Abdelaziz Bouras · Ibrahim Khalil
Belaid Aouni *Editors*

Blockchain Driven Supply Chains and Enterprise Information Systems

Springer

Blockchain Driven Supply Chains and Enterprise Information Systems

Abdelaziz Bouras • Ibrahim Khalil • Belaid Aouni
Editors

Blockchain Driven Supply Chains and Enterprise Information Systems

Springer

Editors
Abdelaziz Bouras
College of Engineering
Qatar University
Doha, Qatar

Ibrahim Khalil
School of Computing Technologies
RMIT University
Melbourne, VIC, Australia

Belaid Aouni
College of Business & Economics
Qatar University
Doha, Qatar

ISBN 978-3-030-96153-4 ISBN 978-3-030-96154-1 (eBook)
https://doi.org/10.1007/978-3-030-96154-1

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword

Industrial modern supply chains are becoming very complex. Mastering their management is a key success factor for companies and enterprises wishing to grow and increase their gains.

We totally understand the huge potential impact that disruptive technologies such as fintech, artificial intelligence, and blockchain have on current and future supply chains. These technologies are demonstrating the ability to increase business performance, by helping to optimize growth, to establish trust and transparency in the business and in the financial transactions, as well as to better secure information and its infrastructure.

At Qatar Rail, we are currently closely following such progress through collaborations with research institutions and research projects, such as the SupplyLedger project which aims at enhancing traditional supply chains using digital technologies.

This book provides opportunities to industries and organizations to explore the benefit of blockchain technology for their business innovations and supply chains transparency.

I thank the authors and editors for their efforts in bridging the gap between research and industry applications.

Doha, Qatar

H.E. Dr. Abdulla Abdulaziz Turki Al Subaie
Managing Director & CEO/Qatar Rail

Preface

This book, titled *Blockchain Driven Supply Chains and Enterprise Information Systems*, aims at establishing a common ground to provide solutions and best practices around blockchain for supply chain management and enterprise information systems. This book considers the implementation of blockchain platforms in both existing traditional supply chain systems and future enterprise information solutions.

The book has 11 chapters related to important blockchain topics, addressing some of the current needs:

The first chapter provides a scientific analysis of key factors that affect the influence of the blockchain on supply chains performance. The analysis was performed using SPSS and AMOS and the study relied on literature review and surveys of Indian firms. The study is valuable for the industry as it helps decision makers assess the current standing of blockchain and assists them in making the decision for the technology adoption. The chapter proposes a research model based on literature review and surveys to identify critical determinants, namely knowledge sharing, higher authority support, and business partner pressure, to be considered when adopting blockchain technology to better increase the supply chain performance.

The second chapter discusses the role of blockchain in establishing trust in traditional supply chain systems. This trust is analyzed based on a case study involving the finance process of supply chain. It focuses on an important discussion on the notion of trust, though globally there is still lack of consensus on what constitutes trust, and there is no generally widely accepted definition. However, some attempts have been made in other domains, such as the work done by the NIST group around a standardized definition of "trustworthiness" as one of the facets of the CPS (cyber-physical systems).

The third chapter proposes a blockchain-powered digital certificate management system for supply chain systems in the context of transportation of dangerous goods. The chapter suggests a blockchain-based digital certificate platform to monitor the transport of dangerous goods as a supply chain process in terms of verification of stakeholders' identity, history of transportation, environmental data, and real-time location. It focuses on the use of Hyperledger Fabric blockchain network to implement the proof of concept which ensures digital management of transport of dangerous goods.

The fourth chapter presents the challenges of global supply chain systems from the perspective of centralized design. A blockchain-enabled ERP system is presented to mitigate the issues in the centralized global supply chain. This chapter deals with centralized and decentralized supply chains. It proposes a taxonomic analysis of challenges and highlights some solution tracks based on appropriate use of technology.

The fifth chapter seeks to show the pertinence of adopting blockchain technology in textile supply chain and the benefits of such technology in term of traceability and temper proofing. It proposes a blockchain-based solution to enhance traceability and information sharing in the textile supply chain.

The sixth chapter deals with IoT-driven food supply chain management systems, taking advantage of blockchain to improve traceability, transparency, and trustworthiness of the transactions. A complete step-by-step operational flow detailing agri-food supply chain management process would help readers understand how traceability is achieved and how the system saves tremendously with cost-effective measures. The proposed architecture highlights traceability, and software architecture details how the architecture can be realized in practice. The proposed concept, that is, from farm to fork, was implemented in Ethereum and Hyperledger Sawtooth.

The seventh chapter highlights the most known consensus algorithms–based blockchains and their application in the healthcare sector, such as proof of work, proof of stake, and proof of authority. The main objective of this chapter is to illustrate applications and implications of several consensus mechanisms in blockchain-based healthcare supply chain systems.

The eighth chapter shows how blockchain can help improve the authenticity and transparency of supply chain transactions in the automotive industry. It has identified the weakness of the existing supply chain system in the automotive industry and explained the challenges of adoption and deployment of blockchain in this area. It gives a great insight to managers and blockchain practitioners on how to overcome the difficulties that they will encounter during implementation of blockchain technology.

The ninth chapter presents a new consensus mechanism for blockchain-based supply chain management systems to provide solutions to data security and establish trust among different supply chain participants. The proposed consensus mechanism offers a less complicated implementation of the distributed ledger and ensures higher efficiency and scalability for achieving consensus. It is designed considering a consortium blockchain network involving all supply chain stakeholders.

The tenth chapter focuses on blockchain technology and its features, such as distributed ledger and smart contracts from a regulation point of view. It defines the current regulatory landscape and international initiatives. The chapter highlights some applications of the blockchain technology through regulation perspective in the finance, healthcare, logistics, and construction sectors. It emphasizes some challenges faced by blockchain technology and comes up with some recommendations to tackle those challenges.

The eleventh chapter presents a broker-based integration of blockchain smart contracts with industrial workflows. It uses Hyperledger Fabric as a permissioned blockchain platform to store the transaction data and manage the lifecycle of smart contracts. It uses as well Odoo which is an open-source framework written in Python. The chapter proposes a proof-of-concept integration with a scenario of a small-scale manufacturing supply chain involving a limited number of actors and demonstrates that the Odoo workflows can easily be adapted to be fully managed using smart contracts. Thus, increasing the security and enhancing the traceability and trust of critical business transactions.

We would like to thank the authors for their valued contributions and efforts and the reviewers for their help and support in achieving this book. We hope that this book serves as a step forward in this exciting area of blockchains for industry and businesses.

Doha, Qatar — Abdelaziz Bouras
Melbourne, VIC, Australia — Ibrahim Khalil
Doha, Qatar — Belaid Aouni

Acknowledgments

This book was made possible by NPRP grant NPRP11S-1227-170135 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

About the Book

This book provides several international case studies across different domains such as healthcare, agri-food, logistics, and transportation. Those case studies are mainly related to the implementation of blockchain platforms on modern systems and the integration of such technology with existing traditional systems. The book highlights as well subjects and concerns such as efficiency of blockchain-based supply chains, blockchain consensus protocols and mechanisms, and blockchain based enterprise information systems. It concludes with some directions and recommendations with regards to the adoption of standardized blockchain frameworks. The editors' and authors' expertise across different contexts and countries has made this book a worthy contribution to both theory and practice. Through its solutions and best practices, this book constitutes an interesting source for practitioners and students interested in the domain of blockchain for supply chains management and enterprise information systems.

Contents

Impact of Blockchain Technology Adoption in Performance of Supply Chain

Manish Mohan Baral, Subhodeep Mukherjee, Venkataiah Chittipaka, and Bhaswati Jana

1 Introduction

The supply chain management (SCM) industry has gone through many disruptions recently. The development of new technologies and their implementations have a high impact on the supply chain, operations, etc. Blockchain technology (BT) allows decentralization and helps in the digitalization of business models [1]. Prior studies [2–11] stated that BT could transform the business models related to SCM, improves the SC process, and improvises SC performance. The SC performance refers to the SC's expanded activities in meeting final customer requirements, including product availability, delivery on time, and all the required inventory and capacity in the supply chain for the reactive delivery of such performance [12]. The benefits of performance measuring systems in the supply chain are overwhelmed by implementation and maintenance costs. This will most likely be applied to small companies without the resources, time, or information required to optimize supply chain activities [13]. When the characteristics or features of BT are considered, then its adoption in the field of the SC will increase for enhancing the SC performance.

BT can help in improving complicated SC issues and also enhance traceability of operations [9], regardless of segment involved: healthcare, security, wine industry, etc. [14–20]. This new technology can be utilized to solve complexities in the SC such as accountability and transparency [21], security [22], reduction in SC

M. M. Baral (✉) · S. Mukherjee
Department of Operations, GITAM School of Business, GITAM (Deemed to be University), Visakhapatnam, Andhra Pradesh, India

V. Chittipaka
School of Management Studies (SOMS), Indira Gandhi National Open University (IGNOU), Maidan Garhi, New Delhi, India

B. Jana
Department of Management, GD Goenka University, Haryana, India

A. Bouras et al. (eds.), *Blockchain Driven Supply Chains and Enterprise Information Systems*, https://doi.org/10.1007/978-3-030-96154-1_1

expense [23], resilience [24], etc. Integrating BT with SCs is a trusted approach for remodeling and supporting SC. Also, BT can be a means of achieving SC sustainability [12].

Most of the prior studies have discussed the benefits and advantages of adopting BT in various fields. To date, its application is not practical and is in its infant stage [25]. There is a lack of empirical study in this area of BT and SCM. Hence, the current study aims to contribute to the existing literature gap by identifying the value of BTA in SCM. This study identifies the antecedents of BTA and its impact on SC performance in developing country perspective. Hence, the proposed model helped get a piece of evidence that the assumed parameters affect SC performance. The study contributes not an only blockchain but also to the SCM.

The rest of the paper is as follows: Sect. 2 discusses the literature survey; Sect. 3 discusses the theoretical framework and hypothesis development; Sect. 4 discusses the research methodology, which includes sampling techniques utilized for collecting data and demographics of respondents; Sect. 5 discusses the data analysis which states the data analysis which provides for EFA, CFA, construct validity, and SEM approach for establishing the model fit; Sect. 6 contains discussion of the current research, contribution to study, and practice and managerial implications; and finally Sect. 7 contains the conclusion, scope, and future research directions.

2 Background of the Study

SC performance plays a critical role in all types of firms and due to operations complexity in the present digital era. Hence, it is essential to understand the BT relationship and SC performance to achieve better efficiency by the firms.

2.1 Application of Blockchain

Over a decade ago, in the cryptocurrency market, BT emerged (Nakamoto, 2008). BT does not require any third-party involvement; it is an individual-to-individual transaction platform. For the business reason, various entities engaged with the transaction function as nodes, and the cycle is being approved through cryptography. These transactions are stored as decentralized and shared ledgers over the participating entities [2]. BT integrates various other technologies like cryptographic technology, database technology, software development, etc. [26]. Blockchain is an encoded computerized record put away on multiple PCs of a public or private organization [3]. It consists of blocks or data records. When these individual blocks are combined in a chain form, a single player cannot change the data stored in the blocks. They can be verified by shared governance protocols and automation [27]. Blockchain is a shared network, so every member keeps a duplicate copy of the record [4]. BT helps provide a single, tamper, shared, tamper-evident ledger that records the transaction per occurrence [28]. All members ordinarily affirm transactions in a BT through an agreement instrument. Once information is recorded and validated in a blockchain, it becomes permanent. A single participant cannot change or modify the transactions [5]. This quality of blockchain differentiates it from the centralized system. This technology helps the SC players to control and share data [6]. If the blockchain becomes so large, a risk of centralization exists that just a few nodes can process a block. This might lead to two blockchain systemic problems: centralizing a public directory such as bitcoin and slowing down the network [29]. Hence, this helps in risk reduction, which exists in the centralized system.

A typical BT-based SC consists of suppliers, manufacturers, distributors, retailers, end users, logistics services, airport, port, and banks which are a provider of financial services. In general, SC firms will shape consortia as vehicles to investigate the capability of BT because joint effort just as cost/hazard sharing is, for example, BT. The implementation of BT is not without challenges. The expected difficulties could be intra- or interorganizational hindrances (like the absence of expertise and knowledge, economic imperatives and data sharing issues), administrative uncertainties, energy utilization, deceptive practices and technological interoperability, and so on [30–32]. Regardless of the expanding exertion by researchers, empirical examination exploring how firms could plan a blockchain empowered SC stays restricted, and confirmations to help the guaranteed benefits are as yet deficient [33]. This research fills the gap by providing empirical evidence for the proposed model.

2.2 Technology Adoption in SC

In the current study, we have identified the determinants of BTA and its benefits on SC performance. There is a need to consider the theories on technology adoption for the literature foundation (Warshaw and Davis, 1985; Davis, 1989). Davis (1989) identified two constructs for predicting technology adoption and its usage at a single firm level. The two constructs are perceived usefulness (PU) and perceived ease of use (PEOU). Over the last three decades, different models were proposed which are based on this theory constructs [34–36].

TAM theory has been extended by [34]. Seven more theories were included on user behavior to get an influential model called the unified theory of acceptance and use of technology (UTAUT). It consists of four constructs: social influence, performance expectancy, facilitating conditions, and effort expectancy. Other variables like age, gender, the voluntariness of use, and experience act as moderators in the model [34]. As a result, studies have utilized an advanced version of the initial UTAUT [37, 38].

TAM constructs have been used in the Indian perspective by [9] for understanding blockchain behavior. They expressed that PEOU is an indicator of PU, which accomplished a solid force of anticipating the expectation to utilize blockchain. Hence, as per the features of TAM and UTAUT, a model has been proposed in this study for BTA and its impact on SC performance. Also, [39] proposed adopting well-known TOE perspectives to examine the BTA in operations and SCM. They found that relative advantage, cost, complexity, and peer pressure significantly impact intention to BTA. Therefore, in the next section, we discuss the proposed research model and the development of the hypothesis using knowledge sharing, higher authority support, business partners' pressure, SC performance, and blockchain technology adoption (BTA) as a dependent variable.

3 Research Model and Development of Hypothesis

3.1 Knowledge Sharing (KS)

KS refers to the knowledge exchange between firms along with their SC players. With the help of BT, the players of the same SC can exchange information and improve traceability [40]. It also includes skills and best practices on the utilization of various SCM processes. KS is concerned with individual behavior while sharing information within the firms [41–43]. If the knowledge is being shared between the players, it will help make the SC more efficient and create transparency in the system. Hence, KS between the partners of firms in the same SC is a critical determinant in BTA. Hence, the proposed hypothesis is:

- H1: KS influences BTA.

3.2 Higher Authority Support (HAS)

HAS has a significant role in accepting and implementing new technologies in a firm. Suppose the higher authority individuals are aware of the benefits of BTA in SCM and support the transition to this new technology in the firm by creating a positive climate within the firm and its staff. In that case, this will help in removing the resistance and get ready to adopt the new technology [12, 15, 21, 44–47]. As BTA in a firm requires allocating human and financial resources, integrating BT with existing IT infrastructures, and BPR in client and supplier relationship management [48]. Hence, HAS is considered as a determinant in BTA. Therefore, the proposed hypothesis is:

- H2: HAS influences BTA.

3.3 Business Partner's Pressure (BPP)

BPP refers to the pressure faced by firms from its business partners [49] and has a critical impact on advanced technology adoption. There is a need to have supply chain collaboration for integrating BT in SCM systems. Suppose a business partner dominating the SC decides to adopt BT to manage SC for cooperating efficiently. In that case, other SC partners also have to adopt BT to maintain the trade relations [21, 48, 50]. A business partner's relationship is a critical element. When we consider the SC perspective, the relations tend to be more complex, and BPP can optimize a firm's capabilities. Also, BPP can impact BTA, and the pressures can come from other stakeholders and trade partners, all capable of adopting BT. BPP has been a critical factor in BTA in SCM in prior studies [14, 40]. Hence, BPP has been considered as an indicator in the current study.

- H3: BPP influences BTA.

3.4 BT and SC Performance (SCP)

Every day there is an exchange of data between the SC networks. With increased complexity (like asymmetry information and the amount of available technology), SC performance enhancement is enhanced. In these circumstances, BT will prove to be very fruitful for improving operations and SC performances; this will also contribute to the revenue generation of a business [51, 52]. This advanced technology will be playing a critical role in solving various challenges like trust and transparency between SC members [53, 54]. As BT improves traceability, there is a gain of transparency and accountability on all members positively. BT can also eliminate the variability of information in SC. As a result, cooperation and trust will improve SC performance. Hence, the proposed hypothesis is:

- H4: BT influences SC performance.

4 Research Methodology

The objective of this study is to examine the BTA for improving SC performance. Secondary and primary sources collected data. Secondary sources include a literature review and other reports, and the primary source has the collection of data through a structured questionnaire. The reliability test of the questionnaire was also done. The target population was SC professionals working in various industries running in India. Multinational companies and listed companies on stock exchange were set as the target population. IT service providers were excluded from the targeted population. The respondents from the selected firms were the IT workforce and officers who have IT information on their firms' present and future tasks. The stratified random sampling method has been used to choose samples from various subsets of populations [55]. After data cleaning in SPSS 20.0, the usable responses used for the analysis were 285 out of 850 targeted professionals who agreed to participate in the survey. Hence, 33.52% was the response rate.

To avoid a common method, bias on the research team has taken few fundamental precautions during the pre-data collection stage. A note was mentioned at the beginning of the questionnaire that indicated the survey is intended for academic research, and confidentiality of data will be maintained. In the gathered dataset, the first cleansing was finished by case screening, trailed by factor screening to clarify variations in the information. Information cleaning measure had been reasoned that missing information had been extraordinarily sparse, and in this way, they were not viewed as a principal supporter of any predisposition. No cases were therefore removed. However, after the data is collected, the research team applied Harman's single factor test. Exploratory factor analysis was performed, and the results show that the first factor explains maximum covariance (32.453%), which is below the recommended value of 50% [56].

SEM was adopted for data analysis. The data analysis was done in four stages: demographics of firms, reliability and validity test, exploratory factor analysis (EFA), confirmatory factor analysis (CFA), and structural equation modeling (SEM). EFA was done to check the total variance explained to identify and group the variables using a rotated component matrix table. SPSS 20.0 was utilized for reliability tests and EFA on data collected. After that, CFA was implemented for testing and approving the model. AMOS 22.0 was used for CFA on gathered data to estimate model results as CFA chooses whether a legitimacy test on an expected model is duplicated [57, 58]. At last, the model fit was determined by SEM for testing of hypothesis.

5 Results

The following section displays output obtained from the performed analysis. First, the analysis of demographics has been displayed in Table 1, followed by reliability and validity measures along with EFA. Thereafter, the model validity measures were calculated which shows the values for composite reliability, convergent and divergent validity measures for the final SEM model. Finally, the model fit measures are displayed which compares the values for model 1 (CFA) and the final model (SEM).

5.1 Demographics of Firms Surveyed

A questionnaire-based survey method was used. Table 1 shows the distribution of respondents based on different industries. The majority of respondents were male (82%), polytechnic level education (52.31%), work experience 6–10 years (40.10%), and healthcare segment (33.42%).

Table 1 Firm demographics

Gender	Percentage
Male	82%
Female	18%
Educational qualification	
Secondary	6%
Polytechnic	52.31%
Bachelor's degree	29%
PG/PhD	12.69%
Work experience	
<5 years	7.80%
6–10 years	40.10%
11–15 years	35.57%
>15 years	16.53%
Industry	
Hotel industry	21.34%
Manufacturing	20.67%
IT service	8.44%
Healthcare	33.42%
Retail	16.13%

5.2 Reliability and Validity

5.2.1 Cronbach's Alpha (α)

Assessment of reliability helps examine the degree of internal consistency between variable measurement items and its freedom of error at any point in time [59]. α-value was utilized to test the reliability of the data for all the constructs as it is the most common measurement method. The values for all the scales must be the above-recommended level of 0.70 [60]. Utilization of 7-point Likert scale was done in preparing the structured questionnaire. For analyzing the information collected, SPSS 20.0 and AMOS 22.0 were used. The latent variable KM has four indicators, KM1, KM2, KM3, and KM4, and its α-value is 0.849; BPP has four indicators, BPP1, BPP2, BPP3, and BPP4, and its α-value is 0.882; HAS has three indicators, HAS1, HAS2, and HAS3, and its α-value is 0.848; BTA has four indicators, BTA1, BTA2, BTA3, and BTA4. Hence, all the values are within the threshold level (Hair et al., 2014), and the 15 components are utilized in further analysis.

5.3 Exploratory Factor Analysis

The first step of the EFA was to evaluate the appropriateness of the sample size. SPSS 20.0 was utilized for EFA. The correlations between its items had been inspected using Bartlett's test of sphericity [61]. Principal component analysis

Table 2 KMO and Bartlett's test

KMO and Bartlett's test		
Kaiser-Meyer-Olkin measure of sampling adequacy		.778
Bartlett's test of sphericity	Approx. Chi-square	2624.257
	df	105
	Sig.	0.000

was performed to identify meaningful bias and express the same qualities. For the interpretation of initial results, the varimax rotation has been utilized; it is assumed (based on the relevant literature) that there does not exist any correlation within factors [61]. With this test, the statistic had generated that should have been significant ($p < 0.05$) for EFA has been considered as an appropriate technique [61].

As a result, Kaiser-Meyer-Olkin (KMO) test was utilized to quantify whether those items are sufficiently correlated and determine whether a factor analysis could be performed. KMO value for the current research is 0.778. The minimum level set for this statistic is 0.60 [55]. The significance value is 0.000, which is less than 0.05, i.e., the probability value level acceptable. Table 2 displays the KMO and Bartlett's test.

The extraction method used was principal component analysis. Only the eigenvalues which have values greater than one were extracted as it explains maximum variance. For the components, the percentage of total variance is explained by component 1 (20.028%), component 2 (18.502%), component 3 (18.409%), and component 4 (15.616%). The cumulative percentage of total variance explained by all three components is 72.553%. Table 3 displays the total variance explained.

The rotated component matrix is important for interpreting the results of the analysis. Rotation helps in grouping the items, and each group contains more than two items, which simplifies the structure. Hence, this is the aim of the goal of rotation. In this research, we have achieved this aim. This helps to identify the cross-loadings on more than one group, and then it can be corrected by removing those that are cross-loaded. In this research, the loadings having less than |.40| are suppressed because loadings of more than |.40| are typically high. So, in the end, we achieve a simple structure. Eleven total variables were grouped under three different components. The rotation method used was varimax rotation. BPP1, BPP2, BPP3, and BPP4 are grouped under the first component with values of 0.825, 0.832, 0.859, and 0.833. KS1, KS2, KS3, and KS4 are grouped under the second component having values 0. 0.817, 0.828, 0.783, and 0.670. SCP1, SCP2, SCP3, and SCP4 are grouped under the third component with values 0.702, 0.768, 0.813, and 0.720. HAS1, HAS2, and HAS3 are grouped under the fourth component with values 0.855, 0.891, and 0.777. Table 4 shows the rotated component matrix output.

Confirmatory factor analysis (CFA) was performed in the next stage, which constructs identified from the literature survey can be tested and how well the variables represent the constructs. Structural equation modeling (SEM) was used for testing the model fit of the proposed research model [57]. When their instrument

Table 3 Total variance explained

Component	Initial eigenvalues			Extraction sums of squared loadings			Rotation sums of squared loadings		
	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %
1	5.887	39.245	39.245	5.887	39.245	39.245	3.004	20.028	20.028
2	2.221	14.806	54.051	2.221	14.806	54.051	2.775	18.502	38.529
3	1.619	10.791	64.842	1.619	10.791	64.842	2.761	18.407	56.936
4	1.157	7.711	72.553	1.157	7.711	72.553	2.342	15.616	72.553

Table 4 Rotated component matrix

	Component			
	1	2	3	4
KS1		.817		
KS2		.828		
KS3		.783		
KS4		.670		
BPP1	.825			
BPP2	.832			
BPP3	.859			
BPP4	.833			
HAS1				.855
HAS2				.891
HAS3				.777
SCP1			.702	
SCP2			.768	
SCP3			.813	
SCP4			.720	

Extraction method: Principal component analysis
Rotation method: Varimax with Kaiser normalization

Rotation converged in five iterations

shows the typical structures inside, this could have been demonstrative to construct validity (CV) [62] and, explicitly, factorial validity.

5.4 *Model Validity Measures*

5.4.1 Composite Reliability

Composite reliability (CR) was also measured for all the components. It is calculated for internal consistency reliability because of its ability to provide better results [63]. The construct KS has a CR value of 0.828; BPP has a CR value of 0.828; and HAS has a CR value of 0.791. Three constructs are >0.7, which indicates that the composite reliability measures are reliable [64]. Table 4 displays the CR values.

5.4.2 Convergent Validity

It is measured with the help of the average variance extracted (AVE). As per [65], AVE is >0.5 for the convergent validity. Table 4 represents AVE values for the constructs. All the values are greater than 0.5, satisfying convergent validity for all the constructs [61].

Table 5 Master validity output

	CR	AVE	MSV	MaxR(H)	KS	BPP	HAS	BTA
KS	0.853	0.596	0.288	0.876	**0.772**			
BPP	0.877	0.643	0.145	0.908	0.327***	**0.802**		
HAS	0.85	0.654	0.24	0.859	0.412***	0.274***	**0.809**	
BTA	0.871	0.633	0.288	0.906	0.536***	0.381***	0.490***	**0.795**

Significance of Correlations:
†$p < 0.100$
$p < 0.050$; **$p < 0.010$; ***$p < 0.001$

5.4.3 Divergent Validity

To calculate this validity, [65] suggested that the AVE of the construct must be more than a square of the correlation between that construct and the other constructs [61]. Table 5 represents the values for divergent validity output (MSV < AVE), and it was obtained using the master validity plugin in AMOS 22.0.

5.5 Structural Model and Testing of Hypothesis

The model fit measures for model 1 (CFA), which has the latent variables, are shown in Table 6. The latent variables along with its indicators are KS, knowledge sharing, along with four indicators, KS1, KS2, KS3, and KS4; BPP, business partners' pressure, has four indicators, BPP1, BPP2, BPP3, and BPP4; and HAS, higher authority support, has three indicators, HAS1, HAS2, and HAS3. The CMIN/Df is 5.710; goodness-of-fit indices (GFI) is 0.847; comparative fit index (CFI) is 0.851; Tucker-Lewis Index (TLI) is 0.782; incremental fit index (IFI) is 0.852, parsimony comparative fit index (PCFI) is 0.608, and parsimony normed fit index (PNFI) is 0.661. All the items' loading was greater than 0.5 and SE < ± 2.5, which is acceptable.

To test the hypothesis, SEM was used [57]. AMOS 22.0 was utilized for this research because of its powerful graphic representations and user-friendly interfaces. The results of the model are shown here. Figure 1 represents the final model and the latent variables and their indicators and dependent variable. The latent variables along with its indicators are KS, knowledge sharing, along with four indicators, KS1, KS2, KS3, and KS4; BPP, business partners' pressure, has four indicators, BPP1, BPP2, BPP3, and BPP4; HAS, higher authority support, has three indicators, HAS1, HAS2, and HAS3; and BTA, blockchain technology analytics, has four indicators BTA1, BTA2, BTA3, and BTA4. The dependent variable is SCP, supply chain performance, with four indicators, SCP1, SCP2, SCP3, and SCP4.

Table 5 shows the model fit values and fit indices. For the final model, the value of chi-square is 699.971, and the degree of freedom is 145. The estimations of absolute fit indices are CMIN/Df is 4.827, CMIN represents the chi-square value, and Df

Table 6 Final goodness-of-fit indices for the CFA and structural model

Goodness-of-fit indices	Model 1	Final model	Benchmark
CMIN/Df	5.710	4.827	Lower limit:1.0; upper limit 2.0/3.0 or 5.0
GFI	0.847	0.819	>0.80
Absolute badness-of-fit measure			
RMSEA	0.129	0.08	⩽0.08
Incremental fit measure			
CFI	0.851	0.838	⩾0.80
IFI	0.852	0.839	⩾0.80
TLI	0.782	0.809	⩾0.80
Parsimony fit measure			
PCFI	0.680	0.710	⩾0.50
PNFI	0.661	0.683	⩾0.50

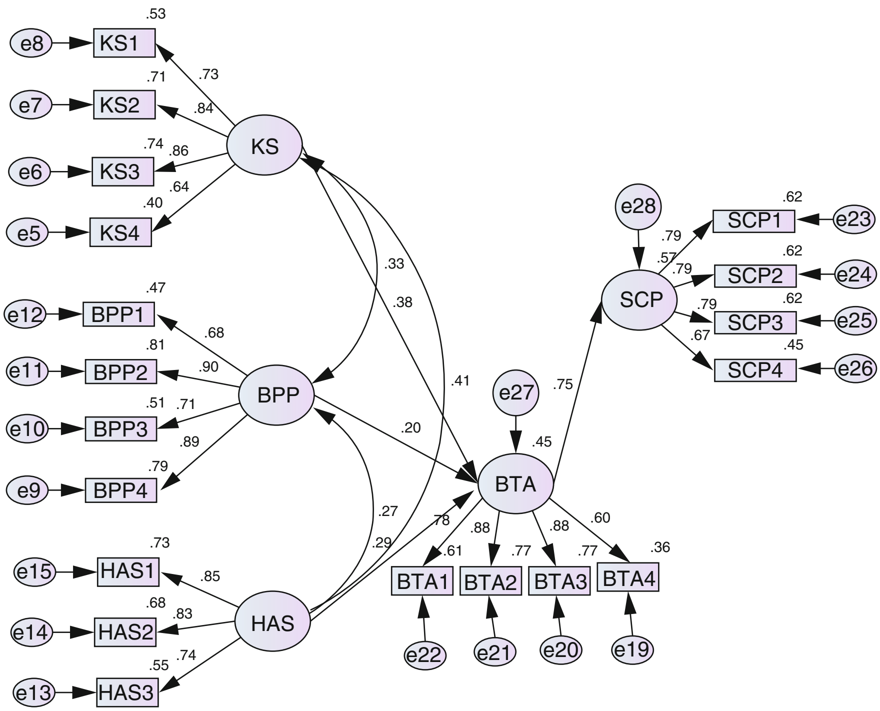


Fig. 1 Blockchain technology adoption model for improving SC performance

represents the degree of freedom, and the value is less than 5, which is the accepted threshold value [66]. The goodness-of-fit index (GFI) value is 0.819, and root mean square error of approximation (RMSEA) value is 0.08, within the threshold value of 0.08. The comparative fit index (CFI) is 0.838; incremental fit index (IFI) is 0.839;

Table 7 Structural model results

	Estimate	SE.	CR.	*P*
BTA < —HAS	0.222	0.052	4.294	***
BTA < —BPP	0.149	0.044	3.36	***
BTA < —KS	0.432	0.084	5.138	***
SCP < —BTA	0.893	0.105	8.508	***

Tucker-Lewis Index (TLI) is 0.809; parsimony comparative of fit index (PCFI) is 0.710; and parsimony normed of fit index (PNFI) is 0.683 which are having values in the threshold level and are acceptable [67]. Figure 1 shows the final structural model generated after analysis in AMOS 22.0.

Hence, we can see that the model fit values of the final model are better than model 1. The mediating variable (BTA) and dependent variable significantly contribute to the three latent variables in establishing the model fit.

Table 7 shows the path estimate analysis results. The result demonstrates the three hypotheses are supported by P-value [64]. Hence, three factors, TP, OP, and EP, have a positive impact on BTA. The square multiple correlations (R^2) help measure how well a regression line estimates the real data points between 0 and 1, which states how well one variable predicts another [64]. The more the value is closer to 1, the better is the model's ability to predict that technology [59]. The proposed model can explain 45% variance in BT adoption and 57% of the variance in SC performance. Hence, the mediating variable (BTA) plays a critical role in establishing the model fit.

6 Discussion

The current study empirically examined the role of the adoption of blockchain technology in supply chain performance. The study also contributed toward the literature of BT and SCM and increased the understanding. Further, structural equation modeling was used for testing the hypothesis. Three hypotheses were proposed for testing the model, and all were found to be significant which is in line with previous literature on adoption of innovation.

KS comprised of four indicators, and all four indicators contributed significantly toward the model fit. The first hypothesis (H1) examined the impact of knowledge sharing on blockchain technology adoption. The second hypothesis (H2) examined the impact of higher authority support on blockchain technology adoption, and the third hypothesis (H3) examined the impact of business partner's pressure on blockchain technology adoption. The validation of all the three constructs is applied in BTA. KS has been a significant contributor in electronic SCM (Lin 2017) but is not related to BT. HAS has been found as a significant contributor in cloud computing adoption studies [21, 50, 68–70] in various segments like SMEs, healthcare, manufacturing, etc. BPP has been found as a significant contributor, which is in line with previous kinds of literature [5, 6, 13, 47, 71]. Hence, in the current study, also the three latent variables contribute significantly toward the model fit. The estimate of KS ($\beta = .432$, $p = .000$), BPP ($\beta = .149$, $p = .000$), and HAS ($\beta = .222$, $p = .000$) is positive, and hence we can conclude that they have significantly positive impact on BTA.

BTA act as a mediating variable. The fourth hypothesis (H4) examined the impact of BTA in SC performance. Also, the prior studies [14, 15, 72–74] were unable to demonstrate transparency in BT on SC performance. But in the current study, BTA impacts SC performance, and the dependent variable SC performance explains 57% of the variance. Hence, the current research helped in adding value to the existing works of literature [20, 75–78].

Also, our results are providing empirical evidence to the findings of the advantages of BTA in SCs [79]. The prior literature talks about BT's adoption increases transparency, privacy and decreases the cost of the SC process. The HAS, KS, and BPP are also described in prior works of literature and discussed their benefits and roles. Hence, in the current study, we provided empirical evidence for the same.

6.1 Managerial Implications

The current study will be helping managers to decide on adopting BT for improving the SC performance. The managers should have in-depth knowledge about the new technology and also about its consequences after its adoption. The latent variables knowledge sharing, business partners' pressure, and higher authority support have significantly contributed to BTA in India. Also, BTA has acted upon as mediating variable and serves as a significant contributor toward improving SC performance and achieving the overall model fit. As per prior studies [23, 80, 81], this study also reports that knowledge is an essential resource for increasing performance. If the managers of various firms develop their knowledge and understanding of BTA in SC performance, they will play a critical role in supporting multiple firm operations.

6.2 Theoretical Contribution, Scope, and Future Research

The current study discussed the BTA and SC performance with a proposed research model. The results validated the theoretical model empirically also. From the output, it is concluded that BTA influences positively on SC performance. Also, the proposed three latent variables contributed positively toward the mediating variable (BTA) and the overall model fit. Also, theoretically, we can say that SC performance can be predicted with the help of few constructs. BT is in the infant stage, but its contribution to SC performance cannot be neglected.

Future studies can be conducted to test the proposed research model in various other developing countries and particular sectors to validate the outcomes.

7 Conclusion

This study aims to identify variables from literature review and propose a research model for BTA, which will ultimately help in SC performance. The proposed model in the present study was supported by the results, which were obtained empirically. These results are in line with the literature, which also included the improvement in SC performances. Also, this study helped us to verify the results empirically and highlighted the advantages of BTA for improving SC performance. The results also contributed toward the theoretical and managerial contributions on BTA. It further motivates the managers to understand the relation between BTA and SCM. Also, scholars can perform more research in this area in various sectors.

Appendix A. Measurement Items

Constructs	Labels	Measures	Sources
KS	KS1	The firm shares blockchain-enabled SC knowledge with its partners	
	KS2	Firm shares market and BT knowledge to SC partners	
	KS3	The firm has enough trust in sharing knowledge with its partners	
	KS4	Knowledge sharing helps in business planning	
BPP	BPP1	The partners enable BT implementation	[82]
	BPP2	Partners are interested in adopting BT	
	BPP3	Partners recommend the implementation of BT	
	BPP4	Partners encouraged the implementation of BT in SC	
HAS	HAS1	A higher authority is interested in adopting BT	[46]
	HAS2	The higher authority has enough knowledge regarding these new technologies	
	HAS3	Higher authority motivates the staff to change from traditional system to advanced technology	
BTA	BTA1	The firm is ready to invest in new advanced technologies	[83]
	BTA2	The firm requires the use of BT for efficiency	
	BTA3	BT will help in providing transparency in the SC process	[11, 12]
	BTA4	BT will enable cost reduction	
SCP	SCP1	BT can improvise the linkage of physical goods to bar codes, serial numbers, etc.	[12, 84]
	SCP2	BT adoption improves the efficiency of the SC process	
	SCP3	BT adoption helps to verify the assigned tasks	
	SCP4	SC can handle the quick introduction of new products	

References

1. Monfared, R. (2016). *Blockchain ready manufacturing supply chain using a distributed ledger*. Accessed 06 Mar 2021. [Online]. Available: http://esatjournals.net/ijret/2016v05/i09/IJRET20160509001.pdfMetadataRecord: https://dspace.lboro.ac.uk/2134/22625.
2. Dolgui, A., Ivanov, D., Potryasaev, S., Sokolov, B., Ivanova, M., & Werner, F. (2020). Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain. *International Journal of Production Research, 58*(7), 2184–2199. https://doi.org/10.1080/00207543.2019.1627439
3. Sunny, J., Undralla, N., & Madhusudanan Pillai, V. (2020). Supply chain transparency through blockchain-based traceability: An overview with demonstration. *Computers & Industrial Engineering*, *150*.https://doi.org/10.1016/j.cie.2020.106895.
4. Ikeda, K., & Hamid, M. N. (2018). Applications of blockchain in the financial sector and a peer-to-peer global barter web. In *Advances in computers* (Vol. 111, pp. 99–120). Academic Press Inc..
5. Aslam, J., Saleem, A., Khan, N. T., & Kim, Y. B. (2021). Factors influencing blockchain adoption in supply chain management practices: A study based on the oil industry. *Journal of Innovation and Knowledge, 6*, 124. https://doi.org/10.1016/j.jik.2021.01.002
6. Tipmontian, Alcover, & Rajmohan. (2020). Impact of blockchain adoption for safe food supply chain management through system dynamics approach from management perspectives in Thailand. *Proceedings, 39*(1), 14. https://doi.org/10.3390/proceedings2019039014
7. Tan, B., Yan, J., Chen, S., & Liu, X. (2018). The impact of blockchain on food supply chain: The case of walmart. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 11373 LNCS, pp. 167–177). https://doi.org/10.1007/978-3-030-05764-0_18.
8. Dutta, P., Choi, T. M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation Research Part E: Logistics and Transportation Review, 142*, 102067. https://doi.org/10.1016/j.tre.2020.102067
9. Kamble, S., Gunasekaran, A., & Arha, H. (2019). Understanding the Blockchain technology adoption in supply chains-Indian context. *International Journal of Production Research, 57*(7), 2009–2033. https://doi.org/10.1080/00207543.2018.1518610
10. Koh, L., Dolgui, A., & Sarkis, J. (2020). Blockchain in transport and logistics – Paradigms and transitions. *International Journal of Production Research, 58*(7), 2054–2062. https://doi.org/10.1080/00207543.2020.1736428
11. Alazab, M., Alhyari, S., Awajan, A., & Abdallah, A. B. (2020). Blockchain technology in supply chain management: An empirical study of the factors affecting user adoption/acceptance. *Cluster Computing, 24*(1), 83–101. https://doi.org/10.1007/s10586-020-03200-4
12. Fosso Wamba, S., Queiroz, M. M., & Trinchera, L. (2020). Dynamics between blockchain adoption determinants and supply chain performance: An empirical investigation. *International Journal of Production Economics, 229*, 107791. https://doi.org/10.1016/j.ijpe.2020.107791
13. Sheel, A., & Nath, V. (2019). Effect of blockchain technology adoption on supply chain adaptability, agility, alignment and performance. *Management Research Review, 42*(12), 1353–1374. https://doi.org/10.1108/MRR-12-2018-0490
14. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research, 57*(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261
15. Wong, L.-W., Tan, G. W.-H., Lee, V.-H., Ooi, K.-B., & Sohal, A. (2020). Unearthing the determinants of Blockchain adoption in supply chain management. *International Journal of Production Research, 58*(7), 2100–2123. https://doi.org/10.1080/00207543.2020.1730463
16. Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. *Supply Chain Management, 23*(6), 545–559. https://doi.org/10.1108/SCM-01-2018-0029

17. Queiroz, M. M., Telles, R., & Bonilla, S. H. (2019). Blockchain and supply chain management integration: a systematic review of the literature. *Supply Chain Management, 25*(2), 241–254. https://doi.org/10.1108/SCM-03-2018-0143
18. Yusof, H., et al.. (2018). Behavioral intention to adopt blockchain technology: Viewpoint of the banking institutions in Malaysia. *International Journal of Advanced Scientific Research and Management*, *3*. Accessed 06 Mar 2021. [Online]. Available: www.ijasrm.com.
19. Gokalp, E., Coban, S., & Gokalp, M. O. (2019). Acceptance of blockchain based supply chain management system: Research model proposal, https://doi.org/10.1109/UBMYK48245.2019.8965502.
20. Chang, J., Katehakis. M. N., Melamed, B., & Shi, J. (Junmin). (2018). Blockchain design for supply chain management. *SSRN Electronic Journal.*https://doi.org/10.2139/ssrn.3295440.
21. Gökalp, E., Gökalp, M. O., & Çoban, S. (2020). Blockchain-based supply chain management: Understanding the determinants of adoption in the context of organizations. *Information Systems Management*, 1–22. https://doi.org/10.1080/10580530.2020.1812014
22. Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications, 125*, 251–279. https://doi.org/10.1016/j.jnca.2018.10.019
23. Kouhizadeh, M., Saberi, S., & Sarkis, J. (2021). Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers. *International Journal of Production Economics, 231*, 107831. https://doi.org/10.1016/j.ijpe.2020.107831
24. Perboli, G., Musso, S., & Rosano, M. (2018). Blockchain in logistics and supply chain: A lean approach for designing real-world use cases. *IEEE Access, 6*, 62018–62028. https://doi.org/10.1109/ACCESS.2018.2875782
25. Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management, 49*, 114–129. https://doi.org/10.1016/j.ijinfomgt.2019.02.005
26. Fosso Wamba, S., Kala Kamdjoug, J. R., Epie Bawack, R., & Keogh, J. G. (2020). Bitcoin, Blockchain and Fintech: A systematic review and case studies in the supply chain. *Production Planning and Control, 31*(2–3), 115–142. https://doi.org/10.1080/09537287.2019.1631460
27. Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A survey on blockchain for information systems management and security. *Information Processing and Management, 58*(1), 102397. https://doi.org/10.1016/j.ipm.2020.102397
28. Banerjee, A. (2018). Blockchain technology: Supply chain insights from ERP. *Advances in Computers, 111*, 69–98.
29. Chang, Y., Iakovou, E., & Shi, W. (2020). Blockchain in global supply chains and cross border trade: A critical synthesis of the state-of-the-art, challenges and opportunities. *International Journal of Production Research, 58*(7), 2082–2099. https://doi.org/10.1080/00207543.2019.1651946
30. Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics, 35*(8), 2337–2354. https://doi.org/10.1016/j.tele.2018.10.004
31. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36*, 55–81. https://doi.org/10.1016/j.tele.2018.11.006
32. Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management, 39*, 80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005
33. Wang, Y., Han, J. H., & Beynon-Davies, P. (2019). Understanding blockchain technology for future supply chains: a systematic literature review and research agenda. *Supply Chain Management, 24*(1), 62–84. https://doi.org/10.1108/SCM-03-2018-0148
34. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly: Management Information Systems, 27*(3), 425–478. https://doi.org/10.2307/30036540

35. Venkatesh, V., & Zhang, X. (2010). Unified theory of acceptance and use of technology: US vs. China. *Journal of Global Information Technology Management, 13*(1), 5–27. https://doi.org/10.1080/1097198X.2010.10856507
36. Venkatesh, V., Thong, J. Y. L., Chan, F. K. Y., & Hu, P. J. H. (2016). Managing citizens' uncertainty in e-government services: The mediating and moderating roles of transparency and trust. *Information Systems Research, 27*(1), 87–111. https://doi.org/10.1287/ISRE.2015.0612
37. Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2019). Re-examining the unified theory of acceptance and use of technology (UTAUT): Towards a revised theoretical model. *Information Systems Frontiers, 21*(3), 719–734. https://doi.org/10.1007/s10796-017-9774-y
38. Dwivedi, Y. K., Rana, N. P., Janssen, M., Lal, B., Williams, M. D., & Clement, M. (2017). An empirical validation of a unified model of electronic government adoption (UMEGA). *Government Information Quarterly, 34*(2), 211–230. https://doi.org/10.1016/j.giq.2017.03.001
39. Wong, L. W., Leong, L. Y., Hew, J. J., Tan, G. W. H., & Ooi, K. B. (2020). Time to seize the digital evolution: Adoption of blockchain in operations and supply chain management among Malaysian SMEs. *International Journal of Information Management, 52*, 101997. https://doi.org/10.1016/j.ijinfomgt.2019.08.005
40. Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics, 2*(1), 2. https://doi.org/10.3390/logistics2010002
41. Low, C., Chen, Y., & Wu, M. (2011). Understanding the determinants of cloud computing adoption. *Industrial Management & Data Systems, 111*(7), 1006.
42. Puklavec, B., Oliveira, T., & Popovič, A. (2018). Understanding the determinants of business intelligence system adoption stages an empirical study of SMEs. *Industrial Management & Data Systems, 118*(1), 236–261. https://doi.org/10.1108/IMDS-05-2017-0170
43. Shahzad, F., Xiu, G. Y., Khan, I., Shahbaz, M., Riaz, M. U., & Abbas, A. (2020). The moderating role of intrinsic motivation in cloud computing adoption in online education in a developing country: A structural equation model. *Asia Pacific Education Review, 21*(1), 121–141. https://doi.org/10.1007/s12564-019-09611-2
44. Badr, F., Nasser, A.-A., & Jawad, M. S. (2019). Factors of cloud computing adoption by small and medium size enterprises (SMEs). *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, 7*(1), 2321–5526.
45. Shee, H., Miah, S. J., Fairfield, L., & Pujawan, N. (2018). The impact of cloud-enabled process integration on supply chain performance and firm sustainability: The moderating role of top management. *Supply Chain Management, 23*(6), 500–517. https://doi.org/10.1108/SCM-09-2017-0309
46. Senyo, P. K., Effah, J., & Addae, E. (2016). Preliminary insight into cloud computing adoption in a developing country. *Journal of Enterprise Information Management, 29*(4), 505–524. https://doi.org/10.1108/JEIM-09-2014-0094
47. 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. https://doi.org/10.1016/j.ijinfomgt.2019.102064
48. Alshamaila, Y., et al. (2013). The usage and adoption of cloud computing by small and medium businesses. *International Journal of Information Management, 33*(5), 861–874. https://doi.org/10.7753/ijcatr0205.1003
49. Alharbi, F., Atkins, A., & Stanier, C. (2016). Understanding the determinants of cloud computing adoption in Saudi healthcare organisations. *Complex & Intelligent Systems, 2*(3), 155–171. https://doi.org/10.1007/s40747-016-0021-9
50. Kumar, A., & Krishnamoorthy, B. (2020). Business analytics adoption in firms: A qualitative study elaborating TOE framework in India. *International Journal of Global Business and Competitiveness, 15*(2), 80–93. https://doi.org/10.1007/s42943-020-00013-5
51. Ramaswamy, H. G. H. D. R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *Journal of Enterprise Information Management, 28*(1), 107–130.

52. Nam, K., Dutt, C. S., Chathoth, P., Daghfous, A., & Khan, M. S. (2020). The adoption of artificial intelligence and robotics in the hotel industry: Prospects and challenges. *Electronic Markets, 31*, 553. https://doi.org/10.1007/s12525-020-00442-3
53. Amini, M., & Bakri, A. (2015). Cloud computing adoption by SMEs in the Malaysia: A multi-perspective framework based on DOI theory and TOE framework. *Journal of Information Technology & Information Systems Research, 9*(2), 121–135.
54. Mrhaouarh, I., Okar, C., Namir, A., & Chafiq, N. (2018). Cloud computing adoption in developing countries: A systematic literature review. *2018 IEEE International Conference on Technology Management, Operations and Decisions, 2018*, 73–79. https://doi.org/10.1109/ITMC.2018.8691295
55. Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European Business Review, 26*(2), 106–121. https://doi.org/10.1108/EBR-10-2013-0128
56. Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology, 885*(879), 10–1037.
57. Byrne, B. M. (2013). *Structural equation modeling with Mplus*. https://doi.org/10.4324/9780203807644.
58. Hair, J. F., Sarstedt, M., Pieper, T. M., & Ringle, C. M. (2012). The use of partial least squares structural equation modeling in strategic management research: A review of past practices and recommendations for future applications. *Long Range Planning, 45*(5–6), 320–340. https://doi.org/10.1016/j.lrp.2012.09.008
59. Kline, R. B. (2015). *Principles and practice of structural equation modeling*. Guilford Publications.
60. Nunnally, J. C. (1994). *Psychometric theory 3E*. Tata McGraw-Hill Education.
61. Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2010). *Multivariate data analysis* (7th ed.). Prentice Hall.
62. Moerdyk, A. (2009). *The principles and practice of psychological assessment*. Van Schaik.
63. Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. *Advances in International Marketing, 20*, 277–319.
64. Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science, 40*(3), 414–433. https://doi.org/10.1007/s11747-011-0261-6
65. Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.1177/002224378101800104
66. Cable, D. M., & DeRue, D. S. (2002). The convergent and discriminant validity of subjective fit perceptions. *The Journal of Applied Psychology, 87*(5), 875–884. https://doi.org/10.1037/0021-9010.87.5.875
67. Byrne, B. M. (2001). Structural equation modeling with AMOS, EQS, and LISREL: Comparative approaches to testing for the factorial validity of a measuring instrument. *International Journal of Testing, 1*(1), 55–86. https://doi.org/10.1207/s15327574ijt0101_4
68. Alkhater, N., Walters, R., & Wills, G. (2018). An empirical study of factors influencing cloud adoption among private sector organisations. *Telematics and Informatics, 35*(1), 38–54. https://doi.org/10.1016/j.tele.2017.09.017
69. Maroufkhani, P., Wan Ismail, W. K., & Ghobakhloo, M. (2020). Big data analytics adoption model for small and medium enterprises. *Journal of Science and Technology Policy Management, 11*(2), 171–201. https://doi.org/10.1108/JSTPM-02-2020-0018
70. Tashkandi, A. A., & Al-Jabri, I. (2015). Cloud computing adoption by higher education institutions in Saudi Arabia: Analysis based on TOE. *International Conference on Cloud Computing, 2015*, 1–8. https://doi.org/10.1109/CLOUDCOMP.2015.7149634
71. Yadav, V. S., Singh, A. R., Raut, R. D., & Govindarajan, U. H. (2020). Blockchain technology adoption barriers in the Indian agricultural supply chain: An integrated approach. *Resources, Conservation and Recycling, 161*, 104877. https://doi.org/10.1016/j.resconrec.2020.104877

72. Saurabh, S., & Dey, K. (2021). Blockchain technology adoption, architecture, and sustainable agri-food supply chains. *Journal of Cleaner Production, 284*, 124731. https://doi.org/10.1016/j.jclepro.2020.124731
73. Di Vaio, A., & Varriale, L. (2020). Blockchain technology in supply chain management for sustainable performance: Evidence from the airport industry. *International Journal of Information Management, 52*, 102014. https://doi.org/10.1016/j.ijinfomgt.2019.09.010
74. Queiroz, M. M., Fosso Wamba, S., De Bourmont, M., & Telles, R. (2020). Blockchain adoption in operations and supply chain management: Empirical evidence from an emerging economy. *International Journal of Production Research*. https://doi.org/10.1080/00207543.2020.1803511
75. Durach, C. F., Blesik, T., Düring, M., & Bick, M. (2020). Blockchain applications in supply chain transactions. *Journal of Business Logistics, 42*, 12238. https://doi.org/10.1111/jbl.12238
76. Wu, H., et al. (2019). Data management in supply chain using blockchain: Challenges and a case study. In *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, 2019. https://doi.org/10.1109/ICCCN.2019.8846964.
77. Dwivedi, S. K., Amin, R., & Vollala, S. (2020). Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism. *Journal of Information Security and Applications, 54*, 102554. https://doi.org/10.1016/j.jisa.2020.102554
78. Tönnissen, S., & Teuteberg, F. (2018). Using blockchain technology for business processes in purchasing − Concept and case study-based evidence. *Lecture Notes in Business Information Processing, 320*, 253–264. https://doi.org/10.1007/978-3-319-93931-5_18
79. 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. https://doi.org/10.1080/00207543.2019.1708989
80. Holotiuk, F., & Moormann, J. (2018). Organizational adoption of digital innovation: The case of blockchain technology. *Research Paper.* Accessed 06 Mar 2021. [Online]. Available: https://aisel.aisnet.org/ecis2018_rp/202.
81. Wang, Z., Wang, T., Hu, H., Gong, J., Ren, X., & Xiao, Q. (2020). Blockchain-based framework for improving supply chain traceability and information sharing in precast construction. *Automation in Construction, 111*, 103063. https://doi.org/10.1016/j.autcon.2019.103063
82. Hwang, Y., Lin, H., & Shin, D. (2018). Knowledge system commitment and knowledge sharing intention: The role of personal information management motivation. *International Journal of Information Management, 39*, 220–227. https://doi.org/10.1016/J.IJINFOMGT.2017.12.009
83. Martins, R., Oliveira, T., & Thomas, M. A. (2016). An empirical analysis to assess the determinants of SaaS diffusion in firms. *Computers in Human Behavior, 62*, 19–33. https://doi.org/10.1016/j.chb.2016.03.049
84. Risius, M., & Spohrer, K. (2017). A blockchain research framework: What we (don't) know, where we go from here, and how we will get there. *Business and Information Systems Engineering, 59*(6), 385–409. https://doi.org/10.1007/s12599-017-0506-0

Revisiting Trust in Supply Chains: How Does Blockchain Redefine Trust?

Warwick Powell, Shoufeng Cao, Marcus Foth, Shan He, Charles Turner-Morris, and Ming Li

1 Introduction

> To give a name to a thing is as gratifying as giving a name to an island, but it is also dangerous: the danger consists in one's becoming convinced that all is taken care of and that once named, the phenomenon has also been explained. – Primo Levi

> What is needed is an electronic payment system based on cryptography instead of trust ... – Satoshi Nakamoto

The idea of trust is often emphasised in the competitive business environment where information asymmetry is a common issue. The emergence and adoption of new technologies, such as blockchain, has seen an often unreflective and uncritical emphasis on the idea of trust in business landscapes. Yet, the invocation of the idea

W. Powell
QUT Design Lab, Queensland University of Technology, Brisbane, QLD, Australia

BeefLedger Ltd, Brisbane, QLD, Australia

S. Cao (✉) · M Foth
QUT Design Lab, Queensland University of Technology, Brisbane, QLD, Australia
e-mail: shoufeng.cao@qut.edu.au

S. He
School of Chemistry and Chemical Engineering, Guangzhou University, Guangzhou, China

College of Science and Engineering, Flinders University, Adelaide, SA, Australia

C. Turner-Morris
BeefLedger Ltd, Brisbane, QLD, Australia

M. Li
Shanghai Key Laboratory of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai, China

China Electronics Standardization Institute, Beijing, China

A. Bouras et al. (eds.), *Blockchain Driven Supply Chains and Enterprise Information Systems*, https://doi.org/10.1007/978-3-030-96154-1_2

of trust creates the need to conceptually revisit it and critically explore its effects on transactions so as to (i) better redefine trust, (ii) when it does and does not matter and (iii) how this relates to the core properties of blockchain technologies in the context of supply chains. Our reading of the academic literature, industry whitepapers and the mainstream press suggests that trust and blockchain technology are concepts that are often used almost interchangeably. Following the definition of blockchain as a 'trust machine' by *The Economist* magazine in 2016, blockchain is widely taken as a trust solution in many areas, including pharmaceuticals [1, 2], food [3–7], gemstones [8], intellectual property and other digital artefacts [9–11], identity registries [12] and financial applications [13–15]. Yet, it has an implicit 'taken for granted' character when it comes to the trust affordances of blockchain technologies.

Despite the prevalence of the trust trope in blockchain discourse, and its frequent invocation in the application case of supply chains, there is little by way of explicit investigation of what is really meant by trust, and whether in fact it matters at all, and if it does matter, under what conditions. The quotes at the beginning of this chapter go to these two points, which underpin this chapter's argument. In the first quote, Primo Levi warns that naming something is gratifying but dangerous, because we run the risk that the act of naming is confused with understanding. The ad hominem invocation of 'trust' whenever blockchain technology and its (claimed) virtues in supply chains are discussed is symptomatic of this move. The second quote is from the original Satoshi Nakamoto Bitcoin white paper [16]. Nakamoto proposed a solution to the double-spending problem in decentralised digital payment systems, which at their heart, sought to obviate the need for a trusted party (understood as an intermediating role between parties to a transaction or exchange) while protecting the system from double-spending. As the quote makes clear, the design of the Bitcoin blockchain architecture – a combination of cryptography and economics – was to replace trust with cryptography. Nakamoto's intervention was not about a 'trust machine' at all; it was about how to enable the exchange of digital value to function reliably without trust presuppositions. Nakamoto concluded the white paper by saying:

> We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. [Emphasis added]

It seems that in much of the discourse since Nakamoto, the word 'instead', in the first quote above, has all but been forgotten. As for the explicit conclusion that the Bitcoin blockchain enables electronic transactions without relying on trust, this too has largely been ignored in the burgeoning supply chain and blockchain literature.

While many studies argued that blockchain creates trust between supply chain partners by ensuring information sharing in an immutable and secure manner [4], others claimed that trust is a necessary precondition for information sharing between companies [17]. This chapter focuses the discussion of trust and blockchain on the food supply chain that is mostly operated with trust-based relationships [18–20].

Batwa and Norrman [21] argue that 'a lack of agreement remains regarding what constitutes trust, and there is no generally accepted definition' (p. 205). In response, this chapter follows on from Levi's cautionary note and aims to recapture some conceptual clarity around the trust concept associated with blockchain technologies and supply chains. The contribution of this chapter is threefold: (i) we discuss what is trust from both the perspective of human relationships and business transactions and posit that blockchain cannot guarantee absolute trust, although it is widely perceived as a trust mechanism; (ii) we present how blockchain can contribute to supply chains beyond the trust assumption based on our learnings from a blockchain use case in food supply chains; and (iii) we reflect how blockchain technology-mediated features can redefine supply chain trust in a broad sense by comparing the rise of technology-enabled social commerce in China.

Section 2 offers a critical review of the blockchain-trust trope in the literature, which develops an approach to understanding trust as distinct from other types of relationships that people are involved in. This is followed by a discussion of the role of blockchain in supply chains in Sect. 3. After presenting our real-life learnings and reflections from an applied use case of blockchain in the beef supply chain in Sect. 4, we reflect on these general themes and their relevance to trust in supply chain environments in Sect. 5. Finally, Sect. 6 concludes this chapter with synthesised results and implications.

2 Trust and Blockchain

The blockchain literature is replete with references to trust. Yet, there is little reflection on what is meant by the idea. Indeed, the various ways in which 'trust' is enlisted in discussions about blockchains lead to less clarity and more confusion. This section explores how we can understand trust from both a human relationship and a business context. On this basis, the blockchain-trust trope is discussed.

2.1 What Is Trust?

Despite the frequent invocation of trust in the blockchain literature, there is little explicit contemplation of trust *tout court*. The same cannot be said for the wider philosophical, psychological and to some extent, the economic literature. Much of the literature presupposes trust to be some form of attribute, either a subjective one, which resides in the minds of actors, often thought of as a stance or an attitude (I trust so-and-so, suggesting that trust is an attribute of my consciousness), or – *pace* Simmel – a social property that exists and operates as a form of invisible social glue that inheres in things (institutions) or other people (so-and-so is trustworthy).

As a cognitive or affective attribute, as generally conceived, trust either connotes a rationalised frame concerned with probabilistic calculus, knowledge and identification [22] or as little more than a set of non-cognitive beliefs or set of affective attitudes. In the latter sense, it is reduced to a set of warm feelings and not much more. Abstractly, these approaches posit trust as either a set of necessary conditions or as static properties. If the former conflates trust with something else, and at best reduces the way we understand trust to be 'calculated distrusting', and the latter sees trust as an affective residue, it is hard to see what is so special about trust at all. Yet, all through the literature – whether it is sociological, psychological or economic – the idea of trust is pivotal and warrants more than this confused treatment.

Seeking to have an understanding of human activity, there is the tendency to elide the richness of the interactions and background practices and knowledge involved in trust and trust building. The richness is about how we understand trust and trusting as an ongoing process, a mutual or reciprocal dynamic relationship, which is formed through trusting between two parties. If trust's distinctiveness is its dynamic richness embedded in the complexities of human-to-human relationships, we are thus better able to grasp what it is that goes towards the formation of trust and why it is always a work in progress. Trust is built through interactions. These interactions between people involve promises, commitments and frustrations. Everyday encounters anchor the ways in which promises, commitments and frustrations play out and shape the thickness or thinness of trust in a relationship. They also, through time, impact the extent to which one could consider the relationship to be one imbued with trustworthiness. Frequent failure, for example, to live up to promises can erode trust as the other party feels let down. This could be as simple as consistent lack of punctuality, as a sign of disrespect, which eventually corrodes the trustworthiness of the relationship. Yet, corrective action – in response to direct or indirect suggestions – can contribute to the revitalisation of trust.

For relationships between people, as Robert Solomon argues in the book edited by Wrathall and Malpas [23], 'trusting is the product of participation and mutual communication in relationships. Trust is not a matter of reliance, and it is not just a matter of expectations (which presume a certain amount of risk ...'. The idea here at the heart of trust *qua* trust is that it is a post hoc shorthand way of describing a lived and dynamic experience. Through these exchanges, the parties themselves are transformed, as is the relationship itself. Research on trust formation in clinical care contexts sheds light on the importance of interpersonal communications in the cultivation of trust. Brown [24], for instance, explores the phenomenology of trust in the context of gynae-oncology care, and shows that interpersonal communication is primary to trust because of the concreteness of intersubjective experience. This is what Bredlau [25] has described in terms of the collaborative endeavour of cultivating shared worlds, which embed in our relationships with others and with the world. She argues in the context of relations between infants and adults that collaboration (i.e. acting together) is the basis of perception and that this entails the cultivation of trust. In other words, trust is not simply a feeling that people perceive; it is an embodied way of perceiving that involves people living their trust in each other through the shared perceptions of the world around them and cultivating these shared worlds in ways that protect rather than damage them.

However, authentic trust is not pure; rather, it is the opposite of this kind of trust that manifests as doubts and uncertainty. Trust cannot be read as separate from the lived state of courage-anxiety as a unity, wherein these states – according to Merleau-Ponty's phenomenology – are conditions of the existence of being:

> As a matter of principle, humanity is precarious: each person can only believe what he recognises to be true internally and, at the same time, nobody thinks or makes up his mind without already being caught up in certain relationships with others, which leads him to opt for a particular set of opinions. Everyone is alone and yet nobody can do without other people ... It is understandable that our species ... should find this situation both cause for anxiety and a spur to courage [26, 27].

The inescapable sociability of human existence is the gist of trust understood as the dynamics that leads a person to go for a set of opinions. This is because no-one's mind is made up in isolation of how people enter certain relationships with others. In other words, opinions are formed together, however provisional they often are. Trust is thus emblematic of the perpetual precariousness of existence and our relation to an enigmatic world [26]. According to Utley [27], trust is when subjects experience an equilibrium between anxiety and courage, which enables a person to get on with life. In this balance, the operation of trust is hidden from view. When confronted with circumstances that call into question the balance, when anxiety emerges as the dominant affective state, subjects are called upon to be courageous. But people are never alone. Acknowledging the presence of doubt and uncertainty gives actors the possibility to overcome them, and in doing so, strengthens trust in their relationship.

In the context of business practice transformation, Fernando Flores and colleagues [23, 28, 29] explore these general themes, and argue that the destruction of trust in a corporate context most readily takes place in environments of change. Change threatens livelihoods and accustomed ways of living and working, and therefore undermines trust. This is because such change impacts any sense of security that may have existed between firms, whatever the anchors of that have been. Such senses of security are vulnerable because they presuppose 'an underlying feeling that our identities are fixed, fragile, and constantly under threat of attack' [30]. In contexts where actors' security is threatened, distrust emerges. Introducing change in this environment can be highly destructive. So, any changes in corporate strategy must align with trust-building activities [30].

