



Technical State-of-the-Art of Supply Chain Visibility

Andrea d'Auria¹, Wout Hofman¹, Erik de Graaf¹ and Jeroen Breteler¹

1. TNO, Soesterberg, Netherlands

Abstract: *This article presents a literature study on the state-of-the-art of the technology adopted for Supply Chain Visibility (SCV) and identifies blockchain as the major player for innovation. The first section highlights the trade-off between immutability and confidentiality in distributed ledger technologies, and discusses the mismatch of interests between academic research and enterprise research and development. Then, three private blockchain platforms (Quorum, Hyperledger Fabric and Corda) are evaluated as solutions for confidentiality in shared databases. The third section examines the role of standards for logistics data. The paper concludes that blockchain is the number one technology contemplated for SCV both in academic discourse and in the private sector, however the former favors immutability and transparency while the latter favors confidentiality. By making this trade-off explicit and analyzing the different solutions offered by the main related technologies, this work contributes to a clearer identification of advantages and disadvantages of options currently available. Additionally, the role of standards is identified as a valuable topic for further research, and an open standard for SCV is deemed to be desirable to ensure interoperability between systems relying on different technology stacks.*

Conference Topic(s): *Systems and technologies for interconnected Logistics (blockchain, digital twins), New communication Networks enabling interconnected logistics*

Keywords: *supply chain visibility, blockchain, distributed ledgers, decentralization, digital twins, standards, data models, confidentiality*

1 Introduction

The future of interconnected logistics will rely on faithful representation of reality in data spaces. The movement of physical goods along supply-chains can no longer be considered as a separate self-standing instance from the data describing such movement or the digital twins describing the goods themselves. This interconnection creates new possibilities – like a higher degree of transparency for Supply Chain Visibility (SCV) – but creates new challenges as well – like the management of shared databases and the confidentiality of related data. This article presents the state of the art regarding the technological direction that SCV is taking both from an academical point of view and with an eye kept on the market. A selection of the most relevant scientific papers has been used to analyze what requirements are privileged and met. The analysis was further elaborated by integrating the technical knowledge on platforms that can support SCV.

In this work the concepts of transparency, visibility and traceability are used in the context of supply chain and data sharing, and they are closely related one to another: transparency, in supply chains, refers to the infrastructure layer where data is confined. Having this layer be transparent means that data in there is visible. Visibility refers to the ability of accessing and seeing a piece of data. Traceability is the capability of following "traces" of an object along a supply chain, for example, one could trace a cargo object being moved from one location to another. Such traces are data about events involving the object. The concept of traceability is

inherently tied to the one of visibility: in order to track an object, one needs to have full visibility on the data that makes up the trace.

More specifically, Supply Chain Visibility can be defined as “awareness of and control over end-to-end supply chain information – including insight in sources of data and whereabouts of goods – enabling agile, resilient, sustainable as well as compliant and trusted supply chains” (Wieland & Wallenburg, 2013).

In section 2 of this document the current state of research is investigated, highlighting the difference between academic and enterprise environments when coming to preferred features and requirements, and a possible explanation for this mismatch is given. The trade-off between immutability and confidentiality is made explicit and formalized.

In section 3 a deeper insight about how the major private blockchain platforms (Quorum, Hyperledger Fabric and Corda) handle private data is given as well as a further elaboration about how their design choices relate to the immutability-confidentiality trade-off.

In section 4 the role of standards is introduced as well, and an overview of the major ones is given.

2 State of the Art

Scientific papers taken into account for the following work are mostly from IEEE, as it is the leading organization for technology advancement and a good compromise to narrow down the literature that could also be found elsewhere.

Through use of the IEEE search engine it emerged that about 41% of the results (20 out of 49) related to SCV in the last two years (2019-2020) also involved blockchain. This highlights a strong interest for distributed ledger technologies (DLT) for SCV.

Even among those not explicitly mentioning blockchain technology, some underline clear requirements for data transparency and smooth coordination (Yanamandra, 2019), which relates to DLT because transparency can be easily achieved with replicated databases, and the use of smart contracts can smoothen and automatize coordination between different stakeholders.

The first general remark that one can observe from a perspective of the functionalities required, is that most of the papers point their attention to visibility of data, tamper-proof characteristics, and trust among stakeholders. The main concerns are, therefore, driven by the data that is currently not available along the supply chain, the data being altered because of self-interest of one party against the others, and the lack of trust between such parties.

