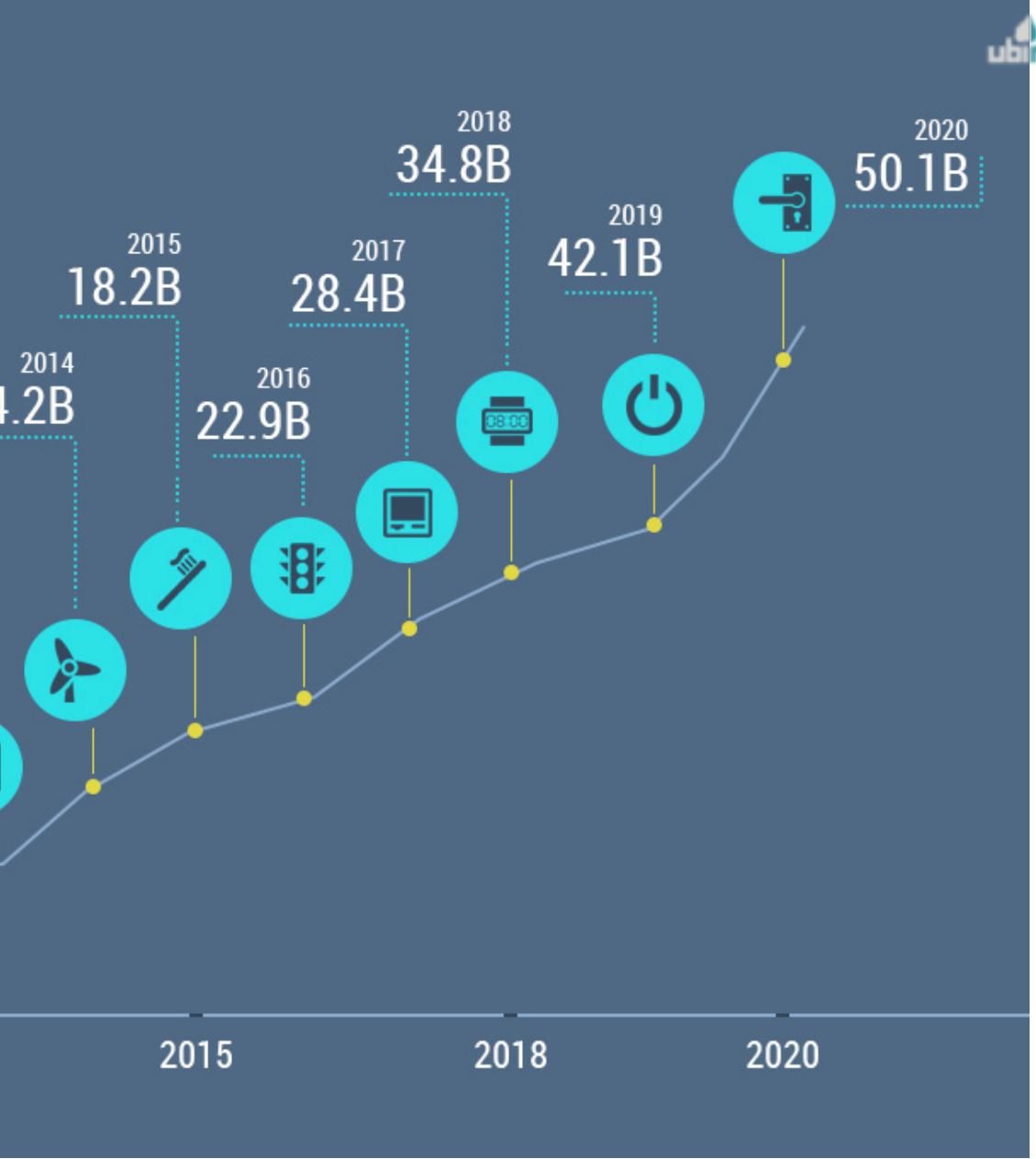
Vernetzte Produktion und die Blockchain

Markus Breuer
Juni 2018

Gartner COOL VENDOR



Das IoT wird gewaltig werden

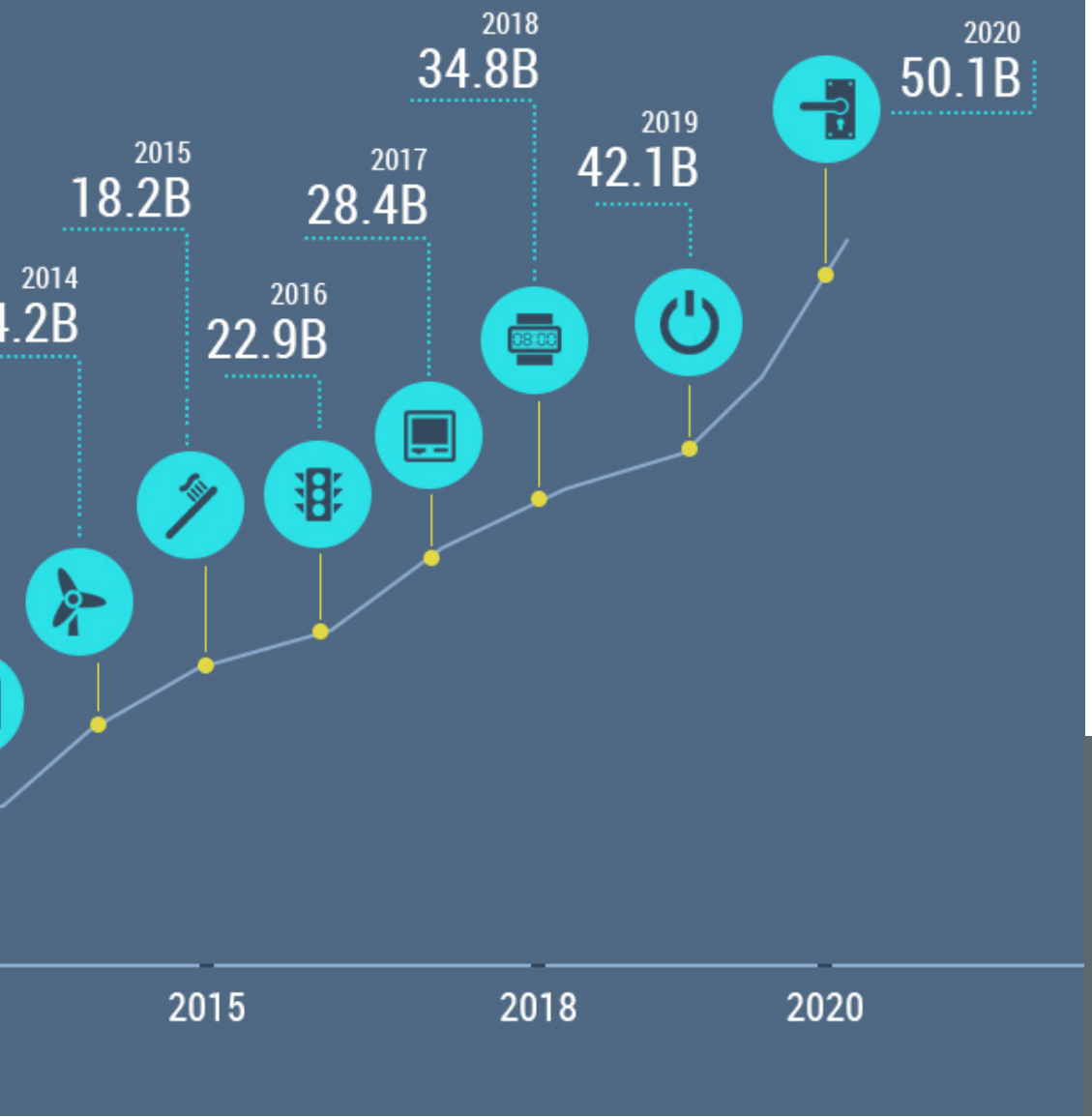
30 – 50 Mrd. *connected devices* im Internet of Things bis 2020

Ungeheure **Datenmengen**!

Neue Möglichkeiten für **Erkenntnisse**!

Neue **Werte** werden geschaffen!

Jede Menge neue **Geschäftsmöglichkeiten**!



Das IoT wird gewaltig werden

30 – 50 Mrd. *connected devices* im Internet of Things bis 2020

Ungeheure **Datenmengen**!

Neue Möglichkeiten für **Erkenntnisse**!

Neue **Werte** werden geschaffen!

