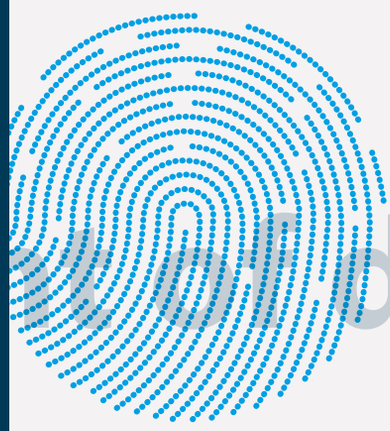


Hash: Fingerpri
digital data

01000011 01101111 01100110 01100110 01100101
01100101 00100000 01000110 01100001 01110010
01101101 00100000 00100011 00110010 00001010
00110101 00100000 01100010 01100001 01100111
01110011 00100000 01111000 00100000 00110001
00110000 00110000 00110000 00100000 01101011
01100111 00001010 00110001 00110011 00101101
00110001 00110001 00101101 00110010 00110000
00110010 00110010 00001010

Digital data input

Coffee Farm #2

5 bags x **1000 kg**

13 - 11 - 2022

Coffee Farm #2

Accountability and Transparency in Global Supply Chains

Digital Traceability and Trust in Complex Supply Networks

Topsector Logistiek

Accountability and Transparency in Global Supply Chains
Digital Traceability and Trust in Complex Supply Networks

Authors
Herman Wagter
Peter de Wever
Hans Keetman
Leon Simons
Guido de Wit
Max Schreuder
Bas van Bree

March 2023

Topsector Logistiek

Connekt

TKI DINALOG
Dutch Institute for Advanced Logistics

Management Summary

This white paper proposes a combination of a key component in block-chain technology and of the architecture of federative data spaces to create a digital 'supply network of trust' which facilitates automated accountability and traceability in global supply networks.

The key questions to get accountability and traceability are:

- How to acquire and transfer data, starting at the base and following the materials throughout the processing steps in the supply network, about the relevant aspects of each step?
- Who has supplied the original data?
- Who has verified or certified that the claims as suggested by the data (such as the claim 'this product was produced at an organic farm with good labor conditions') can be trusted? And can this verifier/certifier be trusted?
- How can it be verified that the (digital) data has not been tampered with by intermediaries in the supply of data?
- How can the tensions between commercial interests to be partly in-transparent and the need for transparency and accountability in the supply chain be resolved?

The trust of the data has two dimensions:

- Non-repudiation of the digital data (integrity).
- Verification/certification of the claims set forward by the data (conformity assessment of reality versus data).

Blockchain technology creates non-repudiation of data by means of a hash-chain and a (consensus) mechanism between all nodes in a network to agree upon the order and validity of transactions. Federated data space frameworks provide the basis to check identities and other claims automatically, and provide access to data at the source (when authorized).

The ledger of transactions in a hash chain is an elegant and proven concept to achieve immutability of consecutive transactions or additions. Adding data in each step to a hash-chain, as goods are transported and transformed in a supply chain network, is a natural mirror of physical movements to a stack of data which gets enriched and extended at every step. The consensus mechanism is not well suited to the reality of supply networks and can be exchanged for signing the data with cryptographic keys.

When links to online data sources are added in the data, accessible according to the federated data space principles, it will allow machine-to-machine verification of data, using:

- Link to the data sources of the entity responsible for a step
  - For example, an API;
  - Access to data is dependent on role (customer, local authority, quality assessment body for supply network, etc.).

- Link to the registers of the Conformity Assessment Bodies that can support the veracity of a particular claim
  - Again, preferable an API;
  - Access to data is dependent on role (customer, local authority, quality assessment body for supply network, etc.).

Combining the hash-chain from block-chain technology with the principles of federated data spaces, a 'stack' of information can be built and transferred alongside the goods in the supply network. The stack of information allows the receiver to trace back through the supply network the consecutive data sources, the data they have added and the certification bodies that can attest the veracity of the data added.

There are natural tensions between commercial and competitive interests to be partly in-transparent and the need for transparency and accountability in the supply network.
A stacked hash-chain as described before gives the transparency required for accountability but may show too much information and could severely diminish the willingness to provide and share data.

The proposed solution relies on:

- the cryptographic hash function that proves that data has not been modified;
- allowing trusted third parties to access the embedded but not shared data about the actual producers, using the hash to verify that data has not been modified.

The party who wants to hide commercially sensitive information (such as a trader) supplies the hash of the underlying data to the customer.

A trusted third party is asked by the customer to:

- ask for the underlying data, to be accessed confidentially, converting the anonymized ID to real identities;
- verify if the fingerprint of the underlying data per producer matches the fingerprint supplied, proving that the data is unmodified;
- verify the digital signing of the data by each producer;
- verify which the trusted third party vouches for the claim;
- report back that the claims have been verified.

The barriers to implementation are hardly technological: the technological components are well-known and relatively mature.

Implementation and adoption means putting the ideas to practice to make them easy to implement and affordable. One advantage is that the adoption can be gradual and viral, starting with supply networks that need to prove their origin, working their way back upstream.

Index

1 Introduction

Society is increasingly looking to global companies to take accountability for their global supply chains. The push for non-financial reporting is worldwide and extends beyond Greenhouse Gas Reporting. The UN Sustainable Development Goals[1] cover a wide range of objectives.

And yet before we can begin to address accountability, we have to acknowledge and remedy the dearth of reliable information.

Closing the information gap is a major challenge.

Some efforts are aimed at improving the information position at the start of a supply chain : organizations like Solidaridad[2], an international nonprofit organization working to create fair and equitable supply chains, are working hand in hand with smallholder farmers, workers, and businesses to close those information gaps bottom-up. Other efforts are aimed at the digital traceability of digital information throughout the supply chain.

For instance:

- blockchain technology has attracted interest as a means to create a shared information position;
- federated data space architectures promise access of data information at the source, bypassing intermediaries who could have an interest in lack of transparency.

