryptographic hash block and distributed ledger. The process enhances trust by ensuring integrity (Trust Property) with a block hash. The pattern-applied process removes the risks of data falsification and ensures the integrity and security of the process.

4.3.2 Transparent Log Pattern

The transparent log pattern applies a blockchain-distributed ledger to the process where the workflow records are stored and managed. This pattern resolves the uncertainty of data falsification and loss arising out of the ethical management of the records and central institution (Trust concern), with the transparency of the distributed ledger. The pattern applies a distributed ledger and maintains transparency with the open ledger and resolves the uncertainty of data falsification for synchronization. A shared ledger ensures transparent record management, in which the blockchain network collaborators can generate, update, and access the records transparently. Transparently managed trust is used as a log that traces the responsible source in the business process, and thus ensures the binding effect of responsibility. The move of resources and data in a workflow is recorded with a timestamp and digital signature, and thus can be traced. Moreover, because sharing a distributed ledger eliminates the role of a central institution, the ethics of the central institution are not taken into consideration. Therefore, the log transparency pattern enhances the integrity and security of the process as it resolves the uncertainty in the records and central institution's ethics through a distributed ledger and ensures transparency (Trust Property).

4.3.3 Workflow Normalization Pattern

The workflow normalization pattern applies smart contracts to ensure the validity of an un-normalized workflow. This pattern uses the smart contract's characteristics of automation, which runs when the pre-defined conditions are met, and resolves the issue of un-normalization (Uncertainty). Pre-defined conditions are task performance conditions that normalize the business process policies, workflow requirements and rules, and input and output data, which are agreed upon by the collaborators. Moreover, because any change or modification in the smart contract is recorded, an attempt to change the condition with a malicious intention can be identified. Based on this feature, the workflow normalization pattern resolves the trust concern of an un-normalized workflow and ensures the workflow validity, resulting in the enhancement of the process' integrity and security

4.3.4 Sequence Management Pattern

The sequence management pattern applies smart contracts to the collaborative process, in which the related workflow is linked, and assigns the controlling role to the process. This pattern deals with the uncertainty in the workflow sequence arising from the execution of the smart contract (Trust concern). To ensure a proper workflow implementation and sequence, the pattern categorizes the smart contract into two types based on its role and uses it in the process execution stage. The two types of the smart contracts are "workflow smart contract," which implements the pre-defined conditions, and "control smart contract," which controls the workflow according to the model sequence. First, the workflow smart contract identifies the validity, and then the control smart contract activates the smart contract that executes the following workflow. The order in the sequence is not confused, because the process execution is following the designed process flow, automatically. Therefore, the sequence management pattern resolves workflow event sequence (Trust Concern), and ensures continuity and validity of the workflow (Trust Property), resulting in the enhancement of the collaborative process trust.

4.3.5 Distributed Network Pattern

The distributed network pattern applies blockchain distributed nodes and consensus to the business process network structure, and thus ensures fault tolerance and prevents the uncertainty risks of irrecoverability and process interruption. This pattern connects the blockchain network to all the

participants and builds it as a distributed node, thus eliminating the central server while maintaining fault tolerance. The node includes all the business process participants. The application of this pattern helps the business process continue without interruption, even when malfunction or failure occurs in some nodes. In addition, because the ledger is distributed in multiple nodes, a fast recovery is possible. The degree of fault tolerance can be applied differently depending on the direction of the consensus used by the governance set in the business process designing stage upon blockchain adoption. Based on this, distributed node pattern resolves the uncertainty about the process network (Trust Concern) ensures fault tolerance (Trust Property), and thereby enhancing the collaborative process trust.

Each trust pattern enjoys mapping with trust elements identified from the collaborative business process and blockchain technology. Trust concern is identified as a medium through which a risk occurs, whereas uncertainty indicates the elements affecting the risk occurrence. Blockchain technology presents a mechanism that resolves the process uncertainty and ensures the integrity of trust property, and the trust property is identified by the elements of trust ensured in the collaborative business process. Table 5 categorizes, compares, and verifies the elements identified in our case study and the blockchain pattern of the trust model. The results are marked as "T" for the trusted case, and "U" for the untrusted case.

