A Blockchain, 5G and IoT-based transaction management system for Smart Logistics: an Hyperledger framework

Blockchain-based transaction management in Smart Logistics: a Sawtooth framework

Guido Perboli
ICELab@Polito & CARS@Polito
Politecnico di Torino
Turin, Italy
https://orcid.org/0000-0001-6900-9917

Vittorio Capocasale
ICELab@Polito & CARS@Polito
Politecnico di Torino
Turin, Italy
vittorio.capocasale@polito.it

Stefano Musso
ICELab@Polito & CARS@Polito
Politecnico di Torino
Turin, Italy
stefano.musso@polito.it

***Abstract*—The recent technological progress has started a revolution in the logistic and supply chain environment, known as *Logistics 4.0*. Such a revolution is based on information sharing and digitalization. For this reason, distributed ledger technolgies (and blockchain in particular) are attracting the interest of countries and companies. In this context, while other papers address the application of the blockchain technology in other logistic sectors, like the food, water, timber, electronic parts and pharmaceutical industries, this is the first paper that specifically addresses the electric vehicles supply chain. This paper also reports some preliminary tests performed on the system.**

***Index Terms*—Blockchain, Logistics 4.0, Smart Logistics, Electric vehicles, Sawtooth**

I. Introduction

Supply chain management (SCM) is "*the systemic, strategic coordination of the traditional business functions and the tactics across these business functions within a particular company and across businesses within the supply chain, for the purposes of improving the long-term performance of the individual companies and the supply chain as a whole*" [45].

The importance of SCM can be easily deduced by its market size, which will reach a value of more than $37 billion by 2027 [55]. However, the optimization of the supply chain as a whole, if compared to the one related to a single company, has to counter the additional trust issues among the actors and the problems related to data distribution, accessibility, reliability and security [53, 54],

Fortunately, in recent years, the technology progress brought what is commonly defined as *the fourth industrial revolution*. In the field of supply chain and logistics, this revolution has taken the name of *Logistics 4.0*, and it is based on information sharing and digitalization [57, 66]. In particular, the blockchain technology (BC) could cover a key role in this context, as demonstrated by the interest manifested by countries and companies [1].

BC can be described as a distributed, append-only registry which can be managed by non-trusting parties in a shared way [54]. As a consequence, it guarantees data authenticity and prevents data tampering by relying on strong cryptographic techniques, it reduces the involvement of trusted third parties and the related trust issues, and it guarantees data persistency and availability as a consequence of its distributed nature. For all this reasons, BC could be the enabling technology for the performance improvement of the supply chain as a whole.

However, the introduction of the BC in the context of logistics and supply chain is not straightforward: both [56, 65] well identify the main barriers that must be overcame. From a technical perspective, two are particularly relevant: BC has significant performance issues and it only deals with digital assets, which makes a possible security vulnerability of the frontier between the physical and the digital world. This means that any device providing information to the blockchain could tamper with the data sent[1].

In this paper, a blockchain-based framework for the electric vehicles supply chain is presented. To the best of the authors' knowledge, this is the first documented attempt to apply the blockchain technology to ensure the correct handling, transportation and recharging of the electric vehicles. In fact, many studies dealt with the application of BC to the supply chain, in particular in the water [44], food [2, 7, 9, 11, 33, 34, 46, 63], electronic parts [15], pharmaceutical [8, 26] and timber [19] industries. Moreover, some papers propose the application of the blockchain in the electric vehicles context, but to address recharging related problems, like batteries lifecycle management [20], security [29, 35, 61], privacy [36] and cost effectiveness [41, 58], which are unrelated to the electric vehicles supply chain.

The organization of the remaining part of this paper is the following: section II presents some of the basic concepts related to the blockchain and the electric vehicles supply chain. Section III offers a description of the implemented system and an analysis of its merits and its limits. Section IV presents some preliminary results obtained by testing the system. Finally, section V concludes the paper.

II. Background

The BC concept is often associated with the ones of shared distributed ledger (DLT) and of smart contract. This section summarizes them and contextualizes them in the Logistics 4.0 revolution.

[1]Such devices are called oracles.

A. Shared distributed ledger

A DLT can be simply described as a database with the following characteristics:

- **ledger:** the database works as a file where only the append operation is permitted, and it is used to store the sequence of the modifications to the original data [32];
- **distributed:** the database is replicated in many storage devices (nodes[2]) [52]. In order to tamper with the database it would be necessary to coherently modify the majority of its copies [25, 40];
- **shared:** each node is in charge to update only its own copy of the database. The state of the database is decided by what the majority of the nodes agrees upon. Thus the control of the database is shared [32].

