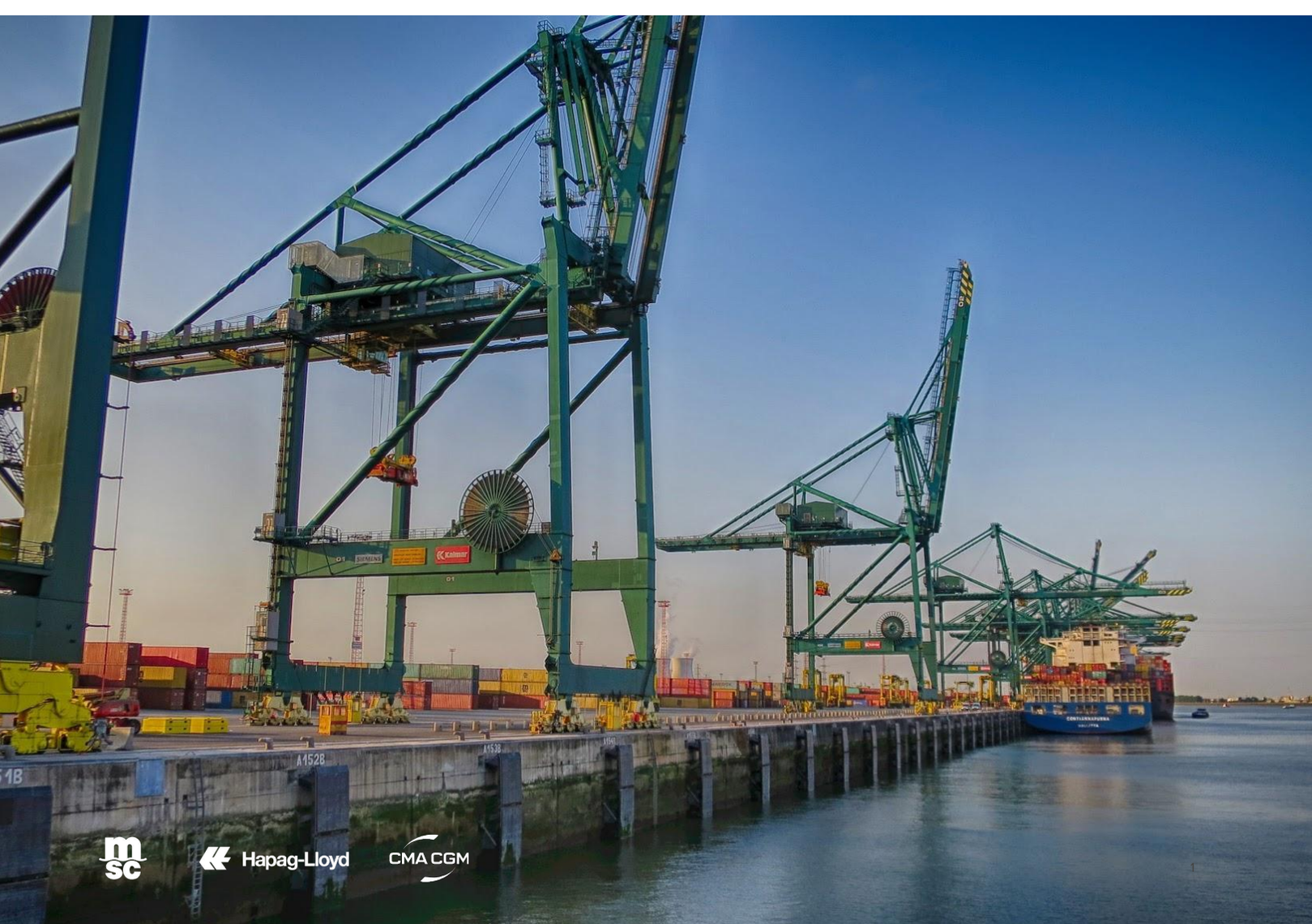
T·MINING

WHITE PAPER

Secure Container Release

Secure Container Release (SCR) is the system of choice for MSC, Hapag Lloyd, and CMA-CGM to secure the container release process, connecting thousands of logistics companies in over 25 countries.



