European Commission | EUIPO EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

ANTI-COUNTERFEITING BLOCKATHON FORUM

BLOCKCHAIN USE CASE

PUBLISHED – 18/10/2019

TABLE OF CONTENTS

1. INTRODUCTION

1.1 BACKGROUND

In June 2018 the EC, together with the EUIPO, organised the EU Blockathon, which was a 48-hour competition to create the next level of anti-counterfeiting infrastructure by the most talented teams. The winners' solutions focused on protecting legitimate goods by empowering the different players involved throughout the supply chain, from manufacturers to consumers, using solutions based on blockchain technology.

The 2018 EU Blockathon gathered a wide community around the problem of IPR infringement, including brands, logistics operators, teams and enforcement officers, such as customs as well as policy makers. It marked an important start of a broad movement to create and connect technical solutions addressing the problems of counterfeiting.

This broad movement has led to the Anti-Counterfeiting Blockathon Forum, which is open to all interested stakeholders and which will develop what the Blockathon began, the design and implementation of the next level of anti-counterfeiting infrastructure.

1.2 SCOPE AND OBJECTIVES

By definition, the anti-counterfeiting blockchain use case has anti-counterfeiting and the protection of IP rights and consumers as its primary objectives. The use case seeks to define activities and interactions that can address these objectives through blockchain technology, in particular by creating a product authentication system that will be almost impossible to breach or corrupt. It will do this by taking into account four perspectives, each associated with specific objectives, stakeholders and activities. By focusing on the relevant perspectives, the reader is able to identify the parts of the use case of most interest to them, provide targeted feedback and shape the future direction of the solution. See Figure 1 - Use Case Perspectives, below.

The use case perspectives are layered one over the other with activities in each layer interacting with those in other layers; for example, the authenticity layer includes the tokenisation ([1]) of goods in the blockchain. All of the other layers — transport, enforcement and provenance — add optional and supplementary features and information that can be associated with the tokenised goods.

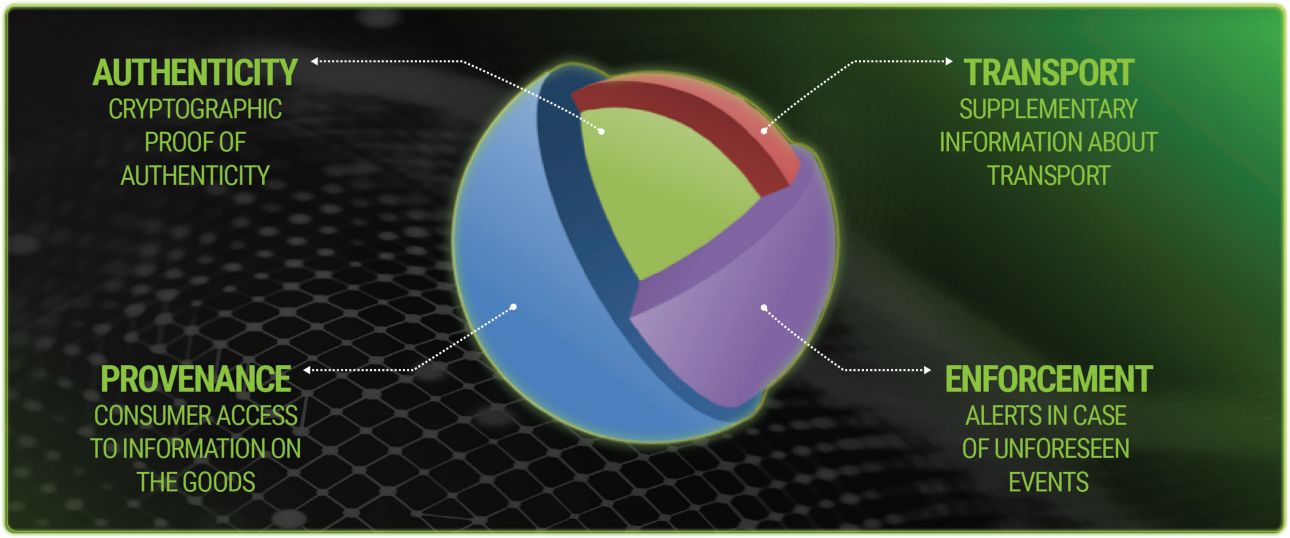


Figure 1 - Use Case perspectives

([1]) A token is a unique digital representation of any applied tracking or identification measure used in a product to distinguish that product from other products. Tokenisation is the technical process to produce a token.

