Are smart contracts too smart for Supply Chain 4.0? A blockchain framework to mitigate challenges

Mohamed Grida
Industrial Engineering Department, Zagazig University, Zagazig, Egypt, and
Noha A. Mostafa
Mechanical Engineering Department, The British University in Egypt, Cairo, Egypt and
Industrial Engineering Department, Zagazig University, Zagazig, Egypt

Received 15 September 2021
Revised 15 November 2021
Accepted 14 December 2021

Abstract

Purpose – Smart contracts are self-executing computer programmes that have the potential to be used in several applications instead of traditional written contracts. With the recent rise of smart systems (e.g. Internet of things) and digital platforms (e.g. blockchain), smart contracts are gaining high interest in both business and academia. In this work, a framework for smart contracts was proposed with using reputation as the system currency, and conducts currency mining through fulfilling the physical commitments that are agreed upon.

Design/methodology/approach – A game theory model is developed to represent the proposed system, and then a system dynamics simulator is used to check the response of the blockchain with different sizes.

Findings – The numerical results showed that the proposed system could identify the takeover attacks and protect the blockchain from being controlled by an outsider. Another important finding is that careful setting of the maximum currency amount can improve the scalability of the blockchain and prevent the currency inflation.

Research limitations/implications – This work is proposed as a conceptual framework for supply chain 4.0. Future work will be dedicated to implement and experiment the proposed framework for other characteristics that may be encountered in the context of supply chain 4.0, such as different suppliers' tiers, different customer typologies and smart logistics applications, which may reveal other challenges and provide additional interesting insights.

Practical implications – By using the proposed framework, smart contracts and blockchains can be implemented to handle many issues in the context of operations and supply chain 4.0, especially in times of turbulence such as the COVID-19 global pandemic crisis.

Originality/value – This work emphasizes that smart contracts are not too smart to be applied in the context of supply chain 4.0. The proposed framework of smart contracts is expected to serve supply chain 4.0 by automating the knowledge work and enabling scenario planning through the game theory model. It will also improve online transparency and order processing in real-time through secured multitier connectivity. This can be applied in global supply chain functions backed with digitization, notably during the time of the pandemic, in which e-commerce and online shopping have changed the rules of the game.

Keywords Smart contracts, Digitization, Industry 4.0, Information exchange, Modelling, Supply chains

Paper type Research paper

1. Introduction

For the past three decades, supply chains have been facing several challenges due to the increasing international competition and the complex business requirements. However, even with these challenges, traditional economic and business models were capable of doing the job and achieving the organizational objectives for most of the cases. Nevertheless, the situation has been drastically changed during the past decade, with the major technological advances that have added both opportunities and challenges for modern organizations

Funding: This research did not receive any specific grant from funding agencies in the public, commercial or not-for-profit sectors.

Journal of Manufacturing Technology Management
1741-038X
DOI 10.1108/JMTM-09-2021-0359

(Haddud *et al.*, 2017). A recent major challenge took place with the spread of the COVID-19 global pandemic which shook the world in 2020 and imposed major challenges on global supply chains, especially medical and food supply chains, due to the lockdown and the panic buying in several countries (Sharma *et al.*, 2020).

With the massive shift towards online shopping and e-commerce during the COVID-19 situation, trust and reputation issues are being critical to ensure safe and seamless processes. The e-commerce revenue in the United States has increased by 44% in 2020, and the share of e-commerce in global retail trade has increased from 14% in 2019 to about 17% in 2020 (unctad.org, 2021). Figure 1 shows the US retail landscape in 2020. This occurred due to the lockdown in several countries and the fear of contracting the virus when shopping or having business meetings physically (digitalcommerce360, 2021).

"COVID-19 Is a Crisis of Trust" Khurshid (2020) – therefore, the authors believe that a framework is needed to address *trust* as an asset that has the potential for mitigating challenges in global supply chains during turbulent times, including pandemics or other crises.

According to Hofmann and Rüsch (2017), to cope with the fourth industrial revolution, also known as "Industry 4.0", organizations have to develop and implement autonomous and self-regulating systems. The advances in information and communication technology (ICT) have a significant impact on information exchange across supply chains; managing such complex networks in real-time requires a sound digital environment that enables value creation in supply chain transactions. In the past few years, blockchain technology and applications have been receiving increased interest in the supply chain world (Kshetri, 2018). Blockchain is the foundation for secure cryptocurrencies such as Bitcoin and Ethereum (Ghobakhloo, 2018; Koutmos, 2019). In the context of Industry 4.0, partners in the supply chain, which can be accordingly called "Supply Chain 4.0", can integrate services in a remote location into their own processes (Xu *et al.*, 2018). Nonetheless, those partners usually have competing interests but, in the same time, need to collaborate seamlessly and require trust, transparency, autonomy and speed in their decentralized transactions. According to a report by DHL (2020), about 10% of the legal disputes on lading bills are due to incorrect data and misunderstanding of traditional contracts; thus, here comes the need for blockchain and smart contracts. Yao *et al.* (2020) suggested using blockchain to coordinate the payment structure in multi-echelons supply chains. Hofmann and Rüsch (2017) identified smart contracts as key blockchain technology that can be used for order processing that is a basic function of operations and supply chain management (OSCM). In that regard, smart contracts

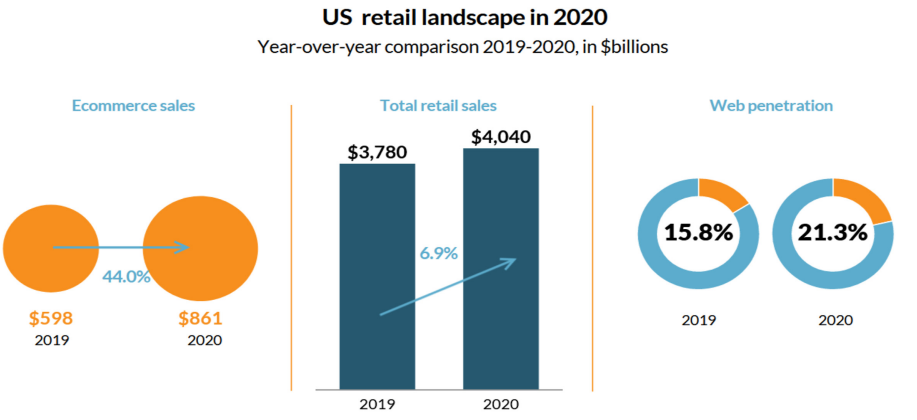

Figure 1.
The increase in e-commerce in the US through 2020

Source(s): Digital Commerce 360, US Commerce Department

can ensure that sufficient funds are available for the transaction under consideration and that all the parties are paid in a timely manner (Sikorski *et al.*, 2017).

The core competence of blockchain technology is its ability to protect its own generated records, such as cryptocurrency transactions, and to maintain the authenticity and integrity of these records (Nakamoto, 2008). However, assuring records' liability is a major limitation of blockchain systems as they do not address the reliability of records created outside their borders "exogenous records" (Lemieux, 2016). Supply chain transactions, which are related usually to physical products and services, are exogenous to the consensus mechanism of blockchains. Even with the integration of the Internet of things (IoT) or radio frequency identification (RFID) with blockchain (Boudguiga *et al.*, 2017; Haddud *et al.*, 2017; Rizzi *et al.*, 2016), human behaviour can manipulate the IoT input, for example, by attaching the RFID tags on empty, wrong or inferior-quality products. Therefore, the majority of supply chain transactions are considered exogenous to the blockchain, because they are not generated by the blockchain and cannot be verified by IoT, for example, conducting a perfect order fulfilment or returning a misused product. Failure to have a consensus about the validity of such simple but vital activities limits the applicability of blockchain and smart contracts to address the supply chain issues within the context of Industry 4.0 (Mercuri *et al.*, 2021).

This paper addresses the above challenges by introducing *trust* as a digital asset that is encapsulated inside the blockchain to provide a good level of integrity for the exogenous records originated outside the boundaries of automation. This strategy is applicable only to permissioned blockchain ledgers and not to enhance the system stability as explained later on. The concept of distributed ledgers is a radical innovation that enables organizations to perform transactions in a decentralized way and comply with the digitalization adopted by supply chain 4.0. Hence, comes the title and the main research question of this work: Are smart contracts too smart for supply chain 4.0?

The paper is organized as follows. Section 2 gives a literature review on smart contracts and their applications in OSCM. Section 3 gives a conceptual framework for realistic implementation of smart contracts and its corresponding functions. Section 4 gives a numerical study based on the proposed framework. Finally, Section 5 draws the conclusions and the potential future work.

2. Literature review

2.1 What are smart contacts?

In a qualitative research performed by Korpela *et al.* (2017), a focus group composed from 30 companies was interviewed to discuss how blockchain technology can support Industry 4.0 and the related digital supply chain. Smart contracts were selected by 44% of the participants as key functionality that can support this digital transformation.