WHITE PAPER

Secure Container Release

The electronic Delivery Order Solution

INTRODUCTION

The Evolution of Container Release

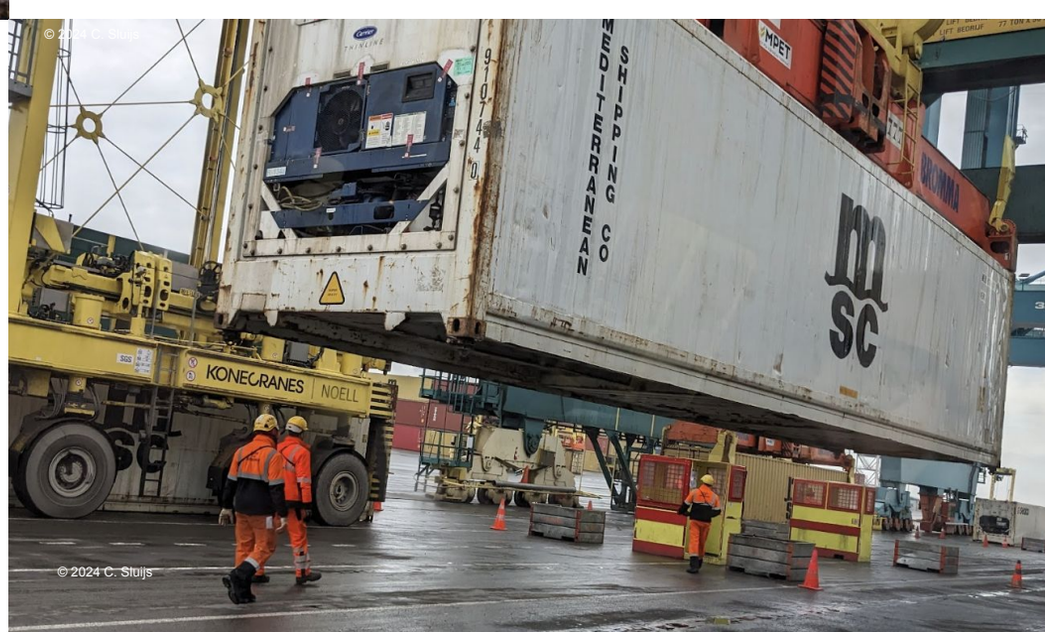
From Paper to Pin codes

Starting in the mid 1990's, the logistics industry took a significant leap towards digitization by introducing pin codes in the container release process. This move aimed to replace the traditional "Delivery Order", where paper documents granted the right to pick up containers at terminals. Pin codes, generated by ocean carriers and communicated to forwarders and transporters, were intended to streamline operations and enhance security.

The introduction of a paperless release process resulted in significant benefits: pin codes improved the efficiency of the process for all parties involved in the chain. That is why many ports worldwide adopted pin codes, sometimes called "release reference".

Over the years, the pin code-based release process demonstrated severe shortcomings. Pin code fraud became widespread, most visibly in West European ports, exposing all parties to significant risks. Risks were not just limited to the container or the cargo, but also port workers involved in the release process - having access to information systems that manage pin codes - became a new target for organized crime.

To mitigate risks and fight against international fraud, several port authorities announced initiatives to improve security in their ports. Today, many local initiatives struggle to gain adoption as they provide a port-oriented solution, failing to accommodate the need for a scalable solution to be used across different ports, supporting the needs of internationalized supply chains.



From Pin codes to Blockchain Technology

In March 2020, Secure Container Release (SCR), an application developed by the Belgian startup T-Mining was introduced in the Port of Antwerp by MSC Belgium and rolled out in production to all MSC's supply chain partners. SCR replaces pin codes with blockchain tokens (similar to NFTs) that can be transferred between the supply chain parties. With SCR, pin code-fraud can be avoided and the blockchain-based audit trail provides transparency in case something would go wrong during the release process.

Today, MSC, Hapag-Lloyd, and CMA-CGM are using SCR to secure their release process. SCR is in production in the ports of Antwerp and Rotterdam and connects over 4.000 consignees, freight forwarders, and transporters in over 25 countries.

On June 1st, 2023, MSC introduced Secure Pick up at MSC PSA European Terminal (MPET), the largest container terminal in Europe, enabling pin code-free container pick up for trucks, barge and rail. With this milestone, MSC concluded a 3-year phased rollout of SCR in the port of Antwerp, gradually fading out the use of pin codes throughout the chain.

Next to improving the security of the release process, SCR offers a digitalization solution allowing all parties to optimize and automate their release process, driving down risks and costs. With 3 of the top 5 ocean carriers connected, SCR has become a multi-carrier solution providing freight forwarders and transporters with one single interface towards multiple carriers and a harmonized release process across different ports. In addition, SCR offers ocean carriers a multi-port solution, reducing their total cost of ownership related to compliance, local port connectivity, and other local requirements.

BEFORE

Delivery Order

Paper Document

Easy Transferable

1994-2010

Pin code

Digital

Unsecure Transfer

2020

Secure Container Release

Digital & Automated

Secure Transfer

Persisting Industry Challenges

Beyond pin code fraud, the container release process presents compliance challenges, operational difficulties, and communication gaps, leading to insecurity, unsafe working conditions, unnecessary costs, and customer dissatisfaction.

Safety & Security Risks
Employees face increased safety threats due to insecure container release protocols.

Compliance Challenges
Adapting to varied and shifting compliance rules for each port.

Operational Difficulties
Complex processes cause delays and inefficiencies in container releases.

Communication Gaps
Inadequate and outdated information increases customer inquiries and dissatisfaction.

The introduction of pin codes to digitize the container release process boosted the industries efficiency but also created significant concerns.

Historically, the right to pick up a container was formalized in a document called the "Delivery Order." The transporter could pick up a container at the terminal with the paper document. The pin code was introduced to improve efficiency and security.