Note that there are correlations between the different perspectives of the anti-counterfeiting use case with those of a classic supply chain. This reflects the fact that anti-counterfeiting is complementary to controls and measures applied throughout the supply chain. Future solution architecture could connect existing supply chain solutions with a future anti-counterfeiting solution such that the anti-counterfeiting solution adds additional capabilities. This and other considerations for the future are included in paragraph 2.2, Future challenges, below.

1.3 DOCUMENT PURPOSE

All solutions start with a clear understanding of the objectives and requirements. Building on the ideas and projects developed at the 2018 EU Blockathon, the European Union Intellectual Property Office (EUIPO) has prepared this use case with inputs from the forum reflecting their ideas, experience and contributions to form the basis for further definition and piloting activity.

1.4 DOCUMENT STRUCTURE

The structure of the document is as follows.

SECTION	DESCRIPTION
Use Case Executive Summary	A high-level textual view of the use case from end to end covering all four perspectives. This section also describes future challenges to address in later implementation stages.
Perspective Sections (Authenticity, Transport, Enforcement and Provenance)	Perspective overview – textual explanation of the use case specific to each perspective.
	Activity diagram – graphical view of activities per stakeholder, activity interconnections and the entries recorded on the blockchain.
	Activity definition – expanded definition of the activities illustrated on the activity diagram.
Data Dictionary	Definition of the data entities referenced in the activity diagram.

2. USE CASE EXECUTIVE SUMMARY

2.1 SUMMARY

The **authenticity perspective** is at the core of the anti-counterfeiting use case, addressing the need to prove that the goods received are genuine. Intellectual property ([2]) rights holders gain access to the anti-counterfeiting blockchain through a Blockchain Access Portal. The portal gives permissions to create tokens in the blockchain representing goods (tokenised goods) and proving the goods' authenticity.

Rights holders may authorise other parties, such as manufacturing and packaging suppliers, to create and handle tokens on their behalf and record events and information for their goods.

The record in the blockchain is a unique and immutable token. As goods pass from one party to another they exchange the token between digital wallets. The combination of a unique product identity and the continuous transferral of the digital identity between wallets will create a mathematical proof that the goods are genuine. For an illustration of this process, see Figure 2 - Tokenised goods pass from one operator to another, below.