Jede Menge neue **Geschäftsmöglichkeiten**!

Und jede Menge neue Möglichkeiten für

… Hacking und Botnets

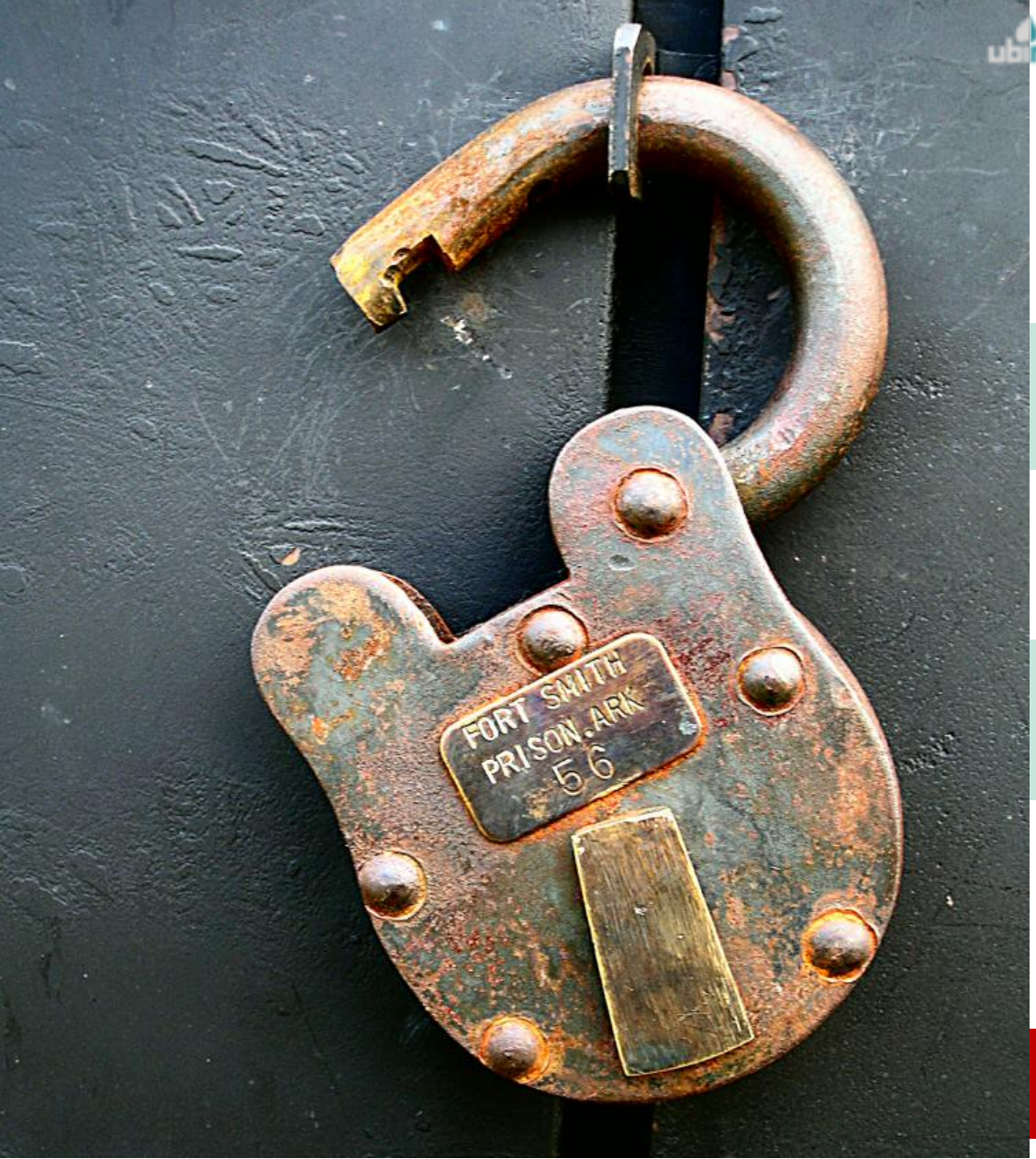
… Betrug im industriellen Maßstab

… Industriespionage, Erpressung, etc.