Consequently, within many academic papers DLT is identified as a good opportunity to tackle those issues.

However, there is a mismatch in expectations between the academical environment and the private sector, supply and logistics stakeholders. This discrepancy is especially evident when taking into consideration the transparency requirement. Transparency means that data will be available and auditable (visible) by all parties joining the network, and the academical works examined in this context very much rely on this assumption. However, transparency – which also relates to a higher degree of immutability – comes at the cost of confidentiality – which is an important requirement for companies. Confidentiality relates to commercial sensitivity of business relations that will be made transparent when blockchain technology is applied for SCV.

In order to better understand the nature of this trade-off, mentioned by Kannengiesser et al (2019), it is worthwhile to highlight what is the link between transparency and immutability. Blockchains are considered a subset of DLT, with the added characteristic that data is replicated at each node. This complete replication is fundamental to reach a consensus in the network and every node is responsible to keep and validate the whole set of transactions from the first genesis

block. Immutability can be guaranteed because the infrastructure is transparent and data is fully visible. As soon as a malicious agent operating a node tried to tamper with data previously shared with the network, such attempt would be immediately evident and could be prevented. The opposite situation is one where only one central non-transparent database exists, with users relying on its data. In this case a malicious agent controlling the central database could tamper with the data, and as long as other parties do not have visibility on historical data it is impossible for them to assess whether there have been alterations.

Most of the investigated papers did not work on a real-world use-case dealing with true needs of a company, and assumed that full transparency and data sharing among stakeholders was a fair assumption. Nevertheless, when the research deals with a real enterprise use-case, the need for confidentiality over data emerges clearly (d'Auria, 2020).

This ambiguity also showed up during the conference of the Blockchain Observatory of the Politecnico di Milano of January 2020: while their research highlighted that the future of the technology relies on public blockchains, almost all the companies invited on the stage were actually developing private solutions (Perego et al, 2020).

The demand for confidentiality over data is stronger among companies, and this is reflected in the implementation choices they make, as shown in Table 1.

Company	Platform	Field
ABI	Corda	Finance
Adledger	Hyperledger Fabric	Advertising
B3I	Corda	Insurance
Finality	Private Ethereum	Finance
Food Trust	Hyperledger Fabric	Agri-food
HM Land Registry	Corda	Notarization
Komgo	Private Ethereum	Finance
LO3 Energy	Private Ethereum	Energy Utility
LVMH Aura	Quorum	Luxury
Marco Polo	Corda	Finance
Santander	Ethereum	Finance
SDX – Six Digital Exchange	Corda	Finance
Tradelens	Hyperledger Fabric	Logistics
uPort Zugo	Ethereum	SSI
Vakt	Quorum	Utility
Verified.Me	Hyperledger Fabric	SSI
Vinturas	Hyperledger Fabric	Logistics
Voltron	Corda	Finance
We.trade	Hyperledger Fabric	Finance

Table 1: Platforms chosen by companies for implementation of their services[4].

The data shown in Figure 1 clarifies that while scientific papers are focused mainly on the features of immutability and trustlessness, companies try to pull more towards the confidentiality side of the trade-off.