Table 5: Case for trust elements and blockchain trust pattern's trust elements

CASE	Trust concern		Uncertainty		Blockchain technology		Trust property		Blockchain trust pattern
4.3.1	Collaborators' ethics	T	Falsification	T	Hash, an immutable block	T	Integrity, Transparency	T	Immutable resource pattern
					Distributed ledger	T			
	Resource	T	Falsification	T	Hash, an immutable block	T	Integrity	T	
					Distributed ledger	T			
4.3.2	Central institution's ethics	U	Falsification	T	An immutable block	T	Transparency	T	Transparent log pattern
					Distributed ledger	T			
	Record	T	Falsification	T	An immutable block	T	Integrity	T	
					Distributed ledger	T	Transparency	T	
4.3.3	Workflow	T	Condition unsatisfied	T	Smart contract	T	Validity	T	Workflow normalization pattern
4.3.4	Event sequence	T	Sequence not ensured	T	Smart contract	T	Continuity	T	Sequence management pattern
			Process invalid	T					
4.3.5	Network	T	Process interrupted	T	Distributed node	T	Fault tolerance	T	Distributed network pattern
			Irrecoverability	T	Distributed ledger	T	Recoverability, integrity	T	

4.4 Discussion

In this section, we introduce questions and discussions for a qualitative assessment of the blockchain pattern-based trust model, based on our contribution to this study.

Rq3. Does the pattern-based trust model ensure data integrity?

Our blockchain pattern-based trust model can ensure data integrity through blockchain technology. All the data generated and shared in the collaborative business process are saved in blocks. The blocks are then linked in the chain through hashing encryption and exhibit immutable characteristics. Compared with the external data, the data inside these blocks are free from error or compromise and can be used for integrity verification.

Rq4. Does the pattern-based trust model enhance the security in the business processes?

Our trust model enhances the security in the process by recovering actions upon the occurrence of data falsification or other risks. In the case of internal risks, it can prevent and solve data-related security issues through blockchain technology. In the case of external risks, although it cannot prevent these risks directly with the blockchain, it can use the technology to check the damage state and perform consistent data recovery.

Rq5. Can the pattern-based trust model remove the risk elements in the healthcare data management process under distributed environments?

Our trust model can be an adequate answer to the following risk elements.

1) A solution to the risk of interaction resource falsification by enhancing the integrity

The risk of resource falsification is obliviated by using the immutable resource pattern. By setting the researcher's ethics and resource as trust concerns, the model builds a blockchain-distributed network to prevent data falsification threats and achieves integrity and transparency with hash and immutable blocks.

2) A solution to the risk of uncertain record falsification by enhancing transparency

A transparent log pattern is used to resolve the issue of record falsification risks. In detail, to prevent the manager's ethical issues and record falsification, the model stores the records in an immutable block and shares them with the distributed ledgers. Consequently, transparent record management and monitoring are facilitated, which enhances transparency.

3) A solution to the un-normalized workflow by enhancing validity and continuity

The model can resolve the issue of workflow non-normalization by using workflow normalization and sequence management patterns. To accomplish this, it applies a smart contract so that the users' service use, that is, the workflow, matches both the pre-set conditions and the designed sequence precisely. Because smart contract runs automatically when the workflow moves to match the pre-set conditions and sequence, it confirms the validity and enhances the continuity of the process.

4) A solution to the risks of network interruption and irrecoverability by enhancing fault tolerance and integrity

The risks related to network continuity can be removed by using a distributed network pattern. For fault tolerance of the network, our model distributes the node as a component and prevents network interruption, as well as realizes the fault tolerance of a PoA consensus algorithm. Further, it enables the process to recover the data in an error-free state through the ledger shared in the distributed nodes.

Our trust model can resolve the risk elements in the collaborative business process by using a pattern that uses blockchain. As technology develops, the collaborative business process suffers more and more threats continuously. Because threats increase as the collaboration grows, continuous management is necessary to build trust from the perspective of Zero Trust security.:

4.5 Limitation

Privacy. Blockchain is closely related to the concerns of privacy; that is, the protection of personal information [52]. As a blockchain network allows access to any type of information, all confidential data are subject to the danger of disclosure. The problem of data exposure in the distributed ledger can be resolved by creating a data encryption key and using the key to control transaction access and protect sensitive information. However, the sharing of sensitive information such as biometric data and health records still has potential privacy issues despite data encryption.

Performance Degradation. Because the size of a block is limited to 1 MB, an off-chain database is required. Nevertheless, recently, more efforts have been made to expand the block size (average block size recorded as 45 MB).

