A new digital tool for making supply chains reliable: Blockchains

Matthieu Hug,
serial entrepreneur, cofounder and CEO of Tilkal

In J.P. Dardayrol, editor of the special issue *Blockchains and smart contracts: The technology of trust?* of *Réalités industrielles*, 2017

Abstract:
Distributed ledger technology — blockchains — holds the promise of reinventing the conditions for trust through decentralized notary systems without go-betweens. Applying them to the financial industry, the subject of many studies and comments, could modify systems of transactions based on trusted third parties. Other applications do not simply replace existing arrangements but even try to establish confidence where it is wanting. An interesting application in the field of health is the tracking of drugs from manufacturer to consumer. Consumers can thus obtain the accountability they demand about the products they consume; and they will be able to judge whether products comply with health or ethical criteria. In other fields, blockchain applications will help fight against the incredible proliferation of all kinds of counterfeit products in all industries: drugs, automobile parts, baby food…

In recent years, various sorts of unlawful trade (counterfeits, "gray markets") have become the top-ranking form of global criminality with "sales" of about $1,000 billion (more than the narcotics trade).[1] What in Europe is imagined to be restricted to luxury goods affects all industries: medication, automobile spare parts, baby milk, bags of Parmesan cheese, mobile telephones, batteries, toys, wine and oysters. Counterfeit medication alone kills more than 700,000 people per year in the world whereas AIDS, by comparison, felled 1.1 million in 2015. The tracking and tracing of products and goods are now a global issue in public health and security.[2]

Although risks are, for the time being, relatively contained in western Europe, the situation is awesome elsewhere on the planet. INAPI, an Algerian organization for protecting trade and brand names, estimates that 80% of products sold in the country are fake. According to Lilly, a pharmaceutical laboratory, 90% of the medication sold on line is illicit.[3] The situation is worsening fast. Worldwide, counterfeiting and unlawful markets have grown tenfold over the past ten years. Several factors account for this:

- The upsurge of e-commerce (in particular marketplace platforms) has made it easier to sell falsified or misappropriated products. It has, in turn, strongly stimulated demand.
- Stronger demand on line has induced the spread of illicit supply chains at the global scale, covering raw materials, wholesale, shipping and logistics.

---

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France).

[2] See:
— KPMG & AGMA, *Gray Markets Report*, 2016, & http://fightthefakes.org.
— Europol & OHIM (Office for Harmonization in the Internal Market), *2015 Situation report on counterfeiting in the European Union*, 70p. April 2015. Available at https://euipo.europa.eu/ohimportal/documents/11370/80606/2015+Situation+Report+on+Counterfeiting+in+the+EU
— OECD/EUIPO, *Trade in counterfeit and pirated goods: Mapping the economic impact*, 137p. (Paris: OECD Publishing), 18 April 2016. Available via: http://dx.doi.org/10.1787/9789264252653-en
— UNODC, "Focus on the illicit trafficking of counterfeit goods and transnational organized crime", 10p., 2014. Available at: http://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_EN_HIRES.pdf

[3] Eli Lilly & Co, *Integrated Report 2015*, Part Operating Responsibly.

- These illicit supply chains are massively interconnected with legitimate supply chains, with which they exchange, mix and replace products at all levels and in all phases.
- The forces involved in unlawful trade have (given its size: €1000 billion) more financial means for organizing their supply chains than any single manufacturer has for stopping them. When, in 2013, 28 pharmaceutical laboratories launched with Interpol a three-year program for countering this trade, they put up $5.9 million, a figure to be compared with seizures of fake medication ($81 million in 2015) and with this global market (probably $150-$200 billion).

The growing demand for transparency from consumers at the end of the chain is, therefore, well justified.

A continuous information chain

Since digital technology is being used to distribute products via illicit supply chains, the question arises of how to make legitimate supply chains more reliable. True, methods for physically marking and tracking products have developed and are being more frequently used. Whereas supply chains have become global, the information from these methods is still kept by stakeholders all along the supply chain. There is practically no consolidated, reliable information about a given product's life-cycle: its localization at a given moment, shipping conditions, place of sale or eventual repackaging.

These gaps in the chain of information work to the advantage of unlawful trade activities. By making up for these blind spots, two major advances can hopefully be made:

- the digital identification of a product (formed by consolidated information about it over its life cycle). Independent and different from track tags, this identification would lay the conditions for effective product authentication procedures.
- a statistical analysis, using specialized algorithms, of the product's life-cycle for detecting anomalies. The latter might be evidence of unlawful trade or might suggest improvements for the operation of the supply chain.

Using a unique identification tagged on the product, actions involving the product will be declared at each stage in the supply chain, from production to end use (*e.g.*, the product's provenance, origin, manufacturing or storage conditions, transportation in a container, etc.) At the end of the supply chain, this chain of digital information will be read by consumers (their smartphones detecting the product's unique tag, *e.g.*, a QR code). This reading will also be an event to be entered in the product's digital record. We have here a simple, single procedure for tracking in real time unknown products, abnormal packaging or sales in unauthorized geographical areas.