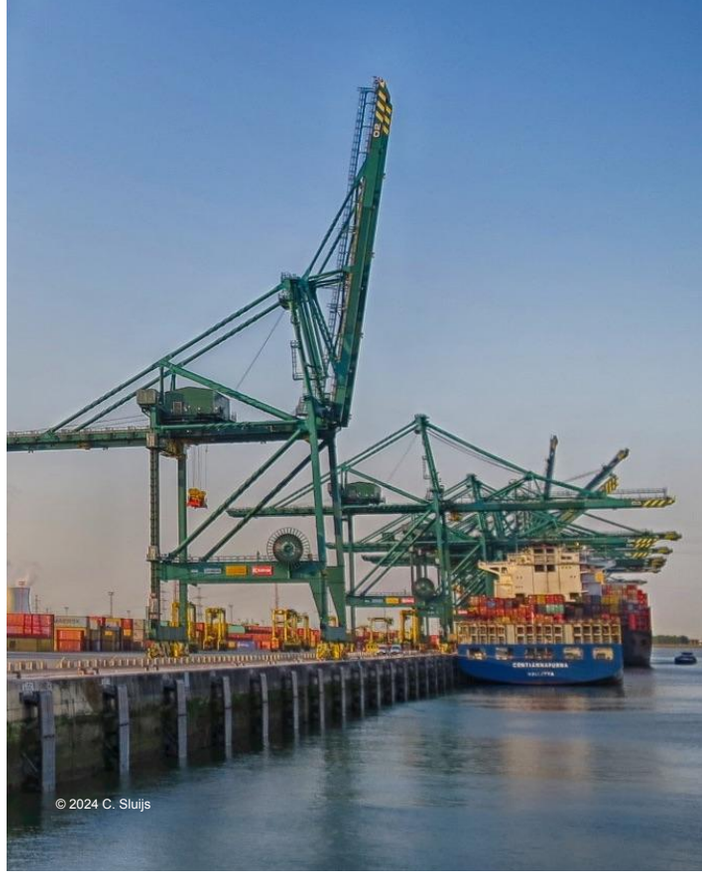
Once a container arrives at the port of destination, a pin code is required to allow the transporter to pick up a container at the container terminal. This pin code is generated by the ocean carrier and communicated to the forwarder responsible for transporting the container to the hinterland. Information such as the container number and associated pin code is forwarded to the transporter (a truck, barge, or train) responsible for picking up the container at the terminal.

These pin codes represent the right to pick up a container, the so-called "pick up right". Essential to pin codes is that they are processed confidentially and securely by the various organizations involved in this process, such as the ocean carrier, the freight forwarder, the transporter, subcontractors, the driver, and the terminal. Pin codes are often distributed via insecure channels, like email, telephone, or text message.

Pin code fraud

Since the introduction of the pin code-based release process, the industry has become aware of its drawbacks. In its annual report on the EU drug markets, Europol directly links the use of pin code with fraud, the rise of organized crime, and the import of drugs via various European ports. Also, industry leaders increasingly recognized the risks of using pin codes to secure the container release process.

Pin code fraud is therefore a known problem in the industry and a significant security risk for all employees and organizations involved. Incidents involving bribed employees illustrate the urgency of the problem and the significant risks for port organizations and their personnel.



Understanding Pin code Vulnerabilities

A pin code is easy to copy and thus not unique.
When distributed eg. via email, someone can forward the pin code to someone with bad intentions. As a recipient, you are not sure you are the only one who receiving the pin code. On the contrary, you are certain that more people have the same right. You cannot *transfer* a pin code, you can only *duplicate* it.

A pin code is hard to keep confidential.
Anyone with access to this information can pass it on to unauthorized persons. Also, information systems can be hacked. Think of identity fraud where someone simply shares his credentials (ie. username and password) to a database or application.

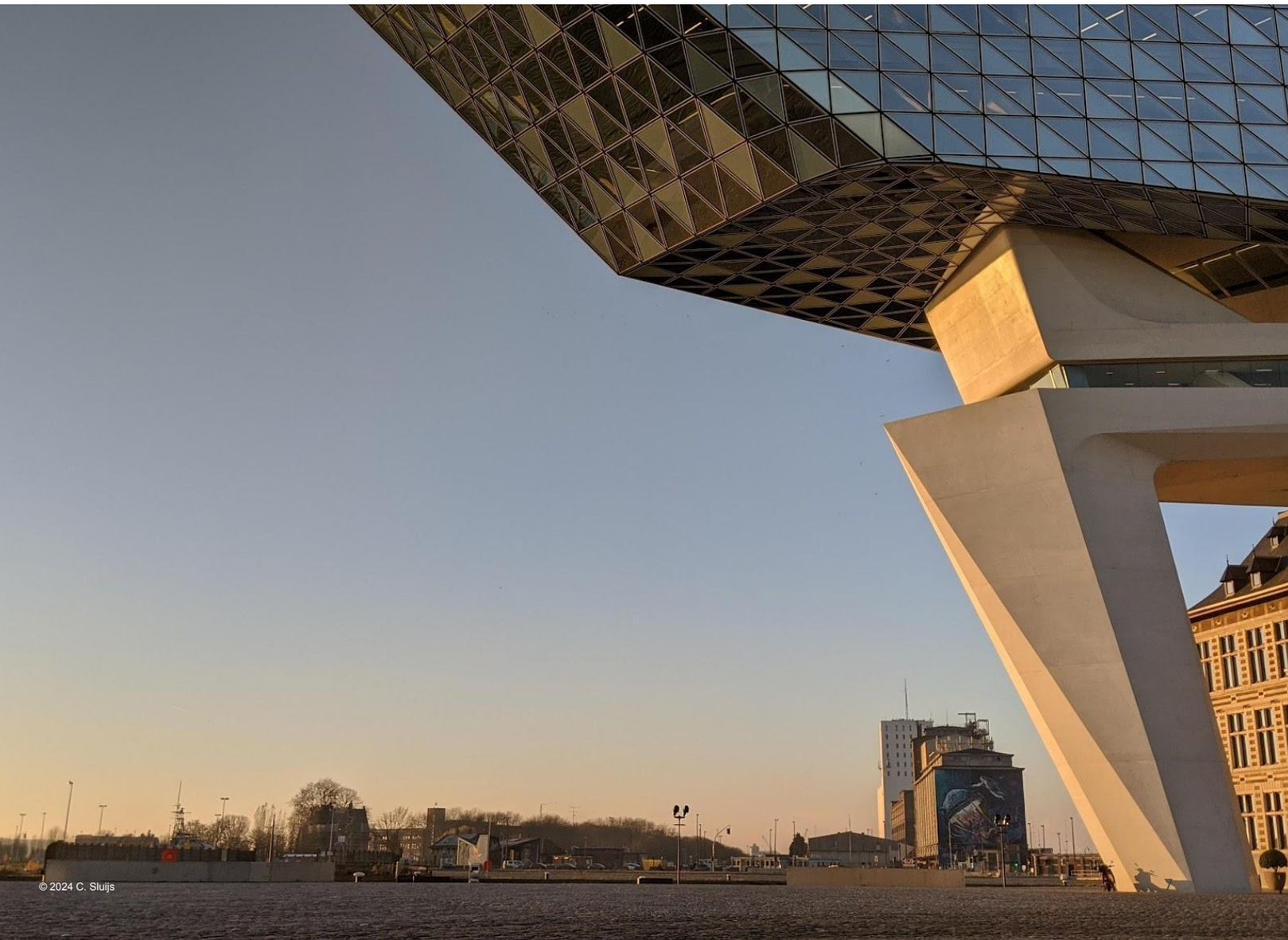
A pin code is impossible to trace.
When you receive a pin code, you cannot see whether this pin code is authentic or correct. In case of an incident, it becomes impossible to trace back and find the root cause.