This white paper proposes a combination of a key component in block-chain technology and of the architecture of data spaces to create a digital 'supply network of trust' which supports accountability and traceability in global supply chains.

1 https://sdgs.un.org/goals.

2 Solidaridad is leveraging digital tools that are locally-relevant, context and commodity specific. These tools are integrated in their programming to support producers to improve production and access finance, while simultaneously incentivizing the production of data. This can provide more supply chain insights, but importantly provides value to the producers and also protects their interests.

2 Supply network of trust

A physical 'supply chain' is in practice a complex network instead of a linear 'chain' of sequential operations. In this paper the term 'supply network' is therefore used.

The operational base of global supply networks is populated by a large number of suppliers, small and large. Active in agriculture, growing and harvesting food or biomaterials, in mining minerals or mineral oils, or in transporting, trading and processing these materials, and so on. Their output is input for large and complex supply networks.

The key questions in accountability and traceability in these supply networks are:

- How to acquire and transfer data, starting at the base and following the materials throughout the processing steps in the supply network, about the relevant aspects of each step?
- Who has supplied the data?
- Who has verified or certified that the claims as suggested in the data (such as the claim 'this product was produced at an organic farm with good labor conditions') can be trusted? And can this verifier/certifier be trusted?
- How can it be verified that the (digital) data has not been tampered with by intermediaries in the supply of data?
- How can the tensions between on one hand commercial interests to be partly in-transparent and on the other hand the need for transparency and accountability in the supply chain be resolved?

2.1 Trust of data

One can argue that the receiver of goods and data is the endpoint of two supply networks: the first is the physical supply network, the second of the supply network of trust of the data.

The trust of the data has two dimensions:

1 **Non-repudiation of data**

Non-repudiation is a security property of data that helps to prevent one party from denying that they took a particular action or made a particular statement, registered as (digital) data. Non-repudation properties are often used in electronic communication and transactions to provide evidence that a particular message or other electronic data was sent or received by a specific person or entity.

Well known methods to provide this non-repudiation are:

1 digital signatures, which are cryptographic keys that can be used to sign and verify the authenticity of electronic messages and documents,
2 checksums (hash) of datasets, proving that data has not been modified since the creation of the checksum, and
3 certificate authorities (CAs), who can provide a secure, verifiable way to establish the relationship between the keys and the identity of the parties involved in a transaction. In chapter 4 a more detailed explanation is given of this method.

In the context of accountability and traceability in supply networks non-repudiation answers the questions of:

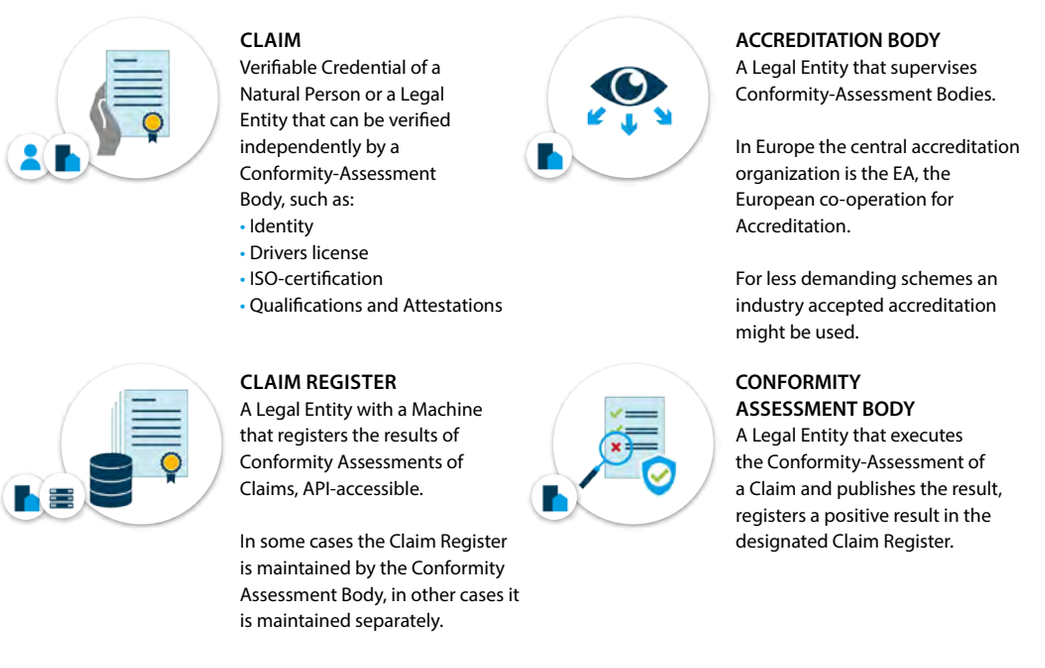
- Who has supplied the data?
- How can it be verified that the (digital) data has not been tampered with by intermediaries in the supply of data?

Non-repudiation does not say anything about the content of the data and its veracity.
In contrast to financial transactions, where there is little doubt as to what a financial value represents, data about physical goods and the conditions of production can easily be misrepresented. The question if the statement ('claim') made by the data can be trusted must be resolved in another manner: verification/certification by trusted third party is the most used method.

2 Verification/certification of claims

A certification/verification process is a formal procedure for evaluating and verifying that an individual or organization meets certain established criteria or standards ('conformity-assessment'), expressed in a certification scheme.
A claim in the data needs to be verified/certified.