Setting up such a platform raises obvious technical questions about the volumetrics of the information and ease of access, but they can be solved. Moreover, it raises complicated questions about confidence in the broad sense of the word. First of all, each party intervening in the supply chain has to share information about its actions, whence obvious questions concerning confidentiality and transparency. Secondly, centralized information risks, given the stakes, becoming a "honeycomb" that attracts hackers and cyberattacks. It will, therefore, be necessary to consolidate information without centralizing it, to share all information while protecting confidentiality. Finally, questions crop up about the reliability of the collected data.

Why blockchains?

The issues related to confidentiality and a decentralized consolidation of information naturally lead to taking distributed ledger technology (DLT) under consideration. But Is it recommended to use a blockchain for supply chains? And if so, how to use it?

From an operational viewpoint, a blockchain can be seen as a distributed database that chronologically records transactions and forbids modifying them. A block of transactions is formed with reference to the block preceding it, and then submitted for validation via a consensus system comprising (all or some) participants in the network. Once a block has been validated, it is very hard to modify it or the transactions on it. Such a modification would entail modifying all later blocks and, at the same time, tricking the network's consensus system.

From a technical viewpoint, blockchain technology can be seen as a protocol for synchronizing data that operates directly on the lowest level of software in the network. This setup is less exposed to an attack than protocols at a higher level.

From these two viewpoints, several (sometimes interdependent) variations can be observed with regard to the consensus system (whether all network members can participate or only a predefined set of members), the access (public or private) to data, the data (whether encrypted or not), etc. The configuration chosen depends on the problem to be handled. In all cases, blockchains are a technological component that provides a precise service, namely the establishment of consensual confidence. This service has two pillars: transactions on a blockchain can be neither canceled (data serve as "proof") nor altered (at least not at a reasonable cost). The crucial question is: for what exact information is consensual confidence to be established?

Implementation on a supply chain

For supply chains, a private distributed registry can serve two purposes: to organize a network for collecting information, and to use this information (later) to prove the origin and content of each piece of information constituting the product's digital identification. This registry will be shared among all individually identified nodes in the network. These nodes correspond to the stakeholders who intervene in the supply chain, typically: suppliers, manufacturers, haulers, distributors or even public institutions. So, this must be a blockchain with "permissions", with a consensus algorithm simpler than the one on an open blockchain. This will improve the performance in comparison open blockchains.

Information from each stakeholder on the supply chain will be collected locally, from within its information system, via a node with an API (application programming interface). The protocol will then recopy this information to each node in the network. These nodes normally correspond to different stakeholders, and each piece of information is encrypted with a key specific to the node. Confidentiality is thus protected.

A blockchain serves to build confidence about the origin of information and, too, about its stability over time (since it cannot be altered). The confidentiality of information is managed via advanced encrypting procedures prior to the blockchain. The scalability of the access to data, their consolidation and statistical aggregation are managed downstream once the data have been extracted from the blockchain.

At no point does the question of the veracity of the data recorded by stakeholders in the registry arise. A false piece of information is still information. It has to be collected too. The information (true or false) provided by stakeholders will be used to analyze the supply chain so as to detect "false" information and correct it. The objective is not to make a registry with "true" information. That would not make sense, since it implies that all cases of malevolent actions or of errors have already been solved. Instead, the objective is to form a registry of data that cannot be

modified so that we can, by analyzing them, detect problems and set up a transparent feedback loop for gradually improving reliability all along the supply chain by making each stakeholder responsible.

This procedure is gradual. It is not necessary for all stakeholders on the supply chain to provide information, since even incomplete information will prime the feedback loop. A new party on the supply chain will, once authorized, connect to the network as a node. The blockchain protocol synchronizes this new node with the rest of the network. Each thus connected stakeholder is a plus for security and for the transparence and utility of the feedback loop. A blockchain is, therefore, a means for gradually bringing together manufacturers and businesses that have interests and vales in common.

Other questions arise about the industrial rollout of blockchain technology, in particular about data storage and the legal framework (especially with regard to personal data). Answers exist, but they extend beyond the scope of this article. After initial tests, the question now to be asked is: how can blockchains be used along with other techniques to cope with problems at an industrial scale?

Conclusion

DLT builds up confidence. The approach presented herein does not try to use technology to force people to have confidence in blockchains or in the data recorded on them. That would mean that the problem to be addressed has already been settled. Instead, let us create the conditions so that data are not altered. The integrity of data and their quasi immutability are the very grounds of the confidence guaranteed by DLT.

Thanks to the immutability of information on a blockchain, algorithms could analyze a product's life-cycle by using the information recorded by the parties who intervene in the supply chain. In this information, they could detect the "weak" signals typical of anomalies of whatever sort: malfunctions, malevolence, irregularities, absence of quality, etc. Feedback loops would be generated that make all stakeholders responsible and ultimately make the supply chain reliable. The idea is to make ongoing improvements (similar to the approach adopted for lean manufacturing) that lay the grounds for transparency, the very basis of a new contract of confidence with consumers.