DECENTRALIZED TECHNOLOGIES

How Decentralized technologies can address widespread industry shortcomings.

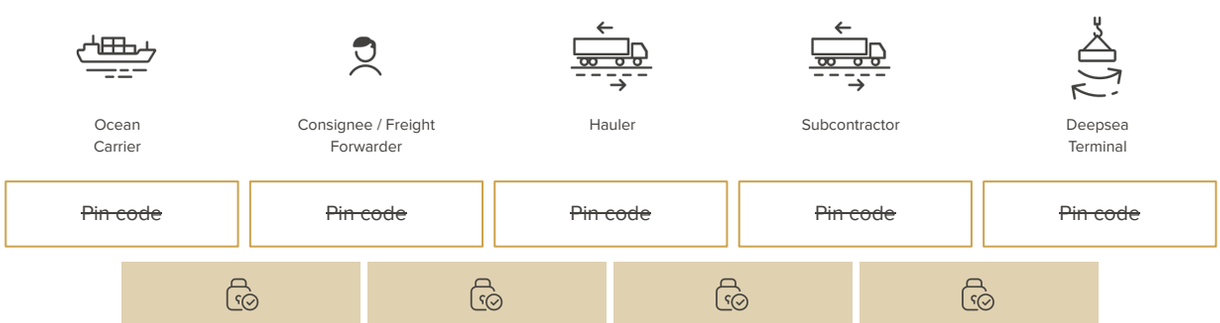
Arguments why pin codes have failed to secure the release process sound logical and are simple to understand. However, they are implicitly linked to how most information technology works today. The internet, for example, is designed to share information easily, but it can not transfer any right or value. Here is where the root cause is. Certain digital assets -eg. the right to pick up a container- are only useful if scarce. Think of money, it loses its value when more is made of it. In what follows, we will describe the different technological challenges that need to be addressed when fixing the container release process.

Unique to blockchain is that it can transfer a digital asset, called ‘a token’, from one person to another without an intermediary. The blockchain network guarantees that every token is unique and can only be transferred once. A token or coin would lose its value if it were not scare, ie. it could be spent more than once. This is referred to as the "double-spending" problem, solved by blockchain, and is a key differentiator compared to traditional, centralized databases.



Next to tokenization, blockchain facilitates immutable data storage. Information is chained together in blocks utilizing cryptographic encryption. Any change to the information breaks the cryptographic chain. The blockchain will compare the data with the data stored on other nodes in the network. In this way, it makes immutable data storage possible since "the truth" is replicated on different nodes - which implies that a blockchain network is by definition decentralized and cannot run on one computer system or server.

Returning to the container release process and pin codes, it becomes clear what added value blockchain technology offers compared to classic centralized technology. Thanks to tokenization, the traditional pin codes are replaced by tokens, which are then passed on between the different participants in the chain. Data records on who owns the token are stored in an immutable way. Now, it becomes clear that blockchain can solve the first challenge of replacing pin codes. A person can pass on a token only once. Think of a relay baton during a race. Once transferred, one no longer holds it. In other words, the right to pick up a container has become unique and traceable. After all, every participant must also identify himself on the blockchain.

