Mutual recognition mechanism of e-documents and data exchanging across borders: centralized and decentralized approaches

Vladimir N. Kustov[a], Ekaterina S. Silanteva[b]

[a] *Saint Petersburg Railway Transport University of Emperor Alexander I, 9 Moskovsky Ave., Saint-Petersburg, 190031, Russia*
[b] *LLC New space of trade, 5 Orlikov lane, 2 Build. 9 Fl. 34 Room, Moscow, 107078, Russia*

Abstract
An integral part of a company's business processes global digitalization and automation is the transition to cross-border electronic legally significant document circulation. This article is devoted to reviewing two different methods of mutual recognition mechanisms: centralized and decentralized.

Keywords
Mutual recognition mechanism, e-documents, data exchanging, cross-border, centralized, decentralized, approaches

1. Introduction

Do you remember the biblical legend [1] that tells how and why people began to speak different languages, the Babel Tower legend? For the respondent positively to this question, we will refresh the memories, but we will briefly describe those who do not know such a tradition[1].

Once upon a time, all people, Noah's clan descendants who escaped during the Flood in the ark built by himself and found refuge near the Ararat Mountains, spoke the same language. Gradually, the human race grew, acquired new knowledge and skills. Besides, having accumulated specific skills luggage, people decided to apply them in practice and build a city and build a high tower, to the very heavens seen from everywhere.

The structure overgrew, rising ever higher toward the sky, which made people extremely happy. Simultaneously, with the tower, the World Flood's things had to wash away - human pride and vanity-revived and strengthened.

God learned about this tower, and he did not like people's ideas. However, God did not punish people by death, but punished them differently: one day, when they started to work, people suddenly stopped understanding each other's speech. They could not continue tower building because they began to quarrel, not understanding what the other wants. Watching this, God decided to help people forcing them to leave the city and leave. People left the unfinished tower and settled in different earth parts. Over time, they forgot about their relationship, they had their traditions, language, rites, customs, and the unfinished city, where the tower was erected, was called Babylon, which means "mixing."

Why did we remember that? The answer is an orientation toward the world (international, cross-border) digitalization and automation of many business processes. However, despite this, do not forget about the individual states' desire to preserve

Models and Methods for Researching Information Systems in Transport, Dec. 11-12, St. Petersburg, Russia
EMAIL: kvnvika@mail.ru (A. 1); the_best_kat@mail.ru (A. 2);

and develop their language, writing, traditions, customs, and digital sovereignty. In keeping part of this digital sovereignty in global digitalization and automation conditions, the principal contradiction arises: different states' cryptographic standards incompatibility. From time immemorial, every people have gone along his development line and do not plan to retreat from it by the current day.

2. Methods of implementation of the mutual recognition mechanism based on the centralized infrastructure

RFC 5217 «Memorandum for Multi-Domain Public Key Infrastructure Interoperability» [8] provides a terminology framework for operational requirements, which can be used by different Public Key Infrastructure (PKI) authorities for establishing trust relationships with each other.

RFC 5217 classifies mechanisms of mutual recognition of Trust services based on an infrastructure of open keys.

2.1. Single Certification Authority (CA) Architecture

So, let's take a closer look the single CA architecture.

In this model, the Mutual Recognition Mechanism (MRM) is provided with trust to the common Certification Authority. It is the most straightforward architecture. Nevertheless, it can be used in cases when several State Parties of the Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and Pacific (Framework Agreement, FA) agree to use the general CA for paperless trade [9].

The model of this Architecture is presented in Figure 1.

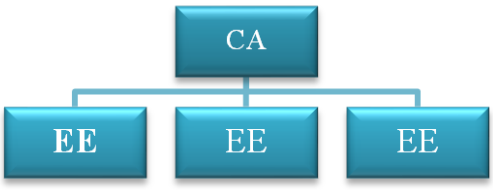

Figure 1. Simple PKI Architecture

A simple PKI consists of a single CA with a self-signed certificate that issues End Entities (EEs) certificates. End entity is the subject of a certificate that is using, or is permitted and able to use, the matching private key only for a purpose or purposes other than signing a certificate.

