



SMART E-MOBILITY CHALLENGE

TRUSTED DATA FROM A CAR: RELIABLE POWER GRID OPTIMIZATION

DSA & CENTER CONNECTED INDUSTRY & ENERGYBASE & UBIRCH
JOIN FORCES TO COMBINE STATE OF THE ART TECHNOLOGY,
MILITARY-GRADE CRYPTOGRAPHY, AND BLOCKCHAIN TECHNOLOGY
IN A CAR TO ENABLE TRUSTWORTHY IOT DATA.

PROBLEM BEING SOLVED

Current security solutions for IoT data don't scale, can't guarantee the authenticity of IoT data end-to-end, and don't offer ways to verify data authenticity whenever needed in the business cases repeatedly. This will become mandatory, if more and more parties are involved in IoT business cases together. Energy providers for example need to be able to fully trust the IoT data they receive to prepare their smart grid. They need to be sure that data coming from the sensor was not manipulated, injected, changed or deleted, and is received in the correct sequence from the correct sensor. Only if this is guaranteed, energy providers can build optimization processes based on IoT data.

SOLUTION BEING PROVIDED

The solution provided focuses on trustworthy energy consumption data coming from the car. The SIM-Card of the car is generating cryptographically signed and linked blockchain-optimized data packages containing the power consumption, energy need, and route of the car and stores them into the blockchain. This enables a functional application like the DSA cloud, which is calculating the time of arrival and power needed at the charging station, to verify the authenticity of the car data, as well as allowing the energy provider to revalidate the request/information they received from the functional cloud.

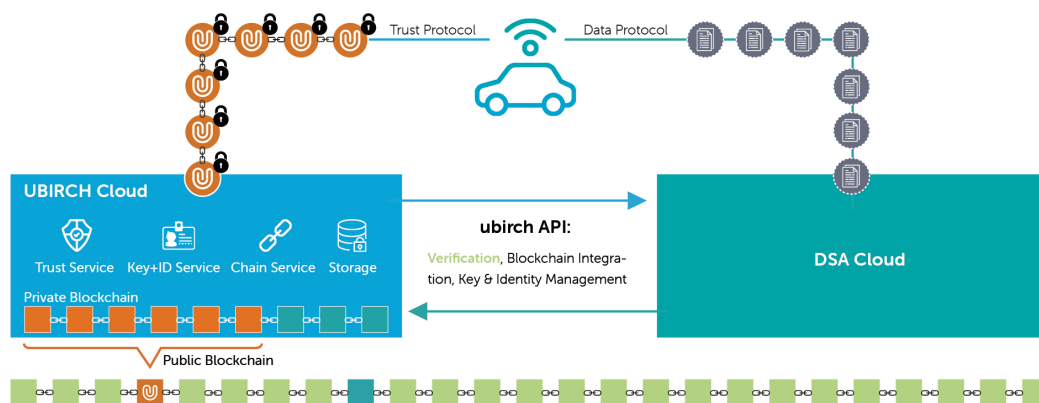
BUSINESS VALUE

Through trustworthy car data and the possibility to (re-)validate the authenticity of data, energy providers can automate processes to optimize their power grid based on an immutable log coming directly from the sensor, being verified against the blockchain. This enables automations, new business cases, and enables data hack detection, therefore preventing damage being done through hacking.

TECHNOLOGY COMPONENTS

This case uses a SIM-Card in the car to seal the data cryptographically directly at its source with a blockchain-style protocol, milliseconds after it has been measured. In the backend data gets anchored into a public blockchain to create an immutable log. The DSA cloud does functional calculations like the estimated time of arrival and energy needed at the charging station. Visualization of power data of the car is done by the Center of Connected Industry using verified data.

RELIABLE POWER GRID OPTIMIZATION – ARCHITECTURAL OVERVIEW



The car produces two data streams for its IoT data, the data protocol and the trust protocol. While the data protocol can be handled by an IoT platform like the DSA cloud, the trust protocol is handled by the ubirch cloud, anchoring the trust package in a two staged approach, utilizing a second layer private blockchain, into a public blockchain. Whenever needed within the business case, the IoT data can be verified for its authenticity using the ubirch API, by looking up the according ubirch protocol trust package.

THESE PARTNERS CONTRIBUTED TO OUR SUCCESSFUL POC



CENTER
CONNECTED
INDUSTRY



FOR MORE INFORMATION

Dominik Lenarczyk
dominik.lenarczyk@ubirch.com
+49 160 903 62 997
www.ubirch.com