T·MINING | BLOCKCHAIN LOGISTICS

Secure Container Release

WHITE PAPER

With Secure Container Release (SCR), T-Mining demonstrates how security in the port can be improved and commercial privacy of the participating companies can be guaranteed.

August 2022

www.securecontainerrelease.com

SECURE CONTAINER RELEASE

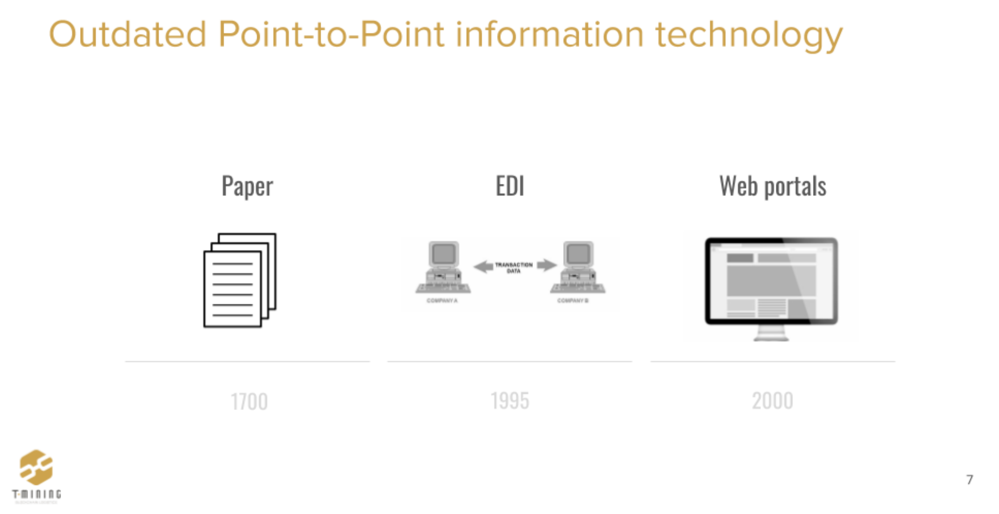
Digitization in the logistics sector has led to a significantly increased automation of intra-company processes. Efficiency gains within one company powerfully drove choices in the field of ICT technologies. Investments in the digitization of business processes where the dependence on third parties is high are more complex and laborious. The fragmented offer and the relatively limited scale of many digital B2B platforms make smooth cooperation difficult. Partly because of this, companies are still digital silos where the exchange and synchronization of data between chain partners are complex and inefficient.

The technology used for digitization and automation between companies is often decades old. For example, paper is still the most critical information carrier in the transport and logistics sector today, although new legislative initiatives, such as eFTI[1] , promise to change this.

[1] Read more: "The electronic freight transport information (eFTI) regulation has been approved by the EU and will enter into force in August 2024."

Electronic Data Interchange (EDI), a technology developed in the 1970s and subsequently used within the logistics sector to exchange data between 2 parties, is still a common way of information exchange, despite its limited scalability. Due to a lack of standardization, point-to-point connections between 2 companies differ significantly and result in high setup and maintenance costs.

Due to the rise of the internet, web portals were developed where users manually enter data into systems of their chain partners, with a high risk of errors. Despite the substantial increase in digitization, significant challenges remain concerning digitizing chain collaboration in a flexible, cost-efficient, and scalable way.



Outdated Point-to-Point information technology

Paper — 1700

EDI — 1995

Web portals — 2000

This paper shows how decentralized technologies such as blockchain can strengthen the digitization of supply chains. The blockchain application *Secure Container Release (SCR*), developed by the Antwerp start-up T-Mining, illustrates how blockchain, as a relatively new technology, can make chain collaboration safer and more efficient. At the beginning of 2020, SCR was put into production in the port of Antwerp. As the first shipping company globally, MSC uses blockchain technology to make the collection of containers in the port safer. After less than 12 months, 800 companies are already connected to this network, and thousands of employees spread over 20 countries are using this application.

In 2017, T-Mining with Secure Container Release was one of the first companies worldwide to apply blockchain in the maritime industry during a Proof-of-Concept in collaboration with MSC, PSA, BDP International, and several carriers, and the company enjoys wide recognition in the area of innovation and expertise in both blockchain technology and the maritime and logistics sector.

