Oracles,
the soft- and hardware layer of trust
between blockchains and the physical world

Vanessa Rabesandratana,
customer success manager, Ledger;
Nicolas Bacca,
chief technical officer, Ledger;
& **Eric Larchevêque**,
co-founder of Ledger

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

Abstract:
Blockchain applications are evolving in a totally virtual environment designed to be fully separate from the real world. Smart contracts, decentralized applications and cryptocurrencies have a limited hold over the physical world around us, as if these two universes exist on planes that are never superimposed. Since the very start, every use of this technology has logically raised questions of the following sort. How can blockchain applications efficiently interact in security with the real world? How can smart contracts efficiently tap external sources of data in security? Tools and interfaces have to be adapted. The trusted platform for relating the real world to blockchains has a name: Oracle.

Oracles are trusted entities signing claims about the state of the "physical world". Depending of what exactly we call the "physical world", and on whether or not a consensus exists about the state to be assessed there, oracles can be of help.[1]

Software oracles

Certifying origins

When the information being sought is available online, simple software-based oracles provide an effective solution for answering simple questions such as: "What is the bitcoin exchange rate in euros?", "Did this plane arrive more than 30 minutes late?" or "Was it raining yesterday in that city?" Data available on the Internet can be extracted from reliable sources such as airlines, financial data aggregators or weather institutes.

[1] The article in French is, in the main, a translation, of an article by Eric Larchevêque : "Hardware Pythias: Bridging the real word to the blockchain", 31 August 32016 on the blog:
https://www.ledger.fr/2016/08/31/hardware-pythias-bridging-the-real-world-to-the-blockchain/
The original article in English has been expanded with additions by Vanessa Rabesandratana and Nicolas Bacca. Noal Mellott (Omaha Beach, France) has revised the parts from the original article in English and translated the new parts from French.

An oracle cryptographically attests the origin of the data with a TLS (transport layer security) certificate and sends the information to a smart contract. The oracle makes a public claim about the contents of secure web pages, and provides an actionable gateway for a decentralized application.

There are technical pros and cons about implementing oracles. Not only must users have confidence that the oracle software will not distort or alter the information; but even more important, they have to trust the source of the information. For weather data from a reputable website, this trust is taken for granted; but what about complex facts or events that are hard to put into words? Should we have blind trust in Wikipedia? Different versions of the same information could put an oracle in check, and its certifying claims would be worthless.

Hard facts can always be crosschecked with different trusted sources (financial tickers, weather data, sports scores, etc.), but this does not hold for more complex questions for which different versions of the same information exist, each version depending on a party who has an interest in presenting biased information.

Oracles based on consensus

Decentralized prediction market platforms, such as Augur, could not exist without "perfect" oracles for gathering information to predict the outcomes of events. The idea is to bet on events of any sort, make inferences from trends and thus obtain a prospective view. Betting on football matches or on trends in the futures market immediately comes to mind; but prediction market platforms also provide critical intelligence about military operations or the fight against terrorism. If someone can be paid safely and anonymously for valid information about a major fact or event, then this information could be placed on a prediction market.

Since certain sorts of information are a government monopoly, regulations do not allow for prediction markets using them. In this case, the only solution is a decentralized approach. As a consequence, oracles for determining the truth of a purported fact by settling the outcomes of wagers must also be decentralized and be confidential. Trust cannot be based on a single source since the latter can too easily be manipulated or censored. Therefore, an appeal must be made to "crowd-knowledge" and to complex consensus systems based on "reputation" and on sanctions to "punish" the parties who fail to be honest.

These decentralized oracles are now at the center of R&D activities for prediction markets such as Augur or Gnosis. Such markets must work "perfectly" in order to generate value.

Hardware oracles

Oracles can handle information about "public" events, *i.e.*, observable by anyone. But what about real-time, nonpublic, user-centered events? Some facts cannot be determined through consensus or certification procedures. For example: Where is this shipping container right now? Is that door locked? How much greenhouse gas has this motor emitted during the past 60 minutes? What is the speed of that truck? How fast is my heart beating?

Local and private data sources

Some applications require information or readings from the physical world, from a targeted object or person. A measurement has to be made locally, often in real time. Since the data are private, a public feed or a consensus system cannot verify their accuracy. Several uses can be imagined, such as tracking services for industry or smart electricity grids.

Let us take the example of a smart contract for a car insurance policy whereby drivers pay a higher premium in the hope of being rewarded for good driving. Part of the premium paid by drivers who speed would go into a pool to be shared out among all "law-abiding" drivers. Road safety associations could make local contributions to the pool so as to provide larger incentives. The difficulty here is to find a secure method and a tamp-proof device for monitoring a vehicle's speed. Were a bad driver to simulate good behavior or to place his tracker on another car, this insurance would fail, and the company providing it would collapse.

Certified information from tamper-proof sensors

To obtain a secure report from sensors and certify its origin, the following are necessary:

- a cryptographic attestation of what is read from the sensor, so as to authenticate the origin of the measurement: each device has a private key signing outgoing payloads (with a nonce to avoid replays).
- an tamp-proof installation of the device serving as a meter, so that it immediately becomes inoperable (by deletion of its private key) when unduly manipulated (connection to another device, false input, etc.)

Sensors with a secure reading system are hardware oracles, the gateways from the physical world to the blockchain.

Deploying these oracles require provisioning the system with master certification keys and device identification keys, and establishing a strategy for supervising the installation (to make sure the devices measure what is to be measured). The anti-tampering features and the protection of the private keys guarantee long-term security and confidence.

Let us now return to the example of car insurance: the tracker oracle would have to have the appropriate certification keys (by obtaining them from device-suppliers). Furthermore, and an auditing strategy would have to be adopted to verify the initial installation (by recourse to external trusted parties/auditors).

The rollout of oracles?

For an increasing number of uses, decentralized applications cannot do without information retrieved from the physical world. Oracles are at the core of the arrangements indispensable for developing this technology.

Businesses have every reason to anticipate this new trend and incorporate in their equipment features from hardware oracles. We foresee in the coming years smart meters designed to be interconnected with blockchains, or electric vehicles with electronic wallets for machine-to-machine payments.

The Internet of things will have to reckon with blockchain technology, which, by nature, facilitates the integration of security features of the sort now sorely lacking. The new world is drawing near.