Trust and commitment are historically company-specific and are shaped by organisational values and culture [31]; these trust-building exercises are the corporate 'putting into practice' of the general idea of focal events, as discussed before. Trust building involves changes to organisational design and process, new forms of commitment making and role formation. Therefore, there is a need for parties involved to evaluate each other's sincerity, competency and her own care for their own identity. Care for identity here means cultivating practices focused on forming and fulfilling commitments and sustaining credibility as someone who makes and fulfils important offers. For Flores [30], therefore, a critical trust-building focal event is 'regular and honest assessments of managers and employees' in open settings. Regularity is necessary to mitigate the early-stage risk of participants gaming the processes (i.e. acting out an expected role to enhance their own positions within the organisation). Conducting such evaluations publicly also mitigates the risk of sustained power plays, as exposure to peers makes it less likely. Public focal events also enable people to see how what they say and do can affect others, leading to change in others as well as in themselves. Such events open up participants in their fullness, not just through speech acts that are verbalised, but through embodied interactions. Through these kinds of focal events, participants come to disclose to themselves and others new ways of being and discover that they do not have to be fragile. These new styles of engagement and interaction enable people to progressively transform themselves through collaborative action into trusting colleagues. Trust colleagues as roles are founded in interactive declaratives via the speech act. Speech acts are commitments that are not discharged until those to whom they are made declared satisfaction. Speech acts are events and processes involving others, in which those making the commitments have responsibility for the ways they are with others in the world. It is through focal events, in which participants can live out requests, offers, promises, orders and declarations that enable new trusting relationships to be formed and tested.

2.2 Blockchain-Trust Trope

If, as Salomon and Flores [29] and others discussed above indicate, trust is an embodied phenomenon resulting from interactive human engagement, phenomenologically experienced as the unified transcendence of courage-anxiety, then it follows that strictly speaking it is not something that inheres in machines. Machines do not have trusting relationships with other machines, and people do not have trusting relationships with machines. Without the risk of feedback and rejection from others, courage-anxiety does not define the state of engagement. Furthermore, that people do not have trusting relationships with machines is because trust is an interactive phenomenon wherein those involved in the creation of trust atmospheres have done so through shared attunements in focal events. Through involvement in these events, participants contribute to the ongoing formation of themselves as well as to change in others. Machines are not changed through these encounters.

Understanding trust in its distinctiveness enables us to critically reflect on how the blockchain literature has approached the question. Consider this discussion by Mougayar [32]:

> If blockchains are a new way to implement trusted transactions without trusted intermediaries, soon we'll end up with intermediary-free trust. ... Intermediary-controlled trust came with some friction, but now, with the blockchain, we can have frictionless trust. (p. xxiii)

So, this raises a question of what needs to be done next when trust is 'free'. Mougayar [32] asked: 'what does a trusted blockchain enable'? Inter alia, he argues that the blockchain offers 'programmable trust'. He describes: 'By inserting rules that represent trust inside transactions, the blockchain becomes a new way to validate these transactions via logic in the network, not via a database entry or central authority. Therefore, a new "trust factor" is created that is part of the transaction itself' (p. 46).

Mougayar's [32] discussion exhibits several conflations. Firstly, he confuses the issue of trust with the presence or absence of trusted intermediaries. As we discuss below, the presence of third parties in transactions is better understood not as a question of trust but rather, as an institutional cost necessary to deal with the state of non-trust. Third parties are necessarily interposed to mediate transactions when the transacting parties are not in trust-based relations. Third parties do not need to be trusted per se to fulfil the functions demanded of them by economic agents involved in transactions but gain their authority from their ability to exact punishment on non-performing parties. This leads to the idea of 'frictionless trust', though we are none the wiser as to what trust means or entails. Secondly, Mougayar [32] presupposes trust to be a tangible *something*, which, akin to a flow of energy or water, seeks out the path of least resistance. In this schema, trust is something that exists somewhere; it is simply a question of where. The idea of trust being something tangible finds its final form by way of programmed rules. For Mougayar [32], such rules 'represent trust inside transactions' so that something called a 'trust factor' is created. These are non sequitur*s*: non-code trust is replaced by rules (in code), which in turn creates a 'trust factor'; and yet, there is no discussion as to what trust actually is, without which it is impossible to contemplate the idea that 'it' can be codified or represented, or more generally, that it merely takes different forms.

The *non sequitur* of the general argument is also clear in Williams' discussion about blockchain and trust [33]. For Williams, blockchains enable the production of immutable records that are visible to all, but where one can remain anonymous. He says, 'You can remain anonymous, but your transaction cannot. Thus, blockchain serves as a robotic generator of unconditional trust between humans. Unconditional, *because no trust is necessary*. Everything is guaranteed by algorithm. With guaranteed trust, there is no fear of fraud' (p. 78). In other places, he invokes the idea of 'mechanical trust' (p. 79). He concludes:

> We each have our own definition of trust ... Trust and trustless are two sides of the same coin. Most of us probably don't have a definition for trustless. At first, it sounds sinister, as in untrustworthy. However, in terms of blockchain, trustless is the trustworthiest possible state. *Trustless means no trust necessary*. It's built in. (p. 82)

Williams [33] concedes that there is no generally accepted idea of trust ('we each have our own definition'). He proceeds to presume that its meaning can be gleaned by counterpositioning it with trustlessness ('two sides of the same coin'). Yet, this is hardly any clearer if for no other reason than that the idea of trust is also inseparable from mistrust and distrust and untrustworthiness. The absence of trust (i.e. a state of trustlessness), we would suggest, is just that; it also implies an absence of mistrust, distrust and untrustworthiness. Trust is not counterposed to trustlessness. Rather, trust is counterposed to mistrust, distrust and untrustworthiness. Trustless, on the other hand, is the absence of the entire rubric altogether. The absence of trust shifts *the register* to something altogether different. Williams [33] in the end concedes this when he says that 'trustless means no trust necessary'. Had he ended it there, we would have a useful place to begin. Unfortunately, because of the failure to think beyond the trust-mistrust-distrust register, Williams is compelled to add that trust is not necessary, because it is 'built in'. Why say that 'no trust is necessary' only to later assert that there is 'guaranteed trust' or 'mechanical trust'? Trust is re-invoked just as we show the possibility of understanding economic transactions in the absence of trust *tout court*.

The discursive trope seems to boil down to this: pre-blockchain, trust has been inherited in third-party institutions that straddled transactions between two parties. Blockchain seemingly replaces these institutions with codes, and many programmers tend to operate under a positivist epistemological stance rather than a constructivist one [cf. 34]. Ergo, so the argument goes, code has replaced third-party institutional trust and embedded trust into the algorithmic architecture itself [cf. 35]. Trust has doppelgänger-like qualities in that whatever 'it' is, it can assume different forms: third-party institutions or algorithmic code. Yet, this begs the question, what is the essence of trust? That is, what makes trust *trust*, and not something else?

These conceptions show that trust is ultimately substantivised with distinct properties, which inheres either in minds or in persons (and possibly things). In some conceptions, such as Hardin [36], both these approaches are pulled together via a game theoretic rubric, which treats trust as a function of human self-interestedness and attitudes of suspicion towards others, where the mediating calculus is one of probability. The technicist blockchain 'take' on trust tends to be of the latter variety, focusing on trust as a property of non-technological institutions, which can be substituted by some idea of 'programmable trust' wherein trust is rendered as a measure of probabilities associated with the actions of others. Ethereum founder's, Vitalik Buterin, recent discussion on trust is along these lines [37]. Within a technicist game theoretic frame, it is possible to dissect so-called devices for commitment that make trustworthiness possible. In the presence of such devices, of probability calculus, behavioural game strategy and ideas of rational expectations, an index of trustworthiness is therefore calculable.

The ability to render the idea of trust calculable within a mathematical frame is no doubt appealing in the context of the possibilities of smart contracts as 'self-executing' code. Here, rendering interactions calculable via a calculus of inputs-outputs, 'if this, then that', introduces a level of certitude about outcomes conditional on prescribed informational circumstances being satisfied, which is claimed to be representative of trust. This is where we demur. To speak of trust in the context of calculus of conditional certitude conflates trust with something else; this something else is more akin and better understood in terms of *reliability*. Calculative reliability is not reducible to trust *tout court*, which as we have argued, is quite a deal fuzzier and ambiguous, and dynamic than the certitude of self-executing code. The certitude that can be 'baked in' to the transactional back-office is not without value, however, as we show when we consider blockchain applications in the context of supply chains below. But, if it does have value, it is in its ability to deliver algorithmic certitude as a kind of what Solomon calls 'calculating distrusting' [23].

We thus make the distinction between trust and reliability. We can add to this distinction some related ones such as dependability, confidence and predictability [29]. Reliability, dependability, confidence and predictability are important aspects of human interactions and social relationships to the world, but aside from being purely metaphoric, the invocation of trust by rights should be preserved for thinking about and describing relationships between and amongst human beings. Machines (including computers) cannot literally be trusted. We rely upon them as we find them dependable and predictable. ‘To equate trust with predictability is a mistake because we are dealing with people in dynamic, reciprocal relationships rather than with recurrent phenomena governed by (more or less) clear, lawlike regularity’ [29]. It is also not merely a question of likelihood or probability that the other will fulfil our expectations. Trusting is a two-way relationship which affects the parties involved, and the relationship itself. Even if we say we trust a machine, the extent to which we trust it does not affect the extent to which it is likely to perform as expected.

3 Blockchain and Supply Chains

The literature posits that the introduction of blockchain technologies into supply chains contributes to the creation of trust and enhances supply chain performance. This section explores this claim from a supply chain functionality perspective and how blockchain can meaningfully contribute to supply chains.

3.1 Supply Chain Functionality and Trust Issues

Supply chains typically involve economic agents interacting across time and space to transform and create products and services, ultimately for end consumption. These agents are connected at a material level in terms of the movement of products from one to the other as the processes of transformation take place. Agents are also connected in a non-material sense via the movement of money in exchange for the movement of goods. The movement of money is governed by the flow of information about the things as money does not flow unless certain informational conditions are satisfied. Financial relations between agents are characterised by credit-and-debt relationships. This usually involves a financial third party to mediate payments through the provision of securitised credit [38–40].

Functional supply chains can be understood as a circulation system with three interconnected flows: the product flow, the money flow and the information flow. Talk of such flows draws on the conceptual imagery of Marx’s discussion about the circulation of capital in *Capital* Volume 2. There, he describes an integrated system where capital assumes three forms – industrial, commodity and finance – and the processes of reproduction and circulation are about how these metamorphose one into another and interact with each other, as constraints and conditions of possibility, through time and space. Figure 1 depicts the supply chain flows in a financialised system, in which money (M) is exchanged for a commodity (C) which is then transformed through a production process (P) to become a new commodity (C^1). This new commodity C^1 is then exchanged for money (M^1), and so on.

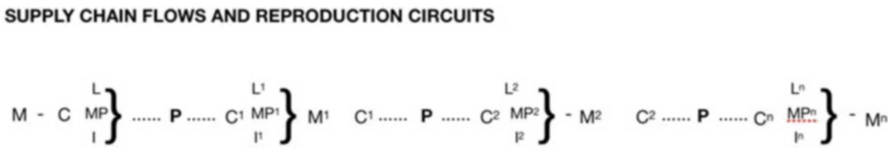


Fig. 1 Financialised supply chain schematic. Note: M money, C commodity, L labour, MP means of production, I information, P production

A full, complete circuit takes place when the original money (M) is realised as M^n after going through the phases of production and sales. A successfully completed circuit is tantamount to the supply chain reproducing itself. The processes of valorisation and transformation take place through time and place, where the work of each phase of transformation – production and then realisation through sales and consumption – has concrete temporal dimensions. The transformation of commodities through processes of production into new commodities takes time, just as the sale of the commodity post-production to either the next phase of transformation or for final consumption. Disruptions to the processes of transformation can, if sustained, have deleterious effects on the processes of supply chain reproduction. Disturbances to the flow of the supply chain circuits of transformation hamper the repetitive metonymy of industrial production and its associated credit finance circuits; and the greater the disturbances, the greater the quantum of money that must be held by each node in the supply chain to ride out the periods of disturbance. In plain terms, the greater the delays in transforming the circuits of production and sale (realisation), the larger volumes of money capital needed to sustain the reproduction of the supply chain's activities. This money capital is sourced from accumulated profits or from credit providers.

Accordingly, reducing the time of circulation of capital (i.e. the completion of a full circuit) is a key dynamic in financialised supply chains, as the shorter the duration of circulation, the less money capital is required to be held in reserve and, typically, the less credit needed. Holding money reserves and incurring costs of credit are both suboptimal utilisations of a given quantum of capital. Assuming that a given return on capital can be realised through the completion of a full circuit, it follows that the faster the circuit can be completed in a given period of time (e.g. 1 year), the greater the return that can be achieved for a given unit of initial capital.

In the sphere of production, mechanisation and automation are the key drivers in reducing the total time of circulation. *Information* plays a contributing role in driving effective mechanisation and automation. It speeds up production converting C to C^1. If information contributes to productivity growth, we can also note the role of information *about the commodities* in the transaction M-C itself as well as its end-of-circuit realisation C^1-M^1. In this formulation, we could say that the hyphen denotes the flow of information. Delays in realisation (i.e. in conversion of commodity capital to money capital form) take place if, for instance, the commodity is unsaleable or where there is insufficient demand. The speed of information flow through enhanced communication technologies also impacts the period of circulation. Advances in communications address information synchrony, but do not necessarily address the issue of information inadequacy and asymmetry. The existence of inadequate and asymmetric information between transactional members results in the trust issues between supply chain partners and, on the other hand, highlights the importance of building trust relationships to mitigate those risks. Early research [17] suggested that trust relationships support information sharing between supply chain partners. However, inter-firm trust relationships are fragile as a firm may take advantage of the other's trust for their own interests. This makes firms cautious of sharing information and communicating risks with their supply chain partners [41, 42], which hinders inter-firm trust building. The introduction of blockchain technology that has immutable and tamper-proof characteristics could be an answer to this paradox.

3.2 How Can Blockchain Meaningfully Contribute to Supply Chains?

The sustainable operations of a supply chain rely on profit accumulation above and beyond reproduction costs. The financial flows within a supply chain effectively distribute the aggregate revenue to the various actors, wherein above-cost surpluses are incrementally captured along the way. Such supply chain activities largely do not rely on trust to function. This is because most transactions associated with products, services and financial flows are finalised by 'strangers' and institutional functionaries [43]. In other words, the condition of functional supply chains is *transactional dependability* in conditions of zero trust.

However, much discussion in the literature claims that there is a significant social cost to establishing trust for commerce, via mechanisms and institutions such as 'the rule of law', and various associated arbitration and court systems and such like [44]. We suggest that these are better understood not as the costs of establishing trust but as the costs of dealing with the consequential uncertainty of outcomes of non-trust, and the costs exacted upon parties due to counterparty non-performance or change of circumstances. The reality is that these institutions are not trust-based but depend entirely upon some capacity to exact punishment [45]. The existence of legally enforceable contracts, governing supply chain transactions, which include punishments in the event of non-performance, is symptomatic of a zero-trust environment.[1] If parties trusted each other, there would be no reason for such contracts and their associated institutional buttresses. The presence of contracts and other institutional desiderata indicates a need for any forms of protection in an absence of trust.

With this understanding, we argue that the deployment of blockchain technologies in supply chain ecosystems is not about instituting trust. Rather, we claim that

[1] There are some similarities in this argument to that advanced by Williamson [46].

blockchain technologies can contribute meaningfully to supply chains in several ways, without the trust predicates so often claimed by blockchain advocates. This can be explained in that the deployment of blockchain is about increasing reliability, and from that dependability, in conditions of zero trust (at best), and distrust/mistrust at worst. In this context, the extent of reliability and then dependability refers to the presence or otherwise of information asymmetry between and amongst participants as the basis of actor decision-making and conduct and the likelihood of actor behaviours and behavioural outcomes to meet required conditions. Should trust emerge at all via these dynamics and interactions, it is a by-product.[2] Additionally, information asymmetry can be understood as an embedded property of supply chains involving multiple parties of varying configurations of power relations, which is a precondition for capricious or opportunistic action. Industry structure is a key institutional and market condition of existence of real supply chains, wherein capriciousness is always present-in-potential.

As an innovative technology with such fundamental features as explicit data validation rules, transparent processes, irreversible record and fraud proofs [37], blockchain has the potential to address the reliance on trust building in addressing these uncertainties and reduce risks of capricious actions in supply chains. In short, blockchain has the potential to reduce information asymmetry and the space for capricious conduct, thereby increasing information reliability. More effective flow of information contributes to increased velocity or circulation of commodities, reducing the amount of capital required to be held in reserve and reducing the presence of uncertainty and the cost of finance.

4 Learning from a Blockchain Use Case in Supply Chains

Supply chain collaboration is a traditional solution to reduce supply chain costs and to improve reliability [49] and become more strategically important in a contemporary business environment exposed to various interdependent risks and disruptions [50]. On this score, the supply chain literature stresses the importance of trust building and maintenance. Unfortunately, trust-based relationships are costly to build and can be easily challenged by opportunistic behaviours and/or changing circumstances [51].

In seeking solutions to tackle trust challenges, BeefLedger has been pioneering the development and commercialisation of an integrated blockchain-enabled beef provenance platform and smart contracting payments regime [19, 20]. Figure 2 shows a snapshot of BeefLedger's blockchain-based beef provenance and smart

[2] Not unrelated is the idea that trustworthiness is a result of safety and dependability, as articulated by Roth [47]. Market design, therefore, must be about safety and dependability for participants. Trustworthiness is a residual consequence. Sabel [48] introduces the idea of 'learning by monitoring' as an explanation of successful collaboration. In this case, trust is the consequence of learning embodied in ongoing monitoring.

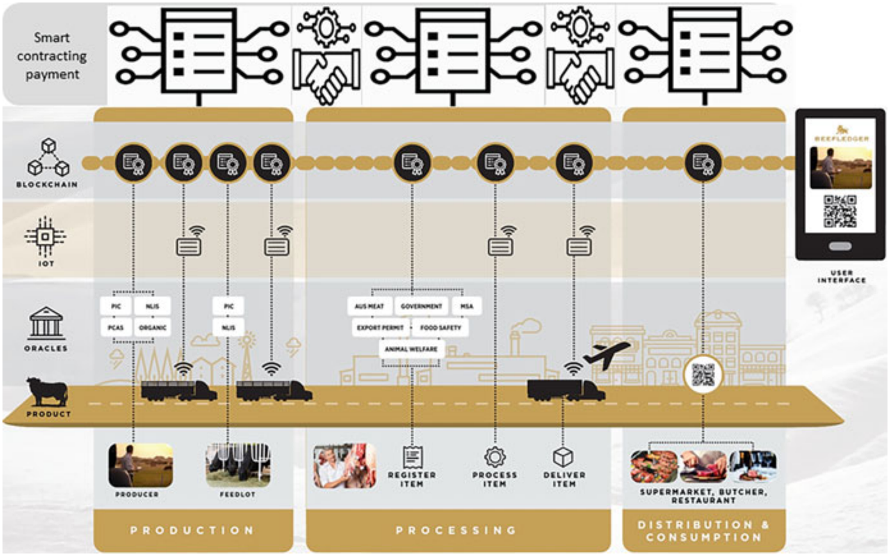


Fig. 2 The architecture for beef provenance and smart contracting payments. (Source: Adapted from Powell et al. [19])

contracting payment architecture. It is a universal digital platform project using blockchain technology with a view to use product provenance data as a basis for increasing the confidence of supply chain participants and streamlining payments. It offers supply chain agents, including consumers, a platform to verify the certification information of the products they purchase and improve the efficiency of the supply chain by reducing information asymmetry amongst transaction parties. BeefLedger makes use of blockchain as a strong validator of transaction records and the power of token economics to optimise the supply chain operations with decentralised models.

Our learnings from the ongoing work with the BeefLedger project offer empirical evidence to revisit the question of trust in supply chains. A beef supply chain generates a wealth of information about cattle breeds, sex, age, feed, weight and locations. It also involves information about meat quality, weight and storage and transport conditions. Verification of this information in compliance with procurement requirements is the condition precedent of the exchange of products for money. Information adequacy and symmetry are pivotal to the provision of credit and the completion of the commodity-money circuit, where payment is in effect the release of funds by the credit provider. The provision of trade credit has been used to facilitate cross-border trade for many centuries [52]. Trade credit has historically taken the form of a promissory note, such as a letter of credit (LC), issued by the credit provider for the purchaser. Figure 3 summarises the procedures defined by the

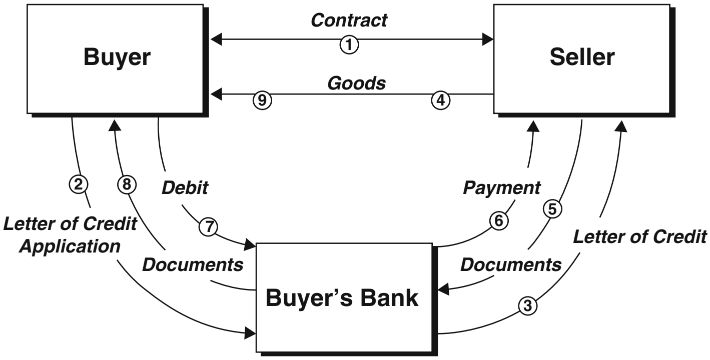


Fig. 3 Transactions and documentary flow, letters of credit. (Source: United Nations, Trade Facilitation Implementation Guide)

Trade Facilitation Implementation Guide of the United Nations.[3] The LC is issued in parallel to the contract of sale executed between the trading parties. Such LCs continue to dominate cross-border trade payments, even today. LCs are issued by the buy-side financier to the sell-side; upon the sell-side satisfying the conditions of the LC, the funds are released. Satisfaction of the conditions of the LC takes *documentary* form. To activate the LC, the sell-side is required to prepare or collate and provide the necessary documents as set out in the LC, to the LC issuer. Upon confirmation of the authenticity and satisfactory nature of the documents, the LC issuer completes the settlement.

In the transaction of beef exports, a typical LC requires the provision of a pile of documents to satisfy documentary conditions and cause the LC to be executed. These documents are provided at times digitally and in most cases in analogue form. This is confirmed by a leading bank agribusiness finance executive who was interviewed by the authors in April 2020. The finance executive stated that the processing of LCs for cross-border transactions still requires the provisioning of copies or originals of documents 'delivered in an envelope to the branch headquarters' whereupon the documents are viewed by a team of (human) evaluators. In the case of beef trade from Australia, the documents are typically (1) commercial invoice (issued by the seller/manufacturer), (2) load out summary report (signed by an Aus-Meat-certified inspector), (3) quarantine or non-wood declaration for containers (issued by the seller), (4) certificate with respect to meat (issued by the Department of Agriculture, Fisheries and Forestry), (5) packing list (issued by the manufacturer), (6) a certificate of origin (issued by the Australian Chamber of Commerce and Industry) and (7) the bill of lading (issued by the shipping agent).

Information about the product is key to the exchange, and accordingly a focus of capricious conduct risk. Capriciousness is characterised by sudden, unaccountable

[3] Accessed here: http://tfig.unece.org/contents/letters-of-credit.htm. 02 October 2020

and/or unpredictable actions on the part of one of the parties involved in the exchange. Letter of credit fraud is a widely acknowledged risk in cross-border commerce as it is warned by the FBI.[4] As a result, the presence of documentary fraud in the performance of letters of credit in cross-border trade is evidence of such informational malfeasance [53–55]. Asymmetrical relationship between different actors involved in a transaction, coupled with siloed data creation and storage systems, is the condition of existence of informationally driven caprice. When information asymmetry enables capricious conduct, supply chain sub-optimality is an almost inevitable outcome. Actions that can impact the timely realisation of commodities to money, such as those associated with informational caprice leading to either hidden action or hidden information, adversely impact upstream actors in the immediate term, and can increase overall supply chain instability by hampering the liquidity and viability of essential producers and service providers. Additionally, the growing need for credit increases the overall cost of the operations of the supply chain.

To address information asymmetry and associated financial losses, our BeefLedger team developed a blockchain-enabled multi-sig consensus mechanism. This multi-sig consensus mechanism not only enables the secure updating of a data state in accordance with specific state change rules but also allocates distributed rights to perform the state update amongst some set of agents. As information is formed or collected and recorded via a set of processes involving more than one party, involving the application of transparent rules, the opportunity for information caprice is significantly diminished. As such, blockchain technologies can provide supply chain agents with an informational base that – through the processes of collective responsibility in their production and subsequent management – they can each rely upon to go about their respective activities and transactions with each other. In other words, blockchain technologies in supply chain contexts remove the fundamental basis for hidden action and hidden knowledge. Without either, markets can be made safer, so that participants can go about their business focused on their interests without strong incentives to game the system [47, 56].

5 Reflections on Technology-Mediated Trust

This section presents our reflections on how blockchain can redefine trust and technology-mediated trust in a broad sense with social commerce in China leveraged by new technologies, such as WeChat – a Chinese social networking app with over one billion users.

[4] https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/letter-of-credit-fraud

5.1 Blockchain Cannot Guarantee Absolute Truths

When considering blockchain as a digital, decentralised and distributed ledger to record transactional information in a chronological order for permanent and tamper-proof records, blockchain-based supply chains can be viewed as a 'tamper-proof system which will stand against any cheating or fraud attempts' [21]. While public (permissionless) blockchains facilitate the 'perfect' situation for absolute truths, the concern about privacy and confidentiality issues reduces its applicability in supply chains. According to Batwa and Norrman [21], 'private blockchains allow only a preselected and limited number of participants to be authorised to use the ledger', where data entries are observed by a small group of witnesses. Blockchains for supply chains cannot deliver absolute truths due to opportunistic behaviours and collusion risks between supply chain actors, and consequently result in trust issues. The trust issue also emerges in a private blockchain-based supply chain where a dominant manufacturer or retailers are a central authority and may manipulate their partners for their own interests.

In addition to the trust issues between supply chain partners, there is an issue with trust in the technology (blockchain) or in the infrastructure. Although the potential has been raised by academia and industry, blockchain infrastructure has yet to evolve as a 'general purpose technology' [57]. Current blockchain consensus mechanisms and data architecture that were developed for cryptocurrency help mitigate malicious data manipulation when data is stored in the blockchain system. However, the 'garbage in garbage out' issue is yet eliminated if fraudulent data is registered onto the blockchain system [19]. Blockchain's inability to ensure data authenticity at the entry points can further reduce the level of trust in the blockchain-based supply chain. The development of fit-for purpose consensus mechanisms and/or sensor-enabled data architecture could be a potential solution to guarantee the reliability and integrity of original data.

5.2 Blockchain Is More Than a Trust Machine

Since blockchain cannot guarantee absolute truths of the information, it is not a synonym for trust. To suggest so is a result of a failure to examine what it is that makes trust to be trust and not something else, and conflates trust with other kinds of relationships, particularly reliability. On the contrary, blockchains enable functional economic relationships to be established in the absence of trust and can achieve this at lower cost than other techniques. The technology delivers what Batwa and Norrman [21] describe as 'a trust-free environment based on the reliability and security of the information stored on the blockchain' – by reducing capriciousness in relation to information. Blockchain can be taken as a transparency machine in which anyone (i.e. supply chain members, authorities and consumers) can join the network and view/census the data on that network. In a supply chain context, such transparency breeds accountability, which can nudge supply chain partners to work more responsibly because they are accountable for their actions.

Trust is an embodied relationship between people, and their interactions involving mutual commitments through time, which is not something that machines (including blockchain and the Internet) do. Trust is neither something that describes the relationships that can form between people and machines, but a by-product of reliability and integrity in an environment exposed by uncertainties and risks. Nakamoto knew this when the Bitcoin white paper explicitly sought to enable digital transactions between people – erstwhile strangers, as identities did not need to be explicitly disclosed – without reliance on trust. This could be done because algorithms, deployed across a decentralised network of computers, could be relied upon to perform without caprice under specific operating conditions. Machines mediated the interaction of strangers (who could not form trust between each other and did not need to in any case) by providing sufficient conditions of reliability and accountability for the exchange to proceed and for the recorded exchange.

We displaced the centrality of trust in supply chain relationships with our real-life use case, showing that reliability is a sufficient condition of existence of supply chain functionality and transparency can breed accountability. This then raises a question of where trust sits, if at all, in a technology-mediated supply chain environment.

5.3 Technology-Mediated Trust in China's Social Commerce

We now reflect on the place for trust and how trust combined with machine-enabled reliability and relationships of extended trust via a technologically mediated 'economy of acquaintances' that has the potential to radically transform supply chain relationships and dynamics in a broad sense. The recent emergence of social commerce in China that combines first-generation e-commerce functionalities (platform-based sales and buying) with social communication features is a good example to illustrate this general point. With social commerce, consumers have access to products through the recommendations from their social acquaintances who share their shopping and consumption experience on their social media, like WeChat. This is a trust-based purchase or what has been called the economy of acquaintances as consumers view information about products and services received from friends more valuable and credible than information from other sources, including the anonymous information from strangers that was the norm in conventional e-commerce models [58].

Webs of interpersonal networks are amplified in China through the affordances of new technologies. In particular, the functionality offered by the WeChat app recasts the ways in which social networks are established, maintained and cultivated. WeChat has now morphed into a social commerce tool, with seamless payment capabilities, as part of China's burgeoning mobile economy [59]. A number of studies have indicated and explored how WeChat has now become increasingly important in the formation of relationship/guanxi networks in China, ranging from peer-to-peer relationships between professional peers [60] and more generally across the community at large.[5] WeChat works for guanxi development because it features low anonymity, high privacy and closed community [61]. As Shao and Pan [62] have shown, ‘platform interactivity and media richness are significant technology affordances that promote users’ guanxi networks, and their influences are mediated by social interaction and shared understanding’.

WeChat indeed offers a technical environment that revivifies sharing, with the additional dimension of speed and scalability efficiency, and which emulates the intimate relationships that underpin the production of trust. Crary [63] paints a somewhat dystopian picture when it comes to the effects of social technologies: ‘One inhabits a world in which long-standing notions of shared experience atrophy, and yet one never actually attains the gratifications or rewards promised by the most recent technological options’ (p. 31). The experience of WeChat as a guanxi-related capability suggests that the dynamics and effects are more ambiguous.

This example shows that when people do not have trusting relationships with technology, it does not mean that technology has no place in the lived dynamics of trust. This is a provisional observation that requires further explorations; but some exploratory empirics seem to support this statement [64]. If it is right, we can envisage a world where WeChat social commerce-enabled capabilities can be mobilised to activate networked cohorts of consumers. This is not only happening with ‘group buying’ models such as Pinduoduo (拼多多) [65] but also with the more recent ‘community group buying’ (社区团购) [66, 67].

6 Conclusions

This chapter explores what it is to trust and what makes trust distinctive and, on this basis, presents the empirical learning of how blockchains can enable supply chain transactions to take place between strangers and corporations in a zero-trust environment, without a traditional enforcement intermediary. To take a step forwards, this chapter reflects how technology, including blockchain, can redefine trust in a broad sense with primary and secondary evidence available. Our investigation of the question of what makes trust trust and not something else offers a space to revisit trust in supply chains with the mediation of new technologies, such as blockchain.

Blockchain technologies fulfil to a greater extent the claims of calculative algorithms insofar as enhancing predictability and dependability are concerned. This is in place of trust. Even so, trust is not without place in the supply chains of today and the future, but not in the ways that blockchain advocates have

[5] See China Internet Network Information Center (2015) Chinese User Behaviour in Social Media 2015 Research Report (2015年中国社交应用用户行为研究报告)

so far suggested. A reimagined supply chain anchored through trusting relationships amongst consumers (viz. group buying dynamics embedded into trust-based WeChat-mediated guanxi networks) on one hand, with emergent intimacy-at-a-distance with producers, could transform supply chain dynamics considerably. Promises and commitments made to each other, by consumer groups and producers, give rise to demands on blockchain technologies to deliver reliable functions. What we can, therefore, imagine is a blockchain-enabled reliability architecture that enables the bridging of consumer and producer communities that can separately work on trusting, safe in the knowledge that their intentional commitments to each other are backed up by reliable information systems that mitigate gaming risks otherwise made possible by asymmetric information. In the end, blockchain technology may not be about trust directly, but it is not entirely irrelevant when it comes to trust in supply chains.

Acknowledgement This study was supported by funding from QUT, BeefLedger Ltd. as well as the Food Agility CRC Ltd., funded under the Commonwealth Government CRC Program. The CRC Program supports industry-led collaborations between industry, researchers and the community.

References

1. Satwik, P. M., Geluvaraj, B., & Ashok Kumar, T. A. (2018). A study on applications of AI, ML, DL and blockchain in healthcare and pharmaceuticals and its future. *International Journal of Computer Sciences and Engineering, 6*, 765–770. https://doi.org/10.26438/ijcse/v6i8.765770
2. Omar, A. S., & Basir, O. (2020). Secure anti-counterfeiting pharmaceuticals supply chain system using composable non-fungible tokens. https://doi.org/10.1201/9780429324932-14
3. Tian, F. (2017). A supply chain traceability system for food safety based on HACCP, blockchain Internet of things. In *2017 international conference on service systems and service management* (pp. 1–6).
4. Creydt, M., & Fischer, M. (2019). Blockchain and more - algorithm driven food traceability. *Food Control, 105*, 45–51. https://doi.org/10.1016/j.foodcont.2019.05.019
5. Kamilaris, A., Fonts, A., & Prenafeta-Boldύ, F. X. (2019). The rise of blockchain technology in agriculture and food supply chains. *Trends in Food Science and Technology, 91*, 640–652. https://doi.org/10.1016/j.tifs.2019.07.034
6. Kamath, R. (2018). Food traceability on blockchain: Walmart's pork and mango pilots with IBM. *The Journal of the British Blockchain Association, 1*, 3712.
7. Lin, J., Shen, Z., Zhang, A., & Chai, Y. (2018). Blockchain and IoT based food traceability for smart agriculture. In *Proceedings of the 3rd international conference on crowd science and engineering (ICCSE'18)* (pp. 1–6). ACM.
8. Cartier, L. E., Ali, S. H., & Krzemnicki, M. S. (2018). Blockchain, chain of custody and trace elements: An overview of tracking and traceability opportunities in the gem industry. *Journal of Gemmology, 36*, 212–227. https://doi.org/10.15506/JoG.2018.36.3.212
9. Gürkaynak, G., Yılmaz, İ., Yeşilaltay, B., & Bengi, B. (2018). Intellectual property law and practice in the blockchain realm. *Computer Law & Security Review, 34*, 847–862. https://doi.org/10.1016/j.clsr.2018.05.027
10. Malaurie-Vignal, M. (2020). Blockchain, intellectual property and fashion. *Journal of Intellectual Property Law & Practice, 15*, 92–97. https://doi.org/10.1093/jiplp/jpaa009

11. Foth, M. (2017). The promise of blockchain technology for interaction design. In A. Soro, D. Vyas, J. Waycott, B. Ploderer, A. Morrison, & M. Brereton (Eds.), *Proceedings of the 29th Australian computer-human interaction conference (OzCHI 2017)* (pp. 513–517). Association for Computing Machinery.
12. Dunphy, P., & Petitcolas, F. A. P. (2018). A first look at identity management schemes on the blockchain. *IEEE Security Privacy, 16*, 20–29. https://doi.org/10.1109/MSP.2018.3111247
13. Mori, T. (2016). Financial technology: Blockchain and securities settlement. *Journal of Securities Operations & Custody, 8*, 208–227.
14. Oh, J., & Shong, I. (2017). A case study on business model innovations using Blockchain: Focusing on financial institutions. *Asia Pacific Journal of Innovation and Entrepreneurship, 11*, 335–344. https://doi.org/10.1108/APJIE-12-2017-038
15. Fosso Wamba, S., Kala Kamdjoug, J. R., Epie Bawack, R., & Keogh, J. G. (2020). Bitcoin, Blockchain and Fintech: A systematic review and case studies in the supply chain. null*, 31*, 115–142. https://doi.org/10.1080/09537287.2019.1631460
16. Nakamoto, S. (2009). Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. See: https://bitcoin.org/bitcoin.pdf
17. Ghosh, A., & Fedorowicz, J. (2008). The role of trust in supply chain governance. *Business Process Management Journal, 14*, 453–470. https://doi.org/10.1108/14637150810888019
18. Hearn, G., Collie, N., Lyle, P., Choi, J., & Foth, M. (2014). Using communicative ecology theory to scope the emerging role of social media in the evolution of urban food systems. *Futures, 62*, 202–212. https://doi.org/10.1016/j.futures.2014.04.010
19. Powell, W., Foth, M., Cao, S., & Natanelov, V. (2021). Garbage in garbage out: The precarious link between IoT and blockchain in food supply chains. *Journal of Industrial Information Integration, 100261*. https://doi.org/10.1016/j.jii.2021.100261
20. Cao, S., Powell, W., Foth, M., Natanelov, V., Miller, T., & Dulleck, U. (2021). Strengthening consumer trust in beef supply chain traceability with a blockchain-based human-machine reconcile mechanism. *Computers and Electronics in Agriculture, 180*, 105886. https://doi.org/10.1016/j.compag.2020.105886
21. Batwa, A., & Norrman, A. (2021). Blockchain technology and trust in supply chain management: A literature review and research agenda. *Operations and Supply Chain Management: An International Journal, 14*, 203–220. https://doi.org/10.31387/oscm0450297
22. Exon, S. N. (2011). Maximizing technology to establish trust in an online, non-visual mediation setting. U. La Verne L. Rev, *33*(1), 27–41
23. Wrathall, M., & Malpas, J. (Eds.). (2000). *Heidegger, coping, and cognitive science: Essays in honor of Hubert L. Dreyfus* (Vol. 2. 2, 415).
24. Brown, P. R. (2009). The phenomenology of trust: A Schutzian analysis of the social construction of knowledge by gynae-oncology patients. *Health, Risk & Society, 11*, 391–407. https://doi.org/10.1080/13698570903180455
25. Bredlau, S. (2019). On perception and trust: Merleau-Ponty and the emotional significance of our relations with others. *Continental Philosophy Review, 52*, 1–14. https://doi.org/10.1007/s11007-016-9367-3
26. Merleau-Ponty, M. (2004). *The world of perception*. Routledge.
27. Utley, F. (2014). Considerations towards a phenomenology of trust. *Symposium, 18*, 194–214. https://doi.org/10.5840/symposium201418111
28. Spinosa, C., Flores, F., & Dreyfus, H. L. (1997). *Disclosing new worlds: Entrepreneurship, democratic action, and the cultivation of solidarity*. MIT Press.
29. Solomon, R. C., & Flores, F. (2003). *Building trust: In business, politics, relationships, and life*. Oxford University Press.
30. Flores, F. (2000). Heideggerian thinking and the transformation of business practice. In *Heidegger, coping and cognitive science: Essays in honour of Herbert L. Dreyfus* (Vol. 2, pp. 271–291). The MIT Press: Cambridge, Massachusetts, United States.
31. Yuan, Y., Feng, B., Lai, F., & Collins, B. J. (2018). The role of trust, commitment, and learning orientation on logistic service effectiveness. *Journal of Business Research, 93*, 37–50. https://doi.org/10.1016/j.jbusres.2018.08.020

32. Mougayar, W. (2016). *The business blockchain: Promise, practice, and application of the next internet technology*. John Wiley & Sons.
33. Williams, S. P. (2019). *Blockchain: The next everything*. Simon and Schuster.
34. Foth, M., Odendaal, N., & Hearn, G. (2007). The view from everywhere: Towards an epistemology for urbanites. In D. Remenyi (Ed.), *Proceedings ICICKM 2007: 4th international conference on intellectual capital, knowledge management and organisational learning* (pp. 127–134). Academic Conferences Limited.
35. Dourish, P. (2016). Algorithms and their others: Algorithmic culture in context. *Big Data & Society, 3*, 2053951716665128. https://doi.org/10.1177/2053951716665128
36. Hardin, R. (1985). Game theory & the nuclear standoff. *Worldview, 28*, 20–24. https://doi.org/10.1017/S0084255900046660
37. Buterin, V.: Vitalik buterin: On public and private blockchains, (2015).
38. Cutler, T., Hindess, B., Hussain, A., & Hirst, P. Q. (2013). *Marx's capital and capitalism today*. Routledge.
39. Fu, J., Matous, P., & Todō, Y. (2018). *Trade credit in global supply chains*. RIETI.
40. Giovannetti, A. (2016). *Trade credit, bank credit and formation of supply chains: Can banks amplify contagion risk?*https://doi.org/10.2139/ssrn.3301348
41. Singh, A., & Teng, J. T. C. (2016). Enhancing supply chain outcomes through Information Technology and Trust. *Computers in Human Behavior, 54*, 290–300. https://doi.org/10.1016/j.chb.2015.07.051
42. Cao, S., Bryceson, K., & Hine, D. (2020). Improving supply chain risk visibility and communication with a multi-view risk ontology. *Supply Chain Forum: An International Journal, 21*, 1–15. https://doi.org/10.1080/16258312.2020.1717990
43. Murphy, P. (2015). The stranger society: The case of economic and social development in the tropics. *Budhi: A Journal of Ideas and Culture, 19*, 107–134.
44. Davidson, S., Novak, M., & Potts, J. (2018). The cost of trust: A pilot study. The Journal of The British Blockchain Association, *1*(2). https://doi.org/10.31585/jbba-1-2-(5)2018.
45. Foucault, M., Davidson, A. I., & Burchell, G. (2008). *The birth of biopolitics: Lectures at the Collège de France, 1978–1979*. Springer.
46. Williamson, O. E. (1993). Calculativeness, trust, and economic organization. *The Journal of Law and Economics, 36*, 453–486. https://doi.org/10.1086/467284
47. Roth, A. E. (2015). *Who gets what – and why: The new economics of matchmaking and market design*. Houghton Mifflin Harcourt.
48. Sabel, C. F. (1993). Studied trust: Building new forms of cooperation in a volatile economy. *Human Relations; Studies Towards the Integration of the Social Sciences, 46*, 1133–1170. https://doi.org/10.1177/001872679304600907
49. McLaren, T., Head, M., & Yuan, Y. (2002). Supply chain collaboration alternatives: Understanding the expected costs and benefits. *Internet Research, 12*, 348–364. https://doi.org/10.1108/10662240210438416
50. Cao, S., Bryceson, K., & Hine, D. (2019). An ontology-based Bayesian network modelling for supply chain risk propagation. *Industrial Management & Data Systems, 119*, 1691–1711. https://doi.org/10.1108/IMDS-01-2019-0032
51. Dyer, J. H., & Singh, H. (1998). The relational view: Cooperative strategy and sources of interorganizational competitive advantage. *AMRO, 23*, 660–679. https://doi.org/10.5465/amr.1998.1255632
52. Mooney, J. L., & Blodgett, M. S. (1995). Letters of credit in the global economy: Implications for international trade. *Journal of International Accounting, Auditing and Taxation, 4*, 175–183. https://doi.org/10.1016/1061-9518(95)90016-0
53. Alavi, H. (2016). Mitigating the risk of fraud in documentary letters of credit. *TalTech Journal of European Studies, 6*, 139–156. https://doi.org/10.1515/bjes-2016-0006
54. Zhang, Y. (2012). Documentary letter of credit fraud risk management. *Journal of Financial Crime, 19*, 343–354. https://doi.org/10.1108/13590791211266340
55. Letter of Credit Fraud. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/letter-of-credit-fraud

56. Vulkan, N., Roth, A. E., & Neeman, Z. (2013). *The handbook of market design*. Oxford University Press.
57. Ozcan, S., & Unalan, S. (2020). Blockchain as a general-purpose technology: Patentometric evidence of science, technologies, and actors. *IEEE Transactions on Engineering Management, 1–18*. https://doi.org/10.1109/TEM.2020.3008859
58. Lin, J., Luo, Z., Cheng, X., & Li, L. (2019). Understanding the interplay of social commerce affordances and swift guanxi: An empirical study. *Information & Management, 56*, 213–224. https://doi.org/10.1016/j.im.2018.05.009
59. Ma, W. (2016). *China's mobile economy: Opportunities in the largest and fastest information consumption boom*. Wiley.
60. Niedermeier, K. E., Wang, E., & Zhang, X. (2016). The use of social media among business-to-business sales professionals in China. *Journal of Research in Interactive Marketing, 10*, 33–49. https://doi.org/10.1108/JRIM-08-2015-0054
61. Wang, X. (2016). *Social media in industrial China*. UCL Press.
62. Shao, Z., & Pan, Z. (2019). Building Guanxi network in the mobile social platform: A social capital perspective. *International Journal of Information Management, 44*, 109–120. https://doi.org/10.1016/j.ijinfomgt.2018.10.002
63. Crary, J. (2014). *24/7: Schlaflos im Spätkapitalismus*. Verlag Klaus Wagenbach.
64. Zhang, Z., & Gu, C. (2015). Effects of consumer social interaction on trust in online group-buying contexts: An empirical study in China. *Journal of Electronic Commerce Research, 16*, 1–21.
65. Ye, Q., Feng, Y., Yang, P., Yang, C., & Yang, L. (2019). The influence of gamification mechanics on online group-buying participation, presented at the 25th Americas Conference on Information Systems, AMCIS 2019, Mexico: Cancun.
66. Sigley, G., Powell, W., & Cao, S. (2020). Community group buying, vulnerable communities and COVID-19 in China. In N. Georgeou & C. Hawksley (Eds.), *State responses to COVID-19: A global snapshot at 1 June 2020* (pp. 50–51). Western Sydney University.
67. Zhang, J. J., & Tsai, W.-H. S. (2015). United we shop! Chinese consumers' online group buying. *Journal of International Consumer Marketing, 27*, 54–68. https://doi.org/10.1080/08961530.2014.967902

The Blockchain-Based Digital Certificate for the Transport of Dangerous Goods

Adnan Imeri, Christophe Feltus, Nazim Agoulmine, and Djamel Khadraoui

1 Introduction

The transport of dangerous goods (TDG), also named hazardous goods (e.g., oils, gas, chemical products, radioactive substances, corrosive products, explosives, medical waste), consists in the carriage of goods presenting potential important risks to the people, to material, and/or to the environment, and which necessitates dedicated and specially reinforced security measures therefore. This transport of dangerous goods (TDG) represents an excessively important activity for the countries of the European Union and worldwide, as most member states increase in transport of dangerous goods in the recent years. The highest increase, in EU, was recorded in 2018 and concern Belgium (77.3%), Slovenia (46.7%), Croatia (42.3%), and Finland (36.7%).[1] According to global statistics [1], dangerous goods may constitute about fifty percent of the global transportation in the next years, should it be by road, railway, air, or seas. Compared to traditional transportation e.g., general supply chains, the TDG is a particular class of transportation that is subject to specific requirements among which the human and environmental safety.

[1] https://ec.europa.eu/eurostat/statistics-explained

A. Imeri (✉)
Luxembourg Institute of Science and Technology, Esch-sur-Alzette, Luxembourg

Université of Evry Val d'Essonne, Evry, France
e-mail: adnan.imeri@list.lu

C. Feltus · D. Khadraoui
Luxembourg Institute of Science and Technology, Esch-sur-Alzette, Luxembourg

N. Agoulmine
Université of Evry Val d'Essonne, Evry, France

A. Bouras et al. (eds.), *Blockchain Driven Supply Chains and Enterprise Information Systems*, https://doi.org/10.1007/978-3-030-96154-1_3

It also incorporates rigorous information immutability and the traceability of the DG movement [2], as indicated in the "Agreement concerning the International Carriage of Dangerous Goods by Road" [3] applicable since 1 January 2021.

In this context, this chapter aims to propose a platform to support the verification of the identity, of the history of transportation, and of the location over time of the dangerous goods by means of blockchain-based digital certificate acting as a method for documented recorded identification. The principle of the blockchain is that a specific data is recorded as a series of "blocks" which is distributed over the network and is accessible by users possessing private keys that they use to identify themselves and electronically sign transactions. This "block" also contains (1) hash values that allow verifying the data and (2) a piece of the hash value from the previous block that guarantee traceability and integrity of the information. When users create more data, new blocks are successively added to this block chain and are recorded with ledger-based technology to track transactions but also to ensure accountability.

In parallel, a digital certificate is a credential which allows an organization to identify and share information in a secure way over Internet or other private network by means of a pair of public/private key. Using jointly **blockchain technology** and **digital certificate** in the paper aims to ensure transaction *transparency* thanks to an unalterable record distributed among many users, *easy access* thanks to the collaborative environment that makes it easier for all agents to rapidly access on the transportation information, less *paperwork* thanks to the electronic distribution of data, and especially, *strong users identification* thanks to the digital certificates' credentials. This signifies, by the way, greater gains in efficiency, more streamlined approach at the management level, more reactivity in the treatment of information, and less risks of treatment-based errors.

Besides proposing a blockchain-based digital certificate for the TDG, our approach also analyzes to what extent the blockchain may be specified to integrate and be compatible with the **Internet of Things** (IoT) technology and specifications. IoT for the TDG has been considered as an important technology to move toward the digital society and is capable of supporting intelligent applications such as container information forecasting, container gate-in and gate-out management, fire control, and environmental parameters monitoring [4]. Our platform is fully compatible with the IoT technology and allows leveraging the benefits generated so far.

1.1 Supply Chain Management

The extraordinarily growing globalization of production and the megabit of data generated by the manufacturing and transportation processes have forced industries to set up supply chain management sufficiently autonomous and efficient to support the integration of key business processes from the original suppliers through the end-users [5]. According to [6], nowadays the commonly accepted paradigms of supply chain management are no more appropriate for operating in *data-driven* *smart manufacturing* and goods transportation, provided the cost and effectiveness impact engendered by the imposed unnecessary constraints on the system. For Li et al. [6], the origin of this problem lies with the lack of structural limitations of the current paradigms, that is., to deal with the massive volume of data emerging at the various stages of production and transportation. This statement is especially relevant for the sector of the TDG, as explained in Sub Section 1.2, provided the overload of information legally required by the governments (e.g., Directive 2008/68/CE, "TMD" decree, Regulation 84-810 and 2003-699, Article L. 5331-2).

1.2 Supply Chain for Dangerous Goods

In this section, we present a study concerning the supply chain of dangerous goods (DGs). Initially, we present the definition of DG, then details of the supply chain of DG highlighting the complexity in the TDG, including the main stakeholders involved in TDG.

Dangerous goods (DGs) are considered as any material or substance or a mixture of substances (gases, liquid, or solids), which exposes potential risks (identified as hazardous) for harming humans, animals, property, and the environment [3]. DGs are classified based on their physical and chemical effects ADR2021. ADR classifies DG in categories such as "Explosives," "Gases," "Flammable liquid," "Flammable solids," "Oxidizing substances and organic peroxides," "Toxic and infectious substances," "Radioactive material," "Corrosive substances," and "Miscellaneous dangerous substances and articles" [3, 7].

The supply chain of DG is complex and belongs to the regulated domains. The complexity originates from the involvement of many regulatory frameworks at the national and international levels. The regulatory framework governs TDG entirely [8]. Table 1 shows the main regulatory frameworks applied in the TDG. In the context of our study, we are mainly focused on road transport of DG as one of the most used transport modes in the supply chain of DG [13].

The TDG requires strict procedures for preparing transportation and its specificity, documentation, and DG treatment. The DG storage, treatment, and reuse or processing (for industrial purposes) refer to the management part of DG. Figure 1, presents the general supply chain for DG. For operation with the DG, various participants are involved, such are "Consignors," "Transporter," "Driver and vehicle crew," "Filler," "Loader," "Unloader," "Consignee," "Tank-operator/portable tank operator," and "DG Safety Advisor." Section 4 of ADR specifies roles (participants) and legal responsibilities for each involved party in TDG [3].

1.3 Research Method

At a methodological level, the research that we tackle concerns the improvement of the traceability in the field of the transport of dangerous goods. Accordingly,

Table 1 International regulatory framework and agreements for TDG, specific to the mode of transport

Mode of transport	Regulatory framework	International organization	Abbrev.
Road (Land)	European Agreement on the International Carriage of Dangerous Goods [3]	UNECE	ADR
Inland Waterway	European Agreement on the international carriage of Dangerous Goods by Inland Waterway Navigation [9]	UNECE	ADN
Rail	Regulation for the International carriage of Dangerous Goods by Rail [10]	OTIF	RID
Sea	International Maritime Dangerous Goods Code [11]	IOM/CCC	IMDG Code
Air	Dangerous Goods Regulations; Technical Instructions For The Safe Transport of Dangerous Goods by Air [12]	ICAO	DGR IACI IT

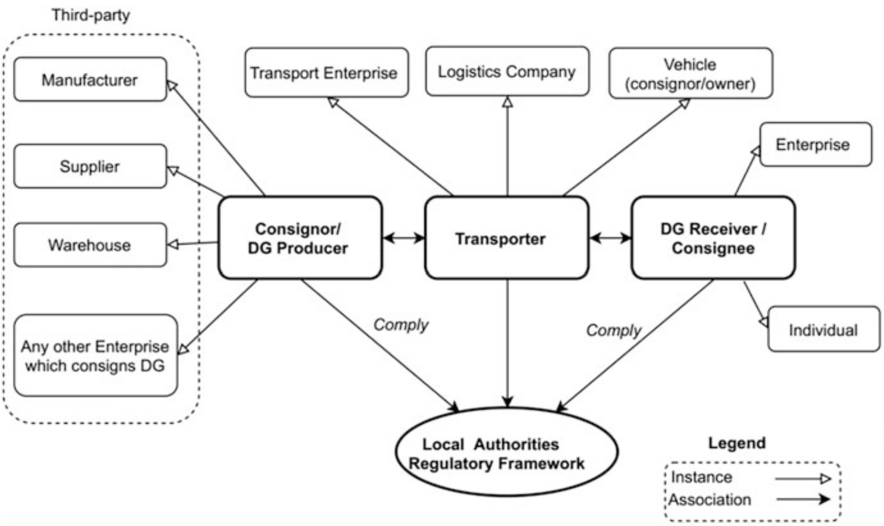


Fig. 1 The involved stakeholders and basic organization of the supply chain for TDG. Inspired from [3]

we have defined and conceptualized a blockchain-based solution that aims to enable following the DG life cycle from its origin (depart point) to destination (processing of DG). Through this research, we strengthen the stakeholders' trust in the TDG chain by raising up the transparency level through the information system which sustains this chain. Accordingly [14], explains that the **Design Science Research (DSR)** paradigm seeks to extend the boundaries of human and organization capability by creating new and innovative artefacts. Practically, provided that we aim to design a new artifact (the BC-based solution) to allow the stakeholder to trust the DG transportation with IT enablers, we acknowledge that this research may plainly be considered in the scope of DSR [15]. As advocated by the DSR theory [14, 15], the method that we use to design this solution is an iterative approach consisting first of analyzing the problem under scope and in defining the requirement for a solution, second of defining and validating the relevant concepts, and third of designing the blockchain-based solution.

Given that our artifact is motivated by real problems and relies on the knowledge of the field, we need to involve practitioners and end-users all along with the artifact-building activities. Therefore, we have applied the design research method proposed by [16]: the Action Design Research method which objective is to strengthen the connections between the end-users (TDG companies) and the researchers by combining the building, intervention, and evaluation (BIE) activities. Given that the elaboration of our artifact strongly relates to the information system, we apply an **IT-Dominant BIE** Generic Schema (Fig. 2). When applied to our research, at step 1, we (researchers) have first performed a workshop to identify the problem of transparency and traceability of DG, in cooperation with the practitioner, that is, The Ministry of Transportation in Luxembourg. The output from this workshop significantly highlights the need to have a platform (solution) that allows "managing" the life cycle of DG in an end-to-end manner. In step 2, we have proposed a conceptual solution for information sharing and traceability related to TDG. The general conceptual solution has been validated by the scientific practitioners in [2, 17]. At step 3, we proposed a BC-based solution (beta version), and at step 4, the proposed solution was presented to the involved stakeholders and end-users and was accepted and supported as the main solution to highlight the transparency in TDG. The components of the solution were published in [7], which proposes blockchain and IoT integration. Finally, at step 5, we plan to extend the solution by integrating it on the main TDG BC-based platform. Finally, according to [18], the evaluation

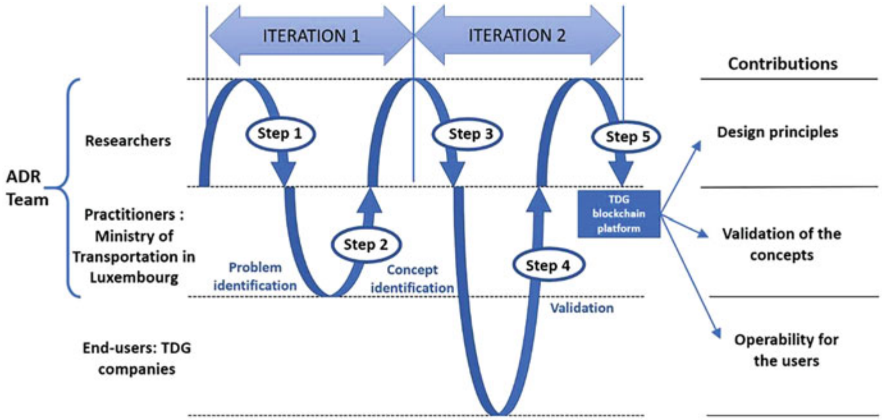


Fig. 2 IT-Dominant BIE (building, intervention, and evaluation) generic schema applied to blockchain platform for TDG design. (Adapted from [16])

of a designed artifact must use precise evaluation criteria. Provided that the goal of our research is to support end-users with an innovative TDG blockchain-based platform, the validation criteria is the operability of this platform, defined in ISO 25010 (SquaRE [19]), that is, the *ability* of the blockchain-based platform to be easily operated by a given user in a given environment. In our context, this given environment consists of the TDG infrastructure operated during the daily activities of the TDG companies. This ultimate validation should be achieved in future works.

The outline of this chapter is organized as follows. Section 2 shows the research motivation and general problem definition. Section 3 presents the main characteristics of blockchain technology. In Sect. 4, we show related works studies. Section 5 shows the conceptual approach for a digital certificate. The proof of concept (PoC) implementation is shown in Sect. 6. Finally, in Sect. 7, we conclude and present our future works.

2 Motivation and Problem Definition

DGs are sensitive and require strict supervision works in order to maintain safety and security. Entirely, the TDG process requires end-to-end transparency and to comply with the regulatory framework (as shown in Fig. 1). Authorities and the involved stakeholders require to know the life cycle of DG, starting from the preparation of DG for transport, the information during the transport, and the definitive treatment of DG. For being able to monitor the TDG, it requires adopting an approach that enhances transparency. This will be achieved with the help of technological means which ensure information immutability, availability, and security [20]. The existing systems, which are largely centralized databases [13], do not have enough technical capabilities to support data immutability and lack of availability since the centralized approach is prone to a single point of failure [7, 8, 13, 21]. Among the raised question is “How to ensure an end-to-end transparency in TDG?” “How to perform full traceability of DG in the process of transport and also in the lifetime of DG?”

Another significant issue in TDG is the dynamic changes of parameters of DG during transportation. Besides **classified substances as DG** several non-dangerous goods might turn into DG when certain environmental conditions are not fulfilled. DG reacts differently on such parameters and may cause damages or other risks such as fire, explosion, infection, and other potential risks. The raised question is, “How to ensure that the specific environmental parameters are kept under control during the transport process?” To respond to these questions, we propose a conceptual solution that responds to the specific problems related to DG. Thus, we examine the technical capabilities of blockchain and IoT for supporting our approach.

3 Background: Blockchain Technology and Its Main Characteristics

Blockchain is a distributed decentralized database that allows storing append-only transaction data. The blockchain network comprises several decentralized nodes that communicate with each other in a peer-to-peer mode. All the nodes included in the blockchain network contain the same ledger, and they rely on communication in distributed nodes, thus avoiding any central authority [22]. The blockchain nodes gather transactions into "blocks." The transactions are initially validated by performing cryptographic checks (public-private key cryptography). The process of adding a new block into blockchain is called "mining," and the nodes that perform this mining are called miners [23]. The miner[2] proposes a new block after performing specific computing power condition [24] or being delegated by other nodes to perform mining [25]. After proposing the new block, it is added to the main ledger chained with the previous block, thus achieving consensus over the transaction state by the majority of involved nodes according to the consensus protocol used, for example, Proof of Work and Proof of Stake [23]. The block of transactions that are stored into the blockchain is immutable, and cryptography tools ensure data integrity [26]. Among the main blockchain fundamental characteristics is that the block of data is linked together, so block N contains the hash address of the previous block N-1 [26, 27]. The tendency to change the information stored into blockchain is denied by consensus protocol which verifies the state of data [22].

The smart contract (SC) is an autonomous computer code encoded to react and support a specific problem [26]. It is deployed on the blockchain and executed based on its specifications to perform a specific task. SC implements a certain level of business logic and, in combination with blockchain technological capabilities, constitutes a powerful tool to solve information-related issues such as transparency, traceability, immutability, availability, and interoperability [17, 26].

4 Related Works Studies

In this section, we present some related works studies toward transparency and traceability in SCM with the help of blockchain and smart contracts.

The research from [28] shows the possible advancements of blockchain technology in operations and supply chain management. It includes enhancing product safety and security, reducing supply chain costs, improving supply chain sustainability, reducing third-party dependencies, and reducing illegal counterfeiting. The research highlights the need for further studying the blockchain technology opportunities for further adaption to supply chain operations. The research in [29]

[2] Different terms are associated with the miner, for example, full node, validator, and backer.

shows a traceability mechanism for the medicine supply chain. The approach intends to trace information from manufacturing to end consumer, which will be retrieved by scanning QR code of medical products. The authorized parties, which are authorized by the regulatory authorities of the medical supply chain, can retrieve this information. This solution, that is, “Medical supply chain” uses permissioned blockchain [30] and has a transaction data structure similar to Bitcoin [31], with a slight difference in encryption of QR code. The research from [32] explores a blockchain-based solution as a proposal to enforce sustainability in supply chain management in terms of worker protection and a safe work environment. The solution intends to respond to the consumer inquiries for social sustainability requested by consumers. It uses blockchain, IoT, and big data analytics to perform traceability from sellers and respond to consumers. The research from [33] shows an approach for digitizing and sharing the vehicles. It intends to solve the issues of vehicle odometer fraud by proposing a blockchain-based solution for storing, managing, and sharing vehicle life cycle information with several stakeholders. Similarly, in [34] a proof of concept is shown for the trading of cars in the “market of lemons[3]”. It uses the principal blockchain technology features, and it organizes the research works based on design science research to provide a trustfree platform. In case of any possible error, the research includes the safeguard mechanism in transaction correction for trading in “market of lemons” [17]. The research from [35] presets a product life cycle (PLM) management. It intends to collect and manage information and knowledge to achieve competitiveness. The raised issues are sharing this information among the involved stakeholders, highlighting concerns in inseparability, openness, and decentralization since PLM is mainly implemented in a centralized way. To overcome the mentioned issues, this research proposes a blockchain-based solution integrated with IoT and M2M. In [36], the certificate of provenance for goods is proposed by using blockchain. The research in [37] presents an independent online shipment tracking framework, which intends to complement the current SCM enterprise-based solutions. The research is related to the transportation of goods from supplier to customer, known as the physical distribution phase. The current online shipment solution is considered restricted to all stakeholders, information is provided by a carrier, the sharing of information is done on a needed basis, and it remains a single source of information. The research from [38] presents *originChain,* a traceability system based on BC and smart contracts. This system intends to provide transparent, tamper-proof traceability data, data availability, and also it considers regulatory-compliance aspects by automatically checking them. It is mainly applied to companies that import products to China. It considers the traceability perspectives of the suppliers and retailers. The supplier’s traceability perspective is to prove the product origin and quality and regulatory compliance, while the retailer’s perspective is on product origin and quality. The *originChain* works as traceability providers, and the stakeholder that needs such a system applies for traceability services. The architecture of *originChain* indicates that the nodes are

[3] Market of Lemons: https://www.investopedia.com/terms/l/lemons-problem.asp

geographically distributed over three different premises and supported by private BC. Data storage aspects in the BC manage several data sources off-chain while storing the hash address of such data on-chain. However, this solution is limited to service providers, and its traceability services are provided following a "contract" signed between parties for the offered traceability services. The research from [39] treats the problem of determining the provenance for the goods in the supply chain. In an inter-organizational and complex supply chain, the physical provenance of goods, for example, pharmaceutic or authentic luxury goods, is not always possible because of technological limitations and the complexity of the supply chain. For solving such issues, this research highlights the potential of BC technology. In combination with IoT and using the ontologies that represent knowledge about provenance and traceability, provenance issues are answered. This research aims to develop an ontology-based BC approach for responding to provenance problems in the supply chain. Using the ontologies is for better data standards and formal specification for automated interfaces, which helps develop a better supply chain. In this context, the TOVE Ontology[4] for fundamental concepts of traceability is used to provide the provenance of goods in SC. Proof of concepts is developed, which uses a "traceable resource unit," an object to be traced from one part to another part of SC [40].

Beyond the current research, our approach presents a dynamic digital certificate for transparency and traceability improvements in the supply chain of DG. It considers dynamic environment parameters retrieved during transportation and warehousing of DG. In the context of our study, the concept of digital certification does not indicate any static issued statement, but indeed it signifies the end-to-end life cycle of specific DG, including all involved stakeholders, processes, and information. We present a concept of a digital certificate associated with a specific TDG process and dynamically maintain changes at the administrative, static (physical level), and dynamic level (environmental data retrieved from the DG surrounding environment). The proposed blockchain-based digital certificate continuously maintains the DG state and remains active until the end of the DG life cycle.