Figure 1
Conformity Assessment Roles

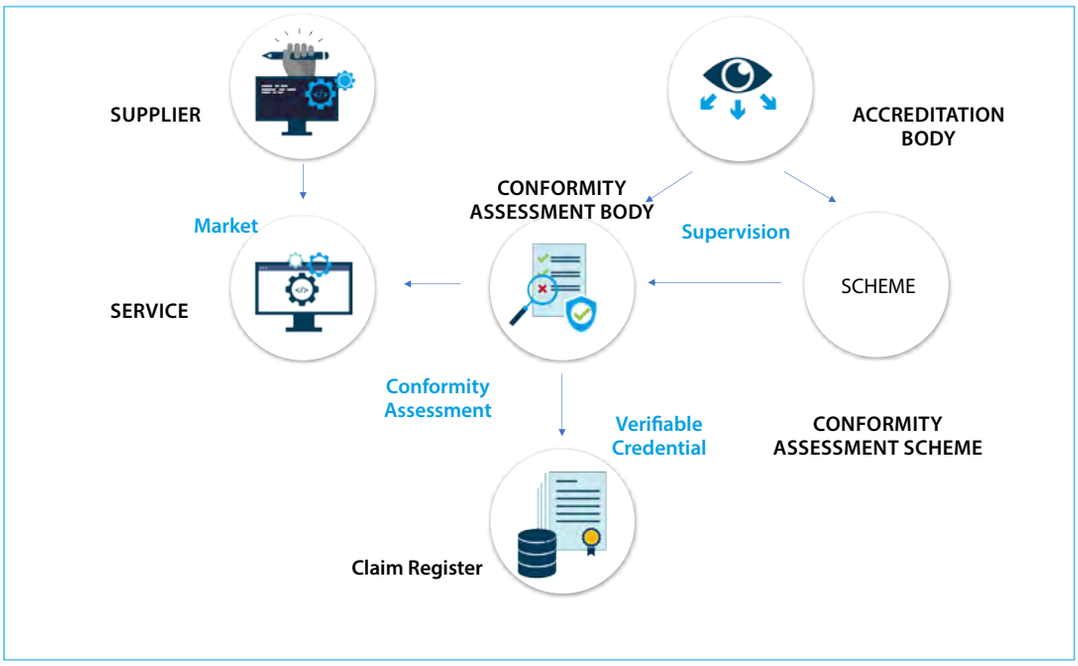


In Europe the highest standard of a certification process is one that is supervised by the EA, the European Cooperation of Accreditation. Industry-driven certification scheme's are also prevalent, using the same roles.

The general description of such a process shows that trust is rooted in the triangle of:

- Accreditation body (Accreditation of Scheme and Bodies)
- Conformity Assessment Scheme (how to assess conformity (process), what are the norms to exceed?);
- Conformity Assessment Body (Organization executing the conformity assessment according to a scheme).

Figure 2
Conformity Assessment Process



In the context of accountability and traceability in supply networks it is therefore necessary:

- to be able to identify the entities ('trusted third party') who are responsible for these roles, for a particular claim.
- to be able to check with these entities if the certification/verification as claimed is supported by them.

The question of trust shifts to: can one trust the 'trusted third party'?

2.2 Trust Sovereignty

Any certification chain ends with a Root Trust Anchor: the root of the 'trusted third party' chain of conformity verification. In theory, if the Root Trust Anchor is dependable, one can trust the chain of conformity verification. However, in reality an organization will create its own assessment of the trustworthiness of any Root Trust Anchor and the parties in the chain of certification that depends on this Root.

This principle is called 'trust sovereignty'.

In order to be able the make this assessment quickly and highly automated, it is necessary that a certification chain can be traced back digitally: a claim should have a digital link to the conformity assessment body that is the 'trusted third party' in this chain. Preferable this conformity assessment body would provide digital links to its chain up to the Root Trust Anchor.

3 Technology supporting accountability and traceability

3.1 Blockchain

Blockchain technology has attracted a lot of interest as a means to create a shared information position in supply networks[3].

Blockchain technology can be analyzed as being composed of three main functions:

- **A shared ledger of transactions in a 'hash chain'**
  A hash chain is a series of data records, each of which is linked to the previous record by a cryptographic hash function[4]. Hash chains are often used in distributed systems such as block-chains as a way to create a tamper-evident record of transactions or other data.

- **A network communication mechanism of transactions and consensus**
  All participants (nodes) in a blockchain are in communication with each other, to exchange transactions, calculate additions to the 'hash chain' and create consensus on the state of the shared ledger/hash chain. Each node holds a complete copy of the shared ledger/hash chain.

- **A consensus mechanism**
  A consensus mechanism is a protocol or algorithm that is used to achieve agreement on the state of a distributed database, such as a blockchain. In a blockchain, the consensus mechanism is used to ensure that all nodes on the network agree on the order and validity of transactions that are added to the chain.

To summarize, a blockchain creates non-repudiation of data by means of a hash-chain and a mechanism (consensus) between nodes in a network to agree upon the order and validity of transactions.

3 For example: https://www.researchgate.net/publication/329813013_Understanding_blockchain_technology_for_future_supply_chains_a_systematic_literature_review_and_research_agenda

4 https://en.wikipedia.org/wiki/SHA-2

3.2 Federated Data Spaces and trust in data

Data Space frameworks such as GAIA-X[5], IDSA[6], FEDeRATED[7] and the BDI[8] are architectures to create a federated cooperation in networks to exchange or access data, based on principles of:

- Data Sovereignty
  - Control of who can access what data is held by the data owner;
- Shared semantic models;
- Accessing data directly at the source, machine-to-machine;
- Machine-to-machine Identification, Authentication and Authorization (IAA) for confidential access to data at the source.

The FEDeRATED and BDI (which is derived from FEDeRATED) frameworks focus on real-world coordination challenges in for example construction and (international) logistics.

One of the challenges in data spaces is to establish trust in machine-to-machine exchanges. The need for a robust IAA mechanism has led to technology, protocols and conformity assessment schemes that can provide a basis for a supply network of trust in data and in the participants in a dataspace.

In particular the method for establishing the identities of organizations, their mandated functionaries and their machines through ID-providers and Certificate Authorities has already been put into EU-regulations[9].

Ample research is put into the issue of trust in so called Verifiable Credentials: in other words into how to verify the claims an entity makes about itself, by links to the registers of Conformity Assessment Bodies that are responsible for certifying a claim.

Claims may be anything, such as:

- Identity;
- ISO certification of the organization;
- Credentials of a certain training level of a person;
- Etc.