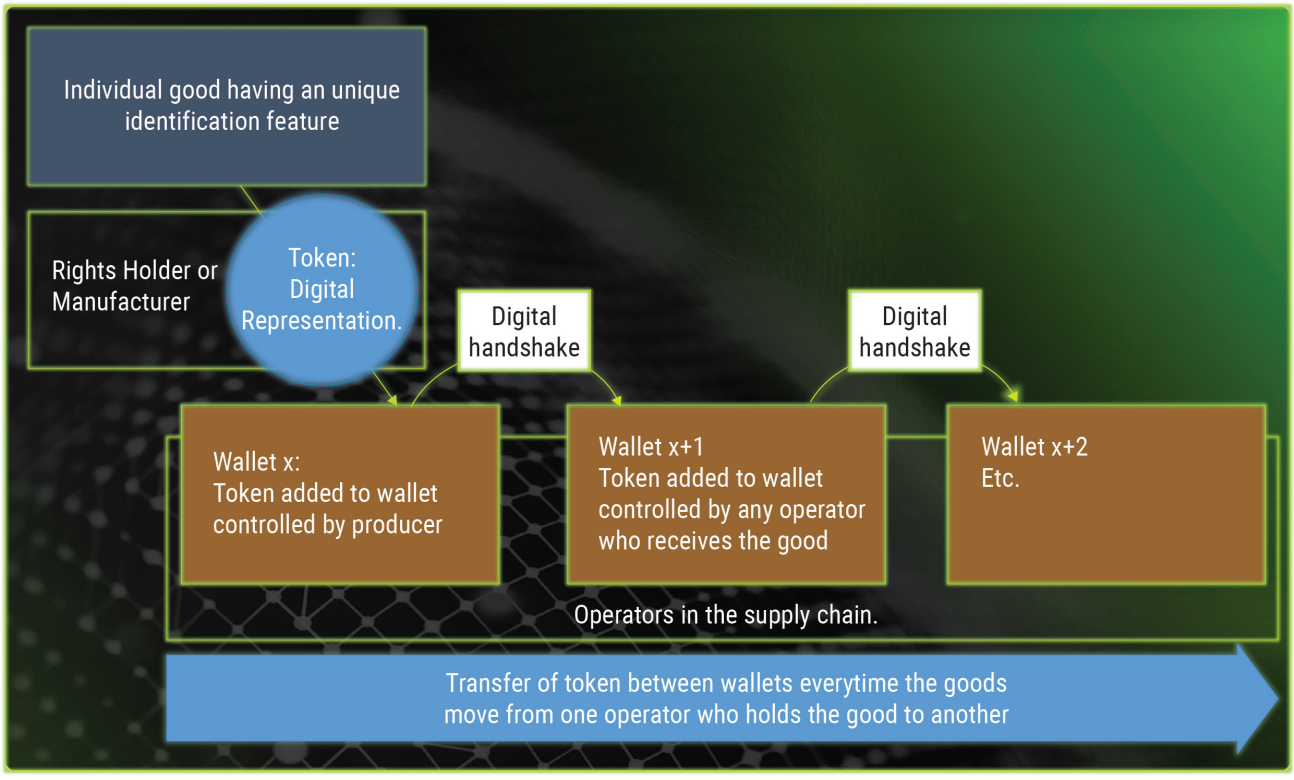


Figure 2 - Tokenised goods pass from one operator to another.

([2]) In Europe, such IP rights come under Regulation (EU) No 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning customs enforcement of intellectual property rights.

Customs and other enforcement authorities can take advantage of tokenised goods with proven authenticity, by allowing their swift passage through customs' checks.

Further optional services are associated with the other perspectives:

Within the **transport perspective**, containment information is stored. The container is tokenised and related to the goods contained using mathematical algorithms. This prevents the need to open a sealed container to check the authenticity of the contained goods each time a container moves between parties in the supply chain.

Optionally the blockchain will hold transport details (i.e. the transfer of goods from one location to another), allowing for the creation of a history of authentic transport records, which may support risk assessments performed by enforcement authorities.

Within the **enforcement perspective**, the blockchain can automatically generate events warning that the integrity of the goods is at risk, or detect an anomaly as goods pass between parties in the supply chain. Permissioned applications can monitor for such events and send notifications to rights holders and enforcement authorities. Optionally the blockchain records customs actions, which lets parties in the supply chain know the status of the transport.

Finally, the **provenance perspective** offers the possibility to further enhance the information held in the blockchain, by recording changes to the state of goods either manually or automatically detected. As well as assure the authenticity of the product, consumers can take advantage of such records to identify the production facility, supply chain movements, the provenance of raw materials, etc.

2.2 FUTURE CHALLENGES

Some of the challenges identified during the development of the use case have been included here for early consideration, discussion and analysis during pilot and implementation stages.

Relationship to existing track and trace systems and supply chain applications

The future blockchain based anti-counterfeiting system should be compatible with existing systems. It should not seek to replace or duplicate functionality already well served. However, it should not exclude new and light applications, which could integrate and exploit the features of the new blockchain solution. This emphasises the need for interoperability though standardisation and/or application programming interfaces (APIs).

Type of products for implementation

Effort and investment in the early stages of the solution's adoption will be relatively high. As such, higher value and

lower quantity products would be likely early targets for implementation. Over time, the solution should scale to support increasing quantities and a range of products while keeping implementation costs and efforts to a minimum.

Products composed of an assembly of goods

The use case treats simple atomic goods passing from the manufacturer to the logistics operators and finally to the consumer. Future implementation should support identifying and authenticating an assembly of goods, such as an aircraft or medical equipment.

Need to tokenise all goods in a single product line

The solution must provide confidence that products managed in the anti-counterfeiting blockchain are associated with guarantees of authenticity. To avoid confusion, a product line should not mix tokenised goods with non-tokenised goods requiring a different treatment.

Low impact on enforcement authorities and rights holders

The future solution must not increase the activity of customs and rights holders. On the contrary, the solution must support both parties to realise benefits through more effective support.

Dependency on the involvement of all parties handling tokenised goods

The use case presents the exchange of tokens through manufacturers, logistics operators and others involved in transporting the goods. Any issues in this chain of transfers would break the proof of authenticity.