2.2. Different Multiple CA Architectures

Trust relations between Certification Authorities could be classified on the following basis:

1) The common use of crypto algorithms;
2) Common Policy of certificates.

Different Multiple CA Architectures is presented in Table 1.

Table 1.
Models of the mutual recognition mechanism

Common policy of certificates	The common use of crypto algorithms: Crypto algorithms are commonly used	The common use of crypto algorithms: Crypto algorithms of at least one party have a limitation on the cross-border distribution (not common use)
Common certificate policy	• Hierarchical PKI Architecture • Mesh PKI Architectures • Hybrid PKI Architectures	Crypto algorithms of at least one party have a limitation on the cross-border distribution (not commonly use)
Different certificate policy	Cross-certification with policy mapping	Trusted Third Party (TTP)

In case when the parties use different CA, but all participants of interaction commonly use cryptographic algorithms and certificate policy of this CA, mutual recognition could be used:

- Hierarchical PKI Architecture;

- Mesh PKI Architectures;
- Hybrid PKI Architectures.

In case the parties use different CA cryptographic algorithms. Certificate policies in the created chains of certification are various; cross-certification with policy mapping can be used for mutual recognition.

Two or more PKIs may choose to enter into trust relationships with each other. Each PKI retains its own set of Certificate Policy Object Identifier (Policy OID) and its own Principal CA for these relationships. In addition to making a business decision to consider a trust relationship, each PKI determines the level of trust of each external PKI by reviewing external PKI Certificate Policy Document(s) and any other PKI governance documentation through a process known as policy mapping. Trust relationships are technically formalized through the issuance of cross-certificates. Such a collection of two or more PKIs is known as a PKI domain.

PKI domain: A set of two or more PKIs that have chosen to enter into trust relationships with each other through the use of cross-certificates. Each PKI that has entered into the PKI domain is considered a member of that PKI domain.

A domain Policy Object Identifier (OID) is a Policy OID that is shared across a PKI domain. Each CA in the PKI domain must be operated under the domain Policy OID. Each CA may also have its Policy OID(s) in addition to the domain Policy OID. In such a case, the CA must comply with both policies. The domain Policy OID is used to identify the PKI domain.

Policy Mapping: A process by which members of a PKI domain evaluate the Certificate Policies (CPs) and other governance documentation of other potential PKI domain members to determine the level of trust that each PKI in the PKI domain places on certificates issued by each other PKI in the PKI domain.

PKI Domain Properties:

1. A PKI domain may operate a Bridge CA or a Unifying CA that defines the domain members by issuing cross-certificates to those members.
2. A single PKI may simultaneously belong to two or more PKI domains.
3. A PKI domain may contain PKI domains within its membership.
4. Two or more PKI domains may enter into a trust relationship with each other, creating a new PKI domain. They may choose to retain the existing PKI domains and the new PKI domain or collapse the existing PKI domains into the new PKI domain.
5. A PKI member may choose to participate in the PKI domain but restrict or deny trust in one or more other members PKIs of that same PKI domain.

The establishment of trust relationships has a direct impact on the trust model of relying parties. As a result, consideration must be taken to create and maintain PKI domains to prevent building inadvertent trust relationships.

PKI Domain Models are:

1. Unifying Trust Point (Unifying Domain) Model.
2. Independent Trust Point Models.
3. Direct Cross-Certification Model.
4. Bridge Model.

Trust Models External to PKI Relationships remains to consider ways to implement the mutual recognition mechanism for cases where other cryptography is used in PKI domains. Such methods include:

1. Trust List Models.
2. Trust Authority Model.
3. Trusted Third Party Model.

Here, the option to use a trusted third party as the most common and most universal one should be considered in more detail. The remaining models can be considered in more fact later.

The trusted security services provided by the specialized providers can be used to provide security in information interaction. Trusted security services can perform functions similar to notaries, apostille, and trusted delivery in paper documents exchange flow. The trusted security services operators must be the trusted third parties (TTP) of the information exchange parties. The activities of TTP must be governed by the international law of the States-participants of the information interaction, or bilateral agreements of the parties of informational interaction.