Smart contracts are "self-executing scripts that reside on the blockchain and allow for proper, distributed, heavily automated workflows" (Christidis and Devetsikiotis, 2017). Smart contracts can be used for exchanging money, property or any value through some transactions over the blockchain with a set of predefined rules and penalties (Biggs *et al.*, 2018). The concept of smart contracts was first introduced by Szabo (1994); he defined the smart contract as "a computerized transaction protocol that executes the terms of a contract". However, due to the technological status by then, it was difficult to adopt such concept in an applicable way. With the rise of information technology and the cryptocurrency platforms, it becomes possible to interact with virtual currency in a shared global ledger.

A smart contract is triggered by addressing a transaction to it, and after validating and verifying this transaction, the smart contract executes autonomously on every node in the chain. For the digital assets in the blockchain (e.g. Bitcoin), the accounts are automatically settled, while for the digital representation of assets off the blockchain (e.g. stocks), accounts

are only settled after the accounts off-chain are matched with the agreed-upon settlement instructions (Hofmann *et al.*, 2018). All the interactions for smart contract operations along the blockchain are verified via signed messages, and all the participants get a cryptographically verifiable trace of these operations. However, some researchers criticize the application of smart contracts and their implementation in blockchains. For example, O'hara (2017) argued that the strictness of self-enforcement of a smart contract can be easily misused and utilized against the contracting parties as it lacks the real-world form of enforcement. The goal of this work is to try to narrow the gap between the virtual world and the real world.

2.2 Smart contracts applications in OSCM

Many works targeted the general architecture and applications of blockchain technology (Tönnissen and Teuteberg, 2019). Some works have addressed smart contracts characteristics and applications in OSCM. Regarding the concepts and characteristics, recent works addressed integrating blockchain technology with business process management (BPM). Viriyasitavat and Hoonsopon (2019) defined two main problems with such integration: time inconsistency and consensus bias that are both resulting from trust issues. They argued that the executions of the contracts should reach its consensus by a set of nodes that are agreed upon by the concerned business partners in order to provide more reliable and flexible consensus. Viriyasitavat *et al.* (2018) have identified some critical issues that face the modern BPM systems, such as verification, evaluation and transformation of the trustworthiness and digitized assets.

Since the blockchain is a decentralized system for interacting with virtual money, a shared global ledger is used to store the balance for every pseudonym and execute user-defined programs. The ledger is a public database that supports information sharing in supply chain demand planning in enterprises (Toyoda *et al.*, 2017), and that can provide proof of origin and traceability (Kshetri, 2017). Nakasumi (2017) proposed a different perspective of the ledger by seeing it as a private database that supports business-to-business trading and facilitates direct transactions and payment services in inventory and demand-levels sharing.

Tracking marine shipments is an important application that combines blockchain and IoT. Traditionally, a single container shipped from East Africa to Europe requires as many as 30 employees and 200 or more transactions to handle the required paperwork. That is why "Maersk", the large shipping company, started working with IBM to use blockchain technology to track their marine shipments (Dobrovnik *et al.*, 2018). IBM is currently working with about 400 organizations to apply blockchain technology; one of these organizations is Walmart, which announced in 2016 that they are using blockchain to record and track the origins of the products in order to improve health and safety standards (Condliffe, 2017).

Gallay *et al.* (2017) elaborated on using blockchain technology to confirm and store contracts and transactions involved in selecting transport carriers and operators. Gao *et al.* (2018) proposed a supply chain management system based on a hybrid decentralized ledger with a block construction mechanism, a storage scheme and information protection method.

Recently, several mechanisms have been developed to the fulfilment of blockchains transactions. Cosmos, based on Tendermint, can be used to connect transactions among different blockchains "Internet of blockchain" (Kwon and Buchman, 2018). Due to its Byzantine fault-tolerant consensus algorithm, it can provide a secure and instant finality of the created blocks. Despite its effectiveness to improve the scalability of blockchain, it may create some type of centralization through having a limited number of transaction validators. On the other hand, lighting network addresses the scalability vs decentralization paradigm of

micro payments through channel payments networks. It is effective to handle multiple micro transactions among a limited number of parties (Poon and Dryja, 2016). However, it may not be a preferred solution to capture large values within the payment channel away from the main blockchain, especially with the limited number of participants in the channel compared to the main blockchain. Sidechains provide another approach to communications among different chains or different cryptocurrencies through creating two ways pegged between the sidechain and the blockchain, where the currency of one side of the peg can be blocked into it until it is processed at the other side of the peg (Back *et al.*, 2014).

Other applications of smart contracts include the enforcement of regulations for pharmaceutical supply chains (Bocek *et al.*, 2017) and food supply chains (Tian, 2016). For a recent review on integrating blockchain with supply chain, the reader is referred to the works by Hackius and Petersen (2017) and Sternberg and Baruffaldi (2018), and for a recent review on blockchain research directions, see Hughes *et al.* (2019). Some important insights were perceived from those works; the survey carried out by Hackius and Petersen (2017) has shown that 60% of the middle managers raise concerns about data security in using blockchain in supply chain context, while the main concern for consultants was the technological maturity of the blockchain. Sternberg and Baruffaldi (2018) concluded that the trustless paradigm that was introduced by blockchain has an unfavourable impact on the transaction climate among supply chain actors; they recommended the use of smart contracts to add value to the supply chain finance. Hughes highlighted the potential of using smart contracts in applications beyond business to serve broader goals – United Nations (UN) Sustainable Development Goals (SDGs).

Alicke *et al.* (2016) have identified six main drivers for supply chain; planning, physical flow, performance management, order management, collaboration and supply chain strategy. Each driver has several levers for supply chain 4.0. For example, regarding physical flow, the levers of supply chain 4.0 include warehouse automation, smart vehicles, *in situ* 3D printing, human-machine interfaces and smart logistics. The McKinsey digital supply chain 4.0 compass is adapted in Figure 2 to highlight the areas that can be boosted by using blockchain and smart. The selected levers were chosen as they address the external relationships in a smart factory, which align with the scope of this work, that is the "exogenous" transactions in the supply chain.

Among these levers, blockchain and smart contracts can play a role in facilitating smart logistics (Liao and Wang, 2018). Accordingly, for the other drivers, the levers that can make use of blockchain technology and smart contracts are online transparency (Queiroz and Wamba, 2019), online order monitoring (Treiblmaier, 2018), real-time replanning (Saberi *et al.*, 2019), order processing (Casado-Vara *et al.*, 2019), end-to-end connectivity (Abeyratne and Monfared, 2016), supply chain innovation and reconfiguration (Queiroz *et al.*, 2019) and automation and scenario planning (Dolgui *et al.*, 2019). According to Abd-alrazaq *et al.* (2021), smart contracts are among the blockchain technologies that can be used in the context of COVID-19. Marbouh *et al.* (2020) have presented seven use cases in which blockchain technology can be used in the context of COVID-19; they proposed a system that uses smart contracts in outbreak tracking. However, the research in these areas is still limited, and further research is needed to address these issues.

2.3 Research gap and the focus of this work

From the literature, it was found that smart contracts can play a significant role in improving the underlying business digital processes. Almada-Lobo (2015) has argued that supply chain 4.0 should be highly transparent and integrated; it also requires a continuous mapping of the physical flow on digital platforms. Besides becoming digital, supply chain 4.0 should become faster, more flexible, more individual, more accurate and hence more efficient.

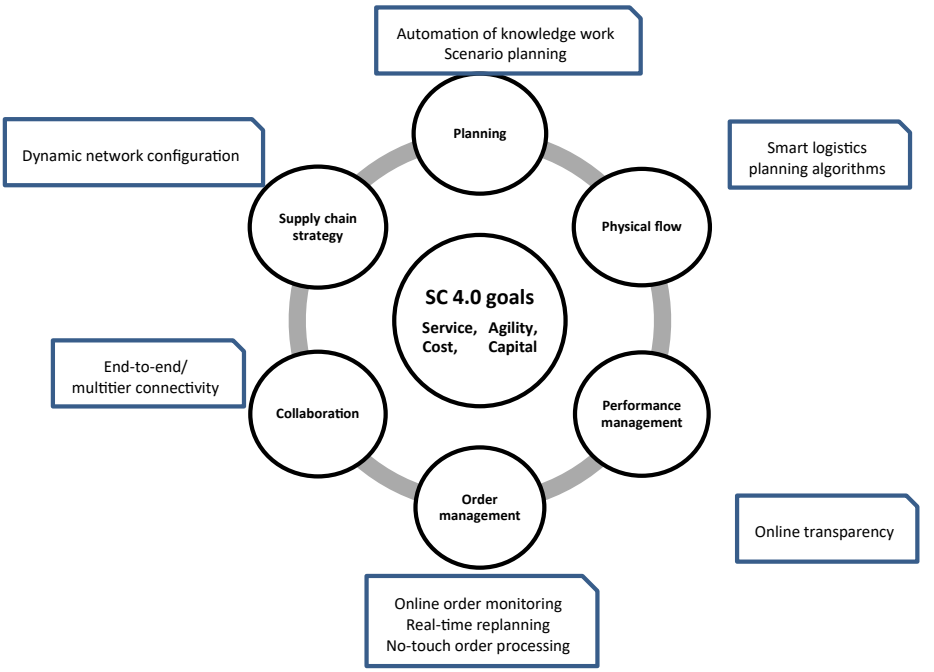

Figure 2.
Supply chain 4.0 levers with expected potential in using blockchain and smart contracts

The proposed framework sought to serve the above levers and to address the aforementioned obstacles of validating the non-electronic smart contract inputs that hinder the implementation of the blockchain technology by utilizing two concepts:

(1) *Reputation is coined as the digital currency.* A participant's wealth of the currency reflects his credit worth in reality, because participants earn currency for executing their transactions honestly. Reputation currency is used as a security deposit for future system transactions. In that sense, as a currency of the ecosystem, participants should be able to exchange it for other currencies.

