UBIRCH

BLOCKCHAIN FOR THINGS

Securing high-volume IoT data transmissions

BLOCKCHAIN FOR THINGS

Securing high-volume IoT data transmissions

By combining well-established cryptographic signatures with blockchain technology, UBIRCH has created an innovative and highly efficient method of securing trust in IoT data forever. We call it Blockchain for Things.

IOT IS GROWING FAST - SECURITY NEEDS TO ADAPT

The internet of things (IoT) is increasingly prevalent in our daily lives within new areas such as smart cities, autonomous cars, Industry 4.0 and products as a service, where sensors and remotely controlled systems are becoming a standard. In most cases, the question whether the sensor data can be trusted is core to the business model.

For consumers, if micro charging or smart parking for your autonomous vehicle isn't reliable, fully automated invoicing will never become standard.

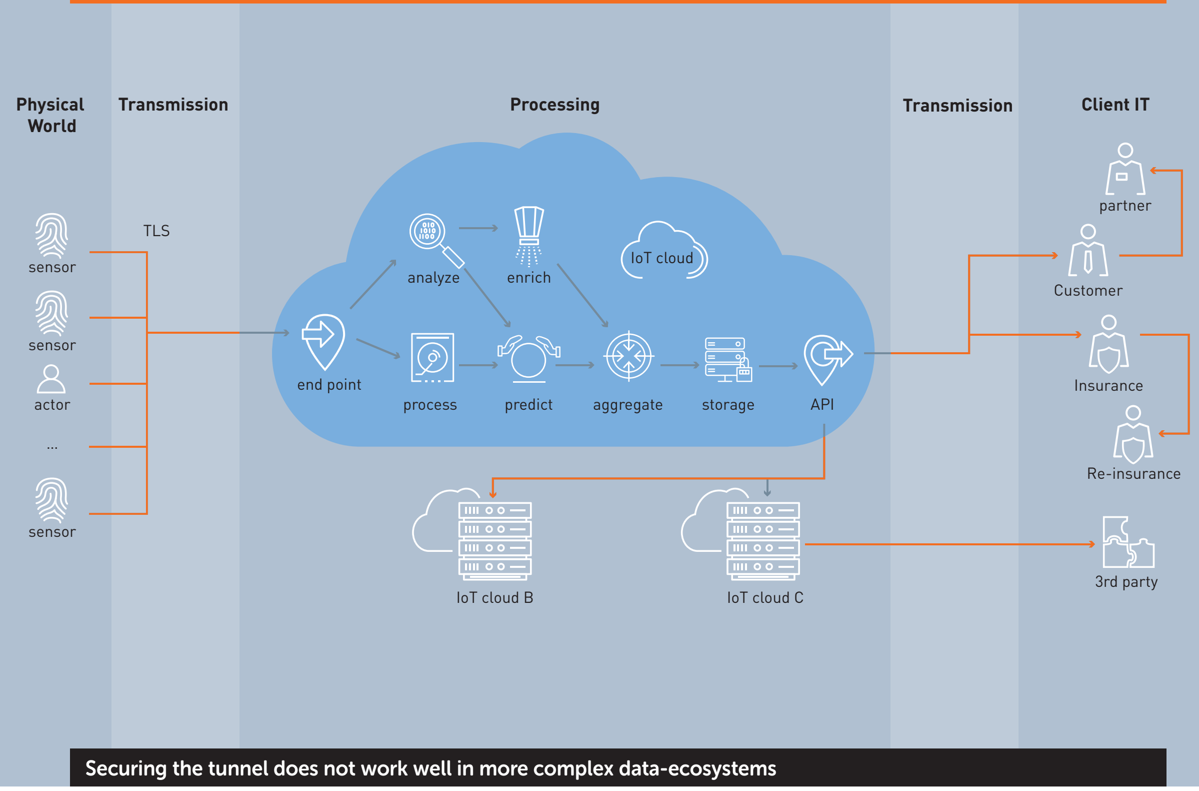
For industry, if remote sensor data from high value assets such as wind-turbines or heavy machinery can be hacked or intercepted, the associate costs could be significant, in addition to dangerous for employees.