Incentives to motivate and assure the correct take-up of the solution require analysis. For the consumer, their engagement in the solution could be incentivised through non-economic benefits derived from direct contact with the rights owner or manufacturer, or as a means of verifying authenticity upon resale. For the rights holder, incentives could include improved supply chain control, being alerted to suspicious activity and given proof of legal compliance and authenticity of goods with a high-brand value.

Support to the secondary market

The end-point of the current use case is the consumer. Proof of authenticity is also applicable for the secondary market, particularly for high-value goods with second-hand value.

The solution could also allow for some interaction at this point to perform other actions, such as data collection or updates to the properties of the goods following a repair and / or upgrade.

Role-based access rights certificates

GDPR and confidentiality requirements must be respected. This may lead to complex access and role management requirements, to handle permissions to connected databases and blockchains.

The organisations in charge of access would need to have the means, reputation and authority required to support this critical responsibility.

For data protection and regulatory reasons it is not best practice to hold all the information in the blockchain. Most of the information can be managed by traditional means such as databases, while anchoring this data in the blockchain.

Data volumes

Considering the potential volume of goods to be tracked, capacity could be a challenge and data to be placed in the blockchain should be limited to only what is needed. That said, blockchain and its related technologies are advancing rapidly and solutions for data volumes can be anticipated.

2.3 ENFORCEMENT AND REGULATION - IMPORTANT CONSIDERATIONS

This use case introduces the **Blockchain Access Portal** as the component for rights holders to gain access to the anti-counterfeiting blockchain and create tokenised goods for selected product lines. The portal also allows rights holders to register delegated trusted parties to create tokens on their behalf and access associated services.

The Enforcement Database ([3])(EDB) contains information on products that have been granted an intellectual property right, such as a registered trade mark or design. Police and customs officials from the 28 Member States can access this tool to view information and product details, making it easier for them to identify counterfeits and take action.

Enforcement Database (EDB) features, such as secure authorisation and product line definition, are relevant to a future blockchain solution and in particular the role of the Blockchain Access Portal. Opportunities for controlled and secure interoperability with the EDB are considerations for a future piloting phase. The EDB's confidential data will never be stored in the blockchain.

Only rights holders can give permissions to other parties to record goods and access associated data and services on the blockchain. Any future anti-counterfeiting blockchain solution must comply with Regulation (EU) No 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning customs enforcement of intellectual property rights.

3. AUTHENTICITY PERSPECTIVE

3.1 PERSPECTIVE OVERVIEW

Authenticity is at the core of the anti-counterfeiting use case addressing the need to prove that the goods handled are genuine.

Rights holders gain access to the anti-counterfeiting blockchain through the Blockchain Access Portal. This gives permissions to create tokens in the blockchain representing actual goods.

Optionally rights holder can use the same portal to identify further parties, such as manufacturers authorised to create goods tokens. They may also specify product lines managed through the blockchain.

([3]) EUIPO, Observatory, Enforcement Database.

At the point of tokenising goods to track in the anti-counterfeiting blockchain, it is imperative to link the blockchain's identity to real-world goods using specific characteristics and identifiers, labelling or packaging (e.g. bar codes, QR codes, chemical fingerprints).

Any user, such as transport companies, enforcement authorities or the final consumer, can scan the goods to check their authenticity.