B. Blockchain

A blockchain is a DLT with the following characteristics:

- the ledger is updated through blocks, which are groups of transactions [40, 47, 69]. Because the state of the ledger is decided by a majority agreement, the sequence of blocks and transactions must be common among the nodes;
- the block that has to be added to the ledger can be decided using various strategies (consensus algorithms), which have a huge impact on the BC properties [6, 53, 69];
- each block contains the hash of its predecessor, thus blocks cannot be deleted, moved or modified once they are added to the ledger [40, 47, 69];
- because nodes do not trust each other, digital signatures are used to verify the authenticity of the transactions [49, 53, 69].

As a consequence, the BC technology has the following properties:

- **authenticity:** because transactions are digitally signed [25, 53, 67];
- **autonomy:** because transactions can be submitted without relying on trusted third parties [5, 40];
- **transparency and auditability:** because the ledger stores the sequence of transactions. Moreover, each node has direct access to its own copy of the ledger [5, 40, 67, 69];
- **immutability:** because each block contains the hash of its predecessor [5, 40, 69];
- **redundancy and persistency:** because the system is distributed [67, 69];
- **resiliency:** In order to tamper with the database it would be necessary to coherently modify the majority of its copies [25, 40].

Blockchain technologies can be classified as [40, 69]:

- **public:** anyone can obtain a copy of the ledger and participate to the consensus process;
- **consortium:** the ledger is maintained by a limited group of entities. This is particularly relevant in the supply chain context, where each node could represent a different company of the supply chain;
- **private:** the ledger is maintained by a single entity. This makes the blockchain not intrinsically different from a distributed database [48];

[2]In this article, the terms *validator* and *node* are used interchangeably

C. Smart contracts

A smart contract can be described as a tamper-proof program (and thus it can have a legal value) [10, 14, 22]. However, the tamper-proof property is hard to guarantee, and that's where the BC technology steps in. As a consequence, it is possible to define a custom business logic with legal validity, and thus to automate simple and repetitive actions, with lower legal costs and reduced human errors [22]. The limit of the applicability of the smart contracts is the human capability to foresee all the possible outcomes of a given situation. In fact, particularly when long-term contracts are involved, unexpected situations are frequent and can only be faced by relying on the good sense of the involved parties [21].

D. Consensus algorithms

As described in subsection II-B, nodes reach an agreement through a consensus algorithm. Various consensus algorithms do exist, and everyone has its own strengths and weaknesses. It is possible to categorize them according to: consensus strategy, finality and fault tolerance.

1) Consensus strategy: consensus algorithms can be either [17, 49]:

- **election-based:** the nodes first agree on a block and then each of them adds it to its own copy of the ledger. Due to the number of exchanged messages, these algorithms are efficient only in the case of small networks;
- **lottery-based:** each node creates a block, adds it to its ledger and propagate it to the other nodes. This approach may lead to the creation of alternative block sequences, known as *forks*, which have a negative impact on the blockchain performance.

2) Finality: it refers to the possibility for a transaction in the blockchain to be reverted: in case of forks, only the blocks belonging to the globally preferred branch are kept, and all the others reverted. For this reason, consensus algorithms can be classified as [6]:

- **deterministic:** once added to the blockchain, transactions can never be reverted;
- **probabilistic:** once added to the blockchain, transactions could end up being reverted with a certain probability, which usually decreases over time (older transactions are harder to revert).

3) Fault tolerance: it is a way to describe under which conditions the nodes using the algorithm are able to reach an agreement. Consensus algorithms can be classified as [6, 17, 49]:

- **Crash Fault Tolerant (CFT):** a consensus is reached also if some nodes stop participating to the consensus process, but not if they act maliciously;
- **Byzantine Fault Tolerant (BFT):** a consensus is reached also if some nodes stop participating to the consensus process, or if they act maliciously.

E. Logistics 4.0 and Blockchain

Currently, in the context of logistics and supply chain, many are the problems related to an inefficient way of sharing information: 60% of all seaborne trade is moved through containers and it is valued at 12 trillion US Dollars in 2017 [31], but a shipment from Africa to Europe can require the interaction of 30 organizations, with 200 interactions among them [23] to fulfill bureaucracy requirements, resulting in a cost of 15% of the cargo value [23]. Solving this issue could lead to a potential gain of 5% of the global GDP and of 15% of the global trade annually [31]. In the food market, frequent are the scandals for food contamination: in North America, after the Escherichia coli outbreak of 2006 [68], two more were registered in 2015 with a total of 60 cases[12], this time involving the Chipotle Mexican Grill restaurant chain, whose share price dropped by 42% [37]. The investigations performed were not able to identify the contaminated ingredient [12]. In China a huge number of food safety incidents happened in the last 20 years [37, 42, 59], with 295 cases only in Beijing in the years 2004-2013 [42]. Almost all the markets (luxury, clothing, drug and more) are affected by an increasing percentage of counterfeit products that has reached the 3.3% of the total world trade [50, 51], with an estimated value of 500 billion dollars [50, 64, 51], of which one billion in the wine sector only [38]. Similarly, in the electric vehicles supply chain, the bureaucracy paperwork needed for inter-continental shipments, the difficulties related to the tracking of defective batteries or battery cells and the poor control over the storage, handling and recharging of the batteries can lead to huge economic losses.