5 Blockchain-Based Digital Certificate for Transparency and Management of TDG

This section shows the conceptual approach for a digital certificate for improving the transparency in transport of DG.

[4] http://www.eil.utoronto.ca/theory/enterprise-modelling/tove/

5.1 Conceptual Approach for Blockchain-Based Digital Certificate

In a single DG lifecycle, the process of transport and management[5] of DG imposes at last three operation phases. The first phase is the “preparation for TDG,” the second phase is the “process of transport of DG,” and the last phase is the “treatment of DG” which certainly finishes the life cycle of a DG. With the concept of “digital certificate,” we intend to maintain traceable information for any DG operational phase. Figure 3 shows the concept of formulation of digital certificate.

At the first phase, that is, “process of transport of DG,” the specification and set of information about “authorization” to transport DG are required. Further, the identification of the involved stakeholders and DG physical characteristics need to be provided. That immediately establishes the core of the *digital certificate* which indicates that a specific set of parameters is established (stored) in distributed ledger with the help of SC. In the subsequent phases of the process of TDG, the “same” digital certificate (specific to DG) is continuously “up-dated” (addind a new parameter to the ledger). Following in the second phase, that is, “process of transport of DG” the information about the transport process is continuously captured and immutably stored in the blockchain. The eventual update on DG characteristics, for example, quantities or physical parameters, is evidenced and reported immediately to the responsible stakeholders. Finally, the third stage, that is, “treatment of DG” gathers all the details about the final treatment of DG, which also indicates the end of the DG life cycle.

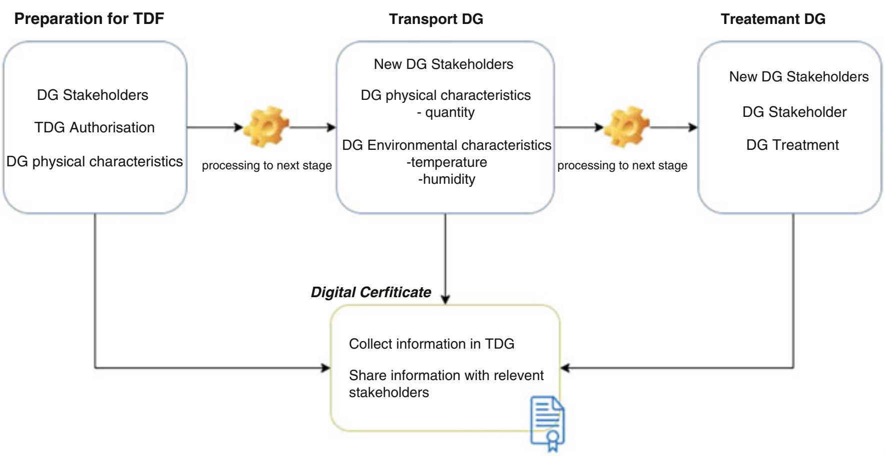


Fig. 3 The concept of the digital certificate from a different process perspective

[5] The term “management” describes storing, maintaining, and processing the DG.

5.2 Digital Certificate as for the DG

This section presents the conceptual design of the digital certificate.

The TDG stakeholders, particularly the competent authorities, require surveillance of DG movement across the geographic area under their jurisdiction in and cross-border context. The stakeholders and even the end customers require information for the physical flow of goods from the departure point to the destination point. To have access to a such information, the establishment of a traceability mechanism is required. Traceability is the possibility to track and trace the history, administration, or location of the DG located in the warehouse or during transportation [2]. Tracking and tracing the information of the active and passive processes in the TDG enhances monitoring and auditing aspects. The active traceability makes it possible to know the exact location of the DG that is in transit. The passive traceability enables the inquiry of any possible information regarding the completed process in TDG.

To manage the traceability aspects, we present the concept of *digital certificate*. The *digital certificate* is established at an early TDG planning phase, before transport starts, by gathering the necessary information, as shown in Sect. 3. The *digital certificate* remains valid during and after the transport process. It contains significant information articles for the TDG. Instances of such information includes "ID_DG_Process," "ID_DG_Provider," "ID_DG_Receiver," "ID_DG_Transporter (Sub_Contractors_ID)," "ID_DG_Good," "loading, quantity at departure (or arrival)," "risk level (sensitivity)," "Truck _ID," "Container_ID," "ID_IoT_Devices," and "Timestamp."

Additionally, we introduce the article "ID_IoT_Devices" representing the set of all IoT devices that are part of our TDG control system. The IoT device allows for capturing digital information from physical objects (truck, containers), provides real-time information for the geographic location of DG, and measures the DG state inside the truck. In [7], we presented an extensive study on the integration of blockchain and IoT. Furthermore, the "Container_ID" identifies any container (or other types of the load of DG), while "Truck_ID" presents the identification of the truck that transports the DG. In a single transport process, there might be several trucks involved. The "timestamp" identifies the date and time of any activity involving the DG. The aforementioned information articles remain available and are updated during the process flow. New values are captured and appended in the *digital certificate* articles based on "local information push" and "real-time" information flow. At any time, the authorized stakeholders may retrieve the *digital certificate* with all the information during an end-to-end process. The information retrieval is further shown in the Merkle-tree style (BC data structure). At a high-level view, the *digital certificate* concept presents a virtual *sub-ledger* formed from the global ledger. It presents an interactive component that allows new information articles to be added based on the need for that information. We propose using SC to gather and store this information as a segregated sub-ledger, maintaining the transaction history for an end-to-end process.

Figure 4 illustrates the concepts of a *digital certificate* in an end-to-end transport. As shown here, the certificate is established with significant information articles

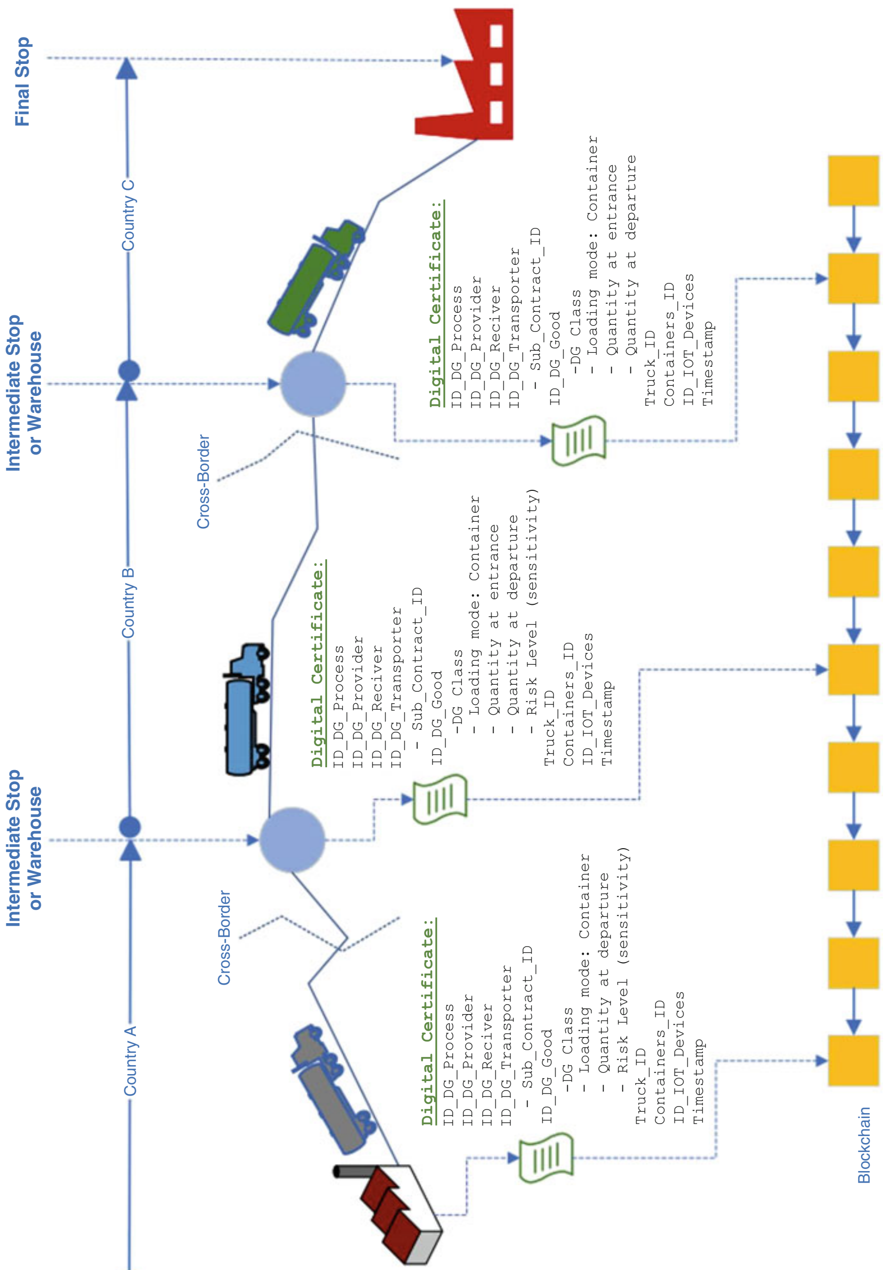


Fig. 4 The concept of digital certificate for digital traceability and management of DG

at the departing point in the transport process. It gathers previous information known from the certification of the stakeholder process and authorization and combines additional detailed information for the transport process. There might be intermediate stops[6] during the transport process in different countries (e.g., from country A to country B). At any entry on the intermediate stop, the *digital certificate* is updated with the last (on the push and real-time) information. The intermediate stop might play the role of warehousing the DG, meaning that the transport will not continue immediately, and the DG received remains stored there for a certain time. The *digital certificate* remains open for this process, identified by articles "ID DG Process." After a certain time, the same DG may be moved to another warehouse or directly to the destination point. It uses the same *digital certificate* to continue the process and update it accordingly.

We formally present some parameters, that is, quantity that we consider continuously in the *digital certificate* with the help of SC.

Consider we have the set of DG noted D.

$$(\forall d \in D)\,(\exists\, quantity\,(d) = \epsilon) \xrightarrow{transportation} (\forall d \in D)\,\big(\exists\, quantity\,(d) = \big(\epsilon' \vee \epsilon\big) \wedge \big(\epsilon \neq \epsilon'\big)\big) \tag{1}$$

In the Eq. (1), the ϵ signifies DG quantity (ϵ' - different quantity). After transporting and warehousing DG, the quantity may differ from its initial measure. This signifies that either the DG is separate in other quantities or used partially (if the warehouse is the destination point). The *digital certificate* calculates these quantities and keeps the ledger updated. Even in the situation in which the separated part is transported to other stakeholders (may be located in other countries), which might be repeated several times (by subcontracting other certified transporters), it still keeps that information until the end of the life cycle of the DG. That highlights aspects of monitoring and control for DG, even if they are separated into smaller quantities. The final step on the digital certificate counts k-parts as the sum of entire quantity of DG ($\epsilon = \epsilon_1, \epsilon_2, \ldots, \epsilon_k$, thus $\epsilon = \sum_i^k \epsilon_i$) from its departure until its treatment. Formally and empirically, that is the first indication that the DG is treated according to the regulatory framework and not misused (thrown in open land or sea).

The digital representation of DG and its characteristics through *digital certificate* enhance the management aspect in TDG. We refer to the ability to manage some characteristics of DG digitally as *digital management.* The *digital management* aspects provide stakeholders with extensive information for the current capacity, type, and related storage information for the DG in the warehouse. Based on that information, they might decide if they possibly host additional quantities of the DG or not. Furthermore, the digital information for the DG distributed in several warehouses allows stakeholders to have the most relevant information about their DG capacities circulation under their ownership. In the context of *digital*

[6] Contrary to the warehouse where DG is stored for a longer time, the intermediate stop is used for driver exchange or rest, and in terms of time, it takes several minutes until to H hours.

management, the information is received digitally. Unlike paper-based approaches, we measure the temperature (or humidity) of the arriving DG and write it on paper. In the paper-based approach, after a certain time, there is not only the disadvantage of one-time temperature measures on arrival, but also there is no mechanism to prove that the temperature was as it is written on the paper. Moreover, there is no way to return on that particular day (or hour) and verify the process flow with empirical data. The *digital management* provides digital information in the end-to-end process. Monitoring the state of DG is during the entire end-to-end process enhances quality control aspects and improves the management aspects of the process, and in addition, it can be verified at any time. Awareness of the current location of the DG and its condition is managed through the TDG control system. This tracking and tracing feature allows quick response in case of emergencies identified autonomously by the IoT devices or by manual alerting (by information push). In both cases, the system provides information to the involved authorities and the emergency response teams.

6 Proof of Concept (PoC): Smart Contract for Digital Certificate

This section aims to show details of the initial proof of concept (PoC) implementation for blockchain-based *digital certificate.*

To evaluate our approach, we used Hyperledger Fabric (HF) Go Lang SDK [41] for implementing the PoC. Our approach proposes a collaborative architecture that allows different stakeholders to join the network and share information based on their operations in TDG. This architecture enables future prospective stakeholders to join the network continuously. To achieve that, we deploy HF-based architecture, which further allows us to develop TDG system components. In this solution, we assume that all the involved stakeholders are allowed to access all information. Thus, we share all this information in a single channel, named *"Global Channel TDG."* Figure 5 shows the architectural organization of the proposed solution. The network is composed at last of four blockchain nodes (knows as *peers* in HF jargon), that is, "DG Receiver," "DG Transporter," "DG Provider," and "Authorities." These nodes use the *"Global Channel TDG"* as a communication channel to exchange information for TDG.

To draw attention to the business logic of the *digital certificate*, we developed SC called *SC_Digital_Certificate.* It is installed (deployed) in the *"Global Channel TDG,"* operates actively on the shared channel, and collects information according to the TDG process stage. Collecting and sharing a particular set of information, the *SC_Digital_Certificate* formalizes a mini-ledger for each DG, thus composing the *digital certificate.* Listing 1.1 presents a small code partition of the *SC_Digital_Certificate,* while the complete code is shown in [42].

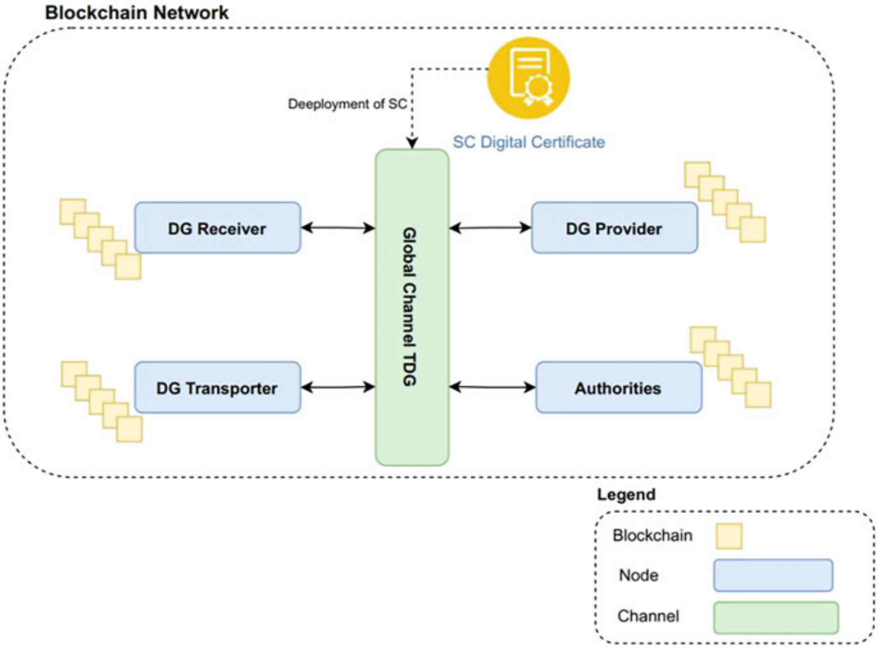


Fig. 5 The network of BC-based stakeholders in TDG

For accessing and testing the digital certificate SC, we have specified an API[7] which enables us to interact with the *digital certificate.* This interaction allows us to retrieve the information that is listed in the *digital certificate.* Listing 1.2 shows the information retrieved from the *digital certificate* in JSON format. The components "id_Certificate":ID_0006101 identifies uniquely the *digital certificate* for curtain DG (or process, identified "id_DG_Process":ID_DG_0011658. In an end-to-end process, the information received is continuously added in the *digital certificate* parameters, thus forming a completed ledger of transaction related to a specific DG associated with a specific process, that is, "id_DG_Process":ID_DG_0011658. The information stored in the digital certificate also serves as a referential point for the other SCs, which are complementarily implemented to support the TDG system. For example, by receiving the information from IoT devices, in case of the temperature, for example, "id IoT Temp Data": +33.11 °C passes the risk level "risk-Level":T + 31 °C, then another SC is triggered to notify the relevant stakeholders for a possibly disastrous situation. Similarly, it maintains trace on the quantity of DG in the departure point, that is, "quantity_At_Departure":6.5 liters/ton, then it checks the quantity at "quantity_At_Entrance" in the warehouse

[7] Application programming interface for GO: https://github.com/hyperledger/fabric-contract-api-go

of at the destination point. That helps to audit the process and being aware of how the DG are distributed among several stakeholders for treatment or are treated at a single destination point.

```
type Certificate struct {
ID_Certificate string ‘json :“id_Certificate”‘
ID_DG_Process string ‘json :“id_DG_Process”‘
ID_DG_Provider string ‘json :“id_DG_Provider”‘
ID_DG_Receiver string ‘json :“id_DG_Receiver”‘
ID_DG_Transporter string ‘json :“id_DG_Transporter”‘
Sub_Contract_ID string ‘json :“sub_Contract_ID”‘
ID_DG_Good string ‘json :“id_DG_Good”‘
DG_Class string ‘json :“dg_Class”‘
 Loading_Mode string ‘json :“loading_Mode”‘
 Quantity_At_Entrance string ‘json :“quantity_At_Entrance”‘
 Quantity_At_Departure string ‘json :“quantity_At_Departure”‘
 Risk_Level string ‘json :“risk_Level”‘
 Truck_ID string ‘json :“truck_ID”‘
 Container_ID string ‘json :“container_ID”‘
 ID_IoT_Devices string ‘json :“id_IoT_Devices”‘
 ID_IoT_Devices_Data string ‘json :“id_IoT_Devices”‘
 Timestamp string ‘json :“timestamp”’
 }
 /*...more lines of code ... */
 func (s *SC_CERTIFICATE) CreateCertificate(ctx contractapi.
 TransactionContextInterface, certificate string) (string,
 error){

 var dg_process_certificate Certificate

 /*...more lines of code ... */

 if process_certificate != nil {
 fmt.Printf(“the certificate already exist with ID %s”,
 dg_process_certificate.ID_Certificate)
 return “The certificate already exists”, err
 }
 /*...more lines of code ...*/

 func (s *SC_CERTIFICATE) UpdateCertificate(ctx contractapi.
TransactionContextInterface ,certificate_updated string) error {

 /*... more lines of code ... */
```

Listing 1.1 The short representation of code for SC Digital Certificate


```
{“id_Certificate”:“ID_0006101”,
“id_DG_Process”:“ID_DG_0011658”,
“id_DG_Provider”:“Esch Hospital”,
“id_DG_Receiver”:“EcoGroup Swiss”,
“id_DG_Transporter”:“AGI Transport Group”,
“sub_Contract_ID”:“--”,
“id_DG_Good”:“DG611768”,
“dg_Class”:“6.1”,
“loading_Mode”:“container”,
```

```
    “quantity_At_Departure”:“6.5 liters/ton”,
    “quantity_At_Entrance”:“6.5 liters/ton”,
    “risk_Level”:“T+31C”,
    “truck_ID”:“TR006987”,
    “container_ID”:“CO698774”,
    “id_IoT_Temp”:“TempIoT:DHT11DG”,
    “id_IoT_Temp_Data”:“+20.17C”,
    “id_IoT_Location”:“EM-506RE”
    “id_IoT_Location_Data”:“49.497509, 5.982500”
    “timestamp”:“14/05/2021 17:01:12”}
```

Listing 1.2 The representation of the digital certificate in JSON format

7 Conclusion and Future Works

Transparency and traceability are critical properties in numerous supply chains. Similarly, in TDG, transparency is highly required from the involved stakeholders, particularly from the authorities as the responsible party to govern this process. In this work, we present the concept of the digital certificate, which enables storing and maintain information for an end-to-end TDG. The digital certificate proposes an active and dynamic mini-ledger that allows continuous monitoring of the DG state. In TDG, there are specific parameters (temperature, humidity) that need to be kept under control to avoid adverse situations. We propose a blockchain-based digital certificate to maintain the TDG process and actively update its state according to the information received from IoT devices or stakeholders. The proposed digital certificate is dynamic, and it is associated with a specific DG, thus enabling the digital management of DG. The dynamicity remains on selection, sharing, and triggering other events with the help of different SC. At the TDG process run-time, collecting this information in real-time enables monitoring the TDG process by responsible stakeholders. The digital certificate enables TDG process audit, thus at any time, the relevant (authorized) stakeholders in TDG can request specific information to verify the correctness of the process.

In the actual pandemic of COVID-19 [43], safe transportation of vaccine is crucial. The issue with the COVID-19 vaccine transportation is the maintenance of low-rate temperature degree, which may expose several risks if the temperature is not maintained in the range of “normality.” In such a situation, to improve transparency, it must have real-time information that remains immutable during the end-to-end process. Thus, the digital certificate would add value to improving transparency since the received real-time information remains immutable.

We consider the proposed approach a contribution to the transparency in supply chain by storing almost dynamically information on the blockchain. In future works, we intend to extend the operation scale of our approach by extending the number of involved stakeholders and providing large-scale IoT devices.

References

1. Lukasik, Z., Kúsmińska-Fija'lkowska, A., & Kozyra, J. (2017). Transport of dangerous goods by road from a European aspect. *Zeszyty Naukowe. Transport/Politechnika Slaska*.
2. Imeri, A., & Khadraoui, D. (2018). The security and traceability of shared information in the process of transportation of dangerous goods. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS),* 1–5. IEEE.
3. U. N. E. C. for Europe (UNECE). (2020, Nov 19). Agreement concerning the international carriage of dangerous goods by road (ADR 2021). In *European Agreement Concerning the International Carriage of Dangerous Goods by Road (ADR).*
4. Ding, L., Chen, Y., & Li, J. (2016). Monitoring dangerous goods in container yard using the internet of things. *Scientific Programming*, 1–25.
5. Mentzer, J. T., et al. (2001). Defining supply chain management. *Journal of Business Logistics, 22*(2), 1–25.
6. Li, Q., & Liu, A. (2019). Big data driven supply chain management. *Procedia CIRP, 81*, 1089–1094.
7. Imcri, A., Agoulminc, N., & Khadraoui, D. (2020). Blockchain and IoT integrated approach for a trusted and secured process to manage the transportation of dangerous goods. *Revista de Sistemas e Computaç ão-RSC, 10*(1), 26–41.
8. Imeri, A., Khadraoui, A., & Khadraoui, D. (2017). A conceptual and technical approach for transportation of dangerous goods in compliance with regulatory framework. *JSW, 12*(9), 708–721.
9. European agreement concerning the international carriage of dangerous goods by inland waterways: (ADN) including the annexed regulations, applicable as from 1 January 2017. volume 1: OCLC: 992936978.
10. RID. Intergovernmental organisation for international carriage by rail (RID). (2019, Jan). https://otif.org/en/?pageid=1105. Accessed on 02/15/2020.
11. OTIF. International martime organization (imdg) code. (2019, Jan). https://www.iata.org/en/publications/dgr/. Accessed on 02/15/2020.
12. IATA. (2017, Jan). Dangerous goods regulations. https://www.iata.org/en/publications/dgr/. Accessed on 02/15/2020.
13. Torretta, V., Rada, E. C., Schiavon, M., & Viotti, P. (2017). Decision support systems for assessing risks involved in transporting hazardous materials: A review. *Safety Science, 92*, 1–9.
14. Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 75–105.
15. Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45–77.
16. Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Action design research. *MIS quarterly,* 37–56.
17. Imeri, A., Agoulmine, N., Feltus, C., & Khadraoui, D. (2019). Blockchain: Analysis of the new technological components as opportunity to solve the trust issues in supply chain management. In *Intelligent Computing-Proceedings of the Computing Conference* (pp. 474–493). Springer.
18. March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems, 15*(4), 251–266.
19. de Noimalizacio'n, O. I. (2011). ISO-IEC 25010: 2011 systems and software engineering systems and software quality requirements and evaluation (SQuaRE)-system and software quality models. *ISO.*
20. Feltus, C., Khadraoui, D., De Remont, B., & Rifaut, A. (2007). Business governance based policy regulation for security incident response. *Crisis*, *7*.
21. Imeri, A., Agoulmine, N., & Khadraoui, D. (2019). A secure and smart environment for the transportation of dangerous goods by using blockchain and IOT devices. In *7th International Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE 2019),* 1–8.

22. Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352–375.
23. Antonopoulos, A. M. (2014). *Mastering bitcoin: Unlocking digital cryptocurrencies*. O'Reilly Media, Inc.
24. Nguyen, G.-T., & Kim, K. (2018). A survey about consensus algorithms used in blockchain. *Journal of Information Processing Systems, 14*(1), 101–128.
25. Bouraga, S. (2021). A taxonomy of blockchain consensus protocols: A survey and classification framework. *Expert Systems with Applications, 168*, 114384.
26. Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., & Rimba, P. (2017). A taxonomy of blockchain-based systems for architecture design. In *2017 IEEE international conference on software architecture (ICSA),* 243–252. IEEE.
27. Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering, 59*(3), 183–187.
28. Cole, R., Stevenson, M., & Aitken, J. (2019). Blockchain technology: Implications for operations and supply chain management. *Supply Chain Management: An International Journal*, 469–483. https://eprints.lancs.ac.uk/id/eprint/131605/
29. Kumar, R. & Tripathi, R. (2019). Traceability of counterfeit medicine supply chain through blockchain. In *2019 11th International Conference on Communication Systems & Networks (COMSNETS),* 568–570. IEEE.
30. Helliar, C. V., Crawford, L., Rocca, L., Teodori, C., & Veneziani, M. (2020). Permissionless and permissioned blockchain diffusion. *International Journal of Information Management, 54*, 102136.
31. Nakamoto, S. (2019). Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot.
32. Venkatesh, V., Kang, K., Wang, B., Zhong, R. Y., & Zhang, A. (2020). System architecture for blockchain based transparency of supply chain social sustainability. *Robotics and Computer-Integrated Manufacturing, 63*, 101896.
33. Brousmiche, K. L., Heno, T., Poulain, C., Dalmieres, A., & Hamida, E. B. (2018). Digitizing, securing and sharing vehicles life-cycle over a consortium blockchain: Lessons learned. In *2018 9th IFIP international conference on new technologies, mobility and security (NTMS)*, 1–5. IEEE.
34. Notheisen, B., Cholewa, J. B., & Shanmugam, A. P. (2017). Trading real-world assets on blockchain. *Business & Information Systems Engineering, 59*(6), 425–440.
35. Liu, X., Wang, W., Guo, H., Barenji, A. V., Li, Z., & Huang, G. Q. (2020). Industrial blockchain based framework for product lifecycle management in industry 4.0. *Robotics and Computer-Integrated Manufacturing, 63*, 101897.
36. Martin, M. First ever European certificate of origin through blockchain — business west. https://www.businesswest.co.uk/blog/first-ever-european-certificate-origin-through-blockchain, 06 2018. Accessed on 05/08/2021.
37. Wu, H., Li, Z., King, B., Ben Miled, Z., Wassick, J., & Tazelaar, J. (2017). A distributed ledger for supply chain physical distribution visibility. *Information, 8*(4), 137.
38. Lu, Q., & Xu, X. (2017). Adaptable blockchain-based systems: A case study for product traceability. *IEEE Software, 34*(6), 21–27.
39. Kim, H. M., & Laskowski, M. (2018). Toward an ontology-driven blockchain design for supply-chain provenance. *Intelligent Systems in Accounting, Finance and Management, 25*(1), 18–27.
40. Imeri, A., Khadraoui, D., & Agoulmine, N. (2019). Blockchain technology for the improvement of SCM and logistics services: A survey. In *Industrial engineering in the big data era* (pp. 349–361). Springer.
41. Fabric, H. Introduction — hyperledger-fabricdocs main documentation. https://hyperledger-fabric.readthedocs.io/en/latest/blockchain.html. Accessed on 05/09/2021.
42. Imeri, A. Smart contract codes. https://git.list.lu/adnan_imeri/thesisaimeri/-/blob/master/SmartContractCodes/SC_Digital_Certificate_DG. Accessed on 05/14/2021.
43. County-Level COVID-19 Vaccination coverage and social vulnerability — united states, December 14, 2020–March 1, 2021. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7993557/. Accessed on 05/15/2021.

An ERP and Planning System Enabled Decentralized Supply Chain Using Blockchain Technology

Arnab Banerjee

1 Introduction

Supply chain is the vital link in any organization that controls the relationship of demand and supply through the coordination of manufacturer, supplier, logistics provider, and customer. The goal of any supply chain is to deliver greater value to end customer, most economically in the shortest possible time with the best possible quality. Supply chain is an established and essential business process that connects a customer's requirement with a supplier through a channel of manufacturer or distributor. There is a tremendous focus to rationalize and improve supply chain processes in the current pandemic situation. To better serve a customer and meet their service level expectations, the supply chain needs to be extremely agile and adaptable, while to be economical, it must be lean. To balance this regime of being agile while being lean has led to many supply chain strategies. Some of the renowned strategies are postponement strategy, adoption of information technology, manufacturing focused strategies, building resiliency and redundancy, adoption of many optimization techniques, and geography-specific strategy like where to manufacture and where to stock or distribute. Due to all these, the supply chain has become increasingly global in the last 20 years. The focus of manufacturing has moved to low-cost economies of Asia, while consumer market and distribution are closer to customers in North America and Europe. This has resulted in a skewed supply chain with a global appeal and complex decision-making process. Today, the supply chain is distributed with an intricate network and lot of dependencies. The time for decision making is becoming an increasing important factor to effectively serve customer at right time with right cost.

A. Banerjee (✉)
Global Supply Chain, Micron Technology, Hyderabad, Telangana, India

A. Bouras et al. (eds.), *Blockchain Driven Supply Chains and Enterprise Information Systems*, https://doi.org/10.1007/978-3-030-96154-1_4

As per the United Nations Conference on Trade and Development (UNCTAD), there are more than 80,000 active multinational companies (*this is as per UNCTAD report of 2006*) [1]. UNCTAD defines a company as multinational if 10% of its revenue is generated outside of the home country. So, the multinational has businesses globally and is generally large corporates. Large corporations have many divisions, product lines, and geography of business, and most of the time, they are all interrelated. Simply stated, these business divisions working independently lead to a decentralized supply chain (DSC), while a central team or division deciding for the entire chain is a centralized supply chain.

Among the various strategies adopted in supply chain, there has been a lot of research on the centralization and decentralization of supply chain. Though there are certain advantages of centralization as well as for decentralization, there is no clear winner. Some well-known companies like HP decided to decentralize the supply chain structure, while Office Depot decided to centralize a previously decentralized supply chain organization [2]. This chapter relooks at the business processes in decentralized supply chain and the challenges it faces in its processes with the adoption of ERP and planning systems. Further, it examines the use and adoption of technology to solve and improve the decentralized supply chain operations.

2 Centralized and Decentralized Global Supply Chain

The supply chain construct began with the centralization as the default realm. The authority and decision-making power lied with few in the entire organization. The centralized decision making is entitled to take decision for all supply chain partners [3]. The centralized supply chain is global in nature, product-wise it could be highly diversified with multiple zones and hubs but the operation is centrally controlled. For example, consider a globalized company that has multiple subassembly plants and a final assembly plant before product is shipped to end customer. The subassembly plants will have their own supply chain with its distribution network, manufacturing operations, customer management, and suppliers. Similarly, final assembly plant will have its own supply chain with its distribution network, manufacturing operations, customer management, and suppliers, or there may be contract manufacturer as well in the network of the supply chain. But all decisions are driven by one central supply chain team which in most cases is based on the final assembly plant or corporate head office.

There are certain forces, market needs, and business reasons for decentralization of supply chain. The market demands for product variety and product mix, the low human labor costs in specific locations, the need for speed to react to customer, the constant eroding of margins, need for specific talents, evolution of Information and Communication Technologies enabling information exchange, and political forces are the principal reasons toward globalization and decentralization.

In a decentralized supply chain, the decision making is housed in the entity facing the immediate customer and managing its supply chain. In a way, it independently

Table 1 Comparison of centralized and decentralized supply chain

Centralized supply chain		Decentralized supply chain	
Pros	Cons	Pros	Cons
Standardized systems and processes	Limited to geographic talent	Better service to customer. Better service level	Lesser bargaining power and economy of scale
Company culture is consistent	Cost ineffective (no cost advantage)	Extremely agile	Reduced control on culture
Better and consistent visibility	Agility and nimbleness is a challenge	Reduced cost operations due to localized effort	Visibility challenges
Leaner supply chain compared to decentralized	Reduced service levels	Better ability to handle market-specific product	Lesser control on operations
Lower logistics spend	Lesser ability to handle market-specific product	Better customer trust and customer relevance	Increased logistics spend
Better control on operations	Reduced supply chain velocity	Increased supply chain velocity	

manages the demand, supply, and resources. The decision making is localized for each area or entity. In the previous quoted example of the globalized company with multiple subassembly plans and a final assembly plant, the decision making is at individual plant managing the supply chain. In a way in the entire supply chain of subassembly plants, final assembly plant, contract manufacturer, and distributors, every entity owns plans and manages it themselves. Based on experience and study, the author has prepared a comparison of centralized and decentralized supply chain. Table 1 shows the comparison with pros and cons.

Centralized global supply chain is an ideal scenario. In today's world with globally spread supply chain where sourcing of products is from all over the world, manufacturing being very Asia centric and distribution being closer to end customer an ideal centralized supply chain is far from being reality. Today, almost all multinational companies with global operations follow a decentralized supply chain.

2.1 *Challenges in Decentralized Global Supply Chain*

There are numerous challenges facing a decentralized supply chain today. It can range from taking an appropriate and informed decision, local optimized performance, attaining global optimal performance, and serving the best to end customer to name a few. In this section, we study such challenges.

The challenges are studied in two folds. The first step is to review the published literatures and identify the problems discussed therein which are still not appropriately solved. A further synthesis and analysis of these challenges are provided with practical examples. Then (second) the author shares the challenges he came across in his experience related to this area which are not having appropriate published literature. The literature review was carried out to understand, analyze, and prepare taxonomy of the issues as per the researchers in decentralized supply chain across the world. Table 2 shows the taxonomy of the challenges in decentralized global supply chain.

In the published problems in Table 2, there are certain aspects which are not clearly highlighted. Ψ1For example, in forecast-related problems, readers will assume that there are techniques available like CPFR or customer forecast generation which should solve the problem of forecasting. But with pandemic hitting the world, the dependency of people became an equal factor. With the aspect of digital information, independence from human effort became immensely important. With most of the transactions going online, the real-time availability of transparent data, which can be trusted and transaction being non-repudiated, became very important. These cannot be solved by traditional CPFR techniques or EDI mechanisms. Due to the introduction of e-commerce and hypersonic fast supply chains, the demand shaping methodology is changing. The supply feed is turning in daily and which is being changed in to an everyday demand sensing and demand shaping process. This is leading to extreme agile and customer savvy supply chain owing to the digital age of buying and selling. This needs an unprecedented level of demand and supply transparency which is not possible with traditional techniques of CPFR. The need for data is far more real time, accurate, and trustworthy. These are some of the aspects not possible with CPFR. Ψ2Similarly, inventory remains a key focus area for every company. No one wants to store unwanted inventory, neither do they want to lock their capital. Every company wants to hedge its risk but want the availability when required. That's why concepts of bonded inventory, vendor managed inventory, and supplier consigned are very popular. Most of these use EDI as the technique of communication apart from emails. The need of the hour is to establish a continuous, trustworthy, transparent system which is not highlighted by these researches.

Review of the published literature brings out a very strong similarity among the problems discussed in the listed papers. All the published research papers build a mathematical model to solve a specific problem which is noteworthy, achievable, very appropriate and helps optimize the supply chain. But in all the cases, it leaves out the softer aspects like that of trust among the entities, information sharing risk, human aspects of information, real-time visibility of information, trust of data, availability of data, standardization of data, variability in data and allied challenges related to these. In some cases, it is noted as an assumption and asked to be treated separately. Another aspect which came up very clearly in these paper reviews is that in many of the cases, there are assumptions that decisions made are completely rational, informed, and devoid of any human behavioral impacts. Realistically, there is not much research done which touches on these aspects, namely:

Table 2 Taxonomic analysis of challenges in decentralized supply chain

Decentralized supply chain challenges		
Groupings	Description	References
Information delays and synchronization issues	Cases of information delay and information loss due to decentralization. Information synchronization and distortion is a known issue in decentralized supply chain	[4, 5]
Organizational barriers, collaboration issues, and decision making	Collaboration challenges among partners due to lack of transparency and visibility. Managerial decisions get challenged from one partner organization to another. Decision making is slow and gets challenged Organizational barriers of material control and cash flow are a significant challenge in decentralized global supply chain	[6, 7]
Challenges in manufacturing and material flow	Collaborative production network Risk in global transportation Coordinating manufacturing complexity Controlling cost Optimizing or trade-off between cost, quality, and flexibility	[8]
Challenges in supplier development	Geography-specific supplier development Development of competing suppliers in different geographies Supplier trust to discourage any chance of opportunistic expropriation	[9]
Challenges in forecasting Ψ1	Sharing of information among various entities which is required to generate an accurate forecast Challenges in confidential policies Challenges in data reliability and standardization Lack of information system's compatibility Increased risk of demand uncertainty	[10]
Supply planning challenges	Local optimization vis-à-vis a global optimization Sharing unreliable/inflated numbers Local constraints playing a role Sharing partial information about things and entities which determine a good supply plan	[11]
Challenges in inventory management Ψ2	Inventory synchronization Optimizing the inventory holding cost across entities for a global supply chain optimization (not driven by individual entity optimization/profit) Replenishment order synchronization Time coordination of decisions and information sharing	[12]
Supply chain risk	Misalignment of incentives between suppliers and buyers Competition among suppliers Competition among buyers Asymmetric information among supply chain parties	[13]
Bullwhip effects	Amplification or stock out of inventory Negative impact on customer service Huge variance in inventory holdings	[14]

(continued)

Table 2 (continued)

Decentralized supply chain challenges		
Groupings	Description	References
Challenges in profit sharing and intercompany accounting	The idea of profit sharing for the global optimization of supply chain is not widely practiced The intercompany accountings are generally not shared and transparency in those is missing	Author's experience
Trust and decision-making issues	The element of trust is highly sensitive in decentralized supply chain	Author's experience
Information transparency issues	Entities with companies or entities across companies though being supply chain partners are not open to share facts, information, and data	Author's experience
Inventory visibility issues	Providing visibility of entity's own inventory is highly sensitive and most of the organizations are not open to this concept	Author's experience

1. How will information be made available seamlessly across supply chain entities?
2. How do we factor in the element of trust in information availability?
3. How to bring the aspect of rationality in information availability and how can these be tied back to decisions made?
4. How to remove the information misalignment to facilitate a sound and rational decision?
5. What are the means and measure of information synchronization?

The subsequent sections of this chapter deal with the options on how to solve these problems. It analyzes and proposes mechanisms on how appropriate and matured technology can solve these problems. It relooks at the fundamental way of structuring and using technology for decentralized supply chain. It identifies pillars and drivers of decentralized supply chain and how technology can improve them to achieve a better supply chain.

3 Supply Chain Enabled with ERP and Planning System: Capabilities and Limitations

Over the years, the supply chain management, and its processes and practices, has undergone a significant improvement. In the last three to four decades, technology has evolved from material requirement planning (MRP) to manufacturing resource planning (MRP II) to enterprise resource planning (ERP) to advanced supply chain planning and optimization (APS/APO), and today it is moving toward integrated business planning, network optimizations, and sales and operations planning. With technology adoption, the supply chain processes improved and brought significant business benefits. Almost all leading global companies run enterprise resource planning (ERP) and demand/ supply planning software [15].

Over the past two decades, ERP has had the most significant impact on supply chain processes and its improvements. However, despite these improvements and enabling of digital processes with enterprise grade digital infrastructure, most companies struggle with visibility into demand, operations, and supply. Bringing the decentralization aspect into it, the challenge becomes murkier and intruding. ERP is a system that integrates the departments of an organization and its resources to maximize utilization and performance. ERP transforms how the organization interacts intrinsically and extrinsically. It provides a platform for all the departments like production planning, material planning, operations, inventory, warehousing, design, sales, distribution, accounting, and customer service to act in unison. ERP marries the information flow to material flow creating a homogeneous environment for business processes and decision making. It removes physical boundaries and strengthens centralized processes but all within an organization or enterprise. It doesn't have the ability to cut across enterprises.

The architecture and topology of ERP fails to bridge the gap across enterprise collaborations [16]. So, data sharing across enterprises is complex and is dependent on many third-party applications. Order tracking and product traceability are currently managed through EDI and messaging systems. Reports and RFID scans are also used at various checkpoints to track the movement of goods. Most of the time across enterprises, transfer of information like that of demand, supply, inventory, and/or master data is exchanged using middleware like Boomi, MuleSoft (*to give an example*), etc. This indicates that the future system must provide real-time data from anywhere and from any system. Removing the dependency of system is one of the major improvements needed. In all these, there are few critical missing pieces which are not addressed by the ERP system. These are, namely, trust and authenticity of data, non-repudiable capability, transparency, and security of data, and above all ability to track changes with no one entity owning all the data. So, a smoother and robust interorganizational data sharing system with capabilities as discussed before is missing. This acts as a major hindrance to serve the customer more effectively.

As in ERP, planning systems have also evolved over the last two decades. They have built in optimization capabilities apart from generating a companywide supply plan for execution. The planning systems have been enhanced to provide budget plans, long-range plans/strategic plans, execution plans, network optimizing plans, sales and operations plan, and rapid plans, to name a few. Capabilities like attribute-based planning, rapid planning, and collaborative planning are developed to cater to specific industry or process needs. The planning software of today has the capability to plan not only for the current organizations but for its partners as well. Today's planning systems support vendor managed inventory and collaborative planning, forecasting, and replenishment (CPFR). But the challenge lies in having the unified master and transactional data to plan. Sharing such sensitive data by partners brings in the element of trust, which is beyond the scope of these planning systems.

4 Pillars and Drivers of Decentralized Supply Chain

Decentralized supply chain will always need to work on an overarching strategic plan across the entities to be successful. The plan will hold all partners of supply chain together with a common objective. Individual entities can drive their own decisions to meet their own local objectives. There are key aspects impacting the decentralized team in supply chain; these are:

- Ability to respond rapidly to supply chain needs
- Sudden demand shifts from customer
- Supply chain breakdown and disruptions impacting supply
- Shortages in upstream supply chain
- Localized disruption in services as happening in pandemics
- Need to cooperate and synchronize in geographically spread teams

These aspects need to be maturely handled by each team. These are possible with empowered decision team and collaborative decision making. The teams should be driven by strong relationships and customer objective in mind and not individual goals of each entity. It must be driven and supported by strategic plans. The plans have to clearly identify the supply chain pillars and drivers. The pillars and drivers must enable a trustable and cohesive decentralized supply chain.

4.1 Pillars of Decentralized Supply Chain

Figure 1 shows the pillars of the decentralized supply chain. The pillars form the founding principles on which the decentralized supply chain can operate. Based on experience and analysis, six founding principles of decentralized supply chain are

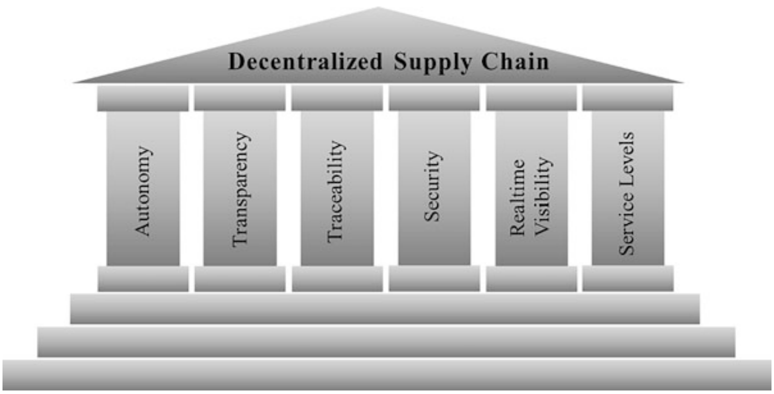


Fig. 1 Pillars of decentralized supply chain

proposed. Each of them has its own function and reason why it ought to be one of the pillars of decentralized supply chain and how it brings all the entities of the supply chain together. Each of the pillars is explained henceforth:

Autonomy This pillar is one of the guiding principles of decentralized supply chain (DSC). This provides the autonomy or independence of each entity to take its decision. But it must align with the overall structure of decentralized supply chain. The autonomy provides the ability to voice concerns and be independent in its decision and action and overall helps to grow and sustain.

Transparency This pillar drives the trust and transparency among the members of the decentralized supply chain. This is a critical element without which the decentralized supply chain cannot exist. Transparency drives alignment and orientation among many other factors.

Traceability Another aspect of decentralized supply chain that can help bring members together as well as make them responsible is the traceability. The data, decision, and information traceability form a key element of membership and reliability.

Security In a decentralized supply chain, there are several entities with numerous transactions among them. Some of these transactions are sensitive like related to design elements which can be highly confidential information or can be process related which are controlled through IP. In such transactions, there are sensitive information like formulae, demand picture, supply scenarios, customer lists, and inventory information which are confidential but are shared. The security and confidence on the security of these information sharing is of paramount importance for the success of the decentralized supply chain.

Real-time Visibility Supply chain is all about synchronizing the material flow with the information flow to meet customer demands. This becomes crucial when there are entities across enterprises. Visibility is an aspect engrained in this act of synchronization. The visibility to some of the key aspects of supply chain is very key for its uninterrupted success. These are, namely, visibility to demand, supply, inventory, in transits, fluctuations, disruptions in production, etc. These can severely impair the supply chain in a decentralized environment. So, getting a proper visibility into these critical aspects of supply chain is key to the success of decentralized supply chain.

Service Levels In a decentralized supply chain setup, the dependency among the entities is high. Service level becomes critical among them to add trust and dependency. So, matching up to the desired service levels and improving upon it calls for the smoother functioning of decentralized supply chain.

4.2 Drivers of Decentralized Supply Chain

Figure 2 shows the drivers of the decentralized supply chain. These drivers are the fusing force which keeps the partners engaged and drive them toward mutual cohesiveness. If any of these drivers are broken, then the mutual coordination among the entities are at risk, and the idea of decentralized but coordinated supply chain leads to a fragmented supply chain. It is very important to have technology, people, and process to enable and support these drivers to have a seamless and coordinated decentralized supply chain.

Based on experience and analysis, these six drivers of decentralized supply chain are proposed. Each of them has its own purpose to drive the cohesion and coordination among the entities for a unified strategic goal of the supply chain. Each of the drivers is explained henceforth:

Economics of Supply Chain Companies move toward a decentralized supply chain for many reasons. But the most important reason is the economics of the supply chain. It should always be in favor of the overall benefit of all partners. It is the economics of making things available to customer on time, in budget, and in right quantity that will drive the decentralization.

Swiftness in Decision Making Decentralized supply chain brings entities across the enterprises together. But bringing new partners in the chain brings the risk of delayed reaction or decision making. Hence, the speed of reaction or swiftness in decision making becomes a critical driver in holding the decentralized entities together toward a common goal. The swifter, smoother, and steadier the decision-

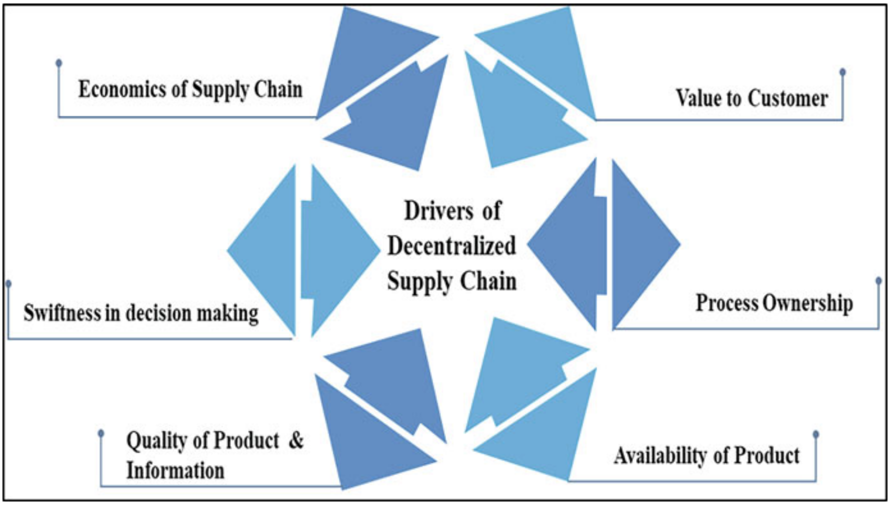


Fig. 2 Drivers of decentralized supply chain

making mechanism is, it will lead to a better performing supply chain among the partners.

Quality of Product and Information There is no denying of the fact that quality of product is the most important factor to win and retain business from customers. But in supply chain, it is the information and flow of information which makes products move. Thus, the quality of information and product helps reduce overhead among the entities and their team. The reduction in overheads reduces friction among teams leading to a well-oiled supply chain. This makes information and product flow smoother and synchronized and improve overall supply chain efficiency. So, these two aspects go together in a decentralized supply chain and drive the performance of all the entities together. This has a dominant impact on supply chain performance and sustenance in the long run.

Availability of Product Classically, supply chain brings product to customer based on their demand from supplier or manufactures it. There are numerous entities in between, and in a decentralized supply chain, the decision making is independently done by each entity. As products move through the supply chain getting transformed/manufactured or distributed toward its customer, the predictable and reliable availability of the product at each logic step at the required time holds the entities together. This predictability and reliability for making the product available decides the credibility of the entity. Superior on time availability marks a worthier credibility and reliability. This improves the supply chain performance.

Process Ownership Supply chain transactions are highly complex processes involving numerous teams, people, and technology. It involves high volume transactions and at times things go wrong or there can be disruptions. It is at these testing time the entities in a decentralized supply chain need to own up the process and solve the problem at hand. Also, they need to proactively change or improve the process to mitigate such risk or problem in the future. Having such confidence building measures and process improvements among the entities brings healthy competition (among entities/partner) and enhances supply chain performance.

Value to Customer For any supply chain, the goal is to serve the customer well. With decentralization of the decision making and processes, this becomes challenging. But the entire chain must be driven by the goal to serve immediate partner and bring value to the end customer. This value can drive the entities to serve each other and in the best interest and best way.

As we understand the pillars and drivers of supply chain, let us now look and understand the technology that can greatly help the decentralized supply chain.

5 Blockchain: A Powerful Technology to Improve Harmonization

Blockchain is a distributed ledger which records transaction data as blocks. The data in the blocks are immutable, secure and chronologically maintains transaction data. Blockchain can also be described as a network where members are a node in the chain. Blockchain uses distributed ledger technology (DLT) and using it the records created are indelible. In simple terms, blockchain acts as a platform (democratized with equal rights) and removes the dependency on a single centralized authority for any transactional data. At the same time, it is secure and transparent. Blockchain securely transfers data and centrally shares information with its members with trust playing an underlying and important role. Blockchain is a powerful mechanism to capture, store, and securely make the data available to all its members. As blockchain brings together several entities without the need for a centralized authority, it improves the coordination, trust, transparency, and harmonization among the entities/ node. The most important aspect of blockchain is it has the capability to bring together independent systems from multiple stakeholders and act as a platform. In a simple representation, Fig. 3 represents how blockchain can be a central element to several stakeholders spread across multiple systems. These stakeholders can use ERP along with any other allied/satellite systems. The data from these stakeholders will flow into blockchain, thus centralizing the transactional data in the blockchain platform. Figure 3 also shows that blockchain is independent of the integrating system and data, and thus it can bring in any new entity easily.

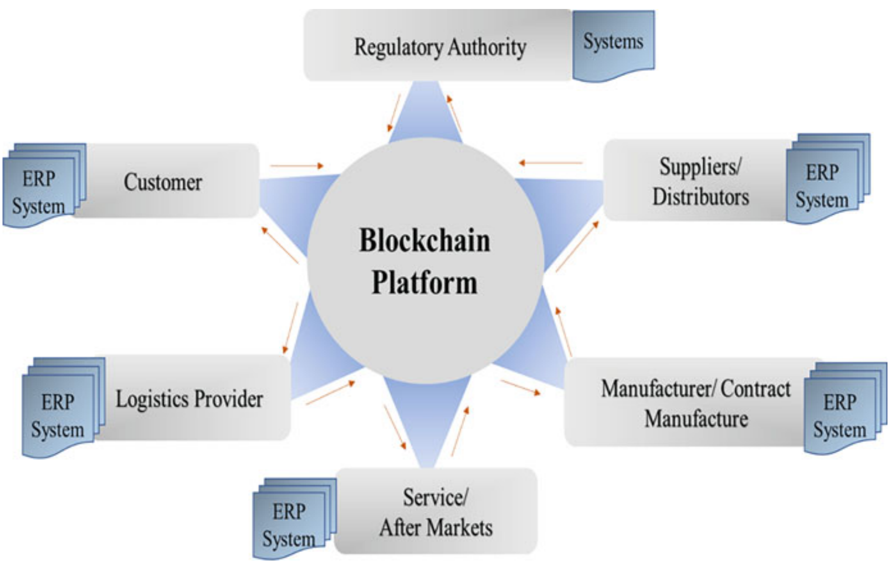


Fig. 3 Blockchain platform for multiple stakeholders

5.1 Types of Blockchain

We can see that blockchain system is a network of members (nodes) connected through a distributed ledger technology. These data are shared among several computers/ nodes rather than being stored on a central server. One of the powerful features of blockchain is on the controlled data access to certain members and the ability to write business logics through smart contracts. In blockchain, the transaction data can be verified by rules (smart contracts) applicable to all unlike a single centralized authority. The biggest benefit of blockchain is the ability to share data seamlessly and securely with partners. There are three types of blockchain as being used today. They offer different types of architecture to operate and integrate. These are as follows:

Open or Permission-less Blockchain These are also known as public blockchain. In this type of blockchain, anyone can join the blockchain network. There is no one partner or node owning or managing the rules of blockchain membership. Here, all the partners together own it and everyone is equal in the network. Bitcoin and Ethereum networks are examples of open blockchain architecture. The open blockchain network is not recommended if the blockchain is for a specific purpose. This blockchain architecture works on the consensus mechanism. The consensus mechanisms are drawn through the proof of work. The proof of work drives the need for authenticators or miners. These play a crucial role as they are the gatekeepers to verify transactions and calculate credits. This architecture requires significant computational power to maintain a large-scale distributed ledger and standardize calculations among numerous participants and authenticators. Due to this challenge, open blockchain architecture is not so readily accepted to work. Though Bitcoin network is one of the earliest known blockchain systems, there are not many like it.

Permissioned or Private Blockchain Network This architecture is more suitable if it's for a specific purpose. In this architecture, there is a particular organization or a single defined owner of the network. The owner of the network defines the specific business rules based on which members are qualified and added. Smart contracts are business rules defined to engage the members and qualify/filter the data to get into blocks. These standardized and well-defined criteria are the cornerstone of the permissioned blockchain. In the permissioned network, participant entry is decided by founding members (node) or a group of existing member (nodes), as decided by founding member. One example of private blockchain networks is Oracle Blockchain Cloud Services developed on Hyperledger Fabric.

Consortium Blockchain Network Consensus network is like a semiprivate blockchain architecture which is owned and controlled by a preselected group of members. It is not necessarily controlled by the founding member or there may be no one founding member. This group of members decides on future memberships, rules, etc. The right to read the blockchain may be public or restricted to the participants. For example, one might imagine a consortium of 15 financial institutions, each of which operates a node and of which 10 must approve every block of data for the block to be valid. A consortium blockchain provides many of the same benefits affiliated with private blockchain like efficiency and transaction privacy. R3 and BiTA are examples of consortium blockchain.

Any kind of blockchain network can be connected to multiple applications or systems. The capability of connecting blockchain networks to enterprise resource planning (ERP) system has been the most beneficial of them all [16, 17]. This has opened the opportunity to connect and transmit the transacting system data securely to partners for seamless data sharing, decision making, and transparency. As rightly stated by Litan et al. (2019), blockchain networks have emerged as a promising innovation to affirm the integrity of data shared among constituents in multiparty process collaboration. This also sets the pitch for the fitment of blockchain in a decentralized supply chain. With blockchain technology, the real-time collaboration, analytical reporting, data-driven decision making, and efficiency of transactions look very promising. This was definitely not possible few years back with the traditional systems. Blockchain has paved the way to devise process and system for making more efficient decentralized supply chain.

6 Decentralized Supply Chain Enabled by ERP, Planning System, and Blockchain

Today, most of the global companies already have ERP as their backbone execution system, while the supply chain is driven by some specialized advanced planning system. ERP enables all business transactions from manufacturing, procurement, and order management to accounting and transactional reporting. Companies collaborate with their suppliers/customer through EDI, XML, or some point-to-point messaging system. Though these specialized systems are very modern and poised for the future, they exhibit the limitations when it comes to across enterprise transactions, coordination, and collaboration. A decentralized supply chain is about the partner entities which makes the product move and meet customer demands based on information shared. It is all about the coordination among the customer, supplier, manufacturer, contact manufacturer, and service providers, etc. that enables the supply chain. Some of the key issues which are a sore point among the partners are trust, security of data, data access among partners, seamless and device-independent data capture, real-time and reliable availability of data, data synchronization, and visibility of data. These and similar points are an outcome of research of many publications as mentioned in Table 2. Apart from it, as the data, process, and complexity proliferate with time in these ERP and planning systems, the visibility, security, scalability, and reliability of process and data diminish leading to inefficiency. This is where the adoption of blockchain along with ERP and planning system enables and powers the decentralized supply chain.

6.1 A Complex and Intriguing System of Systems in Supply Chain

ERP – enterprise resource planning – is a system which uses all the resources of an enterprise and drives coordination and automation among them. It brings procurement, manufacturing, inventory, engineering, order management, warehouse management, accounting, ledger reporting, cash management, e-commerce, and human resource under one single system, driving coordination, automation and scalability.

Planning system –The planning system is an algorithm-driven process of coordinating resources to balance demand and supply based on information signals for ultimately helping delivery of goods to customers. It considers every aspects of supply chain right from manufacturing, inventory, distribution, and procurement to order management. The demand planning aspects have demand forecasting, S and OP Process, and deriving consensus forecast, while the supply planning has plans to meet demands, inventory norms, sourcing decisions, production, and procurement plans.

The global standard today is a system of system for supply chain which combines ERP and planning system for the best possible outcome to drive business process and decisions.

The combination of ERP and planning system together brings with it its own challenges like:

- Across enterprise opaqueness: ERP brings visibility and automation in data and process within an enterprise. But across the enterprises (across systems of ERPs), the visibility to process and data is opaque. It is dependent on reports or EDI messages only.
- Modularity: ERP system is designed and developed in a highly modular way so that it remains flexible. At time due to this modularity, the data availability across enterprise becomes one of its weaknesses.
- Its functionalities are restrictive when it needs to coordinate with other partners and systems.
- Security: The data security threat is a reality in ERP. ERP is definitely not the most secure of the system specially as it has to provide access to outside of the organization where then it has to rely more on the network control rather than ERP system control.
- Transparency and accessibility: With the data stored in different ERP systems, the transparency of process and data is very challenging to achieve among partners. With security access and data access, the process is not only slow and cumbersome but also rudimentary and inefficient.
- Reporting: With data in different systems of ERP the single view of supply chain and its status is difficult to achieve.

To overcome these challenges, the author proposes the use of blockchain along with ERP and planning system for an efficient supply chain which will weave all the entities together. This will be particularly very helpful for decentralized supply chain.

6.2 Decentralized Supply Chain with ERP, Planning, and Blockchain

Bringing the distributed ledger technology (blockchain) into the decentralized supply chain is a game changer. It overcomes most of the process, system, and data challenges as posed by the decentralization. The issues faced in decentralized supply chain as emphasized in Table 2 can be overcome. The author has drawn Fig. 4 to depict how blockchain can help overcome the shortcoming in a decentralized supply chain which is already enabled with ERP and planning system. In Fig. 4, a supplier, customer, manufacturer, and distributors are all independent companies, but each of them becomes a node in the blockchain network. Thus, the blockchain network acts as a unified platform bridging the gaps of data visibility, communication gap, transparency, and traceability, to name a few. Figure 4 can also be explained as

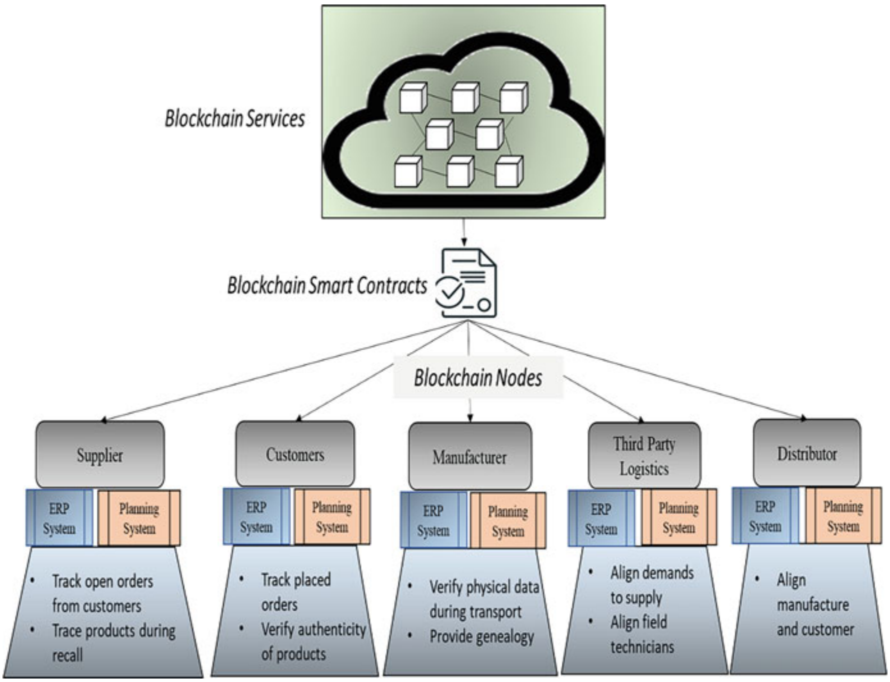


Fig. 4 Blockchain platform for a decentralized supply chain

the transaction data (as required and agreed) from each of the supply chain entity will flow into blockchain. It can be seen in Fig. 4 that each of the entity has its own ERP and planning system representing all independent companies. For the various supply chain challenges discussed in previous sections, the blockchain system of networks is a credible option to solve the problem. With the backdrop of a decentralized supply chain, blockchain offers new ways to automate business processes among the partners without setting up complex and expensive centralized IT infrastructure. In a decentralized supply chain, a blockchain provides capability to have a distributed ledger in a peer-to-peer network where members can interact with each other without a trusted intermediary, in a verifiable manner.

Figure 5 provides another view of a global supply chain where the entities are globally spread. In the figure, each entity is an independent company and has its own processes to run their business for their enterprise. Various ERP and planning systems will be a part of each of the entity. At the same time, it is a part of the blockchain network also. Data from the various ERP/planning system will flow into the blockchain network, and thus the blockchain network will act as a unified structure bringing in the transparency, security, and ownership. The figure shows that various partner entities are involved in transfer of goods and information while they carry on their own supply chain transactions. The data from these entities helps in transparency, financial traceability, accountability and improvises in processes with governmental agencies. There are many industries which are highly regulated, for example, pharma, nuclear components, chemicals, food, mining, and aerospace components, to name a few. In such industries, the onus of providing the right data at the right time for regulatory compliance lies with the

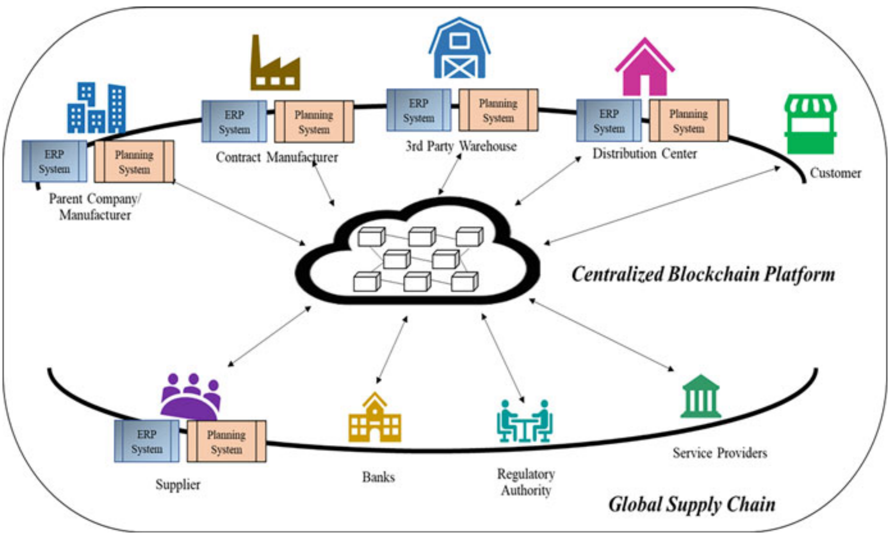


Fig. 5 Blockchain with ERP and planning system for a decentralized global supply chain

manufacturer. In such a case, blockchain is a matured and best fit solution. Bringing in the government regulator into the blockchain network brings in the required transparency as desired and required by regulators. The data being transparent and immutable adds to the worthiness of the cause and is a game changer. Due to this, there are many blockchain-related solutions to comply with US Drug Supply Chain Security Act (DSCSA) and Europe's Falsified Medicines Directive. This has resulted in blockchain solutions like MediLedger project from Chronicled, Akiri, and Medicalchain. But this approach does have a drawback that it needs interoperability among blockchain which is still not very generically available among the blockchain networks and continues to be a major hurdle.

