



## SMART E-MOBILITY CHALLENGE

### TRUSTED DATA FROM A CAR: TRUSTWORTHY DAMAGE DETECTION

LUFTHANSA INDUSTRY SOLUTIONS AND UBIRCH JOIN FORCES TO COMBINE STATE OF THE ART MACHINE LEARNING ALGORITHMS, MILITARY-GRADE CRYPTOGRAPHY AND BLOCKCHAIN TECHNOLOGY ON A CHIP TO ENABLE TRUSTWORTHY IOT DATA.

#### PROBLEM BEING SOLVED

Current IoT security solutions can't guarantee end-to-end authenticity of IoT data and don't offer ways to verify data authenticity whenever needed in business cases. This becomes mandatory if more and more parties participate in IoT business cases together. For example, Insurance companies need to be able to trust the IoT data they receive from their own sensors or partners completely. They need to be sure that data coming from the sensor was not manipulated, injected, changed or deleted and is coming in the right sequence from the right sensor. Only if this is guaranteed, insurers can create new tariffs, business models and processes, based on IoT data.

#### SOLUTION BEING PROVIDED

The solution provided focuses on trustworthy damage detection. It contains a specific sensor unit together with a microcontroller, trained to detect damage of an asset like a car or an airfreight container. The microcontroller generates cryptographically signed and linked Blockchain-optimized data packages containing information about detected damage, time and location of the asset and stores them into the Blockchain. This enables insurers to always verify the authenticity of IoT data they receive.

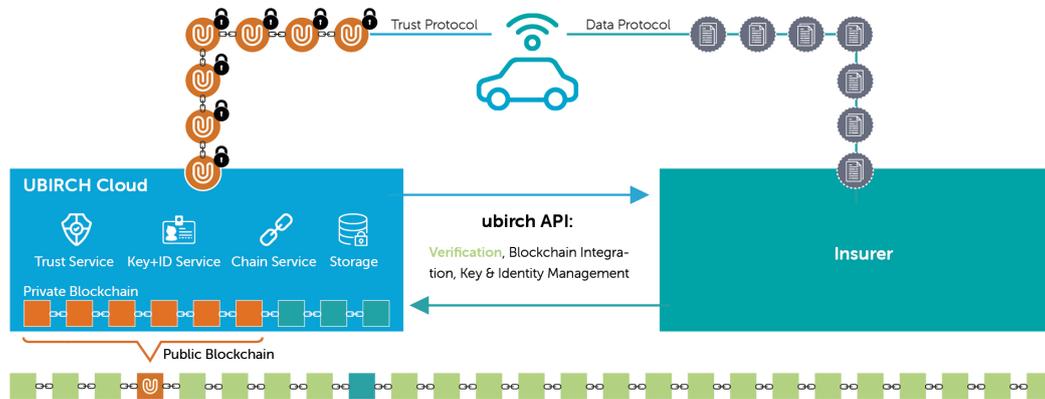
#### BUSINESS VALUE

Through trustworthy damage detection and the possibility to validate the authenticity of IoT data, insurers can automate processes based on trustworthy, immutable data coming directly from the chip, verified against the Blockchain. This enables fast processes, less damage expert reports, even smart contract application and new business cases.

#### TECHNOLOGY COMPONENTS

The case utilizes a Damage Detection Box created by Lufthansa Industry Solutions. It consists of a Pycom LoPy4 microcontroller and a BOSCH BMI160 sensor. The sensor measures acceleration and angular velocity. This data is fed to an ML algorithm which determines if any damage has occurred. The UBIRCH client within the microcontroller seals the data cryptographically at its source with a Blockchain-style protocol, milliseconds after it is measured. The sealed data is sent to the backend using the LoRa network. In the backend, the data gets anchored into a public Blockchain to create an immutable log.

# TRUSTWORTHY DAMAGE DETECTION – 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 or an insurer backend, 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 THIS SUCCESSFUL POC



**Lufthansa  
Industry  
Solutions**