To summarize, federated data space frameworks provide a federated trust framework: this is the basis to check claims (identities and other claims) automatically, and provide access to data at the source when authorized.

5 www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html
6 https://internationaldataspaces.org/
7 http://www.federatedplatforms.eu/
8 https://topsectorlogistiek.nl/bdi-en-dil-een-afsprakenstelsel-voor-event-gedreven-coordinatie-in-de-logistiek/
9 https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

3.3 Combining components to achieve the goal

The ledger of transactions in a hash chain is an elegant and proven concept to achieve immutability which is a part of non-repudation of consecutive transactions or additions.

Adding data in each step in the supply network to a hash-chain, as goods are transported and transformed is a natural mirror of physical movements of goods. Added value in each step of the supply network is mirrored in added information. When the entity responsible for a step signs the data with its private key, the combination creates non-repudiation: the digital file can be trusted by the receiver.

The federated trust framework as developed for data spaces is the basis for trust in the data itself: is the data a true representation of reality?

Let's first look at the use of the hash function and the subsequent signing of the file more in detail in the next chapter.

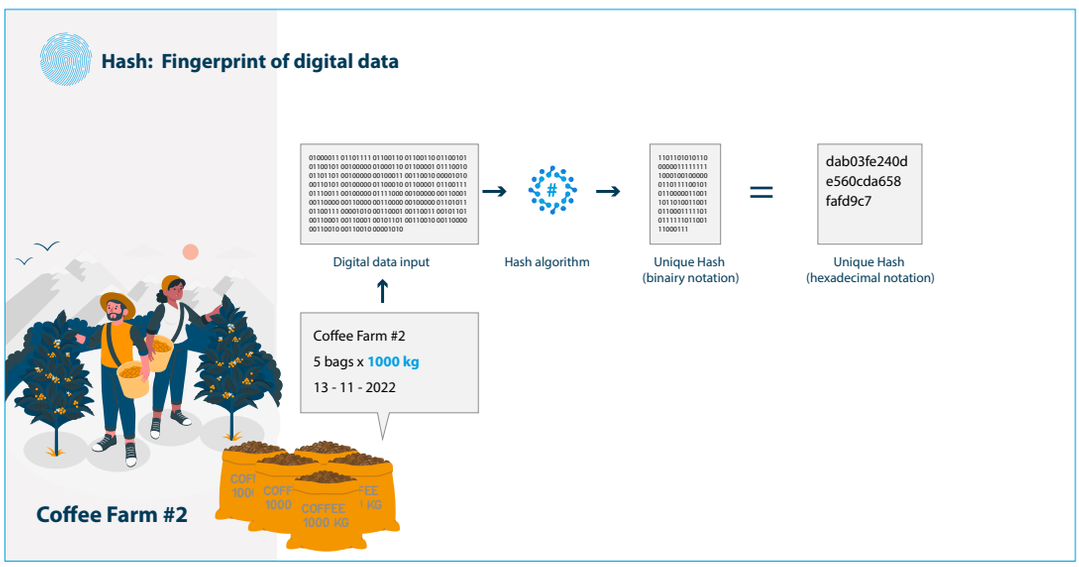
4 Transparency and non-repudation of digital data

4.1 Fingerprint/hash

In figure 3 an example is given of creating a hash of primary data, in this case by a coffee grower that sells green coffee beans to a trader.

The hash is a 'fingerprint' of the digital information. The data file is processed by the hash-algorithm which results in an output: the fingerprint. This computation is standardized and can be executed quickly.

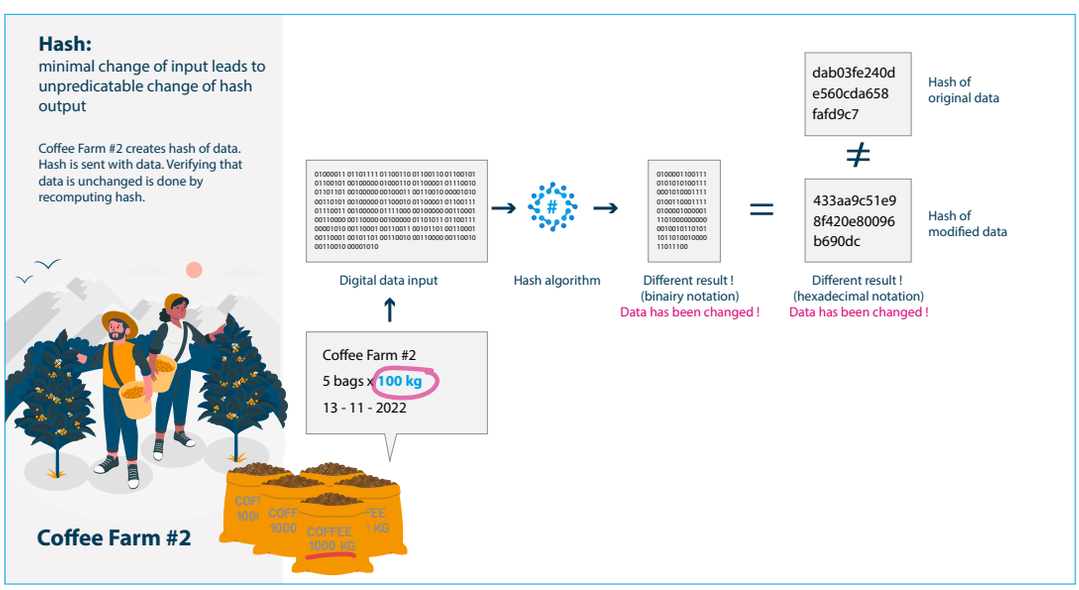
Figure 3
Creating a hash of primary data



Suppose the primary data would be changed by the receiver: instead of 1000 kg per bag the data now states that a bag is 100 kg. The change is minimal: only one digit is removed.

The hash function of the changed file will result in a different output. The change in output is in practical terms deemed unpredictable, meaning that it is practically impossible to modify an input data file in a meaningful manner so that the output (fingerprint) is identical to the original output. Figure 4 shows the difference.