Thus TTP is the electronic equivalent of notaries, apostille, and trusted delivery institutions. TTP is not an entirely new institute; it continues the tradition of confirming the document's integrity and authenticity. From a legal point of view, the electronic document's function must pass from the document owner to a third party - the operator of TTP. It is a key specificity of the informational interface.

The trust is supported by a warranty of authenticity of electronic documents, financial liability for the electronic documents' actuality. It is the basic principle relevant for legally significant transboundary electronic document circulation when the contractors are far apart and in different jurisdictions.

It is a classic solution for providing secure transmission of information via a non-trusted channel.

TTP description was provided in ITU-T Recommendation X.842 «Information technology – Security techniques – Guidelines for the use and management of trusted third party services.» [4] Following this document, a TTP is an organization or its agent that provides one or more security services and is trusted by other entities concerning these security services' activities. The same document contains the most general description of the TTP services' architecture from different PKI domains.

One of the most well-known implementations of the trusted third-party model is Data Validation and Certification Server (DVCS) by the recommendations RFC 3029 «Internet X.509 Public Key Infrastructure. Data Validation and Certification Server Protocols» [2]. It can be used as one component in building reliable non-repudiation services.

One of the protocols realized by the DVCS service is intended for verification of the electronic documents signed with the digital signature. The Validation of Digitally Signed (VDS) Document service is used when a signed document's validity is asserted.

The DVCS verifies [3]:

1. All signatures attached to the signed document using all appropriate status information and public key certificates;
2. The mathematical correctness of all signatures attached to the document and checks whether the signing entities can be trusted by validating the full certification path from the signing entities to a trusted point (e.g., the DVCS's CA or the root CA in a hierarchy).

The DVCS may be able to rely on relevant CRLs or may need to supplement this with access to more current status information from the CAs, for example, by accessing an OCSP service, a trusted directory service, or other DVCS services.

The DVCS will perform verification of all signatures attached to the signed document. A failure to verify one of the signatures does not necessarily fail the entire validation, and vice versa. A global failure may occur if the document has an insufficient number of signatures.