3.2 ACTIVITY DIAGRAM

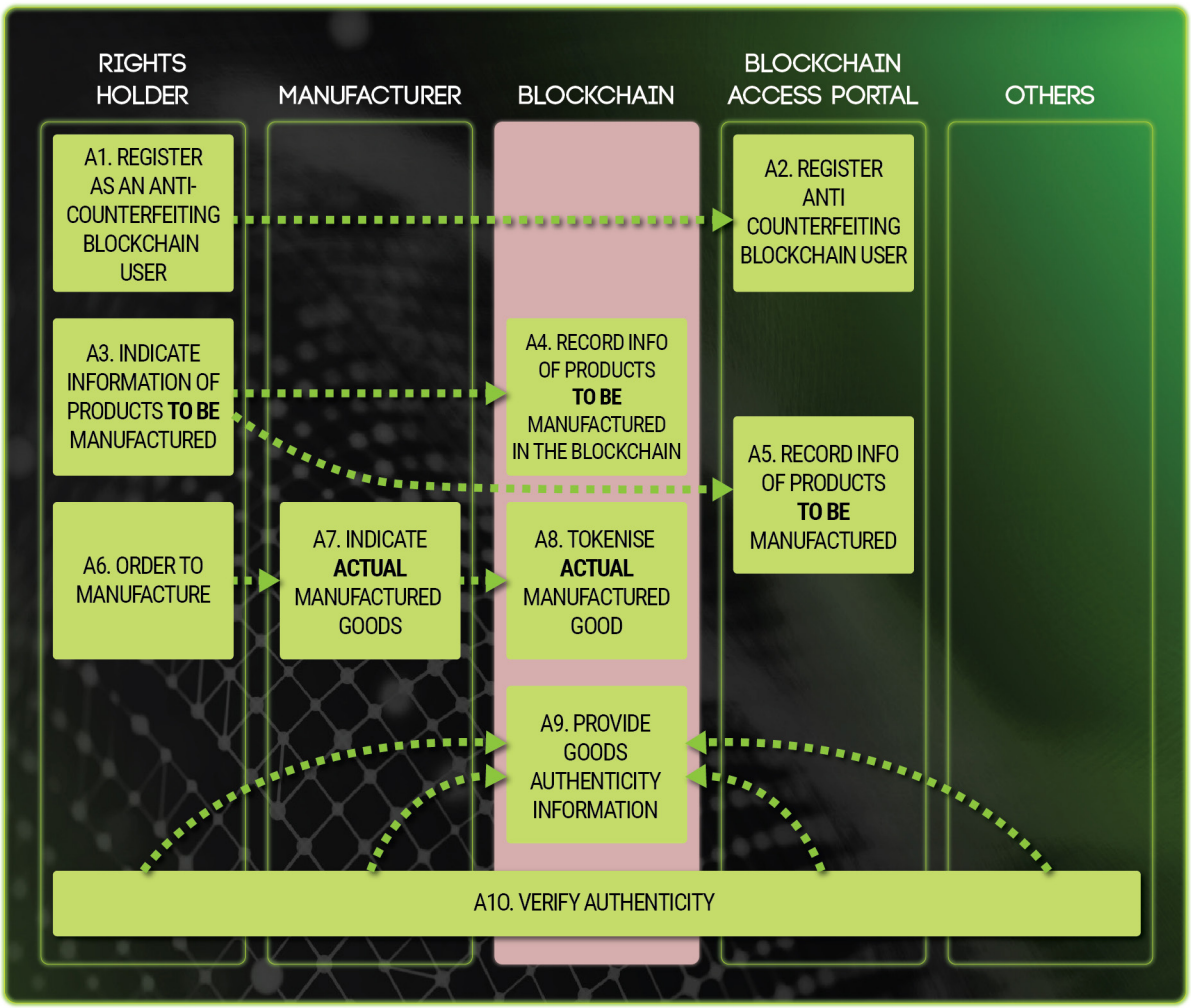


Figure 3 - Authenticity Perspective

3.3 ACTIVITY DEFINITION

ID	ACTIVITY	DESCRIPTION	ACTOR(S)	DATA ENTITY
A1	Register as an anti-counterfeiting blockchain user	The rights holder registers as a user of the anti-counterfeiting blockchain. To record data in the blockchain you have to have rights granted through the Blockchain Access Portal, either directly as the rights holder or indirectly by being given the authorisation of the rights holder (e.g. a manufacturer).	Rights Holder	
A2	Register anti-counterfeiting blockchain user	The Blockchain Access Portal records the rights holder as a registered user of the anti-counterfeiting blockchain.	Blockchain Access Portal	Registered user
A3	Indicate information of products to be manufactured	The rights holder indicates information of the products to manufacture.	Rights holder	
A4	Record info of products to be manufactured in the blockchain	The anti-counterfeiting blockchain records the products to manufacture and track in the blockchain.	Blockchain	Tracked product line
A5	Record info of products to be manufactured	Optionally the Blockchain Access Portal records the product lines tracked in the blockchain. If the product line exists, mark the product line as using blockchain. Otherwise, include all product information.	Blockchain Access Portal	Tracked product line
A6	Order to manufacture	The rights holder gives the order to manufacture to the manufacturer(s).	Rights holder	
A7	Indicate actual manufactured goods	The manufacturer identifies the actual manufactured goods to track in the blockchain.	Manufacturer	
A8	Tokenise actual manufactured goods	The anti-counterfeiting blockchain tokenises the goods to track in the blockchain.	Blockchain	Goods token
A9	Provide goods authenticity information	The anti-counterfeiting blockchain provides an assessment of authenticity (OK or NOT OK).	Blockchain	
A10	Verify authenticity	The stakeholder checks if the product is authentic.	Rights holder Manufacturer Logistics operator Customs/Enforcements Authorities Customer	