The blockchain platform seamlessly brings the physical world data into cyber computing environment and stores it in a distributed ledger. This is the game changing attribute for the decentralized supply chain which bridges most of the gaps and challenges in a multipartner scenario. There are various ways and means by which blockchain along with ERP and planning systems will solve the supply chain challenges. Some of the key aspects are described in subsequent section:

Scalability The data from multiple entities originating from numerous transactions can be feed into the blockchain network. The blockchain network will act as the platform. Enterprise grade blockchain designed by Oracle, Microsoft, and SAP based on Ethereum or Hyperledger can handle big data in the distributed ledgers efficiently. Thus, a scalable data-driven supply chain organization is built cutting across partners. This in a way acts as a platform and removes other barriers as well.

Reliability Some of the key features of blockchain are being non-repudiable and immutable. These two features in supply chain (especially when data transfers across entities) improve the reliability of the transactions. With ERP and blockchain combination, the platform is poised for high velocity, high volume data transfers improving the consistency and reliability of transactions.

Security The data in the blockchain network is not owned or managed by any central authority. Every blockchain member node maintains a copy of the ledger. The data in blockchain is tamper-proof and immutable. These are some of the key capabilities which remove the data security threat in the blockchain platform.

Cost of Ownership Many of the blockchain systems are available as a service (hosted on cloud), costed at per unit of transaction data. For example, Oracle Blockchain Platform Cloud Service is available on per transaction basis [18]. Thus, the cost of ownership of the blockchain platform is data driven. With blockchain available on cloud platform and no upfront cost of infrastructure, the solution becomes affordable and many companies are doing Proof of concept (POC) on trial basis. It can bring tremendous benefit to business with no upfront cost and diminishing cost of ownership. It also makes the investment very affordable.

Transparency and Accessibility The data stored in blockchain platform is the same in every node/member and that can be accessed over web, applications, mobile, or desktop. This greatly improves the transparency of data and its access across all the entities of the supply chain. With the inbuilt security of blockchain and blockchain being the cardinal system of data storage cutting across the entities and enterprises, the data access and usage is seamless and transparent.

The blockchain platform brings benefits to all the supply chain partners in a decentralized operation. But every partner has a different aspect of benefit in the management of its supply chain owing to blockchain. There are certain needs and expectations which will be the same for every entity, while there will be few unique to a particular entity. The following sections detail out how blockchain platform will improve all the entities' coordination and cohesiveness and at the same time bring in more value to customer, saving money and simplifying processes. All the entities are picked up from Fig. 5 as it represents almost all the entities in a global decentralized supply chain:

Parent Company/OEM This is the external customer facing entity which receives end customer orders to be fulfilled. It can have mechanism to share order details in the blockchain network which can in turn help contract manufacturer (and suppliers) with transparency in demand (components). Based on the information shared or willingness to share, it can derive the following:

- Real-time order tracking based on blockchain data (component tracking from supplier, services tracing, logistics tracking, and manufacturing tracking), in short across partners.
- Traceability of product from contract manufacturer or OEM to customer, as it can trace back to customer or Tier N supplier.
- Easier product recall.
- Better root cause analysis of problems in products and supply chain. Better fault-finding capability in main product or components based on data available in blockchain.
- With shared information and visibility to inventory, the demand and supply planning can be more effective and agile.
- Customer order promising, customer order information and tracking can be more accurate and real time. Customers will have more real-time information on their fulfillment of their orders.

Contract Manufacturer Today, most of the manufacturing hubs are in the low-cost economies of Asia. Real-time data availability from trading partners in the blockchain platform (especially subassembly or contract manufacturers) can help all supply chain partners with better visibility and informed decision making. Some of the benefits of the data availability to and from contract manufacturer are:

- Product serialization reporting for authentication and traceability
- Real-time reporting of manufacturing status and quality
- Minute level details of manufacturing/storage conditions for traceability/fault analysis and recall purposes. It also can help know the manufacturing status.
- Real-time information of shipment schedules and status from contract manufacturers

- Confirmation on arrival of subassembly from feeder plants to main plant (progress in supply chain goods movement)
- Suppliers' material shipment schedules and confirmations to contract manufacturers
- Breakdown information/potential supply chain disruptions at contract manufacturer's facility

Third-Party Warehouses Insight into the movement of goods in-transit is always helpful in supply chain. With blockchain, the real-time tamper-proof data of arrivals and departures from warehouse can help all supply chain partners. This insight will provide the following benefits:

- Synchronized logistics with manufacturer and customer support team through the blockchain platform.
- This can help in real-time scheduling of technicians for services of new installations.
- Minute level details of product storage conditions for traceability/fault analysis and recall purposes when the product is moved directly to customer via third-party warehouse from contract manufacturers.
- Real-time monitoring of shipments across geography and on oceans.

Distribution Centers/Warehouses In many of the supply chains, this is the last storage point before product goes to customers or retail chains. The real-time data insights of arrivals/departures, pilferages, losses, and damages will help drive analytics or control tower decisions or insights for reporting into upcoming delivery delays (or problems), exact schedules of arrival, etc. Benefits are listed below:

- Synchronized field service and product delivery with blockchain smart contracts
- Advanced alerts/ASN from manufacturer to customer for preparation and housekeeping
- Minute level details of product storage conditions for traceability/fault analysis and recall purpose
- Synchronized warehouse staffing as per schedules, thereby reducing unnecessary staffing
- Extending the goods movement visibility to all stakeholders including end customers (where possible) for better planning

Banks Many a time banks lack the visibility in supply chain leading to delays in clearances, issuances of legal letter (required for port clearances or border transfers), or payments. It is envisaged that adding banks to the blockchain platform with the required necessary access to data may solve many of the delays faced by companies today in global supply chain. The main shortcoming is the trust due to which layers of proofs and data are required to be submitted to get the clearances (facilitating the delay). Having banks in the blockchain platform with suppliers, manufacturers, and customer can truly change the way commercials are run today. It can completely change the way payments and controls are built in systems to overcome trust deficits.

Service Providers Service providers provide services for installation or repair. The service must be synchronized with the availability of products from contract manufacturer or OEM and needs customer's consents for availability, time, and duration. In today's world, this coordination is completely manual, time consuming, and effort intensive. Many a times availability of product and schedule of technicians are completely out of synch due to visibility to each other's schedule. Having the three key entities (service provider, manufacturer, and customer) in the same blockchain platform with the required data access can completely transform the way the business is carried out today. It can bring in the following benefits:

- The effort in coordination can be transformed to automatic except some manual intervention due to exceptions. Smart contracts will play a big role in this.
- The synchronization of availability of product and service technicians can save time for customers and scheduling effort for manufacturer and service provider.

Regulatory Authority There are many products which undergo regulatory authority testing before they become eligible for sale to customers. These include (but not limited to) medicines, healthcare products, medical devices, etc. Also, there are products which need to undergo some special screening or certifications from authorities for their fitness before being shipped to customers. These are products used in sensitive places like nuclear reactors, boilers, furnaces, or gas chambers. For such certification or fitness of use approval, authorities need a plethora of information and test results to meet its procedures and purpose. Making all the data available to authority makes the process cumbersome and time consuming. It is also marred with corruption, mistrust, and cost escalations. Bringing the entities like manufacturer, customer, and governmental/regulatory authority into the blockchain platform and having the required data access can help transform it into a transparent process. It can bring in the following benefits:

- Authorities can access the required information or data from manufacturer, thereby reducing time of approval.
- The immutability and transparency of data by manufacturer to regulatory authority and customer can herald a new chapter in transparency and trust.
- The sharing of design, ingredients, and process to required parties can help protect the IP. Blockchain will protect the digital assets by regulating the access on the intended information. Blockchain can have smart contracts to verify NDA before providing access to sensitive IP assets. This will avoid data leaks and access by unauthorized parties. Blockchain can enable evidence of creatorship and provenance authentication. Blockchain can control and track distribution of IP products, digital rights management (e.g., online music sites), establishing and enforcing IP agreements, licenses, or exclusive distribution networks through smart contracts. All these can lead to robust IP management.

End Customer Customers today have very limited opportunity to verify the authenticity of a product and to know its provenance. Similarly, end customer's information is almost off limits for most of the manufacturers which makes it very difficult in case of a recall. Blockchain platform can provide the capability to hold this information in the platform cutting across enterprises and making the information available to multiple stakeholders:

- Parent company's ability to know the end customer
- Customer's ability to check product provenance based on smart contracts from blockchain
- Product serialization and end customer information for recall
- Possibility of product feedback from end customer to manufacturer, in a more seamless way.

Blockchain platform can cut across industries and systems enabling partners to adapt to a highly collaborative process of sharing and transacting. The blockchain will be able to provide transparency and security of data at the same time. The enterprise blockchain platform will disrupt the typical way the business of collaboration among partners happens today. Today, it is predominantly reports driven and with blockchain it will be more real time and data driven. Blockchain will completely change the way the entities collaborate today among enterprises for real-time decision making. With these let us now look at the pillars and enablers of supply chain how they are influenced by blockchain.

In many of the global corporations, it is not uncommon to have multiple ERP systems, MES, or WMS. It is generally found that the planning systems, reporting mechanism, and master data systems are centralized in an enterprise, while the execution systems like MES, ERP, and WMS are multiple. The multiplicity comes due to geography/business divisions or even product lines. So blockchain is useful where data needs to be centralized and transparent across the company's boundaries. It is also equally useful in global corporations where systems are disparate and unharmonized/asynchronized within the company's boundaries. In such cases, blockchain can act as the chosen centralized system which may hold data from multiple ERP systems/MES/WMS/TMS and becomes the key source of control towers and analytics. For example, many of the large multinational corporations have geography-based ERP system like Oracle ERP in North America, while Europe and Asia are on SAP. There are also cases where the manufacturing execution systems (MES) are divided by operations like say in semiconductor the front-end operations (wafer manufacturing) are on one MES, while the assembly and test is on a different MES. In such cases, blockchain can act as the chosen platform of centralization. Relevant MES data is collected using IOT system and brought over to the centralized blockchain platform which are shared with multiple stakeholders/nodes and used for various analytics, root cause analysis, and reporting purpose.

6.2.1 ERP and Blockchain Enabling the Pillars of Decentralized Supply Chain

The pillars are the building blocks of a decentralized supply chain. The pillars together make sure the activity of each entity is supported by the others for an

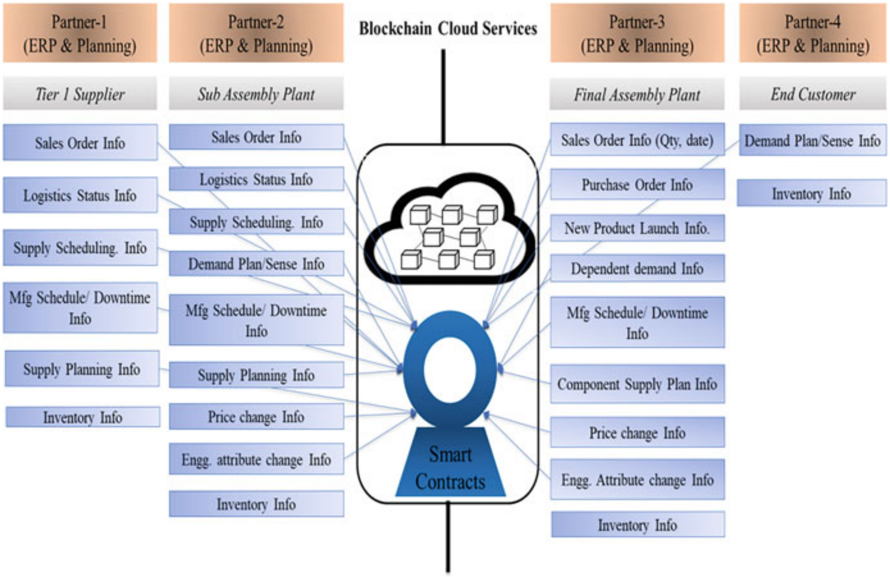


Fig. 6 Supply chain transaction among partners – data centralized in blockchain platform

identified end goal. The entities together make up a smooth supply chain delivering value-added goods to the end customer. Though individual entity profits are important, the end goals of the end-to-end supply chain are paramount. To achieve the goals, these pillars are identified. The blockchain platform together strengthens these pillars in multiple ways. These are further explained through a simplified four-level supply chain which is represented in Fig. 6. Through the figure, it is explained how supply chain transactions across entities undergo a transformative change with the blockchain platform and thus reinforcing the pillars in the decentralized supply chain.

Figure 6 shows there are four supply chain partners, namely, a tier 1 supplier, subassembly plant, a final assembly plant, and a customer. The supply chain transactions are selectively exposed to blockchain platform so that it can drive the desired benefits for end customer.

Transparency There are multitudes of transactions which take places in a supply chain. Some of the key information from a partner is selectively exposed to blockchain platform. Some of the examples as shown in Fig. 6 are price changes/ net prices from final assembly/subassembly plants, demand scenarios from customers and final assembly plants, manufacturing scheduling and downtimes of the manufacturing units, and engineering attribute info from design partners, just to name a few. Availability of this information with the required partners brings in a lot of supply chain transparency and removes the need to build up inventory or lead time in the supply chain to cope with the uncertainty. This transparency will lead to lead time reduction to final customer and reduction in cost of product due to lesser inventory carrying, thus driving more value to customer. The security and trust of blockchain will enable this transparency, and attributes of blockchain will enable the data trust among partners.

Traceability The traceability of the origin, provenance of the product, or its components is a key selling point for many of the products today. This is true for costly products in fashion, food products, and critical equipments. With components/ subcomponent failures/ recalls and insurances, it is applicable for all domestic and industrial products. To bring in the transparent traceability within supply chain where there is no dependency on other partners, the following key data needs to be on the blockchain platform, these are engineering attributes, manufacturing quality results, serial or lot number of inventory, purchase order tracing the demand (for supplier), and sales order tracing the supply (for the final customer/assembly). The data being available in the platform enables to generate genealogy report to trace origins based on transactions and unique identifiers like serial/lot number transacted over purchase or sales orders.

Supply Chain Visibility Supply chain visibility is about knowing the availability of product (quantity and status) in the entire supply chain network. This applies to products from suppliers, logistics providers, manufacturers, third-party service providers, and/or even with customers. During the pandemic of COVID-19, every aspect of supply chain like procurement, sourcing, manufacturing, planning, and logistics struggled. The supply chain shock indicated the need, importance, and focus on supply chain visibility in the business scenario. The research of Alice et al. (2020) and Lian and Fan (2020) signals the need and importance of supply chain visibility. The pandemic exposed the vulnerability or lack of it and brought it to the forefront. It is the supply chain complexity, deficit of trust, or system limitation which binds or limits the visibility. The blockchain platform brings all the supply chain transaction information from each of the partners and makes it centrally available. The following are some of the key tenants of the supply chain visibility:

- Demand picture from customers
- Shipment and logistics insight from 3PL
- Supply picture from supplier and contract manufacturer
- Tentative dates of fulfillment from suppliers
- New Product Introduction (NPI) information from supplier or manufacturer
- Promotions or demand changes from supplier or manufacturer
- Real-time manufacturing status from manufacturer or contract manufacturer

This improves the supply chain performance, opportunity to reduce human dependency, and preparedness for disruption. This also improves fulfillment and brings in transparency with customer, thus improving credibility and trust.

Autonomy In a decentralized supply chain, the partners operate in tandem with each other to serve end customers. But like in any business, the best comes when the operations have the flexibility to have their own decisions and ability to switch or change to meet the tactical plan or attend the most pressing need. This autonomy of business operations for every entity is critical to survive, thrive, and improve. As the blockchain platform brings in the transparency, traceability of transactions, and visibility in supply chain, it also brings in the autonomy for the entities. It empowers them to make changes as per the current plan or scenario and blockchain enables it to share it to other entities. Validations built in the smart contracts will enable a transaction or raise flags if the changes brought over are not meeting any designed criteria or process. There are possibilities to build alerts based on the situation or data received from a partner entity with the help of smart contracts. All these will build in autonomy of the supply chain partners all the while preserving the transparency, traceability, and visibility of transactions.

Service Levels In simple terms, service levels are a function of demand, lead time, information flow, and availability of products. Blockchain enables a seamless and transparent information flow among the trading partners in real time and in synch with the actual product flow. The service levels among the partners will improve as the transparency and supply chain visibility improves. This will be enabled through inventory holding and reduced supply uncertainty. The inventory will be better utilized to meet higher priority demands. Strained supply scenario from suppliers (for components) will help build alternates to keep pace for production. The smart contracts on engineering attribute changes or scheduled engineering change orders can help inventory managers plan and rationalize inventory. This will help in avoiding stock out situation or stockpiles.

On average, it is considered that there are 28 parties involved in transporting one sea container, and all have their own record-keeping systems. If we expand it further to the products coming from suppliers and subassemblies, the number of parties in the decentralized supply chain explodes multiple times. Blockchain, which is a trustworthy digital database at its core, stores the digital records of transactions among all the parties. Thus, blockchain platform not only enhances these pillars but also digitizes the entire decentralized supply chain.

Smart Contracts: A View of Applications in Real World

It is very important that we understand how smart contracts are designed, used, and implemented. The best way to describe and explain this is through examples in real world. Smart contracts are versatile and are used in every aspect of business and supply chain. Smart contracts as described above are business rules written as code into blockchain application layer. The rules are applied to everybody in the network. Smart contracts are thus an automated, secured, trustless, cost-effective, fast, and accurate means of bringing business login in blockchain network. Table 3 provides a curated list of real-life smart contract application in various industries and in various spheres of supply chain.

The smart contracts ingest complex information, convert them into business application logic, and execute it on blockchain network. The data may be coming

Table 3 List of smart contract from various industries

Industry	Smart contract example
Manufacturing supply chain	Change in engineering attribute in master data to trigger notification Planned downtimes to be communicated to high impact customers New product launch info into system can trigger notification to customers
Agri-supply chain	Smart contract to verify the origin of product. Based on which the product is accepted and is delivered Smart contract to verify the date of harvest to accept or reject a lot
Distribution industry supply chain	For a price change from manufacturer, distributor can trigger a notification to customer For ship and debit settlement, smart contracts may be designed to verify rules of authorizations like quantity, date, customer, etc.
Pharma supply chain	Validate origin of ingredients before receiving for drug manufacturing Validation of patient records for drug approval by FDA For Drug Supply Chain Security Act validation of medicines before selling to customers
Insurance industry	Validation of insurer records, vehicle details, and other information before processing claims Real-time data verification from insurer for reinsurance cases

into blockchain from ERP/MES/ planning or any other transactional system. . The source of data or type of data is not a factor, what matters is the data and the applicable logic in it.

6.2.2 ERP and Blockchain Powering the Enablers of Decentralized Supply Chain

As discussed in previous sections, there are various aspects of supply chain like its data, transactions, and setups which can be shared on the blockchain platform. The blockchain platform thus becomes an ubiquitous system available to different partners driving multitudes of supply chain benefits. Figure 7 expands the role of blockchain platform for driving the enablers of the decentralization. The key enablers of decentralization are studied further, and a detailed analysis is carried out as to how the blockchain platform influences and impacts them. The blockchain platform positively affects different aspects of supply chain and drives it to improve the enabler for a more efficient and value-driven decentralized supply chain.

The following are the impacts of blockchain platform on each of the enablers:

Economics of Supply Chain The decentralization should be working in every partner's favor, economically! It is the single biggest factor to enable the decentralization and drive it perpetually. This is possible when the decision making is collaborative. So, having inventory holding transparency, manufacturing downtime transparency, and supply situation transparency drives better efficiency and cost

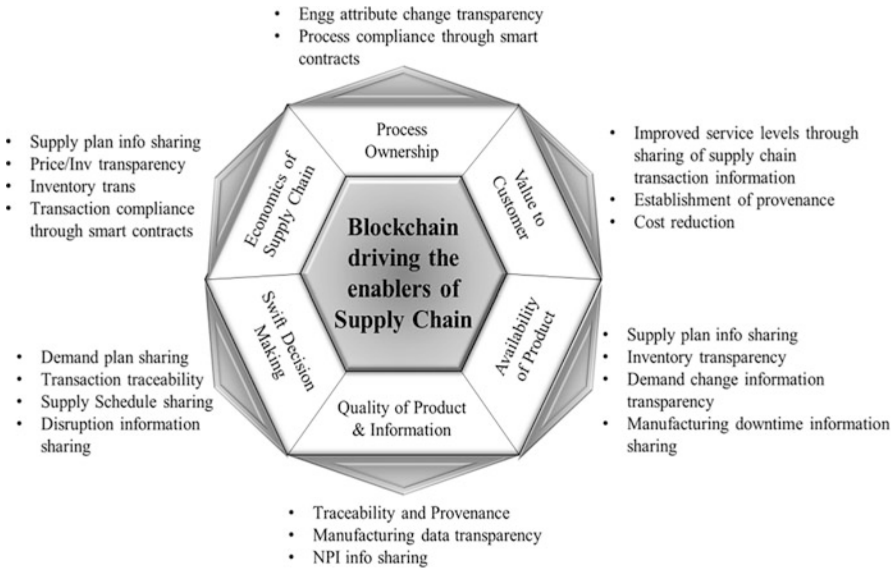


Fig. 7 Blockchain platform impacting the decentralized supply chain enablers

savings, reduces supply chain shock, and removes unwanted inventory. These are possible only with the blockchain platform. Another aspect which greatly influences the profitability and cost is the transparency in demand and supply plans. The sharing of forecasts or potential/expected demands and vis-à-vis the projected supply situation can enable a highly collaborative supply chain driving profitability and reducing cost. Last but not the least, the supply chain transactions' compliance (like purchase order, sales order, inventory transfer, and internal transfers) among the partners can greatly reduce burden, effective use of people, purpose-driven reporting, productive use of workforce, and less of non-value adding work. These are possible only with a blockchain platform which cuts across enterprises and makes data available independent of any single authority owning it. Thus, blockchain platform can enable the decentralization of the supply chain and help the economics of supply chain.

Swiftness in Decision Making The entities forming the decentralized environment bring with them hosts of disparate systems driving their backend supply chain transaction processing (ERP), reporting, demand, and supply planning as well as the manufacturing execution system (MES). The flow of data among the system is driven by EDI, B2B messaging, XML, and middleware technologies. Sometimes the data from one system moves to another system through batch processes with approvals. This builds latency (lack of swiftness) in the data flow which gets evident in the material flow impacting the customer deliverables. This is the symptom which needs to be solved, and one of the most prominent ways of solving this problem is through the centralized data system.

There will be an API-driven real-time interface built from the MES, ERP, and supply chain systems into blockchain platform. The real-time data availability will drive two purposes. Firstly, it will make any kind of data available for decision making. This will enable a swift, smooth, and transparent tactical decision-making process. Secondly, it will allow data to be merged, cubed, or segregated together from different streams and partners and bring it together for analytical purposes and strategic decision making. The availability of data in such a system underlines the features brought by blockchain like the data is true, dependable, and authentic. These capabilities thus differentiate the blockchain-driven platform from other data warehousing systems and its capabilities.

Process Ownership The blockchain platform must serve the transparency not only in data but also in process. Having the process transparency (among partners) will bring in the ownership and will revolutionize the way partners and entities interact in a decentralized supply chain. As the material moves forward toward the end customer along various entities, the interdependence of the entities for data, material, information, and process comes up as a key factor to manage. Typically, today the sharing of information is limited to required information of material, and there is no sharing of process information. In general, in a steady-state condition, this is not required, but if there is a recall or a product issue, then this information becomes important. In reverse logistics scenario, this information is key to return, repair, reprocess, or dispose. With the subscription-based economy picking up and its impact on supply chain, the process information among partners is playing a crucial role. Due to these factors and requirements, the ownership of the process becomes a problem. It's a challenge which needs to be sorted out. Blockchain platform can solve this problem in the following ways:

- Sharing of engineering information and its change thereof can greatly help eliminate or reduce rework, return, and noncompliance. Thus, sharing of the process information securely through blockchain will be made available only for eligible candidates.
- Compliance of transaction processes and proof thereof helps in identifying the process dispersion and root cause of the problem. Blockchain platform will help build the compliances with smart contracts.
- There can be smart contracts built in different processes of manufacturing, logistics, and inspection which can help raise attention from different partners based on the type and nature of nonconformance/issue. It will be purely data driven.
- Sharing of design can be enabled among partners on the blockchain network. This will reduce the traditional sharing mechanism over emails and other mechanism. This can bring in process transparency as well as security.
- Blockchain platform can securely and immutably record the transfer of ownership of the product with accurate time and history. This can be useful for insurance claims and root cause identification issues.
- Built-in security measures can protect fraud transactions thus retaining the ownership of the product and IP.

Quality of Product and Information As discussed in earlier sections, the quality and reliability of the information in the supply chain reduce burden of coordination among partners. This also improve the material flow and supply chain efficiency. Blockchain platform can significantly improve the quality and information aspect of an end-to-end supply chain cutting across multiple partners. One of the key usages of blockchain is to provide product provenance and traceability. It's not that without blockchain it is not possible to have product provenance or traceability, but blockchain's mature technology makes it simple and scalable. Blockchain can enable sharing of manufacturing data and physical environmental data during manufacturing among other things with partner. This will improve product quality and transparency as well as bring in trust. The sharing of supplier problems, specifications, partnering in designs, and improvements thereof are things which can be easily and securely adopted through the blockchain platform and which will immensely improve the quality of product and the information getting shared.

Availability of Product Product availability in supply chain is one of the most used parameters to measure the supply chain health and functioning. In a decentralized scenario, it is the interdependence of product availability among the partners which plays a deciding role in its success or problems. Blockchain platform can eliminate some of the issues and/or it can alleviate some of the problems. The following are some of the nuances through which blockchain can significantly help the decentralized supply chains in managing their enablers:

- Most of the supply chain partners will have their own ERP system. As data traverses through multiple systems, it increases latency, reduces information transparency, and builds information silos. This leads to data redundancy and ultimately impacts the availability of product for its customers or partners. Blockchain's repository of data at every node will reduce data silos and greatly improve the latency and transparency.
- Product quality issues can be sorted out with the platform. Inventory transparency can be built with blockchain and this will improve the product availability across partners.
- Sharing of nonavailability of manufacturing lines due to maintenance or problems, supplier product quality issues, or supplier product availability information helps in achieving transparency. This also facilitates expectation management (of end customers) and positively impacts availability. Sharing of nettable/ good/ shippable inventory available to partners has been found to greatly help partners. This is widely used by distributors to know the manufacturers' availability.
- To improve the collaboration among the customer-supplier, customers can share the build plans using blockchain. Blockchain will seamlessly and transparently allow the supplying entity to know of their products' demand in the future (both near and long term). These will be highly reliable as these will be customer forecasts. Customer using smart contract in blockchain will selectively expose the items' demands to supplier as per the sourcing of the item. Today (without blockchain), supplier forecasts are shared and commitments received but are based on a cadence (frequency) and many a times offline. Blockchain will bring

in the traceability of change and provide room for discussion or agreement on this while being real time, transparent, and secure.

Value to Customer In a decentralized supply chain, there are internal and external customers. Bringing value to customer is always an enriching goal for any supply chain and its partners. The following are the way, means, and mechanism by which blockchain platform can bring this value to customers:

- Cost reduction – Blockchain platform removes dependency on third-party systems and third-party information. Thus, it provides the possibility to decommission legacy systems and infrastructure and significantly reduce IT costs. Partners will have the possibility to reduce the need for manual intervention in aggregation, amending, and sharing supply chain data. The regulatory reporting, compliance reports, and audit documents will become easier and require less manual effort. As a result, employees of every partner will focus exclusively on core supply chain activities. This will result in effort saving and man power rationalization leading to cost reduction/savings.
- Provenance – The establishment of product provenance and traceability will bring in a lot of value to the supply chain and customer. It will also bring in credibility and can help charge premiums for its products. In cases of recall, it can help a seamless recall mechanism, thereby reducing cost of ownership. This will provide an enriching experience to customer and more power to manufacturer.
- Service Levels – In a decentralized supply chain, there are internal and external customers. Having an improved service levels and product availability among the partners brings in a lot of value to customer.

The discussion above portrays the different aspects of the blockchain platform and how it can help drive the enablers of the decentralized supply chain. So, adoption of blockchain for driving these enablers is key for improvement of decentralized supply chain.

6.2.3 Challenges in Integrating Blockchain with ERP

Though there are innumerable benefits in integrating blockchain with ERP for a decentralized supply chain, there are challenges as well. It is prudent to understand and know the challenges of integration beforehand so that it can be prepared accordingly.

Technology acceptance challenge – With an existing ERP, investing in blockchain needs a lot of concrete reason for organizations and leaderships to get convinced. Lack of understanding of blockchain technology among leaders, looking at competitors at what they are doing, lack of standards, and lack of skilled resources are some of the major challenges in acceptance of the technology.

Data-related challenge – Data in blockchain has to be correct and reliable. An incorrect data in blockchain doesn’t serve any purpose and is detrimental to the investments. As data in blockchain is immutable, so it makes the wrong data all the more problematic. With an unreliable data, the supply chain partners with which the blockchain will connect to various ERPs will become incoherent and misaligned. Such a step can have catastrophic effect. So having correct data is very important and key to blockchain's integration with ERP. Data standardization is equally important when blockchain and multiple ERP are coming together. The data has to be consistent when it gets referred by multiple partners/ERPs. As an example, let's say an item with code A in one company needs to be referred with a common name or id across multiple partners, mix up in this will lead to complete failure. So, data standardization across partners is key to this success.

Trust and Partnership Challenges – When supply chain collaborates, then it is not only its system but also its people and processes that collaborate. This collaboration needs immense trust to share data and open up the processes with your partners. Once these barriers are overcome, then only a true transparent supply chain can be established cutting across the barriers of systems and processes.

Scalability and Interoperability – Adopting blockchain is additional cost on top of other systems which are already in place. Blockchain integrating with ERP is primarily done to establish transparency across companies and breaking the data siloes. This leads to data getting replicated across nodes. Also, companies have a single ERP system connecting to multiple blockchain systems, and thus interoperability of blockchain becomes important from long-term sustainable systems perspective.

These are some of the challenges in integrating blockchain with ERP, and companies need to be aware of these challenges when they move toward such an integration.

7 Discussion: Future of Decentralized Supply Chain with Blockchain and ERP

Digital revolution is characterized by the convergence of different technologies for the betterment of product, benefit to customers and business processes. The future of supply chain with blockchain application will also converge people and process, blurring the lines of digital and physical world. It will increasingly use machine learning algorithms, and data from blockchain for the purpose of improving processes, providing visibility and transparency, and continuously aiding in faster and accurate decision making. Blockchain will increasingly become the centralized data repository cutting across systems, enterprises, and partners. It will be blockchain and not individual ERPs which will be hooked to various analytics platforms and reporting mechanisms like Tableau/Power BI, etc. Blockchain will drive the centralized reporting, providing analytical views and driving the decentralized supply chains' efficiency and performance for global corporations.

As the blockchain platform matures, it will be able to bring in more partners and their trustworthy data for decision making which will greatly improve the supply chain and its operations. The systems of ERP, supply chain planning and MES will continue to evolve adding more functions, and technologically it is moving and continue to move to cloud architecture. Moving forward API (application programming interface) will be the mechanism to hook up any external system. This can be facilitated with some middleware applications like Boomi, MuleSoft, or Fusion. This will enable easier adoption of blockchain as also its integration with MES or ERP and planning systems. With this, the data from different applications will democratize in blockchain. Blockchain will drive most of the compliance reporting, partner reporting/information, analytics reporting, KPIs for partners, and supplier negotiation, and this will move to a more centralized and capability-driven operations on the platform while having all the flexibility of decentralization.

There will be more advancement in the interoperability of MES and ERP and blockchain systems. Today, IBM, Oracle, SAP, and Microsoft are building capabilities of interoperability of blockchain services among themselves (Hyperledger and Ethereum) [19]. In the future, the interoperability of blockchain will expand to all big and small ERP vendors. Availability of API in ERP system for integration with leading blockchain vendors will become a selling point and a necessity. These will get smoother with more advancement in technology and will have wider reach adding in the satellite systems apart from ERP. The supply chain partners will come together to form blockchain-driven consortiums which can be industry based, product based, or partner based, and those consortiums will drive the process landscape. These consortiums can even have leading ERP vendors also as a partner to the consortium and can help provide industry standard processes, KPIs, and other services. The blockchain platform will be mostly built as enterprise grade that is designed, developed, and poised to handle huge volume of data. The load of data warehousing and reporting from ERP/planning system/MES will move to blockchain platform. This will have a corresponding impact on the need for skilled resources for underlying technology.

With the blockchain platform, the decentralized supply chain will be transforming from the way it operates today. It will continue to provide the flexibility of decentralized decision making, and at the same time, the platform will provide the benefits of centralization driving efficiency, performance, trust, and service levels.

7.1 Conclusion

Decentralization of supply chain is inevitable and will continue to evolve. The supply chain is increasingly going to be global, decentralized, and geographically spread. Blockchain based on the distributed ledger technology will greatly help improve decentralized supply chain operations and performance. An integrated blockchain with ERP, planning system and MES will be the lynchpin of success for a decentralized supply chain. It can derive significant benefit in supply chain execution as well as in reporting.

The combined architecture of these systems will enable the pillars and enablers of decentralized supply chain. Blockchain platform will enhance the pillars of decentralized supply chain, namely, transparency, traceability, visibility, autonomy, and service levels and at the same time digitizing the supply chain driving performance and execution superiority. The blockchain platform will enhance the decentralization processes and positively impact the economics of supply chain, swift decision making, quality and reliability of product, availability of product, and value to customer. It will transform the supply chain into a digital, connected, and efficient decentralized supply chain.

The architecture presented in this chapter is generic and can help any type of supply chain orchestration. Overall this digital adoption in decentralized supply chain is poised to transform business and serve human mankind for its betterment!

References

1. Cheung, B. (2020). What countries are most multinational corporations based in? *Investopedia*. https://www.investopedia.com/ask/answers/021715/why-are-most-multinational-corporations-either-us-europe-or-japan.asp. Last accessed 2021/4/21.
2. Rangavittal, G., & Sohn, T. (2008). The impact and dynamics of centralization in supply chain decision making. Thesis Project. https://dspace.mit.edu/handle/1721.1/45243. Last accessed on 2021/3/22.
3. MH&L Staff. (2003) Centralized Vs. decentralized decision-making. https://www.mhlnews.com/archive/article/22036969/centralized-vs-decentralized-decisionmaking. Last accessed on 2021/4/24.
4. Chen, F. (1999). Decentralized supply chains subject to information delays. *Management Science, 45*(8), 1076–1090.
5. Saxena, A., Ganesh, K., Saxena, A., & Page, T. (2009). Partially centralised decisions and information synchronisation in supply chain. *International Journal of Enterprise Network Management, 3*(3), 246–267.
6. Fu, H., & Ma, Y. (2019). Optimization and coordination of decentralized supply chains with vertical cross-shareholding. *Computers & Industrial Engineering, 132*, 23–35.
7. Lu, S. Y. P., Lau, H. Y. K., & Yiu, C. K. F. (2012). A hybrid solution to collaborative decision-making in a decentralized supply-chain. *Journal of Engineering and Technology Management, 29*(1), 95–111.
8. Mourtzis, D., & Doukas, M. (2013). Decentralized manufacturing systems review: Challenges and outlook. In K. Windt (Ed.), *Robust manufacturing control* (Lecture notes in production engineering). Springer.
9. Proch, M., Worthmann, K., & Schlüchtermann, J. (2017). A negotiation-based algorithm to coordinate supplier development in decentralized supply chains. *European Journal of Operational Research, 256*(2), 412–429.
10. Tliche, Y., Taghipour, A., & Canel-Depitre, B. (2020). An improved forecasting approach to reduce inventory levels in decentralized supply chains. *European Journal of Operational Research, 287*(2), 511–527.
11. Prasad, T. V. S. R. K., Srinivas, K., & Srinivas, C. (2017). Decentralized production–distribution planning in multi-echelon supply chain network using intelligent agents. *Opsearch, 54*, 217–232.
12. Wang, Q., Chay, Y., & Wu, Z. (2011). Streamlining inventory flows with time discounts to improve the profits of a decentralized supply chain. *International Journal of Production Economics, 132*(2), 230–239.
13. Schmitt, A. J., Sun, S. A., Snyder, L. V., & Shen, Z. M. (2015). Centralization versus decentralization: Risk pooling, risk diversification, and supply chain disruptions. *Omega, 52*, 201–212.

14. Hassanzadeh, A., Jafarian, A., & Amiri, M. (2014). Modeling and analysis of the causes of bullwhip effect in centralized and decentralized supply chain using response surface method. *Applied Mathematical Modelling, 38*(9–10), 2353–2365.
15. Banerjee, A. (2018). Blockchain technology: Supply chain insights from ERP. In P. Raj & G. C. Deka (Eds.), *Advances in computers* (Vol. 111, pp. 69–98).
16. Banerjee, A. (2018). Integrating blockchain with ERP for a transparent supply chain. Infosys White Paper. https://www.infosys.com/Oracle/white-papers/Documents/integrating-blockchain-erp.pdf. Last accessed 2021/3/12.
17. Banerjee, A. (2019). Blockchain with IOT: Applications and use cases for a new paradigm of supply chain driving efficiency and cost. In S. Kim, G. C. Deka, & P. Zhang (Eds.), *Advances in computer* (Vol. 115, pp. 259–292). *Elsevier*. https://doi.org/10.1016/bs.adcom.2019.07.007
18. Oracle. (2018). Blockchain Platform pricing options. https://www.oracle.com/in/application-development/cloud-services/blockchain-platform/. Last accessed 2021/5/8.
19. Owen, P. (2019). Microsoft, SAP announce interoperability of azure blockchain service and SAP cloud platform blockchain service. SAP TechEd 2019. https://www.sapinsideronline.com/blogs/microsoft-sap-announce-interoperability-of-azure-blockchain-service-and-sap-cloud-platform-blockchain-service/. Last accessed 2021/4/5.

Toward the Application of Blockchain Technology to Enhance Traceability and Information Sharing in the Supply Chain of Textile Supply Chain: Application to the Order-to-Cash Process

Manal Hader, Abderrahman El Mhamedi, David Tchoffa, and Abdellah Abouabdellah

1 Introduction

Supply chain transparency has drawn great interest from researchers and practitioners, and with the increase in counterfeit products and unethical labors, supply chain transparency has become an urgent matter [11]. Textile supply chain is among the supply chains that require transparency due to its complexity and its large geographical extensibility of actors which make it very opaque and vulnerable [12]. The participants in the textile supply chain are connected by a network, but they do not have enough visibility about important information related to their work. Furthermore, some of the associated parties utilize unethical methods to create and distribute their products which have led to dramatic issues in the past. This has caught the government's attention to the problems of textile industry and pushed them to put pressure on decision-makers in this sector to remedy it under penalty of sanctions and amends [14]. Other major issues of textile supply chain are counterfeits and security [18]. Counterfeiting issues in the textile industry aren't only confined to final products but also touch semifinished products unlike other sectors [18]. These counterfeit products do not just have an economic impact but can sometimes harm the health of customers given the poor quality of the raw material used (Ekwall, 2009). Traceability is a vital element to all sorts of sectors and supply chains [19] which will enable us to track supply chain process and trace products [8]). In fight against the growth of textile traceability issues, many Internet of things (IoT)-based systems are used to keep track of the items and processes at different

M. Hader (✉)
Paris 8 University, The National School of Applied Sciences, Paris, France
e-mail: manal.hader@etud.univ-paris8.fr

A. El Mhamedi · D. Tchoffa · A. Abouabdellah
Paris 8 University, Kenitra, Morocco
e-mail: a.elmhamedi@iut.univ-paris8.fr; d.tchoffa@iut.univ-paris8.fr

A. Bouras et al. (eds.), *Blockchain Driven Supply Chains and Enterprise Information Systems*, https://doi.org/10.1007/978-3-030-96154-1_5

levels of the supply chain. But up to now, almost all of these technologies are monopolistic, unbalanced, and obscure, which leads to confidence problems such as tampering, manipulation, corruption, and faking information. Furthermore, those monopolistic technologies are subject to breakdown because a simple failure will lead the whole system to crash [15], which leads to a crucial question that has yet to be addressed: whether or not the information supplied by textile supply chain participants in the traceability system can be trusted. As a result, the textile market is unsafe which may expose the customers to serious security concerns. We feel that implementing blockchain technology might be a solution to the mentioned issues that can eliminate dependency on a single entity. Rather than saving information in an obscure environment with the blockchain technology, for every actor in the supply chain, all data about textile goods may be stored in a common and transparent system. This might be a valuable addition to the textile supply chain. The following is a breakdown of the paper's structure. The available reviews on the applicability of blockchain technology and centralized systems in textile supply chains are presented in Sect. 2. Then, in Sect. 3, a typical textile supply chain flow is given, followed by the use of the BigchainDB platform in Sect. 4. Section 5 offers the use case, while Sect. 6 delves more into the benefits and drawbacks of the suggested model for this study.

2 Literature Review

In accordance with ISO 9000:2015, traceability is described as the ability to identify and track the history, distribution, location of products, parts, materials, and services. A traceability system monitors and records the flow of processes, products, and services from vendors, manufactured and ultimately distributed as final products. It provides a number of advantages, including increased visibility throughout the supply chain, improved quality, and greater process control [17]. Traceability also makes it possible to overcome obstacles in a retail network and reduce the risks that come with them in supply chain by determining real-time upstream source and downstream recipients. It also assists with decision-making, remanufacturing, recycling, and product recalls. Previously, investigations were carried out to create various technologies and techniques for tracking products in a supply chain and prevent related risks [5]. Regarding textile industry, Shuchih Ernest Chang et al. [21] argued that the lack of information sharing represents a major obstacle in the supply chain of textile sector in Hong Kong and demonstrated that the lack of standards or a uniform platform for sharing information consists of a direct reason of this. Gobbi and Massa have proposed a model to analyze the traceability system in the Italian textile industry which they named Traceability and Fashion (TF). Their model was adopted by the Union of Italian Chambers of Commerce [7]. Furthermore, with the arrival of IoT, many surveys have recommended the use of relevant technologies for textile supply chain traceability systems. Track and trace systems are used to track items as they move through the supply chain's tiers. It entails assigning a unique code to each product or set of items, such as RFID, and then using that code as a tracking element. Keung and Wu in their research suggested a RFID-based supply chain in the apparel sector. They described how their proposition improves the efficiency of a supply chain by facilitating coordination in processes; however, they concluded that despite the multiple benefits of this technology, security issues in information exchange are still a major concern in this industry, demonstrating the inadequacy of such technologies [9]. Agrawal et al. proposed a method to implement a traceability system centered on products for monitoring and controlling production operations and supply chain transactions. In their study, they provided secured tags that aid in the security of the clothing supply chain at the item level and limit unauthorized entry to the item information. However, they recommended that future studies can be conducted to ensure that the traceability system is secure at the enterprise level to avoid an incident on the information exchanging means [2]. All the studies listed above emphasized the use of a centralized system as one of the most successful approaches to promote data transparency in supply chains to date. Currently, a new disruptive technology known as blockchain has arisen as a major issue with a completely different approach. In their work, Casey and Wong demonstrated the potential benefits of blockchain technology in the manufacturing supply chain [4]. They suggested that the inherited benefits of the blockchain could build trust through visibility and transparency within any operation and transaction in the supply chain. They also offer a use case to demonstrate how blockchain technology can be applied to transform supply chains. Moreover, prior literature has demonstrated that there are multiple advantages of blockchain technology which can be applied in the supply chain to stock and exchange information with other actors such as vendors, customers, etc. Among these researches, some researchers showed that blockchain technology can also be used to decrease intermediaries' use, enabling decreased expenses and increased performance [10]. Based on the literature review, IoT has been used by multiple actors for supply chain traceability. However, these are still centralized systems, and no decentralized systems for product tracking have been deployed in the textile supply chain. In this study, a decentralized information system for textile supply chain monitoring and traceability is built using blockchain and IoT. Compared to centralized systems, this new approach would be a game-changing innovation, providing a secure, transparent, and open information system for all supply chain stakeholders. We feel that our proposal represents a fresh approach to supply chain traceability and substantially improve textile supply chain's performance.

3 Textile Supply Chain (TSC) Management

3.1 The Typical Model of the Textile Supply Chain

Supply chain management (SCM) is described as the connection of the core business processes from final user through first vendors that offer raw materials, services, and information to customers and other players, therefore adding value [3].

The textile supply chain represents an illustration of an integrated supply chain, according to Abernathy et al. [1], who said that the textile industry is a worldwide system. Fibers may be manufactured in one nation, spun into yarns, woven into textiles, and stitched into garments in another country, before being marketed elsewhere in the world [1].

The textile supply chain, in general, entails a number of procedures, a variety of raw materials, and a number of intermediary products. The majority partners of the TSC network are raw material vendors (spinning factories and accessory suppliers), manufacturers (knitting factories), trading firm's holders, retailers, or the end customers. A structure of a textile supply chain is presented in Fig. 1.

The flow of TSC is shown in Fig. 1. The general working steps of traditions of textile supply chain management (TSCM) are as follows:

- In the first step: the textile producers gather their raw materials from several vendors to knit the clothes as clothes produced contain the processes of spinning and knitting. Knitting is a process of building fabric by meshing a sequence of loops of one or more yarns. Spinning is the conversion of fibers into yarn. The finest fashionable clothes require a significant amount of study and patience.
- In the second step: after product manufacture, they send it to the trading firms.
- In the third step: the retailers get the final products which they usually order according to their needs and order forecast.
- In the final step: the retailers sell the clothes directly to the end users.

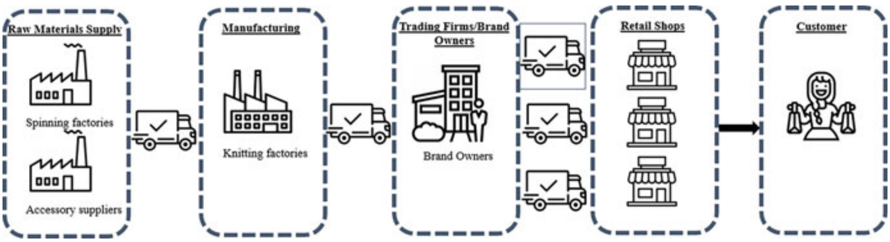


Fig. 1 Working mechanisms of a typical textile supply chain without blockchain

3.2 Major Shortcoming of Existing Supply Chain Management System

With the fast growth of Internet technologies and centralized mechanism, such as an EDI, ERP, and RFID system, a lot of emerging technologies have been used in trace- ability systems of the textile industry's supply chain for the validation and coordination of up-to-date process status information [20].

As previously stated, virtually all of these systems are centralized (as presented in Fig. 2). Moreover, enterprises with small resources still rely heavily on manual operations or phone calls, e-mail correspondence, and web-based service to achieve minimum efficiency which remains ineffective to attend synchronization among supply chain partners.

In addition, the intervention of centralized middlemen, who are expected to enhance confidence between stakeholders, leads to confusion when they experience system dysfunction caused by manipulation or fraudulent attacks.

Because of these issues, the adoption of a coordinated system based on the various assets is not widespread among existing textile companies, which reduces the overall efficiency of the supply chain.

Figure 3 illustrates the framework of the supply chain traceability mechanism that is widely used in business today.

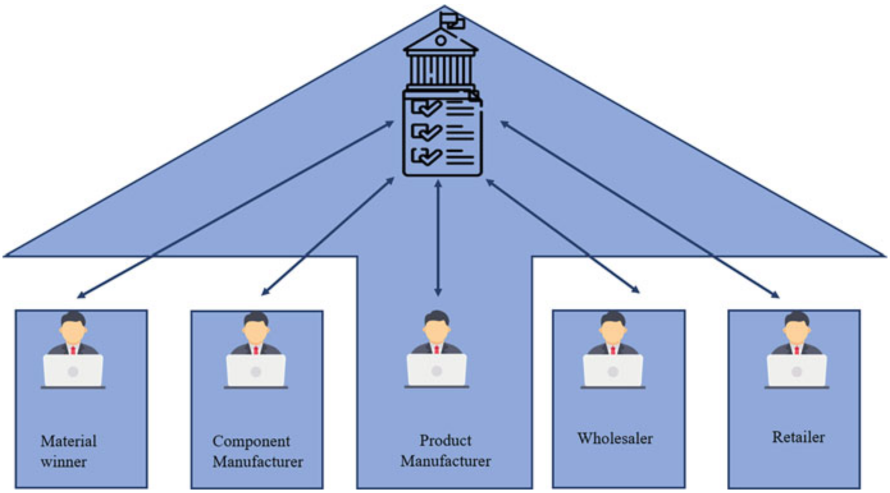


Fig. 2 Supply chain management by centralized entity. (Source: Martin Verwijmeren [22])

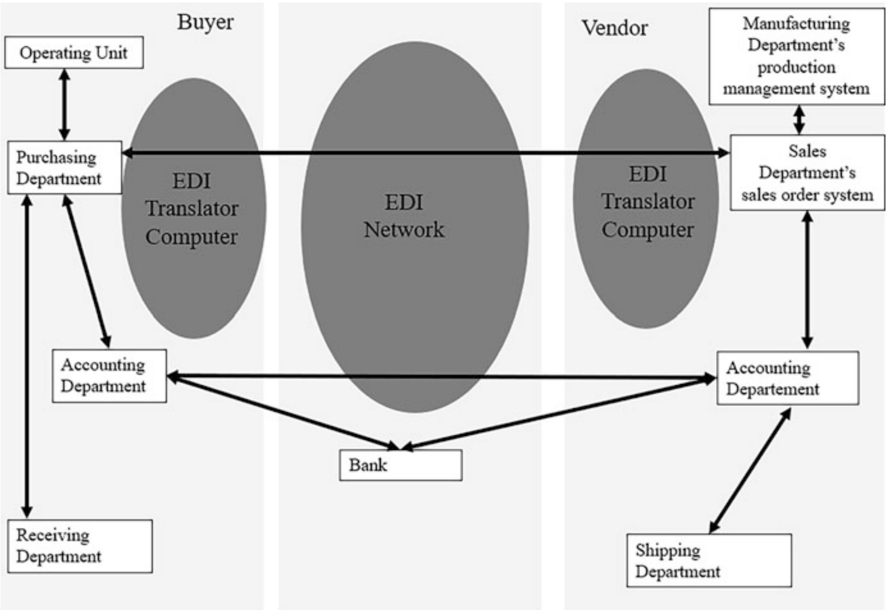


Fig. 3 Traditional method of supply chain traceability (EDI and VAN). (Source: Schneider [20])

3.3 *Textile Supply Chain Management with Blockchain*

Nowadays, the appearance of blockchain which is considered as a groundbreaking technology in decentralized information systems presents a whole new approach. A blockchain presents a connected list of blocks, where each block contains transactions [6]. Each block in the blockchain contains its own hash value as well as the previous block's hash value. As a result, each block is linked to the one before it, forming a "chain." Figure 4 depicts the blockchain technology's fundamental structure.

In this study, we present a textile supply chain traceability system for real-time product tracking based on blockchain which may provide a platform for all supply chain stakeholders to share information with the supply chain stakeholders in an open, trustworthy, secure, reliable, and transparent environment. In a blockchain network, all steps of the supply chain are recorded. Any player in the supply chain may add data to the blockchain in the form of transactions that are recognizable in the system, and all of the data in the blockchain is accessible. Every new transaction in the network is recorded in an immutable block that is time-stamped to maintain track of the specific product in the end-to-end chain and to ensure that the information included in the block is not tampered with. As shown in Fig. 5, our proposed system is a typical decentralized distributed system which integrates Internet of things such as RFID and WSN to collect data. A tag (RFID) is applied

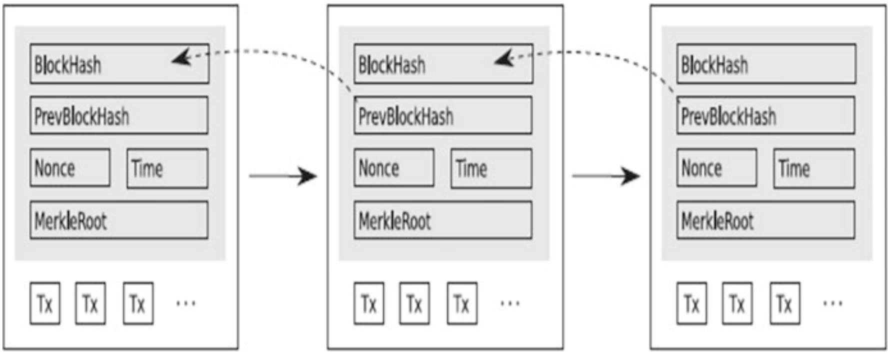


Fig. 4 A basic block diagram of blockchain [6]

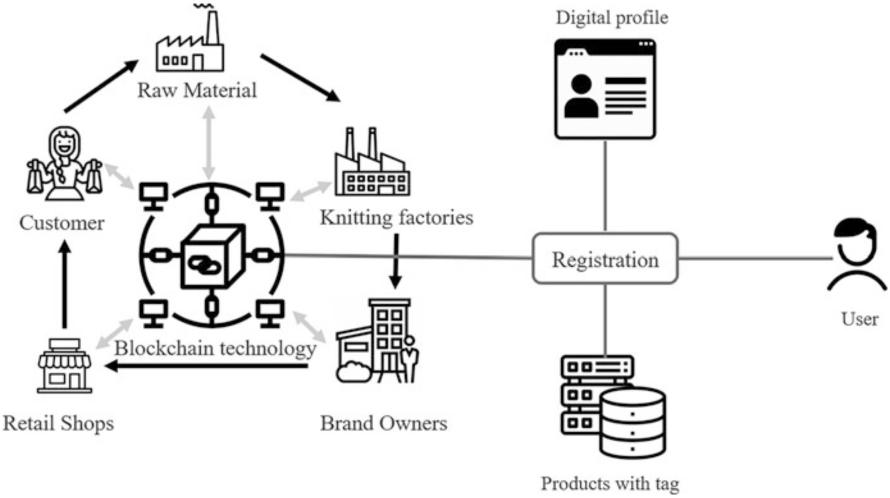


Fig. 5 Overview of textile supply chain management system with blockchain technology

to each product, which has a unique code that connects the physical items to their digital identities in the system. This digital depiction might be used to create a product profile. Users have their own virtual representation, which comprises important associated data. A blockchain-based system eliminates the need for a centralized trust authority; instead, all system users may log in and check the authenticity and history of any product. Security and immutability are guaranteed via a "mining process" which build trust among stakeholders. The general diagram of TSCM with blockchain is shown in Fig. 5.

4 Blockchain for Order-to-Cash

The order-to-cash (O2C) process refers to the part of the operational sales activities of the entire order processing system. It outlines the procedures that a firm must take to manage a sale from order to payment. Customers, vendors, banks, and transportation providers are all involved in the process, which results in a complicated process involving a large number of systems, communication channels, and different interface effort, as well as error-prone manual activities that have a direct impact on the enterprise's success and customer relationships [13]. The order-to-cash process starts with a credit check on a possible client and concludes when the consumer pays for the products received and the business applies the cash. Customers, Customer Service, Operations, Distribution, Sales and Marketing, and Finance and Accounting are the six departments engaged in the order-to-cash cycle. As a result, it is critical for each service to complete its operation, which should be error-free and transfer information correctly via the various regions. Improving this process enables the elimination of inefficiencies and third parties which can impact positively the entire process as we can see in the next part [18]. There are several benefits to streamlining the order-to-cash process. These benefits might be quite valuable, particularly if the firm invests heavily in higher-value-added operations and so on. Furthermore, it aids in the reduction of external funding, which improves profitability by lowering loan interest payments. Finally, it reduces the administrative procedures, time, and cost associated with collection management. The next section demonstrates how blockchain technology may improve current order-to-cash solutions and communications protocols, and how this solution can assist to solve common problems and improve existing order-to-cash procedures.

4.1 Current Order-to-Cash Solutions

Enterprise resource planning (ERP) solutions, which include SAP, Oracle, and PeopleSoft, enable automated data transfer across functional departments in the O2C pipeline. Nonetheless, ERP systems do not handle the management of customer risk, address potential order processing errors, or deal with cash flow following a customer invoicing. ERP systems are now used to manage business operations in most companies. These systems are used for a variety of purposes, including human resources, purchasing, finance, and sales procedures such as the O2C process. ERP systems need to be tailored to the requirements of each organization due to the uniqueness of business operations. The ERP system has a crucial part to play in changing the processes of a company [16]. However, these ERP solutions do not interact with other organizations' systems because each company uses a different ERP solution. Moreover, supply chains are ecosystems with multiple stakeholders and companies, which makes it complicated to have a holistic view of the supply chain and leads most of the time to inefficient processes and poor cross-functional integration. In the case of the (O2C) process, this can lead to inefficient receivables management and the occurrence of process failures, for example, a high error rate in order taking, customers who are unable or unwilling to pay on time, poor collection methods, and inadequate customer inquiry management systems are all factors that contribute to high error rates in order fulfillment. Blockchain technology has the potential to dramatically change this. This technology has the potential to serve as a missing link between many technologies. Additionally, it is difficult to make significant modifications to ERP systems once implemented. For this reason, when incorporating blockchains into legacy ERP systems, it is necessary to be mindful that there should be minimal modifications to existing ERP and minimal disruption to normal business processes.

4.2 The BigchainDB for O2C Process

To overcome the technological limitations of blockchain technologies, which include restricted scalability, low transaction rate, and high-power consumption, we chose to use the BigchainDB platform, which is with high data rate, low response time, strong query features, distributed monitoring, immutable data storing, and embedded support for assets. BigchainDB, in fact, is like a blockchain database [15], as it is defined on the official BigchainDB website. This platform was chosen because it is open source and can run a single node on any virtual machine. BigchainDB transactions are defined by three different elements which are as follows:

1. *The asset*: it represents physical to digital objects that we want to represent, for example, a dress with flowers or a cotton. It is impossible to modify or alter the information inside the asset.
2. *The metadata*: it allows the user to add details and information to the transactions, like origins, characteristics, transporter, etc. And this metadata can be updated for each transaction.
3. *The transaction ID*: it refers to the id of the transaction represented with a hash function over the entire information of the transaction. Figure 6 shows an example, from BigchainDB official site, of these elements.

This platform allows the definition of two main transactions. The first one is the CREATE transaction and the second one is the TRANSFER transaction. The first one allows users to create a new record in the database and the second one enables the user to transfer the ownership of defined record to another user.

.

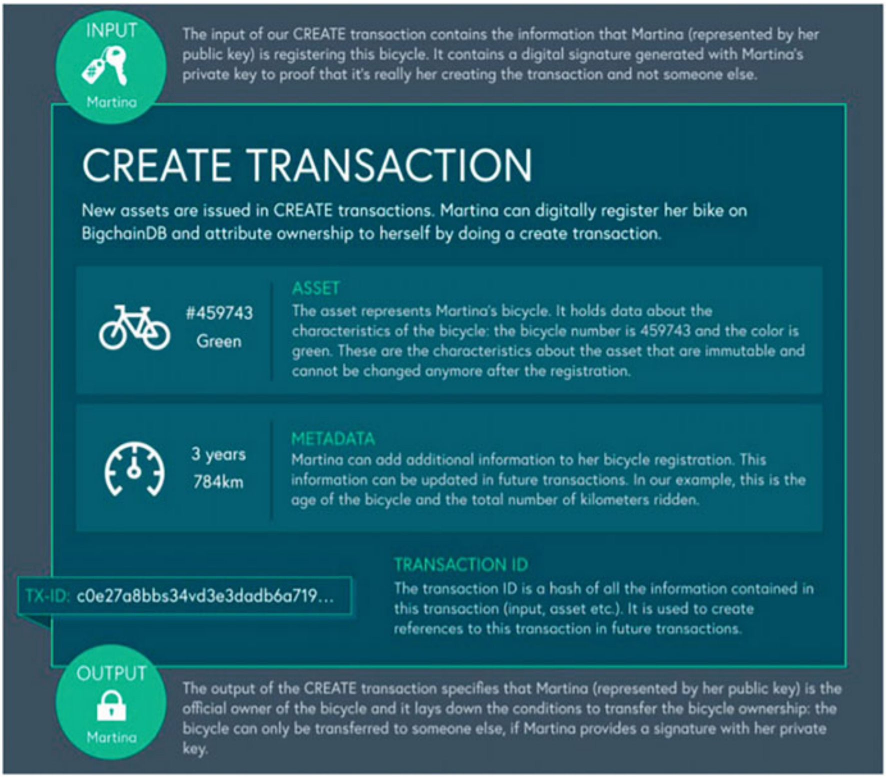


Fig. 6 Example of bicycle transaction using BigchainDB. (Source: BigchainDB official site)

5 Use Case

In this section, a use case of BigchainDB is presented that is integrated into the order-to-cash process. Through the example of the international commerce, it is illustrated exactly the way BigchainDB can streamline, automate, and reduce the complexity of the order-to-cash flow and remove the middleman from the process. As way of illustration, traditional method is illustrated in Fig. 7, while the BigchainDB is illustrated in Fig. 8.

The technological functionalities of the adoption are presented below: Supplier sells goods to a retailer that are delivered by a transportation service provider.

- *Step 1:* the retailer places a sales order with the supplier – When a supplier gets a retailer's order, which includes products, configuration, pricing, and delivery choices, the cycle begins.

  The merchant then requests a letter of credit from its financial institution, which is then issued to the supplier's financial institution.

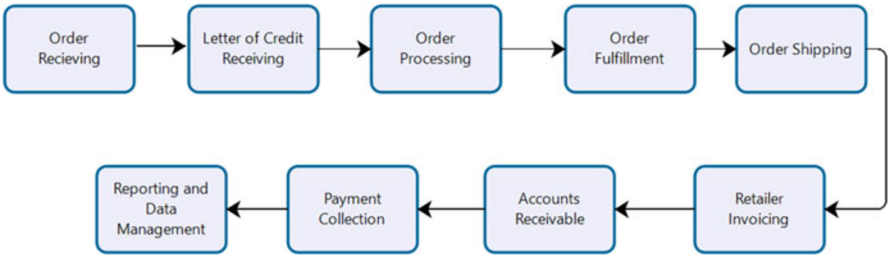


Fig. 7 Conventional order-to-cash process

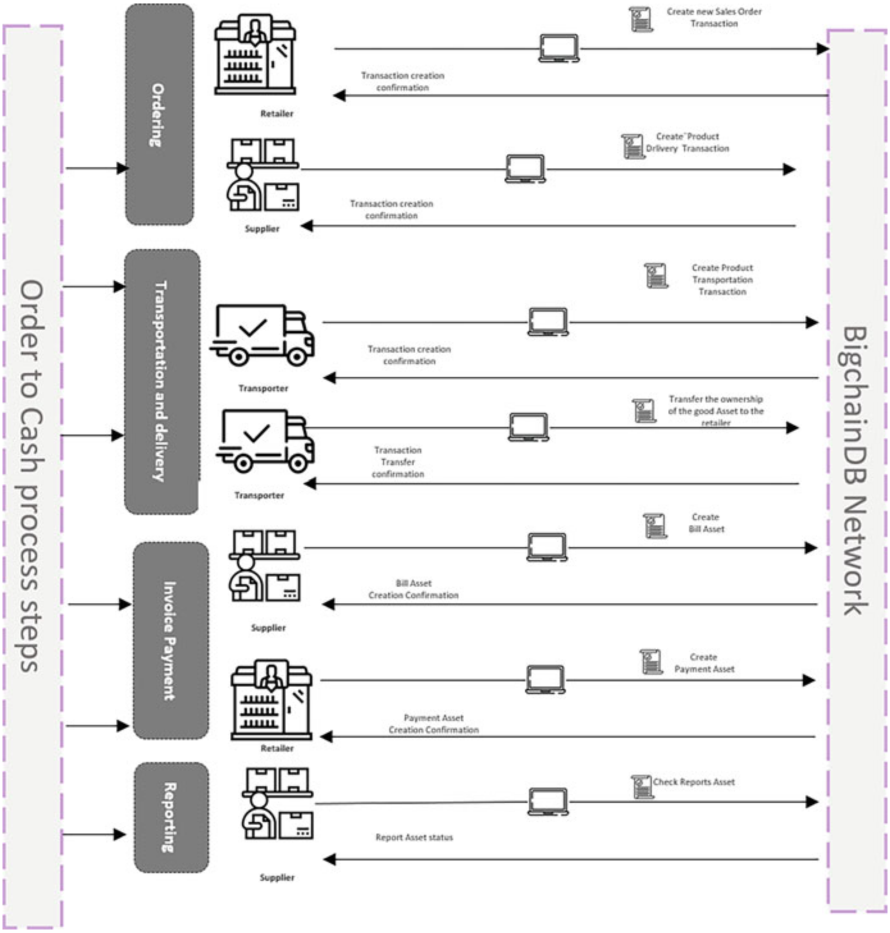


Fig. 8 Proposed procure-to-pay process with smart contract technology

A letter of credit is a document from the retailer's bank (issuing bank) guaranteeing that the retailer's (applicant) commitments to the supplier will be executed according to schedule and mutual agreed terms. If a retailer is unable or unwilling to pay for products, the issuing bank is responsible for covering the entire or remaining balance.