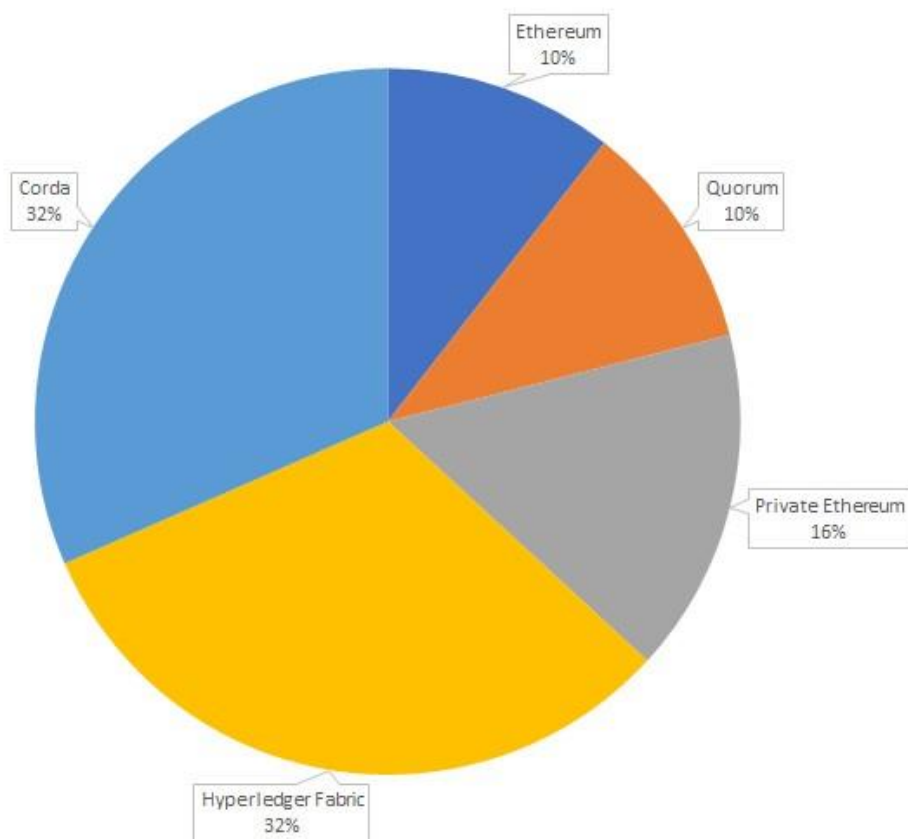


Figure 1: Platform distribution according to Table 1.

One approach (Hofman, 2020) goes deeper into formalizing the functionalities required and assessed that a platform for SCV should integrate:

- A subscription mechanism;
- Digital twins;
- Milestones and events.

These concepts are compatible with DLT.

3 Technologies along the spectrum of the trade-off

While the DLT landscape still maintains some characteristics of chaotic behavior – with new solutions and platforms being born and abandoned frequently – some tools are well established in the environment and regarded as solid and reliable, as the previous chart shows. In the following sections a deeper insight on how the main DLT platforms (namely: Quorum, Hyperledger Fabric and Corda) position themselves along the spectrum of the trade-off discussed in this article is given.

3.1 Quorum

In this article we refer to Quorum as the generic name for the project developed under ConsenSys umbrella which involves two pieces of software: GoQuorum and Hyperledger Besu. The choice of referring to it as one is motivated by the fact that they share the same design choices, and being under the same umbrella they will increase their interoperability over time.

Quorum is an Ethereum-like private blockchain which emulates Ethereum behavior and protocol in a confined environment – i.e. not necessarily open.

On top of the standard Ethereum-like functioning, Quorum provides private transactions (which translates into private smart contracts) allowing only specific nodes to receive private transactions.

When a transaction is submitted privately to the network (a call to a private smart contract) it originates a split in the state of receiving nodes:

- Everyone will receive a transaction with a hashed payload, which will not imply any update of the state per se;
- Only specific nodes will receive the plaintext transaction in a peer-to-peer communication, and will store it in a separate database, and link it to the hashed transaction in the main database, causing an actual update in the state;

So different nodes will see different states according to what they are allowed to see.

Quorum allows also the following “privacy enhancement” features:

Counter Party Protection (CPP): it prevents non-participant interaction on a private contract but allows state divergence (i.e. it will allow nodes to maintain different state through private transaction to “self” or “subset of nodes”). Nodes which are not part of a private smart contract, are still able to submit transactions to a private smart contract by default. They will not be able to record the update of the state, though. If CPP is enabled this behavior is prevented and it can substitute some strategies for access control.

Private State Validation: On top of all the verifications of CPP, it introduces further checks in order to prevent nodes from state deviations. Private transactions to “self” or “subset of nodes” will then fail, the full list of recipients is shared among all nodes and all transactions are validated against it. In standard private smart contracts – or with only CPP enabled – only the sending node knows – and it is free to choose – the list of recipients.

3.2 Hyperledger Fabric

Hyperledger Fabric is an open source private blockchain created by IBM, and it allows deep customization opportunities when coming to private data.

The offered options revolve around two main concepts:

- Channels
- Collections

Channels are wholly separate blockchains within the same networks, i.e. nodes and identities are kept within the network but different subset of nodes can run different blockchains, and there is neither communication nor access between different channels.