4. TRANSPORT PERSPECTIVE

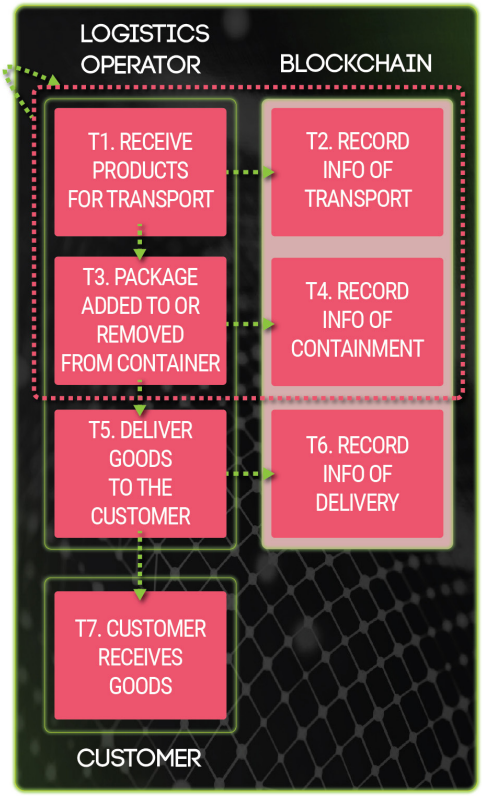
4.1 PERSPECTIVE OVERVIEW

Transport (ship freight, air cargo, etc.) offers a second layer of services after the authenticity core. In this perspective, goods transfer securely between parties. As goods pass through the supply chain, the associated tokens created in the authenticity layer exchange between digital wallets. The combination of a unique product identity and the continuous transferral of the digital identity between wallets will create a mathematical proof that the goods are genuine.

The anti-counterfeiting blockchain holds details of containers so that the tracking of goods continues after sealing them in the container ([4]). This prevents the need to open a sealed container to check on the already tokenised goods (see 3.3 A8 "Tokenise actual manufactured goods") each time the container moves between parties in the supply chain. By scanning the container, it is possible to prove the authenticity of the contained goods. Likewise, when a container is unsealed, the goods and container relationship is broken.

Optionally the blockchain can record further details of the transfer. While this does not enhance authenticity for the goods shipped, it allows for the maintenance of a history of authentic shipping records, which may support a risk assessment from enforcement authorities (see paragraph 5, Enforcement Perspective, below).

4.2 ACTIVITY DIAGRAM



T1, T2, T3 and T4 are iterative, with each iteration representing the passing of goods along the supply chain from one party to another.

"Figure 4 - Transport Perspective"

([4]) A container is considered to be any means of packaging necessary for the transport of the product based on the needs of the logistics operator.

4.3 ACTIVITY DEFINITION

ID	ACTIVITY	DESCRIPTION	ACTOR	DATA ENTITY
T1	Receive products for transport	The logistics operator receives the goods from either the manufacturer or another logistics company. Digital tokens representing the goods pass between digital wallets held by each party.	Logistics operator	
T2	Record info of transport	The anti-counterfeiting blockchain records the transport.	Blockchain	Transport
T3	Package added to or removed from container	The logistics operator either: a) adds the goods to a container, or b) removes the goods from a container.	Logistics operator	
T4	Record info of containment	The anti-counterfeiting blockchain records the link between the goods and the container (added or removed).	Blockchain	Containment
T5	Deliver goods to the customer	The logistics operator delivers the goods to the customer.	Logistics operator	
T6	Record info of delivery	The anti-counterfeiting blockchain records the delivery to the customer.	Blockchain	Delivery
T7	Customer receives goods	The customer receives the goods from the logistics operator.	Customer	

5. ENFORCEMENT PERSPECTIVE

5.1 PERSPECTIVE OVERVIEW

As mentioned, the authenticity perspective ensures with high certainty that goods tokenised in the blockchain come from the rights holder. In addition, the transport layer assures that there has been no issue through the supply chain. Customs and other enforcement authorities can take advantage of this proof of authenticity and safe transport to allow a swift passage of the goods through customs checks.

The enforcement perspective adds further optional activities.