For insurers, the authenticity of data for automating claims is reliant on the authenticity of data to reduce fraudulent activity.

The current solutions for generating trust and data security through TLS encrypted channels requires infrastructure that is not scalable, and does not always guarantee data authenticity. In many instances, these vulnerabilities have already been exploited to the detriment of businesses (e.g. recent hack of a Tesla Model S).

UBIRCH has developed a unique approach - the Blockchain of Things - for securing end-to-end IoT data transmissions forever by combining cryptographic signatures with Blockchain technology.

Multiple Tunnels Are Not A Good Solution



Securing the tunnel does not work well in more complex data-ecosystems

CURRENT SOLUTIONS - TLS AND VPNS DON'T SCALE

Conventional systems that secure IoT devices, such as VPN's, are based on Transport Layer Security (TLS) where data transmission paths are secured by encryption (comparable to an https connection).

This proven technology prevents unauthorized access during data transmission by creating an impenetrable tunnel. However, after decryption, (be it on premise or in the cloud) there is no way to ensure that the data is from a specific device that it is authentic, unchanged or not compromised at any time without authorization.

Traditional TLS capability was also not designed for handling complex IoT applications that rely on numerous different systems, data streams and partners, creating complex data relationships that are hard and overly expensive to maintain.

Vulnerabilities also result from using security keys across many instances, sharing them with numerous parties, and through the usage of symmetrical cryptography, which by default requires the transport of a security key to remote recipients. In many cases hackers have gained access via compromised keys (e.g. z-wave hack exposes up to 100million IoT devices)

USING BLOCKCHAIN

Whilst Blockchain technology offers an innovative solution to solving the IoT data security problem, until now a couple of major challenges have remained:

THE LAST MILE PROBLEM

Most IoT sensors are installed in exposed places (i.e. buildings, machines, vehicles, public spaces, even inside human bodies) where critical data is generated (e.g. body temperatures, vibration-patterns of a machine or acceleration data of a fork lift). The sensors are often battery powered and have limited processing power (no edge computing).

The data therefore needs to travel to the cloud, where it can be stored in the blockchain. This makes it vulnerable to being tampered with along the way. Transmission over the air is critical and raises the question whether the transmitted data really reflects what happened at the edge-device. This “last mile problem” is crucial for meaningful applications of blockchain technology for the IoT

THE PUBLIC VS. PRIVATE PROBLEM – SCALING THE BLOCKCHAIN

Existing public blockchains are relatively slow and expensive to use. A common alternative to scaling current blockchain implementations is to use a private version, often owned and operated by a single party. This has certain drawbacks, as it jeopardises the main trust element of the blockchain architecture. A non-distributed private blockchain might be cryptographically acceptable, but in some instances, bypasses the real consent mechanism.

Newer public blockchains, that scale better and have lower transaction costs, are not necessarily able to handle the amount of data that can be expected from professional IoT systems (e.g. a factory). Even if today’s public blockchain could handle thousands of requests per second, it would still be very expensive and transaction costs could vary significantly, as the underlying tokens might be subject to aggressive trading. Moreover, while a public blockchain delivers the highest values for trust, many IoT device operators would not feel comfortable with storing all the data in a publicly available space.