In recent years, however, sensors started decreasing their size, imprecision and expensiveness, allowing them to be easily deployed. The result is the possibility to identify and locate almost any entity, and more generally to gather a huge amount of data like never before. Moreover, the progress in fields like data mining and machine learning allows to extract meaningful information from sensor data, in order to automatize the decision making process. These advancements, if coupled with the extended connectivity of IoT devices and the improved interoperability of the Internet of Services (IoS), can lead to the creation of completely automated and self-adapting systems (cyber-physical systems) [18, 28, 60, 66], which could optimize the decision making process and the overall supply chain performance. This is known as the "Logistics 4.0" revolution.

In this context, it remains unclear how different companies could trust each other. In fact, any malicious manipulation to the input data coming from the sensors, as well as to the algorithms elaborating it, could damage one or more members of the supply chain. More in general, the new problems of data distribution, accessibility, reliability and security must be addressed.[54, 53]. Fortunately, BC is a solution to all these problems, as described in subsection II-B.

F. Related work

Many papers describe the application of the blockchain to the supply chain, even if not directly in the electric vehicles one. [2] introduces *BRUSCHETTA*, a framework used to track and certify the farming, the harvesting, the production, the packaging, the conservation and the transportation of extra-virgin olive oil. The system relies on a dynamic auto-tuning mechanism in order to cope with the variable transaction volumes of the production environment. In [3], the authors propose a system based on Blockchain, IoT and artificial intelligence to optimize logistics. In [4], the authors describe a general logistic framework for product tracking with a role-based access control system. They underline the difficulties encountered while implementing the system, but they remain optimistic about the future diffusion of similar systems. [7] presents a system used to track local food. An esteem of the cost per transaction is also reported. [8] describes how *Modum.io* uses both BC and IoT to improve the pharmaceutical supply chain, in particular by avoiding unnecessary cooling of the drugs, with potential savings up to $3 billion. In [9], the authors describe a system for the distribution of eggs. They also propose an evaluation from a managerial point of view (food re-call and fraud impact, customer satisfaction, market analysis) for the use case used to test the system. [11] introduces *AgriBlockIoT*, a blockchain-based traceability platform for the agri-food supply chain. The platform is implemented by using two different framework (Ethereum and Hyperledger Sawtooth). The article also reports a performance comparison among the two implementations. [15] describes a system for the tracking of electronic parts. A performance and security analysis is also presented. In [16], the authors propose an IoT and blockchain-based framework to improve the vendor-managed inventory strategy. They also point out the benefits for the members of the supply chain. The system described in [19] could reduce the illegal cutting of timber. [26] describes a system for efficient shipment management which could find applications in the vaccine supply chain. In [27], the authors explain how the system they propose could speed up project deliveries. In [33] it is presented a framework which couples deep learning techniques and BC to optimize the food supply chain. [34] introduces *Harvest Network*, a theoretical framework for food traceability. [43] introduces *TrustChain*, a framework implementing a reputation system, in order to discourage malicious actors' behaviour. In [44], the authors present *AQUACHAIN*, a framework for the water supply chain. The authors also provide a preliminary performance evaluation. In [46], the authors describe a framework for food traceability based on an innovative consensus algorithm (proof of object). [63] describes a framework for food quality monitoring that uses fuzzy logic to esteem the food shelf life. The system is based on a lightweight BC powered by a proof of supply chain share consensus algorithm.

III. System description

The framework described in this section will be used by an important automotive company. Due to the Covid-19

pandemic outbreak, however, both the system implementation and the actual testing have been subject to numerous delays. For this reason, the system here described will probably be subject to modifications, according to the needs of the various stakeholders. At the same time, the tests described in section IV are performed locally, and they are thus only preliminary.

A. Use case

It is not possible to detail the various aspects of the use case, because of a non-disclosure agreement signed by the authors of this paper. However, the use case is related to the electric vehicles supply chain and a limited number of entities will be involved (less than twenty). The system will be used to track the proper storage, handling and recharging of the electric batteries along the whole supply chain. Moreover, every entity in the supply chain has a specific role, which is associated with a specific set of operations allowed.

B. Framework selection

The system is implemented using the Hyperledger Sawtooth framework, which provides a BFT consensus algorithm with a good efficiency on small networks. Sawtooth has been preferred to Hyperledger Fabric as a result of the following analysis:

1) Use Case: Both Fabric and Sawtooth are permissioned blockchain, and thus they are a good fit for an inter-company application.