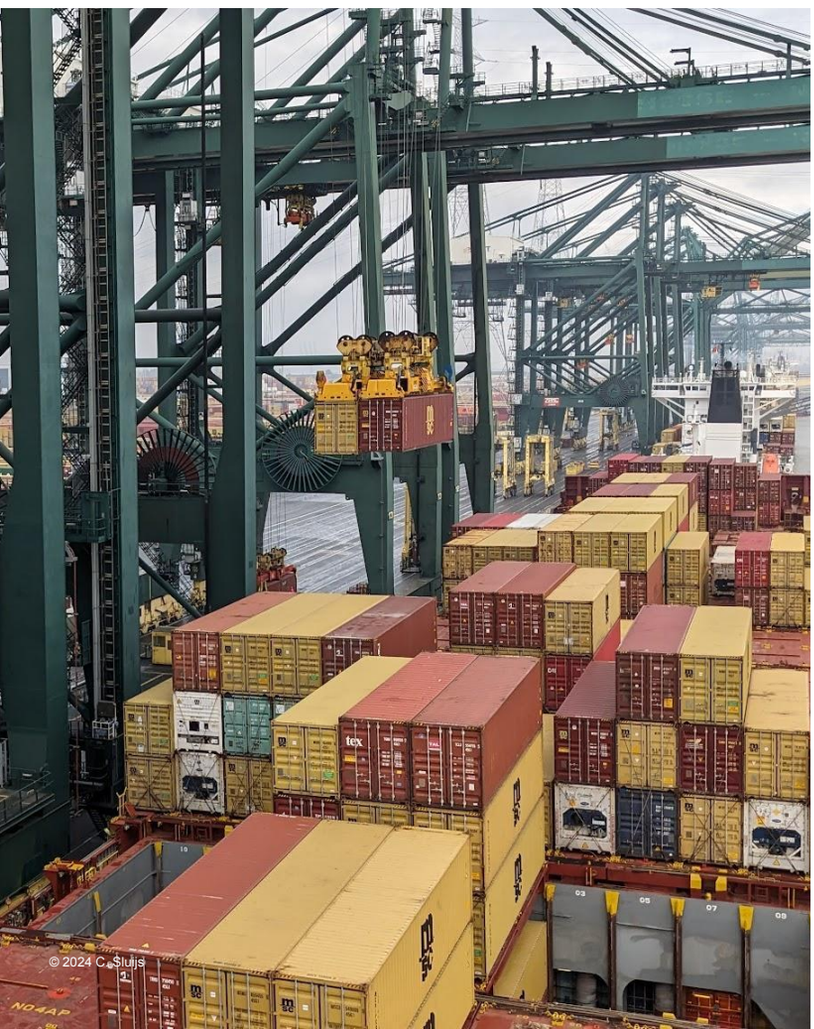


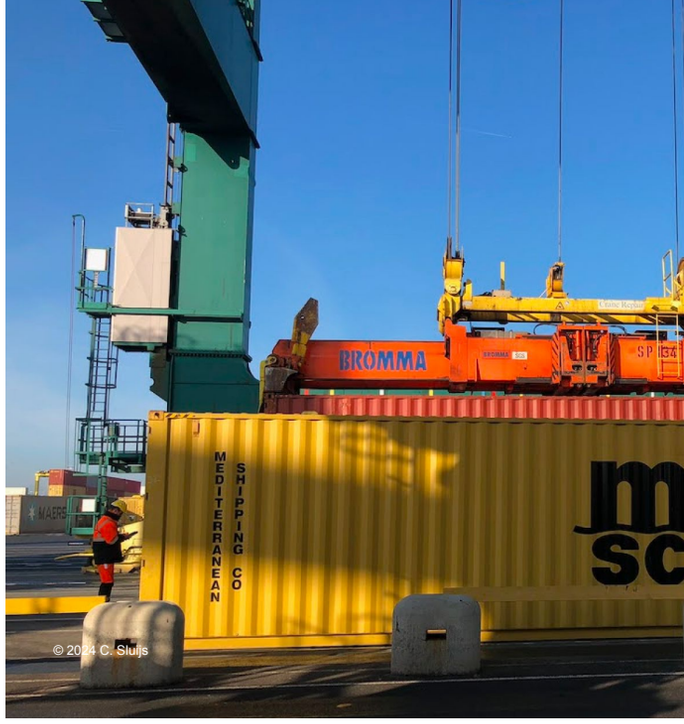
Secure Container Release uses blockchain technology

- Tokenizes the right to pick up a container
- Avoids “stolen” pin codes as pin codes can be duplicated
- Creates a digital trail between all parties involved

Safeguarding Identity with SCR

With this, the second challenge arises: identity. How can one be sure of someone's identity? Pin code fraud is not solved if an organization could participate in the blockchain network under a false identity. That way, the release 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. T-Mining developed the Identity (ID) Wallet to solve this identity issue. This software application is installed on the organization's network when it registers on the SCR application. The ID wallet contains the cryptographic keys of the organization to be used for identification on the SCR application and the underlying blockchain network. This procedure can only be validly performed from the organization’s network. That way, it can be ruled out that someone would try to log in with stolen credentials and manipulate a release right.
Of course, an unauthorized organization could also try to install an ID wallet. For this, three different identification methods were proposed.





The identification process

01 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;

02 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 release right. Without these connections, an organization cannot participate in the release process. It does not receive any information from other organizations. That way, it cannot request and decrypt information from the blockchain;

03 In case of a specialized authority is in place, the identity of this new organization can be checked, validating the identity and key information of the organization involved and confirms it to SCR.

Blockchain and privacy

The last challenge that needs to be addressed is privacy. The transparency created by blockchain technology could create considerable privacy issues when other participants would capture the information stored on the network. By tokenizing the right on blockchain and registering an organization's identity, anyone accessing 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.

Balancing Transparency and Privacy in SCR

In SCR, the ID wallet is essential in offering a proper solution to guarantee privacy. Private connections are stored in the ID wallet. This means that every organization that connects with another organization exchanges unique and, therefore, private cryptographic keys. To understand how this creates privacy: think of your telephone number. Everyone can easily recognize you, when seeing your number. In a database, a record linked to your number can be traced back to you. Now, think of private connections as a unique telephone number for each contact you have. A person that receives your unique number can recognize you. But a third party not. In a database, records could only be linked to you by a person or entity that has received your unique number from you.

Let’s take the example of Organization 'B' receiving a release right from its connection 'A', and ‘B’ transfers it to connection 'C'. Thanks to the ID wallet, it is impossible for 'A' and 'C' to discover (read: decrypt) that this container was passed on through intermediary 'B'. Even more: ‘A’ and ‘C’ will not be able to know each other. Therefore, the risk of bypassing ‘B’ is mitigated. It goes without saying that in a particularly competitive industry, where shipping companies, forwarders, and transporters work together for one container but are competitors for the other container, SCR guarantees commercial privacy.