Wachstumshemmnis #1: Security

70%	aller IoT Devices hackbar
2014:	erstes Auto gehacked
2015:	Flugzeug gehacked durch Entertainment System
2016:	Erste Ransomware für Thermostaten aufgetaucht
2016:	Atomkraftwerk mit Malware infiziert
2017:	Fabriken und öffentliche Einrichtungen durch MQTT Schwachstellen angreifbar

Firmen zögern mit der Vernetzung aufgrund Sicherheits-Bedenken.



Zwei unschöne Wahrheiten

"State of the art" IoT Security **garantiert keine** Vertrauenswürdigkeit (1)

- Nur die Daten**übertragung** ist „sicher"
- Kein Schutz vor Hacking in der Cloud

IoT-Daten in der Blockchain zu speichern, **garantiert keine** Vertrauenswürdigkeit (2)

- Daten können manipuliert/gelöscht werden **bevor** sie die Blockchain erreichen
- Garbage in – garbage out

IoT-Daten sind **selten vertrauenswürdig**

Security and Trust by Design

ubirch hat ein Verfahren entwickelt, um Daten **kryptographisch abzusichern**, und in der **Blockchain** zu verankern**.**

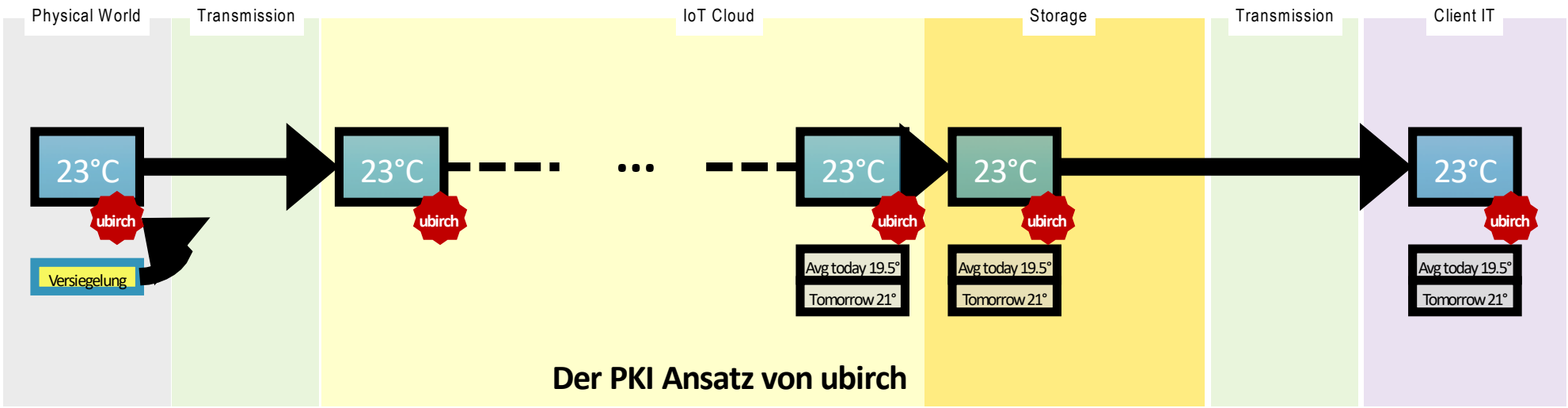
Der ubirch **Notar-Service versiegelt Daten** und garantiert, dass:

1. Daten **nicht verändert** werden können
2. Datenpakete **nicht gelöscht** werden können
3. Datenpakete **nicht dupliziert** werden können
4. Der **Absender der Daten** nicht gefälscht werden kann
5. Der **Zeitpunkt der Aufzeichnung** zuverlässig dokumentiert ist