UBIRCH

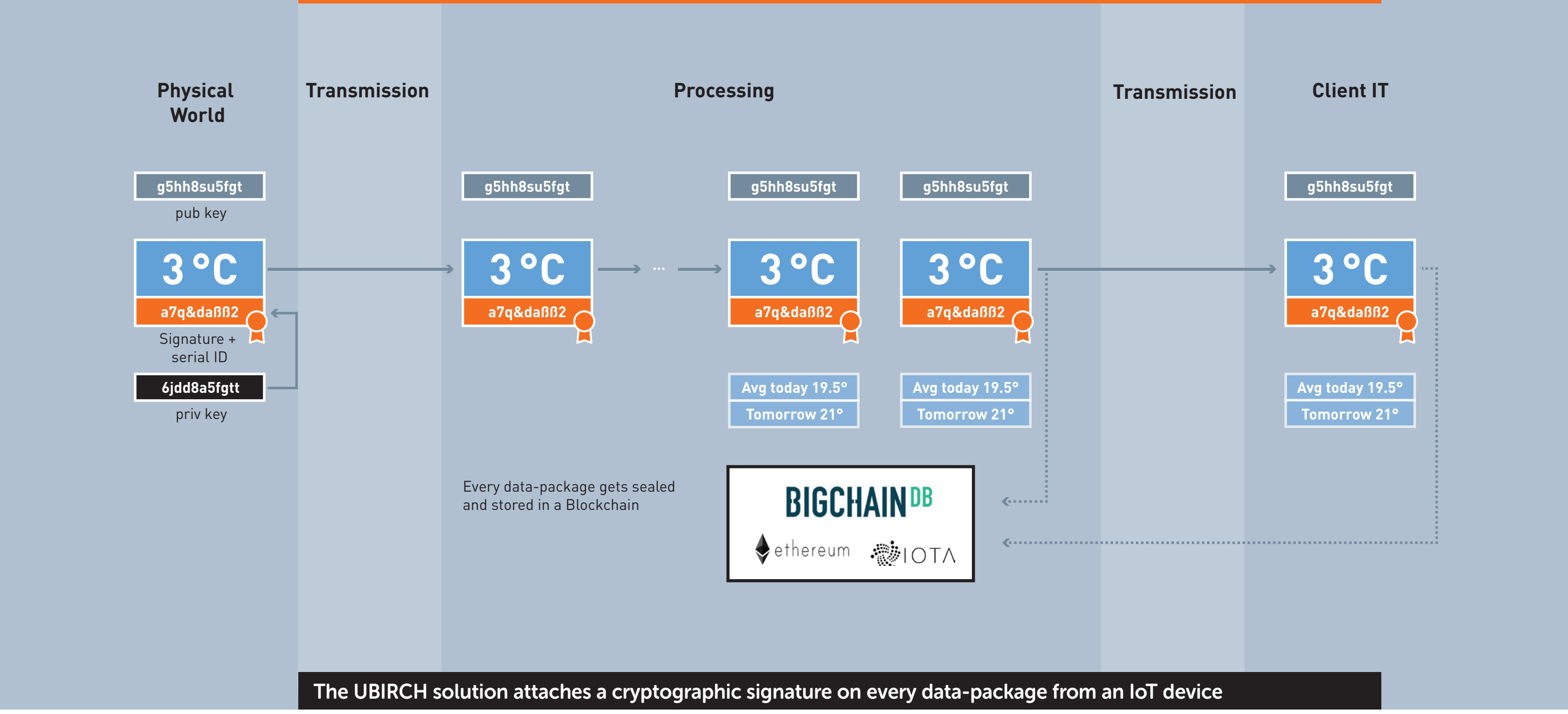
UBIRCH – DATA AUTHENTICITY AT SCALE

UBIRCH uses a fundamentally different approach for securing end-to-end IoT data transmission, called the Blockchain for Things. It generates 100% trustworthy data streams by guaranteeing the integrity and authenticity of each data packet.

THE UBIRCH SOLUTION

1. seals individual data packets instead of securing transmission channels
2. uses a lightweight client (firmware) on the IoT device
3. guarantees security right from the sensor (IoT device)
4. solves the cost/bandwidth problem with a two-stage blockchain architecture

Securing individual data packages



The UBIRCH solution attaches a cryptographic signature on every data-package from an IoT device

MAKING IOT SECURITY SCALABLE BY SEALING DATA PACKETS

Instead of using symmetric cryptography requiring the transmission of security keys to single, and multiple backends, UBIRCH uses asymmetric cryptography.

UBIRCH uses elliptic curves (ECC, curve ed25519) as a means for asymmetric cryptography. This process is superior to traditional RSA algorithms in terms of speed and resources, and is an accepted open source standard that can be used without compromising security.

Each IoT device generates its own key pair consisting of a private key and a public key derived from it.