- *Step 2*: Order fulfillment – In this step, the supplier prepares the sales order for shipment to the retailer, and it includes finding, picking, packing, and handing the goods over to the transporter in exchange for a shipment's proof.
- *Step 3*: The invoice is created and sent to the retailer or an invoice is generated and sent to the retailer.
- *Step 4*: Payment – At this stage, the retailer orders its bank to pay the required amount to the bank of the supplier. The bank of the retailer then pays the bank of the supplier the required amount.
- *Step 5*: Payment is usually logged in a general ledger – When the supplier receives a payment for a given sales order, the accounts department will log it in the general ledger.

In addition to many process steps, the parties in this example use a variety of different IT systems to handle internal processes and external communication. For monitoring of resources and planning of requirements, most companies use ERP systems, like.

Furthermore, many of the major companies use systems that are specifically dedicated for data exchange and communication with third parties. The various IT systems, together with many steps, including numerous participants, create a heterogeneous and complex order-to-cash process. There are various physical papers and messages that must be transferred between parties through post, fax, and, at the very least, electronic via email for the traditional letter of credit method.

This type of communication slows down the company workflow and adds additional manual effort that is difficult to see. When everything goes flawlessly, the process of document exchange takes between 7 and 10 days. Figure 8 depicts the process of a traditional letter of credit.

The goal of the implementation of BigchainDB is to reduce the number of necessary participants, process steps, and actions for executing the order-to-cash process.

Figure 6 illustrates the parts of the process that might be automated or replaced using BigchainDB.

Additionally, there are a number of steps in the process which can be automated, namely, "credit management," "invoice processing," and various payment steps. The subsequent section showcases where BigchainDB is implemented in the traditional order-to-cash process. The new characteristics of the expected order-to-cash process with BigchainDB technology are highlighted in gray in Fig. 9. The banks are substituted by a BigchainDB platform upon which the requirements are implemented. The BigchainDB serves as a sort of distributed ledger to which all the involved parties can access, and the terms are integrated into the blockchain network

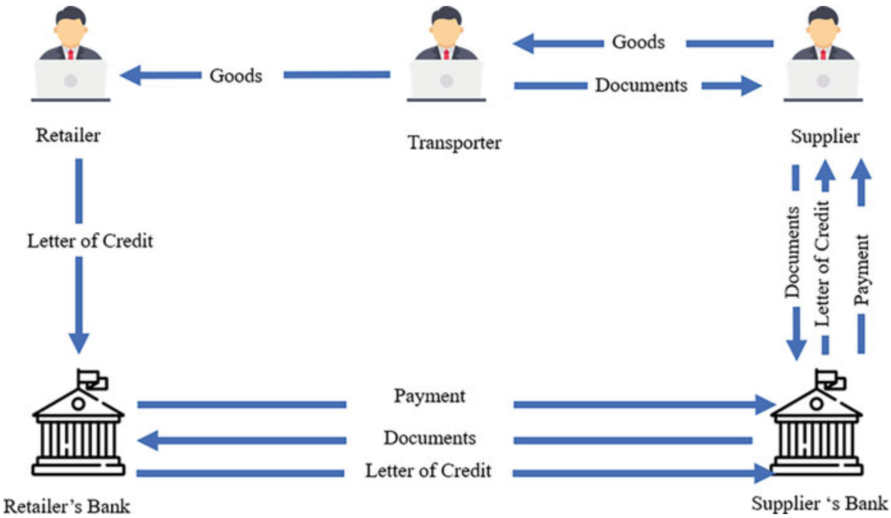


Fig. 9 Conventional credit of letter management

and enabled for "sales and demand matching," "automatic invoice processing and payment," as well as "leaving an audit trace."

To get things started, the retailer issues a sales order on the blockchain to the provider, which is then paired by a terms check implemented in BigchainDB beforehand. The contractual terms are determined by the BigchainDB platform, which ensures that the contractual terms are respected. The retailer checks the order with the delivery after having received the purchased items, and the data of the invoice will be processed automatically after its acknowledgment. The confirmation on accuracy of the transaction automatically initiates the operation of transferring the committed amount to the supplier's account while maintaining a seamless audit trail that is available to all involved parties for further reporting. It is worth mentioning here that for starters, banks are no longer needed. Blockchain brings the required security and trust among the two contractual parties. In addition, unneeded process steps are dropped by using self-executing smart contracts (letter of credit), and several of the remaining processes can be automated (e.g., credit management, invoice processing, and payment).

6 Conclusion

In this paper, we suggest a new strategy for a traceability system in the textile industry's supply chain based on decentralized technology. This system will offer real-time information about apparel products to all supply chain partners, reducing the danger of centralized information systems and providing a more secure, distributed, transparent, and collaborative approach. We also suggested that the BigchainDB platform be used in the order-to-cash process which is considered one of the most important processes in companies. Our proposition can significantly improve efficiency and transparency of this process with the elimination of intermediaries like banks in our use case and can also automate some operations like invoicing and credit management, which will obviously improve supply chain performance and rebuild the stakeholders' and investors' confidence in the textile industry. However, it was determined that for BigchainDB to be market-ready for industry, multiple challenges are yet to overcome especially for creating multi-node servers; we had some difficulties in this case and the documentation is not clear in this regard on their website. Besides that, future research should focus more on the integration between Blockchain technologies and ERP and other existing information systems like WMS (warehouse management system), TMS (transportation management system), PLM (data/knowledge life cycle management), MES (manufacturing execution system), and CAD (design), as it is important to explore how the data will be extracted from these systems and communicated to the blockchain framework.

References

1. Abernathy, F. H., Volpe, A., & Weil, D. (2004). *Previewing the apparel and textile industries after 2005: Prospects and choices*. The Harvard Center for Textile and Apparel Research. http://www.hctar.org
2. Agrawal, T. K., Koehl, L., & Campagne, C. (2018). A secured tag for implementation of traceability in textile and clothing supply chain. *International Journal of Advanced Manufacturing Technology, 99*, 2563–2577. https://doi.org/10.1007/s00170-018-2638-x
3. Håkansson, A., Nguyen, N. T.,Hartung, R. L., Howlett, R. J., & Jain, L. C. (2009) Agent and multi-agent systems: *Technologies and applications third KES international symposium, KES-AMSTA 2009, Uppsala, Sweden, June 3–5, 2009.* Proceedings Bigchaindb-Whitepaper. 2016.
4. Casey, M. J., & Wong, P. (2017). Global supply chains are about to get better, thanks to blockchain. *Harvard Business Review Digital Articles, 13*, *1–6*.
5. Cheung, H. H., & Choi, S. H. (2011). Implementation issues in RFID-based anti-counterfeiting systems. *Computers in Industry, 62*, 708718. https://doi.org/10.1016/j.compind.2011.04.001
6. Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain technology, *Proceedings of 2016 IEEE 13th International Conference on Service Systems and Service Management (ICSSSM)*, pp. 1–6. https://doi.org/10.1109/icsssm.2016.7538424.
7. Gobbi, L., & Massa, I. (2015). Supply chain management in textile sector: The case of the Italian T-fashion traceability system. *International Journal of Environment and Health, 7*, 359–370. https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf
8. Ilie-Zudor, E., Kemény, Z., Ekárt, A., et al. (2014). A solution for information management in logistics operations of modern manufacturing chains. *Procedia CIRP, 25*, 337–344. https://doi.org/10.1016/j.procir.2014.10.047
9. Keung Kwok, S., & Wu, K. K. W. (2009). RFID-based intra-supply chain in textile industry. *Industrial Management & Data Systems, 109*(9), 1166–1178.
10. Koetsier, J. (2017). *Blockchain beyond bitcoin: How Blockchain will transform business in 3–5 years*. Accessed 29 Mar 2019.
11. Kumar, V., Agrawal, T. K., Wang, L., & Chen, Y. (2017). Contribution of traceability towards attaining sustainability in the textile sector. *Text Cloth Sustain, 3*, 5.

12. Kumar, V., Koehl, L., & Zeng, X. (2016). A fully yarn integrated tag for tracking the international textile supply chain. *Journal of Manufacturing System, 40*, *76–86*. https://doi.org/10.1016/j.jmsy.2016.06.007
13. Zhang, L., Allam, A., & Gonzales, C. A.. (2006). Service-oriented order-to-cash solution with business RSS information exchange framework. *2006 IEEE International Conference on Web Services (ICWS'06)*, pp. 841–848. https://doi.org/10.1109/ICWS.2006.121.
14. Lee, S.-Y. (2008). Drivers for the participation of small and medium sized suppliers in green supply chain initiatives. *Supply Chain Management: An International Journal, 13*, 185–198.
15. McConaghy, T., Marques, R., Müller, A., De Jonghe, D., McConaghy, T., McMullen, G., Henderson, R., Bellemare, S., & Granzotto, A. (2016). *BigchainDB: A scalable blockchain database*. White paper, BigChainDB.
16. Müller-Jentsch, D. (2005). *Deeper integration and trade in Services in the Euro-Mediterranean Region: Southern dimensions of the European neighborhood policy*. World Bank.World Bank. https://openknowledge.worldbank.org/handle/10986/733
17. Pigni, F., Crave, S., & Ravaini, A. (2007). Traceability in the textile and clothing industry: Issues and implications for RFId adoption: *The 2nd Mediterranean conference on information systems, MCIS.* Venice*,* Italy, p 2007.
18. Corbellini, S., Ferraris, F., & Parvis, M. (2006). A cryptographic system for brand authentication and material traceability in the textile industry. 2006 IEEE *Instrumentation and Measurement Technology Conference Proceedings, Sorrento,* pp. 1331–1335.
19. Saak, A. E. (2016). Traceability and reputation in supply chains. *Int J Prod, 177*, 149.
20. Schneider, G. P. (2017). *Electronic commerce* (12th ed.). Cengage Learning.
21. Chang, S. E., Chen, Y.-C., & Ming-Fang, L. (2019). Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. *Technological Forecasting and Social Change, 144*, 1–11.
22. Verwijmeren, M. (2004). Software component architecture in supply chain management. *Computers in Industry, 53*(2), 165–178.

Exploiting Cost-Effective IoT Devices for Trustless Agri-Food Supply Chain Management: A Practical Case Study

Miguel Pincheira, Massimo Vechio, and Raffaele Giaffreda

1 Introduction

Today, the vast majority of traditional logistic information systems in Agriculture and Food (Agri-Food) supply chains merely tracks and stores orders and deliveries without providing features such as transparency, traceability, and auditability. These features surely improve food quality and safety; therefore, they are increasingly being requested by consumers [24]. However, the supply chain in Agriculture and Food is a highly complex process due to the disparity of stages and actors involved. Each stage has particular characteristics, and each actor has different requirements. Thus, achieving transparency, traceability, and auditability along this complex process is not a simple task and requires collaboration between all the involved actors [8]. Collaboration requires overcoming several barriers such as the lack of willingness to share information, skepticisms for security and reliability, limitations of actual contractual relations, and mostly the uncertainty about the impact of the information sharing [25].

Thus, several Research & Development communities are concentrating efforts on adopting some specific digital technologies to realize them in the Agri-Food supply chain management. The Internet of Things (IoT) has contributed to this development, with technologies such as RFIDs and Wireless Sensor Networks. An increasing number of cost-effective connected devices enabled remote monitoring of food transportation scenarios with fine granularity. The devices contribute along the whole Agro-Food supply chain, e.g., from production to consumption [22] creating a more detailed and accurate description of the entire process.

M. Pincheira (✉) · M. Vechio · R. Giaffreda
OpenIoT Research Unit, Fondazione Bruno Kessler, Trento, Italy
e-mail: mpincheiracaro@fbk.eu; mvecchio@fbk.eu; rgiaffreda@fbk.eu

A. Bouras et al. (eds.), *Blockchain Driven Supply Chains and Enterprise Information Systems*, https://doi.org/10.1007/978-3-030-96154-1_6

Centralized cloud-based architectures are the current choice for IoT systems, where a validating third party provides services such as authentication, authorization, and data handling for both sensing devices and end users [4]. These architectures simplify the design and the deployment of IoT systems and applications; however, they introduce additional concerns regarding privacy and data management [5, 27]. Moreover, centralized cloud infrastructures typically lack transparency and auditability [3] and present a single point of failure for the entire system. These challenges are vital issues on an Agri-Food supply chain system, requiring radically new approaches for the architectures behind such systems and applications.

In recent years, there has been a growing interest in integrating blockchain technologies into IoT [2] for enabling trustless architectures. Blockchain uses a unique combination of cryptography, data structures, and incentive mechanisms to maintain a particular type of distributed database (i.e., a *ledger*) in a peer-to-peer network. The distributed ledger is immutable by design and offers an auditable and transparent source of information. Blockchain provides a trusted repository of information for IoT systems, where data is secure and traceable, and the data source can be precisely identified [16]. For an Agri-Food supply chain system, blockchain directly benefits the entire process by enabling the seamless inclusion of several actors [23] and making their interactions leaner, faster, and more transparent [2]. Thus, blockchain is attracting increasing interest for security and transparency in various steps in the Agri-Food supply chain process [11, 21]. However, previous work has only focused on the conceptual application of blockchain in Agri-Food supply chains or has failed to address the role of cost-effective IoT devices.

In this chapter, we present a fully decentralized traceability system for Agri-Food supply chain management. The proposed solution is blockchain-agnostic and considers cost-effective IoT sensor devices. The devices produce and consume valuable information along the whole supply chain and directly interact with the underlying blockchain. To assess the feasibility of the proposed solution, we engineered and deployed a prototype for a *from-farm-to-fork* use case: a classical food traceability scenario fostering certified traceability of food along the whole supply chain, e.g., from agricultural production (the farm side) to consumption (the fork side). Then, we focus on evaluating the impact that the blockchain integration process has at the IoT device level in terms of memory, program size, communications, and power consumption, using two different blockchain implementations.

The remaining of this chapter is organized as follows: Sect. 2 summarizes the current state of the art in the adoption of blockchains as an enabling technology for the traceability in Agri-Food supply chains; Sect. 3 describes the proposed system architecture; Sect. 4 contains details about our implementation; Sect. 5 describes our experimental setup; Sect. 6 presents our preliminary results; Sect. 7 concludes the chapter.

2 Related Work

The last few years have witnessed an explosion of research and development activity around the Blockchain technology, mainly within the financial technology (FinTech) industry. Indeed, its intrinsic capability of providing immutable and tamper-proof records, together with its potential of enabling trust and reliability among untrusted peers, represents too attractive features, preventing this technology to stay relegated into a single vertical sector. For this reason, several industries beyond the FinTech sector have already identified the Blockchain technology as a driver for a paradigm shift. For data reliability, ProvChain [9] explored the use of the Blockchain technology in a cloud storage scenario to verify three levels of data provenance: collection, storage, and validation. In this chapter, the use of blockchains showed good results in terms of tamper-proof records and user privacy, with very low overhead for the storage itself. In a similar context, the authors on [15] explored the use of blockchains with smart contracts to achieve secure data provenance, using the Open Provenance Model (OPM) with an access control-based privacy-preserving solution.

Also the adoption of some IoT devices and technologies in the supply chain management sector has attracted a lot of research interest in the last few years. From the impact of autonomous identification system [12] to the application of RFID technologies in logistics [19], the technological maturity of the devices and of the sensors is literally revolutionizing each step of the process. Specifically for the Agri-Food domain, the authors of [18] presented an inventory transparency use case, also adopting some IoT devices. There, the goal was to explore the use of RFID and NFC-based devices to achieve transparency and real-time information production directly on the field, enabling persistence by means of a centralized, cloud-based database. This is indeed the classical paradigm adopted by far the majority of the current IoT-based solutions.

However, the use of both the Blockchain and the IoT technologies in the Agri-Food domain is still an underexplored, yet worth-to-explore, research field. A traceability system based on the blockchain and the RFID technology was proposed in [20], with a sharp focus on Chinese food markets. The work considered fresh food asset tracking as fruits, vegetables, and meat, by means of RFID-based devices for the data acquisition and blockchains for data persistence. The authors of [21] presented a supply chain traceability system for food safety, based on HACCP (Hazard Analysis and Critical Control Points), and focus on transparency. There, they described the process of crop plants in different phases, from harvesting to retailing, without going into the details of a performance analysis. The authors on [11] explore the use of smart contracts for a credit evaluation blockchain-based system to food supply chain management. The authors on [10] present case study applied to Shandong province in China where blockchain-based system, based on a consortium blockchain implementation, is used to optimize trading portfolio of buyers in the food supply chain. With a more practical approach, the authors on [17] present a blockchain-based traceability system, for the soybean. The work presents a detailed description of an implementation using Ethereum network and focused on the smart contracts supporting the system.

Overall, to the best of our knowledge, the current literature lacks a detailed analysis of the impact that a blockchain may have on the traditional IoT-based system and in particular on the more constrained sensing IoT devices. If sensing devices become direct actors on the blockchain system, they can provide a *"root of trust"* for the sense data. Moreover, a trusted source of information not only benefits IoT systems but also other types of blockchain-based applications, with sensing IoT devices acting as trusted oracles [7].

3 Blockchain-Based Traceability

In this section, we describe our proposal of a blockchain-based traceability system for the Agri-Food supply chain. In our proposal, cost-effective sensing devices measure several parameters along the entire process. In order to define the requirements for our proposed architecture, we must first formalize the requirements of a traceability system and then identify the key elements of each stage that provides transparency and trust to the entire process.

3.1 Supply Chain Process

The authors on [1] addressed the issue of a food supply chain from an operation's perspective, identifying several activities and process, as well as actors and items. In order to integrate the IoT environment, they simplify the process into 5 generic stages: Agricultural/Production, Distribution/Transport, Storage, Consumption, Waste/Disposal. On the other hand, the authors in [25] propose a virtualization of the food supply chain, which is represented by an architecture where the real objects are mapped to a virtual object. The authors simplified the supply chain process into four actors: Farmer, Food Processor, Transporter/Trader, and Retailer. For the particular case of Extra Virgin Olive Oil traceability, the author at [26] defined 4 steps for the process: Harvesting, Milling, Storage, and Packing.

Based on these previous works, and similarly to [6], we simplified the process into 3 stages: Farming, Transportation, and Market as shown in Fig. 1. Each of these stages is composed of several activities, with specifics actors, which are important to the traceability and are briefly introduced in the following:

(a) **Provider:** Providers of raw materials, such as seeds and nutrients, but also pesticides, chemicals, etc.
(b) **Producer:** Usually, the farmer, e.g., the responsible of the actions from seeding/planting to harvesting.

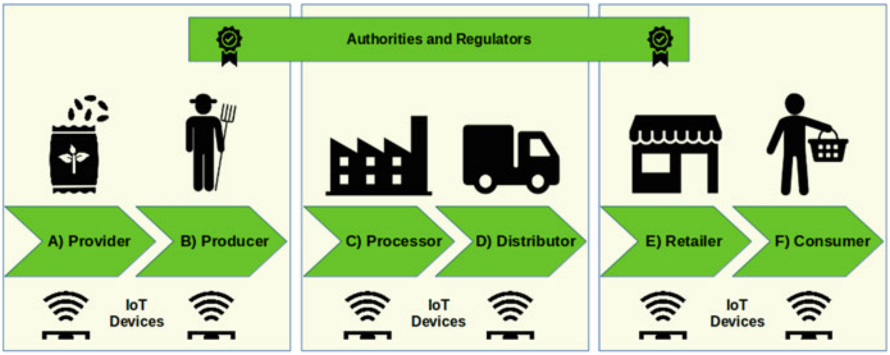


Fig. 1 Simplified version of the Agri-Food supply chain management process [6]

(c) **Processor:** This actor may perform various actions, from simple packaging to more complex processes (e.g., pressing of the olives).
(d) **Distributor:** This actor is responsible of moving the output of the processor (e.g., the product) from processor's site to retailers.
(e) **Retailer:** This actor is responsible of selling the products, representing it either small local stores or big supermarkets.
(f) **Consumer:** The final element of the chain.

Along the whole process, authorities provide standards, regulations, laws, rules, and policies that the involved actors have to comply with.

3.2 Functionalities

To coherently define the high-level functionality of our architecture, we had a bottom-up approach through which we extracted the set of requirements starting from a complete use case, namely, *from-farm-to-fork*. The latter is, indeed, a classical food traceability use case that fosters certified traceability of food along the whole supply chain, from agricultural production to consumption. Our proposed solution shall provide consumers with a complete history of the food he is buying. The only pre-condition is that all the participants (so including the IoT devices) are registered users of the underlying blockchain, meaning that they have the correct public/private key pairs to digitally sign each operation on the distributed ledger. In the following, we summarize the list of extracted requirements:

1. **Raw Materials Purchasing:** Producers and providers store in the blockchain the details of sales and purchases of raw materials, including technical information of products and amounts. Note: Smart tags (e.g., barcode, QR codes) can be used to automatize this process.

2. **Planting:** Producers store in the blockchain information about the planting process (e.g., the amount of seeds used). Note: Sensors can automatize such data entry process (e.g., connected weight scales), while smart contracts can autonomously fire, hence creating records whenever anomalies are detected (e.g., more seeds than the ones registered as purchased).
3. **Growing:** Sensors, at regular intervals, autonomously store in the blockchain information about the growing plants and environment. Note: Smart contracts can asynchronously fire, hence creating records whenever anomalies are detected (e.g., sensor values outside certain thresholds).
4. **Farming:** Farmers store in the blockchain information about each stage of the process (e.g., irrigation, fertilizing, etc.), including the amount of inputs applied. Note: Sensors can automatize such data entry process (e.g., chemical sensors and multisensory systems), while smart contracts can autonomously fire, hence creating records whenever anomalies are detected (e.g., sensor values outside certain thresholds).
5. **Harvesting:** Farmers store in the blockchain details about the harvesting. Note: Sensors can automatize such data entry process (e.g., connected weight scales), while smart contracts can autonomously fire, hence certifying that the process from seeding to harvesting is compliant with certain regulations (e.g., organic, fair trade, etc.).
6. **Delivery to processor:** Farmers transfer the ownership of the products to distributors, directly through the blockchain. Note: Sensors (e.g., GPS sensors) and smart contracts can automatize this process or create records whenever anomalies are detected during the delivery phase (e.g., sensor values outside certain thresholds).
7. **Processing:** Considering the simplest case of a packaging processor, the latter store in the blockchain details about the received amount of product from distributors, the packaged amount, and, eventually, the amount of product lost during the processing phase. Note: Sensors can automatize such data entry process (e.g., connected weight scales), while smart contracts can autonomously fire, hence creating records whenever anomalies are detected (e.g., the packaged amount is larger than the received amount).
8. **Delivery to retailers:** Processors transfer the ownership of the processed product to distributors, directly through the blockchain. Note: Sensors (e.g., GPS sensors) and smart contracts can automatize this process or create records whenever anomalies are detected during the delivery phase (e.g., sensor values outside certain thresholds).
9. **Retailing:** Retailers store in the blockchain details about the received amount of product from distributors. Then, at regular intervals, sensors autonomously store in the blockchain information about the status of the retail environment. Note: Smart contracts can asynchronously fire, hence creating records whenever anomalies are detected (e.g., sensor values outside certain thresholds).

10. **Consuming:** Retailers store in the blockchain details about the sold products, while consumers are able to transparently verify the whole history of a product before buying it. Note: Smart tags can be associated to each package, so that consumers can easily retrieve the whole history of the product.

3.3 Proposed Architecture

We propose an architecture able to rely on the Blockchain and the IoT technologies to achieve transparency, auditability, and immutability of the stored records in a *trustless* environment. In our architecture, sensing devices have a unique blockchain identity and act as trustworthy datasources for smart contracts [7]. Our architecture uses smart contract to implement the business logic of the traceability process. For instance, once basic contract could agree the transport of the raw material to the processing factory. The contract could hold the payment in escrow and based on the information provided by the sensors during the transportation. Sensors could automatically cancel the payment, if, for instance, the temperature or humidity during transportation exceeds the agreed thresholds. Moreover, our architecture allows to seamlessly integrate additional actors that can provide the rewards or certifications, using the transparent and immutable register of all the information captured by the sensor across the entire supply chain process [14]. The architecture is shown in Fig. 2.

To obtain fine-grained information across the entire process, we rely on low-cost, energy-efficient sensing devices. To fully exploit the potential of the combination of the IoT with blockchains, these monitoring devices are considered proper actors of the underlying blockchain [13].

In our architecture, each device manages its own blockchain identity, hence autonomously issuing and signing its own transactions in the blockchain when needed. Thus, each monitoring node can transmit the value it measures directly toward a blockchain node. The transactions are directly fed purposely designed

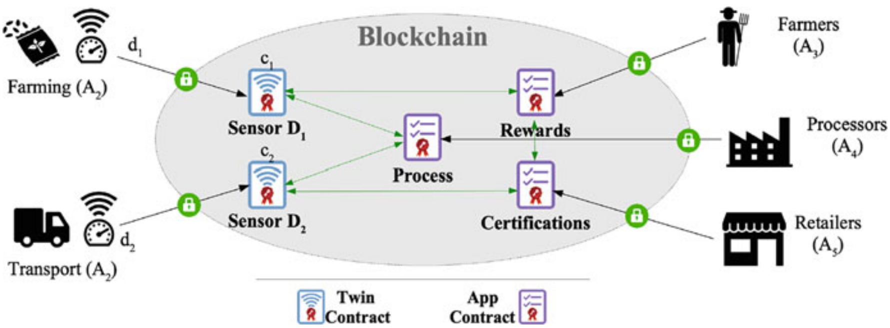


Fig. 2 High-level architecture for blockchain-based traceability

smart contracts deployed in the blockchain network. This process guarantees the integrity of the data by creating immutable, auditable, and non-repudiable records that are easily verifiable by other users.

To keep low the transaction rate of the sensing nodes, we allow for aggregating multiple readings at the sensor side. This means that a sensor node can transact aggregated values to the blockchain (for instance, hourly or daily values depending on the requirements of the application), while the individual data points can be stored in more traditional IoT platforms/services. In this way, the users (or the service provider) can set the frequency of the reports, based on the trade-offs in terms of energy budget of the sensor nodes, transaction cost in the public blockchain, and maximum delay tolerable by the application/business processes.

In our system, each device is represented by a unique smart contract deployed in the blockchain. More formally, if an IoT deployment D is composed of n sensor devices d_i (with $i = 1, \ldots, n$) such that $D = [d_1, \ldots, d_n]$, then we assume that $\forall\, d \in D \quad \exists!\, c \in C$, where $C = [c_1, \ldots, c_n]$ represents the group of smart contracts c_i mapping the i-th device in the blockchain. Therefore, each smart contract can be seen as the device's "digital-twin" in the blockchain (for analogy, we refer to it as the device's "smart-twin"). This contract has a template interface, including both public and private methods. Private methods update the state of the twin in the blockchain and can be invoked only by the device owning the blockchain identity, while public methods simply provide a standardized interface for other smart contracts. Thus, a billing contract or a transportation contract can use device's smart contracts as transparent sources of information in a trustless way.

3.4 Software Framework

We conceptualized our architecture into a layered software framework similar to current IoT layered architectures. The software framework, shown in Fig. 3, is divided into three modules, namely the Device, Gateway, and Blockchain modules. The Device module converts the sensed values into blockchain transactions that are later sent to the corresponding smart contract. The Gateway module is a simple relay component between the device and the blockchain layer. Finally, the Blockchain module gathers together all the smart contracts representing the sensors and the different process of the traceability system. In the following, these modules will be thoroughly described.

3.4.1 Device Module

The objective of this module is to interact with the physical world and create blockchain transactions. This software module run on the sensing devices and has three components: Sensing, Blockchain Integration, and Communications. The sensing components interface with the sensor, and its output is a sensed value from

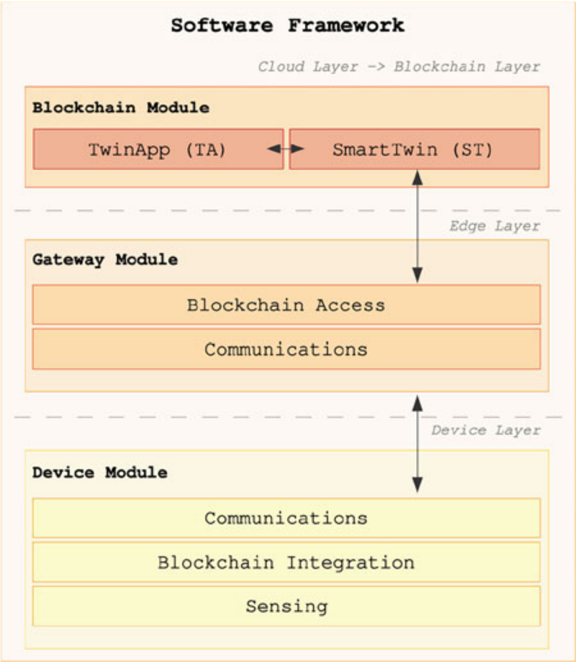


Fig. 3 Layered software framework

the physical world. The Blockchain integration component converts the sensed value into a blockchain transaction, making the device direct actor in the blockchain system. The communications components send the transactions to the blockchain. Typically, this is done using a constrained communication protocol to reach a gateway (on the next layer), which later forwards the transaction to blockchain. The complexity of this component will depend on the blockchain implementation used (to create a transaction) and in the communications protocol selected.

3.4.2 Gateway Module

The objective of this module is to receive the transactions from the lower layer and then forward to the next layer, making the appropriate protocol conversions. The gateway module has two components: Communications and Blockchain access. Communications handles the restricted communication protocol with the lower layer to receive the transaction. Blockchain Access simply forwards the transaction to a peer on the blockchain, typically using the standard TCP access to the Internet. Despite the protocols used, the transaction is digital signed and the device, and it cannot be modified in this layer. The complexity of the module will depend on the communications protocols used.

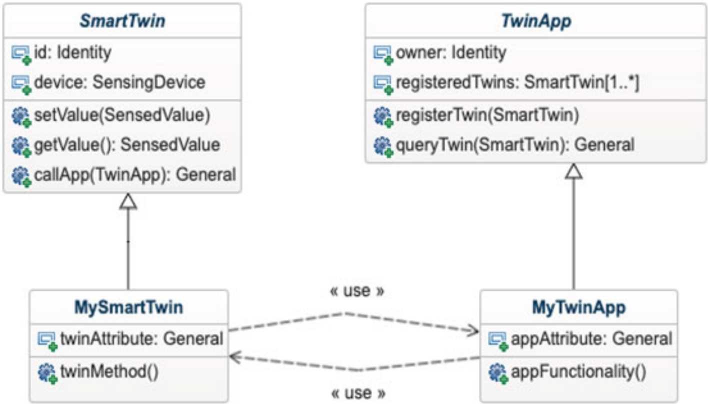


Fig. 4 Smart contracts' classes of the proposed software architecture

3.4.3 Blockchain Module

The objective of this module is to provide all the business logic using the application by using smart contracts and their interactions. We define two types of smart contracts: the Twins and the Apps as depicted in Fig. 4. From a software perspective, these contracts are high-level abstract classes with a series of primitives that can be extended to fulfill the requirements of each application.

The SmartTwins are simplified representations of the IoT devices in the shape of "*smart twins*." As an interface, the SmartTwin implements three methods, namely `getValue()`, `setValue()`, and `callApp()`. `getValue()` is used by the sensing device to update the twin. `getValue()` is used by TwinApp contracts to interact with the SmartTwin. `callApp()` is used by the SmartTwin to interact with the TwinApp. The SmartTwin has two basic properties, a unique identification, and the identity of the sensing device that it represents. It is important to notice that the method `setValue()` is restricted only to the sensing device.

The TwinApps are the types of applications that can interact with SmartTwin and provide two basic methods, namely, `registerTwin()` and `queryTwin()`. In our architecture, SmartTwins are required to first register with a particular application, by using the `registerTwin()` method. After registration, the TwinApp can interact with the SmartTwin using the `queryTwin()` method. The TwinApp maintains two properties, the identity of the owner of the app and a list of all registered SmartTwins that can interact with the application.

This module also provides a REST Application Programming Interface exposing the capabilities of the architecture to other applications. It relies on the API provided by the underlying blockchain network and should allow and easy integration with the existing software systems and other software components (e.g., user graphical interface).

4 Implementation

To better describe and quantitatively assess the benefits of the proposed technology architecture, we implemented it as a fully working prototype. In particular, we focused on the *Delivery to processor* functionality described in Sect. 3.2 as shown in Fig. 5. Our architecture is blockchain-agnostic; therefore, for our evaluation, we tailored our architecture to two different blockchain implementations: Ethereum and Hyperledger Sawtooth. Nonetheless, migrating the architecture to other implementations should not present a major issue. The reasons of choosing these implementations are two-folds. First, we have references for both public and private blockchain networks. Second, the selected blockchains provide different levels of customization for the records included on the ledger (transactions). Ethereum works with a single transaction structure, while Hyperledger Sawtooth allows the definition of a custom transaction structure.

4.1 Device Module Implementation

The values acquired by the sensing devices need to be converted into a blockchain transaction. For Ethereum and Sawtooth, there is no official implementation that can be used in constrained IoT devices, and, to the best of our knowledge, no third-party libraries providing cross-platform compatibility exist. For this reason, we decided to implement our own software library, based on open-source initiatives and favoring cross-platform compatibility over code optimization. We opted for the C language within the Arduino development framework.

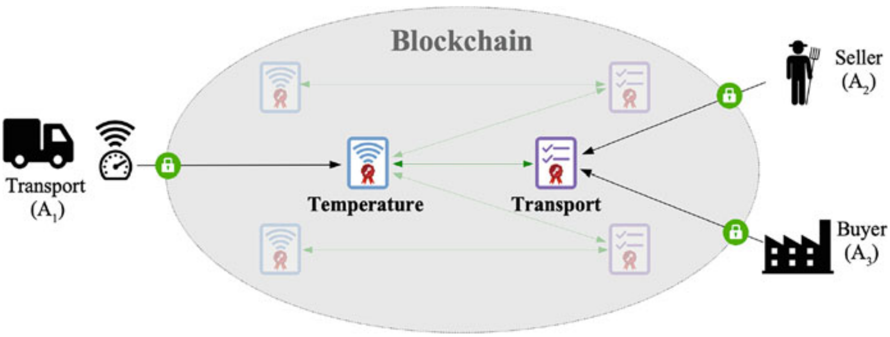


Fig. 5 Implementation of Delivery to Processor functionality of the proposed architecture

4.1.1 Sensing Component

For our prototype, we implemented a sensing stage using a DHT11 temperature and humidity sensor. The sensing stage includes an open-source library to read the values from the sensor that, in this case, is only temperature as an integer.

4.1.2 Blockchain Integration Component

The values acquired by the sensing devices need to be converted into a blockchain transaction, as the minimal unit of information inside the blockchain network. The process of creating a transaction for a particular payload (i.e., the sensed value) varies between implementations; however, the process typically includes 3 steps: encoding for serialization of the data, hashing for integrity of the payload, and digital signing for identity.

For Sawtooth, the encoding uses ProtoBuff, a serialization scheme proposed by google. The hashing of the payload uses the SHA512 algorithm. To sign the transactions, Sawtooth uses the Elliptic Curve Digital Signature Algorithm (ECDSA), with the sepk256 parameters, and the SHA256 hashing. Algorithm 1 shows the process, and while the transaction itself is created half-way the algorithm, the final result is a batch list that might include several transactions.

Algorithm 1: Creating a sawtooth transaction

Result: Sawtooth Transaction (Batch list)
hash_payload = $hash512$(payload);
tx_header = $encodeProtoBuff$();
hash_tx_header = $hash256$(tx_header);
header_signature = $ECDSA$(hash_tx_header, private_key);
transaction = $encodeProtoBuff$();
batch_header = $encodeProtoBuff$();
hash_batch_header = $hash256$(batch_header);
batch_signature = $ECDSA$(batch_header, private_key);
batch = $encodeProtoBuff$();
batch_list = $encodeProtoBuff$();

For Ethereum, the encoding is a custom serialization method called Recursive Length Prefix (RLP). The hashing is the Keccak-256 hashing algorithm, returning a 256-long-bit array. The signature is the same ECDSA as used by Sawtooth. The process of creating an Ethereum transaction is shown in Algorithm 2.

Algorithm 2: Creating an Ethereum transaction

Result: Ethereum Transaction
tx_body = $encodeRLP()$;
hash_tx_body = $hash256$(tx_header);
tx_signature = $ECDSA$(hash_tx_header, private_key);
transaction = $encodeRLP()$;

4.1.3 Communications Components

For a reference, we used serial communications at 115200 bps between the device and the gateway using a USB connection.

4.2 Gateway Module Implementation

The transaction sent by the device is received by this module and forwarded to the next layer. We implemented this module in Python 3.6.

4.2.1 Communications

In our prototype, this module interfaces with the serial port at 115200 and receives the transactions as a byte array.

4.2.2 Blockchain Access

The transaction, received on the serial port, is sent to a blockchain node using a network connection. In this prototype, the nodes (both for Ethereum and Sawtooth) are hosted on a physically different computer server and can be accessed by a REST API.

4.3 The Blockchain Module

For our prototype, we implemented a SmartTwin for temperature sensor and TwinApp for the transportation process. For Ethereum, the smart contracts were implemented using solidity language and compiled for version 0.6.2. For Sawtooth, the contracts were implemented using Python 3.6.

5 Experimental Setup

To evaluate our solution, we tested our cross-platform prototype on different microcontroller (MCU) boards. To address truly constrained devices, we set a maximum clock speed of 100 MHz and selected seven different boards from the AVR, ARM, and ESP32 architectures. While a comprehensive evaluation of all possible IoT boards is far beyond the scope of this chapter, the selected pool should provide a reference for other scenarios. Table 1 presents all the boards, detailing clock speed, program space, memory size, model, and a reference price (updated to May of 2021).

5.1 Hardware and Software Setup

For Ethereum, we used the official Geth client (version 1.10.1-stable) to run two independent nodes: one node for the Ropsten network, working with Proof-of-Work consensus (PoW), and the other node for the Goerli network, working with Proof-of-Authority (PoA). Each node runs on a virtual machine with 4 GB of Ram, 20 GB of SSD, and 4 vCPU on an OpenStack server using a clean Linux Ubuntu installation (version 18.04). For Sawtooth, we used the official client (version 1.2.6) to run a private network using the dev-mode engine as a test network. The scripts that deploy and interact with the smart contracts were implemented using Python (version 3.6) and ran on a Lenovo T490s notebook, with 16 GB of Ram 256 SSD disk, and an Intel i-7 processor at 1.90 GHz over a clean Linux Ubuntu (version 18.04). The notebook and the nodes shared the same LAN connection.

Table 1 The hardware platforms used during our performance evaluation

Device	Model	MCU	Architecture	Clock (MHZ)	Prog. mem. (KB)	SRAM (KB)	Price (EUR)
UNO	Arduino Uno	ATMega328P	8-bit AVR	16	32	2	18
EVERY	Arduino nano every	ATMega4809	8-bit AVR	20	48	6	12
L031	STM32L031	Cortex M0+	32-bit ARM	32	32	8	10
F303	STM32F303	Cortex M4	32-bit ARM	72	64	12	10
L452	STM32L452	Cortex M4	32-bit ARM	80	512	96	12
ESP32	ESP DevKit	WRover-E	32-bit ESP32	80	1024	320	10

6 Evaluation

6.1 Device Module Footprint

Using the statistics provided by the compilers, we estimated the footprint of each component of the device module. The results, in terms of disk usage (flash memory usage), are shown by means of Table 2 (absolute values) and Fig. 6a (normalized to the total available flash memory). The same approach was taken for the memory usage, by means of Table 3 and Fig. 6b. Sensing (Sens) and Communications (Comms) are the same for both implementations. The footprint of Blockchain Integration for Ethereum is represented by Eth, and the Blockchain Integration for Sawtooth is represented by Saw. From these results, we can see that the Sawtooth implementation has a bigger footprint on the device, and only 4 of the 6 boards are capable of running the entire module.

6.2 Device Module Processing Times and Power Consumption

We measured the processing time and power consumption of each board when creating 100 transactions. We used a Otii device[1] cable to provide current measurements with an accuracy of $\pm(1\% + 0.5\,\mu A)$ at 5V with a rate of 1000 samples/s. As a

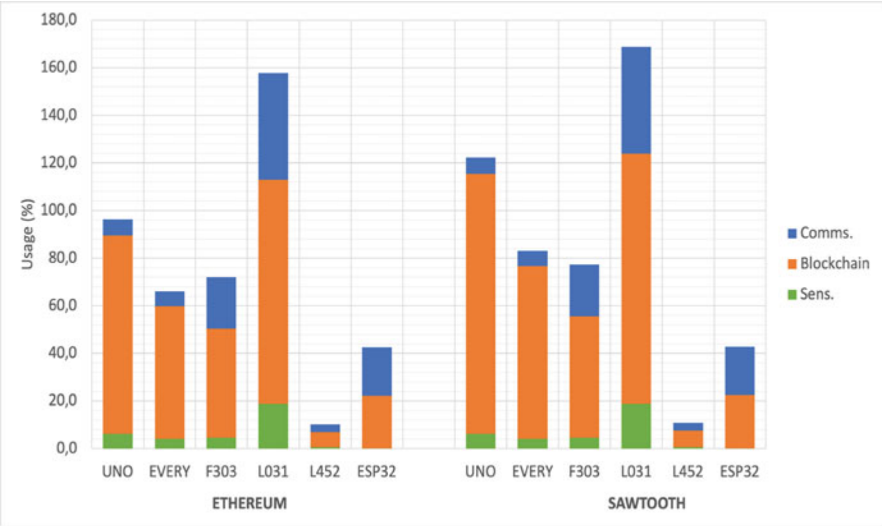
Table 2 Disk usage of the device module (expressed in bytes)

Device	Available	Sens.	Eth	Saw	Comms.
UNO	32,256	2014	26,840	35,214	2202
EVERY	49,152	1956	27,428	35,735	3105
F303	65,536	3040	29,940	33,404	14,240
L031	32,768	6168	30,796	34,432	14,724
L452	524,288	3032	33,120	36,568	17,336
ESP32	1,310,720	1496	289,318	293,674	267,270

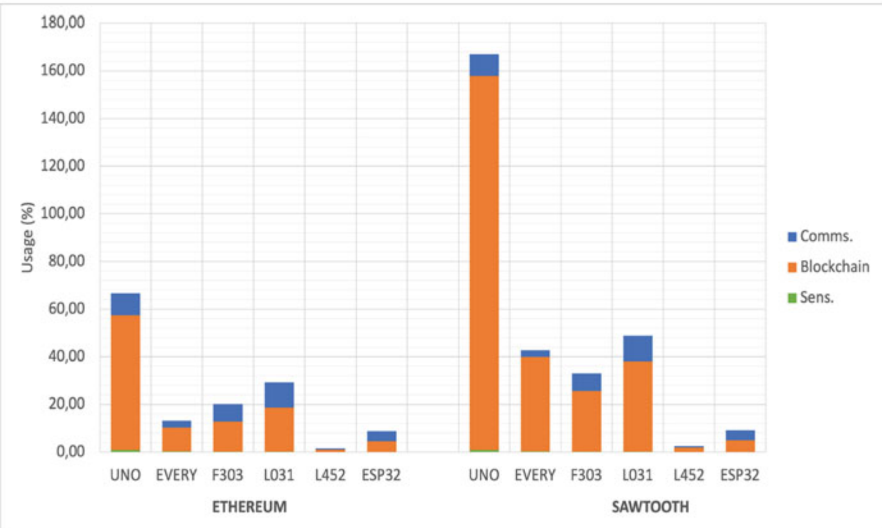
Table 3 Memory usage of the device module (expressed in bytes)

Device	Available	Sens.	Eth	Saw	Comms.
UNO	2048	207	1158	3214	188
EVERY	6144	196	611	2435	177
F303	12288	928	1540	3124	908
L031	8192	896	1508	3102	876
L452	163,840	936	1560	3144	916
ESP32	327,680	13,660	14,996	16,292	13,612

[1] https://www.qoitech.com/.



(a)



(b)

Fig. 6 Footprint of the device module in reference to the total available in each board. (**a**) Disk usage. (**b**) Memory usage

reference, we used an idle state for 5s before each working state (i.e., sensing, blockchain integration, and communications). It is important to notice that now low-power mode was used for the idle state. The average of all the experiments is depicted in Table 4 and Fig. 7a for the Ethereum implementation and in Table 5 and

Table 4 Power requirements (at 5v) during working and idle states on the device module with the Ethereum implementation

Device	State	Current (mA)	Current (var)	Energy (J)	Time (s)
UNO	Idle	34.38	2.85	0.86	5.01s
UNO	Work	34.36	2.37	0.73	4.26s
EVERY	Idle	29.46	0.17	0.73	4.98s
EVERY	Work	30.02	0.23	0.63	4.17s
F303	Idle	65.0	0.12	1.63	5.01s
F303	Work	67.93	1.0	0.08	0.23s
L031	Idle	47.43	0.0	1.18	4.98s
L031	Work	47.39	0.04	0.17	0.7s
L452	Idle	48.79	0.0	1.27	5.0s
L452	Work	50.15	0.08	0.04	0.16s
ESP32	Idle	42.26	0.03	1.06	5.0s
ESP32	Work	61.98	55.23	0.03	0.11s

Table 5 Power requirements (at 5v) during working and idle states on the device module with the Sawtooth implementation

Device	State	Current (mA)	Current (var)	Energy (J)	Time (s)
EVERY	Idle	29.4	0.44	0.73	4.98s
EVERY	Work	29.99	0.58	1.28	8.53s
F303	Idle	64.67	0.27	1.62	5.01s
F303	Work	67.86	1.76	0.2	0.58s
L452	Idle	51.87	0.0	1.35	5.0s
L452	Work	52.95	0.06	0.12	0.44s
ESP32	Idle	42.23	0.02	1.06	5.0s
ESP32	Work	59.93	43.35	0.09	0.31s

Fig. 7b for the Sawtooth implementation. As shown by the results, the processing times for creating a Sawtooth are longer and thus have higher power requirements on the IoT device.

6.3 Transaction Cost

We considered a price of ETH of 307 USD based on the year average price in 2020, as reported by Etherscan.[2] According to the information provided by the *Geth* client, we obtained the gas needed for each type of transaction in our architecture. In a public network, this gas translates into monetary cost by setting a gas price in reference to ETH typically using a $gwei$ where 1 $gwei = 0.000000001$ ETH.

[2] https://etherscan.io/chart/etherprice.

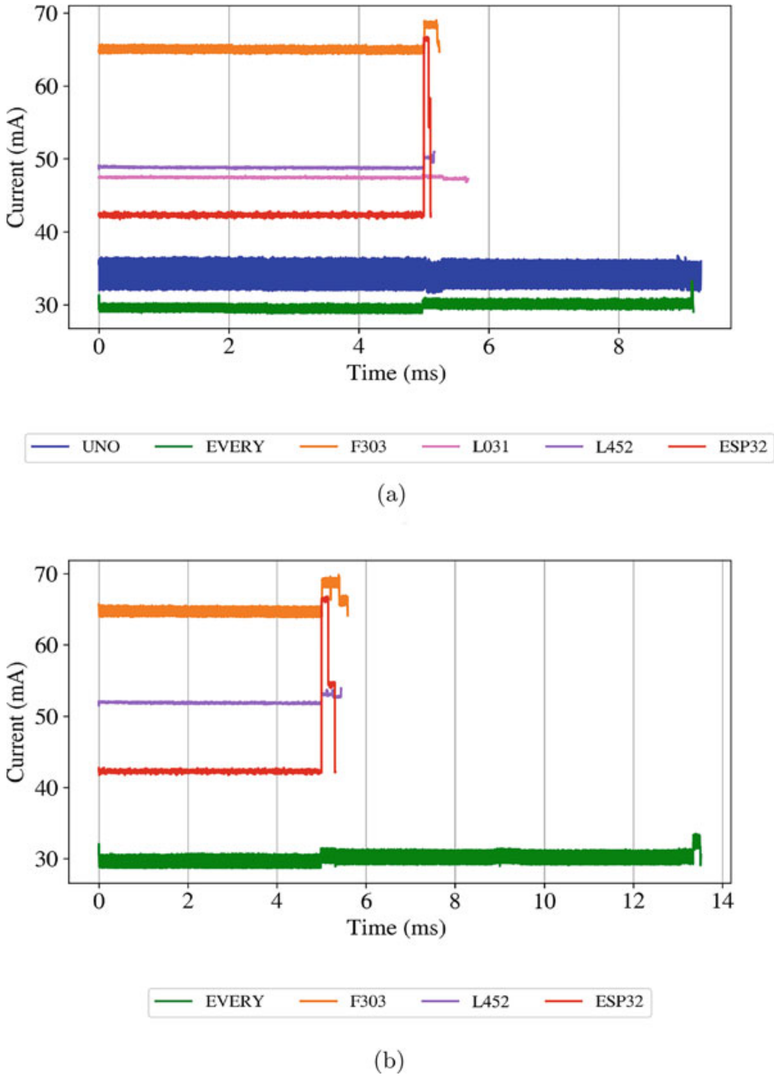


Fig. 7 Power consumption of the device module. (**a**) Ethereum implementation. (**b**) Sawtooth implementation

Higher *gas* values should translate into faster processing times; however, estimating the behavior of a blockchain network is a task beyond the scope of this work. Table 6 translates the gas of the four main transactions into USD using the average price and 3 different *gas* values. In contrast, Hyperledger Sawtooth, as most of private blockchain implementations, does not require the payment of a transaction fee. As we can see in the results, costs of the application on a public network range from a few cents to less than 8 USD.

Table 6 Transaction cost with 1 Ether equal to 307 USD

Transaction	Gas	80 gwei	100 gwei	120 gwei
Create TwinApp	2.071.380	5.09 USD	6.36 USD	7.36 USD
Create SmartTwin	988.000	2.43 USD	3.03 USD	3.64 USD
setValue() on SmartTwin	107.284	0.26 USD	0.33 USD	0.40 USD
queryTwin() on TwinApp	143.947	0.35 USD	0.44 USD	0.53 USD

6.4 Transaction Processing Times

We evaluated the real transaction processing time for executing the `setValue` operation on a SmartTwin contract. We tested this operation, as it is the most frequent transaction in the architecture. We sent one transaction approximately each 30 min over a period of one week on two different networks, namely Ropsten and Goerli. Table 7 shows the processing time for each network, and Figure 8 shows the frequency distributions of these times. The average blockchain processing time was 39 s on the Ropsten and 15 on Goerli using different gas prices. In Sawtooth, the average processing time for the transaction was less than 1 s.

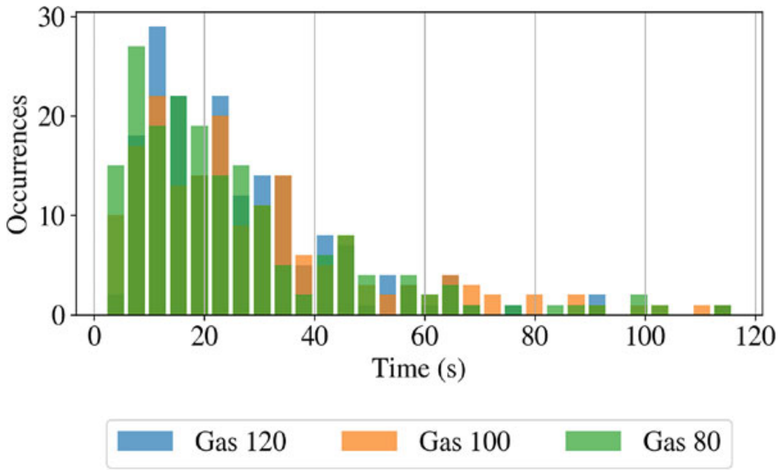
7 Conclusions

Our proposed architecture enables the integration of IoT and Blockchain technologies, creating transparent, fault tolerant, immutable, and auditable records that can be used for an Agri-Food traceability system. Regarding our practical evaluation: even if the Hyperledger Sawtooth-based implementation had better time response in terms of measured metrics with respect to the Ethereum one, both implementations have different properties and capabilities that need to be considered before choosing one over the other. In some cases, it may be convenient to trade off the high latency of Ethereum with its scalability and reliability, since it enables larger numbers of participants and its software maturity is far higher than Hyperledger Sawtooth. Moreover, from an economic perspective, recall that the monetary cost of using the Ethereum network can be avoided, simply by using private networks. From an application perspective, Ethereum imposes the limitation of having a single language for implementing smart contracts, as well as a fixed structure for the records, which may represent a drawback when developing more sophisticated business logic. However, Hyperledger Sawtooth is still far for being considered a mature implementation at the level of Ethereum.

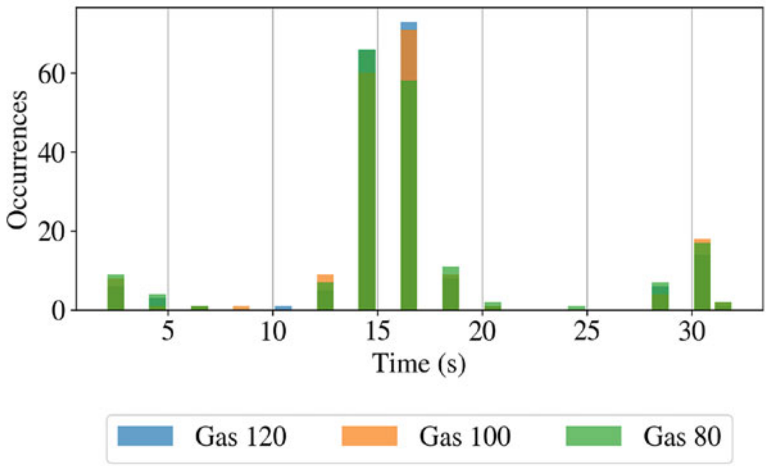
These differences are also noticeable when integrating constrained sensing devices. In our proposed architecture, constrained IoT devices are direct actors of a public blockchain network, directly feeding smart contracts without interposing third-party intermediaries. Using our prototype, we quantitatively assessed the impact both implementations have in terms of memory, program size, commu-

Table 7 Transaction processing times in terms of minimum, maximum, average, and variation on Ropsten and Goerli networks

	Ropsten network				Goerli network			
Gas price	Min	Max	Avg	Std	Min	Max	Avg	Std
80 gwei	04	116	25.05	21.21	02	32	16.26	6.49
100 gwei	02	116	26.16	17.87	02	32	16.30	6.11
120 gwei	02	487	39.45	56.62	02	32	16.09	5.69



(a)



(b)

Fig. 8 Processing times with different gas prices. (**a**) Ropsten network. (**b**) Goerli network nications, and power consumption at sensing node. Our results have shown that affordable, constrained devices can interact directly with the blockchain. A tiny 8-bit microcontroller, with only 32 KB of program space and 2KB of memory, can transform a sensed value into an Ethereum transaction. However, the program space used for these blockchain operations limits further functionalities on the board, such as more complex communications schemes. In contrast, creating a Sawtooth transaction requires more disk and space on the microcontroller, and less constrained devices are needed. Moreover, the processing time and thus the energy requirements of the devices are also higher than those needed by the Ethereum client.

Future works will revolve around the design and the development of the smart contracts supporting the entire proposition. Once the smart contracts are defined, we will evaluate our architecture from an economical point of view. In particular, we will assess the trade-off between transaction fees and processing time on public blockchains, also evaluating the cost of storing the sensed values in the blockchain. This will set the foundation for establishing realistic thresholds of the proposed architecture in a real-world deployment.

References

1. Accorsi, R., Bortolini, M., Baruffaldi, G., Pilati, F., & Ferrari, E. (2017). Internet-of-things paradigm in food supply chains control and management. *Procedia Manufacturing, 11*, 889–895.
2. Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2018). Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Communications Surveys Tutorials, 21*(2), 1676–1717.
3. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., et al. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50–58.
4. Biswas, A. R., & Giaffreda, R. (2014). Iot and cloud convergence: Opportunities and challenges. In *2014 IEEE World Forum on Internet of Things (WF-IoT)* (pp. 375–376). IEEE.
5. Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and Internet of Things: A survey. *Future Generation Computer Systems, 56*, 684–700.
6. Caro, M. P., Ali, M. S., Vecchio, M., & Giaffreda, R. (2018). Blockchain-based traceability in agri-food supply chain management: A practical implementation. In *2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany)* (pp. 1–4). IEEE.
7. Heiss, J., Eberhardt, & J., Tai, S. (2019). From oracles to trustworthy data on-chaining systems. In *Proc. of the IEEE International Conference on Blockchain*.
8. Kassahun, A., Hartog, R., Sadowski, T., Scholten, H., Bartram, T., Wolfert, S., & Beulens, A. (2014). Enabling chain-wide transparency in meat supply chains based on the EPCIS global standard and cloud-based services. *Computers and Electronics in Agriculture, 109*, 179–190.
9. Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In *Proc. of the CCGRID* (pp. 468–477).
10. Mao, D., Hao, Z., Wang, F., & Li, H. (2018). Innovative blockchain-based approach for sustainable and credible environment in food trade: A case study in Shandong province, China. *Sustainability, 10*(9), 3149.

11. Mao, D., Wang, F., Hao, Z., & Li, H. (2018). Credit evaluation system based on blockchain for multiple stakeholders in the food supply chain. *International Journal of Environmental Research and Public Health, 15*(8), 1627.
12. McFarlane, D., & Sheffi, Y. (2003). The impact of automatic identification on supply chain operations. *The International Journal of Logistics Management, 14*(1), 1–17.
13. Pincheira, M., & Vecchio, M. (2020). Towards trusted data on decentralized IoT applications: Integrating blockchain in constrained devices. In *2020 IEEE International Conference on Communications Workshops (ICC Workshops)* (pp. 1–6). https://doi.org/10.1109/ICCWorkshops49005.2020.9145328
14. Pincheira, M., Vecchio, M., Giaffreda, R., & Kanhere, S. S. (2021). Cost-effective IoT devices as trustworthy data sources for a blockchain-based water management system in precision agriculture. *Computers and Electronics in Agriculture, 180*, 105889.
15. Ramachandran, A., & Murat, K. (2017). Using blockchain and smart contracts for secure data provenance management. arXiv preprint arXiv:1709.10000.
16. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems, 88*, 173–190.
17. Salah, K., Nizamuddin, N., Jayaraman, R., & Omar, M. (2019). Blockchain-based soybean traceability in agricultural supply chain. *IEEE Access, 7*, 73295–73305. https://doi.org/10.1109/ACCESS.2019.2918000
18. Srinivasan, S., Shanthi, D., & Anand, A. (2017). Inventory transparency for agricultural produce through IoT. *IOP Conference Series: Materials Science and Engineering, 211*(1), 012009.
19. Sun, C. (2012). Application of RFID technology for logistics on Internet of Things. *AASRI Procedia, 1*, 106–111.
20. Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID and blockchain technology. In *Proc. of the ICSSSM* (pp. 1–6). IEEE.
21. Tian, F. (2017). A supply chain traceability system for food safety based on HACCP, blockchain and Internet of Things. In *Proc. of the ICSSSM* (pp. 1–6).
22. TongKe, F. (2013). Smart agriculture based on cloud computing and IoT. *Journal of Convergence Information Technology, 8*(2), 210–216.
23. Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials, 18*(3), 2084–2123.
24. Verdouw, C., Sundmaeker, H., Meyer, F., Wolfert, J., & Verhoosel, J. (2013). Smart agri-food logistics: requirements for the future internet. In *Dynamics in logistics* (pp. 247–257). Springer.
25. Verdouw, C. N., Wolfert, J., Beulens, A., & Rialland, A. (2016). Virtualization of food supply chains with the Internet of Things. *Journal of Food Engineering, 176*, 128–136.
26. Zanoni, B. (2014). Extra-virgin olive oil traceability. In *The extra-virgin olive oil handbook* (pp. 245–250).
27. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28*(3), 583–592.

Configuring Blockchain Architectures and Consensus Mechanisms: The Healthcare Supply Chain as a Use Case

Ghassan Al-Sumaidaee, Rami Alkhudary, Zeljko Zilic, and Pierre Féniès

1 Introduction

Blockchain technology brings to fruition extensive research on distributed ledger technologies, cryptography and consensus algorithms that had been conducted in computer science for decades [1]. Blockchain was presented for the first time in the white paper of Nakamoto [2]. This mysterious person or group of anonymous developers, we still do not know the real identity of Nakamoto, presented Bitcoin, the first application of blockchain. The most comprehensive and straightforward definition of blockchain can be formulated as a distributed ledger or database of non-erasable blocks of digital assets, information or transactions that are registered by following a precise consensus mechanism where there is no need for a central party to manage the network or maintain its integrity [2–5].

Blockchain applications and unique characteristics attracted wide attention in academia and industry [6–9]. Beyond the financial industry, blockchain can bring many benefits to operations, logistics and supply chain management, such as traceability [10, 11], transparency [12, 13] and security [14, 15]. Several organisations have already deployed blockchain to revolutionise their supply chain networks to improve service quality and ensure a better flow of the financial and physical flows [16–18].

However, the literature on blockchain in supply chains falls short to distinguish between different blockchain architectures. The most sophisticated literature sheds light on three blockchain systems: public, private and consortium [19, 20]. In these

G. Al-Sumaidaee (✉) · Z. Zilic
McGill University, Montreal, QC, Canada
e-mail: ghassan.al-sumaidaee@mail.mcgill.ca

R. Alkhudary · P. Féniès
LARGEPA, Université Paris-Panthéon-Assas, Paris, France

A. Bouras et al. (eds.), *Blockchain Driven Supply Chains and Enterprise Information Systems*, https://doi.org/10.1007/978-3-030-96154-1_7

three systems, transactions are visible to all or some users (referred to as nodes). Also, any user can trace the registered information in real time. However, these systems differ according to access, consensus mechanisms and where data are recorded or stored.

Public blockchains are open networks with no restrictions on participation. Associated addresses publicly identify the network's users. Trust in this system is derived from cryptographic techniques to reach a consensus and validate transactions. Given Bitcoin as an example, the Proof of Work (PoW) algorithm is used as a consensus mechanism. Each user can have an identical copy of the transactions' hashes. Private blockchains extend the technology applications beyond the financial sector. Several organisations have incorporated blockchain's features into their scope of work, albeit with some modifications to suit their needs. Users are not allowed to join the private blockchain network freely. They must obtain permission from the organisation or group of organisations that control the network. Different consensus mechanisms are used in private blockchains, such as the Proof of Authority (PoA) algorithm. Consequently, there is no need for mining to validate transactions. Each entity can have the hash of the registered information. However, there is a need to have servers or use cloud services to stock the source of information. Consortium blockchains are very similar to the private blockchain, except that they have a small number of equally powerful nodes as validators.

This paper offers an insight to supply chains by explaining several consensus mechanisms of blockchain architectures. This is vital because the literature addresses blockchain in a very general way. We illustrate that blockchain systems are not limited to private, public and consortium. We demonstrate that a new supply chain configuration can emerge each time we change the consensus mechanism of blockchain. We focus on the healthcare supply chain, as it adds an extra layer of risk and complexity given its direct impact on patients and public health. In doing so, we outline some of the most state-of-the-art blockchain systems underpinned by the consensus algorithms that we present in this paper, namely, Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT).

The remainder of this paper is structured as follows: Sect. 2 outlines the methodology that we employed to collect and analyze the pertinent literature. Section 3 elaborates on the reported consensus mechanisms and their applications in the healthcare supply chain. Finally, Sect. 4 concludes and provides future research directions.

2 Methodology Used to Collect the Literature

We conducted a systematic literature review (SLR) to collect the pertinent literature on blockchain technology in operations and supply chain management [21–24]. This is to articulate the most well-known consensus mechanisms used today to reach a consensus within blockchain systems and outline their applications in the healthcare industry.

