Computers & Industrial Engineering 175 (2023) 108906

Contents lists available at ScienceDirect

Computers & Industrial Engineering

journal homepage: www.elsevier.com/locate/caie

Implementing a multichain framework using hyperledger for supply chain transparency in a dynamic partnership: A feasibility study

Chi-Chun Chou [a], Nen-Chen Richard Hwang [b], Chang-Wei Li [c], Tawei Wang [d], Yen-Yao Wang [e,*]

[a] California State University, Monterey Bay, Marina, CA 93933, USA
[b] California State University, San Marcos, San Marcos, CA 92096-0001, USA
[c] National Cheng Kung University, Tainan City, Taiwan
[d] DePaul University, Chicago, IL 60604, USA
[e] Auburn University, Auburn, AL 36849, USA

ARTICLE INFO

Keywords:
Supply chain transparency
Information sharing
Permissioned blockchain
Hyperledger
Smart contract

ABSTRACT

As an emerging technology, blockchain is appealing because it ensures authenticity and legitimacy of business activities, improves traceability of products, and enhances supply chain transparency (SCT), thus strengthening trust and confidence among partners. Although academicians and practitioners agree that information sharing is imperative to improve SCT, it is unclear whether and how organizations can take advantage of blockchain technology to manage information sharing when collaborating with partners and competitors in a dynamic supply chain while maintaining privacy and confidentiality. In this study, we attempt to address this issue by building multiple assets and chains with multiple processes, facilitating data aggregation, and maintaining information confidentiality. To achieve these objectives, this study proposes a multi-asset, multichain framework and builds a permissioned blockchain network using Hyperledger Fabric. By constructing "channels" under the proposed framework, this study demonstrates that firms can share information privately and confidentially with partners and competitors in a supply chain and simultaneously improve SCT. Overall, the results obtained from the proof-of-concept analysis suggest that the proposed framework outperforms the public blockchain in terms of information sharing and SCT perspectives.

1. Introduction

The growing usage of blockchain technology has brought disruptive changes to supply chain (Cai et al., 2021; Kumar et al., 2020), accounting (e.g., Chou et al., 2021), and other business practices. This emerging knowhow allows companies to capture events and transactions in near real time, making it possible to store, verify, and share transparent, reliable, and immutable transaction histories in a decentralized ledger system (Kumar et al., 2020). To take advantage of this technological innovation, academicians and practitioners have explored its applications to improve supply chain transparency (SCT) (e.g., Gaur & Gaiha, 2020; Sodhi & Tang, 2019). In essence, SCT implies that a business organization knows exactly what is happening at every stage of its supply chain and can communicate factually and clearly about supply chain operations with internal and external parties. These operations start from the origin and source of events and transactions, manufacturing processes, and product costs to logistics (Bai & Sarkis, 2020). By ensuring authenticity and legitimacy of business activities, enhancing traceability of products, minimizing supply chain risks, and strengthening trust and confidence among partners, blockchain technology has great potential to improve SCT.

Since its applicability is rather preliminary currently, the adoption of blockchains in organizations to enrich SCT remains challenging. For instance, some wonder whether data captured and stored on a public, permissionless blockchain with a fully shared ledger can fulfill the informational needs of an organization's daily operations and decision-making (Wladawsky-Berger, 2018). This concern could even be heftier when a firm collaborates with partners and competitors in a dynamic business arrangement to nurture innovation, leverage resources, improve operational effectiveness and efficiency, and enhance firm value. On the one hand, companies can boost the transparency of information flows through blockchains to improve supply chain visibility

* Corresponding author.
E-mail addresses: cchou@csumb.edu (C.-C. Chou), hwang@csusm.edu (N.-C. Richard Hwang), cwli@gs.ncku.edu.tw (C.-W. Li), david.wang@depaul.edu (T. Wang), yenyao@auburn.edu (Y.-Y. Wang).

https://doi.org/10.1016/j.cie.2022.108906
Received 4 May 2022; Received in revised form 27 October 2022; Accepted 9 December 2022
Available online 14 December 2022

and transparency (Sodhi & Tang, 2019). On the other hand, some firms may take advantage of the information stored on blockchain and shared by collaborative partners to escalate the level of competition for their own benefits (e.g., Bai & Sarkis, 2020; Cui et al., 2022). To mitigate this concern, most blockchain applications on supply chains are either limited to one-on-one information sharing with immediate suppliers and customers or just involve intermediations (e.g., Ripe.io, DLT Labs). To expand the utility of blockchain applications, Cui et al. (2022) pointed out that expanding information sharing with partners and competitors is essential to ensuring the success of a dynamic supply chain relationship.

Although disclosure is at the heart of SCT, it is essential to identify the appropriate parties with whom to share information (Gardner et al., 2019). Applying this argument to interorganizational collaborations, information sharing is crucial for improving trust and creating common ground among entities (Lee et al., 2021; Poppo & Zenger, 2002; Poppo et al., 2016). However, firms may become cautious over information sharing when multiple parties play different, sometimes competing, roles. For instance, corporate executives may be anxious about the potential leakage of critical information, such as product specifications, proprietary technologies, and customer insights, to those with dual roles as partners and competitors (Faems et al., 2008). In this scenario, striking a desirable balance between protecting crucial information, fulfilling decision needs, and supporting collaboration becomes even more demanding in a dynamic partnership with entrusted partners and competitors (Li et al., 2011; Malhotra et al., 2007; Yang et al., 2021). In this case, the adjustments made in terms of what can and should be shared are indispensable to maintaining a sensitive yet dynamic business relationship. To address this issue, Cui et al. (2022) indicated that organizations could consider investing in blockchain technologies to facilitate information sharing, thereby enhancing SCT.

Our motivation to conduct this study is triggered by interactions between members of the research team and the chief technology officer (CTO), who also serves as the blockchain director of the world's largest electronics manufacturer, headquartered in Taiwan. As a strategic endeavor, the affected company decided to enter the electric car (EV) market. To accelerate innovation, it has initiated an ambitious plan to create an open EV ecosystem to promote collaboration among players in the auto industry. When designing the ecosystem, the focal firm determines to provide open access to authorized parties in the supply chain, including product designers, suppliers, manufacturers, and many others. To achieve this goal, blockchain technology will be used to leverage open-source software. What the focal company hopes to accomplish is that blockchain technology can enhance collaboration and improve SCT when developing designs and standards, thus cutting down costs and the number of development cycles. As a result, new business opportunities for the EV market will evolve.

While multiple research projects can be developed via this industry engagement, the focus of this study is to address how the affected manufacturer can effectively manage information sharing and maintain confidentiality while collaborating with partners and competitors. Moreover, it is likely that the members of the partnership will expand over time. Hence, it is necessary to explicitly consider these factors when developing solutions, so participatory entities in the supply chain can not only be awarded appropriate rights in a timely fashion but can also be enabled to access the needed information for decision-making. With continuous engagement with the manufacturer, the research team identifies challenges that could potentially hamper the firm's efforts to achieve SCT in a dynamic partnership setting. Building on these understandings, we created a general blueprint for this study. In addition, this in-depth industrial engagement offers opportunities for us to come up with case scenarios and frame model assumptions in which we reflect on practical situations. By doing so, we can effectively address the challenges encountered by not only the focal manufacturer but also other enterprises with similar situations in the future.

Keeping these backgrounds in mind, the current study attempts to answer the following research question: How could enterprises take advantage of blockchain technology to manage information sharing, improve SCT, and maintain confidentiality when collaborating with partners and competitors in a dynamic business relationship? To address this question, we propose an adaptive information-sharing framework according to permissioned blockchain technology. This framework is intended to support collaborations between partners/competitors, enhance SCT, and maintain confidentiality among participating enterprises. To manage information sharing, a permissioned, multichain-based framework is constructed using "channel-based" privacy. Through proof-of-concepts (POC) applied to Hyperledger Fabric, this study demonstrates how firms can use the proposed framework to (1) capture transactions and events stored in a multiple blockchain network, (2) process operational activities, (3) create and share information with *permitted* partners/competitors in a dynamic partnership, and (4) maintain information confidentiality.

This study contributes to the blockchain technology and SCT literature. First, previous studies have examined how blockchains can enhance SCT (e.g., Chod et al., 2020; Gligor et al., 2022; Rao et al., 2021; Sodhi & Tang, 2019). However, most of them have taken blockchains as a given without examining design issues. Different from what has been reported so far, this study explicitly considers blockchain design by demonstrating how business entities can employ blockchain to collaborate with partners/competitors with special attention to broadening information sharing and improving SCT across various stakeholders. Second, this study addresses a void in Kumar et al.'s study (2020). By implementing a multichain-based framework using "channel-based" privacy, this study optimized the channel configuration to achieve a proper balance between visibility and the competitive edge. Building on the extant literature, this study provides a feasible solution for identifying appropriate stakeholders with whom to share information in the SCT context, particularly when transparency has reached beyond immediate supply chain partners with involving roles. Finally, we employ the POC approach to illustrate how a permissioned multichain framework can fully and seamlessly address the challenges faced by businesses in a dynamic information-sharing context. By doing so, this study provides a feasible solution for corporate executives who seek to understand how blockchains can be employed to strengthen information sharing when forming an alliance to collaborate with partners and competitors.

The remainder of this paper is organized as follows. Section 2 reviews the literature and then develop the conceptual model. Section 3 goes over the design framework. Section 4 outlines hypothetical case scenarios. Section 5 provides a POC when the proposed framework is implemented. Section 6 concludes the study by discussing its theoretical contributions, managerial implications, limitations, and directions for future research.

2. Literature review

This section reviews four research streams in the literature: SCT, information sharing, advantages of adopting blockchains, and challenges of blockchain implementation. Based on this review, we developed a conceptual model.

2.1. Supply chain transparency

Visibility, traceability, disclosure, and openness are often used to represent SCT (Montecchi et al., 2021). As Sodhi and Tang (2019) pointed out, visibility refers to managers' efforts to gather information about upstream and downstream operations in a supply chain, while traceability encompasses a broad range of organizational routines and technological systems necessary to enhance the effectiveness of information integration (Ringsberg, 2014). Moreover, according to Schnackenberg et al. (2020), disclosure refers to the process of sharing organizational information with internal and external stakeholders, while openness refers to a firm's inclination to promote a proactive disclosure culture (Cadden et al., 2013).

Reflecting on the literature, SCT studies can be grouped into six streams: SCT technologies, knowledge integration, governance, sustainability, traceability, and resilience (Montecchi et al., 2021). Research on SCT technologies looks at how to implement information technology to achieve SCT (e.g., Bendoly et al., 2007; Helo & Hao, 2019; Kumar et al., 2020; Lim et al., 2021; Rao et al., 2021). For example, Hasan et al. (2019) combined the Internet of Things and blockchain to perform the monitoring and tracking of products in a supply chain. More recently, Liu et al. (2021) proposed and developed a blockchain-based smart tracking and tracing platform to provide a decentralized traceability solution in the drug supply chain. Regarding knowledge integration studies, this stream of the SCT literature focuses on the relationship between transparency strategies and knowledge integration among supply chain partners (e.g., Xu & Jackson, 2019). Researchers tend to evaluate the effectiveness of SCT as a governance mechanism for promoting openness in an organizational culture (e.g., Cadden et al., 2013). In contrast, studies relating to sustainability are driven by sustainable supply chain management, with the argument that SCT is essential to embed sustainable principles for supply chain management (e.g., Grimm et al., 2014). Studies exploring the use of SCT on traceability have sought to understand how organizational processes support supply chain traceability, in which firms are provided with useful insights into the originality, authenticity, custody chain, and integrity of market offerings (e.g., Agrawal et al., 2021; Montecchi et al., 2021). The last stream of studies on SCT and resilience investigates how SCT can improve organizations' ability to identify risks, manage them, and respond to disruptions (e.g., Basole & Bellamy, 2014). To contribute to the SCT literature, this study focuses on the design issues of blockchains.

Despite the potential benefits of SCT, Sodhi and Tang (2019) indicated that organizations still face challenges in increasing SCT to maximize the benefits of implementing supply chains (Bai & Sarkis, 2020). Since disclosure is the heart of SCT, an affected company must evaluate and determine different types of information disclosure risks when deciding the level of disclosure (Sodhi & Tang, 2019). As documented in the literature, the primary emphasis of SCT studies has been on disclosure itself, and managerial decisions regarding what information to disclose and who to share (Gardner et al., 2019). Although several studies have examined how blockchains could enhance SCT (e.g., Chod et al., 2020; Gligor et al., 2022), insofar, most research reported has treated blockchains as given without focusing on the design features of the technology. More importantly, firms' incentives for blockchain-enabled transparency to manage information sharing have not yet been studied when transparency is expanded above and beyond immediate supply chain partners with evolving roles. To contribute to the literature, this study proposes a permissioned multichain and smart contract-based framework that allows firms to leverage blockchain technology to manage information sharing with business partners and competitors while maintaining confidentiality.

2.2. Information sharing

Information sharing provides opportunities for firms to foster long-lasting relationships and build trust with partners and competitors (Ding et al., 2014). To improve operations and increase profitability, firms may make conscientious decisions to work with others to obtain critical resources, deliver innovative products, and/or provide cutting-edge services (Davis, 2016; Gnyawali & Ryan Charleton, 2018). As the adaptive supply chain theory suggests, the roles in a supply chain must be flexibly reconfigured and accompanied by creative information sharing in a dynamic business environment (Malhotra et al., 2007). Unlike conventional approaches, reconfiguration of roles in the supply chain may require distributors to work on production, manufacturers to take marketing responsibility, and retailers to be involved in product design. To ensure that various functions can work well together under this scenario, supply chain members must gather information and obtain knowledge from partners and use them to redesign interorganizational processes within the supply chain (Dubey et al., 2018; Yang et al., 2021).