(2) *Currency mining is conducted through fulfilling the physical commitment of a smart contract.* The mining reward is calculated based on not only the participant's investment value in the contract, but also the whole status of the blockchain.

After an exhaustive study, it was concluded that the previous mechanisms are effective in facilitating the exchange of cryptocurrencies and digitally verified services; however, they may not be able to validate the non-digitally verified transactions. Some previous works addressed the problem of the lack of trust between partners. For example, Weber *et al.* (2016) argued that instead of making an agreement on one trusted party, participants can share their transactions across a large network of untrusted nodes. But the real challenge is how to trust such untrusted nodes.

Hence, the main research purpose of this work is to provide a mechanism to validate the non-digitally verified "exogenous" transactions through rewarding the different parties of a smart contract for honestly reporting the status of fulfilling these transactions.

Game theory was used to model the proposed blockchain. Bigi *et al.* (2015) used game theory to analyse a platform that addresses the problem of trust by holding a deposit from

both parties; this framework is effective for blockchains with low value transactions. However, it is impractical for higher ones since it will add a considerable cost to both parties and will make the decentralized system a poor choice compared to the centralized one. Therefore, a less costly mechanism is needed to address this problem.

3. Conceptual framework

The proposed framework attempts to provide a blueprint that will be instanced into a blockchain system dedicated to control an ecosystem in the context of OSCM and supply chain 4.0. For example, let us assume that the proposed framework is instanced to control a shared economy distribution ecosystem in which customers want to send some items from one point to another, while suppliers are individuals who can transport these goods. To decentralize the system away from a governmental agency or intermediate company (middlemen), the blockchain should guarantee the payment to the supplier and the value of the transmitted goods to the customer. Another example is the ecosystem of online retailers. Suppliers are advertising online to sell an item and a distal customer wants it to be shipped to his location. The blockchain should guarantee the investment of the first mover. Should the supplier send the goods and wait for the money or should he ask for the money first and transmit the risk to the customer side? Traditionally, a central agency (e.g. e-Bay) should be involved in such ecosystem to secure both parties' investments. In the context of e-commerce, the reputation gained by sellers and buyers is based on the feedback they provide about each other after the conclusion of the transaction. The tricky part is to manage the integrity of such feedback to ensure that it is provided by genuine users (Ryan, 2017).

To accommodate the proposed framework, the following assumptions are made:

(1) Permissioned blockchain is crucial to enforce some level of entering barriers to maintain the value of earned reputation of the ecosystem and to limit players with multi-identities.

(2) Only proof of stake, practical Byzantine fault-tolerant or any other permissioned blockchain consensus algorithm can be utilized.

(3) Nodes are incentivized using the reputation currency, which can be exchanged to other currencies through the framework.

3.1 Trustless transactions and the reputation currency

The proposed blockchain contains four types of contracts into its shared ledger. Two of them are used to execute the blockchain-controlled trustless transactions, and the other two are used to exchange the reputation currency with other types of digital or physical currencies.

3.1.1 The offer contract. An offer contract is initiated by a blockchain member, who acts as a customer/supplier publishing his own request/offer that he privately values at (V_c/V_s). The contract is executed when any other member of the blockchain accepts it. The contract includes three sets of parameters:

(1) *Public parameters* describe the main features of the request/offer (e.g. the area of pick-up and drop-off for the shipment or the features of the product offered for sale). An example is the price (C) expected to pay/get for the deal. If the contract is published or accepted by a supplier ,the price should be higher than supplier's private value ($C \geq V_s$), and if the price is published or accepted by a customer, the price should be lower than his private value ($C \leq V_c$).

(2) *Private parameters* describe the details of this request (e.g. the detailed addresses, pick-up time, shipment weight and volume, etc.).

(3) The security deposit (*S*) required to be held from the supplier until the fulfillment of the request, and the expiry time of this request/offer.

To initiate an offer contract, a customer/supplier announces the service or product he is willing to buy/sell; the time frame of the validity of this announcement should pass his commitment amount to the contract from his reputation. Therefore, if the initiator is the customer, he should allocate the price value (*C*) he is willing to pay for the service. If the supplier is the initiator, he should allocate to the contract the value of the security deposit (*S*) that guarantees the customer investment; for example, a value higher than the two-way shipping cost of the goods to the customer location. If any of the blockchain members accepts to act as the other party by passing the value of (*S*) or (*C*) from his reputation to the contract, then the contract is executed by initiating a new conclude contract and passes both (*C*) and (*S*) to the initiated contract. If no supplier/customer accepts the contract before the expiration of the validity time, the offer contract expires itself and returns the investment back to the initiator.

3.1.2 The conclude contract. As described above, the conclude contract is initiated automatically by the blockchain upon the execution of the offer contract. The conclude contract represents the cornerstone of the proposed framework. The contract is designed as a mechanism that ensures the honest contract fulfilment, which is the desired social outcome. The conclude contract is designed as an extensive form game. The game has a set of equilibriums if and only if the truth is told by both players. Therefore, there is no rational motivation for either party to consider any cheating strategy that ends up with an outcome less than the honest fulfilment of the contract.

Figure 3 depicts the extensive form game that represents the conclude contract and indicates that the supplier has three possible moves: truly fulfilling the contract (*T*), falsely claiming that he fulfilled the contract (*F*) and denying fulfilling the contract (*D*). On the other side, the customer has three possible moves: admitting receiving the requirement (*A*), denying receiving the requirement (*D*) and falsely claiming that he has not received the requirement (*F*). An effective mechanism should enforce the equilibrium only at either (*T*, *A*) or (*D*, *D*) and should exclude any rational choice of the (*F*) strategy for both parties. It should be noted that it is not possible for the blockchain nodes to distinguish between the supplier's strategies (*T*) and (*F*) or between the customer's strategies (*D*) and the (*F*). Therefore, the nodes' consensus algorithms will not be able to address this tool, even with nodes honestly enforcing protocols such as the one introduced by Chen *et al.* (2017). The contract parties' reputation reward is the tool used to enforce this desired outcome.

The mechanism shown in Figure 3 allows each party to announce his choice twice. The utility of customer at each terminal node is indicated at the top, while the supplier utility is indicated at the bottom. The supplier acts as the first mover (node 0). If the supplier announces (*D*), the contract shall be executed instantly by passing the hold amounts of *S* and *C* to the customer and reward both parties by the rewarding function *R* (node 3). The reason a supplier may choose not to fulfil the contract is his belief that the fulfilment cost is higher than the summation of *S* and *C*. The customer responds with either (*A*) or (*D*/*F*) (nodes 1, 2). If the customer responds with (*A*), the contract is instantly executed by passing the values of *S* and *C* to the supplier and rewarding both parties by *R* (nodes 11 and 21). It is noteworthy that node 11 is the most socially desired outcome, while node 21 is undesired because the supplier managed to cheat the customer and to charge him without fulfilling the contract.

If the customer response is (*D*) or (*F*), the supplier shall be asked to reconfirm his fulfilment of the contract (nodes 12 and 22). If he responded with *D*, then the contract shall be executed by sending its hold amount *S* and *D* to the customer and reward the customer but not the supplier because it is assumed that he has cheated in his earlier response (nodes 13 and 23). On the other hand, if he insists that he has already fulfilled the order (*T*/*F*), then the customer shall be asked to reconfirm his earlier response (nodes 14 and 24). If he responds with (*A*), then