- The private key is securely generated on the IoT device and never leaves it. No one has access to this key, because it is stored in a secure memory space on the microcontroller. The IoT device itself therefore signs the messages (for example sensor data) with its private key.

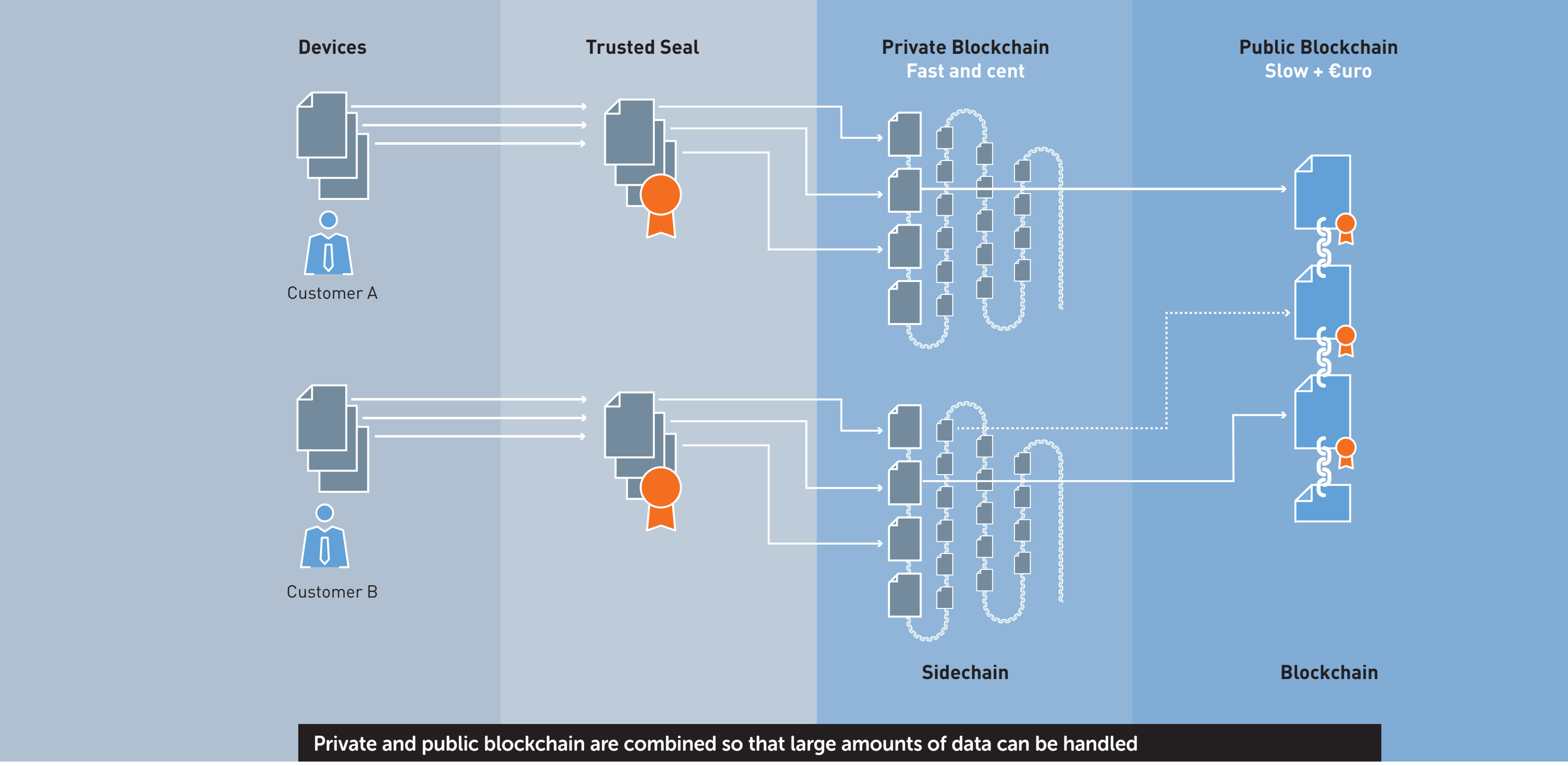
- Using the public key that can be retrieved by a key-server, the receivers can verify both the content and sender of the message. This makes a complete integrity check possible.