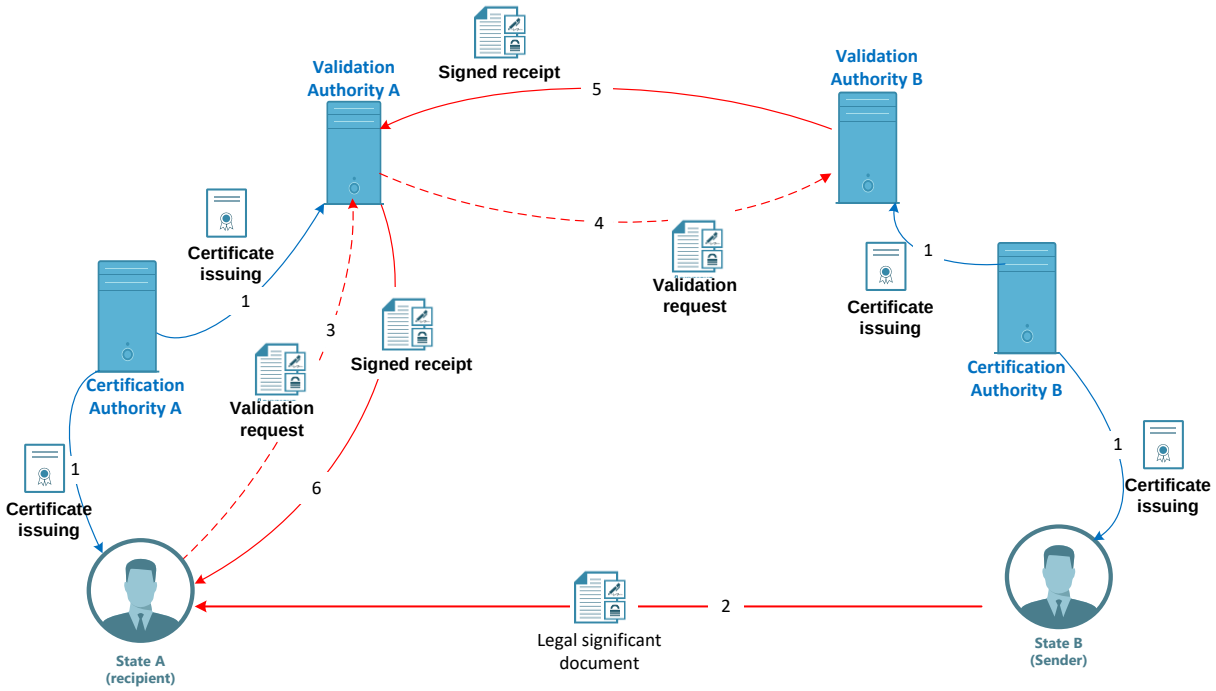

Figure 2. The Diagram of the functioning of MRM based on DVCS for supporting the trust in case of cross-border exchange of electronic trade-related legal and significant documents

The Diagram of the functioning of MRM based on DVCS for supporting the trust in case of cross-border exchange of electronic trade-related legal and significant documents (the sender and the receiver residents of the different states) is shown in Figure 2.

Processing of a request of DVCS received from user 1 includes the following stages (according to Figure 2):

1. Participants of information interaction are included in their public key infrastructure; that is,

they create their key pairs and receive certificates in their Certification Authorities (CAs).

2. User B (the resident of the state B) signs the ED of the EDS created according to the national legislation requirements and sends it to User A.

3. The user A (through a private office (web interface) or using a special software sends a request to the validation authority A.

4. Validation Authority A executes determination of the cryptographic algorithm using which the EDS is created (the certificate of a key of verification of the EDS is issued) according to the object identifier specified in the certificate of a key of verification of the EDS and will readdress it to the Validation Authority B located in the state B. On it using the execution of the sequence of cryptography conversions check of the received request is executed. Following the completed checks, the DVC receipt signed with the EDS of Validation Authority B is created.

5. The DVC receipt signed with Validation Authority B with the check results is transferred to Validation Authority A.

6. Validation Authority A checks the correctness of the DVC receipt accepted from Validation Authority B. At the same time, there is an appeal to the server of service TSP for adding of a stamp of time in the receipt created by results of verification of the DVC receipt created by Validation Authority B and also check of the status of the certificate of a key of the EDS of Validation Authority B using the appeal to service of check of the relevant status of the certificate (OCSP) or certificate revocation lists of CAs which issued the certificate of a key of the EDS of Validation Authority B is executed. Validation Authority A creates the report signed with the certificate of a key of check of Validation Authority A and transfers him to User A.

The requirements for TTP should be the following:

1. TTP has absolute credibility among the information exchange participants.

2. TTP uses the mechanisms of evaluation and compensation of damages.

3. TTP uses the methods of conflict resolution;

4. TTP provides the necessary guarantees.

5. The various national and international requirements to the Certification Authorities may be considered as an analogy.

To provide Mutual recognition of trade-related electronic information when PKIs use different, incompatible between each other Cryptography measures or their domains have separate legal bases, we should use DVCS functioning by RFC 3029 «Internet X.509 Public Key Infrastructure. Data Validation and Certification Server Protocols». DVCS receipt allows providing trust between different PKI domains in the case when their cross-certification technically or legally is impossible.

For correlation of the certificates policy, the receipt of DVC service can map the Policy in the same manner as it is mapped in cross-certification procedures.

In the extension of policy mapping, the intermediate Certification Authority guarantees to the user of the certificate that it will fulfill general guarantees and obligations, even although the other users of the certification chain work in the different policy areas.

Certification Authority (CA) of the integration segment should include one or several mappings for each set of the policies according to which it has issued TTP certificates. This CA shouldn't include mappings for other policies. Thus, the group of Certification Authority of an integration segment and the TTP services using certificates of this CA fulfill the TTE role between domains with the various levels of reliability.

According to which Sender of Certification authority acts, suppose one or several Certificate policies are identical to those, by which Certification Authority of TTP integration segment operates. In that case, these identifiers should be excluded from the extension of policy mapping but included in the extension of certificate policies. Policy mapping has the effect of transforming all policy identifiers in the sender domain's certificates to the identifier of equivalent Policy recognized by the user of the certificate (recipient). In this schema identifier of equivalent, Policy is described in the receipt of TTP service.