Figure 4
Change in input file leads to different fingerprint



The receiver of the data can easily verify if the fingerprint (hash) of the data is the same as the fingerprint that has been provided; this proves that the data has not been modified. The same check can be done by the provider of the data: it proves that the data has not been modified by the receiver.

But how can both parties be sure they agree upon the same fingerprint, and that the sender is the party that vouches for the data and its fingerprint?

The answer is given by the digital signing of the fingerprint by the sender.

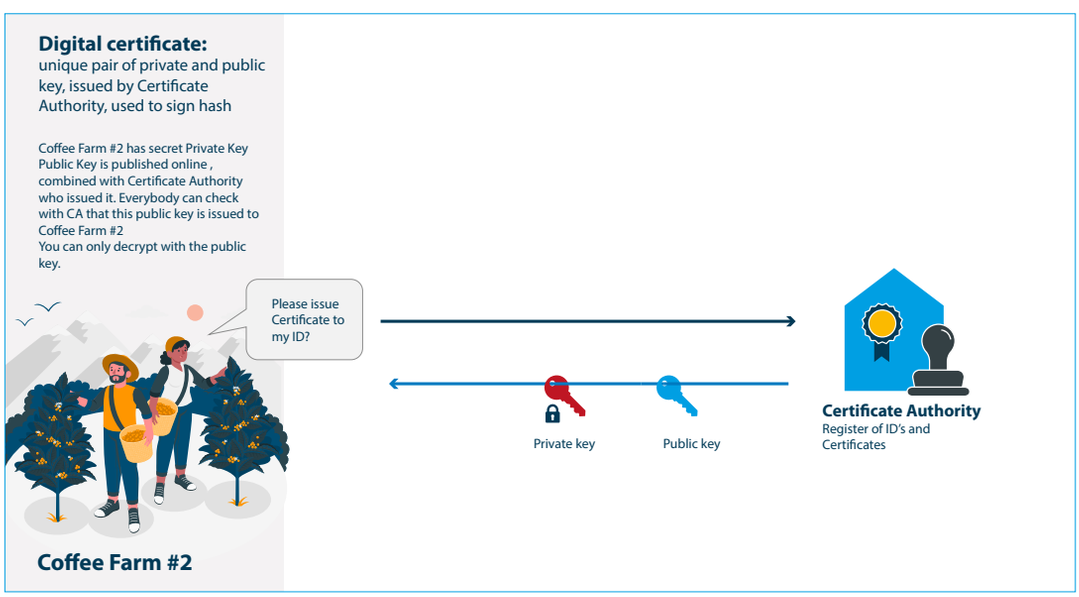
4.2 Public-private key for digital signing

Any party can request to be issued a so-called certificate by a Certificate Authority (CA).
A CA:

- Verifies the identity of the entity and functionaries requesting a certificate.
- Issues a public and private key combination (certificate) which is unique to the entity and transfers them to the entity.
- Registers the entity and its certificate, in the process making the public key public.

The entity should keep the private key confidential and unknown to any outsider. The public key however should be made widely and easily accessible.

Figure 5
Public and private key and digital certificate

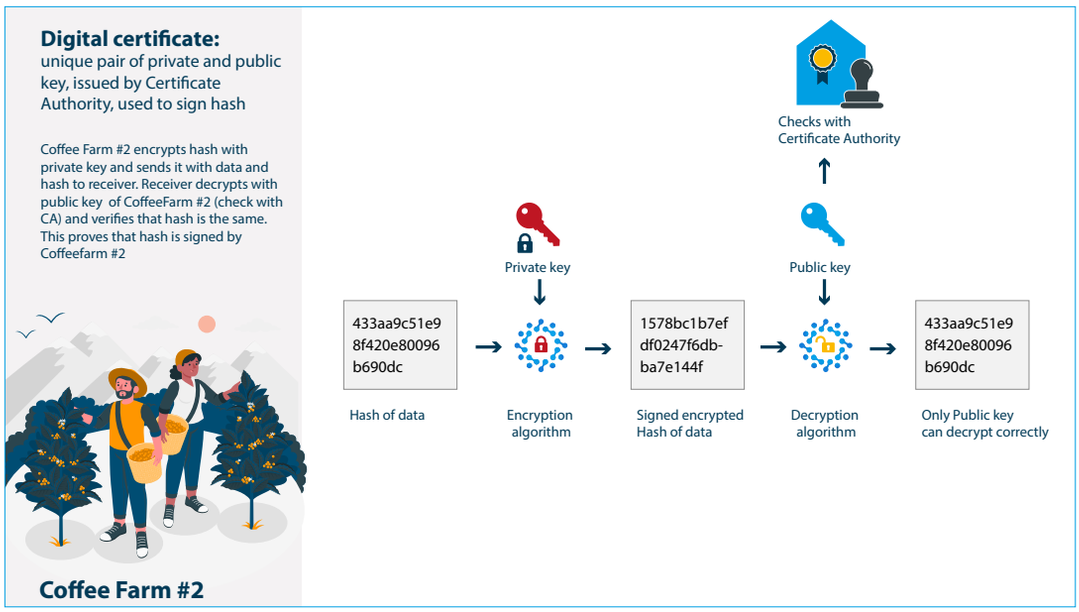


The public and private key share an unique relationship: the private key can be used to encrypt data with a specific algorithm, the public key can be used to decrypt data that is encrypted by the private key. The reverse is not true: one cannot encrypt the data with the public key (using the algorithm specified) and decrypt it successfully with the same public key.

The owner of the private key can encrypt the fingerprint of a digital file. The encrypted fingerprint is sent together with the original digital file to the receiver: the data block.

The receiver can request the public key, verify the identity of the owner of the public and private key-pair with the CA, and decrypt the encrypted fingerprint with the public key.