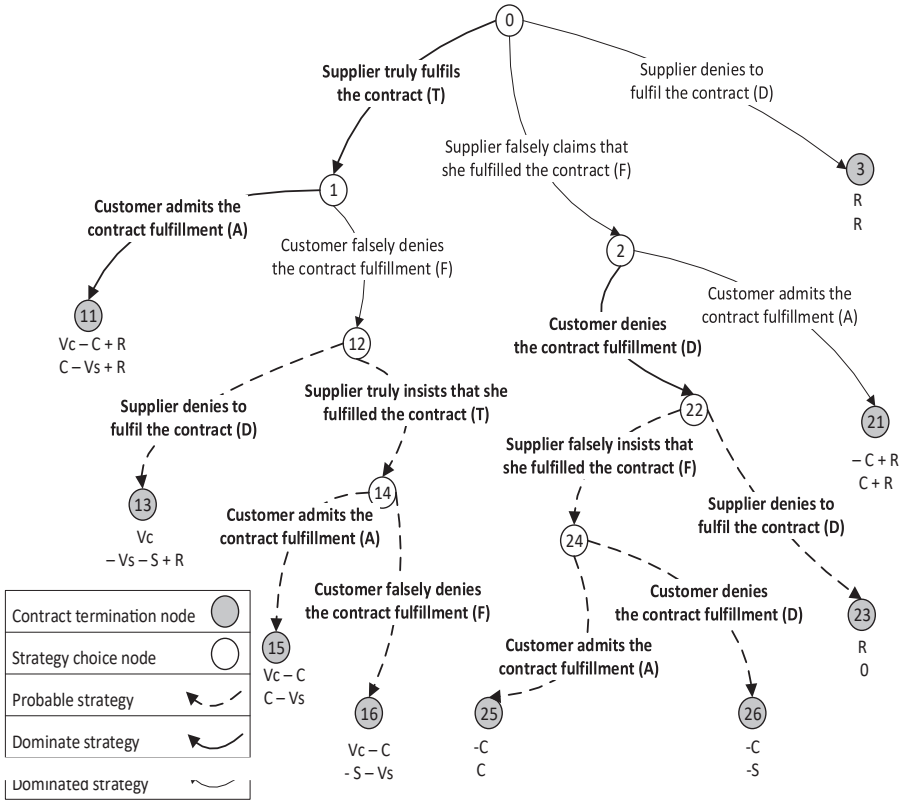

Figure 3.
The information game model of the conclude contract

the contract is executed by passing the hold amount of S and C to the supplier without rewarding any of them as both are assumed to cheat earlier (nodes 15 and 25). Otherwise, if he responds with (D/F), the contract executes itself by voiding its hold amount without passing any value or rewards to either of its parties (nodes 16 and 26).

As shown in Figure 3, the intensive form game can be defined through the set of the actions available to each player A_i where $i \in \{\text{sup}, \text{cus}\}$:

$$A_{\text{sup}} = \{\text{D}, \text{TT}, \text{TD}, \text{FF}, \text{FD}\}$$

$$A_{\text{cus}} = \{\text{A}, \text{FF}, \text{FA}, \text{DD}, \text{DA}\}$$

A set of non-terminal choice node H and a set of terminal nodes Z:

$$H = \{0, 1, 2, 12, 14, 22, 24\}$$

$$Z = \{3, 11, 13, 15, 16, 21, 23, 25, 26\}$$

In order to find the equilibrium of the above game, backward induction is used to predict the game equilibrium. The customer is indifferent between the two options in node 14 because his utility is equal to ($V_s - C$) in both cases (nodes 15 and 16). Therefore, it can be assumed that ($\propto$) percent of customers may respond with (A) and the remaining $(1 - \propto)$ may respond with (F). Therefore, the supplier shall expect to get a utility value of $(1 - \propto)(C - V_s) + \propto (-S - V_s)$. Therefore, the supplier at node 12 shall respond with (T) if he believes that:

$$(\propto)(C - V_s) + (1 - \propto)(-S - V_s) > -S - V_s + R \tag{1}$$

Solving inequality (1) for the value of $\propto$ results in inequality (2):

$$\propto > R/(S + C) \tag{2}$$

It will be illustrated in Section 3.2 that R should be much smaller compared to both S and C. Then, the supplier should conclude that it is highly probable to get a higher utility if he responds by (T) in node 12. Continuing backward to node 1, the customer expects that the supplier may respond by (T); hence, he should respond by (A) if his certain utility obtained at node 11 is higher than the weighted utility obtained from the supplier response at node 12:

$$V_c - C + R > \left(1 - R/(S + C)\right)(V_c - C) + \left(R/(S + C)\right)V_c \tag{3}$$

Therefore, it can be concluded that inequality (3) will be always correct for any positive values of both of S and R.

Theorem 1. A super-rational customer should not falsely claim the supplier's failure to fulfil a contract if the contract includes both positive deposit and reward.

The customer is indifferent between the two options in node 24, and it can be assumed that the $(\propto)$ percent of customers may respond with (A) and the remaining $(1 - \propto)$ may respond with (F). Consequently, the supplier at node 22 shall respond with (T) if he believes that:

$$\propto C + (1 - \propto)(-S) > 0 \tag{4}$$

Solving inequality (1) for the value of $\propto$ results in:

$$\propto > S/(S + C) \tag{5}$$

By comparing inequalities (2) and (5), it can be seen that the supplier needs higher percentages of customers to accept his fake fulfilment than those who accept his real fulfilment to respond with (F), which is not a rational argument. Hence, the supplier may believe that it is highly probable to get a higher utility if he responds by (D) in node 22. Moving backward to node 2, the customer expects that the supplier may respond by (T) based on the value shown in inequality (2). Then, he should respond by (F) if his certain utility obtained at node 21 is lower than the weighted utility obtained from the supplier response at node 22, which is shown by inequality (6):

$$-C + R < \left(1 - S/(S + C)\right)(-C)$$

$$R < SC/(S + C) \tag{6}$$

High values of R may compensate the customer for fake fulfilment and will result in undesired outcomes. Therefore, keeping the low values of R ensures that customers will reject any false claimed fulfilment.

Theorem 2. Any super-rational customer should not admit the false fulfilment of a contract if the reward is less than the multiplication of the deposit and the cost divided by the summation of the deposit and the cost.

Moving to node 0, if the value of R is high enough to violate inequality (6), a super-rational supplier shall not expect to end at node 21, if he responds with (F), and to get higher utility

than node 11, which he shall end at, if he responds with (T). On the other hand, an appropriate value of R shall enforce the supplier to respond with (T) if:

$$C * S/(S+C) + \left(1 - S/(S+C)\right)(-S) < C - V_s + R \tag{7}$$

Simplifying inequality (7) results in:

$$C/S - V_s/S + R/S > 0 \tag{8}$$

Considering that $C > V_s > 0$, and $R > 0$, then inequality (8) will be always valid. Therefore, it can be concluded that suppliers shall respond with (T) at node 0 to end at node 11, which is the game equilibrium.

Theorem 3. A super-rational supplier should truly fulfil a contract if it includes positive reward, positive deposit and the contract cost is higher than his private value of the fulfilment.

3.1.3 The invite contract. The invite contract is initiated and immediately executed when a current member of the blockchain adds a new member and transfers some of his reputation to him. To avoid a hostile takeover of the blockchain, the initial reputation value of the new participants is hardcoded in the blockchain in order to maintain the system secure. Therefore, a new member can be added only if an existing member invites him and transfers part of his reputation to him. Such reputation transfer serves two main purposes: liquidating the reputation coin with a physical currency and enabling the system to scale up by adding new players.

3.1.4 The exchange contract. The exchange contract is used to allow the members, who are mainly customers of the ecosystem, to acquire additional amount of the blockchain reputation token to be able to pay for their orders by exchanging physical or digital currencies into the blockchain tokens. On the other hand, it allows the members to liquidate the currency earned inside the blockchain into physical money. The reason to use exchange contract is to maintain the reputation tokens within the borders of the system as it can not be used as a general-use digital-currency (unlike Bitcoin). Therefore, the exchange contract is used as a method to encapsulate the token into the blockchain.

3.2 The rewarding function

Being the miner for the currency of the blockchain, the reward function represents a cornerstone of the efficient operation of the proposed system since its scalability is directly related to the reward functions' output. On the other hand, if the function rewards too much, then it can cause the currency value to be severely inflated. Three reward functions forms were investigated for the proposed framework.

The first one $R_1(x)$ is calculated based on the interest (ε) for the amount of money (x) invested by the participants of the contract, as shown in equation (9).

$$R_1(x) = x^*\varepsilon \tag{9}$$

The value of (x) represents the transaction cost (C) for the customer and of the security deposit (S) for the supplier. The value of $R_1(x)$ should be higher than the accepted market return on investment (ROI) for length of investment equal to the percentile of the ecosystem transactions in order to reward the ecosystem member for the time value of his investment into the blockchain. For example, if 90% of transactions takes less than 5 days, the ecosystem considers that 10% per year is a good ROI, and that the blockchain utilizes 300% as a premium over the money market price; then, $R_1(x)$ is estimated as 3*0.10*5/365 * (x). ε should have a fixed value and not calculated as a function of the time of each contract to encourage

the blockchain participants to conduct frequent and fast transactions as much as possible and not to use it as a money value storage tool. Moreover, having a fixed reward, that is not time-dependent, pushes both parties to announce their decisions as soon as they are ready to release their investment and rewards.

The second reward function is based on a logistic scaling of the first one. Considering that peer-to-peer distributed systems are ideally proposed for small transactions, the proposed function is designated to encourage the less-than-average transaction size. It passes double the value to the ones around the average deal size in order to limit the very high rewards on the high-value transactions compared to the system's average transaction value. The function adjusts the reward of a transaction with a value as per equation (10).

$$R_2(x) = x^*\varepsilon^*2^*\left(1 - \frac{1}{1 + e^{-g\left(x-\bar{x}\right)}}\right) \tag{10}$$

The term $\bar{x}$ is the average value of transactions in the blockchain. Such extra rewards for small-value transactions compensate participants with smaller transactions for the time and effort they spend for data entry. The g term is the Gini index of the system and is used to represent the steepness of the function. Therefore, there will be less discrimination against the high-value transaction if the reputation value of all members is almost equal; in contrast, if there are few members who are controlling high percentage of the blockchain wealth, the reward function aggressively limits the rewards on high value transactions.