2) Maturity: Both Fabric and Sawtooth are production-ready frameworks. Fabric, however, was born before Sawtooth, and thus well established, as demonstrated by the number of projects based on it (like [2, 15, 33, 43, 53]).

3) Support: Sawtooth has a good official and community-based support. Fabric support, however, is even better [13].

4) Flexibility: Both Fabric and Sawtooth provide a very flexible and modular architecture. Both platforms support the definition of smart contracts in a wide range of programming languages.

5) Resiliency: Because of their modular architecture, both the platforms can swap the used consensus algorithm. By limiting the analysis on the official implementations only, Sawtooth offers both CFT (Raft) and BFT (PBFT, PoET) algorithms, while Fabric only CFT ones (Raft, Kafka).

6) Finality: Raft e PBFT are deterministic algorithms, while PoET is a probabilistic one.

7) Privacy: Sawtooth does not present a functionality to share information whith only a subset of the network, while Fabric does (channels). This feature, however, is not particularly relevant for the use case analyzed by this article.

8) Interoperability: None of the two platforms offers a mechanism to enable the interoperability of two separate networks (but there is a proposal for Fabric [39]). As the previous one, this feature is not relevant for the analyzed use case.

9) Efficiency: Fabric has an efficiency edge compared to Sawtooth. However, Fabric does use only CFT algorithms (which are ligther but less secure than the BFT ones) and it allows to reduce the minimum number of nodes that must process a given transaction (which improves efficiency at the cost of security). Nonetheless, the peculiar transaction processing strategy employed by Fabric (execute-order-validate) should still make it more efficient.

10) Scalability: The PBFT algorithm is a good fit only for small networks, while Raft and PoET do not suffer from such a limitation.

C. Entities

Each entity in the system has a unique identifier.

1) Actor: it is any entity that submits transactions to the system. For each actor, the system stores a unique identifier and the actor's public key. Moreover, each actor is associated with a set of strings to prevent the replay attack: each transaction must contain one of the strings already stored and a replacement to it, which makes the system adhere to the UTXO model.

2) Policy: it associates an operation to the list of actors that are allowed to perform it. Moreover, it allows to delegate an operation to a secondary policy, in case the regulated entity provides one. This is particularly relevant in the following scenario: a battery owner wants to move a battery between two of his warehouses by outsourcing the delivery to an external company. He wants to keep the control over the battery but, at the same time, he needs to grant some permissions to the external company. Unfortunately, he is unaware of how the delivery will be handled: the external company could, in turn, rely on a third party and so on. In such a scenario, the battery owner should ask for the details of how his delivery will be handled and set up the policy accordingly. With the proposed solution, instead, he would delegate the delivery operation to the secondary policy. The external company could then set the policy according to its internal business logic. At the same time, changing the external company would not require to modify the battery owner's policy.

3) Battery: it is associated with two policies: one is defined by the owner of the battery, while the other by its keeper. The latter is considered only if the former delegates one or more operations. The battery state is updated only in case of problems with the battery. The state is composed of: temperature, shock, position, power level, time, owner, keeper.

4) Archive: it represents a circular buffer used to store the updates to the state of the batteries. In this way, the system limits the quantity of data recorded.

5) Proposal: it is used to replace the policy regulating an entity. A policy can be seen as a generalization of the concept of ownership (custodianship). As such, both the former and the new owner (keeper) must agree on the exchange. A proposal stores the list of batteries to update, the proposed new policy and its type (owner or keeper), and the actor who started the exchange.

D. Operations

1) Actor: he can register himself to the system by submitting a transaction containing a unique identifier.

2) Policy: it can be created by any actor. It can also be updated by adding or removing entries from the list of actors which are allowed to perform a given operation.

3) Battery: at the moment of creation, each battery must be associated to a sensor, which is responsible to update the state (position, temperature, power level, shock) in case one of such parameters is not normal. Moreover each battery is regulated by two policies, which can be replaced through a proposal.

4) Archive: it only allows the append operation, which is self-managed and executed as a consequence of the evolving state of the ledger.

5) Proposal: it can be created or accepted. At the moment of creation, the promoter must specify an identifier, the new policy value and type, and the list of batteries affected. The proposal can only be accepted as-is, and it cannot be updated in any way.

E. Security analysis

1) Replay attack: these attacks are prevented by including in each transaction two additional strings: one must match the one currently stored in the system, while the other will be its replacement. In this way, submitting the same transaction twice will generate a mismatch between the string stored in the state and the one provided by the transaction. Of course, transactions must be digitally signed. In order to improve concurrency, a configurable number of strings is associated to each actor, who is also in charge of updating them without repeating any previous value.

2) Phisical attacks: these attacks could compromise the system. However, because the sensors used are placed inside the batteries, this kind of attack is considered to be cost ineffective: each battery system should be disassembled, corrupted, and then assembled again. A possible future improvement could be the integration of physically unclonable functions [24].