Enabling Privacy in Peer-to-Peer Exchanges

In addition, so-called 'peer-to-peer' technology offers additional guarantees regarding privacy. Information is then not exchanged via a central platform or hub, but directly between peers. For example, organization 'A' will receive information from organization 'B' and exchange it with organization 'C', without a central party having access to it.

Classic cloud solutions, which typically centralize information, pose specific privacy and data ownership issues. Incidents with eg. Facebook illustrate 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.

Advantages of Decentralization in SCR

Another advantage of decentralization is that there is no 'single point of failure'. The lack of a central database makes it much more difficult for a hacker to steal data. After all, if there are no pin codes anymore, you can no longer steal them, not even from T-Mining.

RECOMMENDED READINGS

WHITE PAPER
Blockchain in Logistics
www.t-mining.be/white-paper/

BLOG
Why your privacy does matter: a case for Secure Container Release
www.t-mining.be/blog/

CHALLENGES SOLVED

With Secure Container Release, T-Mining introduced an electronic delivery order solution used by 3 out of the top 5 ocean carriers worldwide.

In 2016, T-Mining was founded based on the vision that innovative technology could be applied to improve the security and efficiency of the container release process. Especially, pin code-fraud was seen as a strong use-case for blockchain. With Secure Container Release, T-Mining introduces an electronic Delivery Order solution, solving the pin code-related security concerns, and at the same time introducing a new standard for the container release process across different ports and supply chain parties.

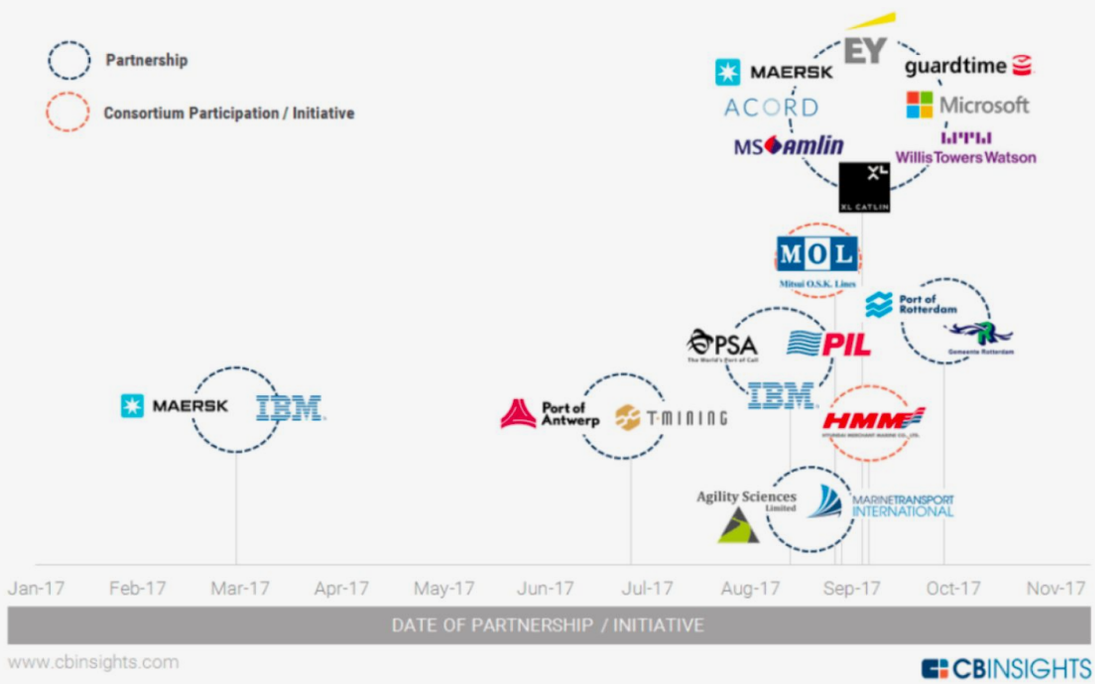
In 2017, during a Proof-of-Concept with oa. MSC and PSA, T-Mining pioneers as one of the first to apply blockchain into the maritime logistics industry.

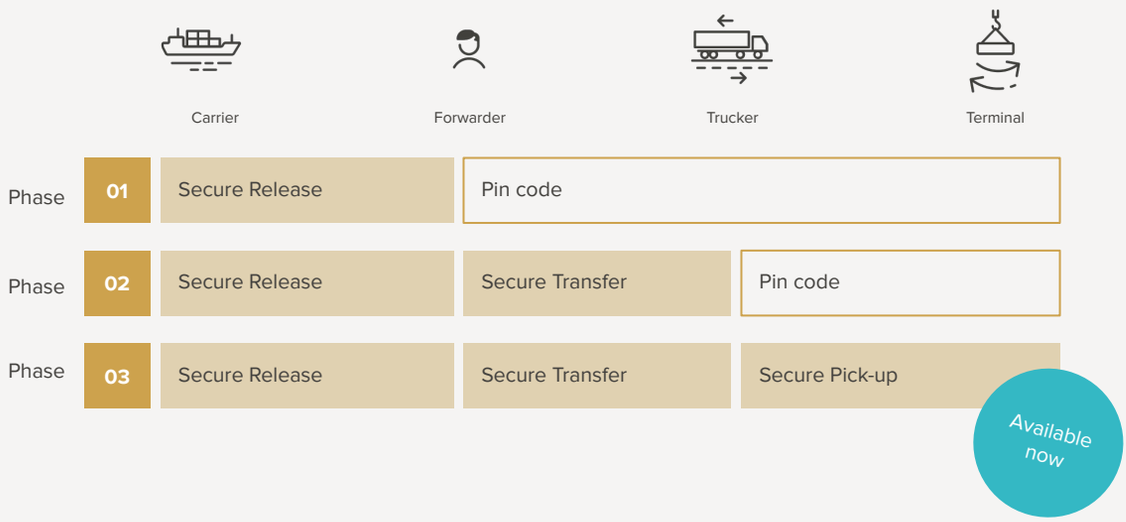
The SCR concept was tested for the first time in real-life conditions. During the entire process, a blockchain token was created, replacing the pin code, and was registered on the blockchain, together with all transactions from the different parties involved.