The third reward function is designated to control the total amount of currency in the blockchain in order to avoid the inflation of the reputation reward as a currency. Equation (11) shows how this function is used to reward a participant on his honesty in fulfilling a contract in which he invested some value.

$$R_3(x) = x^*\varepsilon^*2^*\left(1 - \frac{1}{1 + e^{-g\left(\sum \tau - \frac{\rho}{2}\right)}}\right) \tag{11}$$

R_3 will be more rewarding at the launch of the blockchain where the total reputation of all players is much less than the half of its intended maximum. When the summation of the reputations of all the members approaches the maximum, the function reduces the rewards' values.

4. Numerical study

To validate the proposed framework, a system dynamics simulation model was constructed to simulate the behaviour of the proposed rewarding functions. Three sizes of the blockchain are simulated; small (S), medium (M) and large (L), with 10, 100 and 1,000 participants, respectively. To initiate the model, each of the blockchain founders is given 10 reputation units. The conduct, conclude and the exchange contracts are randomly executed between two randomly selected members of the blockchain, who have enough reputation balance required by the contract. The invite contract is executed only when a member has a balance of more than 20 reputation points. The values of the invite and the exchange contracts are fixed at 10 units as well. Equation (12) is arbitrary used to generate C, where τ represents the customer's available balance.

$$C = \max(\text{round}((\text{rand}[0,1] * \sqrt{\tau_{\text{customer}}})), 1) \tag{12}$$

To comply with the logic that customers will not be involved in a transaction that exceed their balance, the values of the transactions were generated by multiplying a uniformly distributed random number in the range between zero and one with the square root of the customer's available balance.

The security deposit value (S) is randomly set based on equation (13) to be higher than the cost. Based on the presented game model, it is enough to have any positive S to ensure that cheating the other party is a dominated strategy.

$$S = \min\left(\text{round}\left(\frac{C}{(\text{rand}[0,1])}\right), \frac{\max(\tau_{\text{supplier}})}{2}\right) \tag{13}$$

The cost of the transaction is scaled up by dividing it by a uniformly distributed random number between zero and one. Then, it is rounded and compared to the half of the balance of the richest supplier in the blockchain to ensure that there are suppliers that are capable to afford the requested S (Li *et al.*, 2019).

Each of the three sizes of blockchain is simulated for 10,000 transactions and the simulation is repeated for 30 times; the results are presented in Sections 4.1–4.4.

4.1 The total reward amount

As shown in Figure 4, both R_1 and R_2 increase the total amount of the digital currency, and this may result in a depreciation of the blockchain currency. Therefore, having a transparent reward value is more important to the successful implementation of the blockchain than its currency exchange rate.

Despite the overall linear-like performance of the R_2, its aggressive limitation of the high number of transactions dynamically changes the reward based on the transaction value. Therefore, R_2 is only recommended when there is a high risk of taking over the blockchain. In most of the cases, R_3 is recommended because of its predictability at each stage and its control of the currency inflation. Figure 5 shows how R_3 scales down the reward calculated by R_1 for the different instances. It shows that when the total amount of reward approaches the half of its planned value, the function reduces the rewards to control the currency inflation. Therefore, careful setting of the maximum currency amount in the blockchain is important to make a compromise between the scalability of the blockchain and the prevention of the currency inflation. It is clear also that there is no significant effect of the initial size of the blockchain.

4.2 The number of newly added members

The size of a business/social network is critical to its continuity; therefore, the number of the newly added members is considered one of the most critical success factors of the proposed framework. In this section, the effect of different initial blockchain sizes and reward function on the number of the newly added members is investigated. Figure 6 reveals that new participants are invited to join the blockchain regardless of the number of the current participants. As illustrated in Figure 4, the R_2 reward function mines the smallest amount of reputation currency; therefore, the resulting number of added members is the least among the other reward functions. The big variance of the large-sized blockchain indicates that the

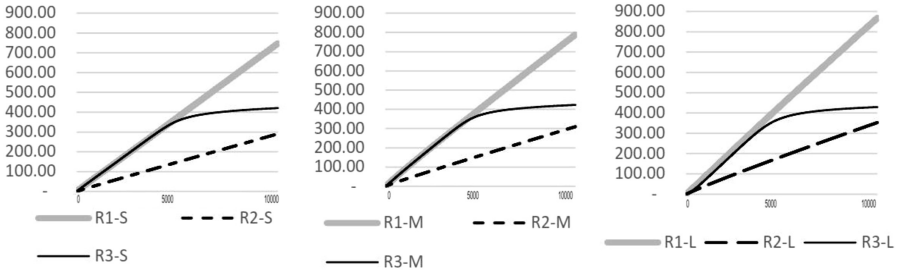

Figure 4.
The total reward amount for each function per each blockchain size

simulation time of 10,000 transactions is not enough for such instance size to reach its steady-state compared to the small and medium-sized instances.

4.3 The Gini tracking of the blockchain

At the start of the simulation, all the participants have the same reputation balance; this perfect uniformity results in zero Gini index. After a while, the transactions distribute the reward randomly across the participants. The Gini index of the blockchain matures at about 0.3, which is almost the Gini index of a uniform distribution. As shown in Figure 7, the Gini index increases sharply in small-sized instances, while it takes much longer to reach maturity with larger-sized instances. The Gini index of large-sized instances is more stable than the small-sized ones, because a single transaction resulting in transmitting a sound portion of a customer balance to his supplier cannot affect the overall index if there are other 1,000 members in the blockchain.

4.4 Resilience to hostile takeover

Like any Internet-based technology, cybersecurity is of critical importance; hence, it is fundamental to check the system's resilience in face of any possible takeover attacks (Nagurney *et al.*, 2017; Ben Yaghlane and Azaiez, 2019). To test the system's resilience,

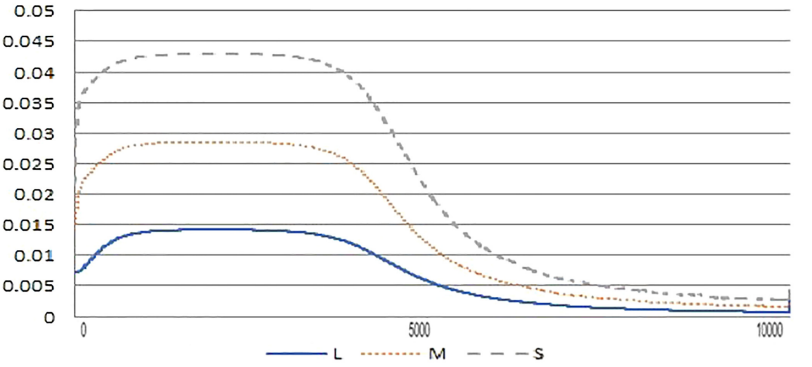

Figure 5.
The progress of the scaling down the ratio of *R*3 for the three sizes of blockchain over instances

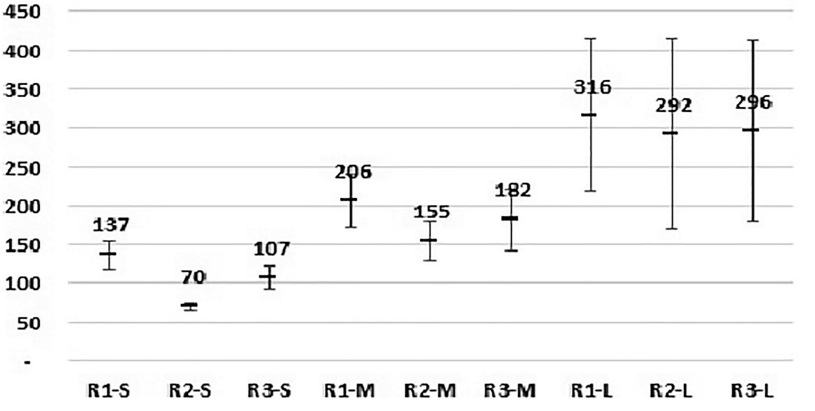

Figure 6.
The average number of the invited new members along with its variance for the reward functions for different sizes of blockchain

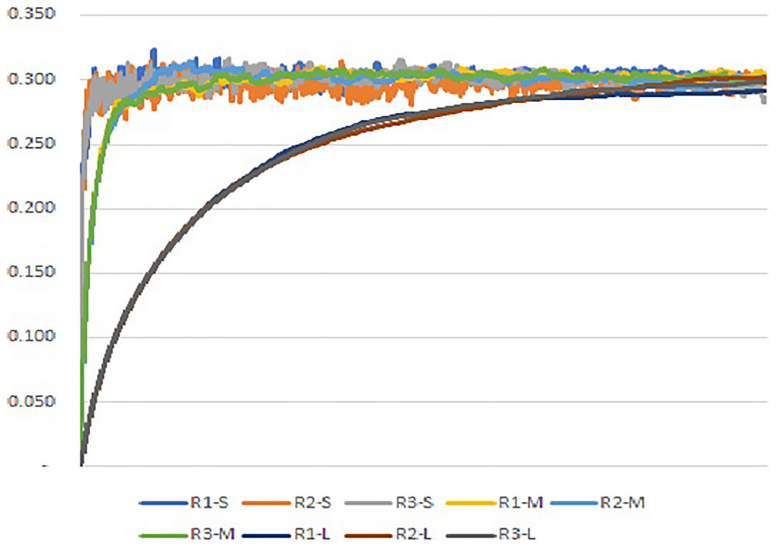

Figure 7.
The progress of the blockchain Gini index versus time for the reward functions for different sizes of blockchain

two attacks are planned at iterations 4,000 and 8,000. The attacks occur when a number of participants hold their balance and try to take over the blockchain by inviting as much as they can of new members to be able to control the blockchain. A resilient system should be able to identify such suspicious behaviour. The premature blockchain contains a considerable number of participants with their initial reputation. Therefore, the R_3 confuses those original members with the attackers. However, for matured blockchains, the function moves its scaling ratio towards a neutral level to prevent the attacker from taking over the blockchain.