Collections are an implementation of private transactions within a channel. The core principle is the following: private transactions are hashed before submission to the ordering service – which appends them to the ledger together with public transactions – and those authorized to see such transactions have a "Private State Database" where plaintext is stored. Private data is disseminated encrypted peer-to-peer among nodes.

Important considerations:

- You do not necessarily have to be a member of a collection to write to a key in a collection, as long as the endorsement policy is satisfied. Endorsement policies can be defined at chaincode level, key level (using state-based endorsement), or collection level. In other words also nodes not allowed to read private transactions in a collection, are allowed to write a private transaction (visible to others) as long as they can make it consistent;
- Data hashes can be verified at chaincode level, meaning that one can prove that a transaction was already submitted to the ledger.

One should opt for channels when entire sets of transactions (and ledgers) must be kept confidential within the set of organizations that make up the channel. It is as effectively running different blockchains within the same network: those outside a channel do not have access to any of its information.

One should opt for collections when transactions (and ledgers) must be shared among a set of organizations, but when only a subset of those organizations should have access to some (or all) of the data within a transaction.

3.3 Corda

Corda is an open source platform backed by R3, which functions in a different way than standard blockchains. The platform is highly focused on confidentiality, yet borrowing concepts from blockchain to provide a certain degree of immutability.

Corda has two main entities participating to the network:

- Nodes
- Notaries

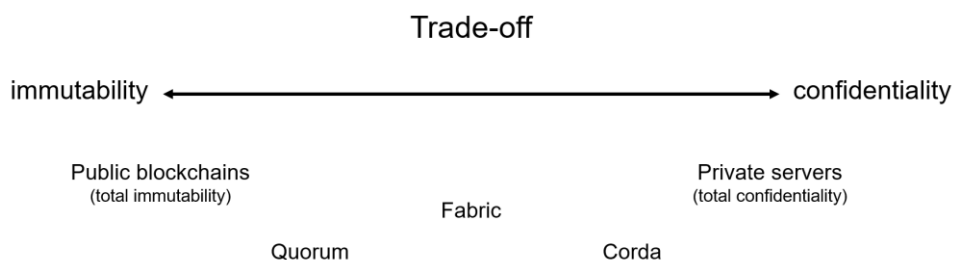
Notaries receive and store hashes of transactions and can validate them; nodes submit transactions on a need-to-know basis. Privacy is therefore granted by default because notaries, which have a broader overall view of the transactions happening in the network, only store fingerprints of them. Nodes have a full view of transactions they submit and receive, but cannot see transactions not related to them, resulting in an only partial view of the ledger.

Within Corda nodes can have a different view of what is there in the ledger, and consistency – and immutability – is guaranteed by notaries.

Communication develops on two levels: nodes disseminate data peer-to-peer, notaries disseminate transactions between them according to a pre-set consensus mechanism.

3.4 Considerations and Comparisons

One can roughly position the examined platforms as follows:



Hyperledger Fabric resulted in a very versatile tool thanks to the wide range of options that allow to use it both as very open and transparent classical blockchain and as a more closed environment with privacy measures in place. In this, it shares some similarities with Quorum for the way it implements the concept of collections: both are based on storing “publicly” (within the network) only a fingerprint of the actual data stored in a separated, confined, database. However, Fabric took this a step further with channels – wholly separated non-communicating blockchains within the same network of nodes – which made it get a step closer to confidentiality and one further from immutability.

Corda, as shown in the previous section, differs more significantly from both the other two and from blockchain platforms in general, as the concept of a replicated database owned by every node – crucial in blockchains – is not implemented in Corda. This makes it more

privacy-prone than the major counterparts, however it also results in a lower degree of immutability. Considering this design is the default in Corda, it pushes it towards the “confidentiality” side of the spectrum.

The borders presented in this paper are not fixed and rigid, they aim to give a rough overview on how different design choices can influence immutability and confidentiality instead: Quorum could enable strict policies and use only private smart contracts moving more to the centre, and Corda, likewise, could disseminate all the data openly and transparently with the whole network. This, in both cases, would imply not fully taking advantages of the strengths of the different design choices that were made for the various platforms.

Being at the “center” of the spectrum does not necessarily mean being in the best position. Saving the most of both equally means losing the most of both. The choice of a platform should rely on a more ad-hoc analysis of what is more important for a specific use-case and on the actual state of development of the platform and community support.