In 2020, MSC was the first ocean carrier to roll out SCR in production in the Port of Antwerp. Soon, Hapag-Lloyd decided to adopt SCR both in the Ports of Rotterdam and Antwerp and also CMA-CGM joined SCR in the Port of Antwerp.

In 2023, MPET was the first terminal to connect to SCR in production in the Port of Antwerp.

T-Mining pioneers as one of the first to apply blockchain into the maritime logistics industry





Phased Approach of SCR

To minimize the adoption barrier, SCR is rolled out using a phased approach, providing backward compatibility with the legacy pin code-based process. By doing so, change is introduced step by step and parties can adopt the new of working at their own pace, avoiding a big bang.

An ocean carrier implementing SCR can work pincode-free in just a few weeks, starting in phase I. A freight forwarder can receive a release from the carrier and convert it into a pin code for distribution to the transporter.

In phase II, the first release party can choose to invite the transporter to SCR and transfer the release or continue using pin codes.

Since June 1st, 2023, MSC entered phase III at the MPET terminal in the Port of Antwerp, offering a Secure Pick-up at the terminal, without pin code, for MSC containers released at MPET.

Effortless Onboarding Process

Next to a tailored product offering for ocean carriers, SCR also addressed the needs of freight forwarders and transporters. Upon invitation from a carrier or other party in the chain, an organization can create an SCR account, setup user accounts for its employees, and an ID wallet to onboard to the network in only a couple of minutes. By default, an ID wallet in the Cloud is offered, ensuring instant onboarding, avoiding any potential disruption or delay in the release process.

During a 3-month free-trial period, the newly onboarded organization can decide to install the ID wallet on their network free of charge, and use the SCR web application via the freemium SCR Basic subscription or upgrade to the SCR Premium subscription, available from €19 per month per port [(1)]. Optionally, a hosted ID wallet in the cloud is foreseen in the SCR Premium subscription to accommodate smaller companies without any IT infrastructure or larger companies that prefer not to install any third party software on their network.

[(1)] Pricing as applicable on January 1st, 2024 and subject to change.

Quick Start and Integration Options

The user-friendly web application has been developed so that new users can start using SCR without any training. The SCR way of working hardly differs from the traditional pin code-based process and introduces new functionalities, focused on improving the productivity and efficiency of the release process. Eg. the functionality to block or revoke a release can now be done by a simple click, saving significant time avoiding telephone or/and email conversations.

Companies that prefer integrating SCR with their existing software solution can automate their release process using SCR API. SCR is pre-integrated with several software solutions, like CargoWise, enabling an easy integration.

Secure Pick-up and Smart Container Release

For deepsea terminals, the SCR product offering includes Secure Pick-up, allowing a transporter to pick up a container that has been assigned.

At MPET, an integration with an ID-provider[2] for transporters facilitates a Secure Pick-up using biometric identification. At the gate, the trucker swipes its ID-pass to gain access to the terminal and pick up the container. Today, Secure Pick-up supports all transport modi, being truck, barge and rail.

Also, Smart Container Release brings additional benefits to Container Terminals, unlocking yard-handling efficiencies. Next Mode of Transport (NMoT) or Retrieve Best Unit (RBU) illustrates how SCR optimizes terminals efficiency and optimizes infrastructure capacity by reducing the number of straddle carrier moves or shortening the waiting time for transporters at the terminal.

[2] In Antwerp, the ID-provider is Alfapass. In other ports, SCR can accommodate local ID- & Access-management solutions.

GROWTH & IMPACT

Secure Container Release lowers costs and drives efficiency.

Secure Container Release grows into a multi-carrier and multi port solution, offering one single interface across different carriers and ports, harmonizing the container release process, lowering operational costs and driving efficiencies

With 3 of the top 5 ocean carriers connected, SCR offers a multi-carrier solution. In the Ports of Antwerp and Rotterdam, the ecosystem benefits from one single interface for receiving releases from the 3 ocean carriers connected, triggering companies to automate their release process using the SCR API given the positive business case. Via the web application, SCR offers new features and additional information compared to the traditional pin code-based process.