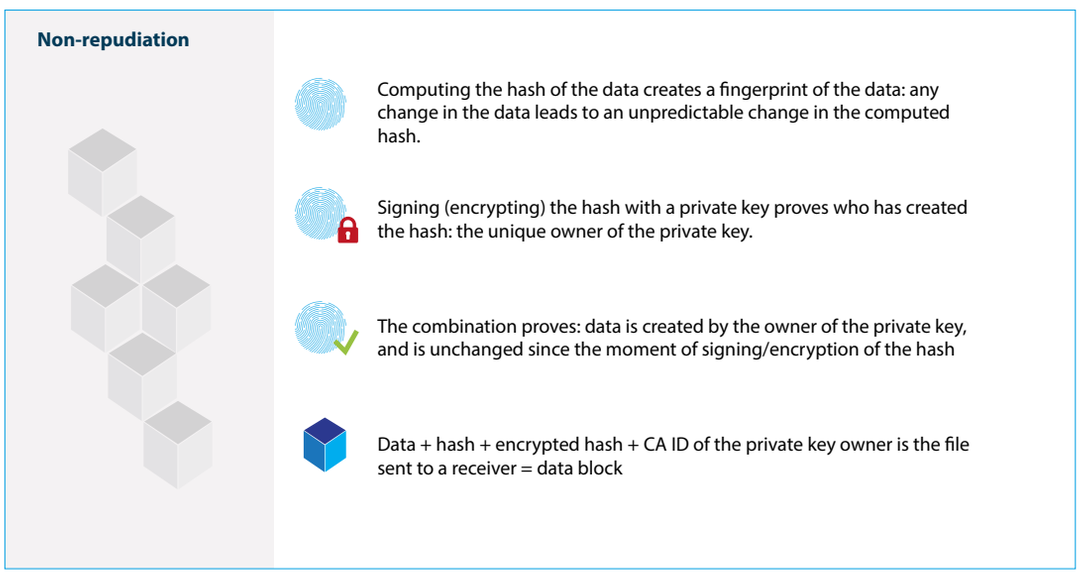
Figure 6
Encryption and decryption of the fingerprint



The data file is run through the hash algorithm: if the resulting fingerprint is identical to the decrypted fingerprint it proves that:

- A specific entity must be the sender of the data file and the fingerprint: only this entity has possession of the private key that allows an encrypted file to be decrypted with the public key.
- The data is unchanged since the generation of the fingerprint by the sender.

Figure 7
Non-repudiation of a data block



This proof can be recreated any time later, just by running the process again. This creates the non-repudiation of a given data block.

4.3 Creating a chain of nested data blocks

The receiver of a data block, for instance a trader in coffee beans may receiver cargo and data blocks from multiple sources. The coffee beans are mixed in a silo and sold to a coffee roaster.

The trader can repeat the process by:

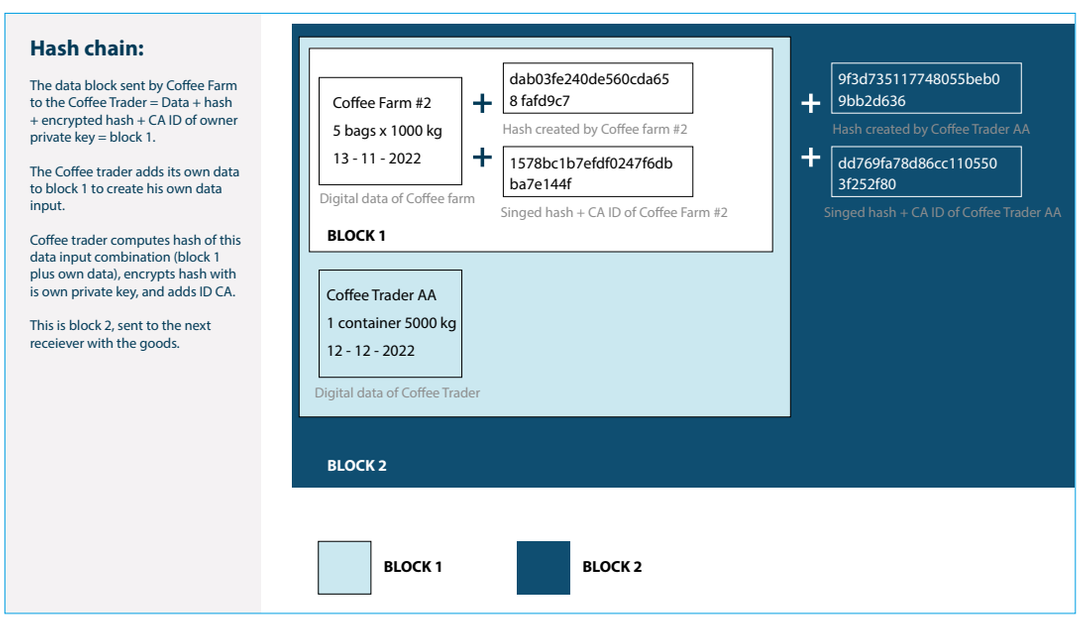
- Combining the data blocks for all relevant sources, treating them as data in a file.
- Add his/her own information to the data file.
- Create a fingerprint of the new combined data file which is a new data block.
- Sign it with its own private key.
- And send the new integrated data block to the coffee roaster.

The coffee roaster can:

- Verify that the data in the data block is unchanged and sent by trader.
- Repeat the process for each nested data block, verifying each component in the file (unchanged, created by a specific source).

This process of nesting data blocks in a newly created data block can be repeated for each step in a supply network: and it allows the final receiver of data to trace back the data through the supply network to its sources.

Figure 8
Nesting data blocks to create a hash chain



4.4 Transparency: adding trust even if transparency is (commercially or practically) limited

The transparency this approach creates is desirable but not enough to establish the trust in the data: there needs to be a method to establish which trusted third party has performed the conformity assessment or a test to verify if the data sent is correct in a material sense. Such as: was this batch of coffee beans grown under conditions (environmental footprint, living wages, labor conditions etc.) that are demanded by the buyer?