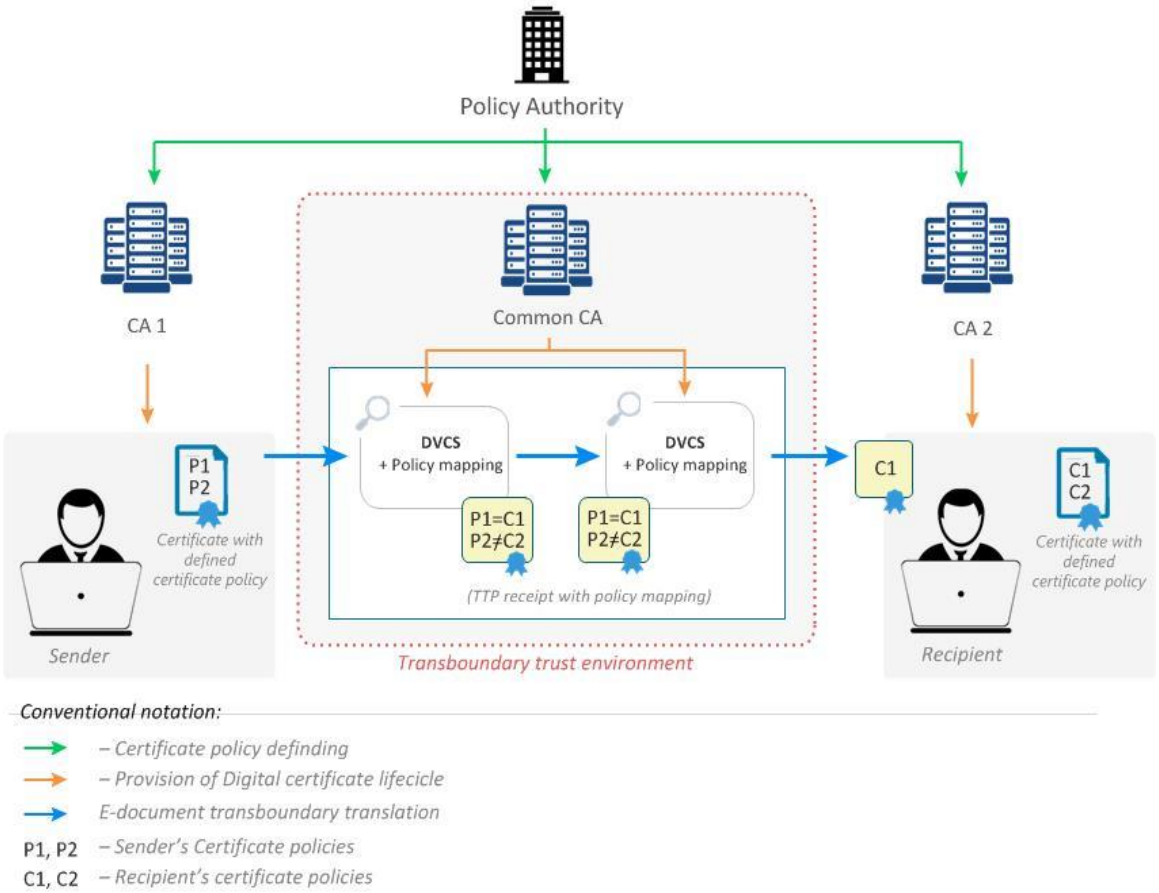

Figure 3. TTP for the domain with different levels of trust

3. Methods of the mutual recognition mechanism implementation based on the decentralized structure

3.1. Blockchain technology

The required trust level may also be supported by the trust infrastructure, built on a decentralized model. One of the technologies allowing to implement of a decentralized model is the blockchain. The idea of blockchain technology is simple. Its broader and more encompassing form, blockchain can be defined as a technology to develop trusted processes and data transactions on an open and distributed network via decentralized consensus among computer systems.

In its more common, widely used form, «a blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties.» Each transaction in the public ledger is verified by the consensus of most of the participants in the system. And, once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made.