User Validated Solution

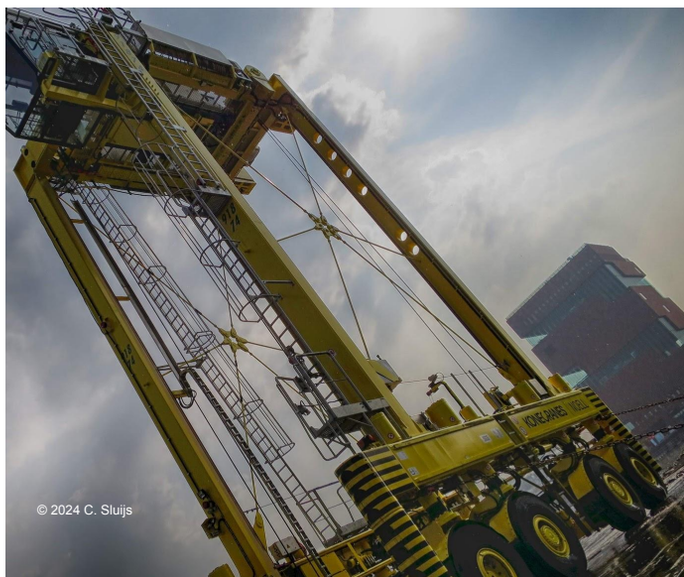
User adoption and qualitative customer interviews amongst SCR users provide clear evidence for significant productivity and efficiency gains provided by the application. User feedback suggests a clear positive stance towards the enhanced security provided by SCR, the self explaining user interface, the increasing visibility on the container status, improved claims handling, fewer manual errors, and the responsive SCR support team ensuring a superior customer experience.

As a multi-port solution, SCR provides a harmonized way of working, allowing local and international participants to benefit from one single interface in different ports, providing economies of scale. More than 1 out of 2 organizations active on SCR operate in more than one port. Also, international participants generate a substantial part of release volumes in one port. Both observations underline the need for a multi-port approach.

Anticipating the high number of incidents related to fraud and organized crime, Port Authorities increasingly announce local initiatives to secure port operations, especially focusing on the container release process. In the Port of Antwerp, NxtPort introduced Certified Pick up early 2024. In the Port of Rotterdam, Portbase is piloting a similar solution. Also other ports have announced proof-of-concepts. However, these initiatives focus on the local release process in one single port, resulting in fragmented solutions, driving complexity and failing to deliver a scalable solution. In addition, Port Community System (PCS) platforms tend to build closed solutions, lagging in technology and IT, and are known to be slow in execution.

For supply chain organizations, the Total Cost of Ownership (TCO) of their container release process is negatively impacted by hidden costs driven by complexity coming from local solutions. Think of lengthy consultation-, negotiation-, and piloting efforts required by local solutions, claiming scarce resources from management, operations, business analysis, and IT.

To accommodate for this increased complexity of local port connectivity and unburdening participants from local compliance, SCR developed the SCR Authority API, providing a direct interface between SCR and the local PCS platform, acting as a shared integration layer amongst participants of the SCR network, lowering costs and pooling investments.

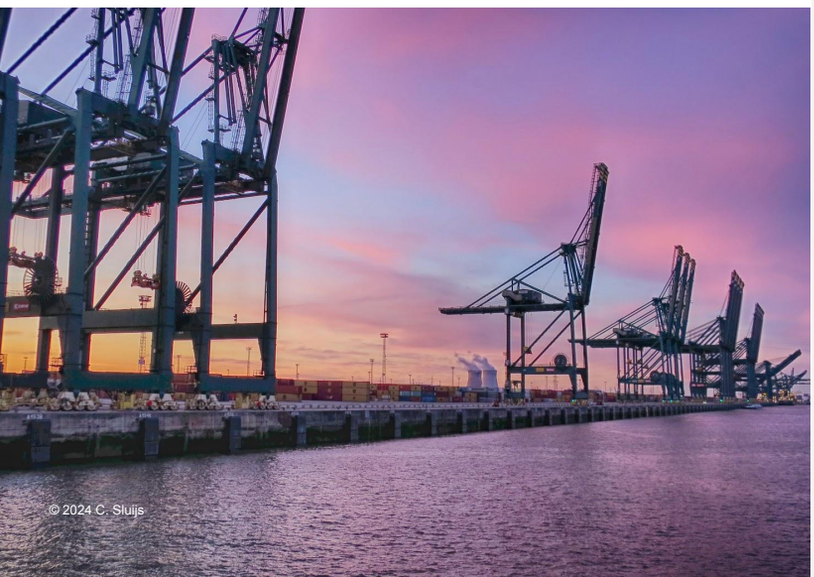


GROWTH & IMPACT

Driving Value for Stakeholders in Container Logistics

What if SCR could offer a solution that enhances safety and security, ensures compliance, and paves the way for a future-ready container release process?

T-Mining's SCR solution extends its value far beyond enhancing safety and security measures.
By leveraging innovative blockchain technology, T-Mining not only addresses the immediate concerns of fraud and theft in container releases but also pioneers in digitization, operational excellence, and enriches customer experience. The solution's transparency and traceability improve efficiency and reliability in the logistics chain.



Safety and Security

We help your team stay safe and ensure you data is secure.

—

01 Employee Wellbeing and Safety

02 Efficient Audit Trails

Digital Innovation

Our solutions continuously evolve, helping you stay at the forefront

—

01 Scalable Solution

02 Accelerated Digitalization

03 Future Proofing

Customer Experience

We keep you and your customers well-informed and supported

—

01 User-friendly Interface

02 Enabling Self-Service

03 Support Team

Operational Excellence

We ensure minimal disruptions and compliance for smoother operations

—

01 Phased Rollouts

02 Compliance and Standards

T·MINING

Secure Container Release is being developed by T-Mining, an Antwerp-based start-up committed to innovation in the maritime logistics sector. Utilizing decentralized technologies like blockchain, T-Mining enhances security, efficiency, innovation, and customer experience. At the core of its philosophy lies a profound respect for privacy and data ownership, reflecting T-Mining's dedication to ethical technology practices. With this approach, T-Mining is set to advance security and efficiency within the industry, demonstrating a commitment to continuous improvement, one solution at a time.

T-Mining NV | Sint Pietersvliet 7 | 2000 Antwerp | Belgium | BE 0667.928.835
www.securecontainerrelease.com
www.t-mining.be