Trust requires additional information to be included in the data blocks. However, in commercial relationships full unmitigated transparency is not always desirable, both from a commercial point of view and a competition point of view. A practical methodology needs to allow parties to limit the amount of data that is sent forward, while retaining the trust level in the data. This also applies to situations where the incorporation of all the data blocks from all possible sources would be impractical: for example when used vegetable oil is collected from many small sources, to be used for biodiesel.

The next chapters elaborate on the federated trust framework.

5 Building trust in Trusted Third Parties (TTP)

5.1 Adding the links to TTP in the data

The digital data as sent by for example the coffee grower represents 'claims' about reality that needs to be verified by a TTP.

A 'claim' is a statement about the organization and the product, for example:

- The entity that is responsible for this stage in the supply network.
  - Including for instance labor conditions, safety, environmental protection.
- The way the product has been handled, inspected or processed.
- The amount of CO_2 added by its processes.
- Specific information on this product or batch.

Starting from the base of the supply network a stack of claims is built and transferred alongside the goods. Every base ('root') of the supply network starts with the first set of data/claims, carrying these claims forward through the network.

Depending on the agreements and requirements in a given supply network, some claims need to be certified by Conformity Assessment Bodies (CAB). They are the TTPs that have assessed claims and have verified a claim according to the applicable scheme or test. This could start with something as simple as the identity of the organization which for example would have been verified by the local Chamber of Commerce. A more complex certification could be the 'Max Havelaar' fair trade certification for coffee bean growers: a well-known certification scheme, administered by the Max Havelaar foundation.

Included in the data should be the link to the CAB that has assessed and verified a claim according to the applicable scheme. It is assumed that these CABs have the capability to allow digital verification of claims. The receiver of the data can check which TTP vouches for the claim, and assess how much trust it will grant the TTP.

A 'Max Havelaar' certified coffee grower selling beans should for instance add[10] in the data, for the batch of beans its identity and a link to the CAB that has verified that the plantation meets the criteria. With the link and the identity of the coffee grower the claim (Max Havelaar certification) and the CAB (Max Havelaar foundation) can be assessed independently by the ultimate user of the (roasted and grinded) coffee beans.

10 Or have a service provider or NGO that performs this task for them.

5.2 Adding the links to the original data

For more demanding supply networks it may be beneficial that the receiver can go back to the source of a given step in the network and request additional data or verification of data at the source.

This feature is one of the key functionalities of the basic architecture of federated data spaces: accessing data at the source, confidentially, on a need-to-know basis. The data spaces designed for use in logistics support this out-of-the-box[11].

The coffee grower or the trader in our example could add the necessary links in their data block to their online data sources, accessible according to the federated data space principles: for example an API where access to data is dependent on role (customer, local authority, quality assessment body for supply network, etc.).

The trust framework of data spaces for logistics and supply chains supports:

- Automated identity authentication of machine-to-machine communication.
- Selective automated authorization of access to data, under control of the data owner.
- Automated verification of digital credentials.

11 Basis Data Infrastructure (BDI)

6 Hiding commercially sensitive data, or aggregating data

There are natural tensions between commercial and competitive interests to be partly in-transparent and the need for transparency and accountability in the supply network.

The methodology as described before provides the transparency required for accountability, but may show too much information which can be detrimental to competition and innovation.

Fortunately the accountability check may be partly delegated to trusted third parties or government agencies, separating commercial information from accountability.

In our example, the coffee trader may want to prove that the greens beans are produced by Fair Trade 'Max Havelaar' coffee growers, without disclosing who the coffee growers are.

The solution relies on:

- the cryptographic hash function (fingerprint) that proves that data has not been modified;
- delegating access to 'confidential' data (need-to-know) to a TTP.

In this example the trader incorporates in its data block only the hash supplied by each coffee grower.

The trader combines his data with these fingerprints/ID's in a new data block and signs it. The trader supplies his data block to the customer (coffee roaster) with the claim that each supplier is Max Havelaar certified.

The coffee roaster cannot check the underlying data, but he can ask a trusted third party to:

- ask for the underlying data at the coffee beans trader, to be accessed confidentially, converting the anonymized ID to real identities;
- verify if the fingerprint of the underlying data per coffee bean producer matches the fingerprint supplied, proving that the data is unmodified;
- verify the digital signing of the data by each coffee grower;
- verify which the trusted third party vouches for the claim;
- report back that the claims have been verified.

The same mechanism can be introduced when it becomes impractical to carry forward all details of the supply network throughout the network: for instance if used vegetable oil is collected in many small locations where unknown sources can dump their used oil. It would be practical if only the oil-collection company keeps tracks of the collection, to be verified when needed. The cleaned, tested en possibly processed product is supplied only with aggregate information. The details would be available to a trusted third party or a certifying body.

7 Implementation

The barriers for implementation are hardly technological: the technological components are well-known and relatively mature. Common barriers in data sharing are non-technical; the fear of changing (ingrained) business processes, risk aversion; e.g. allowing third parties to access data for which an organization is liable and the risk of downstream data misuse often seem to outweigh the potential benefits of data sharing.

The development and deployment of (federated) data spaces is accelerating, supporting the link back to sources of data. The logistics data space developments in particular, support the issues of international supply networks, and the issue of trust in digital data containing claims about the 'real world'.

Implementation and adoption means putting these ideas into practice, making them easy to implement and affordable. As with many of these scheme's, getting to a critical mass of users is a long process and hard work. Non-disclosure of commercially sensitive data while retaining trust is a key feature.

One advantage of our proposed solution is that the adoption can be gradual and viral, starting with supply networks that need to prove their origin, working their way back upstream.

https://www.gartner.com/smarterwithgartner/data-sharing-is-a-business-necessity-to-accelerate-digital-business

A Addendum - Blockchain

Blockchain technology can be analyzed as being composed of three parts:

- **A ledger of transactions in a 'hash chain'**
  A hash chain is a series of data records, each of which is linked to the previous record by a cryptographic hash function[12]. The first record in the chain is known as the 'root' and is typically created by the owner of the chain. Each subsequent record, or 'block,' is added to the chain by calculating the cryptographic hash of the previous block and using the result as the new block's hash value.