3) Collusion: as long as the colluding part is numerically inferior to the 33% of the nodes, the PBFT consensus algorithm should guarantee the correct behavior of the system. It is important to notice, however, that the system heavily relies on the manufacturer of the sensors, who could leak the private key used by one of its sensors. Such a problem could be mitigated by the usage of a trusted execution environment produced by an external company, in order to guarantee that the private key is generated randomly and that it is known only to the sensor itself.

F. Cost Esteem

Table I reports a cost esteem for the system.

TABLE I
ESTEEMED SYSTEM COST IN $/MONTH

Platform	Cost per organization (one node)	Total cost (15 nodes)
Amazon Web Services	350±50 $/month	5300±800 $/month
Microsoft Azure	400±50 $/month	6000±800 $/month
Google Cloud	300±50 $/month	4500±800 $/month

IV. PRELIMINARY TESTS

This section describes the tests performed on the implemented system, according to the Hyperledger guidelines [62].

A. Test environment

The tests are performed using a single computer and the Docker platform to virtualize a BC network of five validators. The transaction processors[3]are implemented in Go, while the clients in Typescript. In order to record the system metrics and to visualize them, InfluxDb and Grafana are used, as described in [30].

1) Hardware configuration:

- MODEL: MacBook Pro (Retina, 13-inch, 2015);
- CPU: Intel Core i5, 2.70GHz, Dual-Core;;
- RAM: 8 GB 1867 MHz DDR3;
- DISK: 121 GB.

2) Software configuration:

- macOS: 10.15.5 (19F101);
- Docker: version 19.03.8, build afacb8b;
- Sawtooth: 1.2;
- Go: version go1.14.3 darwin/amd64;
- Node: v12.16.1;
- Angular: 8.3.1;
- InfluxDB: 1.8;
- Grafana: 6.4.2;
- 83.0.4103.116, launched with the "–disable-web-security" command line option to avoid problems related to the CORS policy,

3) Network configuration:

- Consensus protocol: PBFT;
- Geographic distribution: co-located nodes;
- Network model: 5-node complete graph;
- Number of nodes involved in the test transaction: 5;
- Software component dependencies: none, other than the default ones.

4) Blockchain properties configuration:

- sawtooth.publisher.max_batches_per_block: 1000;
- sawtooth.validator.max_transactions_per_block: 1000;
- sawtooth.poet.ztest_minimum_win_count: 999999999.

5) Validators' properties configuration:

- peering: dynamic;
- scheduler: parallel;
- network: trust;

B. Methodology

1) Test tools and frameworks: the tests are performed in a local environment, thus the client is hosted on the same machine of the network of validators. Network load is generated

[3]In the Sawtooth environment, smart contract are called *transaction processors.*

and captured using the Angular framework and the Google Chrome web browser.

2) Workload: the workload is generated by a simulator which submits 15 transactions per second (tps).

3) Finality threshold: the PBFT is a deterministic algorithm, so the finality threshold parameter is meaningless.

4) Measure type: the focus of this work is on the transaction throughput measure (TPS), defined as: *total committed transactions / total time in seconds* [62].

5) Observation points: the BC performance is measured from the perspective of a validator.

6) Transactions characteristics: the transactions used for testing purposes can all be considered small and simple: even transactions that are linear in the number of entities defined in the system can be considered simple as a consequence of the limited simulation time (and entities created). The dependencies and data access patterns of the transactions follow the ones of a simple production use.

C. Batch size variation

Sawtooth offers the possibility to execute a group of transactions as a whole (batch). In this test, transactions are submitted in batches of various sizes. The results are shown in figure 1.

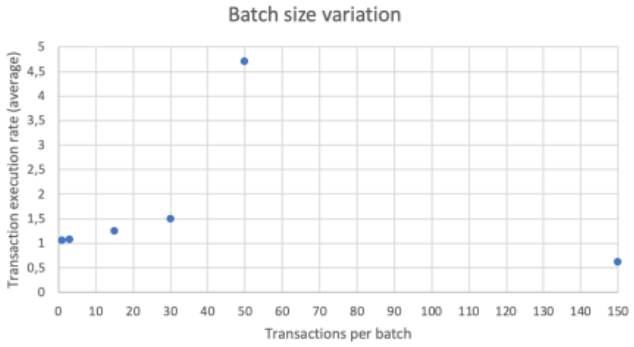

Fig. 1. Test: batch size variation.