We used two academic search engines: Scopus and Business Source Ultimate. Then, the following search string was employed: (blockchain OR blockchains OR "block chain") AND (Health OR Healthcare OR EHealth OR Medical OR Telemedicine). To control quality [25, 26], we limited the review to English language journals classified in Thomson Reuters (listing of 2018). The search was conducted in October 2020, producing 277 academic papers. The authors' read each paper title, abstract and more text needed to include the review only papers that proposed healthcare supply chain systems underpinned by blockchain. This procedure minimised the number of articles to 66 articles. This number is consistent with academic reviews published in peer-reviewed journals [9, 27, 28].

3 Blockchain Architectures and Consensus Mechanisms

This section presents the most known consensus algorithms deployed today to reach a consensus within blockchain systems. We introduce the PoW, PoS, DPoS, PoA and PBFT (see Table 1). We focus on the healthcare supply chain, one of the most appealing industries to use blockchain, to outline some of the most state-of-the-art blockchain systems.

3.1 Proof of Work

Proof of Work (PoW) is the best-known consensus algorithm used in most cryptocurrencies in circulation today. It was mainly developed to solve the problem of double-spending in the literature of computer science. This problem represents fraudulent behaviour that includes spending the same coin multiple times on the Internet. PoW allows users (any node within the blockchain system) to validate and register transactions on the blockchain ledger [19, 29].

Table 1 Consensus mechanism attributes

Consensus mechanism	Power consumption	Centralisation level	Blockchain system	Healthcare adoption	References
PoW	High	Low	Public	Low	[29, 55–57]
PoS	Low	Moderate	Public	Low	[38, 58–60]
DPoS	Low	Moderate	Public	Low	[56, 61–63]
PoA	Low	High	Private/consortium	High	[29, 38, 55, 61]
PBFT	Low	Moderate	Private/consortium	High	[58, 63–65]

This is done through mining, where all nodes on the network use specific machines with considerable computation power to solve a challenging puzzle [30]. Through mining, the validating nodes must find an arbitrary number called a “nonce”. The time to find the new hash (every 10 minutes on average on the Bitcoin network) is controlled by the difficulty level adjusted by the network’s protocol [31]. The validating nodes or miners are rewarded when they successfully verify a group of transactions (a block) and register it on the blockchain ledger.

Yazdinejad et al. [32] proposed a blockchain architecture underpinned by the PoW algorithm for a decentralised hospital network. The new system connects the hospital’s Internet of things (IoT) devices through a peer-to-peer network. The designed system limits the mining process only to nursing stations to reduce the computational power required. Nursing stations are particular nodes authorised to validate and register medical information according to predefined conditions with the help of remote monitoring devices.

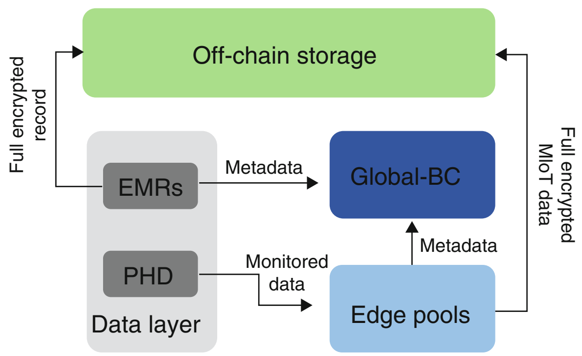
In the same vein, Akkaoui et al. [33] proposed a secure system, EdgeMediChain, for efficient health data management. Both blockchain and edge computing were combined to meet the healthcare supply chain needs. EdgeMediChain consists of four layers, all of which are decentralised and own independent computation power. The system was designed to achieve better performance and facilitate data sharing among the healthcare supply chain entities. Five virtual machines were implemented to test the system. The PoW algorithm was used in one of the virtual machines for global blockchain emulation. The initial results showed that the system accelerated and secured medical data exchange and gained higher throughput.

Figure 1 depicts the proposed model.

3.2 *Proof of Stake*

Proof of Stake (PoS) is another consensus algorithm introduced to reach a consensus within blockchain systems and solve the extensive energy consumption caused by PoW. The PoS algorithm selects nodes randomly with a high coinage to validate

Fig. 1 EdgeMediChain configuration [33]



and register new blocks of transactions on the blockchain ledger [34]. Miners are determined based on their coin share (stake-based system), where any node trying to cheat loses its entire stake (a considerable amount of coins). This ensures an acceptable level of security compared to PoW [35].

The PoS algorithm improves the blockchain network's effectiveness because the mining process is limited to a certain number of nodes. This considerably reduces the extensive energy consumption caused by PoW. In addition, PoS is much more efficient in addressing the scalability problem confronted with blockchain systems underpinned by PoW. The scalability problem is embedded in the limited capability to handle many transactions in a short time [34]. This is a real problem within public blockchains that use PoW.

Malamas et al. [36] proposed a blockchain system to ensure secure access to medical data between different healthcare supply chain entities. The authors claim that the proposed system offers several advantages for patients, doctors, technicians and insurance companies, including fast transaction processing and temporal access roles. In the designed system, the hash of medical data is stored on the blockchain ledger, while the primary data can be still stored on servers. The system was tested in two Ethereum-based blockchains, where PoS was used as the underlying consensus mechanism. PoS accelerated adding new blocks: 1000 transactions per second and a new block added every 12 seconds on average.

Similarly, Yang et al. [37] designed a medical data sharing system based on blockchain. As shown in Fig. 2, the developed system stores the encrypted medical data on the cloud, where the hash associated is stored on the blockchain ledger. This maintains the confidentiality and privacy of the medical data. The systems used the PoS algorithm and included several healthcare supply chain entities such as hospitals, cloud services providers, medical facilities, patients, etc. The authors advocated that the system achieved its objectives to secure data exchange and facilitate real-time communication among healthcare entities.

3.3 Delegated Proof of Stake

Delegated Proof of Stake (DPoS) is a modified version of the PoS algorithm, founded as another alternative to solve the extensive energy consumption caused by PoW. The DPoS algorithm has a different mechanism to reach a consensus within the blockchain system. More precisely, blocks are validated by particular nodes "witnesses" chosen by the other nodes in the network "voters". Voters authorise witnesses (validating nodes) to maintain the blockchain and add new blocks of transactions [38]. Both PoS and DPoS share the exact staking mechanism. In other words, nodes are asked to deposit some coins if they want to be involved in mining. Witnesses are replaced continuously over time. If previous witnesses wished to keep their roles, they should be recognised as honest nodes. This consensus mechanism supports the decentralised approach of blockchain systems more than the PoS

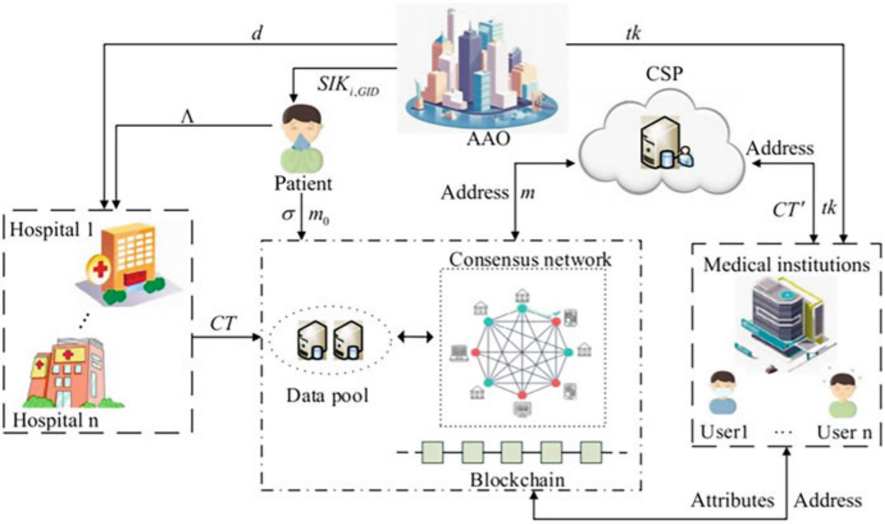


Fig. 2 Medical data sharing model [37]

algorithm, which is almost centralised, where dominant nodes with significant stakes could manipulate the mining process [39].

In contrast to the PoS mechanism, witnesses do not need to own a significant amount of stakes to be selected, as each vote is weighted according to its holder's stake [40]. However, the security level of a blockchain system underpinned by the DPoS algorithm is questioned with a small number of users. In other words, if there are only a small number of users, the entire network is threatened. This is because if 51% of the delegated nodes had agreed to be malicious, the whole network would be compromised.

Abdellatif et al. [41] presented a decentralised and secure healthcare supply chain based on blockchain and edge computing. The system aims to instantly share large amounts of secure medical data among the healthcare supply chain entities. The designed system is underpinned by DPoS and has many components (nodes) such as medical IoT devices that monitor and update patient health status information. Other nodes are allowed to conduct analysis and make sense of the data generated to be after that shared on the blockchain ledger. Official healthcare representatives could join the network and supervise its activities. The designed system entitles the healthcare stakeholders to access and trace all related information in real time.

In a similar vein, Wang et al. [42] proposed a smart healthcare supply chain based on blockchain, GuardHealth, to improve privacy and protect patient's personal information. The authors advocated that GuardHealth is the first system that introduced the graph neural network (GNN) to detect malicious nodes in the healthcare supply chain. The designed system uses the DPoS algorithm to leverage the chain's efficiency and security. The volume of health data represented the delegated stakes on the network. Each entity along the chain encrypts its data and

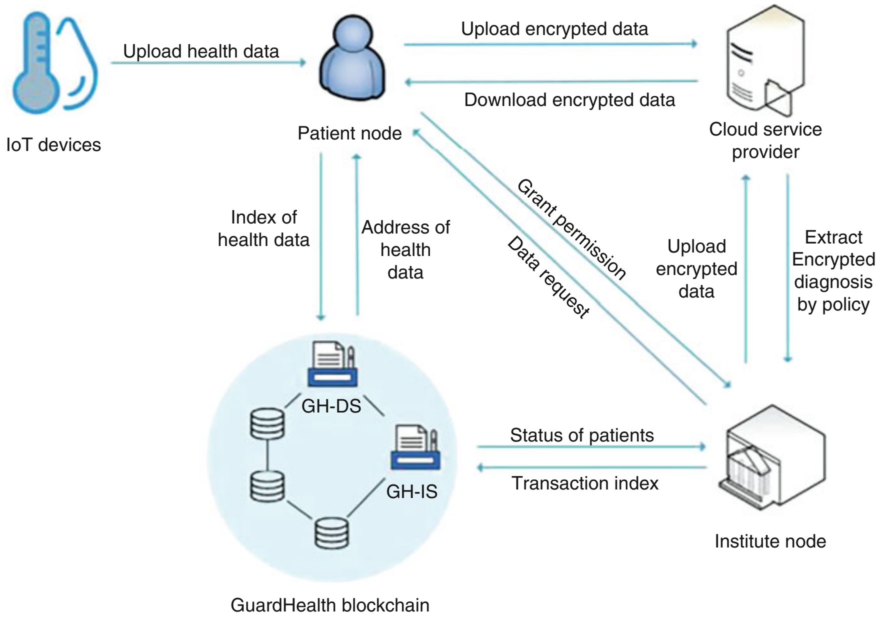


Fig. 3 GuardHealth model [42]

stores it on the cloud. Each entity can choose with whom to share the private key to decrypt the registered information. The system proposed double chains hosted on the cloud—one with the hash of the information and another with the original information. The GuardHealth model is illustrated in Fig. 3.

3.4 Proof of Authority

Proof of Authority (PoA) was introduced in March 2017 by Gavin Wood, the Ethereum co-founder, to solve spam attacks that severely affected the Ethereum Ropsten network [43]. The PoA algorithm is a reputation-based consensus mechanism. In other words, the nodes with a good reputation are considered trusted to add new blocks of transactions [44]. This mechanism is often used within private blockchain systems since users are known, and the validating nodes are limited to a certain number [45]. Some examples of industries where PoA could see successes are financial banking and supply chains. Regarding the healthcare supply chain, the validating nodes must be authentic. This is evident given the high level of data sensitivity which directly affects people's lives.

It would also be pointless for hospitals to build up extensive computational resources to mine new blocks [46]. This is what makes the PoA algorithm much appealing in this industry. The PoA algorithm allows trusted healthcare stakeholders (doctors, labs, administrators, etc.) to validate and add the medical data. This ensures secure and efficient management while allowing immediate access in case of an emergency. However, it is worth mentioning that PoA is relatively centralised because of the small number of validators who control the whole network.

Zhu et al. [47] introduced a consortium blockchain system using the open-source Ethereum blockchain. The system deployed the PoA algorithm to reach a consensus within the system. The system included three types of users: administrators represented by transactions' signers (validating nodes), service providers represented by medical stakeholders and official healthcare representatives. A case study of breast tumour classification with 100 patients was performed. The simulation proved the feasibility of the proposed system.

Lee et al. [48] developed a cross-country platform for personal health records (PHR). The platform was built based on blockchain to store, share and protect patients' sensitive data. It allows healthcare providers to upload and manage medical data. In the designed system, users can hash and encrypt medical data using the SHA-256 and Rivest-Shamir-Adleman algorithms. The authors argued that using the PoA algorithm as a consensus mechanism was efficient where information was registered much faster. Several Southeast Asian countries tested the system and proved its efficiency for sharing PHR (see Fig. 4).

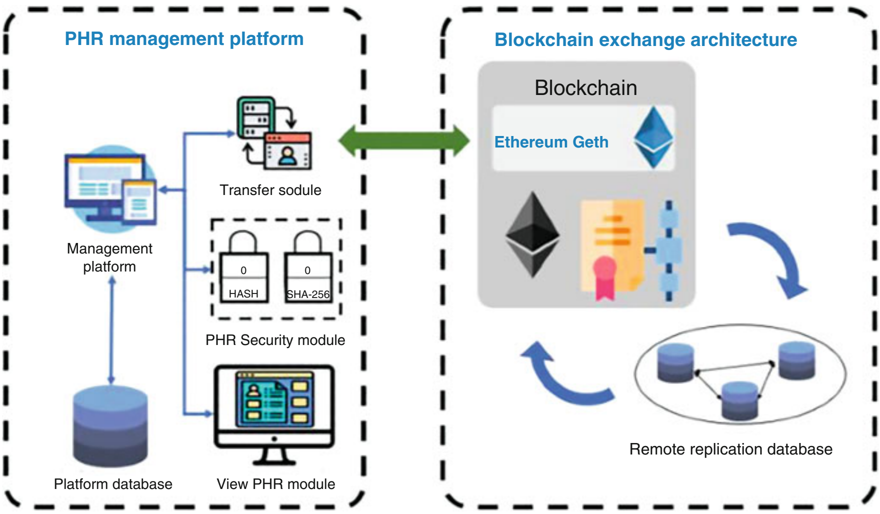


Fig. 4 PHR management platform [48]

3.5 Practical Byzantine Fault Tolerance

Practical Byzantine Fault Tolerance (PBFT) was introduced in 1999 by Miguel and Barbara [49] as a solution to several problems of the original Byzantine Fault Tolerance (BFT) systems [50]. The original BFT algorithm incurs high operational costs compared to other non-BFT systems, as it requires $3f + 1$ replicas to tolerate f fault replicas. If the network has some nodes equal to $3f + 1$, then the number of honest nodes must be greater than $2f + 1$, which means that the dishonest nodes should be less than f [51]. The PBFT algorithm is designed to work properly even if there are some dishonest nodes in the network. The PBFT algorithm is an excellent alternative to PoW and PoS because it does not require considerable computational resources or stakes to reach a consensus. PBFT is often used in consortium blockchain systems [52].

Here, we give an example to explain how PBFT reaches a consensus within a decentralised blockchain system. Suppose four nodes in the network: A, B, C and D. A is the primary node, while B, C and D are backup nodes. Assume that A, B and C are honest nodes, and D is the dishonest node. To start the process, a user creates a request and sends it to node A to forward the request to the backup nodes. If all the backup nodes accepted the message, they move to the prepare phase, and if not, they send a reject message back to the user. If the pre-prepared message is successfully received by more than $2f$ nodes, then the preparation phase is realised, and they will move to the next phase (commit phase). The commit information now will be broadcasted to other nodes. If more than 2f nodes successfully receive the commit message, the final consensus is achieved [50]. It is worth mentioning that there is a specific time for the primary node to send the request, and if it failed, this node is replaced.

Zghaibeh et al. [53] proposed a multilayer and smart health management system based on blockchain. The designed system was managed by three main groups: nodes, users and medical IoT devices. The nodes represent the government layer responsible for managing and controlling the blockchain model (centralised approach). Users are people who share their medical and personal data with the nodes. Finally, the medical IoT devices feed the blockchain ledger with real-time data regarding the patients' medical status. As a perfect fit for the system, PBFT was adopted as a consensus mechanism.

For another example, Pournaghi et al. [54] suggested a system, MedSBA, for a medical data record based on blockchain and attribute encryption algorithm. The attribute encryption algorithm allowed patients to control their medical records. Blockchain was used to guarantee that the data shared is reliable by following a precise consensus mechanism. As shown in Fig. 5, two blockchain systems were implemented: permissioned (private), where the original data is recorded, and permissionless (public), where the hash of data is registered. The designed system represents a typical healthcare supply chain with five entities. The first entity starts with hospitals and health insurance companies. The second is embedded in the cloud services that store the patients' encrypted data. The third is the blockchain

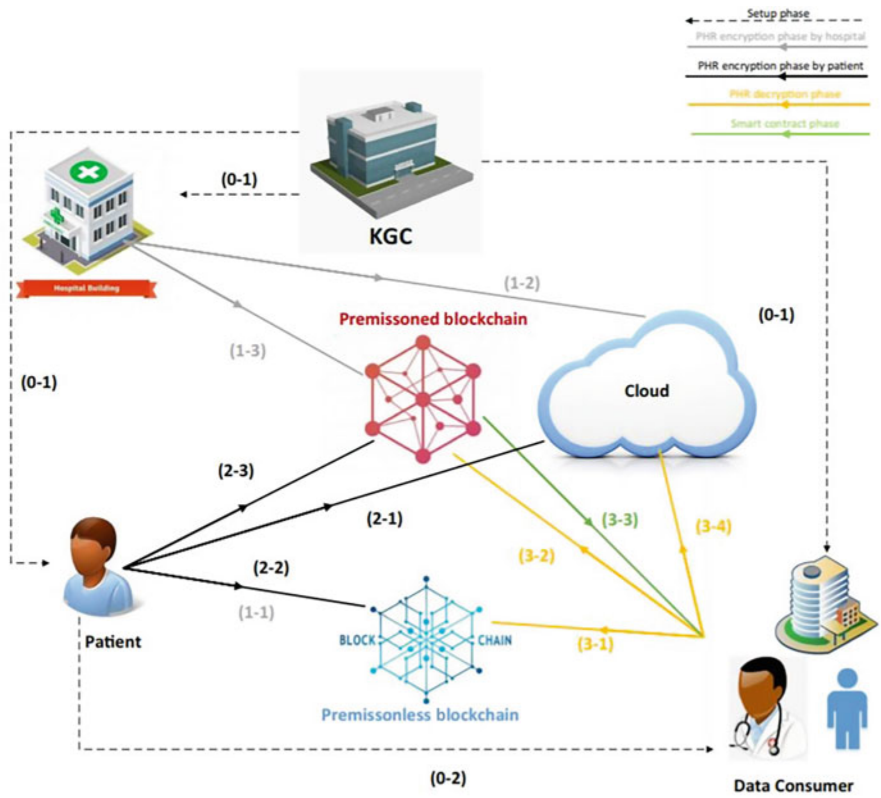


Fig. 5 MedSBA architecture [54]

architecture, including its double chains (private and public). The fourth is other stakeholders that benefit from the registered data. Stakeholders can be legal entities that represent official institutions or other healthcare services. The last entity represents patients that are responsible for their data. In other words, they decide to share their data by giving access to the original data, not merely access to the hash.

To conclude, Fig. 6 demonstrates the mechanisms of the consensus algorithms elaborated in this paper.

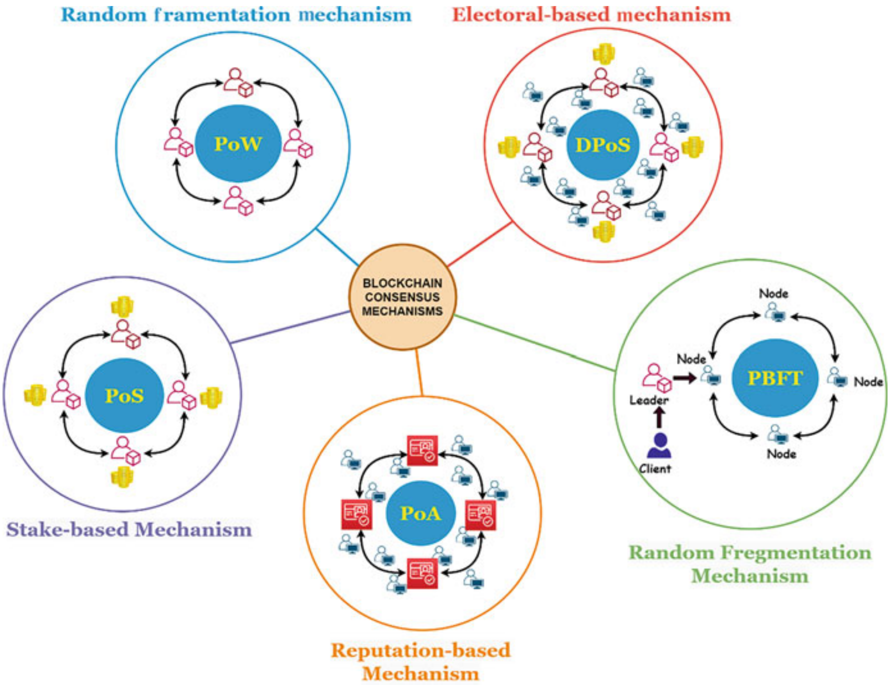


Fig. 6 Blockchain consensus mechanisms

4 Conclusions and Future Research Directions

Blockchain is a central technology that will revolutionise operations and supply chain management across different industries. It represents a paradigm shift towards fully decentralised supply chains. Since 2015, research focusing on using this cutting-edge technology is growing in all directions. The healthcare supply chain is not an exception. Several medical systems have been developed based on blockchain.

This paper presented the most well-known consensus algorithms (PoW, PoS, DPoS, PoA and PBFT) to reach a consensus within decentralised systems. We demonstrated that blockchain architectures and supply chain configurations could change radically each time we change the blockchain system's consensus mechanism. This is important as the literature on blockchain technology in operations and supply chain management falls short to distinguish between different blockchain architectures, let alone analysing the technology's benefits for each system. Additionally, we focused on the healthcare supply chain as a use case to outline the most state-of-the-art applications of the presented consensus mechanisms.

Here, we suggest some important research directions. Consensus algorithms, for example, are an essential element for reaching consensus within blockchain systems. Many consensus mechanisms were explored in this paper to shed more light on their usage in supply chain management. Although these consensus systems solve real problems and reach consensus within decentralised systems, they are far from perfect. They have several weaknesses that invite further research. For example, the PoS consensus algorithm is not free of defects. First, it sets the amount of stake that each validating node should own for the mining process. The problem is that these stakes are not amenable to trade or usage. In other words, if a node is willing to be a validating node, it must sacrifice its coins since these deposits became useless. Second, the PoS system is considered centralised as the validating nodes with a considerable stake are probably chosen for mining. Over time, these nodes could have more influence over the entire network. This contradicts one of the most basic principles of blockchain, being entirely decentralised. Third, although malicious actions executed by the validating nodes make them lose their coins' deposit, there is no mechanism to rule out or feasibly verify the activities of the validating nodes in the network. In a similar vein regarding the PBFT consensus algorithm, it is challenging for the validating nodes to join or leave the blockchain system quickly. The PBFT mechanism restricts the activities of the validating nodes to guarantee a stable and confident environment [66]. These issues solicit further investigation.

References

1. Alkhudary, R., Brusset, X., & Fenies, P. (2020). Blockchain in general management and economics: A systematic literature review. *EBR., 32*, 765–783. https://doi.org/10.1108/EBR-11-2019-0297
2. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf
3. Alkhudary, R. (2020). Blockchain technology between Nakamoto and supply chain management: Insights from academia and practice. *SSRN Journal*. https://doi.org/10.2139/ssrn.3660342
4. Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41*, 1027–1038. https://doi.org/10.1016/j.telpol.2017.09.003
5. Queiroz, M. M., & Fosso Wamba, S. (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. https://doi.org/10.1016/j.ijinfomgt.2018.11.021
6. Cai, Y., Choi, T., & Zhang, J. (2020). Platform supported supply chain operations in the blockchain Era: Supply contracting and moral hazards*. *Decision Sciences, deci.12475*. https://doi.org/10.1111/deci.12475
7. Hald, K. S., & Kinra, A. (2019). How the blockchain enables and constrains supply chain performance. *IJPDLM, 49*, 376–397. https://doi.org/10.1108/IJPDLM-02-2019-0063
8. Kamble, S., Gunasekaran, A., & Arha, H. (2019). Understanding the blockchain technology adoption in supply chains-Indian context. *International Journal of Production Research, 57*, 2009–2033. https://doi.org/10.1080/00207543.2018.1518610
9. Queiroz, M. M., Telles, R., & Bonilla, S. H. (2019). Blockchain and supply chain management integration: A systematic review of the literature. *SCM, 25*, 241–254. https://doi.org/10.1108/SCM-03-2018-0143

10. Agrawal, T. K., Sharma, A., & Kumar, V. (2018). Blockchain-based secured traceability system for textile and clothing supply chain. In S. Thomassey & X. Zeng (Eds.), *Artificial intelligence for fashion industry in the big data era* (pp. 197–208). Springer Singapore.
11. Behnke, K., & Janssen, M. F. W. H. A. (2020). Boundary conditions for traceability in food supply chains using blockchain technology. *International Journal of Information Management, 52*, 101969. https://doi.org/10.1016/j.ijinfomgt.2019.05.025
12. Sander, F., Semeijn, J., & Mahr, D. (2018). The acceptance of blockchain technology in meat traceability and transparency. *British Food Journal, 120*, 2066–2079. https://doi.org/10.1108/BFJ-07-2017-0365
13. 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*, 4378–4396. https://doi.org/10.1287/mnsc.2019.3434
14. Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management, 39*, 80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005
15. Wang, R., Liu, H., Wang, H., Yang, Q., & Wu, D. (2019). Distributed security architecture based on blockchain for connected health: Architecture, challenges, and approaches. *IEEE Wireless Communications, 26*, 30–36. https://doi.org/10.1109/MWC.001.1900108
16. Chang, S. E., Chen, Y.-C., & Lu, M.-F. (2019). Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. *Technological Forecasting and Social Change, 144*, 1–11. https://doi.org/10.1016/j.techfore.2019.03.015
17. Lacity, M. (2018). Addressing key challenges to making enterprise blockchain applications a reality. *MIS Quarterly Executive., 17*.
18. Lu, Q., & Xu, X. (2017). Adaptable blockchain-based systems: A case study for product traceability. *IEEE Software, 34*, 21–27. https://doi.org/10.1109/MS.2017.4121227
19. O'Leary, D. E. (2017). Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems. *Intelligent Systems in Accounting, Finance and Management, 24*, 138–147. https://doi.org/10.1002/isaf.1417
20. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData Congress)* (pp. 557–564). IEEE.
21. Durach, C. F., Kembro, J., & Wieland, A. (2017). A new paradigm for systematic literature reviews in supply chain management. *Journal of Supply Chain Management, 53*, 67–85. https://doi.org/10.1111/jscm.12145
22. Thomé, A. M. T., Scavarda, L. F., & Scavarda, A. J. (2016). Conducting systematic literature review in operations management. *Production Planning & Control, 27*, 408–420. https://doi.org/10.1080/09537287.2015.1129464
23. Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management, 14*, 207–222. https://doi.org/10.1111/1467-8551.00375
24. Webster, J., & Watson, R. T. (2002). Analysing the past to prepare for the future: writing a literature review. *MIS Quarterly, 26*, xiii–xxiii. https://doi.org/10.2307/4132319
25. vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., & Cleven, A. (2015). Standing on the shoulders of giants: challenges and recommendations of literature search in information systems research. *CAIS, 37*. https://doi.org/10.17705/1CAIS.03709
26. Okoli, C. (2015). A guide to conducting a standalone systematic literature review. *CAIS, 37*. https://doi.org/10.17705/1CAIS.03743
27. Alkhudary, R., & Gardiner, P. (2021). Stages in project managers' careers: Learning and growth opportunities. *International Journal of Project Management*. https://doi.org/10.1016/j.ijproman.2021.03.006
28. Mysen, T. (2013). Towards a framework for controls as determinants of export performance: A review and analysis of empirical literature 1995-2011. *European Business Review, 25*, 224–242. https://doi.org/10.1108/09555341311314807

29. Monrat, A. A., Schelen, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access, 7*, 117134–117151. https://doi.org/10.1109/ACCESS.2019.2936094
30. Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., & Danezis, G. (2019). SoK: Consensus in the age of blockchains. In *Proceedings of the 1st ACM conference on advances in financial technologies* (pp. 183–198). ACM.
31. Bozic, N., Pujolle, G., & Secci, S. (2016). A tutorial on blockchain and applications to secure network control-planes. In *2016 3rd Smart Cloud Networks & Systems (SCNS)* (pp. 1–8). IEEE.
32. Yazdinejad, A., Srivastava, G., Parizi, R. M., Dehghantanha, A., Choo, K.-K. R., & Aledhari, M. (2020). Decentralised authentication of distributed patients in hospital networks using blockchain. *IEEE Journal of Biomedical and Health Informatics, 24*, 2146–2156. https://doi.org/10.1109/JBHI.2020.2969648
33. Akkaoui, R., Hei, X., & Cheng, W. (2020). EdgeMediChain: A hybrid edge blockchain-based framework for health data exchange. *IEEE Access., 8*, 113467–113486. https://doi.org/10.1109/ACCESS.2020.3003575
34. Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals. *Applications and Opportunities. IEEE Access., 7*, 85727–85745. https://doi.org/10.1109/ACCESS.2019.2925010
35. Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017). A review on consensus algorithm of blockchain. In *2017 IEEE international conference on systems, man, and cybernetics (SMC)* (pp. 2567–2572). IEEE.
36. Malamas, V., Kotzanikolaou, P., Dasaklis, T. K., & Burmester, M. (2020). A hierarchical multi blockchain for fine grained access to medical data. *IEEE Access., 8*, 134393–134412. https://doi.org/10.1109/ACCESS.2020.3011201
37. Yang, X., Li, T., Pei, X., Wen, L., & Wang, C. (2020). Medical data sharing scheme based on attribute cryptosystem and blockchain technology. *IEEE Access., 8*, 45468–45476. https://doi.org/10.1109/ACCESS.2020.2976894
38. He, Q., Guan, N., Lv, M., & Yi, W. (2018). On the consensus mechanisms of blockchain/DLT for internet of things. In *2018 IEEE 13th international symposium on industrial embedded systems (SIES)* (pp. 1–10). IEEE.
39. Yadav, A. K., & Singh, K. (2020). Comparative analysis of consensus algorithms of blockchain technology. In Y.-C. Hu, S. Tiwari, M. C. Trivedi, & K. K. Mishra (Eds.), *Ambient communications and computer systems* (pp. 205–218). Springer Singapore.
40. Carrara, G. R., Burle, L. M., Medeiros, D. S. V., de Albuquerque, C. V. N., & Mattos, D. M. F. (2020). Consistency, availability, and partition tolerance in blockchain: A survey on the consensus mechanism over peer-to-peer networking. *Annales des Telecommunications, 75*, 163–174. https://doi.org/10.1007/s12243-020-00751-w
41. Abdellatif, A. A., Al-Marridi, A. Z., Mohamed, A., Erbad, A., Chiasserini, C. F., & Refaey, A. (2020). ssHealth: Toward secure, blockchain-enabled healthcare systems. *IEEE Network, 34*, 312–319. https://doi.org/10.1109/MNET.011.1900553
42. Wang, Z., Luo, N., & Zhou, P. (2020). GuardHealth: Blockchain empowered secure data management and Graph Convolutional Network enabled anomaly detection in smart healthcare. *Journal of Parallel and Distributed Computing, 142*, 1–12. https://doi.org/10.1016/j.jpdc.2020.03.004
43. Curran, B. (2018). *What is proof of authority consensus? Staking your identity on the blockchain*. https://blockonomi.com/proof-of-authority/
44. Cong An, A., Thi Xuan Diem, P., Thi Thu Lan, L., Van Toi, T., & Duong Quoc Binh, L. (2019). Building a product origins tracking system based on blockchain and PoA consensus protocol. In *2019 international conference on advanced computing and applications (ACOMP)* (pp. 27–33). IEEE.

45. Singh, P. K., Singh, R., Nandi, S. K., & Nandi, S. (2019). Managing Smart home appliances with proof of authority and blockchain. In K.-H. Lüke, G. Eichler, C. Erfurth, & G. Fahrnberger (Eds.), *Innovations for community services* (pp. 221–232). Springer International Publishing.
46. Hölbl, M., Kompara, M., Kamišalić, A., & Nemec Zlatolas, L. (2018). A systematic review of the use of blockchain in healthcare. *Symmetry., 10*, 470. https://doi.org/10.3390/sym10100470
47. Zhu, X., Shi, J., & Lu, C. (2019). Cloud health resource sharing based on consensus-oriented blockchain technology: Case study on a breast tumor diagnosis service. *Journal of Medical Internet Research, 21*, e13767. https://doi.org/10.2196/13767
48. Lee, H.-A., Kung, H.-H., Udayasankaran, J. G., Kijsanayotin, B. B., Marcelo, A., Chao, L. R., & Hsu, C.-Y. (2020). An architecture and management platform for blockchain-based personal health record exchange: Development and usability study. *Journal of Medical Internet Research, 22*, e16748. https://doi.org/10.2196/16748
49. Miguel, C., & Barbara, L. (1999). *Practical byzantine fault tolerance*.
50. Wu, Y., Song, P., & Wang, F. (2020). Hybrid consensus algorithm optimization: A mathematical method based on POS and PBFT and its application in blockchain. *Mathematical Problems in Engineering, 2020*, 1–13. https://doi.org/10.1155/2020/7270624
51. Zhang, L., & Li, Q. (2018). Research on consensus efficiency based on practical byzantine fault tolerance. In *2018 10th international conference on modelling, identification and control (ICMIC)* (pp. 1–6). IEEE.
52. Zheng, X., & Feng, W. (2021). Research on practical byzantine fault tolerant consensus algorithm based on blockchain. *Journal of Physics: Conference Series, 1802*, 032022. https://doi.org/10.1088/1742-6596/1802/3/032022
53. Zghaibeh, M., Farooq, U., Hasan, N. U., & Baig, I. (2020). SHealth: A blockchain-based health system with smart contracts capabilities. *IEEE Access, 8*, 70030–70043. https://doi.org/10.1109/ACCESS.2020.2986789
54. Pournaghi, S. M., Bayat, M., & Farjami, Y. (2020). MedSBA: A novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption. *Journal of Ambient Intelligence Humanized Computing, 11*, 4613–4641. https://doi.org/10.1007/s12652-020-01710-y
55. Pandey, P., & Litoriya, R. (2020). Implementing healthcare services on a large scale: Challenges and remedies based on blockchain technology. *Health Policy and Technology, 9*, 69–78. https://doi.org/10.1016/j.hlpt.2020.01.004
56. Praveen, G., Anand, M., Singh, P. K., & Ranjan, P. (2021). An overview of blockchain consensus and vulnerability. In T. Senjyu, P. N. Mahalle, T. Perumal, & A. Joshi (Eds.), *Information and communication technology for intelligent systems* (pp. 459–468). Springer Singapore.
57. Kaur, S., Chaturvedi, S., Sharma, A., & Kar, J. (2021). A research survey on applications of consensus protocols in blockchain. *Security and Communication Networks, 2021*, 1–22. https://doi.org/10.1155/2021/6693731
58. Bodkhe, U., Mehta, D., Tanwar, S., Bhattacharya, P., Singh, P. K., & Hong, W.-C. (2020). A survey on decentralized consensus mechanisms for cyber physical systems. *IEEE Access, 8*, 54371–54401. https://doi.org/10.1109/ACCESS.2020.2981415
59. Kaur, M., Khan, M. Z., Gupta, S., Noorwali, A., Chakraborty, C., & Pani, S. K. (2021). MBCP: Performance analysis of large scale mainstream blockchain consensus protocols. *IEEE Access., 9*, 80931–80944. https://doi.org/10.1109/ACCESS.2021.3085187
60. Bamakan, S. M. H., Motavali, A., & Babaei Bondarti, A. (2020). A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications, 154*(113385). https://doi.org/10.1016/j.eswa.2020.113385
61. Azbeg, K., Ouchetto, O., Jai Andaloussi, S., & Fetjah, L. (2021). An overview of blockchain consensus algorithms: Comparison, challenges and future directions. In F. Saeed, T. Al-Hadhrami, F. Mohammed, & E. Mohammed (Eds.), *Advances on smart and soft computing* (pp. 357–369). Springer Singapore.
62. Wan, S., Li, M., Liu, G., & Wang, C. (2020). Recent advances in consensus protocols for blockchain: A survey. *Wireless Networks, 26*, 5579–5593. https://doi.org/10.1007/s11276-019-02195-0

63. Lao, L., Li, Z., Hou, S., Xiao, B., Guo, S., & Yang, Y. (2020). A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. *ACM Computing Surveys, 53*, 1–32. https://doi.org/10.1145/3372136
64. Khan, D., Jung, L. T., Ahmed Hashmani, M., & Waqas, A. (2020). A critical review of blockchain consensus model. In *2020 3rd international conference on computing, mathematics and engineering technologies (iCoMET)* (pp. 1–6). IEEE.
65. Alam Khan, F., Asif, M., Ahmad, A., Alharbi, M., & Aljuaid, H. (2020). Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustainable Cities and Society, 55*, 102018. https://doi.org/10.1016/j.scs.2020.102018
66. Tang, H., Sun, Y., & Ouyang, J. (2020). Excellent practical byzantine fault tolerance. *Journal of Cyber Security, 2*, 167–182. https://doi.org/10.32604/jcs.2020.011341

Blockchain-Based Supply Chain System in Automotive Industry for Small- and Medium-Sized Manufacturing

Yuqiuge Hao, Petri Helo, Nikolaos Tsoniotis, and Rayko Toshev

1 Introduction

With the rapid development of various technologies, the automotive market will be completely different from today. We expect more integrated, personalised, shared and connected cars in the automotive industry [3]. It is believed that the impact of blockchain in the automotive industry is so significant. Therefore, it is vital to be aware of the potential for this disruptive technology and understand how it changes the complex automotive industry.

Blockchain is known as a technology that supports bitcoin and other similar currencies but is also much more than that. In the automotive industry, using blockchain technology can transform products, services and processes. Heutger and Kuckelhaus [4] illustrate several interesting industrial examples of using blockchain technology to managing physical assets in the automotive and its manufacturing industry, for instance, Groupe Renault storing the digital assets of its vehicles on the blockchain, Microsoft and VISEO connecting maintenance events by blockchain and Bosch and local certification authority using blockchain to prevent illegal odometer manipulation [4]. Various cases demonstrate how automotive companies have moved fast to seize the potential of using. There is a lot of research addressing the usage and implementation of blockchain in the automotive industry [1]. From previous research and practical cases, three different use case categories of blockchain application in the automotive industry are summarised, namely, (1) verification and authentication for process improvements, (2) vehicle (assets)

Y. Hao (✉) · P. Helo · R. Toshev
University of Vaasa, School of Technology and Innovations, Vaasa, Finland

N. Tsoniotis
Ideas Forward P.C, Thessaloniki, Greece

A. Bouras et al. (eds.), *Blockchain Driven Supply Chains and Enterprise Information Systems*, https://doi.org/10.1007/978-3-030-96154-1_8

management in transfer and distribution and (3) transparent finance, payments and insurance to increase the security [1, 3, 8, 10].

Although blockchain has many advantages and brings many benefits to the automotive industry, different stakeholders in the industry confront other challenges [10]. It always lacks a clear roadmap when it comes to adopting blockchain. To the best of our knowledge, most researchers focused on the particular phase of the life cycle in the automotive industry. There is a need to design a complete framework to provide on-demand, customised blockchain-based services meeting all critical requirements for the automotive industry. Besides, more and more SMEs join the automotive industry to improve efficiency, optimise investments and processes and increase flexibility [21]. The automotive industry is not only for big players.

Small and medium enterprises (SMEs) have low product volumes and relatively a large number of partners. As a result, these limitations constitute bottleneck problems and restrict SMEs' access to different advanced technologies and business models [17], which, in turn, prevents them from quickly penetrating new markets. Based on Vatankhah Barenji et al. [17], it's crucial to provide a solution for SMEs to solve (1) centralisation management problem, (2) security and trust issues and (3) heterogeneous data challenges. Therefore, using emergent blockchain technology can solve the above barriers and provide a distributed solution for SMEs [19].

This study aims to study blockchain technology and its impact on the automotive industry and SMEs. Subsequently, we will examine the case for a blockchain-based supply chain and elaborate on implementing it in the automotive industry. This paper is based on an ongoing EU Horizon 2020 project AVANGARD (advanced manufacturing solutions tightly aligned with business needs), started in 2019. The project's goal is to design a concept of microfactory for the production of urban electric vehicles and addresses its associated challenges. This project aims to apply Industry 4.0 solutions and minimise the footprint of both the production and use phases of the vehicles. The whole manufacturing and supply chain process are digitalised. From an electronic device, the client will be able to configure the vehicle, make the purchase order and follow the vehicle manufacturing, assembly and delivery evolution. At the same time, the manufacturing system can receive the order and decide the most suitable microfactory of the system to manufacture this vehicle attending to location, workload, availability of goods and environmental impact.

To address our goal of this research, the rest of this paper is organised as follows: an overview of blockchain technology and analyses of blockchain technology's implications for the supply chain are provided in Sect. 2. Section 3 will present an in-depth analysis of using blockchain in a cloud-based automotive supply chain system. In Sect. 4, we will discuss blockchain's growth opportunities and challenges in the automotive industry and how companies can act to the changes. We will also conclude this research in this section.

2 Literature Review

In this section, literature related to the blockchain is discussed. The collected literature is analysed from four levels. The first level is about blockchain technology and its main characteristics. The second level is about its impact on supply chain management. The third level is its impact on the automotive industry, and the fourth level, progressive level, is its impact on SMEs. This will serve as a ground for designing a blockchain-based supply chain system for automotive industry.

2.1 Blockchain Technology and Its Impact on Supply Chain Management

Bitcoin is a hot topic nowadays in this digital currency era. However, the blockchain technology behind it could prove much more significant [6]. Blockchain is a digital, decentralised, distributed ledger technology that provides a way for information to be recorded, shared and maintained by a community. Here are three critical characteristics of blockchain:

- Transparent: The transactions are recorded near real time to the blockchain and also synchronised on multiple computer systems. At the same time, it is visible to all participants with identical copies maintained. This principle can remove disputes, reduce uncertainty and, at the same time, increase trustworthiness [3, 5, 12, 13].
- Decentralised: From the business point of view, it is a peer-to-peer network that is entirely organised and managed by its associated members, without relying on a single middle authority or unified infrastructure that built trust [7]. From the technical point of view, decentralisation indicates a design of distributed system structure to deal with the data processing from verification, storage, maintenance and transmission. In this structure, the trust between distributing nodes is built through mathematical methods rather than centralised organisations [5].
- Immutable: One or more transactions are grouped to form a new block. All members of the network can verify the transactions in the block. If no consensus on the validity of the new block is reached, the block is rejected. Likewise, if consensus exists that the transactions in the block are valid, the block is added to the chain [7]. It is nearly impossible to tamper information to a blockchain without been detected. Blockchain can increase the trustworthiness of data and decrease the chances of fraud [3].

From the time it was developed, blockchain has been described as an efficient and permanent ledger to record events, transactions and information. The various unique features of blockchain technology have seen it considered for applications in many areas to improve the scope of the business areas and operational performance, including commerce, judiciary, finance, banking, healthcare, military and defence, equity crowdfunding, securities issuance, trading and settlement, insurance, notary public, music industry, Internet of Things and other non-financial applications [2].

Today, blockchain is being deployed in many forms. Still, blockchain technology has the potential to open new business models. This is mainly related to the complete public trust that is a unique characteristic of this technology. According to Piscini et al. [31], blockchain technology is a gatekeeper in the emerging trust economy of different parties on the supply chain.

The blockchain can create value for the industry through three main points: (a) unlocking business efficiencies, (b) disintermediating suppliers and (c) enabling new business and customer offerings [9]. In logistics, blockchain technology introduced the digital distributed ledger for shipment management. Similarly, blockchain can be implemented in the supply chain with practical benefits, such as efficient, timely and transparent transactions [2].

According to the Council of Supply Chain Management Professionals (CSCMP), SCM is based on two fundamental approaches: (i) planning, implementing and controlling the primary activities and delivering value for the ultimate customers and (ii) the centralised management and coordination of corresponding business processes within as well as across the companies. Pain points of the supply chain are:

- Weak control by the core enterprise
- Lack of supervision and hard to trace and match
- Information isolation
- Lack of trust

The integration of the supply chain can be considered a force that is trying to uplift the relationships between all the segments in the supply chain to enable better decision-making by providing visibility and highlighting the bottlenecks. Blockchain for supply chain management is a digital innovation and emergent allowing technology. It offers distinctive features such as real-time information sharing, improved security, transparency, reliability, traceability and visibility which improve the efficiency of the supply chain.

2.2 Challenges and Opportunities of Blockchain in Automotive Industry

The industrial sector (including the automotive ones) is considered a primary target of blockchain technology. The first application of blockchain in the automotive industry is digital currency bitcoin and digital payments. However, same as in other industries, the main features of blockchain could be beneficial for applications more than digital currency and digital payment in the automotive industry. Since 2017, at the Frankfurt auto show, auto suppliers ZF and IBM announced they were jointly developing a blockchain-based vehicle services payment platform. Another example is a blockchain-based platform called “Dubbed Car eWallet”. It provides different services to change the vehicle business model more simply and securely, from the car-sharing pool, shopping in the car, dealership maintenance and payments processing. Furthermore, French carmaker Renault is also researching applications for blockchain technology. Blockchain is used to certify information about repair and maintenance when it is resold [30].

The automotive industry has its unique importance, considering its ranges from government regulatory parties, manufacturers, suppliers and vendors to spare parts suppliers [8], and covers many sectors across the entire supply chain from upstream to downstream. The automotive industry becomes a complex and wide-ranging ecosystem [8].

Some of the most typical applications of blockchain technologies are their use in the transfer of assets and digital applications and distributed information records created using smart contracts, considered an ideal way to program logical business and operations. It impacts all industry sectors, and it is not surprising that the automotive industry has also been influenced by this revolution [8].

The integration of the automotive industry and blockchain technology offers exciting solutions to some of the most pressing automotive problems, especially those related to the connected automotive industry. The power of this technology can drive innovation and solutions across the entire automotive ecosystem. To this day, there have been made several efforts to use blockchain for improving the automotive industry. This study identifies various automotive critical functional areas that can be leveraged using blockchain technology and their growth potential.

It is well noticed that blockchain technology is becoming more vital and crucial in the automotive industry. It influences the industry in the same way as other prominent technologies such as artificial intelligence, machine learning, 3D printing and IoT [29].

It has been widely realised that primary automotive industries have started to use blockchain technology in various scenarios over the last 2 years, such as vehicle supply chain, security, car service, autonomous vehicles, manufacturing process, insurance, etc. For example, General Motors (GM), Porsche, BMW have partnered with blockchain start-ups like XAIN, Spring Labs and VeChainThor to address complex issues (Table 1).

Moreover, SME companies are considered the backbone of most of the economies [32], and their survival is vital for a healthy economy. In Europe alone, there are approximately 21 million companies belonging to the SME sector. These 21 million companies provide a source of income for approximately 90 million people on the African continent. SMEs have to be strengthened to overcome the economic challenges surrounding them [20]. Despite their status as the essential part of any economy, SMEs find it difficult to:

- Find investors/finance
- Scale their operations
- Process payments
- Hire additional services

Table 1 Examples of blockchain applications in automotive industry

Key functional areas	Example	References
Smart manufacturing	Identification Blockchain can be used with digital twins, and can monitor and track digital asset information more effectively than traditional manufacturing. Through RFID tags, the authenticity of each material and asset can be verified. In addition, the blockchain can also protect data sharing between machines and prevent counterfeiting problems. This also helps to issue a safe and direct recall and improve quality control	Fraga-Lamas and Fernández-Caramés [10], Li et al. [14]
Supply chain and logistics monitoring	Visibility and traceability of supply chain and logistics. The automotive supply chain is considered to be very complex because it contains many types of assets, stakeholders and parties. A complete supply chain needs to manage the transfer of products and related transactions and the exchange of knowledge between organisations. Blockchain provides visibility, transparency and optimisation of logistics whilst providing seamless integration of transaction, payment and logistics information. For supply chain stakeholders, it is always clear to exchange knowledge and obtain constant details about who performs what, when and where	Kshetri [15], Saberi et al. [16], Sharma et al. [8], Stenholm et al. [24], Supranee and Rotchanakitumnuai [25]
Autonomous vehicles	Car-as-a-Service Blockchain technology contributes to the development of autonomous vehicles. Blockchain solutions can interconnect autonomous vehicles and realise car-sharing services. Data about autonomous vehicles will be exchanged in a safe, reliable and seamless manner. Blockchain can protect user privacy whilst protecting data security. In addition, the platform can process all payments after the trip, and update user records with the history of the trips performed	Sharma et al. [8], Fraga-Lamas and Fernández-Caramés [10], Singh and Kim [26], Pedrosa and Pau [27]
Aftersales services	Ownership transfer Blockchain technology increases the transparency of transactions and simplifies the process of car ownership changes. Buyers and sellers can execute goods transactions by using smart contracts without the need for an intermediary Automated services Most cars have error records. Once this information is shared on the blockchain, service professionals can easily access this information, diagnose problems quickly and repair the car in a shorter time. When the car needs maintenance, the service request can be triggered automatically. This will enable condition-based maintenance services. In addition, maintenance status can be easily tracked without visiting the mechanical station	Sund et al. [28], Sharma et al. [8]

(continued)

Table 1 (continued)

Key functional areas	Example	References
Insurance and security	Insurance Most insurance claims are fraudulent, and covert methods are used when issuing insurance policies and managing stocks, leading to increased operating costs and inefficiency. Blockchain solves this problem by implementing transparent recording of vehicle sensor data in a decentralised network. Blockchain provides new additional services for remote communication, providing insurance companies with driver location, driving duration, acceleration and braking behaviour, vehicle speed and other information. Blockchain can also incorporate insurance into other carriers, such as user files; this process can be called car sharing Security Vehicles are becoming more and more autonomous, which makes them more closely connected and more vulnerable to deadly cyberattacks. This is why the blockchain uses a robust encryption root that cannot be reverse engineered. The distributed ledger feature of the blockchain facilitates data storage and provides immutability	Sharma et al. [8], Fraga-Lamas and Fernández-Caramés [10]

With all the emerging technologies, SMEs must find ways to collaborate and share competency in a trustable manner to seize more business opportunities in a turbulent market environment. The new digitalisation trends and automation can form a significant challenge for SMEs [18]. In many current solutions and research, SMEs have encountered some bottleneck problems. Blockchain technology has been introduced recently for the manufacturing industry as peer-to-peer network which improves the system's security and where third party can be omitted [17].

3 Design of Blockchain-Based Supply Chain System for Automotive Industry

The automotive industry is one of the most promising applications of blockchain. In the previous section, we have evaluated the opportunities of using blockchain across the automotive industry to improve the supply chain. We also analysed the characteristics of blockchain in resolving business issues for SMEs. In this section, we will discuss the scenario in the electric vehicles sector.

Particularly in the electric vehicles (EVs) sector, the reality is that more and more SMEs are capable of developing EVs, and this will reshape the automotive value chain [11]. In most of the automotive industry, a centralised manufacturing model is a primary choice. Many giga-factories are operating in Europe, China and the USA. The current status of automotive factories consists of the production plant in which the final products are stored in the inventory (stock). Afterwards, the distributor collects a specific high volume for its region and each of the retailers' request from the distributor for the needs of the user/market. However, manufacturing plants across Europe seek into reduced wasted materials, energy consumptions and carbon footprint. Therefore, more and more SMEs are involved in manufacturer EVs locally based on local/regional needs. This manufacturing model only consists of modular production and the retailers in the broader region. Therefore, the supply chain is simplified and only consists of suppliers, regional factories, dealers and customers. Here in this demand-driven electric vehicles manufacturing, there are many use cases that need to be improved and verified through blockchain technology.

3.1 Functional Requirement

This paper is based on the ongoing EU Horizon 2020 project AVANGARD (advanced manufacturing solutions tightly aligned with business needs) started in 2019. The goal of the project is to design a concept of microfactory for the production of urban electric vehicles and address its associated challenges. This project aims to apply Industry 4.0 solutions and minimise the footprint of both the production and use phase of the vehicles. The whole manufacturing and supply chain process is digitalised. From an electronic device, the client will be able to configure the vehicle, make the purchase order and follow the evolution of the vehicle manufacturing, assembly and delivery. At the same time, the manufacturing system is able to receive the order and decide the most suitable microfactory of the system to manufacture this vehicle attending to location, work load, availability of goods and environmental impact.

Within this project, the blockchain technology is used to secure the whole process, and also to fulfil the track and trace functionalities of the supply chain and recording transactions amongst stakeholders and machines/software under its immutable and verifiable framework. The proposed blockchain component needs to be able to satisfy the following parameters:

- F1: Support the required decentralisation, which will ensure trust and immutability, whilst unconstructive facilitation of business level processes is guaranteed.
- F2: Record key transactional activities either organically recorded by value chain actors or programmatically sourced by key IoT devices and software components.
- F3: Facilitate granular access to key data points by participating actors based on defined stratification, supported by smart contract functionality.

According to the market demands, the following information needs to be secured by blockchain:

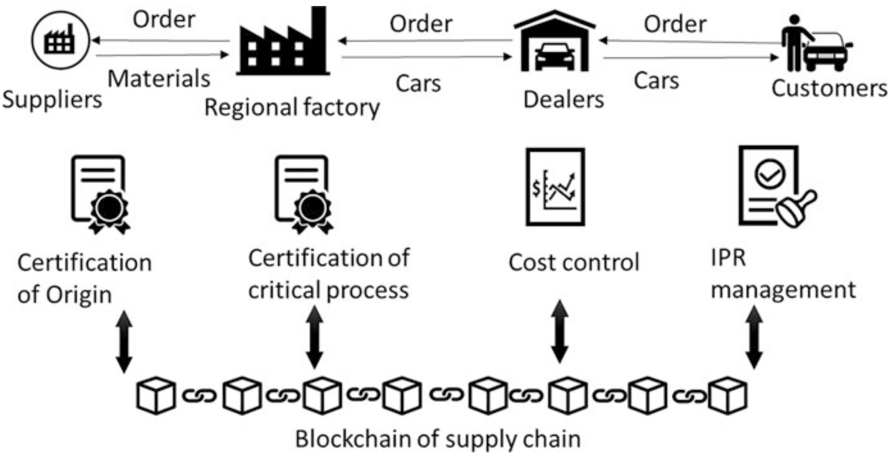


Fig. 1 A scenario of how blockchain technology can support certification and verification in regional demand-driven factory

- I1: Certification of origin – Customers who order the car will receive a certification of origin of all the materials which will be stored on a blockchain network. From suppliers to end consumer, the certifications are accessible and placed on a blockchain to be shared in a secure environment, i.e. made in Italy, Poland, Greece and Portugal.
- I2: Certification of critical process – Besides verifying virtual information of the product, it is also essential to warrant the physical movements of products in the supply chain.
- I3: Cost control – From extraction to end-of-life management and governing supply chain activities and its financial flow with smart contracts, for instance, in areas of financial transitions between participants in the entire ecosystem. For example, EV may use a windshield wiper which comes from a supplier, and to calculate the carbon footprint of whole car, the amount of carbon emission during the production should be shared by the supplier.
- I4: IPR management – Blockchain enabled IPR management system is secure, immutable and traceable. The provided IPR is easily checked by customers and any other participants in the supply chain. The IPR saved in blockchain can also be used when customers want to sell the electric car in the future (Fig. 1).

Based on the business requirements and information requirements, the basic functional requirements of designing a blockchain-based supply chain system in demand-driven electric vehicles factory are as follows (Table 2):

- Customer/user registration. Customers or other users from the participating stakeholders will have to be able to register to the system whilst creating their unique identity in the process. This will allow for logging activities under a unique identification schema.

Table 2 Functional requirements

Requirement driven from	Req ID	Functional requirements
F1,I1	REQ1	Track and trace: materials and products provided by all the suppliers
F2,I2	REQ2	Activity record: manufacturing process, such as processing craft, time, operators and other information
F2,I2	REQ3	Quality control: connect all the key information through IoT technologies, and trace the process and quality in the entire life cycle
F2,I3	REQ4	Sale-service: track the order and supply process, and provide flexible price plan to customers. Customer can reduce waiting time by increasing the price
F3,I4	REQ5	After-sales service: failing product tracing, to recall and maintain the products with quality problems, and record service information

- Stakeholder managed software/hardware registration. Manufacturing value chain stakeholders are expected to register their software (e.g. ERP, MES) or hardware (e.g. 3D printer, etc.) to the blockchain network. This will allow to attest ownership to participating actors, create a unique ID for the software/hardware components and facilitate logging of manufacturing processes, for example, information about production start and end time resulting from MES planning and execution, energy consumed resulting from IoT monitoring, material consumed, logging CO2 production data, etc.
- Customer order requests. The necessary rules and REST APIs will be coded to support the implementation of front-end elements in the web applications that allow the logging of a customer's order including metadata, hashing of design files, etc. This transaction and textual metadata will be logged, files will be hashed and all state changes along with the actual files will also be forwarded to the relevant external databases via the ledger-sync subscriber. In the case of a design, the file upload hash will be compared against prior uploads. If a match is found under a different ID, and not under a suitable Creative Commons license, then the customers will be warned of infringing IP rights. If there is no match, then they will be asked to indicate if they produced the design or not and choose a Creative Commons license. This can be further extrapolated in future iterations to support an open marketplace of designs.
- Quotation, acceptance and payment. The system and/or system users will propose a quote for the order, which will either be rejected or accepted, lead to an order adaptation or proceed with payment. All these transactions will be foreseen, coded in the Transaction Processors for handling and logging, supported by the required REST APIs and logged accordingly. The metadata will similarly be forwarded to the external database via the ledger-sync subscriber.
- With the various software and hardware components registered, the smart contract functionality of the Transaction Processors' code can log agreed upon

activities during the production process, from order finalisation to asset dispatched to the customer. This will be facilitated per case, logged in the blockchain as well as forwarded to the external databases. Furthermore, logged transactions could be accessed granularly by the participating stakeholders, creating a vehicle passport that holds the overall history of the produced vehicle, yet with subsets of metadata and transactional logs accessible depending on defined access rights. As such the blockchain component will facilitate admin roles that can manage access rights for registered users, and potentially system components. Thus, a vehicle passport is envisioned as a complete historical record, yet fostering restricted access based on user roles, thus not exposing sensitive manufacturing information but facilitating the expected transparency to customers and stakeholders alike.

3.2 Technical Architecture

To facilitate the functional requirement described in Sect. 3.1, a block-based supply chain system, namely, BSS, is proposed as an integrated solution to organise and manage all related activities and operations. This subsection will discuss the technical architecture of BSS.

In this BSS platform, it is possible that the system/user can audit and certify some processes and data across the entire supply chain of EV, from suppliers, manufacturer and dealers to customers. As blockchain is a vertical enabler, several functionalities can be facilitated and audited accordingly by employing blockchain-based user identities, transactional activity logging at various levels of abstractions depending on the business modelling of the final solution or the various components to be employed. Subsequently, blockchain logging and transactional activity can be deployed as either privately accessible by some or all of the manufacturing partners or publicly accessible by other stakeholders participating in the manufacturing value chains from collaborators to consumers.

The technical implementation framework of this proposed BSS depicted with a cross-layered structure in Fig. 2. The supply chain consists of suppliers, regional factories, dealers and customers. Therefore, the record for all the generated data whilst EV transfer between each party are store in the form of a distributed leger. In this framework, it consists of five main layers, from top to bottom, namely, user layer, application layer, cloud layer, blockchain services layer and storage layer:

- *User layer:* Different stakeholders in the manufacturing value chains, such as customers, dealers, shop floor operators, manufacturing managers and suppliers, have different access to the cloud and blockchain services. The manager is the head of the supply chain system and initiates system changes based on conditions set in the smart contract.

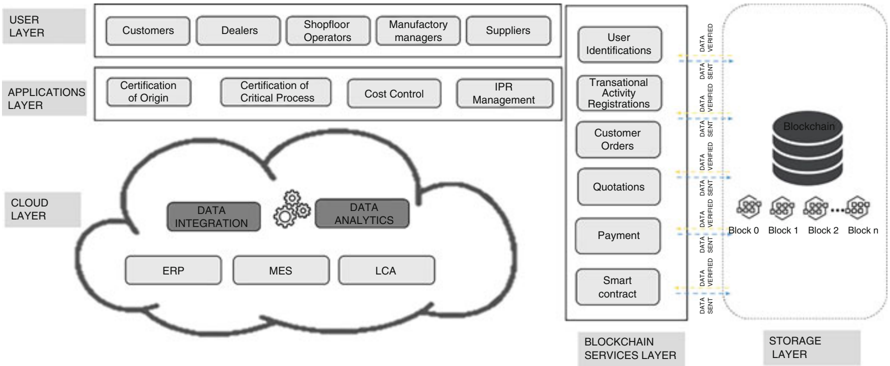


Fig. 2 Blockchain-based supply chain system (BSS) implementation framework

- *Application layer:* This layer defines various typical application scenarios and instances of blockchain-based supply chain. As described in Sect. 3.1, the blockchain can be applied to secure information: certification of origin, certification of critical process, cost control and IPR management.
- *Cloud layer:* The cloud layer is providing a cloud-based infrastructure to connect different tools, such as ERP, MES and LCA, and also integrate different data sets.
- *Blockchain services layer:* The blockchain services layer is responsible for synthesizing all related information from three other layers in vertical position. It consists of six components: user identifications, transactional activity registrations, customer orders, quotations, payment and smart contract.
- *Storage layer*: All the data blocks are generated in this layer. It is not only acting as a data storage but also operating encryption method, managing chain structure and adding timestamp to data block. The chain structure defines block header, block body and address.

3.3 Implementation

In this project, a hybrid blockchain is implemented in order to facilitate value chains of disparate partners, allow access to transactional data under a stratified model from completely private up to and including public access and support ease of integration with various setups such as software tools, IoT devices and stakeholders themselves, all the above without sacrificing decentralisation, immutability and eventually trust amongst participating actors.

By considering the overall technical architecture of BSS and comparing different blockchain framework, Hyperledger Sawtooth was chosen to support BSS. The reasons are as follows:

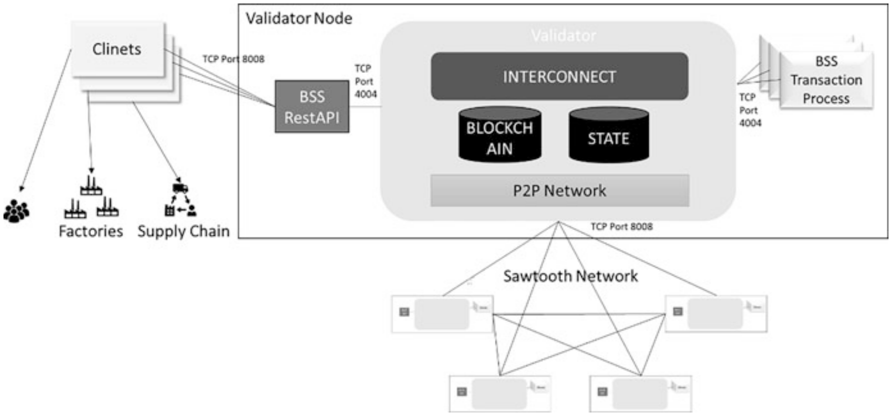


Fig. 3 Sawtooth Validator Node

- Sawtooth can be configured to support both private permission and public permissionless network configurations out of the box.
- Sawtooth's architecture is based on pluggable components that allow for flexibility and scalability.
- Sawtooth requires no transaction costs.

The Sawtooth blockchain node will be set up as per Fig. 3, with the Validator Nodes constructed as a multi-container Docker environment. A Docker within the frame of Sawtooth supports encapsulation, isolation, portability and control over the external communication of each Docker image, supporting scalability, efficient use of system resources, faster software delivery cycles and instant rollout. This approach is considered ideal for supporting the upcoming cloud services integration activities.

