



Building the  
**Web3 Economy**

**JUNE 2021**

# **SUPPLY CHAIN**

## **REFERENCE IMPLEMENTATION**

### **Use Case**

**Parts Traceability**

**MOBI SC0002/RI/2021 Version 1.2**

**Supply Chain (SC) Working Group**

© 2024 MOBI. All rights reserved

# TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

© 2024 MOBI

## 1. Definitions.

“**License**” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

“**Licensor**” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

“**Legal Entity**” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

“**You**” (or “**Your**”) shall mean an individual or Legal Entity exercising permissions granted by this License.

“**Source**” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

“**Object**” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

“**Work**” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

“**Derivative Works**” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

“**Contribution**” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.”

“**Contributor**” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

**2. Grant of Copyright License.** Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

**3. Grant of Patent License.** Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted.

If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

**4. Redistribution.** You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

- a. You must give any other recipients of the Work or Derivative Works a copy of this License; and
- b. You must cause any modified files to carry prominent notices stating that You changed the files; and
- c. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
- d. If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

**5. Submission of Contributions.** Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

**6. Trademarks.** This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

**7. Disclaimer of Warranty.** Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

**8. Limitation of Liability.** In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

**9. Accepting Warranty or Additional Liability.** While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

Licensed under the Apache License, Version 2.0 (the “License”). You may not use this file except in compliance with the License.

**END OF TERMS AND CONDITIONS**

# INTRODUCTION

This standard was issued by MOBI and its members. MOBI is a nonprofit alliance of many of the world's largest vehicle manufacturers, startups, governments/transit agencies, NGOs, financial institutions, e-mobility providers, consultancies, suppliers, logistics providers, and more working to create standards and build the Web3 digital infrastructure for connected ecosystems and IoT commerce.

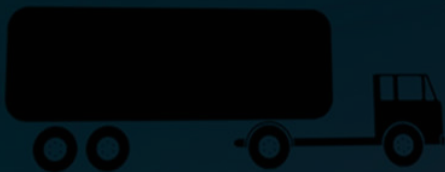
MOBI is creating standards for trusted self-sovereign data and identities (e.g. vehicles, people, businesses, things), verifiable credentials, and cross-industry interoperability, with the goal of making transportation more efficient, equitable, decentralized, and circular, all while preserving the data privacy of users and providers alike. MOBI is technology and ledger agnostic. The work of preparing standards is carried out through MOBI Working Groups. Each member of the consortium interested in a subject for which a Working Group has been established has the right to be represented and participate in that Working Group.

The procedures used to develop this document and those intended for its further maintenance are described in the working group charter. In particular, the different approval criteria needed for the different types of MOBI documents should be noted. Approvals of MOBI Steering Committee and Board of Directors are obtained upon the final document release. Attention is drawn to the possibility that some of the elements of this document may be the subject of intellectual property rights. In accordance with MOBI IPLR policy, a 60-day review period is provided to the MOBI community to disclose any and all IP matters pertaining to this standard. MOBI shall not be held responsible for identifying any or all such rights. Details of any IP rights identified during the development of the document will be in the Introduction upon public release of this standard.

Any trade name used in this document is provided for the convenience of users and does not constitute an endorsement. The Working Group responsible for this document is the Supply Chain (SC) Working Group. Sincere thanks and appreciation are extended to those who contributed their unique insights to the Supply Chain Reference Implementation Architecture.

## CONTACT

[connect@dlt.mobi](mailto:connect@dlt.mobi)  
[www.dlt.mobi](http://www.dlt.mobi)