Figure 8 shows the Gini index that is used to signal out the attacks at different iterations, where X-axis represents the iterations and Y-axis represents the Gini index value. Figure 9 shows the scaling ratio used by the R_3 function to adjust the reward calculated by R_1. It was observed that the attack at iteration 4,000 could be identified by the blockchain for the medium and the large-sized blockchains (shown at middle and the left of the figures) due to prematurity of those blockchains at that stage. Therefore, for the 4,000th transaction of the small blockchain, the R_3 adjusts its scaling ratio to reverse the effect of the attack. The attacks for the 8,000th transaction are identified by the function for all the sizes of the blockchain, and the scaling ratio was adjusted accordingly to stop the attackers.

5. Conclusions

This paper addresses smart contracts and blockchain as key applications of supply chain 4.0. A conceptual framework was proposed and a perfect information game theory model was developed to represent the trust issue of the proposed smart contract model. After that, a system dynamics simulator was used to check the response of the blockchain with different sizes and different reward functions.

Based on the theoretical work and the simulation conducted in this research, some insights can be gained:

(1) Validating the integrity of the blockchain exogenous transactions can be achieved through rewarding the honest reporting of the fulfilment status of these transactions,

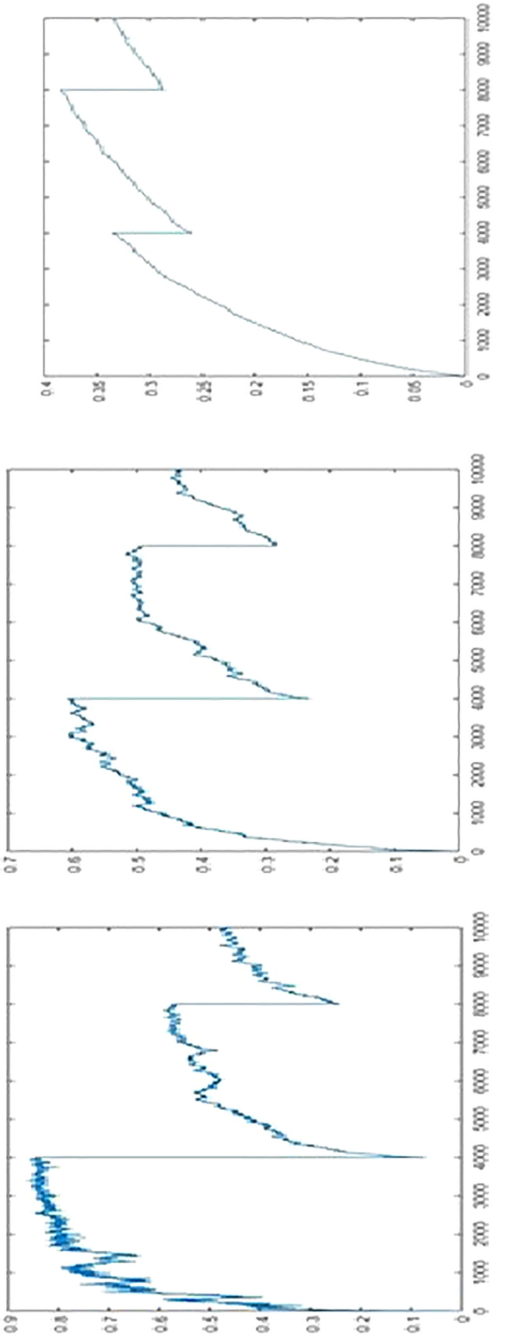

Figure 8.
The Gini index of the blockchain with attacks at the 4,000th and the 8,000th transactions for *R*1, *R*2 and *R*3 (left to right)

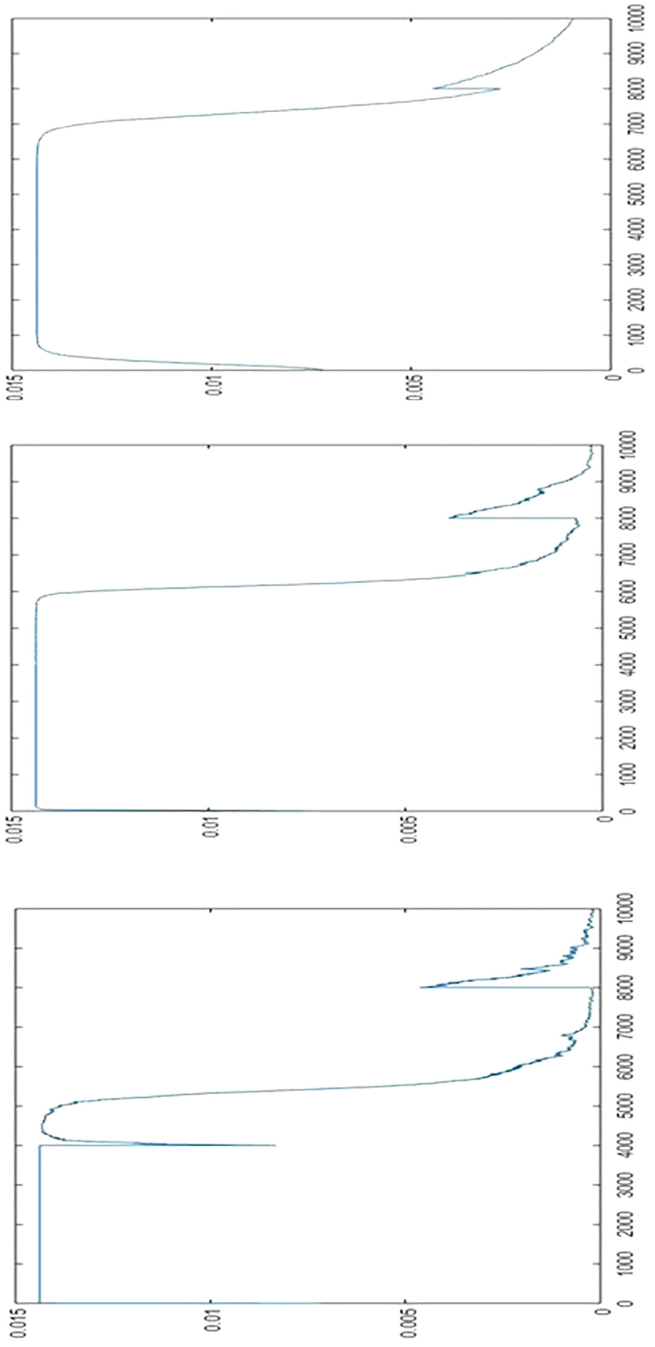

Figure 9.
The scaling ratio with attacks at the 4,000th and the 8,000th transactions for $R1$, $R2$ and $R3$ (left to right)

(2) Honest reporting of the conducted transactions outside the blockchain into the blockchain can be used as the mining activity for the blockchain digital currency,

(3) The reward amount and mechanism are critical cornerstones for the trustless-based smart contracts,

(4) As the time passes, the blockchain becomes more matured and more resilient to takeover attacks, if and only if a proper rewarding mechanism is utilized to prevent the attacker from benefiting from his attack,

(5) The proposed framework is expected to serve supply chain 4.0 levers by automating the knowledge work and enabling scenario planning through the game theory model. It will also improve online transparency and order monitoring and processing in real-time through secured multitier connectivity,

(6) The proposed framework can be applied across several supply chain functions, notably smart logistics and during the times of turbulence,

(7) The trust and transparency offered by the proposed framework should be backed by a broader strategy for digitizing the supply chains and making them more resilient.

Thereby, the results and the discussion of this work support that smart contracts are not too smart to be applied in the context of supply chain 4.0. Rather, this research has shown the relevance and potential of using smart contracts for this area through the mutual advantage achieved for all parties – customers and suppliers who can access data and perform transactions in a secured and trusted environment governed by the proposed framework of smart contracts.