Bevor die Daten die Cloud erreichen

ubirch 1st

Sicherheit & Integrität – Versiegelte Daten



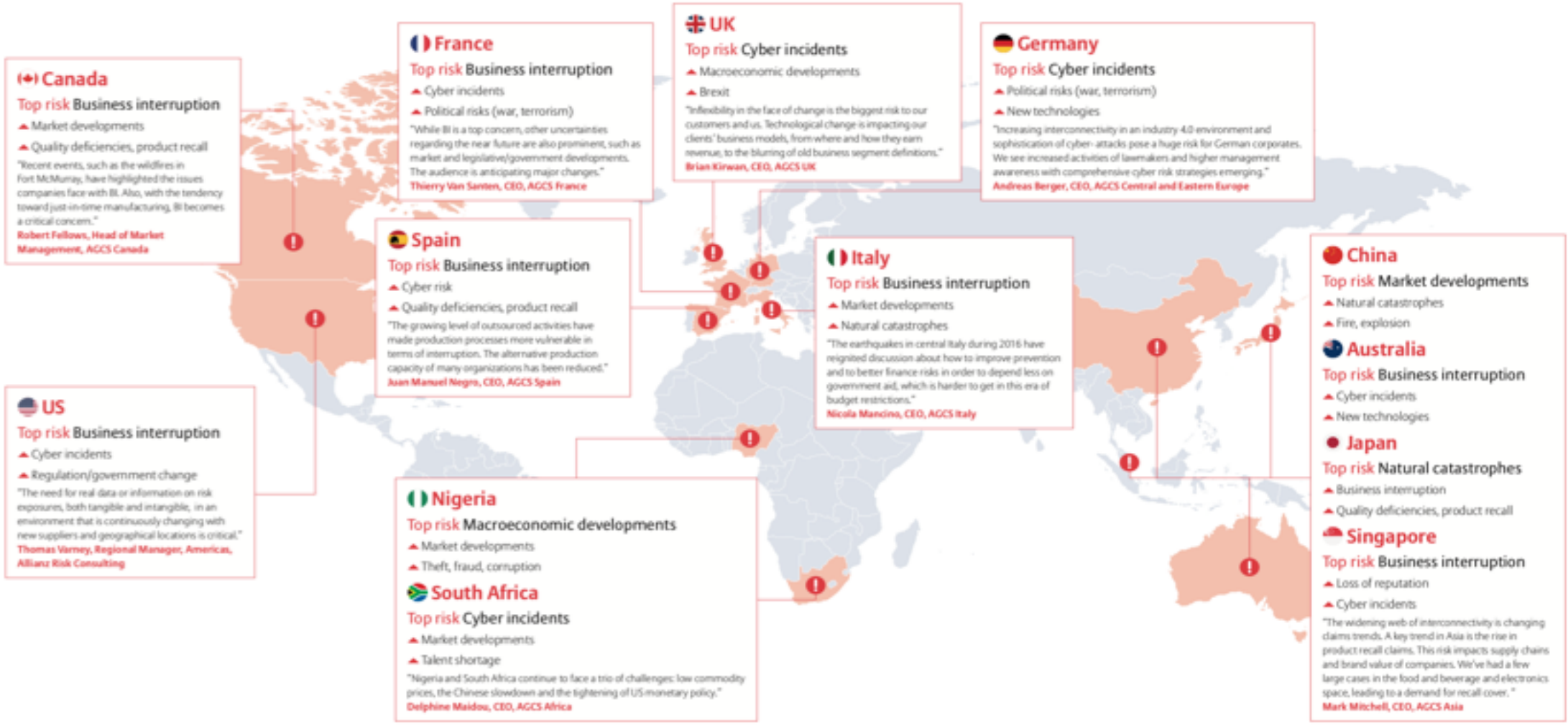
Und …
was hat das jetzt mit Versicherungen zu tun?

Betriebsunterbrechung ist zum im 5. Jahr in Folge das größte Risiko für Unternehmen. Neue Auslöser sind auf dem Vormarsch. [...] die Art des Risikos verschiebt sich zunehmend auf **Nicht-Sachschaden-Ereignisse**.

Ein **Cybervorfall** oder die indirekten Auswirkungen eines terroristischen Gewaltakts sind Ereignisse, die zu großen Verlusten führen können, ohne physische Schäden zu verursachen. **Eine Zunahme solcher Ereignisse wird erwartet**.