D. Submission interval variation

In this test, an increasing wait interval is kept among the submission of two groups of transactions. The results are shown in figure 2

V. Conclusion

This paper, after a discussion on how the blockchain technology could improve the sharing of data and the supply chain digitalization, and thus contribute to a propagation of the *Logistics 4.0* revolution, describes a framework to monitor the proper storage, handling and recharging of the electric batteries, in the electric vehicles supply chain context. The system is based on a flexible access control system, which allows to separate the concerns of the various actors while preserving the security of the system. Moreover, a cost esteem and a security analysis are provided. While the system is resilient to replay attacks, it could be improved in order to reduce the risk of physical attacks or of possible collusion attempts among some supply chain members. Finally, some tests are performed on the system in a local environment. The results obtained can be used to properly configure the system. As a part of an ongoing project, future researches will be aimed at modifying the system in order to satisfy the needs of the project members, and thus to make it more suitable for the electric vehicles supply chain.

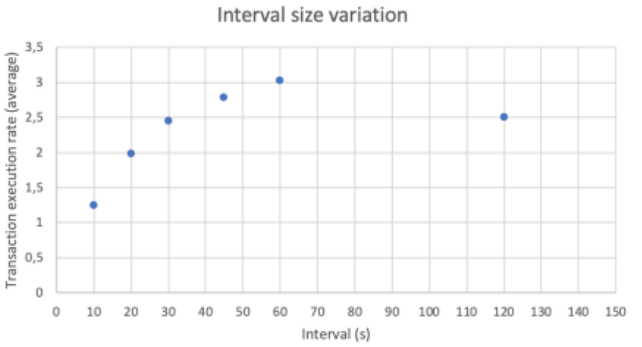

Fig. 2. Test: submission interval variation.

References

[1] Alice Consortium, "Alice recommendations to h2020 work programs 2018-2020," 2016.

[2] A. Arena, A. Bianchini, P. Perazzo, C. Vallati, and G. Dini, "Bruschetta: An iot blockchain-based framework for certifying extra virgin olive oil supply chain," 2019, pp. 173–179, cited By 3.

[3] S. Arumugam, V. Umashankar, N. Narendra, R. Badrinath, A. Mujumdar, J. Holler, and A. Hernandez, "Iot enabled smart logistics using smart contracts," 2018, cited By 7.

[4] L. Augusto, R. Costa, J. Ferreira, and R. Jardim-Goncalves, "An application of ethereum smart contracts and iot to logistics," 2019, pp. 1–7, cited By 1.

[5] A. Baliga, "The blockchain landscape," *Persistent Systems*, 2016.

[6] ——, "Understanding blockchain consensus models," 2017.

[7] G. Baralla, A. Pinna, R. Tonelli, M. Marchesi, and S. Ibba, "Ensuring transparency and traceability of food local products: A blockchain application to a smart tourism region," *Concurrency Computation*, 2020, cited By 0.

[8] T. Bocek, B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere - a use-case of blockchains in the pharma supply-chain," 2017, pp. 772–777, cited By 115.

[9] D. Bumblauskas, A. Mann, B. Dugan, and J. Rittmer, "A blockchain use case in food distribution: Do you know where your food has been?" *International Journal of Information Management*, vol. 52, 2020, cited By 8.

[10] V. Buterin, "Ethereum white paper: A next-generation smart contract and decentralized application platform," 2013.

[11] M. Caro, M. Ali, M. Vecchio, and R. Giaffreda, "Blockchain-based traceability in agri-food supply chain management: A practical implementation," 2018, pp. 1–4, cited By 76.

[12] Center for Disease Control and Prevention. Multistate outbreaks of shiga toxin-producing escherichia coli o26 infections linked to chipotle mexican grill restaurants (final update). [Online]. Available: https://www.cdc.gov/ecoli/2015/O26-11-15/index.html

[13] chainstack.com. Enterprise blockchain protocols evolution index 2020. [Online]. Available: https://chainstack.com/resources/#enterprise-blockchain-protocols-evolution-index-2020

[14] C. D. Clack, V. A. Bakshi, and L. Braine, "Smart contract templates: foundations, design landscape and research directions," *arXiv preprint arXiv:1608.00771*, 2016.

[15] P. Cui, J. Dixon, U. Guin, and D. Dimase, "A blockchain-based framework for supply chain provenance," *IEEE Access*, vol. 7, pp. 157 113–157 125, 2019, cited By 2.

[16] T. Dasaklis and F. Casino, "Improving vendor-managed inventory strategy based on internet of things (iot) applications and blockchain technology," 2019, pp. 50–55, cited By 4.

[17] N. Diarra, "Choosing a consensus protocol for uses cases in distributed ledger technologies," in *2019 Sixth International Conference on Software Defined Systems (SDS)*. IEEE, 2019, pp. 306–309.

[18] L. Domingo Galindo, "The challenges of logistics 4.0 for the supply chain management and the information technology," Master's thesis, NTNU, 2016.

[19] S. Figorilli, F. Antonucci, C. Costa, F. Pallottino, L. Raso, M. Castiglione, E. Pinci, D. Del Vecchio, G. Colle, A. Proto, G. Sperandio, and P. Menesatti, "A blockchain implementation prototype for the electronic open source traceability of wood along the whole supply chain," *Sensors (Switzerland)*, vol. 18, no. 9, 2018, cited By 30.