This work is proposed as a conceptual framework, and future work will be dedicated to implement and experiment the proposed framework for different supply chain 4.0 systems which may reveal other challenges and provide additional interesting insights. This paper opens the doors for further research areas such as:

(1) Investigating the effect of different consensus algorithms on the stability and the scalability of the blockchain.

(2) Developing other types of reward function that can match specific applications and prevent certain type of attacks.

(3) Determining the optimal currency ceiling.

(4) Analysing the effect of the available blockchain liquidity on the scalability of the ecosystem.

(5) Simulating systems with different suppliers' tiers and/or different customer typologies.

(6) Considering environmental aspects of the supply chain.

References

Abd-alrazaq, A.A., Alajlani, M., Alhuwail, D., Erbad, A., Giannicchi, A., Shah, Z., Hamdi, M. and Househ, M. (2021), "Blockchain technologies to mitigate COVID-19 challenges: a scoping review", *Computer Methods and Programs in Biomedicine Update*, Vol. 1, 100001, doi: 10.1016/j.cmpbup.2020.100001.

Abeyratne, S.A. and Monfared, R.P. (2016), "Blockchain ready manufacturing supply chain using distributed ledger", *International Journal of Research in Engineering and Technology*, Vol. 5 No. 9, pp. 1-10.

Alicke, K., Rexhausen, D. and Seyfert, A. (2016), *Supply Chain 4.0 in Consumer Goods*, McKinsey & Company, available at: https://blockstream.com/technology/sidechains.pdf (accessed 18 June 2020).

Almada-Lobo, F. (2015), "The industry 4.0 revolution and the future of manufacturing execution systems (MES)", *Journal of Innovation Management*, Vol. 3 No. 4, pp. 16-21, doi: 10.24840/2183-0606_003.004_0003.

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J. and Wuille, P. (2014), "Enabling blockchain innovations with pegged sidechains", White Paper, available at: https://blockstream.com/technology/sidechains.pdf (accessed 25 September 2020).

Ben Yaghlane, A. and Azaiez, M.N. (2019), "System survivability to continuous attacks: a game theoretic setting for constant attack rate processes", *Journal of the Operational Research Society*, Vol. 70 No. 8, pp. 1308-1320, doi: 10.1080/01605682.2018.1489350.

Biggs, J., Hinish, S.R., Natale, M.A. and Patronick, M. (2018), "Blockchain: revolutionizing the global supply chain by building trust and transparency", available at: https://cdecker.github.io/btcresearch/2018/biggsblockchain.html (accessed 12 December 2020).

Bigi, G., Bracciali, A., Meacci, G. and Tuosto, E. (2015), "Validation of decentralised smart contracts through game theory and formal methods", in Bodei, C., Ferrari, G. and Priami, C. (Eds), *Programming Languages with Applications to Biology and Security*, Springer, Cham.

Bocek, T., Rodrigues, B.B., Strasser, T. and Stiller, B. (2017), "Blockchains everywhere-a use-case of blockchains in the pharma supply-chain", *Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management*, pp. 772-777, doi: 10.23919/INM.2017.7987376.

Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A. and Sirdey, R. (2017), "Towards better availability and accountability for IoT updates by means of a blockchain", *The 2017 IEEE European Symposium on Security and Privacy Workshops*, doi: 10.1109/EuroSPW.2017.50.

Casado-Vara, R., González-Briones, A., Prieto, J. and Corchado, J.M. (2019), "Smart contract for monitoring and control of logistics activities: pharmaceutical utilities case study", in Graña, M., López-Guede, J.M., Etxaniz, O., Herrero, A., Sáez, J.A., Quintián, H., Corchado, E. (Eds), *Advances in Intelligent Systems and Computing International Joint Conference SOCO'18-CISIS'18-ICEUTE'18*, International Joint Conference SOCO'18-CISIS'18-ICEUTE'18. 2018, Springer, Cham, p. 771.

Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y. and Shi, W. (2017), "Decentralized execution of smart contracts: agent model perspective and its implications", in Brenner, M., Rohloff, K., Bonneau, J., Miller, A., Ryan, P.Y.A., Teague, V., Bracciali, A., Sala, M., Pintore, F. and Jakobsson, M. (Eds), *Financial Cryptography and Data Security*, Springer, Cham.

Christidis, K. and Devetsikiotis, M. (2017), "Blockchains and smart contracts for the internet of Things", *IEEE Access*, Vol. 4, pp. 2292-2303, doi: 10.1109/ACCESS.2016.2566339.

Condliffe, J. (2017), "The world's largest shipping company is trialing blockchain to track cargo", *MIT Technology Review*, available at: https://www.technologyreview.com/s/603791/the-worlds-largest-shipping-companytrials-blockchain-to-track-cargo/ (accessed 5 January 2020).

DHL (2020), "Trend research blockchain in logistics; perspectives on the upcoming impact of blockchain technology and use cases for the logistics industry", available at: https://www.logistics.dhl/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf (accessed 1 July 2020).

Digitalcommerce360 (2021), available at: https://www.digitalcommerce360.com/2021/02/15/ecommerce-during-coronavirus-pandemic-in-charts/ (accessed 1 April 2021).

Dobrovnik, M., Herold, D.M., Fürst, E. and Kummer, S. (2018), "Blockchain for and in logistics: what to adopt and where to start", *Logistics*, Vol. 2 No. 3, p. 18, doi: 10.3390/logistics2030018.

Dolgui, A., Ivanov, D., Potryasaev, S., Sokolov, B., Ivanova, M. and Werner, F. (2019), "Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain", *International Journal of Production Research*, Vol. 58 No. 7, pp. 2184-2199, doi: 10.1080/00207543.2019.1627439.

Gallay, O., Korpela, K., Tapio, N. and Nurminen, J.K. (2017), "A peer-to-peer platform for decentralized logistics", *Proceedings of the Hamburg International Conference of Logistics (HICL) Proceedings*, pp. 19-34, doi: 10.15480/882.1473.

Gao, Z., Xu, L., Chen, L., Zhao, X., Yang, L. and Weidong, S. (2018), "CoC: a unified distributed ledger based supply chain management system", *Journal of Computer Science and Technology*, Vol. 33 No. 2, pp. 237-248, doi: 10.1007/s11390-018-1816-5.

Ghobakhloo, M. (2018), "The future of manufacturing industry: a strategic roadmap toward Industry 4.0", *Journal of Manufacturing Technology Management*, Vol. 29 No. 6, pp. 910-936, doi: 10.1108/JMTM-02-2018-0057.

Hackius, N. and Petersen, M. (2017), "Blockchain in logistics and supply chain: trick or treat?", in Kersten, W., Ringle, C.M. and Blecker, T. (Eds), *Digitalization in Supply Chain Management and Logistics, the Hamburg International Conference of Logistics (HICL) Proceedings*, Hamburg, Germany, pp. 3-18, epubli, doi: 10.15480/882.1444.

Haddud, A., DeSouza, A., Khare, A. and Lee, H. (2017), "Examining potential benefits and challenges associated with the Internet of Things integration in supply chains", *Journal of Manufacturing Technology Management*, Vol. 28 No. 8, pp. 1055-1085, doi: 10.1108/JMTM-05-2017-0094.

Hofmann, E. and Rüsch, M. (2017), "Industry 4.0 and the current status as well as future prospects on logistics", *Computers in Industry*, Vol. 89, pp. 23-34, doi: 10.1016/j.compind.2017.04.002.

Hofmann, E., Strewe, U.M. and Bosia, N. (2018), *Supply Chain Finance and Blockchain Technology: The Case of Reverse Securitisation*, Springer, Cham, doi: 10.1007/978-3-319-62371-9.

Hughes, L., Dwivedi, Y.K., Misra, S.K., Rana, N.P., Raghavan, V. and Akella, V. (2019), "Blockchain research, practice and policy: applications, benefits, limitations, emerging research themes and research agenda", *International Journal of Information Management*, Vol. 49, pp. 114-129, doi: 10.1016/j.ijinfomgt.2019.02.005.

Khurshid, A. (2020), "Applying blockchain technology to address the crisis of trust during the COVID-19 pandemic", *JMIR Medical Informatics*, Vol. 8 No. 9, doi: 10.2196/20477.

Korpela, K., Hallikas, J. and Dahlberg, T. (2017), "Digital supply chain transformation toward blockchain integration", *Proceedings of the 50th Hawaii International Conference on System Sciences proceedings*, Hawaii, USA, doi: 10.24251/HICSS.2017.506.

Koutmos, D. (2019), "Market risk and Bitcoin returns", *Annals of Operations Research*, Vol. 294, pp. 453-477, doi: 10.1007/s10479-019-03255-6.

Kshetri, N. (2017), "Can blockchain strengthen the Internet of Things?", *IT Professional*, Vol. 19, pp. 68-72, doi: 10.1109/MITP.2017.3051335.

Kshetri, N. (2018), "1 Blockchain's roles in meeting key supply chain management objectives", *International Journal of Information Management*, Vol. 39, pp. 80-89, doi: 10.1016/j.ijinfomgt.2017.12.005.