Information sharing is a vital resource, often requiring firms to collaborate and share resources and knowledge about their core competencies with competitors (Westergren & Holmström, 2012). In some cases, sharing information with competitors is not only sensitive but also could endanger a company's survival (Li et al., 2011; Loebbecke et al., 2016). When serious tension among supply chain members is triggered, it jeopardizes arrangements made among organizations and causes conflicts between collaborators (Gnyawali & Ryan Charleton, 2018; Soekijad & Joode, 2009). In some cases, one or more members of a consortium may withhold or distort information to outperform other partners or competitors (Smets et al., 2016). Given that supply chain coordination has become increasingly complicated because of escalating business complexity and growing competition intensity, it is challenging to share information because most members are independent companies that tend to focus on their own interests (Huang et al., 2017). These scenarios make the adoption of decentralized technology, such as blockchains, highly relevant for addressing information-sharing dilemmas in a dynamic setting. As reported in the prior literature, numerous researchers have examined various information-sharing issues in supply chains. For example, Huang et al. (2017) considered the coordination of a two-echelon supply chain with multiple suppliers, while Wang and Zhuo (2020) took strategic information sharing in a two-echelon supply chain under a potential supplier encroach into account in their study. More recently, García-Alcaraz et al. (2021) examined the effects of information sharing, decision synchronization, and goal congruence on supply chain performance. In contrast to previous investigations, this study explores how thoughtfully designed blockchains can facilitate information sharing between supply chain participants with divergent, sometimes conflicting, interests.

2.3. Advantages of adopting blockchain

Trust is pivotal to mitigate opportunistic behavior engaged by corporate executives so that the collaboration among partners/competitors can be maintained (Poppo & Zenger, 2002). To address this concern, scholars have suggested that information sharing can strengthen trust and promote collaboration (e.g., Ding et al., 2014; Li & Lin, 2006). While sharing information with others, all parties involved can observe, develop, and confirm trust (Malhotra et al., 2007; Yang et al., 2021). Such arrangements are particularly beneficial in dynamic environments, where intensive exchanges and flexible adjustments are required (Davis, 2016; Poppo & Zenger, 2002). Since trust is a crucial element of information sharing, this study argues that factual transaction data stored on a blockchain improves the reliability of the information available among partners and competitors. We have witnessed several studies that attempt to establish a trusted environment through blockchain technologies. For example, Li et al. (2019) introduced a blockchain-based platform to perform trusted real-time information sharing of logistics resources in E-commerce logistics real estate. More recently, Harish et al. (2021) proposed a platform that leverages blockchain technologies to support the utilization of digital assets of the logistics companies for logistics financing with the goal of establishing a trust environment in the setting of E-commerce retail sales.

As a blockchains can be used to capture, store, verify, and share immutable transaction history, it significantly improves transparency among partners/competitors (Deloitte, 2019). Building a permissioned blockchain strengthens trust and allows parties to manage and control information sharing in a consortium instead of being anonymous members of society (Liu et al., 2019). To explore the benefits of employing a permissioned enterprise blockchain for information sharing, this study proposes a framework using Hyperledger Fabric. To demonstrate how to share information with collaborative partners/competitors while maintaining the confidentiality of proprietary information, we provide a POC in Section 5.

As discussed earlier, the main purpose of an enterprise blockchain is

to support organizations in planning and sharing confidential data in a partnership environment where no single owner is completely trustworthy in the eyes of all users. Since Hyperledger and Corda, examples of enterprise blockchains, would strengthen trust in interorganizational collaborations, they allow us to employ business-side management, such as membership service, identity, and channel management, and to apply technology-side mechanisms supported by blockchains to permanent unalterable records and transaction endorsements made by a group of users. Thus, layers and layers of intermediaries are removed to save middleman costs and processing time. It is particularly beneficial when firms are involved with cross-border trades (Bai & Sarkis, 2020; Cole et al., 2019; Liu & Li, 2020). Using an enterprise blockchain, this study provides an advanced solution to benefit from both business and technology aspects.

Having said that, some might argue that traditional Supplier Relationship Management software or Extended ERP, on top of employing certified agents, may work as well. However, a certified agent is one type of intermediation. Paying these agents to acquire services can be costly and time consuming. Moreover, governance risk will probably accompany intermediation. For example, Enron and WorldCom scandals that occurred in 2001 exemplify that governance risk is associated with auditors, as corruption risk may exist between corporate executives and audit professionals, which causes by ineffective assurance. Since such risks cannot be eliminated entirely by an organization itself, additional regulatory oversights on auditors and other qualified verifiers are required.

2.4. Challenges of implementing a blockchain

While adopting a blockchain can be beneficial, implementing it in a supply chain scenario remains challenging (Queiroz & Wamba, 2019; Wamba & Queiroz, 2020). As Wu et al. (2019) suggested, there are four technical challenges in designing and implementing blockchains: scalability, throughput and latency, data retrieval, and access control. Among them, academicians and practitioners have addressed scalability over an enterprise blockchain, such as Hyperledger, as its primary purpose is to satisfy a variety of business use cases across multiple industries to streamline business processes (Androulaki et al., 2018; Hyperledger Foundation, 2016; Pajooh et al., 2022; Swathi & Venkatesan, 2021; Thakkar et al., 2018). To test scalability, prior studies suggest the employment of two performance outputs: throughput and latency (Pajooh et al., 2022; Swathi & Venkatesan, 2021).

Throughput is defined as the rate of committing valid transactions by a blockchain network in a predefined period, while latency is measured according to the duration from a transaction submitted until it is confirmed and committed. The result then becomes available across a blockchain network (Pajooh et al., 2022). If throughput and latency stay at the same level (or an increase in throughput or a decrease in latency), while the number of transactions, the complexity of transactions, and/or the number of peer nodes increase, the system can be considered scalable. Based on the results of the experiments conducted on Hyperledger Fabric, throughput and latency depend on hardware configuration, blockchain network design, and the complexity of smart contract operations. These experiments also suggest that scalability can be managed by introducing high-performance hardware, enhancing network design, or applying specialized scalable algorithms, such as Apache-spark MLLib. Since the initiative of the Hyperledger Project is to support practical applications, scalability, throughput, and latency issues relating to Hyperledger Fabric have been explored. Thus, the focal point of this study resides in data retrieval and access control over information sharing.

2.4.1. Data retrieval

A high-performance information-sharing system collects trusted data from discrete processes and data sources and then converts them into information based on preprogrammed logics. Once information is generated, collaborative parties must promptly distribute information to appropriate users so that they can utilize it to make decisions. While expanding data dimensions to produce information for sharing in a supply chain is a relatively intuitive concept, a number of implementation issues have arisen in a blockchain environment (Yang et al., 2021). The first issue concerns how to resolve multiple business processes that involve multiple asset exchanges. Unlike existing blockchain applications that focus on a single asset (e.g., a cryptocurrency transaction) or a single process (e.g., food traceability), handling multiple assets or different processes in a blockchain network becomes far more sophisticated because it must be generic and adjustable to cope with real-world applications that require interoperability between multiple blockchains (Belchior et al., 2021).

The second issue relates to the need for blockchains to support a diversified aggregation process to convert transaction-level data into information (Biswas & Gupta, 2019). Reflecting on prior research adopting blockchains in SCT, most of them focus on issues related to transaction data without addressing how to generate information from transaction history. To tackle data aggregation, this study follows Chou et al. (2021) and proposes smart contract technology to fulfill this objective.

2.4.2. Access control

According to Malhotra et al. (2007) and Yang et al. (2021), access control in a blockchain environment means dynamically and adaptively distributing and sharing information internally and externally with multiple parties in a confidential manner. Given the concerns over the confidentiality of proprietary information, determining what information can be distributed and shared is complicated when the information consumers include internal units, such as a production manager, as well as external parties, such as collaborative partners/competitors. Firms may also have to share information with regulators to meet compliance requirements. In this study, our proposed permissioned smart contract-based information-sharing framework has been designed to overcome these challenges. It also overcomes existing supply chain applications of blockchain technology that are either limited to one-on-one information sharing (e.g., Ripe.io) or are involved in disintermediation to create a new information-sharing scenario in which the informational needs of internal consumers, external parties (e.g., partners and competitors), and regulators can all be satisfied.

2.5. The conceptual model of blockchain-enabled SCT in a dynamic setting

Building on the extant literature, we developed a conceptual model. We then proposed a design framework that could be applied to more complex supply chain settings. Driven by the unique nature of blockchains, firms can adopt them to maximize the benefits of SCT. In addition, a blockchain can be employed to facilitate SCT. Referring to the conceptual model presented in Fig. 1, access control and data retrieval are two crucial features of a blockchain. By developing these features, our model can facilitate information sharing by expanding it to multiple stakeholders, including suppliers, competitors, investors, consumers and regulators. The model also allows us to manage information sharing while maintaining confidentiality when collaborating with partners and competitors in a dynamic business alliance.

The three-layer conceptual model demonstrated in Fig. 1 is built on the four-pillar foundation of SCT to ensure visibility, traceability, disclosure, and openness (Montecchi et al., 2021). Since access control is the first line to ensure the confidentiality of information sharing between supply chain participants and the blockchain platform, it needs to be managed in the Portal Layer, which interacts with stakeholders like a portal shell. The portal shell facilitates membership services to identify users (granted peer nodes in an organization), including identity certification through a CA (Certification Authority) service, privacy control, and member registry. All users need to gain verified certificates before

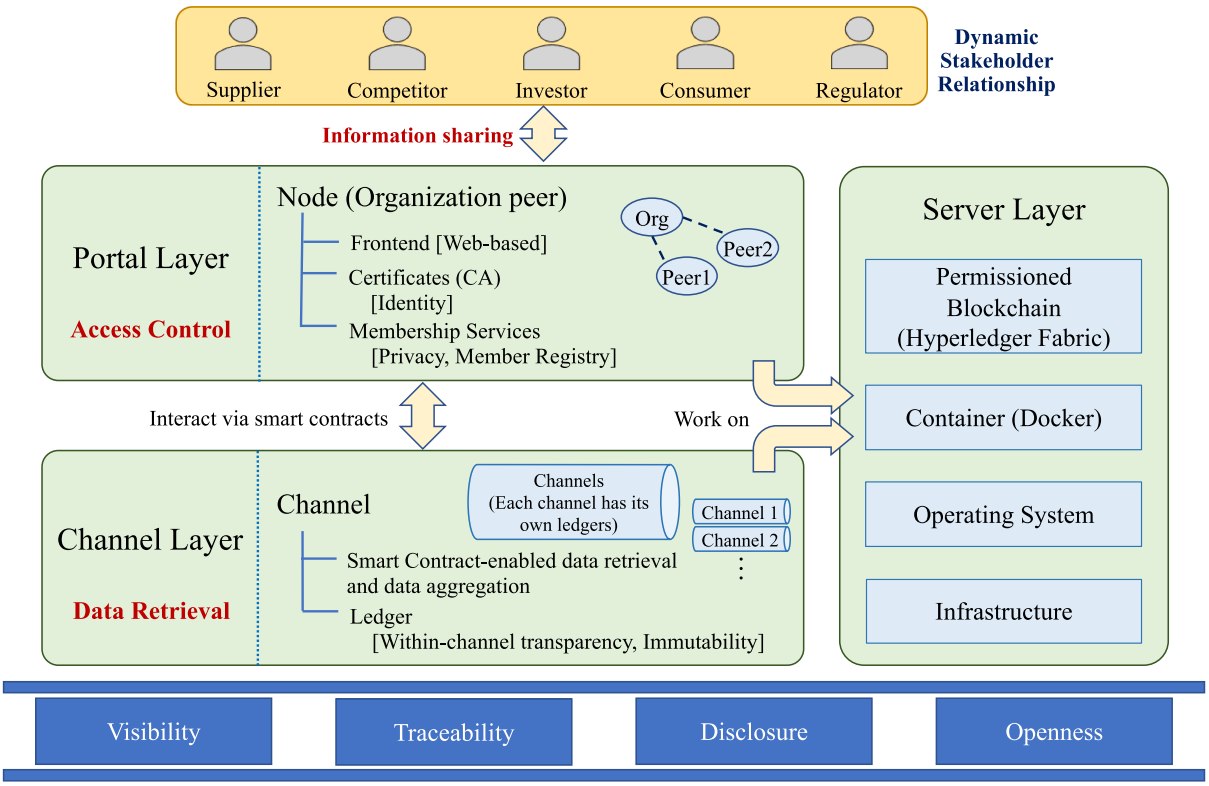


Fig. 1. Blockchain-enabled SCT Model in a dynamic partnership setting.

they can activate any services on the platform. Technically, this portal shell can be implemented using common frontend tools, such as JavaScript, to connect to the channel management service in the middleware layer.

To support an overarching channel management, in the core middleware layer, we propose the adoption of an "information channel" to grant authorized participants access to the ledger data maintained in a channel. The proposed channel-based information sharing is consistent with prior research that recommends the adoption of a permissioned blockchain (such as Hyperledger Fabric) in the context of supply chain management (Bai & Sarkis, 2020; Cole et al., 2019; Liu & Li, 2020). Once a user's identity is verified, the channel management service in the Channel Layer will grant access privileges to the user. Then the user can enter into the channels he/she is registered as a member. To secure data retrieval among authorized users, the insulator mechanism in Channel Layer ensures each channel maintains its own ledgers for participating nodes to share information inside the channel. As discussed in Section 2.4.1, any information circulated in a channel needs to be retrieved, produced, or aggregated through smart contracts to guarantee within-channel transparency. Since the data sources of information aggregation come from the transactional data of multiple assets on blockchains, the immutability can be guaranteed to enhance the information reliability.

To enhance extensibility and scalability (Pajooh et al., 2022; Swathi & Venkatesan, 2021), we propose the adoption of software containers, such as Docker, in the Server Layer to support future extensions for new technologies or new blockchain platforms. A container can bundle a variety of software, packages, and configuration settings, including blockchains such as Hyperledger Fabric. It can separate applications from the system infrastructure to support the idea of a "platform as a service" (PaaS). Users can manage the infrastructure flexibly as they manage applications. Specifically, installing a blockchain in a container allows the platform to have the potential to upgrade data storage (e.g., databases and cloud servers) and computing capacity (e.g., high-performance hardware), as well as to improve network design or more advanced algorithms.

3. Design framework

This section introduces our design principles for the proposed framework and discusses how this framework tackles the three challenges identified in Section 2.4, namely increasing data dimensions through multi-asset interoperability, data aggregation, and access control (data confidentiality).

3.1. Multi-asset, multichain, and multi-process

3.1.1. The importance of multi-asset or multichain to information creation on blockchains

A blockchain tracking the transaction history of a single asset can be treated as a "silo" of data, akin to the way a crypto chain records a money transfer without identifying why the economic value exchange occurs (i.e., in exchange for other assets, such as real estate or other tangible goods). A lack of information about the assets being traded makes the transaction data incomplete, thus disabling subsequent information generation (e.g., analyses by assets, such as sales, costs, or turnovers). Furthermore, the financial picture of transaction-based analysis cannot be fully captured if one cannot cross-reference the duality nature of a transaction.

