

THE Logistics Journal

A Publication of the Transportation Intermediaries Association

July 2017

How to Bring Blockchain to Domestic Freight

By Lance Healy, Banyan Technology

In today's technology driven age, it is hard to track the constant flow of new innovations. If you are in charge of your company's shipping operations or deal in any way with the supply chain process, your primary focus is that shipments arrive safely, on time, and on budget. To achieve these goals it is important to be on the lookout for the latest technology that will improve your operations and open a competitive advantage to your organization.

Blockchain is among the newer technologies to hit the logistics space, and it helps companies reliably trace any shipment from start to finish. One Walmart

executive has already referred to it as "the holy grail" of shipping technology.

Rather than geek out on the technology, the focus should be how it can serve the industry. As a relatively new technology to the industry, blockchain is already making significant waves for some of the world's largest companies. If blockchain really is the holy grail of shipment tracing, it is worth diving a little deeper to see what the technology does and how its functionalities can be applied to domestic shipping.

What is Blockchain?

The term blockchain may make it sound like a medieval prison system, but the technology could not be more liberating. Blockchain strings together pieces of information that are related to one shipment's progress and cannot be controlled by any single company that has access to the information. This results in complete accountability and visibility for any shipment or transaction.

Ian Khan, a keynote technology speaker, lays it out simply by saying, "Blockchain truly is a mechanism to bring everyone to the highest degree of accountability. No more missed transactions, human or machine errors, or even an exchange that was not done with the consent of the parties involved." Because the blockchain technology is constantly monitoring the string of information, there is no chance for any one person to jump in and mess with the data unnoticed.

Continued on page 3

Inside

Sales & Marketing in the Transportation Industry: How Do You Compare?	7
Keeping Cool with FSMA Requirements	12
The Power of Data	15
Measuring your Total Cost of Visibility for 3PLs and Brokers	16
Cargo Claims Exposures for Smaller 3PLs: Stuck Between a Rock (Your Customer) and a Hard Place (Your Carrier)	18
Transcore Freight Payment Index	19
Three Ways to Grow from Transactional to Transformational	20
There's an App for That? Hot Data-Sharing Technology in the Transportation and Logistics Sector	23
What's In Your Risk Management Toolbox?	26
Buyers Begin Their Hunt on LinkedIn	27
DAT North American Freight Index	29



In addition to a super user, find a lead, perhaps in a general manager role, who can oversee the new offering. MTS projects are partner projects, so they require a project lead and a plan, then ongoing resources to execute.

Service, service, service

MTS is as much of a service-based business as it is a technology business. This means you need more of a partnering mentality than what a transactional sales process requires. The focus should not only be on cost, but on performance and service. And your customers are expecting that too: an Inbound Logistics survey found that 78 percent of respondents rated service as

more important than cost, and 39 percent said poor customer service was the reason 3PL partnerships fail.

MTS takes a different style of thinking and a different approach, but it's not magic. Your customers have limited transportation skillsets and are looking to you to provide simplicity; they want a one-stop shop. 3PLs with an eye to the future understand that expanding with MTS and leveraging existing customer relationships can provide transformational value and growth to both their own organization and their customers.

The author, J.P. Wiggins, is vice president of logistics at 3Gtms. He may be reached at (203) 567-4610 or jpwiggins@3gtms.com.

There's an App for That? Hot Data-Sharing Technology in the Transportation and Logistics Sector

By Stephanie S. Penninger, Benesch, Friedlander, Coplan, & Aronoff, LLP

The availability of app and web-based technology is spreading and becoming a "must have" and "go to" for transportation companies in their efforts to stay relevant and compete within their industry. Many shippers now require motor carriers to offer sometimes costly app-based technology services to their drivers, and brokers and shippers are prevalently tracking shipments using GPS. Tinder is not the only matchmaking going on. Shippers and brokers are hooking up with motor carriers to haul their customers' cargo through apps or on websites.