4 The Role of Standards

Going beyond technology, only a small portion of the examined papers took the requirement for a common data model into account, and only one paper considered it a crucial step for the achievement of effective software development (Grest, Luras et al, 2019). As the industry is looking with interest at the subject, some standards are developed to support SCV. A common data sharing infrastructure – like a blockchain – can enforce a data model coded into smart contracts for everyone joining the network. However, such a system must be able to interoperate with external systems and thus share a common grammar. Agreeing on a common standard can help both to enhance adoption of a shared infrastructure, and to ease interoperability between different ones.

Besides these standards, there are also various platforms providing visibility, either with proprietary interfaces or based on (open or de facto) standards. Examples of these platforms are Tradelens (visibility of container transport via sea, developed as joint initiative by Maersk and IBM) and Transfollow (visibility of road transport).

We can find among others the following SCV-related standards:

- OpenTripModel (OTM)
- EPCIS Data Model (GS1 Standard)

4.1 OpenTripModel

OpenTripModel (OpenTripModel Documentation, 2021) (OTM) was funded by the Dutch government, developed initially by Simacan but now public and open for contribution. Its maintenance is organized by SUTC (Stichting Uniforme Transport Code), governed by the major road transport association TLN and the association of shippers with their own transport and forwarder (EVO/FENEDEX). Some important companies (DLG and PostNL Transport among others) have already experimented with it.

The main characteristics are the following:

- The model is independent of how transport within a supply chain is organized;
- The model is intended to be independent of any transport modality, although it is not applied as such and SUTC does not have participation of other transport modalities beside road;
- The data is human and machine-readable;
- The model is extensible;

The model is based on the concepts of Lifecycle, Entities and Events. The Lifecycle provides a context to the phase of an operation – ”planned”, ”projected”, ”actual” or ”realized”. Entities are the basic components of the supply chain – location, vehicle, actor, etc. Entities could be envisioned as Digital Twins. Events are also Entities, but they are tied to a Lifecycle. They model the relations between Entities.

4.2 EPCIS Data Model – GS1

The basic unit of data in EPCIS (Electronic Product Code Information System) is the EPCIS event (GS1 Official Website, 2021), which is a structure that describes the completion of one business step within an overall business process. A group of EPCIS events provides a detailed description of a business process.

Each EPCIS event is composed of the following:

- **What**
The identifiers of the objects related to the event;
- **When**
The date and time when the event took place;
- **Where**
The identifier of the location at which the event occurred, and identifier of the location where the objects are expected to be following the event;
- **Why**
Information about the business context.

This standard is currently adopted by for instance the Metro Group.

4.3 Considerations on Standards

Standards are a complex issue. Standards for interfaces, products, or services need to be produced in such a way that implementers can access them (publicly available, potentially against low costs) and can assess how the standard was developed. Standards can be categorized according to the nature of their development and maintenance processes:

- Open standards – those that are developed by recognized standardization bodies
- De facto standards – those that have not been developed and are not maintained by a recognized standardization body, but are used by most organizations.
- Proprietary standards – those that have been developed and are maintained by a limited group of organizations. The procedures are not transparent.

In this view, OTM can be considered as a proprietary standard. It is not yet a de facto one. TradeLens, for instance, develops a de facto standard for SCV for sea transport. It has been the basis for Vinturas, where IBM also participates in the development of the solution.

5 Conclusion

Blockchain is the number one technology contemplated for Supply Chain Visibility in research. However, there is a distinct view between academic research and research and development in the private sector: the former supports transparency and the latter requires confidentiality. Given this, research is required into access control and data management for SCV in blockchain technology. Different technologies have different solutions to this challenge. In the realm of private blockchains the major actors made different design choices in order to offer to the market different capabilities in terms of immutability and confidentiality. While the needs for immutability and confidentiality are the main drivers when choosing a platform for a given use-case, this trade-off often goes undiscussed in the literature. By making it explicit and analyzing it in this work, we have highlighted the possibilities and opportunities that DLT – blockchain technologies in particular – open for SCV, and at what cost they come. DLT can in fact

effectively enhance immutability and visibility of supply-chain data; at the same time a careful choice of the platform and a meticulous tweaking of its privacy features can effectively mitigate the loss of confidentiality.