## **AUTHORS**

Johannes Sedlmeir, FIM Research Center

## **REVIEWERS**

Pramita Mitra, Ford

Dominik Batz, BMW Group

## **CONTRIBUTORS**

Loren Adams, Accenture

Chris Ballinger, MOBI

Sebastian Banescu, Quantstamp

Olof Belfrage, CEVT

Roger Berg, DENSO

Betul Betul Kahya, MOBI

José Manuel Cantera, IOTA Foundation

Josh Cartellone, Accenture

Alisa DiCaprio, R3

Thad Dungan, AWS

Chris Floersch, Honda

Josh Fodale, Ford

Kami Gaweda, Arxum

Jeremy Goodwin, SyncFab

Shannon Hamilton, DLT Labs

Philips Harrison, Fifth-9

Carsten Hiemsch, IBM

Thi Hong Tran, NAIST

Chris Hwee, Honda

Karthik Krishnamurthy, AWS

Marco Lang, Marelli

Jens Lund-Nielsen, IOTA Foundation

Piyush Manocha, Accenture

Daniel Miehle, BMW

Vinay Munjewar, SyncFab

Heiko Musa, BMW

Diwakar Muthu, Ford

Richard Nolk, CEVT

Drew Paroz, Honda

Dean Philips, AWS

Angela Ruthenberg, AutoData Solutions

Kristin Marie Slanina, Thirdware

Anne Smith, IOTA

Kellie Treppa, Thirdware

Carl Youngblood, AWS

## **MOBI TEAM**

Tram Vo, CEO + Founder

Grace Pulliam, Communications Manager

Chris Ballinger, Advisor + Founder

Andreas Freund, CTO


Rajat Rajbhandari, Head of Standards & Certification

Matt Shi, Supply Chain Lead

Betul Kahya, Mobility Lead

Griffin Haskins, Finance Lead

# TABLE OF CONTENTS



Executive Summary .....	1
List of Acronyms .....	2
Glossary of Terms .....	3
Objective of this Document .....	6
Use Case Summary .....	8
Technical Building Blocks and Architectural Considerations .....	12
Technical Workflows .....	15
Use Case Requirements and How the Architecture Addresses Them .....	17
Bibliography .....	20

## EXECUTIVE SUMMARY

*Blockchain/Distributed Ledger Technology in supply chain improves efficiency and automation by coordinating multi-stakeholder processes and dissemination of mutually beneficial events.*

Blockchain/Distributed Ledger Technology (DLT) provides many capabilities to make supply chains more transparent and efficient. It can address acknowledged challenges of today's complex supply chains, for example, by making it easier to check for data integrity and authenticity, allowing the prevention of double-spending of production decisions, parts custody, recalls etc. Blockchain improves efficiency and automation by coordinating multi-stakeholder processes and the dissemination of events.

*Blockchain/DLT provides a trust anchor to support multiple stakeholders to authenticate each other's identities and data.*

Two foundational capabilities are required to address these challenges, i.e., the ability for stakeholders to securely authenticate each other's identities and exchange data, and the ability to track and trace part lifecycle events from birth to end of life. Both of these capabilities require a single source of truth for supporting multi-stakeholder workflows around trusted data, and that's where blockchain / distributed ledger technology act as a pivotal enabler.

*Significant challenges exists in implementing blockchain/DLT primarily in solving tradeoffs of privacy, scalability, and replicated storage.*

However, there are also significant technical challenges involved with the adoption of blockchain in supply chains, as the specific scalability and privacy requirements of each use case need to be met. Tackling these challenges, which are associated with the replicated storage and execution of transactions on a blockchain, is the goal of many ongoing research and industry projects. Solutions that have been proposed exhibit different tradeoffs: for example, integrating Trusted Execution Environments or developing hand-crafted solutions based on advanced cryptography, such as Secure Multiparty Computation or Zero-Knowledge Proofs, can avoid information exposure but add additional complexity and computational overhead.

Other established methods, such as writing only transaction hashes on a blockchain, are simple to implement; yet they cannot bring the anticipated benefits in every use case as this approach reduces the number of participants with access to the blockchain or the information is stored on-chain and hence accessible to other participants and smart contracts. Besides the application-layer design choices, there are also many degrees of freedom regarding the setup of a blockchain-based supply chain solution on the infrastructure layer: Tradeoffs exist for the usage of permissionless or permissioned architectures; and, in the latter case, there may be one blockchain that comprises the whole supply chain ecosystem, one blockchain per node, or even many blockchains that may involve only two or three parties each.