Based on the conceptual model in Fig. 1, our proposed design framework ensures that the data related to a business transaction are adequately recorded, verified, stored, and immutable for all practical purposes when multiple blockchains interact. Fig. 2 presents a design framework that incorporates connectivity among various blockchains to address the singularity issue inherent in the blockchain for each asset by including a network of blockchains with multiple assets. The dotted rectangles demonstrate the scope of the channels for each subset of participants.

The design framework depicts an example of multiple assets or a multichain. For example, one company might sell land and receive cash

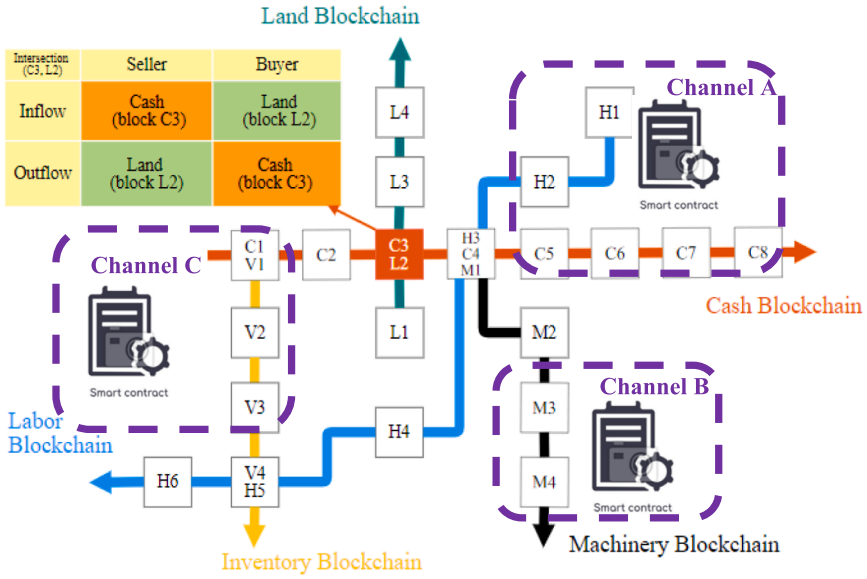


Fig. 2. The design framework of a channel-based, multi-asset blockchain platform with smart contract functionality.

in the sale of a parcel of land. In a silo-like blockchain that deals only with a single asset, the duality of the land sale transaction cannot be captured. Therefore, we propose the adoption of a cross-referenced multichain to tackle the duality nature of transactions. As Fig. 2 illustrates, each line represents one blockchain label—L, C, M, H, and V are represented as land, cash, machinery, labor, and inventory, respectively. The number after a label is a simplified notation that represents a transaction id (instead of using a combination of block id and a hashed transaction id) in a specific asset blockchain (e.g., L1, H5, etc.). The intersection between chains is also a simplified representation of cross-referenced transactions. For example, at the center of Fig. 2, the intersection of a land blockchain (labeled as L) and a cash blockchain (labeled as C) represents a transaction that is cross-referenced as (C3, L2). In the proposed multichain framework, transactions can be recorded and stored in mutual references as journal entries in the double-entry accounting system or as duality relationships, as indicated in the original REA Accounting model proposed by McCarthy (1982).

The platform maintains a trusted history of all traded assets in a blockchain network with duality-oriented interoperability among different assets on a decentralized and credible peer-to-peer (P2P) network. As Fig. 2 suggests, once a transaction such as (C3, L2) is confirmed, mutual references are recorded on each side of the transaction simultaneously, using the transaction address of the dual transaction as the reference key.[1] This key identifies the two dual transactions between the buyer, who pays for the purchase of either a fungible asset (e.g., homogeneous products, such as nuts and bolts) or a non-fungible asset (e.g., unique products, such as the title of a parcel of land), and the seller who receives the payment. Adopting this approach, the economic duality must be either part of the blockchain protocol or can be implemented on the platform through smart contracts.

To facilitate the exchange and access of data between different blockchain networks, some new blockchains (e.g., Ripple, Blocknet, Aion, Wanchain, and Cosmos) provide cross-chain interoperability that enables developers to transfer data and value across different networks (Geroni, 2021). These solutions include the adoption of Oracles (DLT-Repo 2021; Cryptopedia, 2021), sidechains (Cryptopedia 2021; Singh et al., 2020), or bridges/swaps (Cryptopedia, 2021; Leland, 2021). Unlike most cross-chain interoperability projects that focus on transaction data interchanges between existing blockchain networks, we consider the built-in capability to create new, multiple, and cross-related assets on a blockchain platform as a more efficient and economic approach to fulfill the need for information sharing. As it stands, Hyperledger Fabric is among the most highly sought-after blockchain platforms that provide these features. Table A-1 in Appendix A summarizes and compares selected features between Hyperledger Fabric (a private and permissioned blockchain network) and Ethereum (a public and permissionless blockchain network).

3.1.2. *From multi-asset and multichain to multi-process*

Once data are completely recorded on a multi-asset, multichain platform, the built-in smart contract functionality further guarantees that multiple business processes with complex business logic can be implemented (Chou et al., 2021). Because smart contract technology adopts "Turing Complete" programming languages (e.g., Go, Solidity, etc.), it ensures that all computational problems can be solved (Brainerd & Landweber, 1974). Hence, a multi-asset, multichain blockchain platform with built-in smart contract functionality can achieve the goal of multi-process handling and fulfill the need for information sharing among multiple parties in various scenarios.

3.2. *Aggregate transactions to information*

In a blockchain, the main data sources for aggregation include transaction history, internal transactions (data transmitted inside a contract but not directly stored in the main chain), and event logs. On a blockchain that supports smart contracts or chaincodes, most data sources can be retrieved through the native programming languages of smart contracts. However, data aggregation in public blockchains encounters several operational challenges. The first has to do with confidentiality. On a perfectly decentralized public blockchain, the address of a smart contract that handles data aggregation can be randomly exposed to irrelevant nodes. To mitigate the risk of undesirable access to confidential data being processed in a smart contract, contract creators may need to incorporate extra whitelist control to prevent such access. However, the cost of developing and maintaining the whitelist can be exempted in a permissioned blockchain that supports a membership service such as Hyperledger. The second challenge is the potential high

[1] Conceptually, the reference key can be deemed a composite key built into a transaction that includes the blockchain identity, block number, and transaction ID that allows the other half of the dual transaction to locate it.

gas cost for computation. For example, every node contributing to the data source for aggregation in Ethereum must pay an unpredictable price (DLT-Repo, 2021). However, for permissioned blockchains, such as Hyperledger, gas costs can usually be exempted by the centralized authority, thus mitigating the risk of price fluctuation.

3.3. Data confidentiality

The original blockchain was launched as a public, permissionless shared ledger. Any interested party can write transaction data to a public, transparent, and distributed platform without a centralized authority. On such a platform, trust is not built on traditional business awareness. Instead, it is guaranteed when the state of a block of transactions becomes nearly immutable based on the theory of cryptography (Antonopoulos, 2017). To mitigate concerns over confidentiality and prevent undesirable incidents from happening as firms collaborate with competitors/partners, a permissioned blockchain appears to be a more viable solution than a permissionless blockchain.

On a permissioned blockchain, the events and activities are known to a set of identified, and often vetted, participants (i.e., partners/competitors). This type of know-your-customer-like membership service ensures confidentiality among participants, including the originating firm itself and its collaborative partners/competitors, under channel-based architecture. Through the creation of channels, participants are organized into subsets according to the roles assigned to each party, which, in turn, grant rights to view authorized events/transactions. In this setting, only those participating in a channel have access to the *permitted* data, thus preserving the participants' confidentiality within the blockchain network. A permissioned blockchain effectively functions as a traditional enterprise system, offering a combination of business traits (e.g., membership service and channel-based privacy), blockchain-specific traits (e.g., immutability and smart contract enabling), and performance traits (e.g., higher transaction throughput). Thus, a permissioned blockchain possesses attributes that can be implemented as a practical blockchain to fulfill an enterprise's needs (Gartner, 2019).

3.3.1. Channel-based privacy

The primary purpose of a permissioned platform is to maintain confidentiality among partners/competitors. To achieve this objective, the following elements should be added to a permissioned platform, according to Hyperledger (2019):

- *Identity*: All peers on the platform must be identified or identifiable through registration at a specific Certification Authority (CA); all peers in the network are, thus, known to one another. All transactions must be detectable and traceable by regulators and auditors.
- *Channel*: Peers on a permissioned platform can establish special "channels" that include specific subsets of participants. Visibility to transactions is granted through channels. Only nodes that participate in a channel have access to transaction data and the smart contracts required to input or read data.
- *Membership service*: This service grants permissions for resources and access to information for specific identified or identifiable peers on the platform.

Fig. 3 shows a typical channel creation and modification process for a permissioned blockchain. Firms A and B are initially authorized by the membership service provider (MSP) to form Channel SC-1; similarly, Firms C and D form Channel SC-2 (Panel A in Fig. 3). Therefore, A and B can create transactions in Ledger SC-1 (the ledger data contained in SC-1) and access the entire transaction history of Ledger SC-1, while C and D can conduct transactions in Ledger SC-2 and access the entire transaction history of Ledger SC-2. Assuming that D no longer partners with C after a specified time period, the orderer[2] of SC-2 can operate the MSP to immediately revoke D's access to Ledger SC-2 by terminating the data broadcasting service for D. Thus, D can access SC-2 data only prior to the point at which D left SC-2 (Panel B in Fig. 3). D is subsequently permitted by the MSP of SC-1 to join SC-1 (Panel C in Fig. 3). At this juncture, D can create and access all transaction data contained in SC-1. This type of dynamic membership adjustment cannot be seen in any public blockchain. Hence, a permissioned blockchain is totally different from a permissionless blockchain in terms of data confidentiality.

3.3.2. Dynamic role assignment

The lack of role assignment in a public blockchain may be problematic for many business scenarios. In the supply chain context, for example, downstream firms might wish to take advantage of blockchain's "single source of truth" feature to share irrevocable information for different shippers' performance to eliminate the risk of traceability and accountability (Infopulse, 2019). However, the anonymous nature of a public blockchain would discourage them from doing so because a public blockchain does not support role assignment. Collaborative firms in the supply chain may be reluctant to share performance information with parties outside the supply chain. Since every transaction and code is visible to every node in the network, a public blockchain cannot automatically fulfill the need to restrict access.

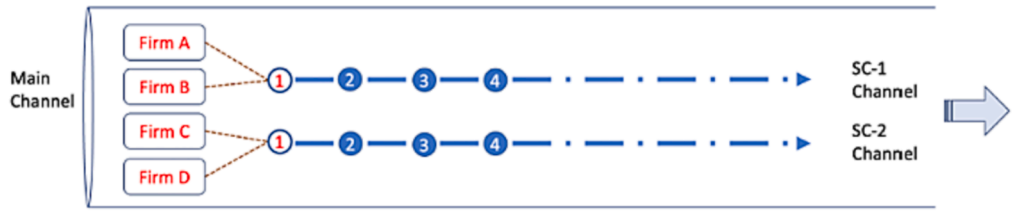
A built-in role-assignment feature is vital for a dynamic business environment. Like the authentication table in a legacy information system, it is necessary to assign roles dynamically to ensure the appropriate distribution of shared information. In a supply chain environment, for instance, a business partner could become a competitor. As illustrated in Panel B of Fig. 3, a long-term supplier (i.e., Firm D) may join a competitor's supply chain to expand its business. When such a role change occurs, a quick adjustment of the information-sharing configuration is essential to maintain the confidentiality of information and to support the continuity of the information-sharing process for all stakeholders. Thus, the use of a permissioned blockchain is preferable for implementing an information-sharing scheme and maintaining confidentiality when a firm must collaborate with its competitors to form a dynamic partnership in a supply chain.

4. Hypothetical case scenarios

To demonstrate how our proposed multichain framework works using Hyperledger, we created a hypothetical group of firms in the electronic products industry with a focus on the electric car (EV) market. We chose this structure because establishing partnerships with competing enterprises is rather common in the industry. This type of dynamic partnership creates a demand for the blockchain framework we propose, as it allows firms to share information for decision-making while dynamically maintaining trust and data confidentiality. The scenarios for this hypothetical case were established based on our interactions with industry leaders, which enabled the research team to use the POC approach to illustrate how to build a permissioned multichain network with appropriate channels and role assignments when sharing information with partners/competitors.

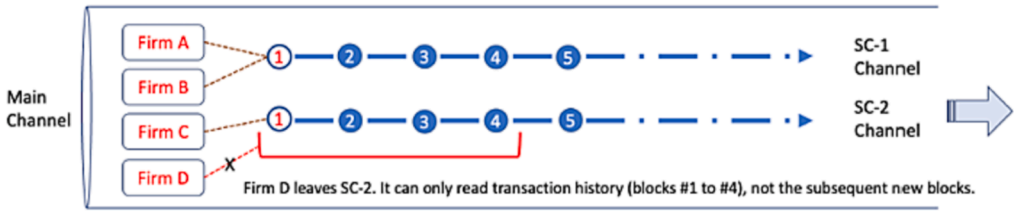
[2] In Hyperledger, the orderer node is responsible for packaging transaction into a block and forwarding the block to the admitted peer nodes for further validation and broadcasting. It also creates and maintains the list of admitted peer nodes since it handles the block delivery task.