A distributed network is a type of computer network that is spread over different networks. It provides a single data communication network, which can be managed jointly or separately. Besides shared communication within the network, a distributed network often also distributes processing. In a distributed network, the responsibilities for data transactions and computations are not given to any specific node. On the contrary, they are spread across the web, which is responsible as a whole for the results of a given process, like in some biological ecosystems, such as an ant community, where the construction of an ants' nest is the result of independent contributions by each ant. Blockchain technology guarantees that the distributed network's overall behavior, programmed to execute a particular process, is trustworthy. In this context, blockchain tries to respond to contemporary real-world scenarios' complexity by offering technology and a methodology for designing distributed applications that operate with private data in an openly verifiable way.

A distributed transactions system based on blockchain technology by its nature implements a ledger. This concept is at the core of the regulatory activities carried out by a wide range of authorities, institutions, and businesses. A more transparent, trusted, and globally recognized accounting

mechanism of this kind could dramatically facilitate and harmonize processes in e-Business and cross-broader trade scenarios. Even if, at the current stage of development, blockchain technology hasn't served the purpose of trade facilitation directly, it is already clear that, in the next decade, its contribution could be substantial. These positive expectations shouldn't prevent us from evaluating the limitations of an international trade approach enabled by blockchain technology, for example, in the context of legally binding agreements among traders.

3.2. Case study: Transparent e-documents and data exchange with the use of blockchain

Blockchain technology in the supply chain can be used to monitor costs, labor, losses, and emissions at each point in the supply chain. A distributed registry can also be used for verification of authenticity or compliance with fair trade rules by providing information on the origin of the goods. The delivery information can be a transaction every time you interact with a shipment.

A related technology called «Smart Contract» can be embedded in a block and triggered when a certain condition is met. For example, a payment transfer can occur automatically when a shipment reaches the customer's location.

3.3 PKI and Blockchain: Key study for agriculture value chain (AVC)

In this article, the authors would like to present the key study for agriculture value chain (AVC) based on the combination of PKI and blockchain technologies.

First, we will start from the decentralized approach based on the digital blockchain platform.

The most convenient way to implement blockchain technology is to create a digital platform that organizes interaction between different groups of participants who need to know certain information about each other's activities. The ability to organize interaction is essential for forming long-term productive business relations between the participants of the agricultural value chain. The idea of this platform was provided by Evoteq Company.

The digital platform [5] (see Figure 4) is open to interaction and integration through the cloud, making it accessible to all agricultural value chain participants. The digital platform architecture can significantly scale up without loss in quality and efficiency that will expand it to new product groups and new participants of the platform. The platform provides a high level of trust between participants using blockchain technology, creating clear and open conditions for their use.

This platform contains various blocks that allow to track-and-trace goods from farm to retailer.

These parts are:

- The source of the crop or the agricultural process
- Lab Testing information.
- Organic and Halal Certificates.
- Dispatch Details and Logistics provider details starting to add value.
- Recording of receipt from the agricultural source.
- Lab Testing and reports on receipt.
- Halal or Organic certifications or any other accreditations.
- Lot or batch numbers and processing information.
- Any contamination reports and holding actions.
- Storage information (temperature and humidity control).
- Batch release info and id codes.
- Logistics release info and logistics provider.
- Crop yield, Dietary info for live animals, mortality rates.
- Tagging of live animals.
- Crop Harvesting information and data tagging, with batch, date of release.
- Suppose we are exporting any shipping details. Bills of Lading / Airway bills and destination Final Value add to the Supply Chain and the most vulnerable to abuse.
- Goods in from source or primary processor.
- Recipe formulations and ingredients traceability.
- Production batch codes and production dates.
- Nutritional Information.
- Storage Information
- Certifications.
- Issued Barcodes or other identifiers.
- Expiry date information.
- Logistics Information.
- Shipping details dispatch date and destination.
- Goods out info.
- Vehicle Temperature monitoring.