Nonetheless, users of newer transportation and logistics technology should bear in mind that the benefits of technology use are not without significant risk, and steps must be taken to mitigate against new exposures.

What is it and what are the benefits?

Vendors now offer users and providers of transportation services GPS-driven crowdsourcing technology products that capture real-time information to map and relay exchanges of information between service users and providers.

For example, uShip matches shippers wanting freight to be transported with carriers to haul the loads

while the Ubers of cargo transportation, GlobalTranz and Fleet, help shippers find freight brokers to arrange transportation of domestic and international shipments, respectively. Trucker Path, meanwhile, enables drivers to map routes, locate loads ready to be hauled, find parking, fuel stops and weigh stations, manage loads, view metrics, etc. If you have sea legs, ships can be chartered through the use of the GetMyBoat app. Maersk and Alibaba are reported to have partnered up to enable shippers to track ocean-going shipments. Additionally, Walmart has been experimenting with the use of blockchain technology to bring traceability and transparency into its food supply network and better ensure food safety during transport.

New data-sharing technology can also be used for driver and crew onboarding services, temperature monitoring, measuring productivity, and to improve operations and reduce costs generally.

What kind of information do apps and online platforms collect or generate?

These new online and app-based technology platforms work by sharing information that is oftentimes sensitive. Information collected and shared by apps and online platforms include:

- User names or personal identifying information
- Financial information

- Date and time the vessel, truck, cargo container, or other transportation equipment is in operation or use
- Location of vessel, truck, container or other transportation equipment (as determined by satellite or terrestrial sources)
- Engine hours
- Distance travelled, truck routing, or vessel sailing schedules (including terminal or port arrivals and departures)
- Speed of the carrier

What are the risks?

Sometimes too much information can be harmful, particularly when a transportation company may be imputed with having knowledge of all of the data in its possession or made “available” to it, including data that is used for regulatory compliance.

For instance, if a shipper were to engage and require a freight broker to use an app that collects driver information, including hours of service, and it became apparent through the app that the driver was making a delivery for a particular shipper in violation of the driver’s hours of service, the shipper or broker could potentially be imputed with that knowledge. This would be even more detrimental if the driver were to, because of fatigue, cause a truck accident. Arguably, a broker having accessed this abundance of driving information (and perhaps, thereby, being too connected with the driver through the app) could be viewed as having exercised too much control over the driver’s actions, such that the broker could be held responsible for the driver’s actions as if the broker were the driver’s actual employer under a vicarious liability theory.

Further, as with Electronic Logging Devices (ELDs), drivers may be concerned about privacy and harassment issues associated with app use since some of their personal information is collected through the use of trucking apps. Similarly, carriers may be concerned about their proprietary information being disclosed to their competitors through service providers’ sharing of information with third parties or because of cybersecurity attacks. Email messages oftentimes trick users into downloading malware, allowing criminals to access computer systems to read files, obtain personal and financial information, and send messages from email accounts.

Many data sharing technology service providers have terms of service and/or “privacy” policies, to which one agrees by using the app or the services. These terms and conditions and policies typically provide that the service provider cannot guarantee the

security of any data disclosed online or through use of the app. Further, these policies shield the service providers from any liability for security breaches unless the breach is caused by the service provider’s negligence. The service provider’s terms may also permit the service provider to share user data with third parties or require disputes arising out of the use of the app to be resolved in foreign countries through the application of foreign law.

In the open seas, GPS tracking of containers on containerships has reportedly led to higher incidences of cargo theft and cyberattacks interfering with vessel operations. In the event of a cyberattack, Automatic Identification Systems (AISs), Global Navigation Satellite Systems (GNSSs), Electronic Navigational Charts (ENCs), and Electronic Chart Display and Information Systems (ECDISs) charts could disappear from bridge screens or be modified. A compromised AIS, for example, might prevent a ship from providing movement information, create phantom vessels, make it appear to other AIS users that a vessel was in a false location, or make structures disappear. Similarly, a compromised

In the open seas, GPS tracking of containers on containerships has reportedly led to higher incidences of cargo theft and cyberattacks interfering with vessel operations.