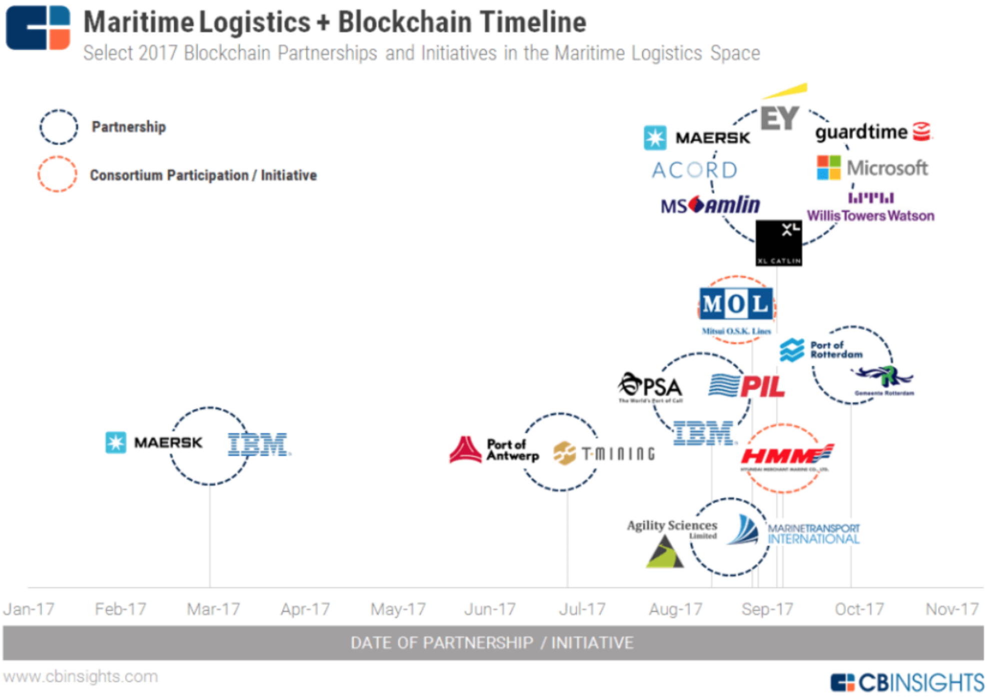


Figure 1: CB-Insights - 2017[2]

In a Europol report[3] from 2019, the **lack of digitization of chain cooperation is directly associated with the increasing drug problem** in various European ports. For example, it has become apparent that the collection process for import containers from, for example, Latin America is susceptible to fraud.

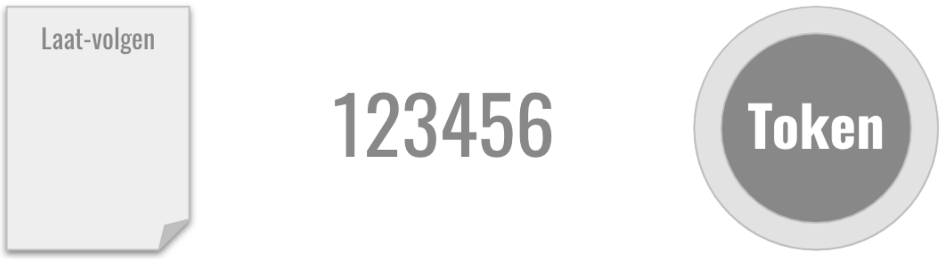
A pin code is required to pick up a container that is imported via a European port at the terminal by a truck driver. This pin code is generated by the shipping

[2] Read more: CB-Insights: Major Links in The Global Trade Supply Chain That Blockchain Could Transform
[3] Read more: The 2019 EU Drug markets report

company and communicated to the forwarder responsible for transporting the container to the hinterland. Information such as the container number and associated pin code is forwarded to the carrier responsible for collecting the container at the terminal.

Employees with access to this information are bribed by organized crime to pass on these PINs. For example, 100,000 euros is offered for one pin code.