*Use cases in supply chain are diverse in terms of requirements pertaining to data protection, antitrust regulation. Hence, one-size fits all reference architecture is difficult to design.*

On the other hand, use cases differ considerably regarding the sensitivity of the related data in terms of data protection regulation, antitrust regulation, and their classification of business secrets. Stakeholders also do not have the same technical capabilities and willingness to adopt innovative yet complex solutions that help to leverage the advantages of blockchains while addressing the challenges. In summary, the heterogeneity of use cases and the variety of potential design choices prevent the feasibility of a one-size-fits-all blockchain architecture as a solution.

*This reference architecture focuses on standardized bilateral communication using extensive API calls, decentralized identity with blockchain/DLT as a trust anchor.*

Consequently, this reference architecture focuses on discussing the benefits and potential interplay of different blockchain setups, embedded into a system that provides a basic communication layer, and the role of privacy enhancing technologies. The system would offer a rich toolkit to account for the spectrum of requirements of use cases that need to be implemented. The reference implementation suggests standardized bilateral communication and process management between business partners in the supply chain in combination with replicated execution on a DLT where useful.

Application Programming Interfaces (API) can shield the specific choices of stakeholders regarding their integration of a blockchain behind a layer of abstraction and enable multi-stakeholder workflows such as recalls through the supply chain without disclosing related information to third parties. This design is facilitated by cross-organizational digital identities for all parties, managed in a decentralized approach that may be anchored to a blockchain and oriented at the W3C DID and Verifiable Credentials (VC) standards that have already built the basis for the MOBI VID II Reference Implementation.

Decentralized identity management enables a cross-organizational access management for the standardized API endpoints that we propose as the base infrastructure for the exchange of information between business partners, as well as the source for demonstrating permissions on a joint DLT platform. As this approach supports many degrees of exposing the exchanged information to further stakeholders, benefits of increased transparency can be leveraged while challenges associated with sensitive data, that blockchains frequently encounter, can be avoided.

*This architecture uses “cascading API calls” and smart contracts based event handling.*

Depending on the use case under consideration, multi-stakeholder processes, such as recalls, can be automated through “cascading API calls” or smart-contract based event handling. This spectrum hence supports both coordinating use cases that allow for a high degree of transparency across multiple stakeholders with a highly robust design that does not rely on the availability of information from each individual party in the supply chain of a specific component in a recall.

The standard hence motivates the combination of digital identities, bilateral data exchange, distributed ledgers, and privacy-enhancing technologies to offer transparency to the extent that is required and providing the benefits of smart contracts in terms of efficiency where the related information exposure is justified or privacy-enhancing technologies can reduce information exposure while maintaining the core benefits.

## LIST OF ACRONYMS

---

BMS	:	Battery Management System
EV	:	Electric Vehicle
OEM	:	Original Equipment Manufacturer
SOH	:	Battery State of Health

## GLOSSARY OF TERMS

---

This section contains the definitions of all technical and specific terms used throughout this document.

**Application Programming Interface (API):** An API is defined as a specification of possible interactions with a software component, allowing two applications to interact with each other. It defines the kinds of calls or requests that can be made, how to make them, the data formats that should be used, the conventions to follow, etc.

**Decentralized Identifier (DID):** A W3C Decentralized Identifier represents a globally unique identifier that can be resolved to a DID Document, or de-referenced on a specific distributed ledger network, much like a URL on the Internet.

**Differential Privacy (DP):** A method for obfuscating sensitive information by adding noise with expectation value 0 to data. Differential Privacy is best suitable in scenarios where large datasets are aggregated as the expected value of the average does not change under adding noise whose distribution is centered at 0, and where mathematical guarantees for the indistinguishability of entities with respect to query results are required.

**Homomorphic Encryption (HE):** Homomorphic Encryption allows performing computations on encrypted data (i.e., making meaningful operations without decrypting and knowledge of the decryption key). HE is either very limited in scope (either additions or multiplications, such as in the Paillier cryptosystem) or brings significant performance challenges when arbitrary operations need to be supported (“fully homomorphic encryption”).