Each Validator Node will include the Validator, the Transaction Processors, the Consensus Engine and the required REST APIs and Clients. The *Clients* could interface with any system, software, device or any stakeholder interacting with BSS interfaces. The *BSS RestAPI* receives requests from the front-end implantation and facilities communication with the Validator. The *BSS Transaction Processor* holds application-specific code equivalent to smart contract functionality. Implementation will be undertaken in the Python programming language.

The multi-container Docker environment will clone the pilot implementation setup, based on the following configuration (Table 3):

3.4 Blockchain Demonstrator

This subsection presents a blockchain-based demonstrator for the proposed blockchain-based supply chain system (BSS). In the demonstration, we described a

Table 3 Blockchain component configuration

AWS cloud server – Sawtooth blockchain component	
Instance type	1 × EC2
Server type	Large
Storage	64 GB SSD
Processor	2 × vCPUs (Intel Xeon Processor, up to 3.0 GHz Intel Scalable Processor, each vCPU thread of an Intel Xeon core)
Memory	8 GB
Operating system	Ubuntu 18.04.5 LTS

use case of certificates exchange and data sharing with other partners by members of a manufacturing supply chain in the EV market. The implementation has to fulfil the following requirements:

- Allow members to create their own network of partners.
- Allow members to create, upload and manage a certificate with fixed and variable properties.
- Allow members to share the certificate with other members either a certificate or its metadata.
- All members can verify the authenticity of a certificate if it has been uploaded by a member of the supply chain.
- Allow members to handle custodianship and ownership separately taking under consideration one of the main complexities of any value chain.
- Support policies to facilitate transfer of custodianship and/or ownership to members of a partner network.
- Visualise at least one set of variable parameters and allow for manual update of their values.

Figures 4, 5, 6, and 7 present the screenshot of the dashboard of proposed BSS.

Figure 4 demonstrates the dashboard which holds an overview of Number of assets users' own across facilities and those that users don't own but are currently in users' facilities. Users can create asset categories, and check assets in transit, Sent/Received shipment requests, and also check number of partners in users' network. Other data are also included, along with a map for visualising the shipments in transit or already delivered.

Figure 5 demonstrates how to add a new partner. A partner can be either a colleague from user's company or a driver from a logistics company in the case of this demo. Colleagues can be co-owners of any assets that the user has, just by adding them to assets. To add a partner, user needs to know their Blockchain or Partner Key which acts as a unique identifier. By pressing Add, a request is sent to partners which they §can accept or decline. Conversely, user can delete it if it was sent by mistake. By pressing the eye icon, user can see more details about this partner.

Fig. 4 The main page of BSS

Figure 6 shows thee shipment routs. Once the shipment requests have been sent, user can go to Locations > Map and see shipments in Transit or Delivered. Upcoming features will include a filter to customise the time span user wants to check out. In Transit shipments are depicted in a dashed line. Delivered shipments are depicted with a solid line. Now that shipments are sent and delivered, user can go to Locations > Assets by location and monitor how many of user's assets are where. In this list, user can see how many of the common assets amongst user and partners are located to which location and how many of the assets users don't own but are currently in user's location.

Figure 7 depicts the transaction records. This is a blockchain-powered supply chain pilot system. All relevant transactions are logged in the blockchain and can be accessed by participants, as depicted in Fig. 7. Participants are restricted to access only those transactions that derive from their own network of partners. Measures are in place to avoid data spillovers between networks. Finally, as transactions increase in numbers, the user is facilitated to filter them for quick identification per:

- Transaction type
- Partner transactions
- Asset-oriented transactions

4 Discussions and Conclusions

Blockchain technology is a revolutionary innovation that can transform lots of existing traditional systems into more secure, distributed, transparent, collaborative systems whilst empowering its users. Blockchain-driven solutions can seamlessly aggregate all information, provide important services and add value to industrial

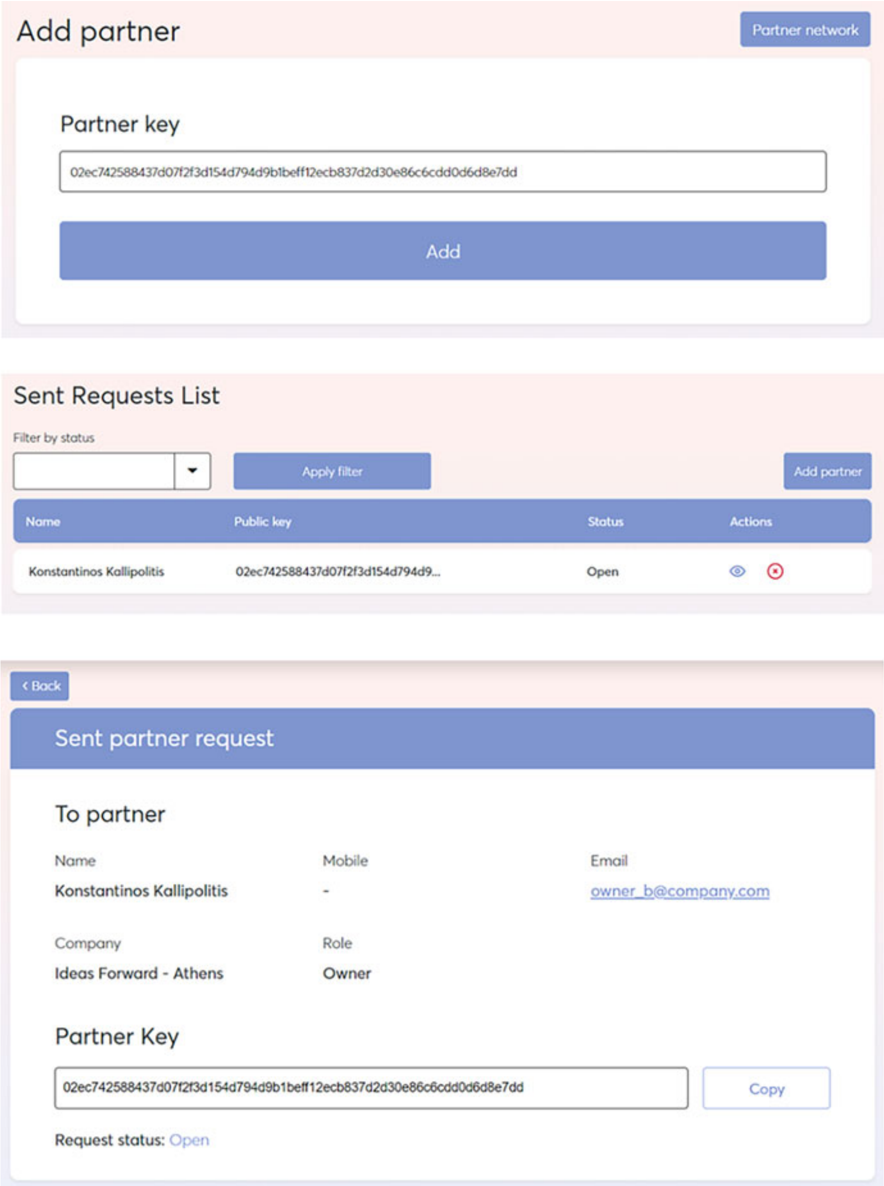


Fig. 5 Add new partner information pages

companies. The most important capability of blockchain is that it helps to unlock the full potential of other advent technologies, such as cloud, augmented reality, IoT and 3D printing. With the development and growth of maturity, blockchain technology will allow manufacturers to fully deploy other advanced technologies

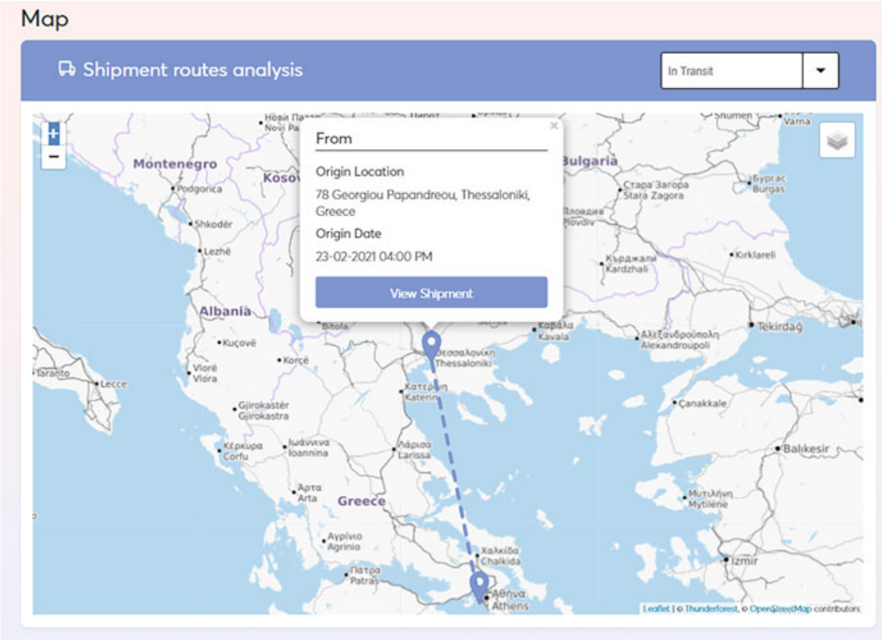


Fig. 6 The shipment routs analysis shown on map

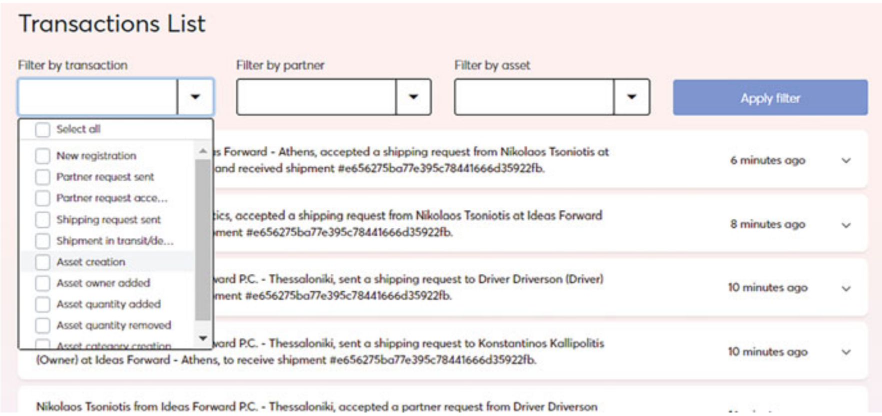


Fig. 7 The transaction is listed in the blockchain

and innovative business models. Therefore, more efficient factory operations that require data sharing and collaboration between complex companies and machine networks will be created and become the new norm for the entire industry [22].

This research demonstrates integration of blockchain and supply chain in automotive industry. In the future, the entire automotive industry could collaborate on a single trustable blockchain-based platform to store the information of every vehicle and related assets, including important events, transactions and status updates. This would allow, for example, certification of origin, IPR management and maintenance data to be stored together as a comprehensive record. However, the primary requirement to make the blockchain-enabled functionalities become a reality is the industry-wide collaboration [4].

In many previous research papers or practical cases, the examples of blockchain are being implemented in global international giants. However, when it comes to SMEs, they often tend to suffer from resource constraints in technology adoption [23]. Therefore, we proposed a blockchain-based architecture to support SMEs in the automotive industry, namely, blockchain-based supply chain system (BSS).

Firstly, this research paper demonstrates using blockchain to register transactional activities in the supply chain system. This data is fully traceable and visible to authorised parties such as the customers, dealers, shop floor operators, manufactory managers and suppliers. Manufacturing companies can provide a very useful and practical data management service to their customers. Secondly, this BSS aims to support the certification exchange amongst partners. Blockchain is used as an enabling technology to secure access and interactions and also to provide an immutable audit trail. Thirdly, For SMEs, there's a necessity to be effective. Blockchain can ensure trust between different parties to share and update data in an effective manner. According to our pilot implementation and demonstration, it is proved that blockchain technologies will build a trustful ecosystem for the automotive market.

Hereby, we summarise three main benefits of using blockchain in the automotive industry to manage the supply chain:

1. Improvement of business efficiencies: The record on blockchain will become a reference for future supplies and a source of learning and continuous improvement. This will improve the quality control and help in possible recall and maintenance.
2. Supporting business transparency: The end-users and every participant who are interested in early-stage materials can know the process. Registering materials information and sharing the information with customers can increase customer satisfaction.
3. Enhancing business offerings: Blockchain-based solutions can create additional value-added services. The manufacturer can not only ensure that the correct version of the part is provided to the customer but also ensure that the number of authorised copies is provided, thereby eliminating the risk of version control errors.

Nevertheless, it is very challenging to implement blockchain to support supply chain system, especially in SMEs. It is challenging to collect data from machines and processes employed in production activities whilst ensuring data immutability and ownership is respected throughout. It is even more challenging to gather data from stakeholders' activities and interactions within a value chain. Although blockchain solutions can create value for industrial organisations in several different ways, this does not mean that it is an equally viable solution for all companies or industrial manufacturing. Furthermore, regulators worldwide are still examining the potential responses to the ever-increasing influence of blockchain-led solutions. Based on many previous cases, regulatory concerns are the number one barrier to blockchain adoption [22].

Most companies have seen the benefits of blockchain. However, since blockchain is a foundational technology that is adopted gradually instead of sudden, it might take years until it profoundly changes the supply chain management landscape.

Acknowledgements This work is under the framework of EU project AVANGARD. This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 869986. The dissemination of results herein reflects only the authors' view, and the commission is not responsible for any use that may be made of the information it contains.

References

1. Rabah, K. (2018). Convergence of AI, IoT, big data and blockchain: A review. *The Lake Institute Journal, 1*(1), 1–18.
2. Aslam, J., Saleem, A., Khan, N. T., & Kim, Y. B. (2021). Factors influencing blockchain adoption in supply chain management practices: A study based on the oil industry. *Journal of Innovation & Knowledge, 6*(2), 124–134.
3. Lawson, T. (2018). *Accelerating technology disruption in the automotive market: Blockchain in the automotive industry*. Deloitte. Accessed by: https://www2.deloitte.com/cn/en/pages/consumer-business/articles/blockchain-in-the-automotive-industry.html
4. Heutger, M., & Kuckelhaus, M. (2018). *Blockchain in logistics*. DHL. Accessed by: https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf
5. Chen, G., Xu, B., Lu, M., & Chen, N. S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments, 5*(1), 1–10.
6. Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc..
7. Hackius, N., & Petersen, M. (2017). Blockchain in logistics and supply chain: Trick or treat? In *Digitalization in supply chain management and logistics: Smart and digital solutions for an industry 4.0 environment. Proceedings of the Hamburg international conference of logistics (HICL)* (Vol. 23, pp. 3–18). epubli GmbH.
8. Sharma, P. K., Kumar, N., & Park, J. H. (2019). Blockchain-based distributed framework for automotive industry in a smart city. *IEEE Transactions on Industrial Informatics, 15*(7), 4197–4205.
9. Sánchez Pérez, A. M., Tarifa Fernández, J., & Cruz Rambaud, S. (2020). Assessing blockchain investments through the learning option: An application to the automotive and aerospace industry. *Mathematics, 8*(12), 2213.
10. Fraga-Lamas, P., & Fernández-Caramés, T. M. (2019). A review on blockchain technologies for an advanced and cyber-resilient automotive industry. *IEEE Access, 7*, 17578–17598.
11. Özel, F. M., Davies, H. C., Ernst, C. S., & Nieuwenhuis, P. (2014). How to strategically position European SMEs as part of an electric vehicle technology value chain. *International Journal of Electric and Hybrid Vehicles, 6*(3), 227–254.

12. Ko, T., Lee, J., & Ryu, D. (2018). Blockchain technology and manufacturing industry: Real-time transparency and cost savings. *Sustainability*, *10*(11), 4274. English, M., Auer, S., & Domingue, J. (2016). Block chain technologies & the semantic web: A framework for symbiotic development. In *Computer science conference for University of Bonn Students*, J. Lehmann, H. Thakkar, L. Halilaj, and R. Asmat, Eds (pp. 47–61). sn.
13. Sundarakani, B., Ajaykumar, A., & Gunasekaran, A. (2021). Big data driven supply chain design and applications for blockchain: An action research using case study approach. *Omega, 102*, 102452.
14. Li, Z., Barenji, A. V., & Huang, G. Q. (2018). Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. *Robotics and Computer-integrated Manufacturing, 54*, 133–144.C.
15. Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management, 39*, 80–89.
16. Saberi, S., Kouhizadeh, M., & Sarkis, J. (2018). Blockchain technology: A panacea or pariah for resources conservation and recycling? *Resources, Conservation and Recycling, 130*, 80–81.
17. Vatankhah Barenji, A., Li, Z., Wang, W. M., Huang, G. Q., & Guerra-Zubiaga, D. A. (2020). Blockchain-based ubiquitous manufacturing: A secure and reliable cyber-physical system. *International Journal of Production Research, 58*(7), 2200–2221.
18. Paardenkooper, K. (2019). Creating value for small and medium enterprises with the logistic applications of blockchain. In *International conference on digital technologies in logistics and infrastructure (ICDTLI 2019)* (pp. 269–274). Atlantis Press.
19. Wu, H., Li, Z., King, B., Ben Miled, Z., Wassick, J., & Tazelaar, J. (2017). A distributed ledger for supply chain physical distribution visibility. *Information, 8*(4), 137.
20. Ilbiz, E., & Durst, S. (2019). The appropriation of blockchain for small and medium-sized enterprises. *Journal of Innovation Management, 7*(1), 26–45.
21. Calabrese, G. (2001). Small-medium suppliers and the new car industry. *International Journal of Automotive Technology and Management, 1*(4), 471–489.
22. Galea-Pace, S. (2020). *The role of blockchain in manufacturing*. Manufacturing Global. Com, https://www.manufacturingglobal.com/smart-manufacturing/role-blockchain-manufacturing. Last accessed: 2021/05/01.
23. Gupta, N. (2019). *Should small and medium-sized enterprises adopt blockchain?*. Medium.com Last access: https://medium.com/akeo-tech/should-small-and-medium-sized-enterprises-adopt-blockchain-ff6c1cca784f. Last accessed: 2021/05/01.
24. Stenholm, D., Stylidis, K., Bergsjö, D., & Söderberg, R. (2017). Towards robust inter-organizational synergy: Perceived quality knowledge transfer in the automotive industry. In *DS 87-6 proceedings of the 21st international conference on engineering design (ICED 17) Vol 6: Design information and knowledge, Vancouver, Canada, 21-25.08. 2017* (pp. 011–020).
25. Supranee, S., & Rotchanakitumnuai, S. (2017). The acceptance of the application of blockchain technology in the supply chain process of the Thai automotive industry. In *Proceedings of the international conference on electronic business (ICEB)* (Vol. 2017, pp. 252–257).
26. Singh, M., & Kim, S. (2017). Blockchain based intelligent vehicle data sharing framework. *arXiv preprint* arXiv:1708.09721. D.
27. Pedrosa, A. R., & Pau, G. (2018). ChargeltUp: On blockchain-based technologies for autonomous vehicles. In *Proceedings of the 1st workshop on cryptocurrencies and blockchains for distributed systems* (pp. 87–92).
28. Sund, T., Lööf, C., Nadjm-Tehrani, S., & Asplund, M. (2020). Blockchain-based event processing in supply chains—A case study at IKEA. *Robotics and Computer-Integrated Manufacturing, 65*, 101971.
29. Zoria, S. (2019). *How is blockchain technology impacting the automotive industry*. Medium.com. https://medium.datadriveninvestor.com/how-is-blockchain-technology-impacting-the-automotive-industry-728875a7c940. Last assessed: 2021/05/01.

30. Boucher, N. (2020). *The blockchain, transformation vector for the future of the automotive industry*. Renault Group. https://www.renaultgroup.com/en/news-on-air/news/the-blockchain-transformation-vector-for-the-future-of-the-automotive-industry/. Last assessed: 2021/07/28.
31. Piscini, E., Hyman, G., & Henry, W. (2017). Blockchain: Trust economy tech trends 2017. *Deloitte Insights*. https://www2.deloitte.com/insights/us/en/focus/tech-trends/2017/blockchain-trust-economy.html
32. Kumar, R., Singh, R. K., & Dwivedi, Y. K. (2020). Application of industry 4.0 technologies in SMEs for ethical and sustainable operations: Analysis of challenges. *Journal of Cleaner Production, 275*, 124063.

Designing an Efficient Consensus Protocol for Supply Chain

Mohammad Saidur Rahman, Ibrahim Khalil, and Abdelaziz Bouras

1 Introduction

Supply chain is a complex ecosystem with multiple participants with different roles and responsibilities. For example, *retailers*, *distributors*, *manufacturers*, *suppliers*, and *customers* are a few key participants in a typical supply chain system (see Fig. 1). Traditional supply chain management systems are designed based on cloud computing technology to ensure scalability and accessibility of supply chain data from anywhere at any time [30, 19]. However, the cloud computing platform cannot be fully trusted [6, 23, 24]. Giving an example from the supply chain point of view, supply chain data stored in the cloud can be altered or false data can be injected by the dishonest cloud service provider to give financial advantage to dishonest participants during the supply chain operations. Data in the supply chain system can be altered by an internal and external attacker to give benefits to one or more supply chain stakeholders or hamper the supply chain process [2]. Therefore, a trustworthy platform is required to prevent data modification attack.

Blockchain technology is getting increased attention by the researchers from the industries and academia to design trustworthy systems in different sectors such as healthcare [31], manufacturing [1], agriculture [7] including supply chain systems [25, 10, 18]. Blockchain is a distributed ledger that is distributed among all nodes

M. S. Rahman (✉)
RMIT University, Melbourne, VIC, Australia
e-mail: mohammadsaidur.rahman@rmit.edu.au

I. Khalil
School of Computing Technologies, RMIT University, Melbourne, VIC, Australia
e-mail: ibrahim.khalil@rmit.edu.au

A. Bouras
Qatar University, Doha, Qatar
e-mail: abdelaziz.bouras@qu.edu.qa

A. Bouras et al. (eds.), *Blockchain Driven Supply Chains and Enterprise Information Systems*, https://doi.org/10.1007/978-3-030-96154-1_9

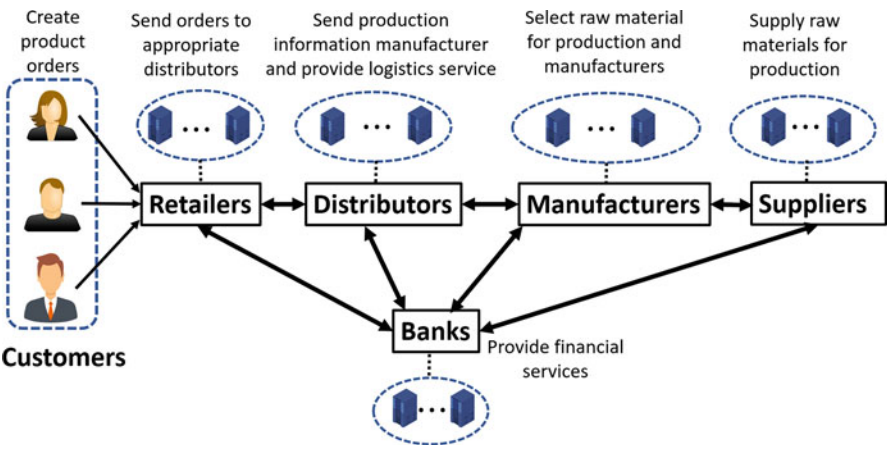


Fig. 1 An overview of a supply chain system

that are connected in a peer-to-peer fashion. The distributed ledger is created using a special type of data structure that stores data as blocks, and blocks are logically linked together via cryptographic hash algorithm [26]. As the data are replicated among all nodes in the network, it is extremely difficult to modify any data or insert fake data. Thus, blockchain provides security of stored data and can build trust among stakeholders of a supply chain system. A consensus mechanism [17] is one of the key mechanisms in blockchain-based system that will ensure the consistency and integrity of supply chain data.

Several researches have been conducted that show the prospects of blockchain-based supply chain system [16, 25, 1]. Nevertheless, a little attention is given to the consensus mechanisms that would fit well in the supply chain system. The existing blockchain-based supply chain systems apply consensus mechanisms that are mainly designed for cryptocurrency such as Bitcoin [28]. The cryptocurrency is fundamentally different from supply chain systems. The supply chain system involves transactions from stakeholders with different types of roles and responsibilities. It is extremely important to select a consensus mechanism that is suitable for supply chain. Especially, the transactions in supply chain require fast consensus for avoiding any delay in the operations. Hence, our method employs a novel consortium consensus mechanism for supply chain systems by leveraging multisignature technology. Multisignatures [15] enable multiple signers to create a compact signature for a message block. The multisignature can be considered useful for verifying a block before adding it to the blockchain [9]. The proposed consensus mechanism that leverages the multisignature schemes for block verification offers a less complicated implementation of the distributed ledger and ensures higher efficiency and scalability for achieving consensus. Overall, this chapter has the following focus:

1. Designing a consensus mechanism is developed to focus on supply chain systems. The consensus mechanism has two parts: *leader selection* and *block*

mining. The proposed consensus mechanism adopts a leader selection method similar to RAFT [21].

2. Developing a multisignature-based block mining process is introduced for higher efficiency and scalability. The proposed consensus uses the identity-based multisignature [13] for proposing a block and verification process.

2 Background

In this section, we give a brief introduction of the consensus mechanism and identity-based multisignature schemes that are the bases of our proposed consensus mechanism.

2.1 Consensus Mechanism in Blockchain

In general, the *consensus mechanism* in a blockchain network is a part that makes the nodes agree on a single piece of data [17]. In other words, the mechanism decides whether a block is going to be added in the blockchain or not. The process of adding blocks to the linked list is a significant factor to security and scalability. This can be achieved with a state machine replication (SMR) algorithm. The SMR algorithm makes a network agrees on a unique, constantly growing, ordered set of transactions. The terms consensus mechanism and SMR algorithm are closely related. Hence, they are often used interchangeably.

In order to achieve consensus, an algorithm has to provide two properties: *safety* and *liveness*. The safety in the consensus mechanism means that a new entry to the transaction log cannot be changed later once nodes confirmed it. The liveness represents that a transaction submitted by an honest user gets accepted if the user has sufficient connectivity. As consensus mechanisms are Byzantine Fault Tolerant (BFT), blockchains are deemed to be trustless. In a blockchain network, other nodes may behave in malicious ways. Therefore, blockchain users do not need to trust others. In general, consensus algorithms cannot tolerate more than a third of the nodes being malicious [22]. A blockchain may allow more byzantine faults. There are several consensus mechanisms that are widely used in blockchain such as *Practical Byzantine Fault Tolerance (PBFT)*, *Proof of Elapsed Time (PoET)*, *Steller Consensus Protocol (SCP)*, *Hashgraph*, *Raft*, and *Tendermint* [5].

The consensus mechanism depends on the architecture of the blockchain network. Blockchain networks can be classified as *public*, *consortium*, or *private* blockchain in order of decreasing degrees of openness available for participation by nodes [27]. The *public blockchain* is also referred to as a permissionless blockchain since any node can freely enter and exit the network. The public chain is the earliest and most widely used blockchain architecture. Bitcoin [20] is the most widely known example of the public blockchain. The *private blockchain* is also known as the permissioned blockchain and is only used in private organizations or institutions

[3]. Unlike public blockchains, private blockchains are generally not open to the outside world and are only open to individual individuals or institutions.

The consortium blockchain is a hybrid architecture comprising features from both public and private blockchains. A consortium blockchain is also a permissioned blockchain, in which participation is limited to a consortium of members to participate; each node might refer to a single organization or institution in the consortium. The number of nodes in a consortium blockchain is determined by the size of the pre-selected participants in the blockchain. For example, a supply chain blockchain is designed for a consortium of twenty participants. In that case, the maximum number of nodes in this consortium blockchain is twenty, and the number of nodes required to reach the consensus depends on which consensus algorithm the consortium blockchain uses. The consortium chain accesses the network through the gateways of member institutions. The consortium chain platform generally provides members' information authentication, data read and write permission authorization, network transaction monitoring, member management, and other functions. Each member can have permissions assigned by the consortium to access the ledger and validate the generation of blocks. The well-known Hyperledger project is an example of a consortium blockchain [8]. Since there are relatively few nodes participating in the consensus process, the consortium blockchain generally does not use the PoW mining mechanism as the consensus algorithm. Consortium chains' requirements for transaction confirmation time and transaction throughput are very different from those of public chains.

2.1.1 Raft Protocol

Raft [21] or the Raft Consensus Algorithm is developed to facilitate practical implementation for industry applications. The main idea of RAFT is that each node in the blockchain starts from the identical initial state and executes a series of instructions in the same sequence. The primary objective of the Raft consensus mechanism is achieving a consistent state. As a result, the Raft uses a consistent algorithm log method to synchronize instructions and manage replicated logs.

In Raft algorithm, nodes are divided into three roles that are mutually convertible. Roles include: *leader*, *follower*, and *candidate*. Only one node can act as a leader in the whole cluster of nodes. The number of nodes in a cluster must not be less than five. The leader is designated to receive user requests, maintain replication logs, and communicate with followers.

At the start of the time, all nodes are followers that passively respond to requests from the leader. Follower nodes do not exchange any message with each other, while they are acting as passive nodes. A follower node responds to log replication requests received from the leader node and responds to election requests that are sent from candidate nodes. The follower node passes the election request directly to the leader node once a follower receives a request from the user.

A candidate node initiates the election process. In the absence of a leader node, due to a crash or network failure, one or more blockchain nodes propose them as

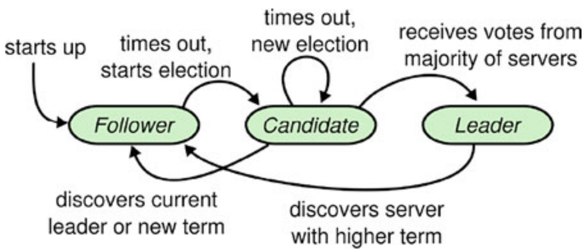


Fig. 2 An overview of server states of RAFT protocol [21]

candidate nodes and initiate an election process for electing a new leader node. After the successful execution of the election process, a candidate node is selected as the leader node, and the status of the candidate node is changed to leader. Figure 2 shows how the three roles change states. Each round of an election process is called a *term* that elects only one leader. Term is represented by a continuously increasing number.

The Raft algorithm consensus has two phases: *leader election* and *log replication*. The leader election phase is activated by a mechanism called *heartbeat mechanism* where a leader node broadcasts a message to all follower nodes periodically and maintains its authority. Otherwise, any of the follower nodes switches its role to candidate role and initiates a leader election mechanism assuming that the leader has failed [21]. Next, the new candidate node increases its current term and asks votes for itself. In addition, the new candidate node broadcasts a message called *RequestVoteRPC* to other blockchain nodes and waits for any of the following situations [21]:

– A candidate node that wins the election with more than half of the server votes becomes a leader node.
– A candidate loses the election as another candidate node has got more than half of the votes. The loosing candidate node receives the corresponding heartbeat from the winner and becomes a follower node.
– No winner is found, and the election process is re-instantiated after a random timeout period. The term increases.

The log replication phase is the second phase where the leader node accepts the user request. Based on the request, it updates the log information and broadcasts a heartbeat message to all follower nodes. All follower nodes synchronize the leader node's log once the heartbeat message is received.

2.2 *Identity-Based Multisignature Scheme*

A multisignature includes a group of participants for signing the same message and generates an output known as multisignature [4]. The multisignature can be verified with the set of public keys of the participants that sign the message. The verification of standard multisignature schemes needs the public keys of all signers. Therefore in applications where bandwidth is a bottleneck, it can be useful to consider identity-based multisignatures where verifiers only need unique identifiers of signers instead of public keys.

The identity-based multisignature scheme can be *serial*[11] or *parallel*[13]. This chapter leverages the concept of parallel multisignature scheme: a parallel multisignature scheme where all signers sign a data or file in parallel [11]. The identity-based multisignature scheme is developed based on the concept of identity (ID)-based cryptosystems. In ID-based cryptosystem, a user's public key is derived from their identity, and private key is computed by a trusted third party known as private-key generator (PKG). ID-based cryptosystems provide better flexibility of the key management over the traditional public-key cryptosystems (PKCs), and signature can be verified with signer's identity [12].

3 Multisignature-Based Consensus Mechanism

In this section, we discuss our proposed consensus mechanism for supply chain systems. We develop a consensus mechanism that consists of two parts. In the first part, an election process determines a *leader node* among the blockchain nodes. The leader node selection process is inspired by the RAFT Consensus algorithm [21]. We assume that we have b number of participants in a supply chain management system that forms a consortium of participants. Each participant takes part in the consensus mechanism. However, our version of the RAFT inspired leader node election algorithm divides blockchain nodes into two groups—a single *leader node* and the rest of the nodes are *proposer nodes* (see Fig. 3).

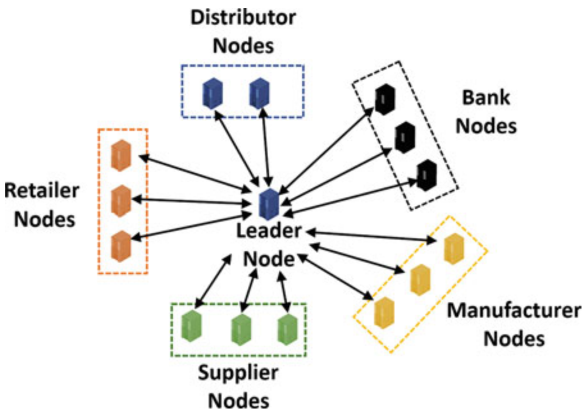


Fig. 3 Overview of the consortium of the proposed RAFT-based consensus

3.1 Leader Node Selection

Initially, all nodes are proposers and receive transactions from users. A node is randomly selected as the leader node to mine the first block. As a result, nodes are divided into two groups. The leader node periodically sends a request to all proposer nodes. A proposer node passively responds to the requests from the leader. If a proposer does not receive any request from the leader node, it initiates the leader election process by claiming itself a candidate. It is possible that multiple nodes have declared themselves as candidate. Nodes that have failed to declare them as candidate will be considered as voters and vote their suitable candidate. If a candidate gets a maximum number of votes, the node declares itself as the leader node and starts sending messages to the proposer.

3.2 Block Mining

The second part involves the block mining process that is developed by leveraging an identity-based multisignature scheme [13]. The block mining process involves two phases: *proposal phase* and *verification phase*. In the proposal phase, blockchain nodes use the multisignature scheme for initiating the mining phase and certify a proposed block. The certified block can be verified by the leader node in the verification phase. An overview of the block mining process is illustrated in Fig. 4. The steps are as follows:

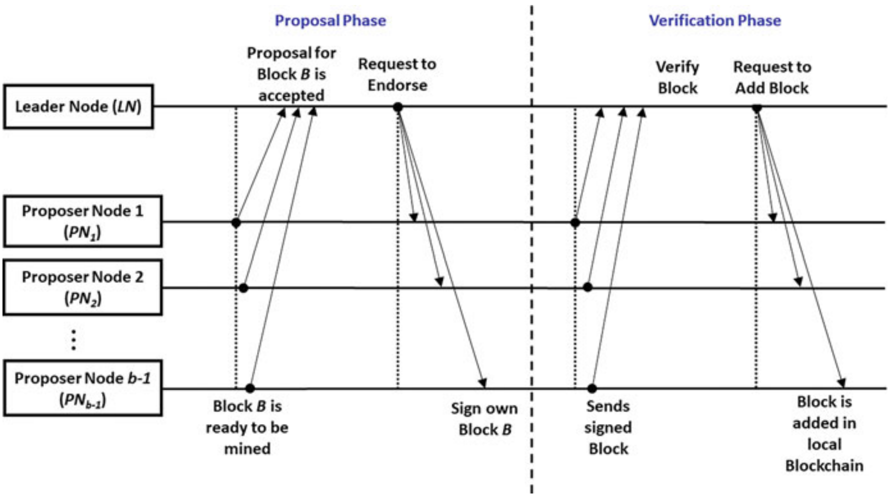


Fig. 4 Overview of the block mining process

1. A *leader node* (LN) is elected by the nodes of the blockchain network for a short period of time according to the leader selection mechanism of RAFT protocol. For example, only for mining the current block. Other nodes become *proposer nodes*. LN generates required keys for proposer nodes. Keys include a public key (PK), a master key (MK), and private key s_i for each proposer node (i.e., miner). LN sends PK and the respective private key s_i to each proposer node.
2. In a blockchain network, each proposer node or miner contains *a proposed block* $\mathcal{B}$ that needs to be added in the blockchain. Each miner signs their respective proposed block $\mathcal{B}$.
3. Once $\mathcal{B}$ is signed, each miner generates their own signature verification parameter and shares their signature verification parameters to each other to produce a combined signature verification parameter. Finally, each miner sends the signed $\mathcal{B}$ and the combined signature verification parameter to LN.
4. LN uses verification parameters to verify all received signed blocks $\mathcal{B}$. If all blocks are verified correctly, LN asks proposer nodes to add the proposed block in the blockchain.

The aforementioned tasks can be divided into four parts: (1) public-key generation by LN, (2) private-key generation by LN for all miners, (3) signing proposed block by miners, and (4) block verification by LN. Detailed discussion of each part is provided below.

3.2.1 Preliminaries

Assume that there are b number of blockchain nodes in the blockchain network BCN. The set BCN_{nodes} of blockchain nodes can be represented as: $BCN_{nodes} = \{bn_1, bn_2, \ldots, bn_b\}$. In our proposed consensus mechanism, we assume that a blockchain node $bn_i^{'} \in BCN_{nodes}$ is elected as a *leader node* LN using a leader election algorithm for consortium blockchain networks [21]. The LN is elected for a limited time period. For example, the LN is elected only for mining the current block. A new LN is elected from the BCN_{nodes} to mine the next block. The LN acts as a key generator and the block validator. The rest of the nodes $\{b_1, b_2, \ldots, b_{b-1}\}$ act as proposer nodes.

3.2.2 Key Generation by LN

As we stated earlier, the leader node LN generates the required key based on an identity-based multisignature scheme. LN runs a key generation algorithm to generate a master key and public key for itself. The master key of LN is used to generate the signing parameters of proposer nodes. On the other hand, the public key is used for verifying the block proposed by proposer nodes.

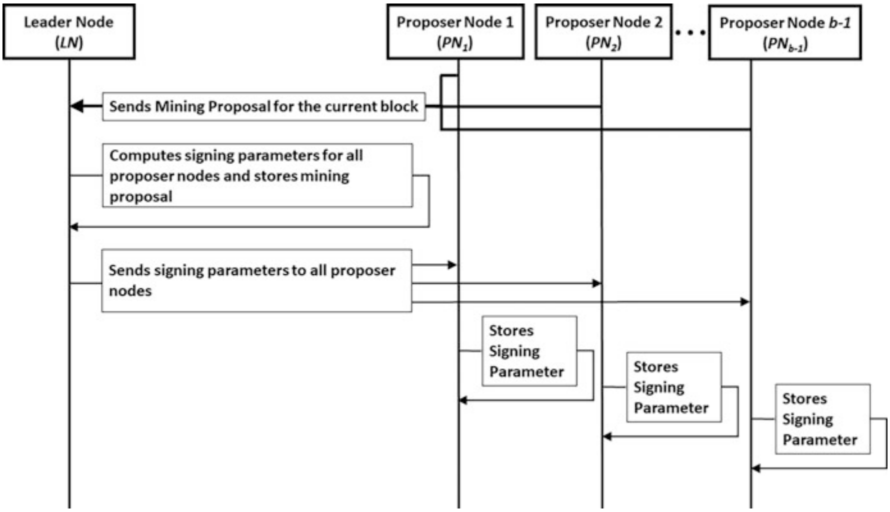


Fig. 5 Overview of the proposal for mining

3.2.3 Blockchain Node's Mining Proposal Generation

A proposer node generates its *signing key* sk_i in collaboration with LN. The signing key is generated in a way so that it can be used to sign only the current block (i.e., the block to be mined), and the key cannot be used for signing any previous block. Hence, sk_i includes the *proposer node ID*, *current block number*, and *timestamp*. As a result, corrupted proposer blockchain nodes cannot use their private keys for creating fork (i.e., two different but equally valid versions of the blockchain) [29]. An overview of the mining proposal generation is presented in Fig. 5. The generation of PR_i has the following steps:

1. A proposer node bn_i sends its identification number (ID_i), the sequence number of the block to be mined ($\mathcal{B}$), and timestamp $\mathcal{T}_i$ to LN.
2. If $\mathcal{B}$ is the current block number and $\mathcal{T}_i$ is greater than the timestamp when the last block mined, LN generates a *mining proposal* by hashing ID_i, $\mathcal{B}$, and $\mathcal{T}_i$ using a hash function.
3. LN signs the ID_i, $\mathcal{B}$, and $\mathcal{T}_i$ using LN's master key and generates a miner's signing key sk_i. The signing key sk_i is sent to the proposer node.
4. The LN stores the mining proposals from all blockchain nodes as a collection: $J = \{J_1, J_2, \ldots, J_{b-1}\}$.

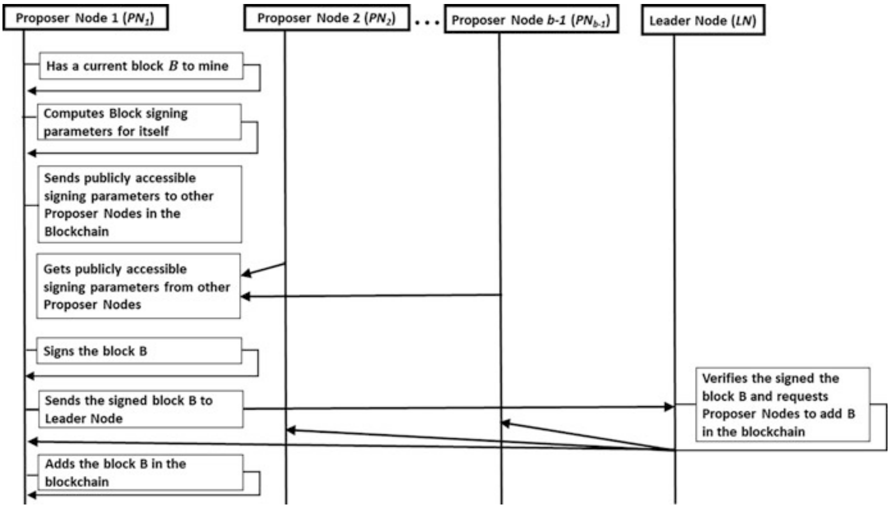


Fig. 6 Overview of the block signing process

3.2.4 Signing Proposed Block by Proposer Nodes

In the signing process of a proposed block $\mathcal{B}$, all of the proposer nodes sign in a combined manner by leveraging an identity-based multisignature scheme. All proposer nodes use their respective signing key and the leader node's public key. An overview of the block signing process is shown in Fig. 6. The signing process involves the following steps:

1. Using the identity-based multisignature scheme, every proposer node computes their own *publicly accessible signing parameters* to sign the current block in a manner so that the signed block can be verified by the leader node.
2. Each proposer node broadcasts its parameter to other proposer nodes.
3. Upon receiving other proposer nodes' publicly accessible signing parameters, each proposer node combines them to compute a parameter that is the same for all proposer nodes.
4. Each blockchain node signs their current block $\mathcal{B}$ with the combined parameter and the signing key received from the leader node to generate the signed block. The signed block is sent to leader node LN.
5. LN verifies signed blocks, sent by proposer nodes, with its master key. The verification is successful if all signed blocks have the same state. Once the blocks are verified, LN recommends all blocks to add their proposed block to the current blockchain and announces the mining process as complete.

4 Performance Analysis

In this section, the performance of the proposed RAFT and multisignature-based consensus algorithm for supply chain is discussed. The analysis is performed in terms of security and efficiency from the perspectives of both RAFT protocol and identity-based multisignature.

4.1 Security Analysis

As it is stated earlier, the proposed consensus mechanism involves two parts. The first part is the *leader selection* that is built on the RAFT protocol. Hence, the security of the leader node selection process depends on the security of the RAFT protocol. In our proposed consensus mechanism, there is only one leader node and $(b - 1)$ proposer nodes. The leader node is responsible for the key generation of all other proposer nodes, and it is selected based on the votes of the majority of the proposer nodes. Thus, the leader node is assumed to be trusted. Moreover, the life span of a leader node is limited [14]. The second part of the proposed consensus mechanism is designed based on multisignature scheme where all signers must sign the same block to add the block in the blockchain. Also, the identity-based multisignature scheme forces each proposer node to add their identity in the mining process, which helps the leader node to generate individual signing keys. At the time of signing a block, the proposer nodes involve each other's secret parameters, which makes the signing process secured. Finally, the leader can influence the mining process if only if all proposer nodes are corrupted. From that point of view, the proposed consensus mechanism is secured.

4.2 Efficiency

Unlike the existing consensus mechanism, our proposed consensus mechanism does not involve high-computational resources. As multisignature scheme requires fewer steps and keys for the verification of the signed entity, it itself is an efficient process. Hence, signing and verification of the proposed block with multisignature scheme are efficient. Nevertheless, the actual time for the mining process involving multisignature scheme may vary depending on the multisignature scheme that is used.

5 Conclusion

In this chapter, we present a novel consensus mechanism for the supply chain management system. The proposed consensus mechanism is designed considering a consortium blockchain network involving all supply chain stakeholders. Blockchain nodes select a leader node to mine a block using RAFT protocol that allows changing the leader node for each mining task to ensure trust and security mining process. The identity-based multisignature scheme makes the consensus process lightweight and practical. Nevertheless, the proposed consensus mechanism creates an avenue of further investigation to find the suitability of this consensus mechanism in diverse supply chain scenarios. Different types of leader node selection processes and multisignature schemes should be investigated to find a consensus mechanism that would fit all supply chain scenarios.

Acknowledgments This chapter was made possible by NPRP grant NPRP11S-1227-170135 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

References

1. Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology, 5*(9), 1–10.
2. Akinrolabu, O., New, S., & Martin, A. (2018). Cyber supply chain risks in cloud computing-bridging the risk assessment gap. *Open Journal of Cloud Computing, 5*(1), 1–19.
3. Aras, S. T., & Kulkarni, V. (2017). Blockchain and its applications—a detailed survey. *International Journal of Computer Applications, 180*(3), 29–35.
4. Bagherzandi, A., & Jarecki, S. (2010). Identity-based aggregate and multi-signature schemes based on RSA. In *International workshop on public key cryptography* (pp. 480–498). Springer.
5. Baliga, A. (2017). Understanding blockchain consensus models. In *Persistent*.
6. Baumann, A., Peinado, M., & Hunt, G. (2015). Shielding applications from an untrusted cloud with Haven. *ACM Transactions on Computer Systems, 33*(3), 1–26.
7. Bermeo-Almeida, O., Cardenas-Rodriguez, M., Samaniego-Cobo, T., Ferruzola-Gómez, E., Cabezas-Cabezas, R., & Bazán-Vera, W. (2018). Blockchain in agriculture: A systematic literature review. In *International Conference on Technologies and Innovation* (pp. 44–56). Springer.
8. Cachin, C., et al. (2016). Architecture of the Hyperledger blockchain fabric. In *Workshop on distributed cryptocurrencies and consensus ledgers* (Vol. 310). Chicago, IL.
9. Drijvers, M., Gorbunov, S., Neven, G., & Wee, H. (2020). Pixel: Multi-signatures for consensus. In *29th USENIX Security Symposium (USENIX Security 20)* (pp. 2093–2110).
10. Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics, 2*(1), 2.
11. Gangishetti, R., Gorantla, M. C., Das, M. L., & Saxena, A. (2006). Identity based multisignatures. *Informatica, 17*(2), 177–186.
12. Gorantla, M. C., Gangishetti, R., & Saxena, A. (2005). A survey on ID-based cryptographic primitives. *IACR Cryptology ePrint Archive, 2005*, 94.

13. Harn, L., Ren, J., & Lin, C. (2009). Efficient identity-based GQ multisignatures. *International Journal of Information Security, 8*(3), 205–210.
14. Huang, D., Ma, X., & Zhang, S. (2019). Performance analysis of the Raft consensus algorithm for private blockchains. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50*(1), 172–181.
15. Itakura, K., & Nakamura, K. (1983). A public-key cryptosystem suitable for digital multisignatures. *NEC Research & Development* (71), 1–8.
16. Korpela, K., Hallikas, J., & Dahlberg, T. (2017). Digital supply chain transformation toward blockchain integration. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.
17. Lamport, L., Shostak, R., & Pease, M. (1982). The byzantine generals problem. *ACM Transactions on Programming Languages and Systems, 4*(3), 382–401.
18. Longo, F., Nicoletti, L., Padovano, A., d'Atri, G., & Forte, M. (2019). Blockchain-enabled supply chain: An experimental study. *Computers & Industrial Engineering, 136*, 57–69.
19. Manuel Maqueira, J., Moyano-Fuentes, J., & Bruque, S. (2019). Drivers and consequences of an innovative technology assimilation in the supply chain: cloud computing and supply chain integration. *International Journal of Production Research, 57*(7), 2083–2103.
20. Nakamoto, S. Bitcoin whitepaper (2008). https://bitcoin.org/bitcoin.pdf (17.07.2019)
21. Ongaro, D., & Ousterhout, J. (2014). In search of an understandable consensus algorithm. In *2014 {USENIX} Annual Technical Conference (USENIX ATC 14)* (pp. 305–319).
22. Pease, M., Shostak, R., & Lamport, L. (1980). Reaching agreement in the presence of faults. *Journal of the ACM, 27*(2), 228–234.
23. Rahman, M. S., Khalil, I., Alabdulatif, A., & Yi, X. (2019). Privacy preserving service selection using fully homomorphic encryption scheme on untrusted cloud service platform. *Knowledge-Based Systems, 180*, 104–115.
24. Rahman, M. S., Khalil, I., Atiquzzaman, M., & Yi, X. (2020). Towards privacy preserving AI based composition framework in edge networks using fully homomorphic encryption. *Engineering Applications of Artificial Intelligence, 94*, 103737.
25. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research, 57*(7), 2117–2135.
26. Sun, H., Wang, X., & Wang, X. (2018). Application of blockchain technology in online education. *International Journal of Emerging Technologies in Learning, 13*(10).
27. Tasca, P., & Tessone, C. J. (2017). Taxonomy of blockchain technologies. Principles of identification and classification. arXiv preprint arXiv:1708.04872.
28. Urquhart, A. (2016). The inefficiency of bitcoin. *Economics Letters, 148*, 80–82.
29. Webb, N. (2018). A fork in the blockchain: Income tax and the bitcoin/bitcoin cash hard fork. *North Carolina Journal of Law & Technology, 19*(4), 283.
30. Wu, Y., Cegielski, C. G., Hazen, B. T., & Hall, D. J. (2013). Cloud computing in support of supply chain information system infrastructure: understanding when to go to the cloud. *Journal of Supply Chain Management, 49*(3), 25–41.
31. Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain technology use cases in healthcare (Vol. 111, pp. 1–41).

Blockchain Technology Regulation: Time for Standardized Frameworks

Assam Hammi, Anjaneyulu Jinugu, Malike Bouaoud, Ahmed Hefnawy, and Abdelaziz Bouras

1 Introduction

Blockchain is an innovative technology consenting new distributed software architectures, where the data structure is a list of blocks. The operation's principle with regard to this data is to securely record and combine transactions that have happened within the blockchain network in order to transfer the ownership of digital assets [1]. Blockchain technology compromises an encouraging substitute where a centralized management system is not desirable or possible. Blockchain and its distributed ledger technology (DLT) promises unchangeability and truthfulness of data without the necessity of a third party. Thus, blockchain, as disruptive technology, is revolutionizing the existing systems of trust. It also carries self-execution processes; this can be achieved with its smart contract functionality. However, when we start implementing blockchain technology in real projects, and after passing the demonstration phase of feasibility, we face many constraints with regard to the lack of common terminology, legal status of contracts, and individual privacy and data protection. The establishment of international blockchain standards

A. Hammi (✉) · A. Bouras
Qatar University, Doha, Qatar
e-mail: assam.hammi@qu.edu.qa; abdelaziz.bouras@qu.edu.qa

A. Jinugu
Ministry of Transport and Communications (MoTC), Doha, Qatar
e-mail: ajinugu@motc.gov.qa

M. Bouaoud
Qatar Central Bank, Doha, Qatar

A. Hefnawy
Delos Delta, Australia

A. Bouras et al. (eds.), *Blockchain Driven Supply Chains and Enterprise Information Systems*, https://doi.org/10.1007/978-3-030-96154-1_10

might appear necessary. This would influence blockchain future development, as this technological paradigm is still at an infancy-innovative phase.

2 Background

Unlike other existing systems, the specificity and strength of blockchain technology is no longer to require the use of a trusted third party to validate the transfer of ownership but to be able to share, through consensus, the responsibility for this validation on a community (through "mining" machines). Such move from centralized registers technology to distributed ledger technology needs consensus and mature standardization. Such standards start as technical applications which need to be harmonized, converged, and matured into international standards. Blockchain technology is expected to respect alike sequence [2]. Many standards development organizations (SDOs) have initiated efforts in order to normalize blockchain and DLT in terms of interoperability and identify what sectors could benefit most from this nascent technology by delivering a common and clear shared technical foundation for industry [3]. This will accelerate adoption's degree of the blockchain technology among digital economies of services and goods. As per the British Standards Institution (BSI) report prepared by RAND Europe [4], the priority areas proposed about the potential role of standards in supporting the development and adoption of the blockchain and DLT are illustrated as timeline in relation to these areas (see Fig. 1). This timeline includes three terms; the short term where terminology and vocabulary are highlighted, then from the medium term to the long term, where other areas must be focused on such as interoperability, security, privacy, and data governance without forgetting end-user identity and provenance tracking as well as the technical aspects.

As mentioned previously, many SDOs made initiatives to standardize the blockchain technology [3], i.e., ISO, IEEE, NIST, etc. A timeline summarizing those efforts is depicted in Fig. 2.

- The ISO has formed with Standards Australia (SA), a technical committee (ISO/TC 307), to address blockchain and DLT standardization concern.
- The International Securities Association for Institutional Trade Communication (ISITC) has formed with the Organization for the Advancement of Structured Information Standards (OASIS) the blockchain and DLT working group to define a technical standard in terms of safety and security.
- The World Wide Web Consortium (W3C) has initiated a blockchain community group to produce message format standards for blockchain, guidelines for usage of storage, etc.
- The Institute of Electrical and Electronics Engineering (IEEE) has launched a standard program of blockchain among other "the Standard for the Framework of Blockchain Use in IoT4."

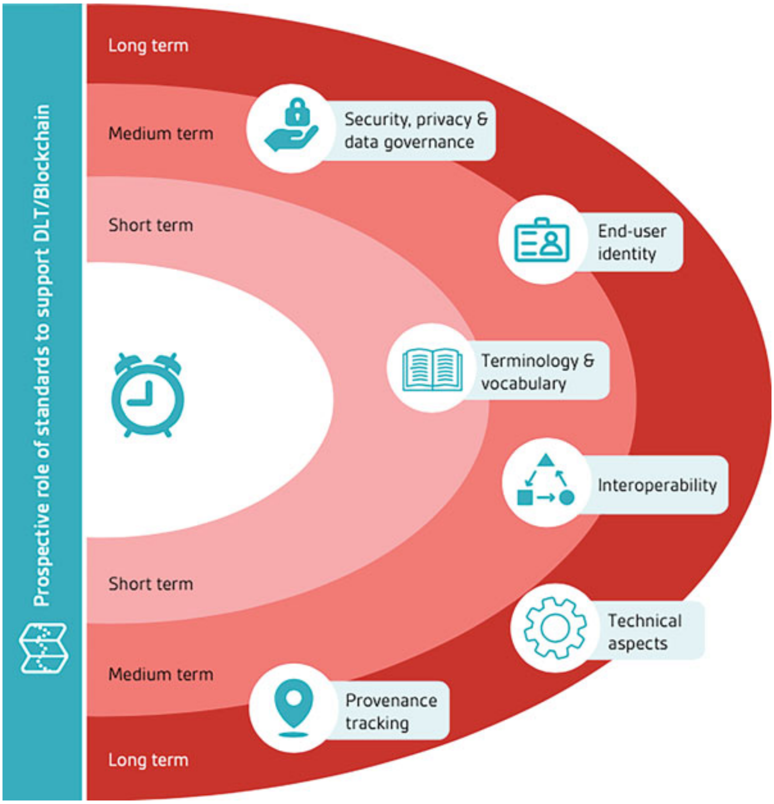


Fig. 1 Areas where standards could potentially play a role in supporting DLT/blockchain. (Source: RAND Europe [4])

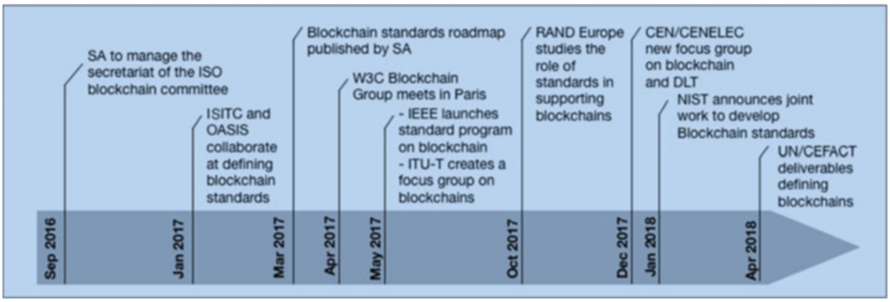


Fig. 2 Various organizations have started devoting efforts to standardize blockchains and DLT (enhanced by the authors)

- The Telecommunication Standardization Sector (ITU-T), under the International Telecommunication Union (United Nations), has formed a focus group on application of blockchain and DLT to propose a way forward for related standardization work in ITU-T study groups.
- The European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC) has formed a focus group on blockchain and DLT to identify possible specific European standardization requirements.
- The National Institute of Standards and Technology (NIST) cooperated with ISO in order to define blockchain standards that will improve US government services.
- The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) made a draft for a public review of white paper on the technical applications of blockchain to its deliverables[1]; the blockchain project team sought the use of blockchain for trade-related use cases.

- A report entitled "Distributed Ledger Technology: beyond blockchain" was disseminated by the government office for science in the UK[2] which clearly stated that "Government needs to consider how to put in place a regulatory framework for distributed ledger technology. Regulation will need to evolve in parallel with the development of new implementations and applications of the technology." The report presented a couple of recommendations related to the global perspective, governance, security, privacy and disruptive potential, etc.
- The European Securities Markets Authority (ESMA) had highlighted from a public policy point of view the possible strengths and weaknesses that blockchain and DLT would have on securities markets. By publishing a discussion paper entitled "The Distributed Ledger Technology Applied to Securities Markets,"[3] ESMA has attempted to have feedback from the industry to be taken into consideration when promulgating policies and regulations; however, ESMA did not explicit any reaction on that time.
- The Commodity Futures Trading Commission (CFTC) as a US regulator had investigated how blockchain and DLT would be used in the market. It suggested to adopt a regulatory approach that encourages DLT investment and innovation [5]. The CFTC Technology Advisory Committee (TAC) renowned that the absence of blockchain standards is due to the nascent technology which is still under development, meaning that its application will be incremental.
- The Securities and Exchange Commission (SEC) is another US regulator that was dynamically investigating possible application of blockchain and DLT in

[1] https://uncefact.unece.org/display/uncefactpublicreview/Public+Review%3A+Blockchain+Whitepaper

[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

[3] https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf

the public securities market; one of the SEC commissioners alerted that "as the market holds Blockchain technology, regulators need to be in a position to lead"[4].

- Since 2013, China started promulgating a series of policies, laws, and regulations related to blockchain in order to promote the healthy development of this technology and to reduce investment risks. One of the recent policies issued by the State Internet Information Office is called "Regulations on blockchain information service management" [6].
- For the moment, there are no specific regulations dealing with blockchain and DLT in Australia.[5] Despite that, the Australian Securities and Investments Commission (ASIC) released an information sheet called "INFO 219 Evaluating distributed ledger technology"[6] that highlights the approach to the regulatory issues with regard to blockchain adoption and DLT solution.

3 Blockchain Applications Through Regulation Perspective

3.1 Financial Sector

To properly define the scope of regulation for the use of blockchain in the financial sector, it is important to understand the various use cases with blockchain. Indeed, the multiple use cases are supported by different levels of acceptance or adoption. The first and foremost use case is related to the forms of payments and mainly the use of blockchain for currencies. People around the world have discovered the development of new form of currencies that bear no legal tender. However, they gained a large interest from the public due to their decentralized nature as well as the confidentiality that these currencies are holding against a central regulator with a sense of freedom. The rise in popularity of the cryptocurrencies has pushed national governments to act upon it. Nowadays, central banks, the main financial sector regulator and guarantor of national currencies, are working at issuing central bank-issued digital currencies (CBDCs) that also changes the role of the regulators with regard to currency notes. Indeed, this implies multiple changes in the way the currency is disseminated as well as raise questions on the necessity to develop the wholesale market, i.e., the roles of the private banks may not hold any currency in the future. The other use of blockchain still relates largely to the domain of payment transactions and specifically the transfer of money to end users. The electronic transfer from account to account for decades relies on a heavy infrastructure. The

[4] https://www.sec.gov/news/speech/surfing-wave-technology-innovation-and-competition-remarks-harvard-law-schools-fidelity

[5] https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/australia

[6] https://asic.gov.au/regulatory-resources/digital-transformation/evaluating-distributed-ledger-technology/

use of blockchain for payment transfer allows for increase speed of operations for near instant transaction which clearly competes with traditional payment methods.

It has to be noted that both use cases can leverage both centralized (CLT) and decentralized ledger-based technologies (DLT) as the transfer of digital assets' ownerships can be validated by both old and new ledger techniques. However, for the latter, and in terms of regulations, there is currently no precise way to trace those transfers[7]unlike the centralized ledger where a manner to securely achieve that goal (transfers of digital assets' ownerships) is applied via trusted third parties under the supervision of a control authority (regulator). Regulations still have to fill the gap with every major development of technology such as blockchain, whether by completing existing legal text related to old technology or by finding a common denominator between the old and new technology of a kind that market integrity and stockholders' security. The traditional approach in regulating the financial sector is often based on the principles of "whitelisting" as an analogy to the term used in cybersecurity. Indeed, the only authorized systems would become eventually those that are defined by a central regulator, bearing a legal tender and excluding de facto any other form of development.

3.2 Logistics Sector

Blockchain-based applications for logistics sector intend whether to alternate the existing practices and current logistics procedures in a digitized form or to fully eliminate them [6]. For example, Wave, which is a blockchain application, eradicates completely what's called bill of lading (the well-known document delivered by shipper to acknowledge receiving cargo for shipment) and directly connects the producer and the purchaser by a blockchain solution where the two parties involved can access to the shipment data with full transparency. Nevertheless, the blockchain application from Chain of Things (CoT) lab which is called Chain of Shipping[8] focuses on how to alleviate fraud and inefficiencies in the shipping and logistics industry by the use of IoT to digitize bill of lading. Modum.io AG company [7] combined blockchain technology and IoT sensors in the pharmaceutical logistics sector. During the process of medical products transportation, smart contract guarantees the record of data and the accessibility of all parties by providing a code representing a contract that is self-executing to ensure temperature category compliance as per EU regulation (GDP 2013/C 343/01) Good Distribution Practice of medicinal products for human use.[9] Once again, no clear regulations are yet in

[7] http://www.revue-banque.fr/banque-investissement-marches-gestion-actifs/article/reglementation-blockchain-defi-neutralite-techn#restricted_content

[8] https://www.chainofthings.com/news/2016/12/10/chain-of-shipping-conference-a-review

[9] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:343:0001:0014:EN:PDF

force in this area, and the adoption of the blockchain-based applications for logistics sector may confront by barriers in terms of legal rules.

3.3 Healthcare Sector

Blockchain technology offers a holistic potential as well in terms of decentralization, security, immutability, and privacy in the healthcare area by storing and sharing electronic medical records, personal healthcare data, etc. Different blockchain-based applications deal with healthcare information exchange such as BlocHIE [8] which is designed for sharing and storage of data among medical institutions and patients. The platform is composed of blockchain network where the collected healthcare is stored, hospitals and clinics where patients' diagnostic records are shared with other medical institutions through the blockchain network, and IoT devices that share the daily healthcare data of individuals in an automatic manner to the blockchain network. However, there are concerns with regard to protection of privacy laws when it comes to personal data. The fact that immutability is one of the strong data integrity features of blockchain ensures that once the data record is saved, it cannot be changed or erased. This is contradictory with legal obligation such as GDPR regulation in the EU [9] (General Data Protection Regulation) that reinforced the rights of individuals to request personal data to be deleted.