Information collected on authentic goods, such as shipping routes and legitimate parties involved in the supply chain, may aid enforcement assessments of non-blockchain handled goods. For example, by comparing legitimate transport records (e.g. stages of a journey recorded in the blockchain) with goods of similar product lines, anomalies could be detected.

The blockchain could also aid enforcement by automatically generating alerts when events and movements at the level of the goods or holding containers could affect the integrity of the goods. In such cases, applications monitoring events in the blockchain could generate notifications to rights holders and enforcement authorities.

Optionally the blockchain records a customs authority's actions. This may help parties in the supply chain know the status of a transport.

5.2 ACTIVITY DIAGRAM

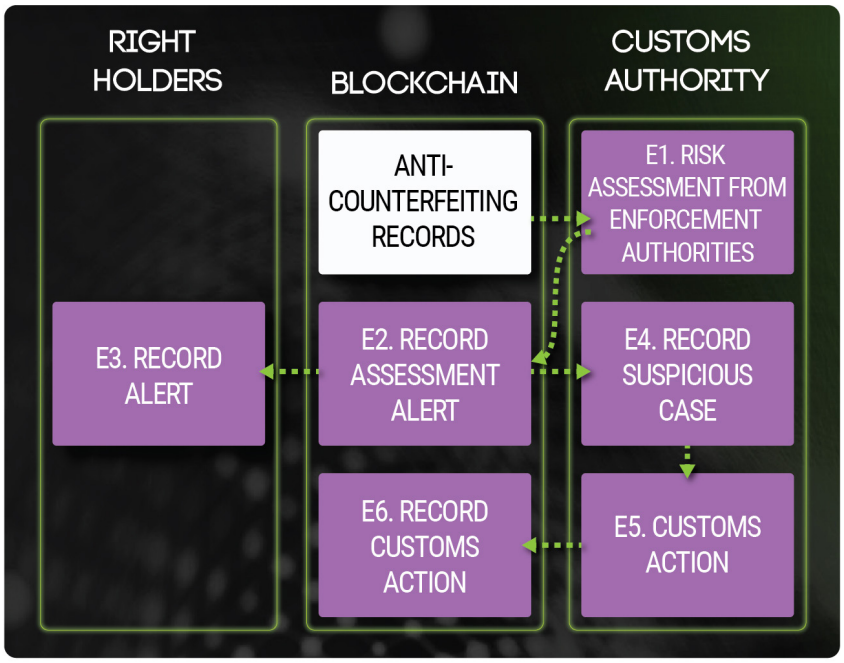


Figure 5 - Enforcement Perspective

5.3 ACTIVITY DEFINITION

ID	ACTIVITY	DESCRIPTION	ACTOR	DATA ENTITY
E1	Risk assessment from enforcement authorities	In future, tools would be able to retrieve information from the blockchain to support assessments of authenticity. Information retrieved could trigger the creation of a blockchain alert associated with one or more goods. Such alerts may be the consequence of failed transfers between parties in the supply chain or resulting from change in state (see paragraph 6, Provenance Perspective, below). Information retrieved could support risk assessments of products not managed by the blockchain. For example, anomalies raised by comparing legitimate transport routes with routes of other goods from similar product lines.	Customs authority	
E2	Record assessment alert	The anti-counterfeiting blockchain records an enforcement assessment alert. In some cases, the activities E3 'Record alert' and E4 'Record suspicious cases' happen automatically (e.g. a sealed container unlawfully opened).	Blockchain	Alert
E3	Record alert	The rights holder records an alert.	Rights holder	
E4	Record suspicious case	The customs authority records a suspicious case.	Customs authorities	
E5	Customs action	Customs perform any of the following actions on a tracked good: • inspection • destruction of goods • seizure.	Customs authorities	
E6	Record customs action	The anti-counterfeiting blockchain records the customs authority action.	Blockchain	Customs action

6. PROVENANCE PERSPECTIVE

6.1 PERSPECTIVE OVERVIEW

As mentioned, the authenticity perspective ensures with high certainty that goods identified by blockchain tokens come from the identified rights holder or from the manufacturer though a controlled supply/logistics chain. Through simple applications, consumers could take advantage of this proof of authenticity to assure them that the goods purchased are genuine.

The provenance perspective supports further optional records in the blockchain for the customers' information. Such records may identify the production facility, supply chain movements, the provenance of raw materials, etc.