Panel A. Initial State



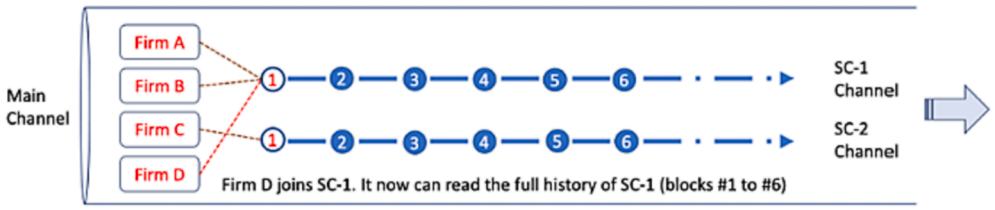
Channel	Members
Main Channel	Firm A, B, C and D
SC-1 Channel (supply chain 1)	Firm A and B
SC-2 Channel (supply chain 2)	Firm C and D

Panel B. Firm D Leaves SC-2



Channel	Members (Before modification)	Members (After modification)
Main Channel	Firm A, B, C and D	Firm A, B, C and D
SC-1 Channel (supply chain 1)	Firm A and B	Firm A and B
SC-2 Channel (supply chain 2)	Firm C and D	Firm C

Panel C. Firm D Joins SC-1



Channel	Members (Before D joins SC-1)	Members (After D joins SC-1)
Main Channel	Firm A, B, C and D	Firm A, B, C and D
SC-1 Channel (supply chain 1)	Firm A and B	Firm A, B and D
SC-2 Channel (supply chain 2)	Firm C	Firm C

Fig. 3. Channel creation and modification.

4.1. Status of the electronic products industry and the managerial dilemma

Over the past two decades, industrial growth has been driven by consumer demand for advanced electronic products, especially in areas such as EVs. Rapid technological development in the EV market exerts enormous pressure on firms to find ways to keep up with demand. To maintain competitiveness, firms must continually focus on finding additional resources, making capital investments, and upgrading production facilities to improve operational effectiveness and efficiency.

As part of the effort to meet the market demand for EV, firms producing electronic components play a pivotal role in the supply chain.[3] The newly emerged business opportunities require new supply chains to be established and existing ones to be reorganized. Although restructuring their supply chains can yield benefits to companies, corporate executives also encounter challenges when operating in uncharted territories. One dilemma is how to manage information sharing when collaborating with business partners and competitors.

[3] https://www.scientificamerican.com/article/chip-shortage-threatens-bidens-electric-vehicle-plans-commerce-secretary-says/.

4.2. Attributes of firms in the partnership

The partnership portrayed here comprises three companies: A-TECH, B-LOGIC, and C-BYTE. A diagram depicting the relationship of partnerships among these firms is shown in Fig. 4.

A-TECH, a publicly listed firm and one of the leaders in the industry, specializes in manufacturing electronic components. A-TECH's business model focuses on creating value for shareholders based on product design and production. A-TECH has done an excellent job in both areas and has become a posterchild in the electronic products industry. B-LOGIC is another major publicly listed company in the industrial segment that specializes in product design. Through several rounds of complex and often heated negotiations, A-TECH signed a contract in 2015 to become a business partner of B-LOGIC, serving as an original equipment manufacturer (OEM). This partnership provides opportunities for A-TECH to create products designed by B-LOGIC that were not produced or sold by A-TECH at the time the partnership was formed. Initially, A-TECH did not compete directly with B-LOGIC. Driven by the successful partnership, the level of collaboration between B-LOGIC and A-TECH increased as time went on. By 2020, the OEM business from B-LOGIC was contributing 25 % of A-TECH's total revenue and 15 % of its net income after taxes.

C-BYTE, a private company, is a newcomer to the industry. As a newly established firm, C-BYTE has limited financial resources. The executives of the firm have made a strategic decision not to build their own manufacturing facility. Instead, the firm invested heavily in research and development and product design. C-BYTE has had several technological breakthroughs that substantially improved its industry standing and was actively searching for a company that could manufacture products based on C-BYTE's designs and product specifications. In 2020, C-BYTE management approached A-TECH and signed a contract for A-TECH to serve as its OEM partner. C-BYTE is in direct competition with B-LOGIC, as they make similar products in the same industry. Unlike the products currently made by A-TECH for B-LOGIC, the products designed by C-BYTE are far more technologically advanced. As such, C-BYTE is likely to take over a significant percentage of B-LOGIC's market share. By 2020, the OEM business from C-BYTE was accounting for 5 % of A-TECH's total revenue and 8 % of its net income after taxes.

4.3. Evolution of the partnership

The partnership between A-TECH and C-BYTE heated up rapidly after the firms tied the knot. In May 2021, A-TECH actively discussed a possible deal to acquire C-BYTE. Soon after the initial talk, A-TECH and C-BYTE signed a memorandum and entered a quiet period while their application for the acquisition was under regulatory review. As part of this process, C-BYTE was required to reveal a large quantity of internal data to A-TECH's management, including a breakdown of sales revenues and customers' details. In addition, A-TECH received a report on the design specifications and technological insights of C-BYTE products.

After A-TECH's potential takeover of C-BYTE was announced, A-TECH executives held a meeting with B-LOGIC's management to determine whether this potential deal would affect the existing OEM arrangements linking the two companies. The management of A-TECH and B-LOGIC agreed that they should continue the business relationship so long as the data provided by B-LOGIC to A-TECH remained confidential and secure. Moreover, A-TECH agreed not to use this information to compete with B-LOGIC if regulators approved C-BYTE's acquisition.

The business relationships between and among A-TECH, B-LOGIC, and C-BYTE evolved in three phases. In Phase I, from mid-2015 to July 2020, A-TECH entered into a partnership agreement with B-LOGIC as an OEM. The products manufactured for B-LOGIC did not directly compete with any products made and sold by A-TECH during this phase. In Phase II, from August 2020 to August 2021, A-TECH became an OEM partner of C-BYTE. Although the products made for C-BYTE did not compete directly with any products manufactured and sold by A-TECH, these products did compete directly with goods made by A-TECH for B-LOGIC. Finally, in Phase III, from September 2021 to the present, H-CORE became the newly formed company after A-TECH acquired C-BYTE. While H-CORE and B-LOGIC are now competitors in a particular segment of the electronic products for the EV market, the original collaboration between the two companies continues.

4.4. Information-sharing scheme

The information-sharing scheme takes place across three phases. In Phase I, A-TECH serves as an OEM for B-LOGIC, and the two companies are not in competition. Under this scenario, B-LOGIC can grant permission for A-TECH, as an OEM partner, to check the inventory level of the products that A-TECH manufactures for B-LOGIC. However, this right does not extend to B-LOGIC's other products. The inventory information shared by B-LOGIC allows A-TECH to adopt the vendor-managed inventory (VMI) method, which automatically triggers production when necessary to avoid out-of-stock issues. The information transmitted by B-LOGIC to A-TECH consists of the aggregated results based on B-LOGIC's purchases from A-TECH and other vendors (these other vendors' identities are masked).

In Phase II, A-TECH serves as an OEM partner for both B-LOGIC and C-BYTE. Since these two firms are in direct competition, B-LOGIC and C-BYTE grant permission for A-TECH to check their respective inventory. As part of the VMI arrangement, B-LOGIC and C-BYTE allow A-TECH to trigger production automatically to avoid out-of-stock issues. Since B-LOGIC and C-BYTE do not share information, two separate channels must be created.

In Phase III, H-CORE Inc. is formed as a new company after A-TECH successfully acquires C-BYTE. H-CORE and B-LOGIC's business relationship continues, but they are now business partners as well as competitors. To manage information sharing when collaborating with a competitor, B-LOGIC grants permissions for H-CORE, an OEM partner, to check its inventory and allows H-CORE to trigger production automatically to avoid out-of-stock issues. However, access to inventory data has been restricted to H-CORE's employees who handle business activities with B-LOGIC. Therefore, a subgroup H-CORE-A is created so that access restrictions could be enforced.

Since both A-TECH and B-LOGIC are publicly listed companies, they are required by laws and regulations to file quarterly reviews and annual audits with the Securities and Exchange Commission. Auditors are required to verify account balances, so channels must be created to function as surrogates of regulatory agencies to verify the information collected and stored on the blockchain. As part of their substantive analytical procedures, auditors are also allowed to use accounting numbers to calculate financial ratios. However, auditors do not need to access some of A-TECH and B-LOGIC's internal information, such as production schedules and design specifications, as these are not part of mandatory information to be verified or included for financial reporting purposes.

5. Proof-of-concept

This section provides the POC using Hyperledger Fabric to demonstrate how the proposed framework can take advantage of the blockchain to fulfill information sharing in a dynamic partnership.

5.1. General settings of POC

For simplicity, we assume that B-LOGIC has two main products: B1 and B2. A-TECH manufactures approximately 70 % of B1 for B-LOGIC, while the remaining 30 % of B1 is made by other vendors. In Phases I and II, A-TECH obtains B1 inventory information by deducting B-LOGIC's total sales quantity of B1 (by masking all customers' identities) from the total quantity purchased of the product (by masking other vendors'

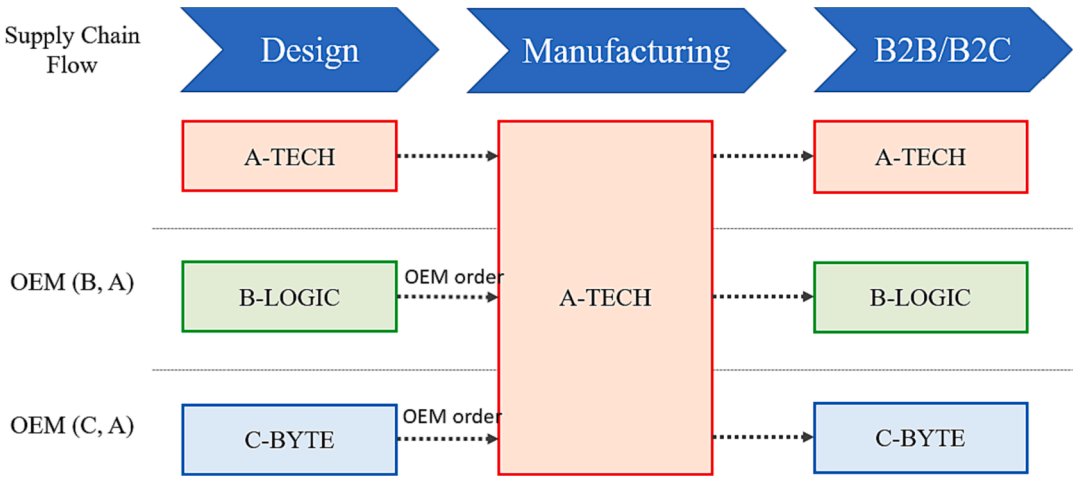


Fig. 4. Relationships among firms in a supply chain.

identities). The partnership between A-TECH and C-BYTE in Phase II resembles the relationship between A-TECH and B-LOGIC in Phases I and II. In addition, we assume that C-BYTE has only one product, C1, and that A-TECH manufactures about 80 % of the product. In Phase III, B-LOGIC adjusts the access group from A-TECH to H-CORE to reflect their concern over information sharing and data confidentiality after H-CORE becomes a collaborative competitor. Table 1 summarizes the resulting information-sharing channels.

The channels presented in Table 1 are divided into two panels: Panel A depicts the Product B1-related channels and Panel B depicts the Product C1-related channels (B2 is not included in the POC because it is outside the partnership between A-TECH and B-LOGIC). Each row in the table represents a separate channel that grants the visibility of transactions to relevant participants. In Panel A, the entire B1 transaction history is divided into the customer channel (B1_Sales) and the vendor channel (B1_Purchases) since customers and vendors are two different groups. Unlike the transaction records for B1_Sales or B1_Purchases, the purpose of B1_Qty channels is to generate and share aggregated information to implement the partnership built on the B1 OEM between A-TECH and B-LOGIC. As the data aggregation column shows, the information generated and shared in B1_Qty is the current inventory level of B1, which results from the total quantity sold minus the total quantity purchased. The optional suffixes I, II, and III shown in the channel titles indicate which phases the channel is active in. For example, B1_Qty_III represents the data aggregation channel that is applied in Phase III when B-LOGIC imposes new access restrictions on its

Table 1
Information-sharing channels for POC Panel A Product B1 – A-TECH and B-LOGIC Panel B Product C1 – A-TECH and C-BYTE.

Channel	Assets	Active Phases	Information Shared	Data Aggregation	From	To	Channel Members
B1_Qty_I_II	Product B1	Phase I, Phase II	Inventory Level – B1	*Aggregation Chaincode* $B1\_QTY = \sum PurchaseQuantity_{B1} - \sum SalesQuantity_{B1}$	B-LOGIC	A-TECH	B-LOGIC: Data Provider, Data User A-TECH: Data User
B1_Qty_III	Product B1	Phase III	Inventory Level – B1	*Aggregation Chaincode* $B1\_QTY = \sum PurchaseQuantity_{B1} - \sum SalesQuantity_{B1}$	B-LOGIC	H-CORE-A	B-LOGIC: Data Provider, Data User H-CORE-A: Data User
B1_Sales	Currency, Product B1	Phase I, Phase II, Phase III	Details of B1 Sales	*Transaction Chaincode No Aggregation*	Peers	Peers	B-LOGIC: Peer B-Customers: Peers
B1_Purchases	Currency, Product B1	Phase I, Phase II, Phase III	Details of B1 Purchases	*Transaction Chaincode No Aggregation*	Peers	Peers	B-LOGIC: Peer B-Vendors:Peers (including A-TECH in Phase I and II, and H-CORE in Phase III)

Channel	Assets	Active Phases	Information Shared	Data Aggregation	From	To	Channel Members
C1_Qty	Product C1	Phase II	Inventory Level – C1	*Aggregation Chaincode* $C1\_QTY = \sum PurchaseQuantity_{C1} - \sum SalesQuantity_{C1}$	C-BYTE	A-TECH	C-BYTE: Data Provider, Data User A-TECH: Data User
C1_Sales	Currency, Product C1	Phase II	Details of C1 Sales	*Transaction Chaincode No Aggregation*	Peers	Peers	C-BYTE: Peer C-Customers: Peers
C1_Purchases	Currency, Product C1	Phase II	Details of C1 Purchases	*Transaction Chaincode No Aggregation*	Peers	Peers	C-BYTE: Peer C-Vendors:Peers (including A-TECH)

partnership with H-CORE (only subgroup A of H-CORE, denoted as H-CORE-A, can access B1 quantity). The permissioned members in each channel are listed in the last column.

The design of channels for C1 resembles that for B1. Thus, in the following POC, we present only the implementation results for Panel A of Table 1 because the implementation for Panel A can be replicated for Panel B with minor changes.