2017 Allianz
Risk Barometer

Snapshot: Top Business Risks Around The World in 2017



Canada
Top risk **Business interruption**
- Market developments
- Quality deficiencies, product recall

"Recent events, such as the wildfires in Fort McMurray, have highlighted the issues companies face with BI. Also, with the tendency toward just-in-time manufacturing, BI becomes a critical concern."
Robert Fellows, Head of Market Management, AGCS Canada

US
Top risk **Business interruption**
- Cyber incidents
- Regulation/government change

"The need for real data or information on risk exposures, both tangible and intangible, in an environment that is continuously changing with new suppliers and geographical locations is critical."
Thomas Varney, Regional Manager, Americas, Allianz Risk Consulting

France
Top risk **Business interruption**
- Cyber incidents
- Political risks (war, terrorism)

"While BI is a top concern, other uncertainties regarding the near future are also prominent, such as market and legislative/government developments. The audience is anticipating major changes."
Thierry Van Santen, CEO, AGCS France

Spain
Top risk **Business interruption**
- Cyber risk
- Quality deficiencies, product recall

"The growing level of outsourced activities have made production processes more vulnerable in terms of interruption. The alternative production capacity of many organizations has been reduced."
Juan Manuel Negro, CEO, AGCS Spain

UK
Top risk **Cyber incidents**
- Macroeconomic developments
- Brexit

"Inflexibility in the face of change is the biggest risk to our customers and us. Technological change is impacting our clients' business models, from where and how they earn revenue, to the blurring of old business segment definitions."
Brian Kirwan, CEO, AGCS UK

Germany
Top risk **Cyber incidents**
- Political risks (war, terrorism)
- New technologies

"Increasing interconnectivity in an industry 4.0 environment and sophistication of cyber- attacks pose a huge risk for German corporates. We see increased activities of lawmakers and higher management awareness with comprehensive cyber risk strategies emerging."
Andreas Berger, CEO, AGCS Central and Eastern Europe

Italy
Top risk **Business interruption**
- Market developments
- Natural catastrophes

"The earthquakes in central Italy during 2016 have reignited discussion about how to improve prevention and to better finance risks in order to depend less on government aid, which is harder to get in this era of budget restrictions."
Nicola Mancino, CEO, AGCS Italy

Nigeria
Top risk **Macroeconomic developments**
- Market developments
- Theft, fraud, corruption

South Africa
Top risk **Cyber incidents**
- Market developments
- Talent shortage

"Nigeria and South Africa continue to face a trio of challenges: low commodity prices, the Chinese slowdown and the tightening of US monetary policy."
Delphine Maidou, CEO, AGCS Africa

China
Top risk **Market developments**
- Natural catastrophes
- Fire, explosion

Australia
Top risk **Business interruption**
- Cyber incidents
- New technologies

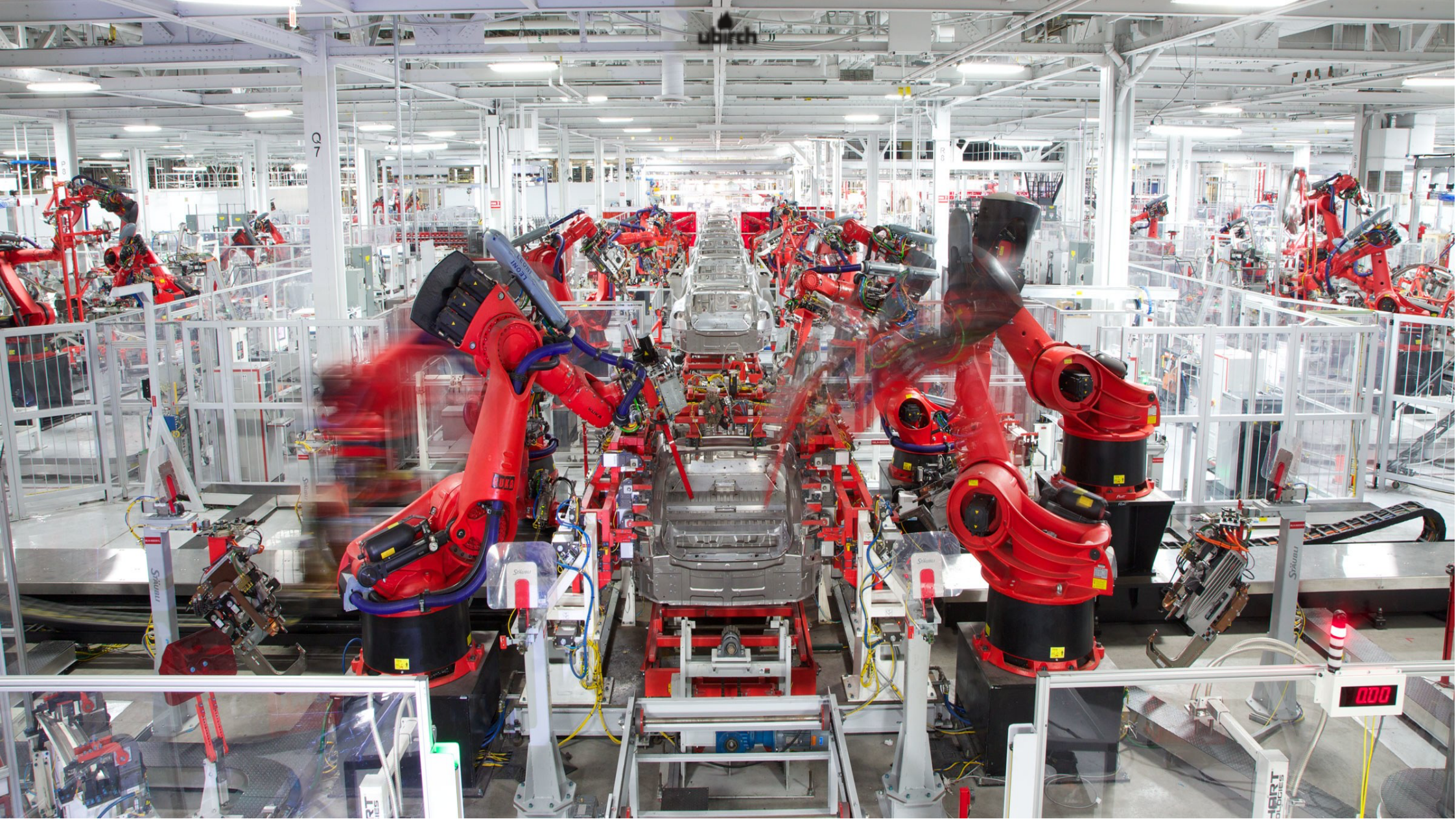
Japan
Top risk **Natural catastrophes**
- Business interruption
- Quality deficiencies, product recall