3.4 Architecture, Engineering, and Construction Sector

Several public organizations from various sectors are supporting blockchain initiatives and following approaches that keep them up with the novelty of this technology [10]. Among others, the Architecture, Engineering, and Construction (AEC) sector is investigating on how blockchain technology could present benefit to the field, and how to integrate this technology with the adopted ones such as Building Information Modeling (BIM) and Digital Twins (DT) [11]. Bimchain.io,[10] which is a French start-up, has developed a proof of principle to integrate blockchain within BIM in order to accelerate BIM process and workflow. The aim is to make fast transition from dual process to distributed BIM process by using smart contracts. Thus, PoC (proofs of contributions) are linked to the BIM 3D model with automated payments ensuring that all participants are devoted to reach a certain quality level. There is mutual relationship between BIM and blockchain; data either can be incorporated from blockchain and its DLT to BIM model or can be sent from BIM model to blockchain itself informing about changes and updates that must be considered for use later by smart contract to execute automatic payments, for example [12]. The

[10] https://bimchain.io/technology/

fact that there is only one source of true information related to all aspects of the process gives to the integration of blockchain technology within BIM process an important role step for the whole sector's development. Xiong, Feng et al. designed a blockchain-based Construction Supply Chain (CSC) framework to tackle challenges facing the old approaches, i.e., postponements, waste of data, and transmission costs. By eliminating intermediaries, reduction of limitations would be possible as they also introduced a private key distribution method in blockchain to help recover lost private keys [13]. The Centre for Digital Built Britain (CDBB) made necessary the investment in research linked to blockchain regulations in the AEC sector, and required the transformations of developed business models to provide a good demonstrator for the AEC sector [14].

4 Challenges

Most of the countries in the world are open to freedom of speech, and it is being safeguarded by their constitution. On the other hand, assets are owned by people with the governed laws and regulations, and these laws are developed to keep them closed. Similarly, blockchain or cryptocurrencies should be regulated with right laws and regulations as these are digital assets. So, there is the need of the hour for the regulators to understand the regulations and challenges of blockchain technology.

Deloitte [15] conducted a global survey on blockchain technology in 2020; the top two greater barriers to adopt blockchain technology among the organizations are (1) replacing or adapting existing legal systems and (2) potential security threat. Haitham [16] said that definition of some regulatory terms such as legality of transaction ownership and trade finality needs to be updated or changed in the blockchain technology arena. Moreover, confidentiality of transactions and data privacy are the two major concerns of the regulators while implementing the blockchain technology. Sakho et al. [17] mentioned that recently a lot of people invested in blockchain or cryptocurrencies, and they revealed that this environment is tremendously volatile due to enormous cases of financial thefts, scams, and stock market manipulations. These scenarios are increasing nowadays and the authors concluded that the lack of regulation is a major concern.

The European Union (EU) understood salient potential benefits of blockchain technology and distributed ledger technology (DLT). EU proactively planned to develop laws and regulations to update the potential of these technologies. Unfortunately, a lot of European institutions felt that these technologies should be adopted by more institutions, that more innovation is needed, and that proof of concepts should be developed. Based on all these factors, regulators of EU may have to wait some more time to regulate these emerging technologies [18]. The USA and EU embraced smart regulatory hands-off approach in financial and related sectors for future innovation in blockchains [19]. In addition, blockchain technology is not limited to a particular country's jurisdiction, and thus many legislations should be rewritten or be changed when the blockchain technology takes off fully in collaboration with other nations [20]. Blockchain technology-related services should be regulated by multiple government agencies, and it is very sensitive and difficult to draft laws for the blockchain technology [21]. So, regulators should not undervalue these challenges while developing regulations of blockchain technology.

Cermeño [22] stated that in principle technology cannot be regulated, but its events can be regulated including the blockchain technologies, and he has discovered 11 blockchain regulatory challenges in the financial sectors:

- Reduction of anonymity of transaction through Anti Money Laundering (AML) directives Know Your Customer (KYC)
- Legal nature of blockchains including territoriality and liability
- Recognition of blockchains as immutable, tamper-proof sources of truth
- Conciliation of "right to be forgotten" and blockchain's immutability
- Legal validity of documents stored in blockchain as a proof of possession or existence
- Legal validity of financial instruments issued on the blockchains
- Real-world enforceability, territoriality, and liability of smart contracts
- Treatment of shared information in blockchains from the perspective of cross-border flow of data and data protection
- Use of the blockchain as a valid ruling register for the IoT
- Regulatory reporting information standards definition on the blockchain
- Definition of a regulatory sandboxes approach to test blockchains

In the contemporary digital world, financial system across the globe is governed by combination of technical and legal codes. Therefore, to introduce the blockchain technology into the financial system, regulators have certain questions to be answered [23]:

- Do regulators make rules?
- Are the rules fixed or changeable?
- In case of fraud, can regulators access the data to investigate it?
- Blockchain technology is garbage-in and garbage-out, who will maintain quality of data?

Garcia-Teruel [24] highlighted that in real estate sector, the following legal challenges need to be addressed for an efficient implementation of blockchain technology:

- Verification of identity of the parties: most of the blockchains does not require any personally identifiable information (PII) to create new wallet, and thus if any financial transaction is complete without proper identification, that transaction is illegal.
- Control of legality and effectiveness of the contract: in a mortgage loan, obligation of detecting and informing parties with regard to possible unfair terms before it got approved. Blockchain technology is a distributed system that does not need any legal checks before approving the loan.

Table 1 DLT features and regulatory challenges [26]

Feature	Samples of regulatory challenges
Distribution, shared ledger	Applicable law with respect to nodes set up in different states Legal subjects in multiple jurisdictions Distributed storage solutions to meet the requirements of production environments Interoperability requirements New civil or commercial law forms, organizations, and contracting Protection of secrecy in open environments
Autonomy and responsibility	Legal smart contract definition and enforceability (valid source code execution) Boundaries of anonymity Applicable law Liability of smart contract managers (SC layer governance) Intellectual property of code
Tamper evidence and resistance	Regulation that needs the correction or removal of data in the ledger: Data protection laws/right to be forgotten Content that infringes on third parties' rights (e.g., copyright, trademark, etc.) Illegal content
Incentive mechanism and digital assets	Coin, token, tokenization legal common (UNCITRAL) definition ICO definition and minimal requirements for investor protection Crypto asset/token financial system: legal concept and boundaries Supervisory policies and procedures by applicable rules
Openness and transparency/anonymity	AML issues, secrecy leaks, personal security Anonymization (no name/encrypted users vs KYC) and pseudonymization

- Co-ownership and other rights in rem: in EU governments should agree for particular properties to change ownership, and it is not possible in smart contract.
- Amendment of the ledger: human errors may happen during registration of any property, and this type of cases cannot be handled in blockchain technology.

One of the approaches to overcome the challenges and regulate the blockchain technology is to develop blockchain standards in alignment with the prevailing regulatory standards for cybersecurity, risk management, cloud computing, and financial services [25].

ITU-T focus group on application of blockchain and DLT has analyzed selected features of DLT and their regulatory challenges. More details about the DLT features and regulatory challenges are mentioned in Table 1.

ITU proposed recommendations for each challenge for the users as well as the regulators, and these are not discussed in detail in this manuscript. The selected DLT properties are:

- Distribution and ledger sharing
- Autonomy and responsibility
- Tamper evidence and resistance
- Incentive mechanism and digital assets

- Openness, transparency, and anonymity

The regulatory challenges for the DLT attribute distribution and ledger sharing are:

- Suitability of laws to nodes developed in different states
- Responsible subjects in various jurisdictions
- Production servers' storage locations
- Heterogeneity of operating systems, programming languages, and nodes' management at various locations
- Digital civil or commercial law agreements like multilateral association agreements
- Various countries' data protection rules
- Data collection, management of data, and analysis of data outside the country boundaries

The regulatory challenges for the DLT attribute autonomy and responsibility are:

- Legalization and enforcement of smart contract
- Automatic decision-making (ADM) as it is very complex and less transparent
- Limitations of legal liability for actors who play the key role in information system operation

The regulatory challenges for the DLT attribute tamper evidence and resistance are:

- Managing technological changes
- Correction or removal of personal and nonpersonal data in the ledger

The regulatory challenges for the DLT attribute incentive mechanism and digital asset are:

- Legal definition of the terms coin, token, and tokenization
- Definition for initial coin offerings (ICO) and set minimal requirements to protect investors
- Boundaries for the crypto asset/token financial system
- Supervisory policies and procedures by applicable rules

The regulatory challenges for the DLT attribute openness, transparency, and anonymity are [26]:

- Auditing issues due to high levels of privacy
- Competition challenge due to complete transparency

Across the globe, some countries are already working on overcoming the abovementioned challenges of blockchain technology in collaboration with industry leaders, academicians, legislators, regulators, and governments. Similarly, as there are no stipulated standards and policies in Qatar on the blockchain technology, Qatari regulators should develop policies and standards to be one of the top leaders in the arena of emerging technologies.

5 Discussion

Blockchain and its DLT present a lot of advantages and benefits such as safety, traceability, and cost-effectiveness, which are considered as key elements in the supply chains sector, where many players are committed from the early production's stage to the market handover. Those players are mainly producers, suppliers, consumers, and policy makers who are brought together via blockchain technology such as DLT and smart contracts to improve the overall effectiveness of their sector [27]. However, the role of regulators remains far away due perhaps to their affiliation to different organizations that are using different programs and applications [28]. Kamilaris et al. stated in their study [29] that any kind of digital assets (cryptocurrencies) cannot be trusted in food supply chains without a form of policies that make it a complete solution; hence, the absence of common regulation on how blockchain technology should be used is still persisting.

According to MarketsandMarkets, the global blockchain market size is projected to grow from USD 258 million in 2020 to USD 2409 million by 2026, at a compound annual growth rate (CAGR) of 45.1% during the forecast period [30]. In the same vein, the blockchain market size in Qatar was projected at USD 0.8 million in 2018 and is estimated to grow by 120% annually and will reach USD 19.4 million in 2022.[11] To capture Qatar's blockchain market, several public and private organizations have started several projects to work on blockchain technologies. Some of the initiatives in Qatar are made through Qatar National Research Fund agency (a member of Qatar Foundation) in different sectors such as finance and FinTech, logistics and supply chains, energy, and smart grids. Such developments are made in collaboration with several higher education institutions such as Qatar University and Hamad Bin Khalifa University. The latest QNRF ROS[12] seminar highlighted some of these initiatives. Some of them are made in partnership with local stakeholders, such as ministries and local industries. For instance, Qatar University and the Royal Melbourne Institute of Technology (RMIT) of Melbourne are currently implementing the SupplyLedger on efficient blockchain-based supply chain systems, involving MOTC and Qatar Railways Company as stakeholders. MOTC as government authority responsible for land transport, maritime transport, information technology, digital society development, and cybersecurity is looking to the outcome of the project toward issuance of new policies and regulations related to the adoption of blockchain technology for the supply chain in Qatar. Qatar Rail which is the responsible authority for the country's new rail network, including

[11] https://tdv.motc.gov.qa/Investment-Catalogue/Blockchain

[12] https://www.qnrf.org/en-us/Newsroom/Press-Releases/fintech21-research-outcome-seminar

Doha Metro and Lusail smart city Tram, is collaborating as technical partner for the proof of concept related to the logistics sector. Hamad Bin Khalifa University team has developed a smart contract-based energy trading platform, using a specialized Ethereum blockchain network. This platform supports energy providers to directly trade their energy surplus with electric vehicle owners in a peer-to-peer manner. A last example is related to MEEZA, a local IT services and solutions provider, which partnered with the CWallet to power the blockchain-based digital wallet platform services. This platform ensures that personal data of MEEZA users is protected at all costs with highest standards.[13]

6 Conclusion

The increasing evolution's pace of the emerging technologies, such as blockchain and its DLT, rises a critical need to revise and/or enforce many of today's regulations, especially those related to new network-based technologies. Indeed, the existing rules' obsoleteness does not frame these emerging technologies. Decision-makers and governments across the globe should consider making ready an adequate regulatory environment in order to facilitate the adoption/implementation of such technologies. This should incorporate a set of standardized frameworks and best practices to take up the full benefit of these new technologies. We have described in this paper the existing regulation landscape related to blockchain and its DLT highlighting some challenges and ways to overcome them.

Acknowledgments This publication was made possible by NPRP grant NPRP11S-1227-170135 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

References

1. Marsal-Llacuna, M.-L., & Oliver-Riera, M. The standards revolution: Who will first put this new kid on the blockchain? In *2017 ITU kaleidoscope: Challenges for a data-driven society (ITU K)* (Vol. 2017). IEEE.
2. Hyland-Wood, D., & Khatchadourian, S. (2018). A future history of international blockchain standards. *The Journal of the British Blockchain Association, 1*(1), 3724.
3. Gramoli, V., & Staples, M. (2018). Blockchain standard: Can we reach consensus? *IEEE Communications Standards Magazine, 2*(3), 16–21.
4. Deshpande, A., et al. (2017). Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards. In *Overview report* (p. 40). The British Standards Institution (BSI).

[13] https://www.meeza.net/?s=CWallet&lang=en

5. Kakavand, Hossein, Nicolette Kost De Sevres, and Bart Chilton. "The blockchain revolution: an analysis of regulation and technology related to distributed ledger technologies." Available at SSRN 2849251 (2017).
6. Wang, Q., Min, S., & Li, R. (2020). Is China the world's blockchain leader? Evidence, evolution and outlook of China's blockchain research. *Journal of Cleaner Production*, 121742. Weernink, Marissa Oude, et al. "The blockchain potential for port logistics." (2017).
7. Bocek, T., et al. (2017). Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In *2017 IFIP/IEEE symposium on integrated network and service management (IM)*. IEEE.
8. Jiang, S., et al. (2018). Blochie: a blockchain-based platform for healthcare information exchange. In *2018 IEEE international conference on smart computing (smartcomp)*. IEEE.
9. Esposito, C., et al. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Computing, 5*(1), 31–37.
10. Carson, B., et al. (2018). *Blockchain beyond the hype: What is the strategic business value* (pp. 1–13). McKinsey & Company.
11. Mason, J. (2017). Intelligent contracts and the construction industry. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction, 9*(3), 04517012.
12. Giuda, D., Martino, G., et al. (2020). The construction contract execution through the integration of blockchain technology. In *Digital transformation of the design, construction and management processes of the built environment* (pp. 27–36). Springer.
13. Xiong, F., et al. (2019). A key protection scheme based on secret sharing for blockchain-based construction supply chain system. *IEEE Access, 7*, 126773–126786.
14. Lamb, K. "Blockchain and smart contracts: What the AEC sector needs to know, 2018."
15. Deloitte. (2020). *Deloitte's 2020 global blockchain survey from promise to reality*. Deloitte Insights.
16. Al Salmi, H. (2020). Blockchain in post-trade: Blocked by regulations and legal challenges. *Journal of Securities Operations & Custody, 12*(1), 21–28.
17. Sakho, S., Jianbiao, Z., Essaf, F., & Mbyamm Kiki, M. J. (2019). Blockchain: Perspectives and issues. *Journal of Intelligent & Fuzzy Systems, 37*(6), 8029–8052.
18. Jurgita, M. (2018). Blockchain and virtual currency regulation in the EU. *Journal of Investment Compliance, 19*(3), 33–38.
19. Yeoh, P. (2017). Regulatory issues in blockchain technology. *Journal of Financial Regulation and Compliance, 25*(2), 196–208.
20. Harwood-Jones, M. (2016). *Blockchain and T2S: A potential disruptor*. Standard Chartered Bank.
21. De Filippi, P., & Hassan, S. (2018). *Blockchain technology as a regulatory technology: From code is law to law is code*. University of Illinois at Chicago Library.
22. Cermeño, J. S. (2016). Blockchain in financial services: Regulatory landscape and future challenges for its commercial application. *BBVA Research Paper, 16*(20), 1–33.
23. Ozili, P. K. (2019). Blockchain finance: Questions regulators ask. In *Disruptive innovation in business and finance in the digital world* (pp. 123–129). Emerald Publishing Limited.
24. Garcia-Teruel, R. M. (2020). Legal challenges and opportunities of blockchain technology in the real estate sector. *Journal of Property, Planning and Environmental Law., 12*(2), 129–145.
25. Meguerditchian, V. (2017). *Roadmap for blockchain standards report*. Standards Australia.
26. ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT). (2019). *Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework*.
27. Li, Zhi, et al. (2018). Toward open manufacturing. *Industrial Management & Data Systems*.
28. Lee, Hau L., et al. (2017). *Technology in agribusiness: Opportunities to drive value*. White paper.
29. Kamilaris, A., Fonts, A., & Prenafeta-Boldύ, F. X. (2019). The rise of blockchain technology in agriculture and food supply chains. *Trends in Food Science & Technology, 91*, 640–652.
30. MarketsandMarkets. (2020). *Blockchain IoT Market by Component (Hardware (IoT Sensors & Crypto-Wallets), Software and Platform, and Services), Application (Smart Contract, Security, and Asset Tracking and Management), Organization Size, Vertical, and Region – Global Forecast to 2026*. MarketsandMarkets.

TMSLedger: A Transactions Management System Through Integrated Odoo Hyperledger Smart Contracts

Abdelhak Belhi, Houssem Gasmi, Assam Hammi, Abdelaziz Bouras, Belaid Aouni, and Ibrahim Khalil

1 Introduction

In the design and manufacturing of products, many actors in a supply chain scenario interact with each other to manufacture a product. These communication channels are intended to be used for the exchange of goods and services between these actors. However, the complexity often increases exponentially with new actors, and effectively managing the good communication between these actors and securing their transactions becomes quite a complicated task. Issues related to traceability, transparency, sustainability, reliability, and efficiency often arise in highly collaborative scenarios involving many stakeholders.

Proven in the financial sector and logistics industries, blockchain technology is a collaborative platform that guarantees the security of transactions by design with advanced consensus and cryptography mechanisms. It has the particularity of allowing trust between collaborators without being dependent on a third party or a regulatory authority. There are many types of blockchains as one can find fully public blockchains, widely used with cryptocurrencies, and licensed blockchains (private or consortium) which are used in commercial and industrial applications.

A. Belhi (✉)
Joaan Bin Jassim Academy for Defense Studies, Doha, Qatar

H. Gasmi · A. Hammi · A. Bouras
Computer Science and Engineering, College of Engineering, Qatar University, Doha, Qatar
e-mail: houssem.gasmi@qu.edu.qa; assam.hammi@qu.edu.qa; abdelaziz.bouras@qu.edu.qa

B. Aouni
College of Business and Economics, Qatar University, Doha, Qatar
e-mail: belaid.aouni@qu.edu.qa

I. Khalil
School of Computing Technologies, RMIT University, Melbourne, VIC, Australia
e-mail: ibrahim.khalil@rmit.edu.au

A. Bouras et al. (eds.), *Blockchain Driven Supply Chains and Enterprise Information Systems*, https://doi.org/10.1007/978-3-030-96154-1_11

What is unique about these supply chains is that they often include many participants who interact with each other to make a product. Problems such as intellectual property, deadlines, product quality, etc. are directly linked to the effectiveness of cooperation with these actors. In traditional systems, it is often extremely difficult to track and identify communication problems. However, blockchain has proven to be an architecture that solves such challenges through design.

Blockchain technology has many advantages, but unfortunately does not have the ability to easily adapt to existing collaborative platforms, especially in the industrial sector despite the fact that it is considered disruptive and has a lot of potential [1–3].

Blockchain is now being integrated into many applications in domains related to manufacturing, supply chains, etc. However, due to the complexity and nature of the established platforms, blockchain integration is far from being a straightforward task due to the difference in architecture and the way transactions are executed.

Through this chapter, we study the integration of blockchain with industrial information systems focusing on a simple manufacturing supply chain case study. We propose a proof of concept of blockchain integration through a popular open-source blockchain platform and an enterprise information system. For this task, we selected the Odoo framework which is an open-source platform for developing a wide variety of enterprise information systems. The processing of transactions and their critical data storage will then be offloaded from the Odoo framework to be handled by blockchain smart contracts as well. For this task, we selected the Hyperledger Fabric blockchain development platform. Hyperledger Fabric allows the creation of blockchain smart contracts. The two platforms (Odoo and Hyperledger) were selected as they are open-source, which facilitates the development of our integration approach. As per the architecture, we mostly focus on a broker-based integration consisting of a software component that is integrated with Odoo and communicates with the blockchain network to manage Odoo workflow processes using customized smart contracts. We present our proof of concept which is based on an exemplar small-scale manufacturing supply chain and demonstrate how can blockchain be integrated into this scenario (see Fig. 1).

The remainder of this chapter is organized as follows. In Sect. 2, we present a state-of-the-art overview of related works on blockchain integration in the context of industrial applications. In Sect. 3, we present our integration method for integrating blockchain through Hyperledger smart contracts with the open-source supply chain/PLM platform Odoo. The choice of this platform was mainly due to its openness and the availability of its documentation. However, such integration should also be possible with platforms allowing API integration. In Sect. 4, we present the implementation of our approach. Finally, we draw our conclusion in Sect. 4 and highlight a set of future challenges.

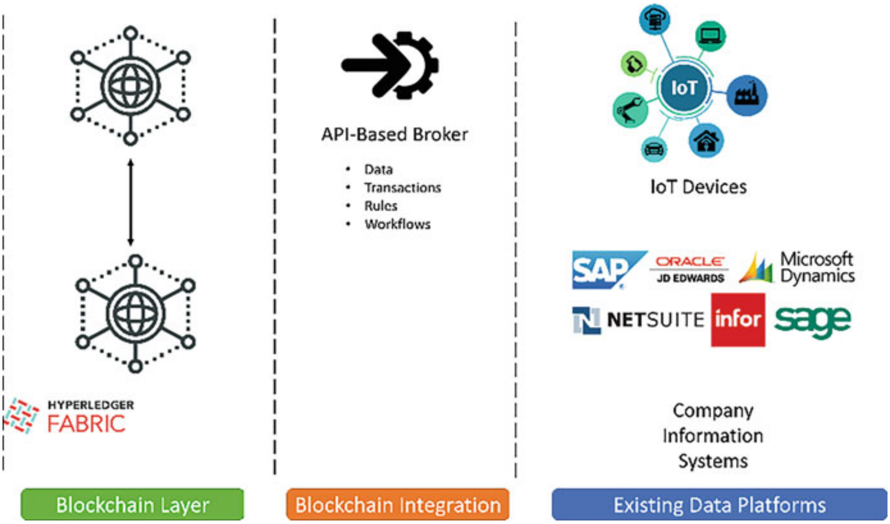


Fig. 1 Integration of industrial information systems highlight

2 Related Work

Since its financial success, blockchain is deemed a disruptive technology in several sectors due to its concept of securing transactions by design. In modern industrial applications, IoT device management is one of its great uses as it ensures the security of sensor and device data from end to end [4, 5]. Blockchain is now considered as an enabling technology for the effective implementation of decentralized applications and was found to enforce the United Nation's sustainable development goals in modern companies [6]. It had been the subject of many contributions related to smart manufacturing and Industry 4.0.

Numerous contributions investigated blockchain integration with different facets of supply chain management. A review of recent applications involving blockchain in the context of supply chain management was presented in [7]. In [8], the authors perform an empirical study involving blockchain integration on operation management and manufacturing and present a detailed analysis of potential drawbacks and obstacles that prevent its effective integration. The authors of [5] study the integration of blockchain, the Internet of Things (IoT), and machine learning for enhancing quality control in smart manufacturing. The authors of [9] study the impact of blockchain integration with supply chains in the context of additive manufacturing. In [10], the authors present a novel blockchain-based application to maintain productivity in the context of automotive spare parts manufacturing. From a more practical point of view, the authors of [11] present a novel blockchain-based service composition model called Block-SC in the context of cloud manufacturing (CM) aiming at providing an efficient collaboration platform of service composition.

In [12], the authors present a new blockchain-based shared manufacturing framework enabling peer-to-peer resource sharing while preserving trust using a smart contract network and a proof-of-participation consensus mechanism. A blockchain-based architecture of cyber-physical systems in the context of manufacturing was presented in [13]. A contribution name "ManuChain" investigated the combination of a permissioned blockchain model with a holistic optimization model.

In the context of supply chain management, numerous applications have been proposed. The authors of [14] presented the use of design tools and ontologies to develop blockchain-based supply chains where they translated traceability information into smart contracts to enforce the domain constraints. In [15], the authors proposed a model of integration between supply chains and blockchains. The authors of [16] proposed applying blockchain technology to architect an industrial platform powered by a product-centric information management system. A study of blockchain integration with aircraft parts supply chain was presented in [17]. The authors used a blockchain, not only for traceability but also for parts usage and performance monitoring which positively impacted safety and data integrity.

From a manufacturing perspective, moving to the era of Industry 4.0, smart manufacturing is becoming a reality through emerging technologies such as blockchains, Internet of Things (IoT), cloud manufacturing (CM), and artificial intelligence (AI). Manufacturing giants such as BMW and Ford are adopting blockchain technology to improve the efficiency of their supply chains and attain business innovation. Leading technology companies and innovative start-ups collaborated to create the Trusted IoT Alliance which aims to develop the necessary standards to integrate blockchains and IoT. The main goal of the standard is to develop smart contract interfaces that enable the exchange of data between blockchain-enabled systems. The alliance efforts are focused on using blockchains for the trusted identification of hardware and documentation immutability.

To encourage the adoption of blockchains by the industry, the cloud-based blockchain as a service (BaaS) was proposed by various vendors. Businesses can use this cloud-based solution to develop, host, and use their blockchain applications which include their smart contracts through a blockchain infrastructure that is developed by a vendor. It provides tools that simplify the management and deployment at scale. Similar to the increasing trend of software as a service (SaaS) where access to the software is granted on a subscription-basis, BaaS enables businesses to tap into a blockchain network using its configuration without having to invest in developing their blockchain infrastructure and without requiring in-house expertise in the subject especially for resource-constrained enterprises [18].

The Mobility Open Blockchain Initiative (MOBI) is an initiative formed by giant automotive companies such as General Motors (GM), Ford, and BMW to help in making automobiles safer, more affordable, and accessible using blockchain technology. To give new cars a digital entity, MOBI specified the first blockchain-based car identity standard. This enables the tracking of significant events during the lifetime of the car. The blockchain digital identity can also be used to exchange information between cars such as location, speed, travel direction, driver behavior, and even driver intention predictions [19].

Blockchains are very resilient platforms that have multiple advantages in collaborative applications. Unfortunately, a lot of work has to be undertaken in order to achieve a smooth and seamless integration. There seems also a lot of interest to integrate this technology in manufacturing and supply chains as it enables a whole wider spectrum of applications and opens the way for peer-to-peer trust.

3 Broker-Based Manufacturing Workflow Management Through Smart Contracts

In this section, we present our proposed architecture as well as a proof-of-concept integration between an established small-scale manufacturing supply chain and a permissioned blockchain. As it is known, most industrial information systems are based on a client/server architecture where information and processing are centralized. This has some advantages but presents various risks related to security, availability, and trust. Indeed, systems such as ERP, PLM, WMS, and TMS are some of the highly collaborative industrial applications, and yet their information is somehow centralized [20, 21]. Blockchain, since its revolution in the financial sector, was considered a disruptive technology as it renews or redefines the concept of trust between peers and introduces new mechanisms for establishing peer-to-peer transactions while ensuring security among other benefits through concepts such as consensus, etc. Our solution shifts the management of business workflows from a centralized ERP platform (Odoo) to a distributed blockchain platform (Hyperledger). This means that the tracking of a transaction is more robust and also all transactions are final (see Fig. 2). In the following, we present details of our solution by presenting its design principle, architecture, studied proof of concept, as well as some tests and evaluations.

3.1 Case Study Scenario

The scenario of the case study (highlighted in Fig. 3) consists of the following actors:

- *Customer:* a food factory that needs a new machine to improve its efficiency and increase its production
- *Designer:* a design firm specialized in industrial machines design
- *Manufacturer:* bespoke machine manufacturing company
- *Supplier:* raw materials supplier
- *Transporter:* goods transportation company

The supply chain starts with a customer which wants to get a design for a machine. He formulates his requirements in a document and sends it to a designer

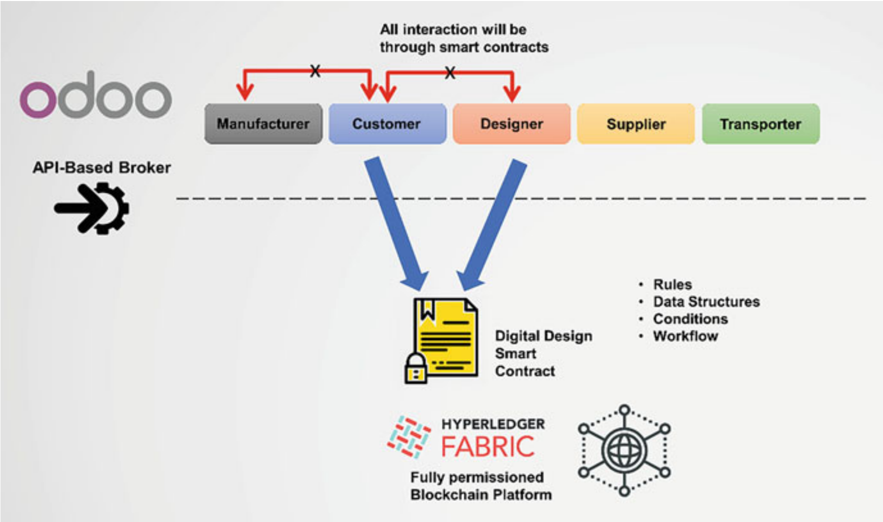


Fig. 2 Integration higher-level architecture

for quotations. The designer then evaluates the financial standing of the customer and upon satisfying a certain rating, prepares the design and sends it to the customer. If the customer accepts a design, the typical transactions between him and the designer take place (quotation, invoice, etc.). Once the design is finished, it is delivered to the customer who will, in turn, send it to a manufacturer with the same interaction patterns. The presentation of the case study focused mainly on the interaction between the customer and the designer where the following aspects are highlighted:

- The smart contracts representing the different actors in the blockchain such as the customer, designer, and manufacturer
- The smart contracts representing the transactions between actors such as the one representing the relation between the customer and designer
- The representation of the domain entities such as design and quotation
- Asset transfer in the blockchain, for instance, transferring the ownership of the design from the designer to the customer and vice versa.
- Create and transfer fungible tokens using an account-based model for payment aspects
- Establishing private channels between groups of actors in the blockchain

The system has been implemented using the Hyperledger Fabric platform as it is the most suitable platform allowing a permissioned access to the blockchain besides other features that will be highlighted in the next sections.

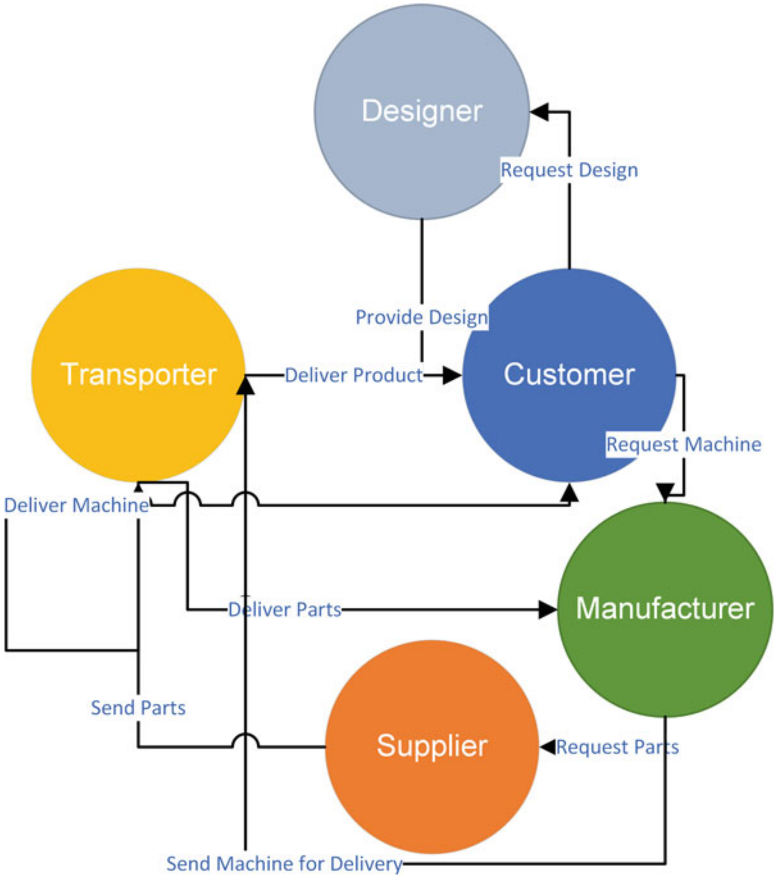


Fig. 3 Proof-of-concept supply chain

3.2 Architecture and Design

When analyzing blockchain frameworks such as Ethereum and Hyperledger, it turned out that these frameworks, in addition to providing core blockchain transaction concepts and data storage, provide a rich and well-established programming interface allowing to run the decentralized transactions through smart contracts performing changes to blockchain data.

Our goal through this chapter is to manage the supply chain workflows as well as the transaction in the Odoo ERP/PLM framework using Hyperledger Fabric smart contracts. However, to ensure the soundness of the system and to guarantee the integrity of data when combining both platforms, there needs to be a one-to-one mapping between the data and the business logic in both platforms. This can be achieved using one of our proposed integration strategies. The first strategy (see

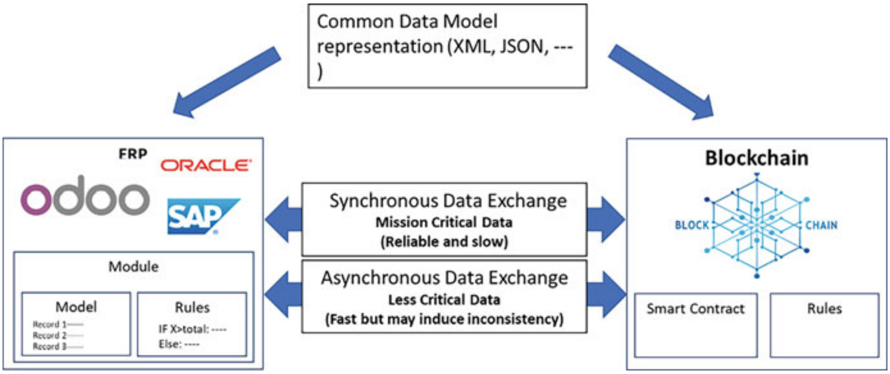


Fig. 4 Common model integration architecture

Fig. 5 Existing ERP integration architecture

Fig. 4) assumes that a fresh implementation of an industrial information system such as an ERP will be established and thus maintains interoperability between both platforms by design. It uses a common data model regrouping rules and data structures written in a markup language such as XML or JSON. A translation module is implemented in each platform, and a library written in Python is used in our example with the Odoo ERP platform, and another one written in JavaScript for Hyperledger.

The second strategy (see Fig. 5) assumes that both platforms are independent from each other, and a software component called an "Integration Broker" acts as a messaging platform between both systems. This broker can be compared to an API but it implements advanced functionality and does not perform actions by itself. Instead, it connects to the blockchain via the Hyperledger JavaScript SDK and provides a RESTful API which is used by Odoo to interact with the Hyperledger smart contracts.

In our proof of concept, we only included our second integration strategy based on the Integration Broker. The first strategy is currently under development and will be subject to our future work.

As per the workflow management, we concluded that managing workflows in both platforms can be risky and might induce errors due to communication issues and trust challenges. In our integration, all critical workflow management

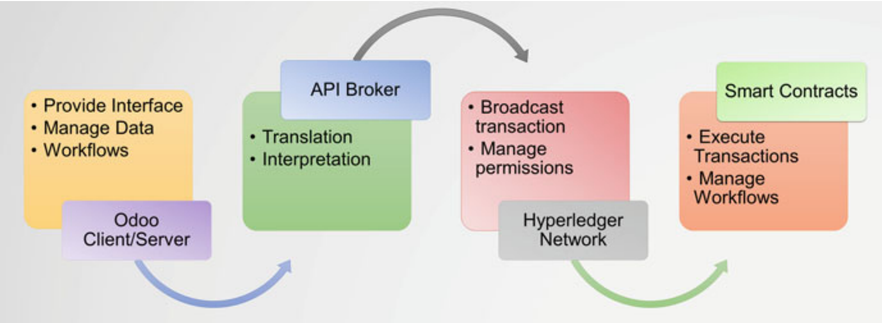


Fig. 6 Integration data flow

happens through the blockchain using smart contracts. For each workflow, a smart contract involving the collaborating actors and making all necessary data controls is established and instantiated following the steps highlighted below:

1. Assuming that transaction or workflow processes have been already established and coded in a smart contract template (JavaScript used in our experiments with Hyperledger), the smart contract is instantiated between the collaborating actors.
2. Following instantiation, the information is naturally broadcasted to all blockchain nodes (by design). All participating nodes have the same blockchain data (data + smart contracts). A strong consensus mechanism manages the consensus of the data. No further modifications are possible to the structure of the contract other than the ones defined before the instantiation.
3. The workflow process is managed using the methods and procedures defined in the smart contract template. These methods, when triggered, are executed in all nodes, and the consensus is preserved by design.
4. When the workflow is completed, the contract will be still instantiated in the blockchain. No further action can be performed including the deletion of the contract or the data, as all blockchain transactions and data are final.

The following figure (Fig. 6) summarizes the data flow between the integration framework components.

Following the definition of the design principle and the establishment of a small supply chain to develop our proof of concept, we established the integration using the broker-based solution as it is more suitable for existing ERP installations and is more straightforward in terms of implementation. Although we already started working on the common meta-model solution, it turned out to be much harder than the broker-based one in terms of implementation and will be subject to our future contributions.

4 Blockchain Implementation

For the proof-of-concept implementation, we used JavaScript as the implementation language for smart contact and hosted the Hyperledger Fabric on Linux as it uses Docker extensively which is recommended to run on Linux to avoid technical issues. The different aspects of the implementation are presented in the next sections.

4.1 Domain Entities

The use case consists of the domain concepts such as design, design request, quotation, invoice, receipt, etc. So how are these concepts created in the blockchain? All concepts in the blockchain are inherited from a class called *State* predefined in Hyperledger Fabric (Fig. 7). It has a unique key and a life cycle current state of the concept where the key and current state are determined by the specific subclass. The class has also helper functionality to convert to and from the JSON format. An example domain concept in the system is the *IndustrialDesign* concept. To define it, we inherit from the *State* class and add the entity-specific properties. The *currentState* and *currentFeeState* are defined as enumerated values. The *createInstance* method is used to generate instances of the entity.

Domain entities are typically initiated in smart contracts either to create a new instance such as a new Invoice or retrieved as an existing instance from the database for further processing. The definition of entities can be nested, for instance, the *Invoice* is composed of a list of *LineItems* which is also defined in the same manner by extending the *State* class.

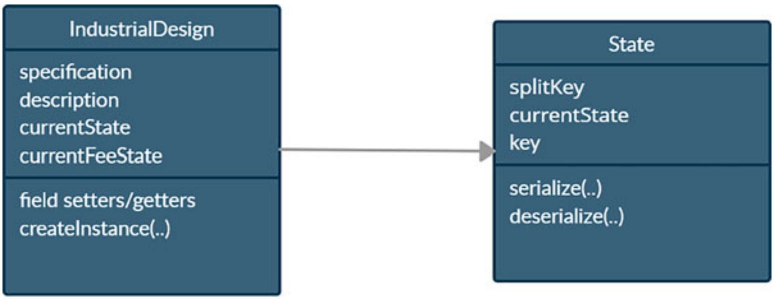


Fig. 7 Concept representation in Fabric

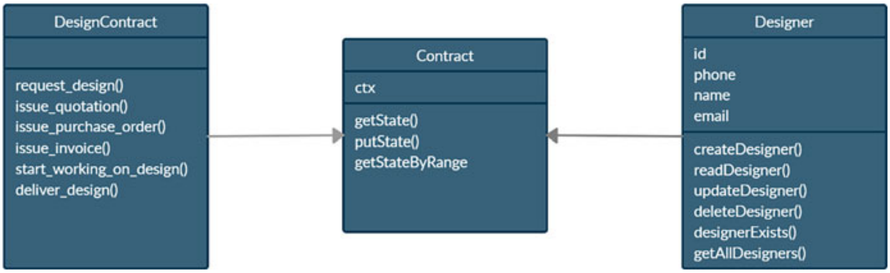


Fig. 8 Smart contracts in Fabric

4.2 Smart Contracts

Smart contracts in the blockchain are used in our case study to represent two concepts: the actors in the system such as the customer and the relation between actors such as the relation between the customer and the designer. All smart contracts inherit from the *Contract* class as shown in (Fig. 8). The smart contracts for the actors in the system contain mainly the Create, Read, Update, Delete (CRUD) operations.

All the *Designer* methods take as a first argument a *ctx* variable that represents the blockchain context. This variable is used to manipulate the entity in the blockchain, for instance, to store a *Designer* in the blockchain, we invoke the *ctx.putState()* method. The relation between actors of the system is governed by smart contracts which are defined in Fabric as a regular class where the methods of the class represent the contract clauses that should be honored (Fig. 8). For instance, the relation between the *Customer* and the *Design* is defined in the *DesignContract* class as follows:

Smart contract 1: Request an IndustrialDesign from a designer
Input:*ctx, requester, designer, design_code, spec, description, requestDate*
Retrieve the customer(*requester*)
Create design request(*requester, designer, design_code, spec, de-scription, requestDate*)
If*customer_credit_rating* > *3***then**
Set design state(*ACCEPTED*)
end
else
Set design state(*REJECTED*)
end
Store the design(*contract_id, design*)

As with entities, the smart contract functions also require the passing of the blockchain context variable *ctx* to access the blockchain database. Another example is the *design delivery* smart contract which is defined as follows:

Smart contract 2: Deliver the design to the customer
Input:*ctx, contract_id*
design ← retrieve the design contract(*contract_id*)
job_days ← get the difference between the request date and today(*contract_id*)
fees_reduction = Update fees based on delay(*contract_id*, *job_days*);
design.fees = *fees* + *fees_reduction*
store_the_design(*contract_id, design*)

This design delivery smart contract calculates the delay in the delivery of the design and based on that update the agreed-upon fees. If there is no delay, the *Designer* will be paid full fees; otherwise, his fee will be deducted according to the length of the delay.

4.3 Asset Transfer

Transferring assets between supply chain members in the blockchain is just a matter of changing an attribute in an entity to represent the owner. The *pay design fees* smart contract changes the owner of the design from the designer to the customer after settling the payment as follows:

Smart contract 3: Pay design fees
Input:*ctx, contract_id, customer_id*
financial transaction logic [Details in Smart Contract 4]
design ← retrieve the design contract(*contract_id*)
design.owner = *customer_id*
store_the_design(*contract_id, design*)

4.4 Financial Transactions

The financial transactions between supply chain members are implemented using the ERC-20 account-based model [22]. A smart contract can either create or transfer fungible tokens using an account-based model. In this model, there is an account for each participant that holds a balance of tokens. A *mint* transaction creates tokens in an account, while a *transfer* transaction debits the caller's account and credits another account. To test the model, we allowed all the participants to call the *mint* function to create a certain limited amount in their account. The smart contract *mint* function takes the client certificate as the client identity through an API and credits their account with the requested number of tokens. To transfer money to another account, a *transfer* function is called to transfer the requested tokens to the account of the recipient. The recipient should provide their client ID to the sender to complete the transfer. The following is an example of a financial interaction between the *Customer* and the *Designer* where the customer calls the *mint* function to generate 7000 tokens and then transfer 300 to the *Designer*:

Smart contract 4: Transfer money
Input:*ctx, designer_id, customer_id*
mint(*customer_id*, 7000)
customer_balance ← get available mints (*customer_id*) // *output*: 7000
designer_balance ← get available mints (*designer_id*) // *output*: 0
accountId = get account id(*designer_id*)
transfer from customer to designer*(customer_id, accountId, 300);*
customer_balance ← get available mints (*customer_id*) // *output*: 6700
designer_balance ← get available mints (*designer_id*) // *output*: 300

4.5 Private Channel Transactions

Hyperledger Fabric uses an immutable ledger for each channel in addition to the chaincode that manipulates the state of assets. This ledger either can be visible to all the network participants or can be limited to a specific subset of participants. In the latter case, participants will have their segregated transactions and ledger. To balance between total transparency in the network and the needed privacy between subgroups of participants, we created dedicated channels for subsets of participants and authorized them to use their private data. We further obfuscated the data by encrypting the values in the chaincode using the AES cryptographic algorithm before sending it to the ordering service which will append it to a block in the ledger. The encrypted data in the ledger can only be decrypted using the user key that was used to encrypt the data.

4.6 Blockchain Integration

As discussed before, we selected the Odoo open-source platform as an industrial information system and the Hyperledger Fabric as the blockchain platform. We established a small manufacturing supply chain scenario involving five actors being customer, manufacturer, designer, transporter, and supplier. These actors are collaborating in order to make a product. Figure 3 represents a diagram of this supply chain.

All actor interfaces are implemented in Odoo. However, the transactions that are undertaken between actors, which traditionally should be undertaken in Odoo, are performed in the blockchain using smart contracts. Odoo only interacts with the blockchain and triggers critical transactions. All communication between Odoo and Hyperledger is performed using a broker component implemented in Node.JS which conveys all the transactions that will be executed in the blockchain using smart contracts from Odoo. The broker relies on the Hyperledger JavaScript SDK for connecting the broker to the blockchain network. A RESTful API was established to allow secure and reliable communication between Odoo and Hyperledger Fabric. This API implements all the necessary security tools to allow communication between both platforms.

All client interfaces for workflow management were adapted to get use of the API broker. Figure 9 shows the Odoo interface for the design contract between the customer and the designer. The interface implements all the usual UI elements such as lists, etc. The transaction state is the most obvious data field that only gets changed following an invocation of the smart contract associated with the task.

As depicted in Fig. 9, we can see the interface allowing interaction with the design workflow. The current state of the design is a value that is controlled by the smart contract deployed in the blockchain. The colored buttons control the state of the design contract. Switching from a state to another is conditioned by business logic rules that are enforced in both Odoo and the smart contract to ensure the soundness of the system. As an example, the design cannot be moved to the delivered state unless a file is attached. This is enforced in Odoo to notify the user before the action is sent to the blockchain, and if by any chance the restriction in Odoo is not enforced due to an issue or due a tampering attempt, the smart contract will not shift to the delivered state if a file is not attached. Additionally, as can be seen in Fig. 9, it is worth noting the UI element displaying the PDF file of the design was customized by us. Figure 10 shows the Kanban view of the designs organized by their status.

4.7 Tests and Evaluations

To test and evaluate our proof of concept, we implemented the complete workflow of the interaction between the customer and the designer in our small-scale supply chain. In the following, we present the typical workflow of providing a design between the designer and the customer following a request to issue a design coming from the customer. The actor performing these actions is the designer. The contract which is named “Design contract” has six states, three of which are highlighted in this example (2, Initiated; 4, Started working on the design; 6, Delivered). The other

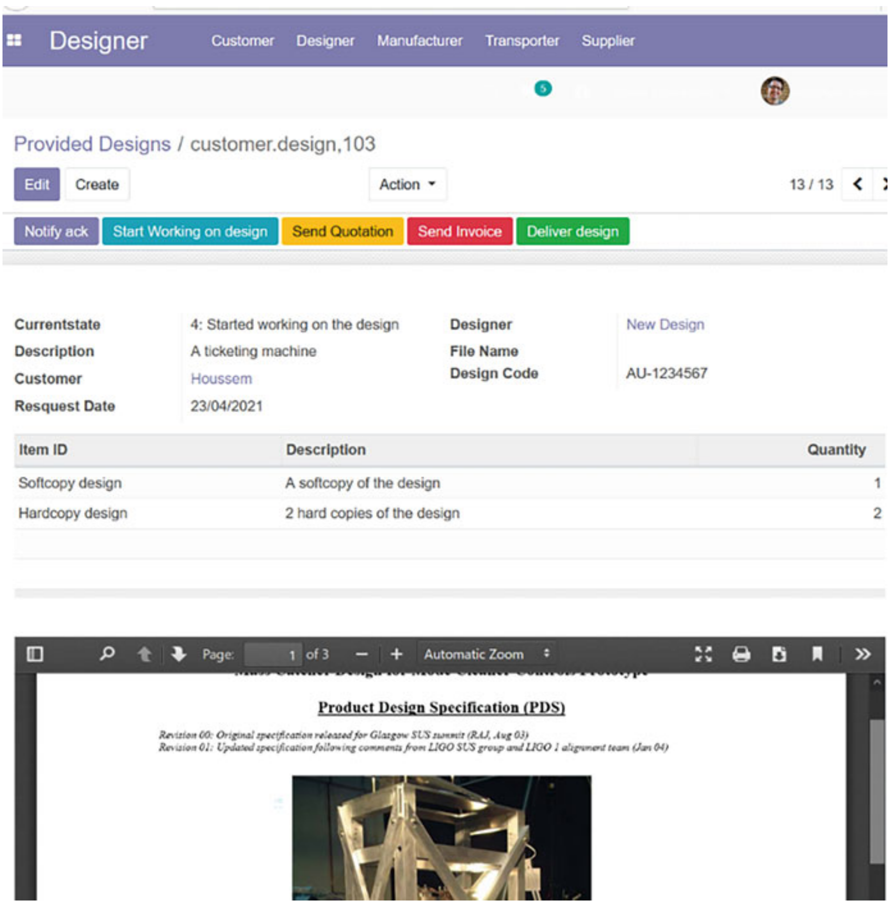


Fig. 9 Odoo interface

states are intermediate states or exceptions. A rule stating that the contract cannot move to the final state (6) unless the design includes a file is included in the smart contract.

1. The **first** step highlighted in Fig. 11 is the initiation of the contract by the customer.
2. The **second** step highlighted in Fig. 12 is the contract state from the perspective of the designer after he acknowledges it and clicks "Start working on the design" button.
3. The **third** step highlighted in Fig. 13 is the design edition interface where all the information, as well as the file, are added.

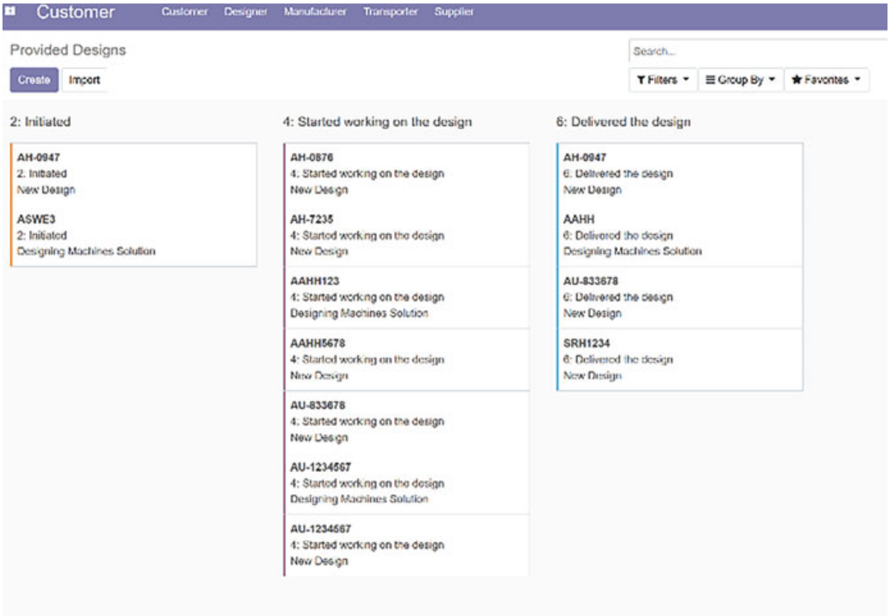


Fig. 10 Designs *Kanban* view (status from the blockchain)

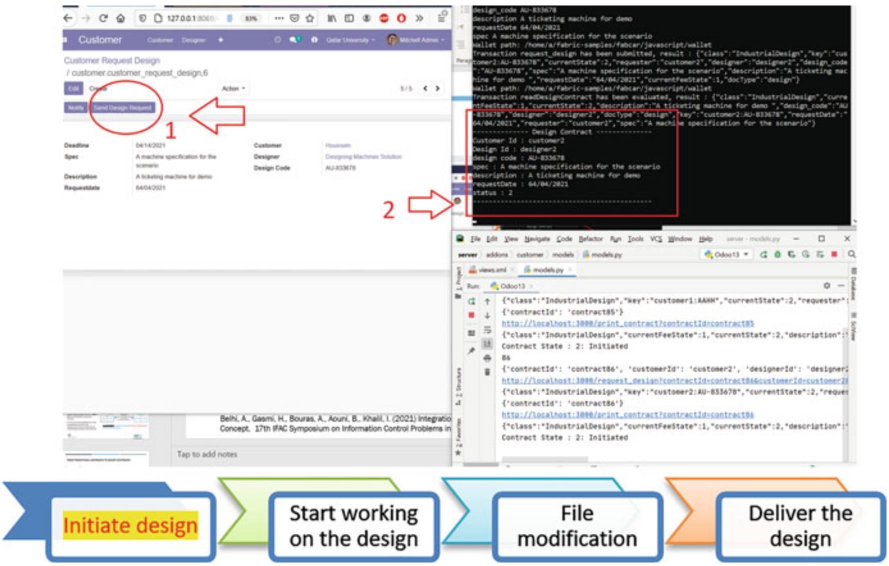


Fig. 11 Customer initiates the design

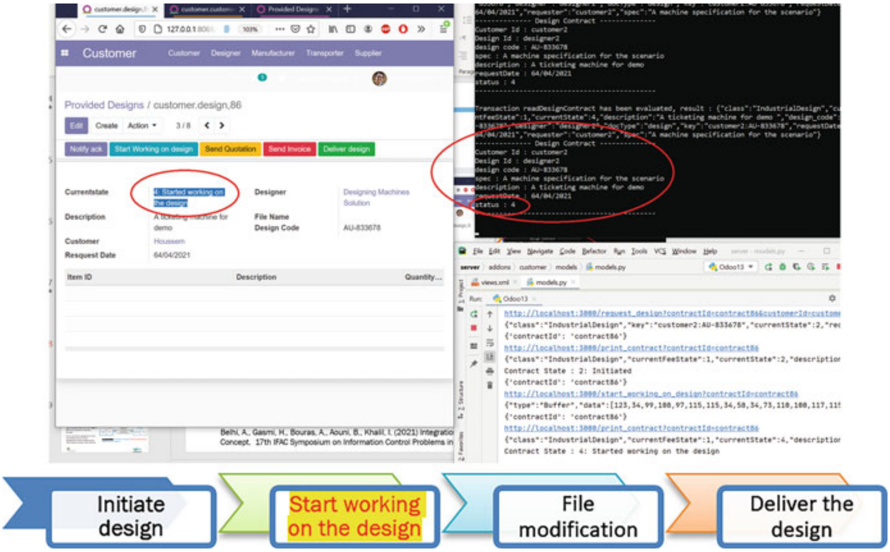


Fig. 12 The designer starts working on the design

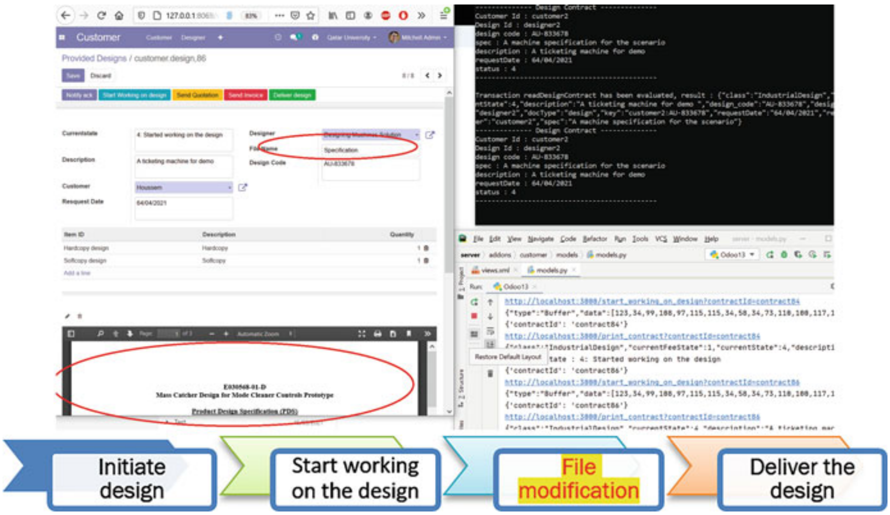


Fig. 13 The designer edits the design and adds the file

4. The **final** step which is highlighted in Fig. 14 is the final step where the designer delivers the design.

As per the evaluation in terms of time. Adding an extra software component indeed adds more complexity. In the synchronous mode and depending on the integration strategy in the API broker, the average delay to get a commit from the

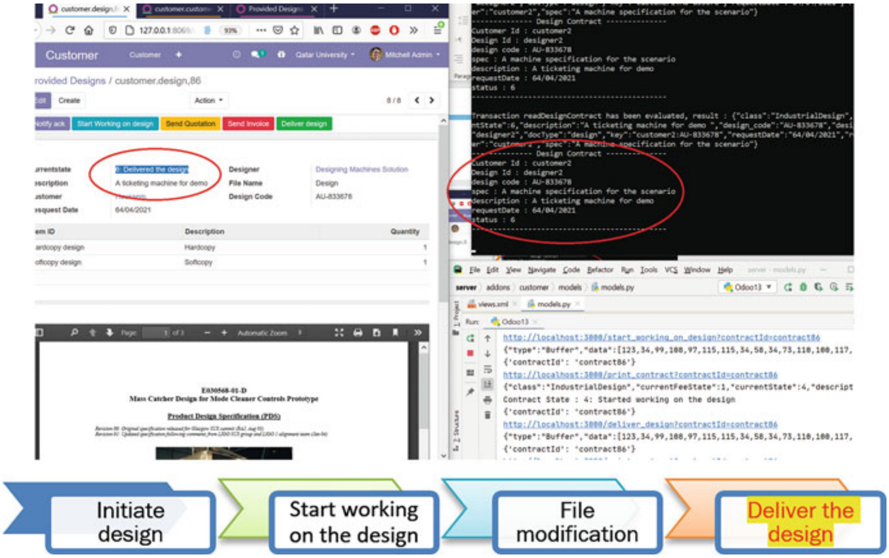


Fig. 14 The designer delivers the design

blockchain in Odoo (bidirectional path) takes between 0.5 s and 2.0 s. This can be seen as tolerable in some cases, but in other cases, it cannot be acceptable. In asynchronous mode, the system has the same transaction execution time as by default. However, Odoo will commit transactions independently from the blockchain. Data integrity checks comparing the state of the data between Odoo and blockchain are used to spot any synchronization issues. We concluded that synchronous mode, which commits data in the blockchain making Odoo depend on 100% from the blockchain, is suitable if the additional wait time of 0.5–2.0 s is tolerable or if the application is very critical. The asynchronous mode does not provide the same level of confidence as actions are committed in each platform independently although a data integrity checking component is present to check the synchronization between each platform.

5 Conclusion

Blockchain's impact on manufacturing and industrial applications was compared by some people to the wheel invention. This disruptive technology showed its potential in revolutionizing product design and manufacturing in many ways. In this chapter, we were interested in ways to integrate this technology with industrial information systems such as PLM, ERP, WMS, etc. We presented a broker-based integration of blockchain smart contracts with industrial workflows. We used Hyperledger Fabric as a permissioned blockchain platform to store the transaction data and manage the life cycle of smart contracts. Hyperledger Fabric was mainly selected as it is an open-source platform used extensively in the enterprise environment. As for the information system, we used Odoo which is an open-source framework written in Python. We presented our proof-of-concept integration with a scenario of a small-scale manufacturing supply chain involving a limited number of actors and demonstrated that the Odoo workflows can easily be adapted to be fully managed using smart contracts, thus increasing the security and enhancing the traceability and trust of critical business transactions. We highlighted the fact that we have two main integration strategies although we only presented a broker-based one. The integration based on the common meta-model (interoperability) will be subject to our future works.

Acknowledgments This publication was made possible by NPRP grant NPRP11S-1227-170135 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors (www.supplyledger.qa).

References

1. Thiraviya Suyambu, G., Anand, M., & Janakirani, M. (2020). Blockchain – A most disruptive technology on the spotlight of world engineering education paradigm. In *Procedia computer science* (pp. 152–158). Elsevier B.V. https://doi.org/10.1016/j.procs.2020.05.023
2. Belhi, A., Bouras, A., Patel, M. K., & Aouni, B. (2020). Blockchains: A conceptual assessment from a product lifecycle implementation perspective. In *IFIP international conference on product lifecycle management* (pp. 576–589).
3. Rahman, M. S., Khalil, I., & Bouras, A. (2021). A framework for modelling blockchain based supply chain management system to ensure soundness of smart contract workflow. In *BT – 54th Hawaii International Conference on System Sciences, HICSS 2021, Kauai, Hawaii, USA, January 5, 2021*., http://hdl.handle.net/10125/71295
4. Pal, K., & Yasar, A. U. H. (2020). Internet of things and blockchain technology in apparel manufacturing supply chain data management. In *Procedia computer science* (pp. 450–457). Elsevier B.V. https://doi.org/10.1016/j.procs.2020.03.088
5. Shahbazi, Z., & Byun, Y.-C. (2021). Integration of blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing. *Sensors, 21*, 1467. https://doi.org/10.3390/s21041467
6. Leng, J., Ruan, G., Jiang, P., Xu, K., Liu, Q., Zhou, X., & Liu, C. (2020). Blockchain-empowered sustainable manufacturing and product lifecycle management in industry 4.0: A survey. *Renewable and Sustainable Energy Reviews, 132*, 110112. ISSN 1364-0321. https://doi.org/10.1016/j.rser.2020.110112
7. Dietrich, F., Ge, Y., Turgut, A., Louw, L., & Palm, D. (2021). Review and analysis of blockchain projects in supply chain management. In *Procedia computer science* (pp. 724–733). Elsevier B.V. https://doi.org/10.1016/j.procs.2021.01.295
8. Lohmer, J., & Lasch, R. (2020). Blockchain in operations management and manufacturing: Potential and barriers. *Computers and Industrial Engineering, 149*, 106789. https://doi.org/10.1016/j.cie.2020.106789
9. Kurpjuweit, S., Schmidt, C. G., Klöckner, M., & Wagner, S. M. (2021). Blockchain in additive manufacturing and its impact on supply chains. *Journal of Business Logistics, 42*, 46–70. https://doi.org/10.1111/jbl.12231

10. Hasan, H. R., Salah, K., Jayaraman, R., Ahmad, R. W., Yaqoob, I., & Omar, M. (2020). Blockchain-based solution for the traceability of spare parts in manufacturing. *IEEE Access, 8*, 100308–100322. https://doi.org/10.1109/ACCESS.2020.2998159
11. Aghamohammadzadeh, E., & Fatahi Valilai, O. (2020). A novel cloud manufacturing service composition platform enabled by blockchain technology. *International Journal of Production Research, 58*, 5280–5298. https://doi.org/10.1080/00207543.2020.1715507
12. Yu, C., Jiang, X., Yu, S., & Yang, C. (2020). Blockchain-based shared manufacturing in support of cyber physical systems: Concept, framework, and operation. *Robotics and Computer-Integrated Manufacturing, 64*, 101931. https://doi.org/10.1016/j.rcim.2019.101931
13. Lee, J., Azamfar, M., & Singh, J. (2019). A blockchain enabled cyber-physical system architecture for industry 4.0 manufacturing systems. *Manufacturing Letters, 20*, 34–39. https://doi.org/10.1016/j.mfglet.2019.05.003
14. Kim, H. M., & Laskowski, M. (2018). Toward an ontology-driven blockchain design for supply-chain provenance. *Intelligent Systems in Accounting, Finance and Management, 25*, 18–27.
15. Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics, 2*, 2.
16. Mattila, J., Seppälä, T., Holmström, J.: Product-centric information management: A case study of a shared platform with blockchain technology. (2016).
17. Madhwal, Y., & Panfilov, P. B. (2017). Blockchain and supply chain management: Aircrafts'parts'business case. *Annals of DAAAM Proceedings, 28*.
18. Singh, J., & Michels, J. D. (2018). Blockchain as a service (BaaS): Providers and trust. *Proceedings – 3rd IEEE European Symposium on Security and Privacy Workshop EURO S PW 2018*, 67–74. https://doi.org/10.1109/EUROSPW.2018.00015
19. Powell, L. M., Schwartz, J., & Hendon, M. (2021). The mobility open blockchain initiative: Identity, members, technologies, and future trends. In *Revolutionary applications of blockchain-enabled privacy and access control* (pp. 99–118). IGI Global.
20. Sureephong, P., Chakpitak, N., Buzon, L., Bouras, A.: Cluster development and knowledge exchange in supply chain., http://arxiv.org/abs/0806.0519, (2008).
21. Khedher, A. B., Henry, S., & Bouras, A. (2011). Integration between MES and product lifecycle management. In *ETFA2011* (pp. 1–8). https://doi.org/10.1109/ETFA.2011.6058993
22. Zahnentferner, J. (2018). Chimeric ledgers: Translating and unifying UTXO-based and account-based cryptocurrencies. *IACR Cryptology ePrint Archive, 2018*, 262.

Index

A. Bouras et al. (eds.), *Blockchain Driven Supply Chains and Enterprise Information Systems*, https://doi.org/10.1007/978-3-030-96154-1