5 Conclusion and Future Work

The collaborative business process attempts to resolve the risks in the process, such as falsification, inconsistency, and misuse of data, by using blockchain to achieve an organic connection between the concerned parties and e process integrity. However, due to the lack of specification and verification measures concerning the enhancement of integrity, confirming the adequacy of trust-building was a challenging task. To overcome this limitation, we normalized a pattern that uses blockchain to enhance the integrity and security of the process and proposed a trust model that can verify the effect.

In the proposed trust model-based method, first, we defined "trust" as the integrity of workflow for collaboration, and categorized the interaction that requires trust according to the main user and tasks. Then, we organized six attributes required to build the "trust" in interaction and applied them to the trust model as the model verification criteria (trust property of the elements of trust). Next, we sorted the elements of trust in the collaborative business process and identified them in five risk areas. At this stage, we also normalized the process as a pattern that integrates blockchain technology, is capable of corresponding to the elements of trust, and specified the method to enhance trust. Finally, we built a trust model based on the pattern that used blockchain and verified it by developing a prototype of the healthcare data-sharing process. The prototype has verified the adequacy of trust enhancement based on integrity and security achievement by protecting the privacy and preventing the risks of data falsification, in a trust model-applied data-sharing process. However, the fundamental challenges of blockchain which are privacy and limited block size remain limitations in our study.

In terms of model application, our blockchain trust pattern can be used as a trust-building guidance tool for a collaborative business process model. Further, this trust model can verify the trust enhancement for a collaborative business process under a distributed environment.

Our next study will be focused on the analysis of the trust model effects depending on the blockchain environment. We intend to build and apply a pattern-based trust model in a private blockchain and compare the corresponding trust-building and its verification depending on the blockchain environment. These studies are expected to promote the development of trust models for collaborative business processes.

Funding Statement: This work was supported in part by a grant of the Korea Health Technology R&D Project through the Korea Health Industry Development Institute (KHIDI), funded by the Ministry of Health & Welfare, Republic of Korea (Grant Number: HI19C0870) and in part by Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (P0012724, The Competency Development Program for Industry Specialist).

Author Contributions: JJ, JK, MS and MK contributed the conception and design of the study. JK performed the development of implementation. JJ performed the empirical analysis, and JJ wrote the first draft of the manuscript. JJ, MS and MK wrote sections of the manuscript. All authors contributed to the manuscript revision, and read, and approved the submitted version.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Q. Chen and M. Hsu, "Inter-enterprise collaborative business process management," in *Proc. 17th Int. Conf. on Data Engineering*, Heidelberg, Germany, pp. 253–260, 2001.

[2] U. Dayal, M. Hsu and R. Ladin, "Business process coordination: State of the art, trends, and open issues," in *Proc. of the 27th Int. Conf. on Very Large Data Bases (VLDB)*, Roma, Italy, vol. 1, pp. 3–13, 2001.

[3] M. Müller, N. Ostern, D. Koljada, K. Grunert, M. Rosemann *et al.,* "Trust mining: Analyzing trust in collaborative business processes," *IEEE Access*, vol. 9, pp. 65044–65065, 2021.

[4] Q. Zeng, F. Lu, C. Liu, H. Duan and C. Zhou, "Modeling and verification for cross-department collaborative business processes using extended petri nets," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 2, pp. 349–362, 2014.

[5] A. Cabrera and E. F. Cabrera, "Knowledge-sharing dilemmas," *Organization Studies*, vol. 23, no. 5, pp. 687–710, 2002.

[6] B. Krishnankutty, S. Bellary, N. B. Kumar and L. S. Moodahadu, "Data management in clinical research: An overview," *Indian Journal of Pharmacology*, vol. 44, no. 2, pp. 168, 2012.

[7] J. Krämer, N. Stüdlein and O. Zierke, "Sharing needs caring: Experimental insights on the optimal design of B2B data sharing platforms," *Data as a Common Good*, vol. 66, 2022.

[8] M. L. Ouakouak and N. Ouedraogo, "Fostering knowledge sharing and knowledge utilization: The impact of organizational commitment and trust," *Business Process Management Journal*, vol. 25, no. 4, pp. 757–779, 2018.

[9] M. S. Gal and D. L. Rubinfeld, "Data standardization," *The New York University Law Review*, vol. 94, pp. 737, 2019.

[10] N. Stüdlein, "Developing a framework for strategic data sharing barriers among competitors," *Data as a Common Good*, vol. 16, 2022.

[11] D. D. Shin, "Blockchain: The emerging technology of digital trust," *Telematics and Informatics*, vol. 45, pp. 101278, 2019.