Singapore
Top risk **Business interruption**
- Loss of reputation
- Cyber incidents

"The widening web of interconnectivity is changing claims trends. A key trend in Asia is the rise in product recall claims. This risk impacts supply chains and brand value of companies. We've had a few large cases in the food and beverage and electronics space, leading to a demand for recall cover."
Mark Mitchell, CEO, AGCS Asia

This risk map shows the top risk for businesses in **selected** countries. It also shows rising risk concerns across these territories year-on-year.

Source: Allianz Global Corporate & Specialty


ubirch

Im vierten Jahr in Folge sind die Unternehmen zunehmend über **Cybervorfälle** besorgt. Die Bedrohung geht weit über Hacking, Datenschutzverletzungen oder Datendiebstähle hinaus, [...]

In einer Industrie 4.0-Umgebung können nicht korrekt verarbeitete oder missinterpretierte Daten die Produktion zum Stillstand bringen.

2017 Allianz
Risk Barometer

Absicherung von Produktionsdaten (Industrial IoT)

1. *proof of origin* für Bauteile
2. *tolerance allocation*
   - Kleine Fertigungsabweichungen werden zusammen mit den Bauteilen im Value Chain weiter gegeben.
   - Im nächsten Schritt werden zu große mit zu kleinen Bauteile kombiniert

   -> perfekte Qualität

- Fälschung oder falsche Zuordnung von Daten kann zu Riesenschäden führen

T-LABS BLOCKCHAIN GROUP
fir an der RWTH Aachen
SICK Sensor Intelligence. .msg
SCOR The Art & Science of Risk
bdr. BUNDESDRUCKEREI
Microsoft
Cumulocity A SOFTWARE AG COMPANY

The Blockchain for Things

ubirch hat ein Verfahren entwickelt, um Daten **kryptographisch abzusichern**, und in der **Blockchain** zu verankern**.**

Der ubirch **Notar-Service versiegelt Daten** und garantiert, dass:

1. Daten **nicht verändert** werden können
2. Datenpakete **nicht gelöscht** werden können
3. Datenpakete **nicht dupliziert** werden können
4. Der **Absender der Daten** nicht gefälscht werden kann
5. Der **Zeitpunkt der Aufzeichnung** zuverlässig dokumentiert ist

Bevor die Daten die Cloud erreichen

ubirch 1st