5.2. POC on hyperledger fabric

To fulfill the requirements of our conceptual model presented in Fig. 1 and the design framework demonstrated in Fig. 2, we find that Hyperledger Fabric provides an ideal platform for implementing POC cases, as it provides built-in channel management and membership services and supports multiple asset creation and smart contracts (known as "chaincode" on Hyperledger Fabric). These features make Hyperledger Fabric a well-suited blockchain-enabled middleware to facilitate the Channel Layer, as shown in Fig. 1. In addition, Hyperledger Fabric provides a development kit for an application interface (API) gateway for frontend applications to connect to it. Therefore, its channel management service can be extended to the frontend to develop a Portal Layer that allows multiple users to participate. Hyperledger Fabric also provides Docker images for all components, including peer nodes, channels, and CA. Therefore, it can take advantage of the extensibility and scalability of using a container, as depicted in the Server Layer. In Appendix B, we summarize the background information and demonstrate how to set up the Hyperledger Fabric network for the following POC.

5.2.1. The creation of peer nodes

A node on a blockchain is a device with computing capacity (e.g., a computer or a smartphone) that participates in essential activities, such as trading, executing smart contracts, verifying transactions, or storing the results of transactions, and must comply with the same protocols as a blockchain (Chou et al., 2021). A typical node, like the peer node on Hyperledger, creates, stores, broadcasts, and preserves blockchain data. The creation of peer nodes on Hyperledger Fabric involves more complex procedures than those required for a public blockchain because every peer node needs to be assigned to an organization. Table 2 summarizes the design details of the five peer nodes created in our POC example to implement the hypothetical case, as shown in Panel A of Table 1.

For asset-trading purposes, three peer nodes that can create transactions must be created, namely the stereotype node of B-LOGIC's customers in Channel B1_Sales (node id: peer0.org3.example.com), the stereotype node of B-LOGIC's vendors in Channel B1_Purchase (node id: peer0.org4.example.com), and B-LOGIC itself (node id: peer0.org1.example.com). For information-sharing purposes, two more nodes in Channel B1_Qty_I_II are created to represent A-TECH employees who are granted read-only rights for B1 quantity (node ids: peer0.org2.example.com and peer1.org2.example.com). The access rights for the B1 quantity of the Node peer1.org2.example.com are revoked in Phase III to reflect the new partnership after H-CORE is formed. Fig. 5 demonstrates the POC result of creating Peer0 for Org1 (B-LOGIC), Peer0 for Org2 (A-TECH in Phases I and II and H-CORE-A in Phase III), and the orderer.

The implementation details for the peer nodes are illustrated in Fig. 6, using the example of B-LOGIC's representative node: peer0.org1.example.com.

5.2.2. The creation of multi-assets/multichain

As Panel A of Table 1 shows, the channels for B1_Sales and B1_Purchases require the creation of two assets: Currency and Product B1. Unlike many other blockchain platforms, which maintain the ledger of a single asset, Hyperledger Fabric supports the creation of multiple assets in each channel through chaincodes. Once the chaincode of an asset is deployed on Hyperledger Fabric, we can use the shell command to create transaction records for asset trades and the associated currency transfers simultaneously to fulfill the "duality" nature of these transactions. The data structure of the stereotypes Currency and Product B1 are DigitalCurrency and Inventory, respectively, as shown in Fig. 7. Currency is an instance of DigitalCurrency, whereas Product B1 is an instance of Inventory. The structure of assets resembles the data table layout in a traditional enterprise database. Unlike the single asset blockchain, which only captures transaction records on a multi-asset platform, this supports data management, which is much richer and highly diversified.

We also created a numerical example of the purchase and sales transactions of Product B1. Fig. 8 shows a screenshot of Hyperledger's default command line view for three hypothetical purchase transactions that were incurred in the B1_Purchase channel: 30 units of B1 purchased on 01/05/22, 30 units of B1 purchased on 01/10/22, and 40 units of B1 purchased on 01/20/22. The amounts of purchases are also recorded to reflect the dual transaction of the currency transferred.

Fig. 9 presents the same query results in a browser view to demonstrate the feasibility of using common frontend scripts to interact with on-chain data. The browser view contains JavaScript-based forms that allow users to identify themselves, including organization and node identities. The frontend client then sends a connection request through

Table 2
Peer nodes and orderers.

Organization (Alias in Hyperledger chaincodes)	Peer (Local unique name in an organization)	Peer Identifier (Global unique name)	Role
B-LOGIC (Org1)	Peer0	peer0.org1.example.com	B-LOGIC's representative node
A-TECH (Phase I and II)H-CORE-A (Phase III) (Org2)	Peer0	peer0.org2.example.com	A-TECH's representative node in Phase I and II; H-CORE's representative node that still works as a partner of B-LOGIC in Phase III (a.k.a. H-CORE-A)
A-TECH (Phase I and II)H-CORE (Phase III) (Org2)	Peer1	peer1.org2.example.com	A-TECH's representative node; H-CORE's representative node that no longer works as a partner of B-LOGIC in Phase III (a.k.a. H-CORE)
B-Customers (Org3)	Peer0	peer0.org3.example.com	The stereotype node of all customers
B-Vendors (Org4)	Peer0	peer0.org4.example.com	The stereotype node of all vendors
Orderer (OrdererOrg)	N/A	orderer.example.com	Orderer does not belong to any organization and is not allowed to trade. It is responsible for providing the order for transactions published, cutting blocks with ordered transactions, and distributing them to peers on Hyperledger.

```
cwli@woei-PC:/$ docker ps -a --format "table {{.ID}}\t{{.Image}}\t{{.Names}}"
CONTAINER ID   IMAGE                               NAMES
34e085a02d4b   hyperledger/fabric-tools:latest     cli
e9904196945f   hyperledger/fabric-peer:latest      peer0.org2.example.com
23f38ff3e384   hyperledger/fabric-peer:latest      peer0.org1.example.com
678b5b120011   hyperledger/fabric-orderer:latest   orderer.example.com
```

Fig. 5. Peer node creation for the POC.

```
name: test-network-org1
version: 1.0.0
client:
  organization: Org1
  connection:
    timeout:
      peer:
        endorser: '300'
organizations:
  Org1:
    mspid: Org1MSP
    peers:
    - peer0.org1.example.com
    certificateAuthorities:
    - ca.org1.example.com
peers:
  peer0.org1.example.com:
    url: grpcs://localhost:7051
    tlsCACerts:
      pem: |
          organizations/peerOrganizations/org1.example.com/tlsca/tlsca.org1.example.com-cert.pem
    grpcOptions:
      ssl-target-name-override: peer0.org1.example.com
      hostnameOverride: peer0.org1.example.com
certificateAuthorities:
  ca.org1.example.com:
    url: https://localhost:7054
    caName: ca-org1
    tlsCACerts:
      pem:
        - |
          organizations/peerOrganizations/org1.example.com/ca/ca.org1.example.com-cert.pem
    httpOptions:
      verify: false
```

Fig. 6. The implementation details of B-LOGIC's representative node: peer0.org1.example.com.

```
type DigitalCurrency struct {
        CurrencyID   string. `json:"CurrencyID"`
        CurrencyName  string. `json:"CurrencyName"`
        AmountMinted. int. `json:"AmountMinted"`
        Unit  string `json:"Unit"`
}

type Inventory struct {
        InventoryID  string `json:"InventoryID"`
        ProductName  string. `json:"ProductName"`
        TotalQuantity  int `json:"TotalQuantity"`
}
```

Fig. 7. Stereotype of DigitalCurrency and Inventory in POC.

an API gateway. The API gateway was developed in Node.js[4] using Hyperledger Fabric's SDK[5] (software development kit). After the connection is built, the user's identity data will be transmitted to Hyperledger Fabric to retrieve the user's certificate by activating the CA service. Once the user's identity is verified by the CA, the user will be granted access to the channels to which the user belongs. Then, the user can choose the channel he/she would like to send a query. The list of all query functions implemented in our POC case will then be shown in a dropdown menu for the user to select and send the query to the platform. Then, the platform converts the query request to its default commands to invoke the responding chaincode to execute the query. Finally, the query result is sent back to the frontend through the API gateway, as shown in Fig. 9.

Fig. 10 shows a screenshot of Hyperledger's default command line view for two hypothetical sales transactions in channel B1_Sales: 30 units of B1 sold on 01/15/22 and 50 units of B1 sold on 01/25/22.

[4] Node.js is a an open-source, cross-platform, back-end JavaScript runtime environment that allows developers to write and execute command line tools and server-side scripts.

[5] The Hyperledger Fabric SDK for Node.js provides a powerful API to interact with a Hyperledger Fabric blockchain. The SDK is designed to be used in the Node.js JavaScript runtime. See: https://hyperledger.github.io/fabric-sdk-node/release-1.4/index.html.

```
cwli@woei-PC:~/fabricProject/test-network$ peer chaincode query -C channel1 -n basicPurchase
-c '{"Args":["GetAllAssets"]}' | jq
[
  {
    "PurchaseID": "P001",
    "Date": "01/05/22",
    "ProductName": "Product B1",
    "ProductTransferFrom": "A-TECH",
    "ProductTransferTo": "B-LOGIC",
    "CurrencyTransferFrom": "B-LOGIC",
    "CurrencyTransferTo": "A-TECH",
    "Quantity": 30,
    "Amount": 1500
  },
  {
    "PurchaseID": "P002",
    "Date": "01/10/22",
    "ProductName": "Product B1",
    "ProductTransferFrom": "A-TECH",
    "ProductTransferTo": "B-LOGIC",
    "CurrencyTransferFrom": "B-LOGIC",
    "CurrencyTransferTo": "A-TECH",
    "Quantity": 30,
    "Amount": 1500
  },
  {
    "PurchaseID": "P003",
    "Date": "01/20/22",
    "ProductName": "Product B1",
    "ProductTransferFrom": "A-TECH",
    "ProductTransferTo": "B-LOGIC",
    "CurrencyTransferFrom": "B-LOGIC",
    "CurrencyTransferTo": "A-TECH",
    "Quantity": 40,
    "Amount": 2000
  }
]
```

Fig. 8. Purchase transaction examples in Channel B1_Purchase – command line view.

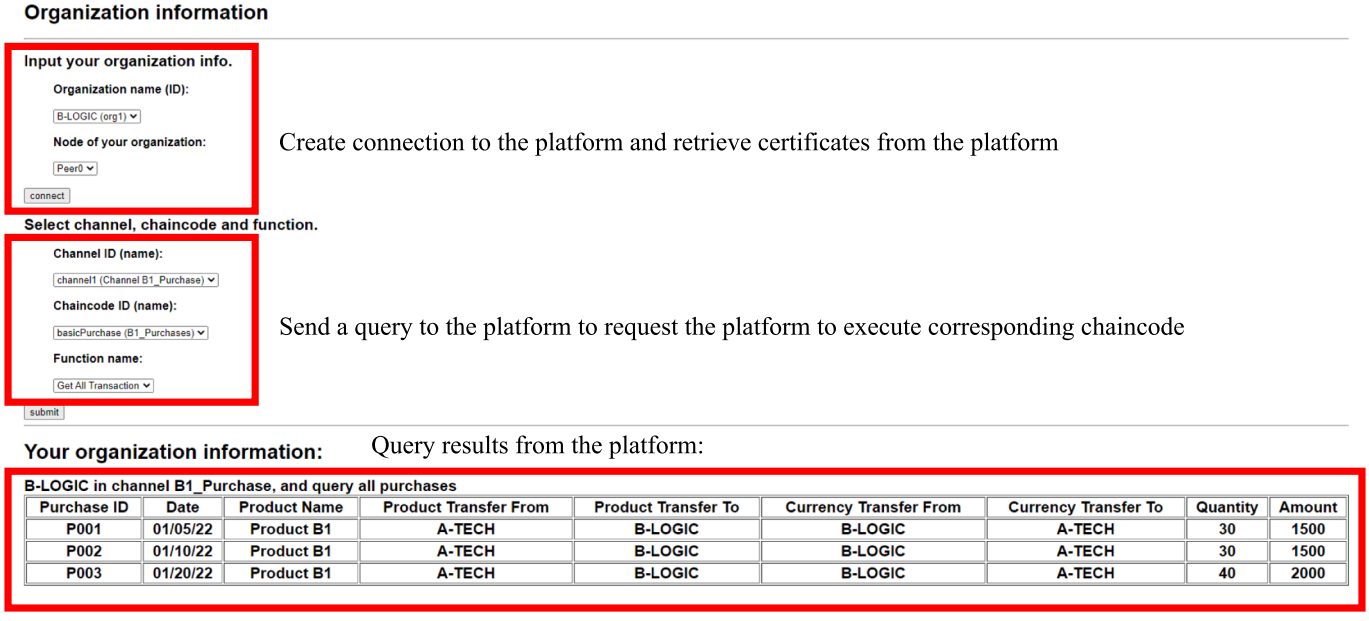
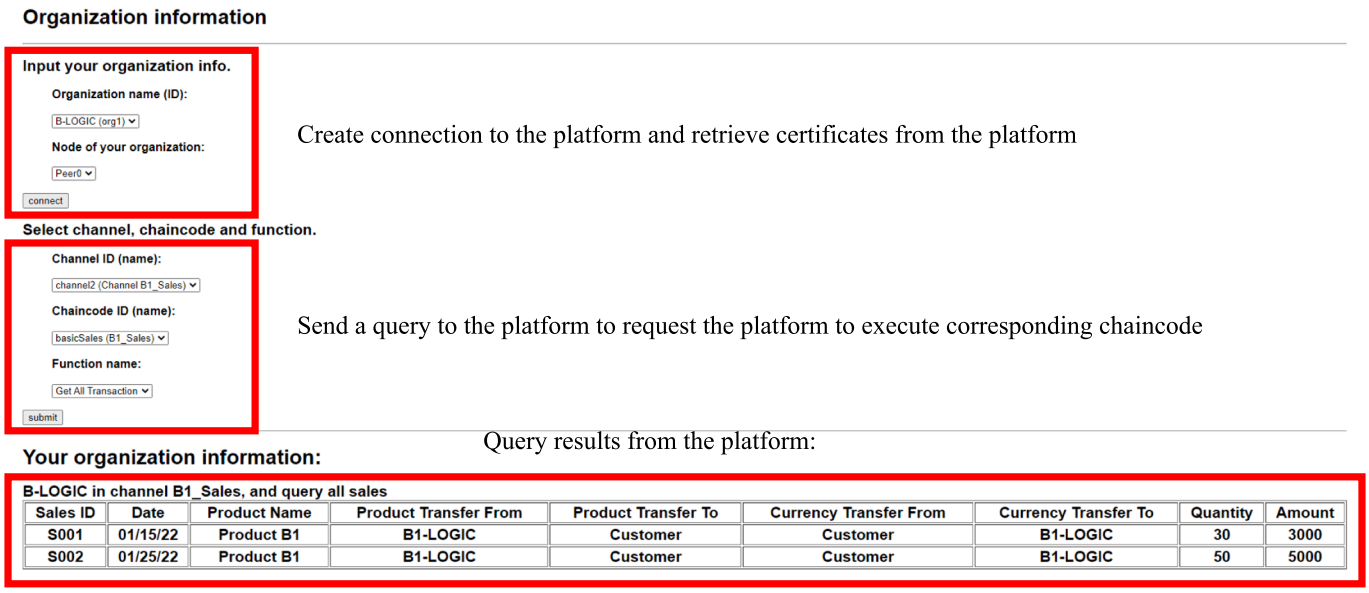


Fig. 9. Purchase transaction examples in Channel B1_Purchase – browser view.

```
cwli@woei-PC:~/fabricProject/test-network$ peer chaincode query -C channel2 -n basicSales
 -c '{"Args":["GetAllAssets"]}' | jq
[
  {
    "SalesID": "S001",
    "Date": "01/15/22",
    "ProductName": "Product B1",
    "ProductTransferFrom": "B1-LOGIC",
    "ProductTransferTo": "Customer",
    "CurrencyTransferFrom": "Customer",
    "CurrencyTransferTo": "B1-LOGIC",
    "Quantity": 30,
    "Amount": 3000
  },
  {
    "SalesID": "S002",
    "Date": "01/25/22",
    "ProductName": "Product B1",
    "ProductTransferFrom": "B1-LOGIC",
    "ProductTransferTo": "Customer",
    "CurrencyTransferFrom": "Customer",
    "CurrencyTransferTo": "B1-LOGIC",
    "Quantity": 50,
    "Amount": 5000
  }
]
```

Fig. 10. Sales transaction examples in Channel B1_Sales – command line view.