Also, in the provenance layer, detectors allow for the automatic recording of data associated with the tracked goods. This information may provide positive feedback, such as 'the temperature of the goods remains constant', 'the goods have reached their destination on time' or negative feedback, such as 'the container has been opened illegally'.

Negative events allow for the automatic generation of blockchain alerts (see paragraph 5, Enforcement Perspective, above).

6.2 ACTIVITY DIAGRAM

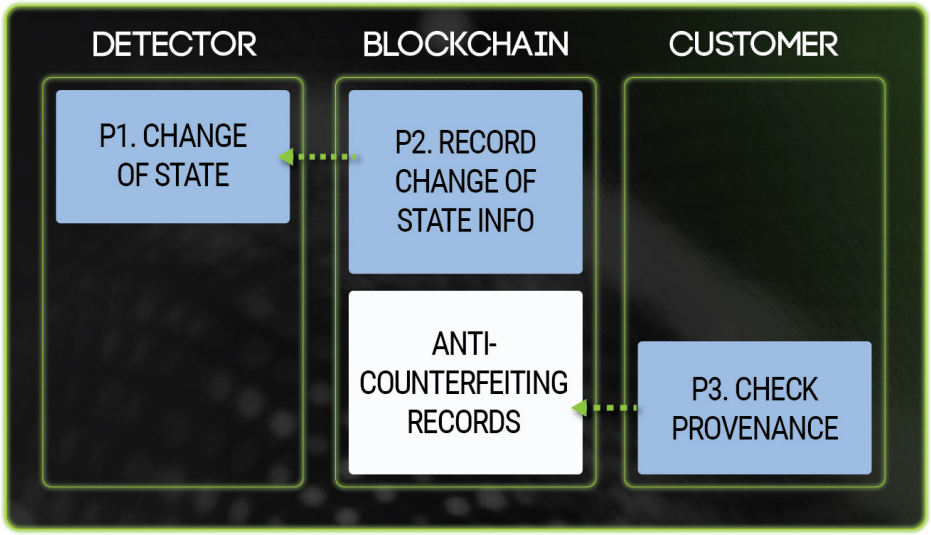


Figure 6 - Provenance Perspective

6.3 ACTIVITY DEFINITION

ID	ACTIVITY	DESCRIPTION	ACTOR	DATA ENTITY
P1	Change of state	A change of state is detected. This could be detected manually or automatically. Change of state information may provide positive feedback, such as proof of careful handling, data of customer interest, or negative feedback, such as changes of state that affect the integrity of the goods.	Detector	Change of state information
P2	Record change of state info	The anti-counterfeiting blockchain records the change of state information. In some cases, (e.g. an electronic seal is broken) the activity E2 'Record assessment alert' happens automatically.	Blockchain	Change of state information
P3	Check provenance	The customer requests provenance knowledge of a product.	Customer	

7. DATA DICTIONARY

7.1 DATA ENTITY "REGISTERED USER"

This entity contains the following types of data:

- Rights holder identifier
- Timestamp

7.2 DATA ENTITY 'TRACKED PRODUCT LINE'

This entity contains the following types of data:

- Rights holder identifier
- Product line identifier
- Manufacturer identifier
- Identifier of the user creating the record
- Timestamp

7.3 DATA ENTITY "GOODS"

This entity contains the following types of data:

- Token identifier
- Goods real world identifier (e.g. QR code)
- Product line identifier
- Identifier of the user creating the record (manufacturer or rights holder)
- Timestamp

7.4 DATA ENTITY "TRANSPORT"

This entity contains the following types of data:

- Goods token identifier
- Identifier of the user creating the record (the receiving entity)
- Type of transport
- Timestamp

7.5 DATA ENTITY "CONTAINMENT"

This entity contains the following types of data:

- Container identifier
- Identifiers of goods contained
- Status of container (open, sealed, etc.)
- Identifier of the user creating the record (handling entity)
- Timestamp

7.6 DATA ENTITY "DELIVERY"

This entity contains the following types of data:

- Goods token identifier
- Identifier of the user creating the record (the delivering entity)
- Timestamp

7.7 DATA ENTITY "CHANGE OF STATE INFORMATION"

This entity contains the following types of data:

- Detector identifier
- Identifiers of goods affected
- Status of goods
- Timestamp.

European Commission | EUIPO EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

ANTI-COUNTERFEITING BLOCKATHON FORUM

BLOCKCHAIN USE CASE