[20] B. Florea and D. Taralunga, "Blockchain iot for smart electric vehicles battery management," *Sustainability (Switzerland)*, vol. 12, no. 10, 2020, cited By 1.

[21] J. Frank, K. Chin, and S. Silverstein. The man that won the nobel prize in economics for contract theory shares his thoughts on smart contracts. [Online]. Available: https://www.businessinsider.com/nobel-prize-winner-in-economics-shares-his-thoughts-on-smart-contracts-2018-5?IR=T

[22] M. Giancaspro, "Is a 'smart contract' really a smart idea? insights from a legal perspective," *Computer Law & Security Review*, vol. 33, 06 2017.

[23] T. Groenfeldt. Ibm and maersk apply blockchain to container shipping. [Online]. Available: https://www.forbes.com/sites/tomgroenfeldt/2017/03/05/ibm-and-maersk-apply-blockchain-to-container-shipping/#10045ed13f05

[24] U. Guin, P. Cui, and A. Skjellum, "Ensuring proof-of-authenticity of iot edge devices using blockchain technology," 2018, pp. 1042–1049, cited By 12.

[25] N. Hackius and M. Petersen, "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*, 2017, pp. 3–18.

[26] H. Hasan, E. AlHadhrami, A. AlDhaheri, K. Salah, and R. Jayaraman, "Smart contract-based approach for efficient shipment management," *Computers and Industrial Engineering*, vol. 136, pp. 149–159, 2019, cited By 7.

[27] P. Helo and A. Shamsuzzoha, "Real-time supply chain—a blockchain architecture for project deliveries," *Robotics and Computer-Integrated Manufacturing*, vol. 63, 2020, cited By 8.

[28] E. Hofmann and M. Rüsch, "Industry 4.0 and the current status as well as future prospects on logistics," *Computers in industry*, vol. 89, pp. 23–34, 2017.

[29] X. Huang, C. Xu, P. Wang, and H. Liu, "Lnsc: A security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13 565–13 574, 2018, cited By 70.

[30] Intel Corporation. Using grafana to display sawtooth metrics. [Online]. Available: https://sawtooth.hyperledger.org/docs/core/nightly/1-2/sysadmin_guide/grafana_configuration.html

[31] P. Jain, "Improving the process of container shipping using blockchain," 2018.

[32] H. Kakavand, N. Sevres, and B. Chilton, "The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies," *SSRN Electronic Journal*, 01 2017.

[33] P. Khan, Y.-C. Byun, and N. Park, "Iot-blockchain enabled optimized provenance system for food industry 4.0 using advanced deep learning," *Sensors (Switzerland)*, vol. 20, no. 10, 2020, cited By 1.

[34] M. Kim, B. Hilton, Z. Burks, and J. Reyes, "Integrating blockchain, smart contract-tokens, and iot to design a food traceability solution," 2019, pp. 335–340, cited By 11.

[35] M. Kim, K. Park, S. Yu, J. Lee, Y. Park, S.-W. Lee, and B. Chung, "A secure charging system for electric vehicles based on blockchain," *Sensors (Switzerland)*, vol. 19, no. 13, 2019, cited By 6.

[36] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Computer Science - Research and Development*, vol. 33, no. 1-2, pp. 71–79, 2018, cited By 44.

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

[38] A. Lechmere. Wine vault offers security in a digital age. [Online]. Available: https://www.wine-searcher.com/m/2016/12/wine-vault-offers-security-in-a-digital-age

[39] T. Li. Fabric interop working group. [Online]. Available: https://wiki.hyperledger.org/display/fabric/Fabric+Interop+Working+Group

[40] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *International Journal of Network Security*, vol. 19, pp. 653–659, 09 2017.

[41] C. Liu, K. Chai, X. Zhang, E. Lau, and Y. Chen, "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 25 657–25 665, 2018, cited By 50.

[42] F. Liu, Y. Liu, J. Gao, and J. Zhang, "Food safety incidents in beijing: occurrence patterns, causes and wider social implications," *Palgrave Communications*, vol. 1, p. 15029, 2015.

[43] S. Malik, V. Dedeoglu, S. Kanhere, and R. Jurdak, "Trustchain: Trust management in blockchain and iot supported supply chains," 2019, pp. 184–193, cited By 4.

[44] N. Maouriyan and A. Krishna, "Aquachain-water supply-chain management using distributed ledger technology," 2019, pp. 204–207, cited By 1.

[45] J. T. Mentzer, W. DeWitt, J. S. Keebler, S. Min, N. W. Nix, C. D. Smith, and Z. G. Zacharia, "Defining supply chain management," *Journal of Business logistics*, vol. 22, no. 2, pp. 1–25, 2001.