Sales ID	Date	Product Name	Product Transfer From	Product Transfer To	Currency Transfer From	Currency Transfer To	Quantity	Amount
S001	01/15/22	Product B1	B1-LOGIC	Customer	Customer	B1-LOGIC	30	3000
S002	01/25/22	Product B1	B1-LOGIC	Customer	Customer	B1-LOGIC	50	5000

Fig. 11. Sales transaction examples in Channel B1_Sales – browser view.

Fig. 11 shows the same query results in the browser view.

5.2.3. Data aggregation

On Hyperledger Fabric, any data aggregation can be executed using chaincode. In our POC case, as shown in Panel A of Table 1, Channel B1_Qty collects purchase and sales data from Channel B1_Purchase and Channel B1_Sales, regardless of phase, to calculate the current inventory level for B1. Using the same numerical examples as those presented in Figs. 8 and 10, a query chaincode is created to obtain the updated inventory quantity according to the query date, as illustrated in Fig. 12.

Some selected query results for different dates are shown in Fig. 13. On 01/31/22, the updated inventory quantity of B1 is 20 units (calculated as total purchase [100 units] minus total sales [80 units]). Although Fig. 13 is a highly simplified example of data aggregation, it is important to note that the chaincode supported by Hyperledger Fabric can successfully complete much more complex computations. The browser view in Fig. 14 shows the same aggregation results using the same frontend solution as introduced in the previous section.

5.2.4. Confidentiality – the creation and modification of channels

As illustrated in Fig. 3, Hyperledger Fabric allows users to structure multiple channels to ensure the confidentiality of the information shared in a supply chain. The three channels (B1_Qty, B1_Sales, and B1_Purchase) identified in Panel A of Table 1 were created as follows: (1) define the configuration of a channel; (2) write relevant information into the channel creation transaction, including organizations, ordering service, channel profiles, and channel policies; (3) use a running instance of the Hyperledger Fabric test network to create the system channel; (4) create an application channel for the peer organizations; (5) assign peers to the appropriate application channel(s); and (6) assign a chaincode to the new channel.

Figs. 15 and 16 present the initial channel information for B-LOGIC

```
echo "query from data aggregation channel, you are B-LOGIC."
peer chaincode query -C mychannel -n basicDataAggregation -c '{"Args":["GetAllInformation"]}' | jq '[.[0:3]]'

echo "get quantity from purchase channel, you are B-LOGIC."
qty_purchase=$(peer chaincode query -C channel1 -n basicPurchase -c '{"Args":["GetAllAssets"]}' | jq '[.[].Quantity] | add')
echo "quantity purchase = $qty_purchase"
echo "get quantity from sales channel, you are B-LOGIC."
qty_sales=$(peer chaincode query -C channel2 -n basicSales -c '{"Args":["GetAllAssets"]}' | jq '[.[].Quantity] | add')
echo "quantity sales = $qty_sales"
echo "calculate quantity of remaining, you are B-LOGIC."
qty_remaining=`expr $qty_purchase - $qty_sales`
echo "quantity remaining = $qty_remaining"

invokeCC() {
  arg1=$qty_purchase
  arg2=$qty_sales
  arg3=$qty_remaining

  args=$(jq \
          -n --arg qtyp "$arg1" \
          -n --arg qtys "$arg2" \
          -n --arg qtyr "$arg3" \
          '{"function":"CreateInformation","Args":["013122001","01/31/22", $qtyp, $qtys, $qtyr]}'
  )
  echo "new information:"
  echo "$args"

  peer chaincode invoke -o localhost:7050 --ordererTLSHostnameOverride orderer.example.com --tls --cafile "${PWD}/organizations/ordererOrganizations/example.com
/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem" -C mychannel -n basicDataAggregation --peerAddresses localhost:7051 --tlsRootCertFiles
"${PWD}/organizations/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/ca.crt" --peerAddresses localhost:9051 --tlsRootCertFiles "${PWD}/orga
nizations/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt" -c "$args"
}

invokeCC "$qty_purchase" "$qty_sales" "$qty_remaining"

sleep 5 &
echo "please wait for update"
wait
echo "query from data aggregation channel, you are B-LOGIC."
peer chaincode query -C mychannel -n basicDataAggregation -c '{"Args":["GetAllInformation"]}' | jq
```

Fig. 12. Query chaincode for Channel B1_Qty(s).

and A-TECH prior to the formation of H-CORE. As these figures demonstrate, B-LOGIC's peer node (peer0.org1.example.com) has joined channels B1_Qty (alias: mychannel in our POC example), B1_Sales (alias: channel1 in our POC example), and B1_Purchase (alias: channel2 in our POC example), while A-TECH's second peer node (peer1.org2.example.com) has joined B1_Qty (alias: mychannel). The focus here is on the second peer node of A-TECH since its access right in Channel B1_Qty is assumed to be revoked later, after H-CORE is formed.

Figs. 17 and 18 present the channel information after access right for A-TECH's second peer node (peer1.org2.example.com) in B1_Qty has been revoked. Looking at the bottom of Fig. 11, the last block in Channel B1_Qty (mychannel) is block #9. If one node (e.g., B-LOGIC) has full access to the ledger, it can access all the data from blocks #1 to #9. However, after revoking the access rights for A-TECH's second peer node (peer1.org2.example.com), as Fig. 17 shows, the last block peer1.org2.example.com can access is blocked after #8. Although peer1.org2.example.com can still access the old data from blocks #1 to #8, it can no longer receive new blocks from the orderer of Channel B1_Qty (mychannel). The results of the modification, shown in Fig. 17, are thus consistent with the requirements for Panel B in Fig. 3; the orderer of B1_Qty terminates the data broadcasting service for A-TECH's second peer node, so Peer peer1.org2.example.com can only access the past data (from blocks #1 to #8) up to the time it leaves B1_Qty.

As part of the model evaluation, we also conducted additional experiments using Ethereum to compare the results obtained for those collected with Hyperledger Fabric. Selected implementation details of the experiments on Ethereum are summarized in Appendix B. The results suggest that our proposed framework outperforms the public Ethereum blockchain in the context of information sharing in a dynamic partnership.

6. Discussion

Driven by pressures from multiple stakeholders, SCT has attracted considerable attention from academicians and practitioners (Gligor et al., 2022; Sodhi & Tang, 2019). As a promising emerging technology, blockchains have shown great potential to improve SCT by ensuring the authenticity and legitimacy of business activities, enhancing the traceability of products, minimizing supply chain risks, and strengthening trust and confidence among partners (Gaur & Gaiha, 2020; Sodhi & Tang, 2019). Although scholars have indicated that information sharing is an integral part of transparency, how information is communicated between supply chain partners can either enhance or constrain SCT (Morgan et al., 2018; Rao et al., 2021). In particular, firms investing in blockchains to enhance SCT often encounter challenges when it comes to creating collaborations with others and deciding what information to share (Cui et al., 2022). This scenario becomes even more evident in a dynamic partnership in which a trusted supplier becomes a competitor (Malhotra et al., 2007; Yang et al., 2021). Therefore, we note that many supply chain applications using blockchains are either limited to one-on-one information sharing with immediate suppliers and customers or involve disintermediation (e.g., Ripe.io, DLT Labs), which restricts information sharing (Cui et al., 2022). In this study, we propose a new adaptive information-sharing framework based on permissioned blockchain technology that will enable firms to collaborate with partners/competitors while maintaining much-needed confidentiality among enterprises and supporting better SCT at the same time.

6.1. Theoretical contributions

This study contributes to the SCT literature and emerging blockchain research in several ways. First, most published articles have considered blockchains as given without discussing the features of blockchains further, even though prior research has documented that blockchains could facilitate SCT by supporting the exchange of operational data. More importantly, it remains challenging to implement blockchains precisely to have appropriate access control for multiple stakeholders to capture and process transaction information. To address this issue, we

Fig. 13. Selected query results from the query chaincode – command line view.

began by responding to calls made by Sodhi and Tang (2019) and other scholars (e.g., Rao et al., 2021) for finding ways to use blockchain to enhance supply chain visibility and transparency. Second, diverse business practices exist among firms and between industries. To improve SCT, we developed an approach to expand existing frameworks to support broader information sharing with competitors and partners. Third, the study conducted by Kumar et al. (2020) did not fully address how to design and implement a multichain-based framework with a desirable channel configuration. To address this void in the literature, this study develops a conceptual model, uses it to structure a framework, and then provides a POC to strike a proper balance between visibility and the competitive edge. Finally, trust and confidentiality are of the utmost importance when negotiating business arrangements. To contribute to the literature, this study addresses these factors by proposing a multi-asset, multichain, and permissioned blockchain framework that highlights critical implementation characteristics crucial to managing information sharing using blockchains as the platform. In doing so, this study provides a practical pathway to render assurance to those in charge of building a new supply chain consortium so that executives can confidently engage in collaborations with business partners and competitors.

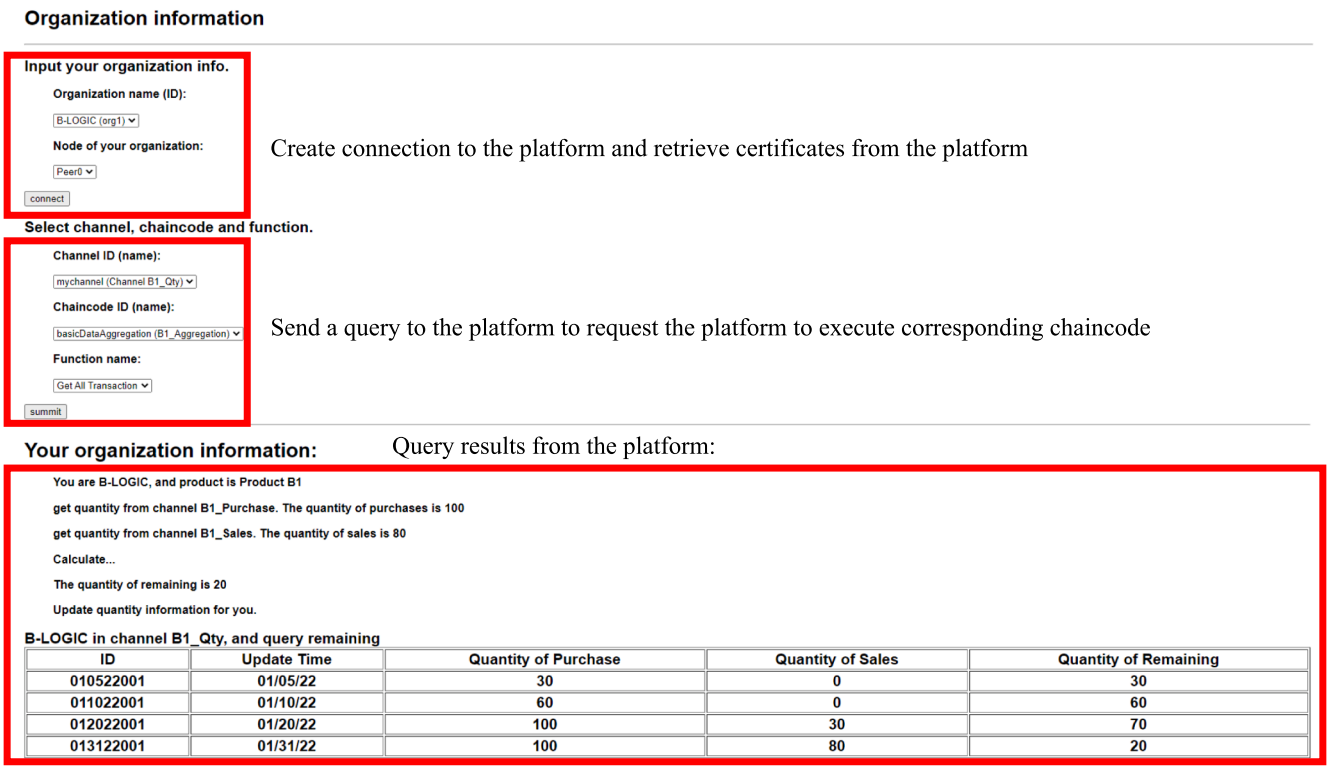


Fig. 14. Selected query results from the query chaincode – browser view.