**Logistics Service Provider (LSP):** Logistics service providers, commonly referred to as third-party logistics (3PL) providers, are companies that specialize in the handling, storage and transportation of goods.

**Master Data:** Specifications and information related to products and business partners, such as supplier’s address and banking information. Master data management aims to provide data and processes for collecting, matching, persisting, and distributing such data within an organization but potentially also with business partners to ensure a single source of truth that provides consistency and control.

**(Secure) Multiparty Computation (MPC):** Allows the computation of a function with multiple inputs provided by different entities where every participant does not learn the others’ private inputs but only the final result. Often, MPC also involves methods to make sure that the participants perform their task correctly, e.g., through using ZKP. This is based on cryptographic primitives such as secret sharing (splitting an input into multiple parts and distributing it to other parties), and/or oblivious transfer (sending multiple messages to another party and making sure that the recipient can only decrypt exactly one of them, but the sender does not learn which one). In this sense, MPC is strictly more general than ZKP, as the

latter requires a party that has access to all private inputs for a computation to create a proof of the correct execution of a program.

**Open ID Connect (OIDC):** A standard for federated identity management (that is often used in enterprise single sign-on and social login) in which clients (such as a mobile application or a server) can request and receive information about valid sessions. In essence, a user proves attributes attested by a dedicated identity provider (such as the company HR or IT department, or Google/Facebook) by means of a signed JSON document that contains information about their identity.

**Oracle:** A standard for federated identity management (that is often used in enterprise single sign-on and social login) in which clients (such as a mobile application or a server) can request and receive information about valid sessions. In essence, a user proves attributes attested by a dedicated identity provider (such as the company HR or IT department, or Google/Facebook) by means of a signed JSON document that contains information about their identity.

**Original Equipment Manufacturer (OEM):** An Original Equipment Manufacturer is an organization that makes devices from component parts either made internally or sourced from other organizations.

**Trusted Execution Environment (TEE):** A Trusted Executive Environment is hardware for which the manufacturer guarantees that code is executed correctly on it (“remote attestation”) and no information is leaked outside the hardware. A prominent example is Intel’s Software Guard Extensions (SGX) solution. By creating a private key inside the TEE and only making the corresponding public key available, information can be encrypted in a way that makes sure it can only be decrypted inside a TEE.

**Verifiable Credential (VC):** The W3C Verifiable Credential Standard defines Verifiable Credentials as “a part of our daily lives; driver’s licenses are used to assert that we are capable of operating a motor vehicle, university degrees can be used to assert our level of education, and government-issued passports enable us to travel between countries. This specification provides a mechanism to express these sorts of credentials on the Web in a way that is cryptographically secure, privacy-respecting, and machine-verifiable.

**Verifiable Presentation (VP):** A verifiable presentation is a tamper-evident presentation encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification. Certain types of verifiable presentations might contain data that is synthesized from, but do not contain, the original verifiable credentials (for example, zero-knowledge proofs). (Source: W3C, 2022)

**Zero-Knowledge Proof (ZKP):** In cryptography, a zero-knowledge proof is a method by which one entity (the prover, assumed to be computationally powerful) can prove to another party (the verifier, assumed to be computationally restricted) that a particular statement is true without revealing any further information.

Full access to this Standard is available to  
MOBI members.

If you are not part of the MOBI community and  
would like to become a member, please fill out our  
“Membership Inquiry Form” at [dlt.mobi/participate](https://dlt.mobi/participate).

Members gain access to standards, working groups,  
and many other benefits.

**Join us in building the Web3 Economy!**

GET INVOLVED

✉ [connect@dlt.MOBI](mailto:connect@dlt.MOBI)

🌐 [dlt.MOBI](https://dlt.MOBI)

✂ [@dltMOBI](https://twitter.com/dltMOBI)

📺 [MOBI](https://www.youtube.com/channel/UCMOBI)

📱 [@MOBI](https://www.instagram.com/dltMOBI)