[46] S. Mondal, K. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, and P. Chahal, "Blockchain inspired rfid-based information architecture for food supply chain," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5803–5813, 2019, cited By 18.

[47] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Cryptography Mailing list at https://metzdowd.com*, 03 2009.

[48] A. Narayanan. "private blockchain" is just a confusing name for a shared database. [Online]. Available: https://freedom-to-tinker.com/2015/09/18/private-blockchain-is-just-a-confusing-name-for-a-shared-database/

[49] T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," *Journal of Information Processing Systems*, vol. 14, pp. 101–128, 01 2018.

[50] OECD. Trade in fake goods is now 3.3% of world trade and rising. [Online]. Available: https://blogs.lse.ac.uk/businessreview/2018/02/08/how-blockchain-can-help-the-fight-against-counterfeit-goods/

[51] OECD and EUIPO. Trends in trade in counterfeit and pirated goods: the updated picture. [Online]. Available: https://ec.europa.eu/growth/content/trends-trade-counterfeit-and-pirated-goods-updated-picture_en

[52] S. Ølnes, J. Ubacht, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," 2017.

[53] G. Perboli, S. Musso, and M. Rosano, "Blockchain in logistics and supply chain: a lean approach for designing real-world use cases," *IEEE Access*, vol. PP, pp. 1–1, 10 2018.

[54] G. Perboli, V. Capocasale, and D. Gotta, "Blockchain-based transaction management in smart logistics: A saw-tooth framework," in *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 2020, pp. 1713–1718.

[55] R. Rake. Supply chain management market by component (solution and services), solution type (transportation management system, warehouse management system, sourcing & procurement, supply chain planning, and manufacturing execution system), deployment model (on-premise and cloud), user type (small & medium sized enterprises, and large enterprises), and industry vertical (retail & consumer goods, healthcare & pharmaceuticals, manufacturing, food & beverages, transportation & logistics, automotive, and others): Global opportunity analysis and industry forecast, 2020-2027. [Online]. Available: https://www.alliedmarketresearch.com/supply-chain-management-software-market

[56] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *International Journal of Production Research*, vol. 57, no. 7, pp. 2117–2135, 2019.

[57] N. Schmidtke, F. Behrendt, L. Thater, and S. Meixner, "Technical potentials and challenges within internal logistics 4.0," in *2018 4th International Conference on Logistics Operations Management (GOL)*. IEEE, 2018, pp. 1–10.

[58] F. Silva, M. Ahmed, J. Martínez, and Y.-C. Kim, "Design and implementation of a blockchain-based energy trading platform for electric vehicles in smart campus parking lots," *Energies*, vol. 12, no. 24, 2019, cited By 2.

[59] D. Stanway and N. Macfie. China uncovers 500,000 food safety violations in nine months. [Online]. Available: https://www.reuters.com/article/us-china-food-safety/china-uncovers-500000-food-safety-violations-in-nine-months-idUSKBN14D046

[60] J. O. Strandhagen, L. R. Vallandingham, G. Fragapane, J. W. Strandhagen, A. B. H. Stangeland, and N. Sharma, "Logistics 4.0 and emerging sustainable business models," *Advances in Manufacturing*, vol. 5, no. 4, pp. 359–369, 2017.

[61] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4601–4613, 2019, cited By 49.

[62] The Hyperledger Performance and Scale Working Group. Hyperledger blockchain performance metrics. [Online]. Available: https://www.hyperledger.org/resources/publications/blockchain-performance-metrics

[63] Y. Tsang, K. Choy, C. Wu, G. Ho, and H. Lam, "Blockchain-driven iot for food traceability with an integrated consensus mechanism," *IEEE Access*, vol. 7, pp. 129 000–129 017, 2019, cited By 13.

[64] A. Vey and A. Monari. How blockchain can help the fight against counterfeit goods. [Online]. Available: https://blogs.lse.ac.uk/businessreview/2018/02/08/how-blockchain-can-help-the-fight-against-counterfeit-goods/

[65] Y. Wang, J. H. Han, and P. Beynon-Davies, "Understanding blockchain technology for future supply chains: a systematic literature review and research agenda," *Supply Chain Management: An International Journal*, 2019.

[66] S. Winkelhaus and E. H. Grosse, "Logistics 4.0: a systematic review towards a new logistics system," *International Journal of Production Research*, vol. 58, no. 1, pp. 18–43, 2020.

[67] K. Wüst and A. Gervais, "Do you need a blockchain?" in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. IEEE, 2018, pp. 45–54.

[68] F. Yiannas, "A new era of food transparency powered by blockchain," *Innovations: Technology, Governance, Globalization*, vol. 12, no. 1-2, pp. 46–56, 2018.

[69] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, p. 352, 10 2018.