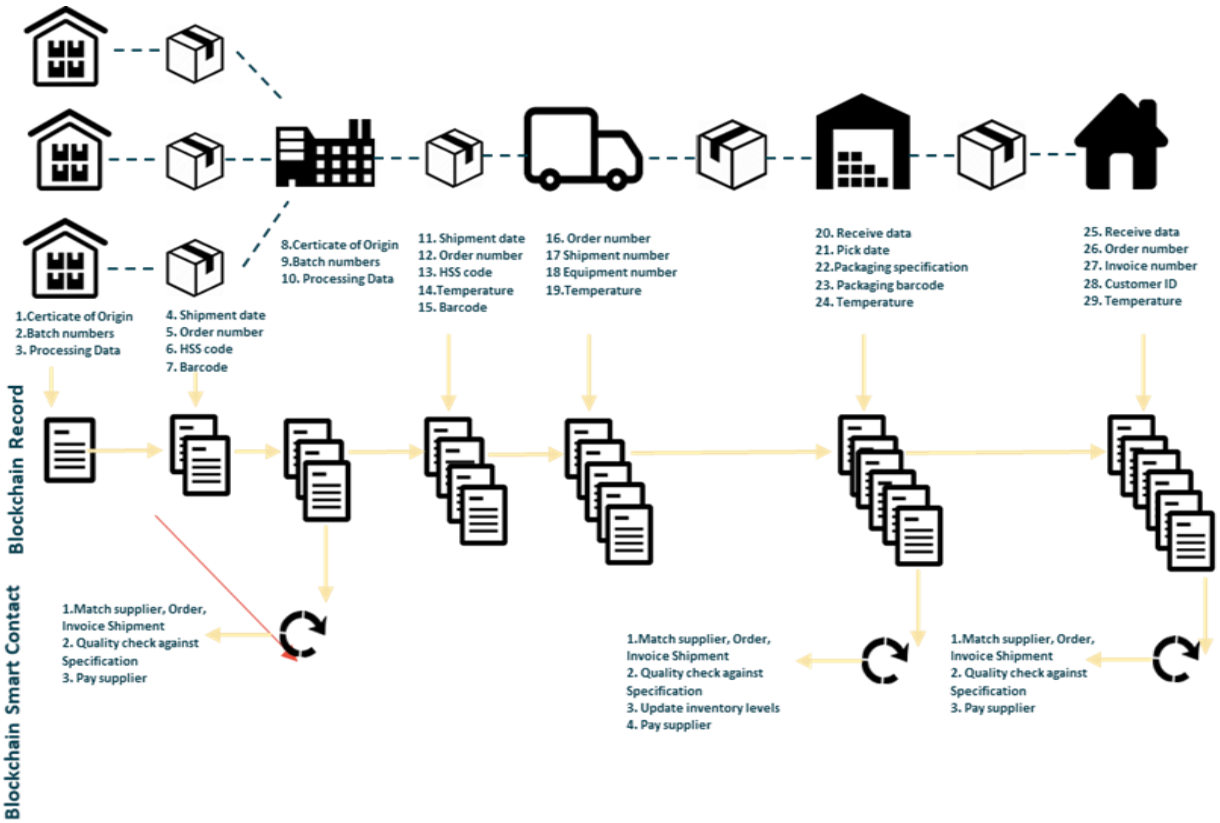

Figure 4. Blockchain use in the value chain

- Delivery confirmation.
- Protecting the consumer.
- Goods in and Temperature check.
- Expiry date check (remaining shelf life complies).
- Storage details.
- EPOS Data.

Blockchain platform gives a possibility to provide supplier managed inventory service and develop a complete dietary information database.

The consumer can check the product through barcoding information.

Allows the consumer to know where a product is sold.

The digital platform of the agricultural value chain can be connected and interact with the digital platform of the EAEU.

The economic benefits offered by this cloud solution can improve the efficiency of the entire value chain. It solves the following tasks:

1. Allows downloading product data at any stage of the value chain.
2. Provides continuous access to data.
3. Ensures the integrity and security of the supply chain.
4. Ensures that only proven, legally compliant products are available on store shelves.
5. Protects the integrity of the products and provides the possibility of recalling the manufacturer's goods to correct defects.
6. Allows checking for compliance with special needs (diabetic, organic, Halal goods).
7. Allows suppliers to track products on the market.
8. Allows users to check the supply chain.
9. Allows inspectors to verify the validity and acceptability of goods.
10. Protects the supply chain from counterfeiting.