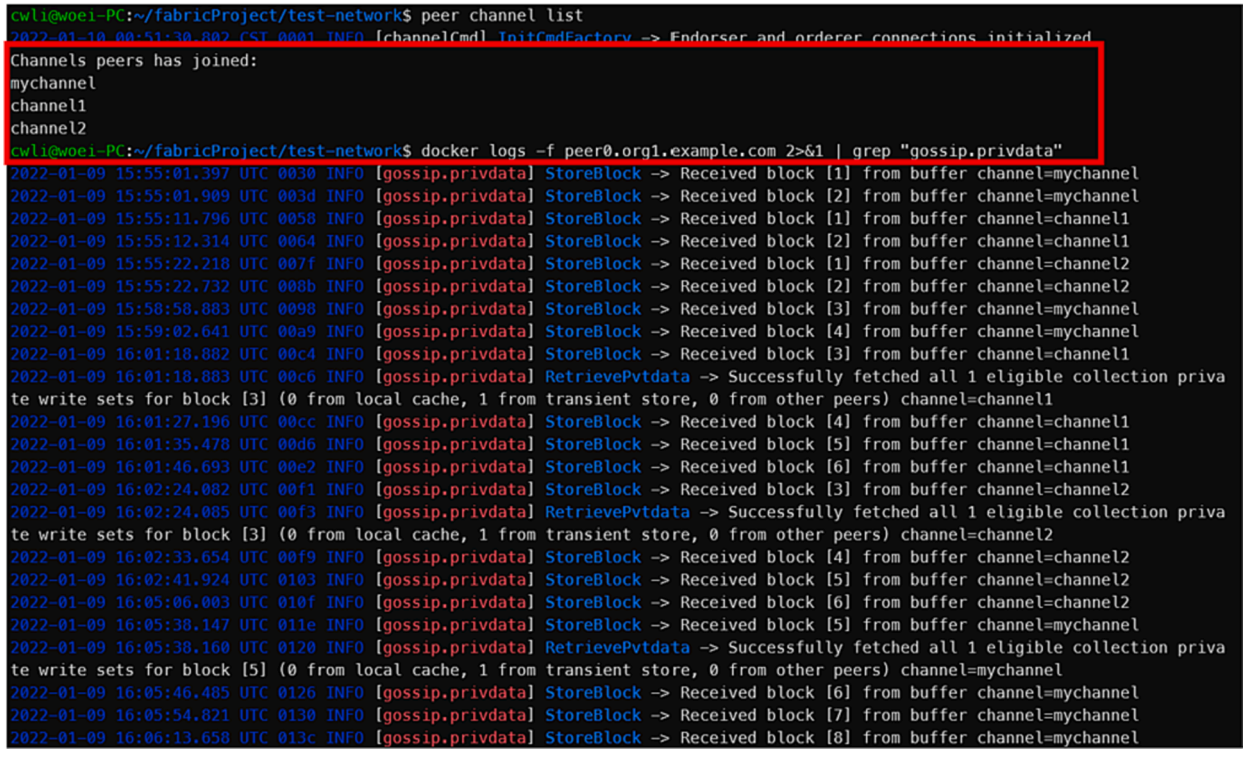


Fig. 15. Channel creation – B-LOGIC (peer0.org1.example.com).

6.2. Managerial implications

Several policy implications can be drawn from the findings reported in this study. For corporate executives, it is imperative not only to appreciate the potential benefits a blockchain network can bring to a business organization but also to understand the challenges it may impose on employees at various levels and functions. To support employees and enable them to take advantage of new opportunities and overcome challenges, firms need to invest in and provide resources to bring the affected individuals and functions up to speed. For

```
cwli@woei-PC:~/fabricProject/test-network$ peer channel list
2022-01-10 00:50:10.089 CST 0001 INFO [channelCmd] InitCmdFactory -> Endorser and orderer connections initialized
Channels peers has joined:
mychannel
cwli@woei-PC:~/fabricProject/test-network$ docker logs -f peer1.org2.example.com 2>&1 | grep "gossip.privdata"
2022-01-09 15:59:02.286 UTC 0032 INFO [gossip.privdata] StoreBlock -> Received block [1] from buffer channel=mychannel
2022-01-09 15:59:02.306 UTC 003b INFO [gossip.privdata] StoreBlock -> Received block [2] from buffer channel=mychannel
2022-01-09 15:59:02.324 UTC 0042 INFO [gossip.privdata] StoreBlock -> Received block [3] from buffer channel=mychannel
2022-01-09 15:59:02.641 UTC 004b INFO [gossip.privdata] StoreBlock -> Received block [4] from buffer channel=mychannel
2022-01-09 16:05:38.148 UTC 005c INFO [gossip.privdata] StoreBlock -> Received block [5] from buffer channel=mychannel
2022-01-09 16:05:46.484 UTC 005f INFO [gossip.privdata] StoreBlock -> Received block [6] from buffer channel=mychannel
2022-01-09 16:05:54.822 UTC 0062 INFO [gossip.privdata] StoreBlock -> Received block [7] from buffer channel=mychannel
2022-01-09 16:06:13.658 UTC 0067 INFO [gossip.privdata] StoreBlock -> Received block [8] from buffer channel=mychannel
```

Fig. 16. Channel creation – A-TECH's 2nd node (peer1.org2.example.com) in phases I and II.

```
cwli@woei-PC:~/fabricProject/test-network$ peer channel list
2022-01-10 01:55:45.351 CST 0001 INFO [channelCmd] InitCmdFactory -> Endorser and orderer connections initialized
Channels peers has joined:
mychannel
channel1
channel2
cwli@woei-PC:~/fabricProject/test-network$ peer channel getinfo -c mychannel
2022-01-10 01:55:49.753 CST 0001 INFO [channelCmd] InitCmdFactory -> Endorser and orderer connections initialized
Blockchain info: {"height":10,"currentBlockHash":"egnucX26xzkzzJdS2vw/6dZP/XYhFhqlbtKjcwNHy1U=","previousBlockHash":"90GT5SX/r8
NHXaff5dHWZkKM/kY1kbc4fszwbdkUM7Y="}
cwli@woei-PC:~/fabricProject/test-network$ docker logs -f peer0.org1.example.com 2>&1 | grep "gossip.privdata"
2022-01-09 15:55:01.397 UTC 0050 INFO [gossip.privdata] StoreBlock -> Received block [1] from buffer channel=mychannel
2022-01-09 15:55:01.909 UTC 003d INFO [gossip.privdata] StoreBlock -> Received block [2] from buffer channel=mychannel
2022-01-09 15:55:11.796 UTC 0058 INFO [gossip.privdata] StoreBlock -> Received block [1] from buffer channel=channel1
2022-01-09 15:55:12.314 UTC 0064 INFO [gossip.privdata] StoreBlock -> Received block [2] from buffer channel=channel1
2022-01-09 15:55:22.218 UTC 007f INFO [gossip.privdata] StoreBlock -> Received block [1] from buffer channel=channel2
2022-01-09 15:55:22.732 UTC 008b INFO [gossip.privdata] StoreBlock -> Received block [2] from buffer channel=channel2
2022-01-09 15:58:58.883 UTC 0098 INFO [gossip.privdata] StoreBlock -> Received block [3] from buffer channel=mychannel
2022-01-09 15:59:02.641 UTC 00a9 INFO [gossip.privdata] StoreBlock -> Received block [4] from buffer channel=mychannel
2022-01-09 16:01:18.882 UTC 00c4 INFO [gossip.privdata] StoreBlock -> Received block [3] from buffer channel=channel1
2022-01-09 16:01:18.883 UTC 00c6 INFO [gossip.privdata] RetrievePvtdata -> Successfully fetched all 1 eligible collection priva
te write sets for block [3] (0 from local cache, 1 from transient store, 0 from other peers) channel=channel1
2022-01-09 16:01:27.196 UTC 00cc INFO [gossip.privdata] StoreBlock -> Received block [4] from buffer channel=channel1
2022-01-09 16:01:35.478 UTC 00d6 INFO [gossip.privdata] StoreBlock -> Received block [5] from buffer channel=channel1
2022-01-09 16:01:46.693 UTC 00e2 INFO [gossip.privdata] StoreBlock -> Received block [6] from buffer channel=channel1
2022-01-09 16:02:24.082 UTC 00f1 INFO [gossip.privdata] StoreBlock -> Received block [3] from buffer channel=channel2
2022-01-09 16:02:24.085 UTC 00f3 INFO [gossip.privdata] RetrievePvtdata -> Successfully fetched all 1 eligible collection priva
te write sets for block [3] (0 from local cache, 1 from transient store, 0 from other peers) channel=channel2
2022-01-09 16:02:33.654 UTC 00f9 INFO [gossip.privdata] StoreBlock -> Received block [4] from buffer channel=channel2
2022-01-09 16:02:41.924 UTC 0103 INFO [gossip.privdata] StoreBlock -> Received block [5] from buffer channel=channel2
2022-01-09 16:05:06.803 UTC 010f INFO [gossip.privdata] StoreBlock -> Received block [6] from buffer channel=channel2
2022-01-09 16:05:38.147 UTC 011e INFO [gossip.privdata] StoreBlock -> Received block [5] from buffer channel=mychannel
2022-01-09 16:05:38.160 UTC 0120 INFO [gossip.privdata] RetrievePvtdata -> Successfully fetched all 1 eligible collection priva
te write sets for block [5] (0 from local cache, 1 from transient store, 0 from other peers) channel=mychannel
2022-01-09 16:05:46.485 UTC 0126 INFO [gossip.privdata] StoreBlock -> Received block [6] from buffer channel=mychannel
2022-01-09 16:05:54.821 UTC 0130 INFO [gossip.privdata] StoreBlock -> Received block [7] from buffer channel=mychannel
2022-01-09 16:06:13.658 UTC 013c INFO [gossip.privdata] StoreBlock -> Received block [8] from buffer channel=mychannel
2022-01-09 17:54:39.642 UTC 0156 INFO [gossip.privdata] StoreBlock -> Received block [9] from buffer channel=mychannel
```

Fig. 17. Channel modification – B-LOGIC (peer0.org1.example.com).

```
cwli@woei-PC:~/fabricProject/test-network$ peer channel list
2022-01-10 01:58:52.973 CST 0001 INFO [channelCmd] InitCmdFactory -> Endorser and orderer connections initialized
Channels peers has joined:
mychannel
cwli@woei-PC:~/fabricProject/test-network$ peer channel getinfo -c mychannel
2022-01-10 01:59:00.684 CST 0001 INFO [channelCmd] InitCmdFactory -> Endorser and orderer connections initialized
Blockchain info: {"height":9,"currentBlockHash":"90GT5SX/r8NHXaff5dHWZkKM/kY1kbc4fszwbdkUM7Y=","previousBlockHash":"sdaKzuRlerbzi57uzeDSYZU
lYncIWvpX9rwzhi0TxSO="}
cwli@woei-PC:~/fabricProject/test-network$ docker logs -f peer1.org2.example.com 2>&1 | grep "gossip.privdata"
2022-01-09 15:59:02.286 UTC 0032 INFO [gossip.privdata] StoreBlock -> Received block [1] from buffer channel=mychannel
2022-01-09 15:59:02.306 UTC 003b INFO [gossip.privdata] StoreBlock -> Received block [2] from buffer channel=mychannel
2022-01-09 15:59:02.324 UTC 0042 INFO [gossip.privdata] StoreBlock -> Received block [3] from buffer channel=mychannel
2022-01-09 15:59:02.641 UTC 004b INFO [gossip.privdata] StoreBlock -> Received block [4] from buffer channel=mychannel
2022-01-09 16:05:38.148 UTC 005c INFO [gossip.privdata] StoreBlock -> Received block [5] from buffer channel=mychannel
2022-01-09 16:05:46.484 UTC 005f INFO [gossip.privdata] StoreBlock -> Received block [6] from buffer channel=mychannel
2022-01-09 16:05:54.822 UTC 0062 INFO [gossip.privdata] StoreBlock -> Received block [7] from buffer channel=mychannel
2022-01-09 16:06:13.658 UTC 0067 INFO [gossip.privdata] StoreBlock -> Received block [8] from buffer channel=mychannel
```

Fig. 18. Channel modification – A-TECH's 2nd Node (peer1.org2.example.com) in phases III.

accountants, auditors, and professionals in other business fields, it is essential to recognize that technological advancement is no turnaround. It is therefore essential to encourage employees to have a sense of urgency, eagerness to learn, and willingness to work in an environment that requires all of us to move forward. With support from corporate executives, we can work together to lift business organizations to a higher ground of competitiveness.

For regulatory agencies, it is evident that having an immutable history of transactions stored in blockchains at their disposal will enhance trust among information consumers in a wide range of enterprises. Blockchain has the potential not only to improve the transparency and reliability of financial statements but also to reduce the cost of capital, facilitate resource flows, enhance operational efficiency and effectiveness, strengthen trust between business partners/competitors, and ensure confidentiality when sharing information. It is our hope that regulators can take the lead and provide support to make blockchains a reality in the business community.

6.3. Limitations and future research

As with all academic research, the findings of this study should be interpreted with caution for the following reasons. One issue has to do with the choice of research method. Although adopting design science as a research methodology has merits for delivering a conceptual understanding of issues of interest, researchers are encouraged to conduct further empirical studies to validate the multichain framework proposed in this study to strengthen our confidence in the outcomes demonstrated and the associated policy implications. The other major limitation is that crucial factors may not have been identified or considered in the analysis. For instance, trust among parties and information-sharing transparency can vary due to culture, the legal environment, and the enforcement of the legal environment. Driven by these factors among industries and between countries, more work is needed to explore how these factors may influence the implementation of the multichain framework proposed in this study. To investigate these issues and mitigate concerns over research limitations, scholars should continue to explore theories from various disciplines, expand this study's scope, and conduct further examinations to advance our understanding of the many complex issues related to blockchain implementation, supply chain management, and information-sharing transparency.

As for directions for future studies, numerous issues deserve attention. To name a few, those interested in management disciplines could find it highly beneficial to develop new research frameworks according to the underlying technologies of blockchain to address a wide range of issues. In addition to information sharing and SCT, issues such as transfer pricing, related party transactions, performance evaluation, external reporting and internal communications, internal controls, and fraud prevention are all worth investigating. As blockchain technology will continue to shape and reshape the information ecosystem in the ever-changing world, it is desirable for academicians and practitioners to conduct managerial analyses of the proposed framework and other blockchain-related issues, so we can gain in-depth understandings of its economic or social impacts on our daily life.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.cie.2022.108906.