DATA-LEVEL PROTECTION

The UBIRCH process also differs from current solutions, as it uses cryptographic protection to secure data at the individual data item/packet level of messages, which means that the integrity of each data item is secured with an individual signature.

This can be compared with a notarial seal and it gives every user in the value chain the opportunity to perform a full, easily automated, check before processing the data. This check can take into account the identity of the sender, the integrity of the data (including recording time) and the correct order of data packages, depending on user requirements.

Scaling blockchain



Private and public blockchain are combined so that large amounts of data can be handled

SECURING THE SENSOR

The UBIRCH system secures the IoT sensor by implementing a lightweight client (firmware) directly on the edge device, ideally even onto the sensor itself, or depending on the local requirements, the Scada-Controller/SPS System can be a good place, as well. The client performs the basic cryptography needed to establish a "blockchain-ready" data package: key-generation, establishing trust with any (authorised) backend, sealing and/or verifying data-packages and linking them cryptographically to the previous data-package in order to seal not only the actual payload, but also the order of the packages from that sensor.

SOLVING THE SCALABILITY PROBLEM: THE 2-STAGE BLOCKCHAIN ARCHITECTURE

The UBIRCH architecture consists of configurable components accessible via an API, and managed by the customer through an IoT management dashboard.

A dedicated service handles the integration of data into the UBIRCH side-chain and an additional integration of meta blocks in a public blockchain, depending on the requirements. This combination of a highly scalable side-chain and a public blockchain helps to achieve high transfer rates at low transaction costs and maintains all the advantages of a cryptographic linking of data-packages. Depending on the client need, the actual payload can also be transferred through the UBIRCH system – but it is not necessary in order to secure the IoT data. The major objective of the UBIRCH system is to provide and store seals for data-transactions that can be used for verification by the client system.

The UBIRCH solution can be integrated in IoT Management Systems

PROTECTION AGAINST CYBER ATTACKS

In addition to checking the integrity of data packages, the UBIRCH system can also be used to prevent a number of typical attack scenarios on IoT infrastructure, including

- “man in the middle“
- “replay“ attacks
- hacking IoT devices with the malicous intent, botnet creation or ransomware.

Attacks like “man in the middle“ or malicious content can be eliminated through private key signatures verification on valid data packages. “Replay attacks“ are made impossible by linking signed data packages with each other cryptographically, where the backend can detect duplicated data packages and exclude them from processing.

API INTEGRATION

The UBIRCH API allows integration with 3rd party systems (e.g. client IT/cloud, IoT cloud systems, ERP systems), using message protocols like MQTT, AMQP and REST.

The UBIRCH validation component can also be made available as a container for direct integration into the client’s IT system, so that data packets can be verified once more before triggering internal events or being stored.

INTEGRATION ON SENSOR HARDWARE/IOT DEVICES

A library can be installed on devices with minimal hardware requirements (e.g. ARM Cortex M0 or higher) through a firmware update. Software on the device then performs all necessary cryptographic operations, locally,

The resource requirements of the library even allow deployment on SIM-, or Smartcards; a port to other hardware platforms can also be provided.

REFERENCE HARDWARE

If you are looking to create your own hardware designs based on the ubrich crypto node, for testing or referencability, we can supply a “ubridge“ reference board. This features an MCU with hardware crypto-support (NXP K82), a GSM module and a Sub 1GHz radio-frequency module.

UBIRCH

UBIRCH – 4 REASONS WHY

Securing IoT data from the source

Leveraging the Blockchain to secure distributed IoT data

Securing sensors against infiltration

Scalability for complex IoT Ecosystems

Founded in 2014, has offices in Cologne and Berlin, where it services global customers. Named "Cool Vendor" by Gartner, UBIRCH is a market leader in IoT security leveraging Blockchain.

CONTACT

UBIRCH GmbH · Gürtelstr. 25
D-10247 Berlin · Germany
Stephan Noller
info@ubirch.com