  The use of hash values in this way helps to ensure the integrity of the data in the chain, as any attempt to alter the data in a block will result in a change to the block's hash value. This will, in turn, cause the hash values of all subsequent blocks to change, making it immediately obvious that the data has been tampered with.

  Hash chains are often used in distributed systems such as block-chains as a way to create a tamper-evident record of transactions or other data.

- **A network communication mechanism of transactions and consensus**
  All participants (nodes) in a blockchain are in communication with each other, to exchange transactions, calculate additions to the 'hash chain' and create consensus on the state of the shared ledger/hash chain. Each node holds a complete copy of the shared ledger/hash chain.

- **A consensus mechanism**
  A consensus mechanism is a protocol or algorithm that is used to achieve agreement on the state of a distributed database, such as a blockchain. In a blockchain, the consensus mechanism is used to ensure that all nodes on the network agree on the order and validity of transactions that are added to the chain.

  There are several different types of consensus mechanisms that can be used in a blockchain, including:
  Proof of work: In a proof of work (PoW) consensus mechanism, nodes on the network compete to solve a complex mathematical problem, and the first node to solve the problem gets to add the next block to the chain.

  Proof of stake: In a proof of stake (PoS) consensus mechanism, nodes are chosen to create the next block based on the number of coins they hold, or their 'stake' in the network.

  Delegated proof of stake: In a delegated proof of stake (DPoS) consensus mechanism, nodes on the network vote to elect a limited number of 'delegates' who are responsible for adding blocks to the chain.

  In a permissionless blockchain any party can join a blockchain and become a node.
  In a permissioned blockchain, only authorized participants are allowed to join the network, access the data stored on the chain, or validate transactions. The authority to grant access to the network is typically controlled by a single entity or a small group of entities.

To summarize, a blockchain creates non-repudiation of data by means of a hash-chain and a mechanism (consensus) between nodes in a network to agree upon the order and validity of transactions.

12 https://en.wikipedia.org/wiki/SHA-2

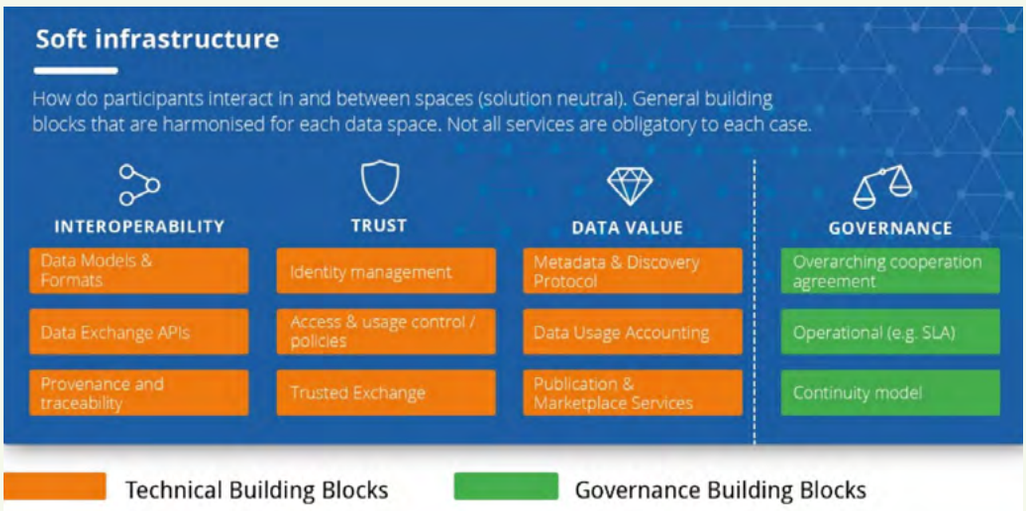
B

Addendum - Federated Data Spaces

Data Spaces: generic and specific approaches

The EU OPEN DEI initiative has defined a data space as 'a decentralized infrastructure for trustworthy data sharing and exchange in data ecosystems based on commonly agreed upon principles', requiring technical and governance building blocks ('soft infrastructure').

Fig 1. OPEN DEI soft infrastructure building blocks



The initiatives to develop and implement dataspaces can be placed in two categories:

- Generic initiatives, aiming at basic federative data sharing capabilities applicable to and over multiple sectors and application areas.
- Specific initiatives, targeting a specific sector and/or a specific application area and providing domain-specific data sharing and value adding functionalities.

Industry or sector led initiatives, such the European Open Science Cloud (EOSC)[13], the International Data Space Association (IDSA)[14] and GAIA-X[15] develop reference architectures and implementations, partly generic, partly specific for a particular ecosystem or business challenge. Each ecosystem is focused on developing and exploiting the potential of federated data sharing in their own context, leading to specific priorities and choices in their soft infrastructure.

As most organizations will be active in multiple data spaces, the question of supporting interoperability between data spaces from the perspective of the organizations is one of the challenges.

13 https://eosc-portal.eu/about-eosc-portal

14 https://internationaldataspaces.org/

15 www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

B

Data economy and physical economy

One of the major drivers for investing in federated data spaces is the business potential for the emerging data economy: being able to innovate by combining and processing data from all kinds of data sources, while the data owners are able to keep control of their data and monetize its use.

Other drivers are more related to benefits in the physical economy, as in high-tech manufacturing networks or global supply chains. The federated data exchange is a means to innovate and be more competitive in the physical economy.

The FEDeRATED framework and the BDI which is derived from the FEDeRATED concepts are focused on challenges in the physical economy where coordination between many actors and proof of compliance in Business-to-Business (B2B) and Business-to-Government (B2G) interactions are dominant drivers. For example in global supply chains with import-export controls, in construction, or in engineering & contracting.

Topsector Logistiek
Ezelsveldlaan 59
2611 RV Delft
+31 15 251 65 65
www.topsectorlogistiek.nl

Topsector Logistiek