The introduction of blockchain technology into the track&trace system will enable manufacturers, importers, and distributors to track their internal processes better.

The introduction of a digital track&trace platform, according to experts estimates, will achieve 99% accuracy of inventory data compared to 40-70% accuracy as it currently stands, which will optimize production and imports and significantly affect the reduction of the cost of goods [6].

During a pilot program conducted with Walmart, the testing showed that by using blockchain to track food, you could reduce the time it takes to track mango packaging from farm to store in just two seconds instead of days and

weeks. During the pilot, more than 100,000 mangoes from a Queensland supplier in Northern Australia were withdrawn by Biosecurity SA after fruit fly larvae were discovered in mangoes in Adelaide's foothills. The responsiveness of the recall allowed the organization to maintain its reputation [7].

So, within a supply chain, blockchain technology could be used to monitor costs, labor, waste, and emissions at every point of the supply chain, verify the authenticity or fair trade status of products by tracking them from their origin, shipping details could constitute a transaction at every interaction with a shipment – and customer(s) would know about it, trigger an action automatically.

However, there is a question: how can we combine decentralized and centralized approaches? The answer is - we will use business tools: a digital platform for track-and-trace AVC and a social network for trusted e-documents exchange.

A business network is based on a social network plus trusted cross-border e-document flow, based on PKI [8], that allows a customer to build a business network, choose the partner, and make deals, find investments, etc. This network is fully compatible with AVC based on the blockchain system.

Both these systems make AVC transparent and business processes simpler.

4 Conclusion

The authors reviewed two potential approaches to the mutual recognition mechanism: centralized and distributed. Suppose Trust services engaged in document lifecycle (incl. the chain of inter-domain gateways between the document's issuer and recipient) have different qualification levels. In that case, the overall level of qualification may be equal to the lowest of them. The level of trust could be provided in two different ways: transboundary trust environment and blockchain ecosystem.

We discussed a case study on the agriculture value chain example. Within a supply chain, blockchain technology could be used to monitor costs, labor, waste, and emissions at every point of the supply chain, verify the authenticity or fair-trade status of products by tracking them from their origin, shipping details could constitute a transaction at every interaction with a shipment – and customer(s) would know about it, trigger an action automatically.

Social network plus trusted cross-border e-document flow, based on PKI, allows a customer to build a business network, where the business entity can choose the partner, make deals, find investments, etc. These two systems are fully compatible and provide mutual recognition of e-data and e-documents via the whole AVC.

References

[1] Genesis Book. (11: 1-9). URL: http://bibliya-online.ru/chitat-bytie-glava-11/.

[2] RFC 3029 "Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols". URL: http://www.faqs.org/rfcs/rfc3029.html.

[3] Product description "TTPS "Litoria DVCS". URL: http://www.gaz-is.ru/produkty/dokumentooborot/gis-dvcs.html.

[4] Information technology - Security techniques - Guidelines for the use and management of trusted third party services (X.842). URL: https://www.itu.int/rec/T-REC-X.842-200010-I/en.

[5] Smarttrack. Global supply platform to ensure global supply chain integrity. URL: https://evoteq.com/en/our-projects/smarttrack.

[6] M. L. Simanovskaya, E. S. Silanteva, The use of digital technologies to increase the competitiveness of small and medium-sized businesses in the food sector / / State Management: Russia in Global Politics, Proceedings of the XVII International Conference (May 16-May 18, 2019), University Book Faculty of Public Administration of Lomonosov Moscow State University, Moscow Russia, 2019, pp. 159-165.

[7] Case Study: How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric. URL: https://www.hyperledger.org/learn/publications/walmart-case-study.

[8] RFC 5217 - Memorandum for Multi-Domain Public Key Infrastructure Interoperability». URL: https://tools.ietf.org/html/rfc5217.

[9] Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and Pacific (Framework Agreement, FA) agree to use the general CA for paperless trade. URL: https://www.unescap.org/resources/framework-agreement

facilitation-cross-border-paperless-trade-asia-and-pacific-0.