These pin codes represent the right to collect a container, the so-called "pick upright" or collection right. Essential to these pin codes is that they are processed confidentially and securely by the various organizations involved in this process, such as the shipping company, the forwarder, the transporter, subcontractors, the driver, and the terminal. In practice, it appears that these pin codes are often distributed via insecure communication, such as email, telephone, or text message. PIN code fraud is, therefore, a known problem in the sector and a real security risk for the employees and organizations involved. Here too, this chain is only as strong as its weakest link. Recent incidents involving bribed employees illustrate the urgency of the problem and the need for a solution that can serve the entire chain.



Before
Delivery Order
+ Easy transferable
- Paper document

2010
PIN-code
+ Digital
- Unsecure transfer

2020
Secure Container Release
+ Digital & automated
+ Secure transfer

Initially right to collect a container was contained in a document called the "Follow-up." Anyone who could present the document to the terminal could receive the container. The PIN has been introduced as a digital solution in many ports for several years. Later it turned out that these pin codes were not a safe solution.

What makes these PINs unsafe? There are some simple explanations for this:

(i) **A PIN code is easy to copy.** Indeed, when sent around via email, it cannot be ruled out that someone will forward this information to someone with bad intentions. Naturally, the same applies to a highly secured application. Even then, someone with access to this information can still efficiently distribute this information outside of the application;

(ii) A logical consequence of this is that **holding a secret PIN code can be challenging to use**. Anyone with access to this information can pass it on to unauthorized persons. Conversely, access can be gained to secret information through hacking, for example, through identity fraud (for example, simply passing on login details to a database or application);

(iii) **A PIN is not unique**. As a PIN recipient, you are not sure that you are the only one who has the right to collect a container. You are certain that more people have the same right. You cannot transfer a pin code; at most, you can duplicate it;

(iv) **A PIN is almost impossible to trace**. When you receive a pin code, you cannot see whether this pin code is authentic, let alone correct. Conversely, the same applies when someone with bad intentions can efficiently distribute them without leaving a (digital) trace.

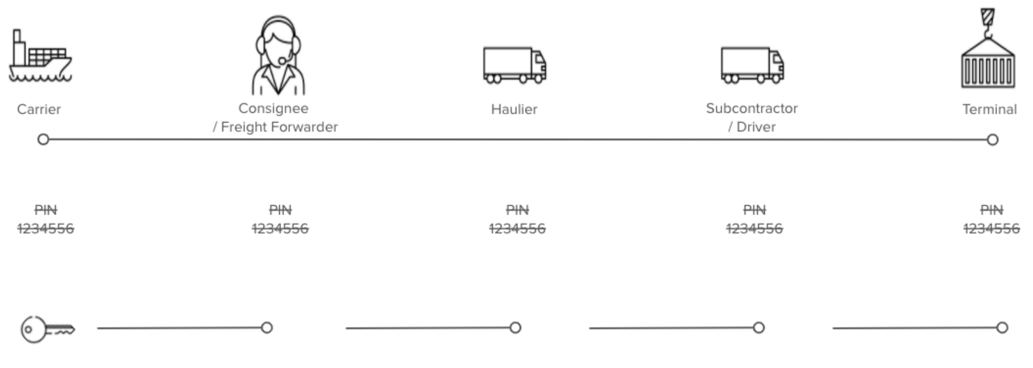
The above arguments are of course logical. What's more, **it is noteworthy that PINs are still used today** to secure the container release process. This of course has to do with the nature of digital systems as we know them today. The internet, for example, is designed to distribute information very simply and quickly.

But that is precisely where a problem arises. Certain rights - such as the right to collect a container - are only useful or valuable if they are also scarce. Think of money, which loses its value when more is made of it.

This is exactly where blockchain technology makes up the difference. The most famous application of blockchain today is **Bitcoin**, the most renowned cryptocurrency. Unique to blockchain technology is that bitcoins can be transferred from one person to another without an intermediary, being the bank. The bitcoin network guarantees that every coin is unique and can only be spent once. A coin would lose its value if it were not uncommon and could be spent more than once. This is also called the "double-spending" problem, which blockchain technology solves. This is an essential distinction from classic, central databases.

Blockchain guarantees - among other things - unchangeable data storage. Information is chained together in blocks utilizing cryptographic encryption. The slightest change to the information stored in a block breaks the cryptographic chain. Then the blockchain will compare the data with that stored on other nodes in the network. In this way, it can be ascertained whether something is "true" since "the truth" is always kept on different nodes - which implies that a blockchain network is by definition decentralized and cannot run on one computer system or server.