Secondly, the role of standards is identified as a valuable topic for further research. In practice there are multiple efforts to develop a proprietary or de facto SCV standard. However, an SCV standard is rarely considered a relevant matter in the context of SCV despite the crucial role that has in the enhancement of interoperability. Solutions with a proprietary interface achieving market adoption are preferred by enterprises (the so-called network effect). Given this, it is useful to come to an open standard for SCV, i.e. a standard that is developed and maintained by a recognized standardization body. Once this is available, various SCV solutions can be developed. It would be of value also to map for instance OTM to the functionality described in Hofman (2020).

References

- Consensys. Retrieved 2021, from GoQuorum Official Documentation: docs.goquorum.consensys.net/en/stable/
- d'Auria, A. (2020). Porting blockchain smart contracts - A feasibility study.
- Divey, S. J., Hekimoglu, M. H., & Ravichandran, T. (2019). Blockchains in supply chains: potential research directions. *2019 IEEE Technology and Engineering Management Conference (TEMSCON)*.
- Grest, M., Luras, M., Montarnal, A., Sarazin, A., & Bousseau, G. (2019). A meta model for a blockchain-based supply chain traceability. IEEE.
- GS1 Official Website: www.gs1.org/standards/epcis - Retrieved 2021
- Hofman, W. (2020). Semantics - Supply Chain Visibility (SCVL) - discussion paper.
- Hyperledger Fabric Official Documentation: hyperledger-fabric.readthedocs.io/en/release-2.2/ - Retrieved 2021
- Jangir, S., Muzumdar, A., Jaiswal, A., Modi, C. N., Chandel, S., & Vyjayanthi, C. (2019). A Novel Framework for Pharmaceutical Supply Chain Management using Distributed Ledger and Smart Contracts. *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*.
- IEEE Search Engine: https://ieeexplore.ieee.org/search/searchresult.jsp?queryText=supply%20chain%20visibility&highlight=true&returnType=SEARCH&matchPubs=true&ranges=2019_2020_Year&returnFacets=ALL&searchWithin=blockchain - Retrieved 2021
- Kannengiesser, N., & Lins, S. (2020). What Does Not Fit Can be Made to Fit! Trade-Offs in Distributed Ledger Technology Designs. *Hawaii International Conference on System Sciences (SSRN Electronic Journal)*.
- Karuanchi, M. D., Sheeba, J., & Devaneyan, S. P. (2019). Cloud Based Supply Chain Management System Using Blockchain. *2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICECCOT)*.
- Kshetri, N., & Loukoianova, E. (2019). Blockchain adoption in supply chain networks in Asia. *IT Professional*.
- Li, Z., Wu, H., King, B., Miled, Z. B., Wassick, J., & Tazelaar, J. (2018). A Hybrid Blockchain Ledger for Supply Chain Visibility. *2018 17th International Symposium on Parallel and Distributed Computing (ISPD)*.
- OpenTripModel Documentation: www.opentripmodel.org/docs - Retrieved 2021
- Perego, A. (2020). Annual Report.
- Pundir, A. K., Jagannath, J. D., Chakraborty, M., & Ganpathy, L. (2019). Technology Integration for Improved Performance: A Case Study in Digitization of Supply Chain

- with Integration of Internet of Things and Blockchain Technology. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*.
- R3. (n.d.). Retrieved 2021, from Corda Official Documentation: docs.corda.net/docs/corda-os/4.6/key-concepts.html
- Raj, R., Rai, N., & Agarwal, S. (2019). Anticounterfeiting in pharmaceutical supply chain by establishing proof of ownership. *TENCON 2019 - IEEE Region 10 Conference*.
- Sahoo, M., Singhar, S. S., Nayak, B., & Mohanta, B. K. (2019). A blockchain based framework secured by ECDSA to curb drug counterfeiting. *10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*.
- Singi, K., Bose, J. C., Podder, S., & Burden, A. P. (2019). Trusted Software Supply Chain. *2019 34th IEEE/ACM International Conference on Automated Software Engineering (ASE)*.
- Transfollow Official Website: transfollow.org - Retrieved 2021
- Wieland, A., & Wallenburg, C. M. (2013). The influence of relational competencies on supply chain resilience: a relational view. *International Journal of Physical Distribution and Logistics Management*.
- Yanamandra, R. (2019). A framework of supply chain strategies to achieve competitive advantage in digital era.