[12] C. D. Ciccio, A. Cecconi, J. Mendling, D. Felix, D. Haas *et al.,* "Blockchain-based traceability of inter-organisational business processes," in *Int. Symp. on Business Modeling and Software Design*, Vienna, Austria, pp. 56–68, 2018.

[13] D. A. Johnston, D. M. McCutcheon, F. I. Stuart and H. Kerwood, "Effects of supplier trust on performance of cooperative supplier relationships," *Journal of Operations Management*, vol. 22, no. 1, pp. 23–38, 2004.

[14] F. A. Al-Zahrani, "Subscription-based data-sharing model using blockchain and data as a service," *IEEE Access*, vol. 8, pp. 115966–115981, 2020.

[15] C. -T. Tseng and S. S. Shang, "Exploring the sustainability of the intermediary role in blockchain," *Sustainability*, vol. 13, no. 4, pp. 1936, 2021.

[16] P. M. Panayides and Y. V. Lun, "The impact of trust on innovativeness and supply chain performance," *International Journal of Production Economics*, vol. 122, no. 1, pp. 35–46, 2009.

[17] M. Rosemann and M. Zur Muehlen, "Integrating risks in business process models," in *Proc. of the 16th Australasian Conf. on Information Systems (ACIS)*, Jeju Island, South Korea, pp. 1–10, 2005.

[18] N. Helil, M. -C. Kim and S. -Y. Han, "Trust and risk based access control and access control constraints," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 5, no. 11, pp. 2254–2271, 2011.

[19] M. Kim and S. O. Park, "Trust management on user behavioral patterns for a mobile cloud computing," *Cluster Computing*, vol. 16, no. 4, pp. 725–731, 2013.

[20] M. Kim and S. O. Park, "Group affinity based social trust model for an intelligent movie recommender system," *Multimedia Tools and Applications*, vol. 64, no. 2, pp. 505–516, 2013.

[21] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, vol. 21260, 2008.

[22] C. Di Ciccio, A. Cecconi, M. Dumas, L. García-Bañuelos, O. López-Pintado *et al.,* "Blockchain support for collaborative business processes," *Informatik Spektrum*, vol. 42, no. 3, pp. 182–190, 2019.

[23] D. Tapscott and A. Tapscott, "How blockchain will change organizations," *MIT Sloan Management Review*, vol. 58, no. 2, pp. 10, 2017.

[24] F. Milani, L. García-Bañuelos and M. Dumas, "Blockchain and business process improvement," *BPTrends Newsletter (October 2016)*, 2016.

[25] M. F. Madsen, M. Gaub, T. Høgnason, M. E. Kirkbro, T. Slaats *et al.,* "Collaboration among adversaries: Distributed workflow execution on a blockchain," in *Symp. on Foundations and Applications of Blockchain*, Los Angeles, California, USA, pp. 8, 2018.

[26] Y. Chen and C. Bellavitis, "Blockchain disruption and decentralized finance: The rise of decentralized business models," *Journal of Business Venturing Insights*, vol. 13, pp. e00151, 2020.

[27] L. Mercenne, K. -L. Brousmiche and E. B. Hamida, "Blockchain studio: A role-based business workflows management system," in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conf. (IEMCON)*, Vancouver, Canada, pp. 1215–1220, 2018.

[28] H. Jin, Y. Luo, P. Li and J. Mathew, "A review of secure and privacy-preserving medical data sharing," *IEEE Access*, vol. 7, pp. 61656–61669, 2019.

[29] R. Whiddett, I. Hunter, J. Engelbrecht and J. Handy, "Patients' attitudes towards sharing their health information," *International Journal of Medical Informatics*, vol. 75, no. 7, pp. 530–541, 2006.

[30] M. Kim, J. Seo, S. Noh and S. Han, "Identity management-based social trust model for mediating information sharing and privacy enhancement," *Security and Communication Networks*, vol. 5, no. 8, pp. 887–897, 2012.

[31] X. Liang, M. Barua, R. Lu, X. Lin and X. S. Shen, "HealthShare: Achieving secure and privacy-preserving health information sharing through health social networks," *Computer Communications*, vol. 35, no. 15, pp. 1910–1920, 2012.

[32] J. Kim and M. Kim, "Intelligent mediator-based enhanced smart contract for privacy protection," *ACM Transactions on Internet Technology (TOIT)*, vol. 21, no. 1, pp. 1–16, 2021.