Returning to our release rights and associated pin codes, it becomes clear what added value blockchain technology offers compared to classic centralized technology, such as a cloud solution or a definitive database. **Due to the tokenization, the traditional PIN codes are replaced by "relay batons,"** which are then passed on between the different participants in the chain. Each "relay baton" can only be passed once. Once transferred, one no longer has any rights. In other words, the collection right has become unique and traceable. After all, every participant must also identify himself on the blockchain.



Secure Container Release uses blockchain technology

- tokenizes the right to pickup a container
- avoids "stolen" PIN-codes as PIN-codes can be duplicated
- creates a digital flow between all parties involved

The second challenge immediately arises here: **identity**. How can we be sure of someone's identity? After all, the problem of PIN code fraud is not solved if an organization could participate in the blockchain network of Secure Container Release under a false identity. That way, the takeaway right could still be passed on to criminal organizations. Think of an employee who, instead of a pin code, now shares his login details to the application in exchange for money.

To solve this identity issue, an Identity (ID) Wallet was developed, which is a piece of software that is installed on the computer network of the organization concerned when he registers on the application. The ID wallet contains cryptographic keys with which the organization can identify itself (think of a login & password, for example) on the SCR application and the underlying blockchain network. This identification procedure can only be validly performed from the corporate network. That way, it can be ruled out that someone would try to log in with stolen credentials and manipulate a takeout right.

Of course, an organization with bad intentions could also try to install an ID wallet and gain access that way. For this, three different methods were proposed.

(i) Firstly, an organization can only register – and therefore install an ID wallet – on Secure Container Release if they have been **invited** by an existing member. Similar to a classic Service Club, new members are only nominated by existing members, who already have the trust of the group;

(ii) Once accepted, this invitation turns into a **private connection** between both organizations. In this way, the new organization 'enjoys' the confidence of the inviting organization. This connection is necessary to receive and pass on a collection right. Without these connections, an organization cannot participate in the security process. It also does not receive information from other organizations. That way, it cannot request (and decrypt) information from the blockchain;

(iii) The identity of this new organization is also **checked** with a specialized authority, in the Port of Antwerp, this is C-Point, which validates the identity of the organization involved and confirms it to the SCR solution.

The final significant challenge that arises next is **privacy**. The transparency created by blockchain technology could create considerable privacy issues if other participants could capture this information. By tokenizing the collection right on blockchain and registering the identity of an organization, anyone with access to the blockchain network can find out who works with whom and how often. Of course, users can be denied access to this information via the SCR application, but since a blockchain network is by definition decentralized, there are different blockchain nodes, which are hosted by various organizations. Each node contains a copy of the information, which could be read with the necessary knowledge and skills.

In order to be able to offer a comprehensive solution that guarantees privacy, the ID wallet also plays an important role. Private connections are used in the ID wallet. This means that every organization that establishes a connection with another organization exchanges unique and, therefore private cryptographic keys. Compare the private connections with a unique telephone number, with which each of your contacts can reach you. In contrast to the same telephone number - with which everyone who knows your telephone number - can easily identify you, a private connection therefore offers **guaranteed privacy**. Thus, validate an organization 'A' whether he has a valid pick-law received from his known connection 'B', then transmit them to another connection 'C'. But it is impossible for 'B' and 'C' to find out (read: decrypt) that this container was passed on through intermediary 'A'. It goes without saying that in a particularly competitive sector, where shipping companies, forwarders and transporters work together for one container but are competitors for the other container, this is literally a 'much needed' guarantee.

In addition, so-called 'peer-to-peer' technology offers additional guarantees regarding privacy. **Information is then not exchanged centrally, but locally.** For example, organization 'A' will receive information from organization 'B' and in turn exchange it with organization 'C', without a central party having access to this information.

Classic cloud solutions, which typically centralize information, pose specific privacy and data ownership issues. Recent scandals around e.g., Facebook learn that if data is managed by one central party, it depends on how this organization handles the data. Certainly, in a commercial B2B context in which information is described as the new 'gold', companies are increasingly aware of this risk.