Kwon, J. and Buchman, B. (2018), "Cosmos: a network of distributed ledgers", available at: https://cosmos.network (accessed 22 October 2020).

Lemieux, V.L. (2016), "Trusting records: is Blockchain technology the answer?", *Records Management Journal*, Vol. 26 No. 2, pp. 110-139, doi: 10.1108/RMJ-12-2015-0042.

Li, J., Liu, T., Niyato, D., Wang, P., Li, J. and Han, Z. (2019), "Contract-based approach for security deposit in blockchain networks with shards", *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 75-82, doi: 10.1109/Blockchain.2019.00019.

Liao, D.-Y. and Wang, X. (2018), "Applications of blockchain technology to logistics management in integrated casinos and entertainment", *Informatics*, Vol. 5, p. 44, doi: 10.3390/informatics5040044.

Marbouh, D., Abbasi, T., Maasmi, F., Omar, I.A., Debe, M.S., Salah, K., Jayaraman, R. and Ellahham, S. (2020), "Blockchain for COVID-19: review, opportunities, and a trusted tracking system", *Arabian Journal for Science and Engineering*, Vol. 45, pp. 9895-9911, doi: 10.1007/s13369-020-04950-4.

Mercuri, F., della Corte, G. and Ricci, F. (2021), "Blockchain technology and sustainable business models: a case study of devoleum", *Sustainability*, Vol. 13, p. 5619, doi: 10.3390/su13105619.

Nagurney, A., Daniele, P. and Shukla, S. (2017), "A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints", *Annals of Operations Research*, Vol. 248 Nos 1-2, pp. 405-427, doi: 10.1007/s10479-016-2209-1.

Nakamoto, S. (2008), "Bitcoin: a peer-to-peer electronic cash system", available at: https://bitcoin.org/bitcoin.pdf (accessed 10 October 2020).

Nakasumi, M. (2017), "Information sharing for supply chain management based on block chain technology", *Proceedings of the 2017 IEEE 19th Conference on Business Informatics*, pp. 140-149, doi: 10.1109/CBI.2017.56.

O'hara, K. (2017), "Smart contracts – dumb idea", *The Digital Citizen*, March/April, pp. 97-101.

Poon, J. and Dryja, T. (2016), "The bitcoin lightning network: scalable off-chain instant payments", available at: https://gist.github.com/goking/7ba43d30a032cce53919c85d2d10aac6 (accessed 20 June 2020).

Queiroz, M.M. and Wamba, S.F. (2019), "Blockchain adoption challenges in supply chain: an empirical investigation of the main drivers in India and the USA", *International Journal of Information Management*, Vol. 46, pp. 70-82, doi: 10.1016/j.ijinfomgt.2018.11.021.

Queiroz, M.M., Telles, R. and Bonilla, S.H. (2019), "Blockchain and supply chain management integration: a systematic review of the literature", *Supply Chain Management: An International Journal*, Vol. 52 No. 2, pp. 241-254, doi: 10.1108/SCM-03-2018-0143.

Rizzi, A., Romagnoli, G. and Thiesse, F. (2016), "A new framework for RFID use cases in fashion and apparel retailing", *International Journal of RF Technologies*, Vol. 7 Nos 2-3, pp. 105-129, doi: 10.3233/rft-150075.

Ryan, P. (2017), "Smart contract relations in e-commerce: legal implications of exchanges conducted on the blockchain", *Technology Innovation Management Review*, Vol. 7 No. 10, pp. 10-17.

Saberi, S., Kouhizadeh, M., Sarkis, J. and Shen, L. (2019), "Blockchain technology and its relationships to sustainable supply chain management", *International Journal of Production Research*, Vol. 57 No. 7, pp. 2117-2135, doi: 10.1080/00207543.2018.1533261.

Sharma, A., Bahl, S., Bagha, A.K., Javaid, M., Shukla, D.K. and Haleem, A. (2020), "Blockchain technology and its applications to combat COVID-19 pandemic", *Research on Biomedical Engineering*, doi: 10.1007/s42600-020-00106-3.

Sikorski, J.J., Haughton, J. and Kraft, M. (2017), "Blockchain technology in the chemical industry: machine-to-machine electricity market", *Applied Energy*, Vol. 195, pp. 234-246, doi: 10.1016/j.apenergy.2017.03.039.

Sternberg, H. and Baruffaldi, G. (2018), "Chains in chains – logic and challenges of blockchains in supply chains", *Proceedings of the 51st Hawaii International Conference on System Sciences*, pp. 3936-3943, available at: http://hdl.handle.net/10125/50382.

Szabo, N. (1994), "Smart contracts", available at: http://szabo.best.vwh.net/smart.contracts.html (accessed 14 October 2020).

Tian, F. (2016), "An agri-food supply chain traceability system for China based on RFID and blockchain technology", *Proceedings of the 2016 13th International Conference on IEEE Service Systems and Service Management*, pp. 1-6, doi: 10.1109/ICSSSM.2016.7538424.

Tönnissen, S. and Teuteberg, F. (2019), "Analysing the impact of blockchain-technology for operations and supply chain management: an explanatory model drawn from multiple case studies", *International Journal of Information Management*, Vol. 52 Supp. 101953, doi: 10.1016/j.ijinfomgt.2019.05.009.

Toyoda, K., Mathiopoulos, P.T., Sasase, I. and Ohtsuki, T. (2017), "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain", *IEEE Access*, Vol. 5, pp. 17465-17477, doi: 10.1109/ACCESS.2017.2720760.

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: An International Journal*, Vol. 23 No. 6, pp. 545-559, doi: 10.1108/SCM-01-2018-0029.

unctad.org (2021), "How COVID-19 triggered digital and e-commerce turning point", available at: https://unctad.org/news/how-covid-19-triggered-digital-and-e-commerce-turning-point (accessed 5 April 2021).

Viriyasitavat, W. and Hoonsopon, D. (2019), "Blockchain characteristics and consensus in modern business processes", *Journal of Industrial Information Integration*, Vol. 13, pp. 32-39, doi: 10.1016/j.jii.2018.07.004.

Viriyasitavat, W., Xu, L.D., Bi, Z. and Sapsomboon, A. (2018), "Blockchain-based business process management (BPM) framework for service composition in industry 4.0", *Journal of Intelligent Manufacturing*, Vol. 31, pp. 1737-1748, doi: 10.1007/s10845-018-1422-y.

Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A. and Mendling, J. (2016), "Untrusted business process monitoring and execution using blockchain", in La Rosa, M., Loos, P. and Pastor, O. (Eds), *Business Process Management*, Springer, Cham, BPM 2016, doi: 10.1007/978-3-319-45348-4_19.

Xu, L.D., Xu, E.L. and Li, L. (2018), "Industry 4.0: state of the art and future trends", *International Journal of Production Research*, Vol. 56 No. 8, pp. 2941-2962, doi: 10.1080/00207543.2018.1444806.

Yao, M.-J., Lin, J.-Y., Lee, C. and Wang, P.-H. (2020), "Optimal replenishment and inventory financing strategy in a three-echelon supply chain under the variable demand and default risk", *Journal of the Operational Research Society*, Vol. 72 No. 10, pp. 2196-2210, doi: 10.1080/01605682.2020.1776165.

About the authors

Mohamed Grida is an associate professor in Industrial Engineering Department, Zagazig University. In addition, he is the founder and CEO of CAD/CAM/CIM and 2B Corp, which are two of the leading Middle East companies in the fields of enterprises' information technology integration, CAD/CAM consultation and technology retailing. He earned both his BS and PhD degrees in industrial engineering from Zagazig University in Egypt, while he earned MSc degree in industrial engineering from the American University in Cairo, Egypt. Dr. Grida was a visiting scholar at Hong Kong University of Science and Technology and a visiting professor in October at the University of Modern Science and Arts in Egypt. His research interests include supply chain, ocean logistics, enterprise information systems, game theory, machine leaning, artificial intelligence and human–computer interaction. On the professional side, Dr. Grida attended several training courses on management, enterprise resource planning and cloud computing by Dassault systems, Microsoft and Intel in USA, Singapore, Hong Kong, France and Poland. He conducted a number of professional projects in the fields of information technology with Dassault Systems, Intel, Aramco, Lenovo, Dell and HP.

Noha A. Mostafa is an assistant professor of industrial engineering and management, Zagazig University. She is currently a lecturer in The British University in Egypt. She did her BSc and MSc in industrial engineering from Zagazig University. She was a visiting PhD student in Tokyo Institute of Technology, Japan, in 2016. She finished her PhD degree in 2017 from Egypt–Japan University of Science and Technology (E-JUST), Egypt; the topic was the integration between different functions of the supply chain. Noha has broad research interests including supply chain management, logistics, sustainability, quality management, design thinking, value engineering, data analytics and information systems. She is the founder and faculty advisor of IEOM student chapter in Zagazig University. Noha A. Mostafa is the corresponding author and can be contacted at: noha.mostafa@bue.edu.eg; namostafa@eng.zu.edu.eg