[33] X. Xu, C. Pautasso, L. Zhu, Q. Lu and I. Weber, "A pattern collection for blockchain-based applications," in *Proc. of the 23rd European Conf. on Pattern Languages of Programs*, Irsee, Germany, pp. 1–20, 2018.

[34] J. Weking, M. Mandalenakis, A. Hein, S. Hermes, M. Böhm *et al.,* "The impact of blockchain technology on business models–a taxonomy and archetypal patterns," *Electronic Markets*, vol. 30, no. 2, pp. 285–305, 2020.

[35] M. Behera, A. Sarangi, D. Mishra, P. K. Mallick, J. Shafi *et al.,* "Automatic data clustering by hybrid enhanced firefly and particle swarm optimization algorithms," *Mathematics*, vol. 10, no. 19, pp. 1–29, 2022.

[36] J. Weking, M. Mandalenakis, A. Hein, S. Hermes, M. Böhm *et al.,* "6G driven fast computational networking framework for healthcare applications," *IEEE Access*, vol. 10, pp. 94235–94248, 2022.

[37] W. Viriyasitavat and A. Martin, "In the relation of workflow and trust characteristics, and requirements in service workflows," in *Int. Conf. on Informatics Engineering and Information Science*, Kuala Lumpur, Malaysia, pp. 492–506, 2011.

[38] N. Gol Mohammadi and M. Heisel, "Enhancing business process models with trustworthiness requirements," in *IFIP Int. Conf. on Trust Management*, Darmstadt, Germany, pp. 33–51, 2016.

[39] V. J. Morkunas, J. Paschen and E. Boon, "How blockchain technologies impact your business model," *Business Horizons*, vol. 62, no. 3, pp. 295–306, 2019.

[40] M. C. Mont and L. Tomasi, "A distributed service, adaptive to trust assessment, based on peer-to-peer e-records replication and storage," in *Proc. Eighth IEEE Workshop on Future Trends of Distributed Computing Systems. FTDCS 2001*, Bologna, Italy, pp. 89–95, 2001.

[41] Q. Lu, A. Binh Tran, I. Weber, H. O'Connor, P. Rimba *et al.,* "Integrated model-driven engineering of blockchain applications for business processes and asset management," *Software: Practice and Experience*, vol. 51, no. 5, pp. 1059–1079, 2021.

[42] M. Müller, N. Ostern and M. Rosemann, "Silver bullet for all trust issues? Blockchain-based trust patterns for collaborative business processes," in *Int. Conf. on Business Process Management*, Seville, Spain, pp. 3–18, 2020.

[43] X. Liu, Z. Wang, C. Jin, F. Li and G. Li, "A blockchain-based medical data sharing and protection scheme," *IEEE Access*, vol. 7, pp. 118943–118953, 2019.

[44] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *2016 2nd Int. Conf. on Open and Big Bata(OBD)*, Vienna, Austria, pp. 25–30, 2016.

[45] K. Fan, S. Wang, Y. Ren, H. Li and Y. Yang, "Medblock: Efficient and secure medical data sharing via blockchain," *Journal of Medical Systems*, vol. 42, no. 8, pp. 1–11, 2018.

[46] A. Jabłoński and M. Jabłoński, "Trust as a key factor in shaping the social business model of water supply companies," *Sustainability*, vol. 11, no. 20, pp. 5805, 2019.

[47] S. Bögel, S. Stieglitz and C. Meske, "A role model-based approach for modelling collaborative processes," *Business Process Management Journal*, vol. 20, no. 4, pp. 598–614, 2014.

[48] J. Sunny, N. Undralla and V. M. Pillai, "Supply chain transparency through blockchain-based traceability: An overview with demonstration," *Computers & Industrial Engineering*, vol. 150, pp. 106895, 2020.

[49] W. Viriyasitavat and D. Hoonsopon, "Blockchain characteristics and consensus in modern business processes," *Journal of Industrial Information Integration*, vol. 13, pp. 32–39, 2019.

[50] M. Hashmi, G. Governatori, H. -P. Lam and M. T. Wynn, "Are we done with business process compliance: State of the art and challenges ahead," *Knowledge and Information Systems*, vol. 57, no. 1, pp. 79–133, 2018.

[51] J. Kim and M. Kim, "DeepBlockShield: Blockchain agent-based secured clinical data management model from the deep web environment," *Mathematics*, vol. 9, no. 9, pp. 1069, 2021.

[52] N. Kshetri, "1 blockchain's roles in meeting key supply chain management objectives," *International Journal of Information Management*, vol. 39, pp. 80–89, 2018.