An additional advantage of decentralization is that with Secure Container Release, there is no '**single point of failure**'. The lack of a central database with all pin codes makes it much more difficult for a hacker to steal data. After all, if there are no more pin codes, you can no longer steal them, not even at T-Mining.

Note that the above also implies that **not all data is written to the blockchain**. For example, the blockchain is mainly used for the tokenization of the right, so that this right can be transferred, which is similar to the principle of bitcoin or other cryptocurrencies.

In addition to technical challenges, there are also **important practical challenges associated with blockchain technology**. First of all, blockchain assumes in almost all cases the use of a common network by all different participants and users. In this context, we also speak of a consortium. Crucial here is good coordination and consultation between the stakeholders. After all, different parties must agree to work out and use a standard solution. In addition, one strong party can also encourage the other participants to use one system. A mandatory nature or initiative of a public body can also facilitate such coordination.

Obviously, the solution must also be **sufficiently accessible.** For example, Secure Container Release follows the existing release process and supports the most important functions such as the possibility to block a container in certain cases or to revoke the collection right. The way of working hardly changes for the participants involved. Secure Container Release has been developed in such a way that users can use the application almost without any training.

From a technical point of view, any complexity surrounding blockchain technology has been kept to an absolute minimum. For example, it is required to install an ID wallet on the company network of the organization concerned. Apart from a few possible firewall adjustments, a new organization can be up and running in less than 30 minutes. Larger companies usually have more complex ICT procedures, which means that such an installation cannot be carried out immediately. To avoid that the release process would come to a standstill in this way, a temporary Cloud wallet is set up with which the organization can start in a fast and secure way.

Users can then log in via the **SCR web application** to consult an overview of the released containers and to transfer these - entirely pin code-free - to the next party in the chain. In the background, the identity of the organization is always checked by means of the ID wallet when logging on and transferring. In this way, the ID wallet fulfills the role of an advanced and secure 'Two-Factor Authentication' procedure.

Larger forwarders and carriers usually already have an existing software solution to organize the release process, among other things. An **SCR API** available for this, which makes an integrated - and thus fully automated - solution possible.

Secure Container Release is **one of the few blockchain-based solutions in the Maritime and Logistics sector**. Since the beginning of 2020, MSC Belgium is the first shipping company to use Secure Container Release in the port of Antwerp. Later that year, a pilot project was started in the port of Rotterdam with four different shipping companies on board. Also Hapag Lloyd and CMA-CGM are actively rolling out SCR in the Port of Rotterdam and Antwerp.

Today, Secure Container Release connects more than 1.300 companies in over 25 countries.

T-MINING

Secure Container Release is being developed by T-Mining, an Antwerp start-up that has developed various solutions for the Maritime and Logistics sector, always based on decentralized technologies such as blockchain. Inspired by the vision and philosophy behind blockchain, T-Mining develops decentralized applications in a radically innovative way. T-Mining uses new values and insights around respecting privacy and the ownership of data.

Conclusion

With the roll-out of Secure Container Release in the port of Antwerp and Rotterdam, T-Mining is demonstrating that blockchain technology is gradually finding its way into concrete business applications and can be used on a large scale.

Blockchain offers an important advantage here, namely the guarantee that the right to collect a container remains unique. This means that this solution is more secure and more resistant to hacking. SCR also offers an important efficiency advantage. Digitization avoids manual actions and errors and allows the release process to be automated.

This solution illustrates how a complex chain of different players can work together in a secure manner and exchange data while respecting the commercial privacy of the participating companies.

Secure Container Release's decentralized architecture means that crucial information, such as a company's identity, remains under control of the company. This information is only stored on the servers of the company itself.

In contrast to the known Cloud-based SaaS solutions, there is no centralization of sensitive information such as the identity or the commercial relationships of a company. This means that T-Mining itself does not have access to this information.

***

Secure Container Release

Secure Container Release is being developed by T-Mining, an Antwerp start-up that has developed various solutions for the Maritime and Logistics sector, always based on decentralized technologies such as blockchain. Inspired by the vision and philosophy behind blockchain, T-Mining develops decentralized applications in a radically innovative way. T-Mining uses new values and insights around respecting privacy and the ownership of data.

www.t-mining.be