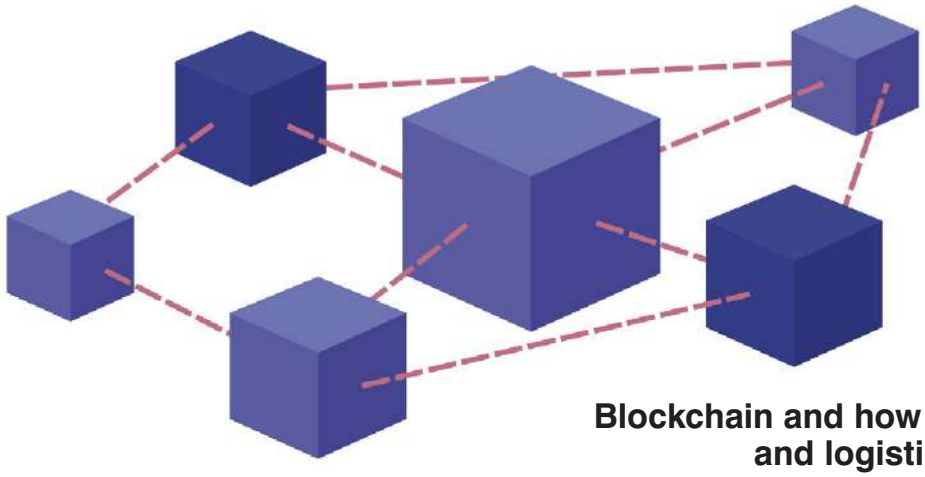

**Blockchain and how it can make transport and logistics more cyber secure**

# The trust factor and human error in supply chain security

by **Marcin Lewicki**, *CEO & Founder, Sternkraft*

**The global supply chain network is a system of self-existing individuals connected to each other in an undefined way. Information goes from one organization to another according to rules that aren't specified globally. In most of the cases, two cooperating organizations have their individual methods of exchanging information – analogue, like paper invoices or certificates, or digital such as the state and the position of the transported cargo. Sometimes organizations agree to use the same processes, procedures, and tools to exchange data. This, however, doesn't mean they all have the same internal rules. These companies store our data, so it's crucial for us to know if our partner has put in place the proper internal rules and processes thanks to which the data infrastructure is safe. The question arises: can we take the human factor out of the 'trust equation'?**

**STERNKRAFT**
TELEMATICS

The business of transport and logistics suffers from growing numbers of threats like cargo and fuel theft or burglary. This has led the Berlin-headquartered Sternkraft to develop Safeway, an advanced cargo security system that combines hardware with the latest technology. For more info, please click www.sternkraft.com/en

We all know that one thing is to gain a certificate, but actually sticking to the rules is another pair of shoes altogether. The latter is undermined by factors such as trust and human error. Is working with Maersk a safe option? It should be. Why? Because the Light Blue means something in the industry. I know I can trust them.

**One hard drive to save them all**

Yet, I'd be very surprised back on 27 June 2017. Such a respectful and well-certificated corporation, with a lot of great minds on-board, was hacked by a piece of malware that wasn't even targeted at Maersk in the first place! The fallout was nothing short of epic – no more no less, but the giant went analogue for two whole weeks. Conclusion? One cannot simply take trust on, well, trust.

It's hard to say what was Maersk's main shortcoming back two years ago. Surely they weren't prepared for what happened. What we know now, though, is that the whole company was using systems that weren't upgraded with the latest patches while passwords were of really low complexity. End result? One small NonPetya malware destroyed the entire infrastructure. Like in an action movie, Maersk survived because they were able to retrieve the single last copy of their system that wasn't hijacked – in Ghana. For comparison, all – all! – of their 150 domain controller backups were down. At that time, it was the most important hard drive disc for the entire container shipping industry. Mission – get to Ghana and bring that HDD to England. One existing backup server rescued the whole 45,000 computers and 4,000 servers-big company.

Photo: Sternkraft

So, even if I had trusted Maersk – the incident would affect me. Making simple Windows updates and having to go through two-factor authentication on each and every computer – this would have saved Maersk $300m that summer. But it isn't that the Danish conglomerate is the only whipping boy; other heavyweight players also lost millions because of the NotPetya attack. Merck admitted to their shareholders they lost $870m because of shutting down the ability to manufacture drugs. The French Saint-Gobain, which delivers construction and high-performance materials, saw $400m going down the pipe; FedEx – $400m; Mondelēz, the manufacturer of i.a. Cadbury chocolates – $188m; Reckitt Benckiser, the British producer of Durex condoms – $129m; and so on and so forth.

**One, big, decentralized, yet shared by everyone shipment registry**

What if we could grasp human trust with a mathematical formula? Imagine a situation where you know exactly where your shipment is; what is the temperature inside the container; whether somebody has tampered with the seals; opened the doors; or even stolen the entire unit. Carriers, suppliers, intermediaries, insurers, regulators are involved in the supply chain, meaning there's plenty of room where communication, data transparency, and safety can be compromised.

SAP, Oracle, Salesforce – they all work on cloud-based solutions to improve freight and order management, transportation planning, costs, reporting, and analytics. What if we could use one big database to identify and track each cargo globally? What if we could allow access to this database to everyone and, while using it according to the rules, change the registry of each transport in time? What if we create one, big registry of shipments, totally inaccessible for unauthorised parties?

The so-called Distributed Ledger Technology (DLT) – better known as blockchain – provides such a global format. It's interoperable, immutable, and secure. It's a data standard that's accessible by authorized parties and cannot be changed. Each transport's ledger is shared by many, delivering a decentralized database that's synchronized by each member. Blockchain cryptography and smart contracts make rules visible to everyone and used by everyone, but data are only accessed by those who own a "password." Such a database and interface layer allows connecting any end-user application to it. Decentralization, which stands for immutability and having a synchronization backup strategy, helps to secure the data. The role model to follow is Samsung SDS, a member of the Transported Asset Protection Association, and its ongoing project with the Port of Rotterdam and ABN Amro Bank. "Our blockchain based project is the answer to the cyber security of our times. It will secure and improve freight processes like nothing before," says Jacques De Smit, Regional Logistics Director, Samsung SDS.

**Secure the future**

In Sternkraft's Internet of Things project called Safeway, a test DLT solution, is being implemented. Safeway is a solution that combines hard- and software and allows monitoring goods in both curtainsider and semi-trailers, and doing it in- and externally. All algorithms implemented in our cameras help to prevent thefts. The alarm is activated whenever something strange is happening, e.g., someone is next to the cargo and behaves suspiciously, or the temperature inside the unit changes rapidly. BinarApps creates a management system for logistics to monitor transport and generate an alert if any unwanted situation occurs. Each transport ID number with its attached documentation will be stored in a partially public DLT database. Each of the Safeway's users will be the owner of at least one copy of the database node. Nodes are synchronised and, thanks to cryptography, 100% valid. This way they'll participate in creating a decentralized copy of what could be called the data centre's heart.

Maersk is probably well-secured by now. The management board took up the challenge and started to treat cyber security seriously. Meanwhile, blue chip companies need to take on the responsibility to not only secure the present, but also the future. There's a way of feeling more cyber comfortable, as long as it's called blockchain. ■