References

Agrawal, T. K., Kumar, V., Pal, R., Wang, L., & Chen, Y. (2021). Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. *Computers & Industrial Engineering, 154*(107130), 1–12.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, Angelo De Caro, K., 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., Weed Cocco, S., and Yellick, J. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. *Proceedings of the Thirteenth EuroSys Conference (EuroSys '18). Association for Computing Machinery, USA, 30*, 1–15.

Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the open blockchain*. O'Reilly Media Inc.

Bai, C., & Sarkis, J. (2020). A supply chain transparency and sustainability technology appraisal model for blockchain technology. *International Journal of Production Research, 58*(7), 2142–2162.

Basole, R. C., & Bellamy, M. A. (2014). Supply network structure, visibility, and risk diffusion: A computational approach. *Decision Sciences, 45*(4), 753–789.

Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021). A survey on blockchain interoperability: Past, present, and future trends. *ACM Computing Surveys (CSUR), 54*(8), 1–41.

Bendoly, E., Citurs, A., & Konsynski, B. (2007). Internal infrastructural impacts on RFID perceptions and commitment: Knowledge, operational procedures, and information-processing standards. *Decision Sciences, 38*(3), 423–449.

Biswas, B., & Gupta, R. (2019). Analysis of barriers to implement blockchain in industry and service sectors. *Computers & Industrial Engineering, 136*, 225–241.

Brainerd, W. S., & Landweber, L. H. (1974). *Theory of Computation*. Incorporated, John: Wiley & Sons.

Cadden, T., Marshall, D., & Cao, G. (2013). Opposites attract: Organisational culture and supply chain performance. *Supply Chain Management: An International Journal, 18*(1), 86–103.

Cai, Y. J., Choi, T. M., & Zhang, J. (2021). Platform supported supply chain operations in the blockchain era: Supply contracting and moral hazards. *Decision Sciences, 52*(4), 866–892.

Chod, J., Trichakis, N., Tsoukalas, G., Aspegren, H., & Weber, M. (2020). On the financing benefits of supply chain transparency and blockchain adoption. *Management Science, 66*(10), 4378–4396.

Chou, C.-C., Hwang, N.-C.-R., Schneider, G. P., Wang, T., Li, C.-W., & Wei, W. (2021). Using smart contracts to establish decentralized accounting contracts: An example of revenue recognition. *Journal of Information Systems, 35*(3), 17–52.

Cole, R., Stevenson, M., & Aitken, J. (2019). Blockchain technology: Implications for operations and supply chain management. *Supply Chain Management-An International Journal, 24*(4), 469–483.

Cryptopedia 2021. Cross-Chain Interoperability: What it Means for Blockchain. Cryptopedia. Retrieved on August 9, 2022 from https://www.gemini.com/cryptopedia/why-is- interoperability-important-for-blockchain.

Cui, Y., Gaur, V., & Liu, J. (2022). *Supply chain transparency and blockchain design*. SSRN. Retrieved on August 9, 2022 from.

Davis, J. P. (2016). The group dynamics of interorganizational relationships: Collaborating with multiple partners in innovation ecosystems. *Administrative Science Quarterly, 61*(4), 621–661.

Deloitte.. (2019). Breaking down the blockchain wall. Retrieved on August 9, 2022 from *The Wall Street Journal*. https://deloitte.wsj.com/articles/breaking-down-the-blockchain-wall-01550023333.

Ding, M. J., Jie, F., Parton, K. A., & Matanda, M. J. (2014). Relationships between quality of information sharing and supply chain food quality in the Australian beef processing industry. *The International Journal of Logistics Management, 25*(1), 85–108.

DLT-Repo,. (2021). Data aggregation methods of blockchain oracles. Retrieved on August 9, 2022 from https://dlt-repo.net/data-aggregation-methods-of-blockchain-oracles/.

Dubey, R., Altay, N., Gunasekaran, A., Blome, C., Papadopoulos, T., & Childe, S. J. (2018). Supply chain agility, adaptability and alignment: Empirical evidence from the Indian auto components industry. *International Journal of Operations & Production Management, 38*(1), 129–148.

Faems, D., Janssens, M., Madhok, A., & Looy, B. V. (2008). Toward an integrative perspective on alliance governance: Connecting contract design, trust dynamics, and contract application. *Academy of Management Journal, 51*(6), 1053–1078.

García-Alcaraz, J. L., Díaz-Reza, J. R., Montalvo, F. J. F., Jiménez-Macías, E., Blanco-Fernández, J., & Lardies, C. F. J. (2021). Effects of information sharing, decision synchronization and goal congruence on SC performance. *Computers & Industrial Engineering, 162*, Article 107744.

Gardner, T. A., Benzie, M., Börner, J., Dawkins, E., Fick, S., Garrett, R., … Wolvekamp, P. (2019). Transparency and sustainability in global commodity supply chains. *World Development, 121*, 163–177.

Gartner,. (2019). Gartner top 10 strategic technology trends for 2020. Retrieved on August 9, 2022 from https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020.

Gaur, V., & Gaiha, A. (2020). Building a transparent supply chain. Retrieved on August 9, 2022 from *Harvard Business Review* https://hbr.org/2020/05/building-a-transparent-supply-chain.

Geroni, D. (2021). Blockchain Interoperability: Why Is Cross Chain Technology Important? 101 Blockchains. Retrieved on August 9, 2022 from https://101blockchains.com/blockchain-interoperability/.

Gligor, D. M., Davis-Sramek, B., Tan, A., Vitale, A., Russo, I., Golgeci, I., & Wan, X. (2022). Utilizing blockchain technology for supply chain transparency: A resource orchestration perspective. *Journal of Business Logistics, 43*(1), 140–159.

Gnyawali, D. R., & Ryan Charleton, T. (2018). Nuances in the interplay of competition and cooperation: Towards a theory of coopetition. *Journal of Management, 44*(7), 2511–2534.

Grimm, J. H., Hofstetter, J. S., & Sarkis, J. (2014). Critical factors for sub-supplier management: A sustainable food supply chains perspective. *International Journal of Production Economics, 152*, 159–173.

Harish, A. R., Liu, X. L., Zhong, R. Y., & Huang, G. Q. (2021). Log-flock: A blockchain-enabled platform for digital asset valuation and risk assessment in E-commerce logistics financing. *Computers & Industrial Engineering, 151*, Article 107001.

Hasan, H., AlHadhrami, E., AlDhaheri, A., Salah, K., & Jayaraman, R. (2019). Smart contract-based approach for efficient shipment management. *Computers & Industrial Engineering, 136*, 149–159.

Helo, P., & Hao, Y. (2019). Blockchains in operations and supply chains: A model and reference implementation. *Computers & Industrial Engineering, 136*, 242–251.

Huang, Y. S., Hung, J. S., & Ho, J. W. (2017). A study on information sharing for supply chains with multiple suppliers. *Computers & Industrial Engineering, 104*, 114–123.

Foundation, H. (2016). Linux foundation's Hyperledger project announces 30 founding members and code proposals to advance blockchain technology. Retrieved on August 9, 2022 from https://www.hyperledger.org/announcements/2016/02/09/linux-foundations-hyperledger-project-announces-30-founding-members-and-code-proposals-to-advance-blockchain-technology.

Infopulse,. (2019). Blockchain in supply chain management: Key use cases and benefits. Retrieved on August 9, 2022 from https://medium.com/@infopulseglobal_9037/blockchain-in-supply-chain-management-key-use-cases-and-benefits-6c6b7fd43094.

Kumar, A., Liu, R., & Shan, Z. (2020). Is blockchain a silver bullet for supply chain management? Technical challenges and research opportunities. *Decision Sciences, 51*(1), 8–37.

Lee, J.-Y.-H., Saunders, C., Panteli, N., & Wang, T. (2021). Managing information sharing: Interorganizational communication in collaborations with competitors. *Information and Organization, 31(2), 100354*, 1–25.

Leland,. (2021). Bridges and Swaps: The Future of Interoperability. Retrieved on August 9, 2022 from https://lsquaredleland.medium.com/bridges-and-swaps-the-future-of-interoperability-76d68b9fd0d2 Medium.

Li, S., & Lin, B. (2006). Accessing information sharing and information quality in supply chain management. *Decision Support Systems, 42*(3), 1641–1656.

Li, M., Shen, L., & Huang, G. Q. (2019). Blockchain-enabled workflow operating system for logistics resources sharing in E-commerce logistics real estate service. *Computers & Industrial Engineering, 135*, 950–969.

Li, Y., Liu, Y., & Liu, H. (2011). Co-opetition, distributor's entrepreneurial orientation and manufacturer's knowledge acquisition: Evidence from China. *Journal of Operations Management, 29*(1–2), 128–142.

Lim, M. K., Li, Y., Wang, C., & Tseng, M. L. (2021). A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries. *Computers & Industrial Engineering, 154, 28(1), 107133*, 1–14.

Liu, M., Wu, K., & Xu, J. J. (2019). How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain. *Current Issues in Auditing, 13*(2), A19–A29.

Liu, X., Barenji, A. V., Li, Z., Montreuil, B., & Huang, G. Q. (2021). Blockchain-based smart tracking and tracing platform for drug supply chain. *Computers & Industrial Engineering, 161*, Article 107669.

Liu, Z. Y., & Li, Z. P. (2020). A blockchain-based framework of cross-border e-commerce supply chain. *International Journal of Information Management, 52*(102059), 1–18.

Loebbecke, C., Van Fenema, P. C., & Powell, P. (2016). Managing inter-organizational knowledge sharing. *The Journal of Strategic Information Systems, 25*(1), 4–14.

Malhotra, A., Gosain, S., & El Sawy, O. A. (2007). Leveraging standard electronic business interfaces to enable adaptive supply chain partnerships. *Information Systems Research, 18*(3), 260–279.

McCarthy, W. E. (1982). The REA accounting model: A generalized framework for accounting systems in a shared data environment. *The Accounting Review, 57*(3), 554–578.

Montecchi, M., Plangger, K., & West, D. C. (2021). Supply chain transparency: A bibliometric review and research agenda. *International Journal of Production Economics, 238*(108152), 1–15.

Morgan, T. R., Richey, R. G., Jr, & Ellinger, A. E. (2018). Supplier transparency: Scale development and validation. *The International Journal of Logistics Management, 29*(3), 959–984.

Pajooh, H., Rashid, M. A., Alam, F., & Demidenko, S. (2022). Experimental performance analysis of a scalable distributed Hyperledger Fabric for a large-scale IoT testbed. *Sensors, 22*(13), 4868. https://doi.org/10.3390/s22134868

Poppo, L., & Zenger, T. (2002). Do formal contracts and relational governance function as substitutes or complements? *Strategic Management Journal, 23*(8), 707–725.

Poppo, L., Zhou, K. Z., & Li, J. J. (2016). When can you trust "trust"? Calculative trust, relational trust, and supplier performance. *Strategic Management Journal, 37*(4), 724–741.

Queiroz, M. M., & Wamba, S. F. (2019). Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA. *International Journal of Information Management, 46*, 70–82.

Rao, S., Gulley, A., Russell, M., & Patton, J. (2021). On the quest for supply chain transparency through Blockchain: Lessons learned from two serialized data projects. *Journal of Business Logistics, 42*(1), 88–100.

Ringsberg, H. (2014). Perspectives on food traceability: A systematic literature review. *Supply Chain Management: An International Journal, 19*(5–6), 558–576.

Schnackenberg, A. K., Tomlinson, E., & Coen, C. (2021). The dimensional structure of transparency: A construct validation of transparency as disclosure, clarity, and accuracy in organizations. *Human Relations, 74*(10), 1628–1660.

Singh, A., Click, K., Parizi, R., Zhang, Q., Dehghantanha, A., & Choo, K. R. (2019). Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *Journal of Network and Computer Applications., 149*. https://doi.org/10.1016/j.jnca.2019.102471

Smets, L. P., Langerak, F., & Tatikonda, M. V. (2016). Collaboration between competitors' NPD teams: In search of effective modes of management control. *R&D Management, 46*(S1), 244–260.

Sodhi, M. S., & Tang, C. S. (2019). Research opportunities in supply chain transparency. *Production and Operations Management, 28*(12), 2946–2959.

Soekijad, M., & Joode, R. V. W. D. (2009). Coping with coopetition in knowledge-intensive multiparty alliances: Two case studies. In G. B. Dagnino, & E. Rocco (Eds.), *Coopetition Strategy* (pp. 166–185). Routledge.

Swathi, P., & Venkatesan, M. (2021). Scalability improvement and analysis of permissioned-blockchain. *ICT Express, 7*(3), 283–289. https://doi.org/10.1016/j.icte.2021.08.015

Thakkar, P., Nathan, S., & Viswanathan, B. (2018). *Performance benchmarking and optimizing Hyperledger Fabric blockchain platform*. IEEE MASCOTS.

Wamba, S. F., & Queiroz, M. M. (2020). Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities. *International Journal of Information Management, 52*(102064), 1–9.

Wang, J., & Zhuo, W. (2020). Strategic information sharing in a supply chain under potential supplier encroachment. *Computers & Industrial Engineering, 150*(106880), 1–18.

Westergren, U. H., & Holmström, J. (2012). Exploring preconditions for open innovation: Value networks in industrial firms. *Information and Organization, 22*(4), 209–226.

Wladawsky-Berger, I. (2018). Blockchain beyond the hype. Retrieved on August 9, 2022 from *The Wall Street Journal.* https://www.wsj.com/articles/blockchain-beyond-the-hype-01545248813?tesla=y.

Wu, H., Cao, J., Yang, Y., Tung, C. L., Jiang, S., Tang, B., … Deng, Y. (2019). Data management in supply chain using blockchain: Challenges and a case study. In *28th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1–8). IEEE. https://doi.org/10.1109/ICCCN.2019.8846964.

Xu, X., & Jackson, J. E. (2019). Examining customer channel selection intention in the omni-channel retail environment. *International Journal of Production Economics, 208*, 434–445.

Yang, L., Huo, B., & Gu, M. (2021). The impact of information sharing on supply chain adaptability and operational performance. *The International Journal of Logistics Management, 33*(2), 590–619.