GPS signal could change a ship’s direction and provide false interpretations of course parameters to the ship’s navigation systems. This could all result in dastardly collisions or allisions and colossal liability exposure for the vessel owners and operators.

Who owns it?

Who owns the data being shared through online app-based and other platforms is typically dictated by the contracts or service provider’s terms and conditions governing the service provider’s and service user’s relationship.

Without a written contract, you could be subjected to the service provider’s one-sided terms and conditions, which oftentimes grant the service provider a

nonexclusive, royalty-free, sub-leaseable and transferable license to use your data. This use is typically without any obligation on the service provider's part, and provides the service provider with full license to use, reproduce, distribute, publish, display, perform, transmit, stream, broadcast, modify and otherwise utilize your data and any modifications and derivatives thereof.

Of course, without negotiating otherwise, a license to use the service provider's app or online platform is generally much more limited—only for internal business purposes, and the user agrees to indemnify the service provider for any claims that arise from breaching the service provider's terms and conditions and "applicable law."

Limiting Exposure

Before using the new technology, confer with professionals. To limit exposure when entering into relationships with app and other online-based data-sharing platform service providers, it is imperative that you ensure that your contract sufficiently protects the ownership of and sharing of a driver's personal information and company proprietary information, and that you push back on service provider terms and conditions that do not.

Further, information technology personnel can help you minimize the risk of a cybersecurity attack by making sure that you keep a good up-to-date anti-virus on all computers. You will also want to be sure to change operational-systems passwords often, and be aware of and limit access to and the use of computer systems. Be sure that "sensitive data" is stored only on hard drives and not on the network whenever possible, block websites that are known common malware points of entry, use a secure web portal for online transactions requiring the use of log-in credentials, limit use of bill pay, online banking, and similar activities, particularly when on board vessels. It is also important to inform crew members and truck drivers about the prudent use of social media so that personal identifying and corporate proprietary information is not shared to third parties.

It is also advisable to establish a privacy and data security governance program, assigning roles and responsibilities to corporate personnel, and developing a training program identifying security data breach risks and measures for protecting against those risks. Information retention and destruction policies should be included in the program. Obtain buy-in from the top down within your company. Determine who will need to know about any data breach that occurs and how you will notify those entities and individuals, both in-

ternally and externally. The privacy and data security governance program should be flexible and updated periodically. It should also be audited to determine where any gaps exist so that they can be fixed.

In some sense, the use of apps and online portals for sharing data and information puts freight brokers at greater arm's length from the contract carriers' drivers—where they need to be (you do not want to contact drivers directly to determine shipment status, location, etc.). However, arranging for communications between brokers and motor carriers' dispatch personnel through app-based and similar technology, in lieu of drivers, is preferable.

The privacy and data security governance program should be flexible and updated periodically. It should also be audited to determine where any gaps exist so that they can be fixed.

When using GPS technology, shippers and brokers should not hold out or represent, in applicable agreements, on their websites or otherwise, that they are providing or will provide "control" or a tracking device. Instead, indicate that the carrier may provide a vehicle equipped with the device and the recorded tracking information or that you have the ability to track or monitor shipments (i.e., the cargo itself and not the driver or vehicle) through the carrier's transportation of the shipment. Indicate in the shipper/carrier and broker/carrier agreements that the carrier will use and install a tracking device and relay shipment-monitoring information to you as the broker or shipper. The carrier should be left to determine the details as to how it will track shipments and relay the recorded information to the broker or shipper.

The author, Stephanie S. Penninger, is an Attorney with Benesch, Friedlander, Coplan, & Aronoff LLP's Transportation & Logistics Group. She may be reached at (312) 212-4981 or spenninger@beneschlaw.com