# Blockchain is more than a buzzword

By Bruno Letellier, CTO - Mobile Operators at IDEMIA

**# PAYMENT**
**# IDENTITY**

POSTED ON 02.26.18

- Blockchain is easier to understand than you think – here's a snap overview
- Moving keys from the Cloud to a securer physical element opens the door to new blockchain applications in real life

Since blockchain arrived on the scene in 2009, the technology has made headlines for its ingenuity, its potential to disrupt countless sectors. But it's more than a buzzword, it's an innovation that pushes into a new stage of our digital lives. So how does it work? Buckle up as we take off on a crash course.

## Breaking it down block by block

Let's say you want to serve an organic, responsibly farmed hamburger for dinner. The idea behind blockchain — an unmodifiable chain of information — is that you're able to guarantee that you know exactly what ends up on your plate. At a glance, you would be able to see what the cow ate everyday, its living conditions and how the meat was processed and sold. All these "blocks" of information, once logged in by the farmer, butcher and transporter, are time-stamped, attributed to the author and cannot be changed by anyone else. Ever. Sure, you could find this information today by conducting a study or visiting the farm, but blockchain provides immediate, trustworthy and tamper-proof information in real time.
While the scope of blockchain doesn't extend to hamburgers yet, it has become a widely accepted "ledger" of information for bitcoin transactions, medical records, and identity management.

## Trust is built in the blockchain

By design, the blockchain is a secure repository for data that allows us to share information with anyone, anywhere in the world. And while having a detailed ledger of activity is all well and good, how can we be sure that the information is reliable? This is where private keys come into play. Only users with the correct key can contribute to their blocks of information. So the farmer in our analogy can only log in information related to the farm, and not the meat processing, packaging or transportation. The transparency of the database means that all activity is tracked and can be analyzed by anyone with access to the blockchain – holding all users accountable for their contributions.

## The keeper of the keys

The use of private keys is a real differentiator of the blockchain as it allows data to be managed autonomously and in a decentralized way; however it also opens the door to the possibility of corruption. While locking access to the blockchain certainly adds a level of security, it also creates something to be stolen: the key. If the private key is stolen, the thief can irreversibly write in the ledger on behalf of the key holder. And today, private keys are stored in the cloud –

a very convenient location; however having all the keys in one place creates a very tempting target for hackers.

IDEMIA, the global leader in trusted identities, is moving these keys from the cloud to a secure element, storing them in a secure hardware vault and making sure that only its rightful owner can use it to write in the blockchain. Once the key is stored in the secure element its access can be secured with the user's own biometric data. Once the key is associated with a verified identity, the owner is in full control and can no longer be impersonated. Besides, with the dispersal of all of the keys, instead of hacking into one platform and gaining access to all stored keys, would-be hackers would have to hack each user individually – a far more difficult task.

## Blockchain IRL (in real life)

In addition to security, moving private keys into a physical secure element adds convenience to the equation and brings the blockchain into our physical world. Today, cryptocurrency can only be used online because that is where keys are stored. The promise of the physical secure key is that we'll be able to pay with this currency in real life. Tomorrow, we can buy a cup of coffee from a connected vending machine. That machine will write the purchase down in the ledger, and with a wave of the smartphone, we securely pay for the coffee. Cryptocurrency is safer, life is simplified, everyone wins.

At IDEMIA, identity management and verification is ingrained in our DNA, so we're up to the challenge of securing your identity, so only you can be you. And in the blockchain world, an ironclad identity authenticates the entire chain of information and opens the door to endless applications. To be continued...