ESMT BERLIN

dena German Energy Agency

Background paper

Vulnerabilities in smart meter infrastructure – can blockchain provide a solution?

Results from a panel discussion at EventHorizon2017

Imprint

Publisher
Deutsche Energie-Agentur GmbH (dena)
German Energy Agency
Chausseestrasse 128 a
10115 Berlin, Germany
Tel: +49 (0)30 66 777 - 0
Fax: +49 (0)30 66 777 - 699
E-mail: info@dena.de
Internet: www.dena.de

and

ESMT European School of Management and Technology GmbH
Schlossplatz 1
10178 Berlin
Tel: +49 (0)30 21 231-0
E-Mail: info@esmt.org
Internet: www.esmt.org

Authors
Christoph Burger, ESMT
Dr. Ana Trbovich, GridSingularity and Energy Web Foundation
Dr. Jens Weinmann, ESMT

Editor
Philipp Richard, dena

The authors wish to express their gratitude to the panelists Christoph Jentzsch, Jan-Peter Kleinhans, Netanel Rubin, Dr. Jens Strüker and Thomas Weisshaupt. The authors also are indebted to Irene Adamski for her valuable comments and suggestions.

The statements in this text marked by name represent the opinion of the participants in the panel discussion at the EventHorizon2017 and not necessarily the position of dena/ESMT.

Cover Image: ESMT

Date: 02/2018

Contents

1 Executive summary

Can blockchain reduce potential hazards for smart meters? Findings from a panel discussion of the conference "EventHorizon 2017"

In contrast to conventional meters, which simply track total electricity consumption over a certain time horizon and need to be monitored manually, smart meters are equipped with a digital data transmission facility, which allows consumers and utilities to manage electricity consumption and production based on two-way communication.

Smart metering technology is an essential element of the digital transformation of the energy system. Its analysis is linked to the public discourse on smart cities, which can be categorized in three complementary narratives:

The *narrative of innovation* focuses on the benefits that new technologies bring to daily life. Smart meters can enhance a household's quality of life by providing transparent information about energy consumption. They also increase overall economic welfare by delivering tacit value derived from improved knowledge about patterns of electricity consumption and improved coordination of end users.

Within the *narrative of empowerment* smart meters can be interpreted as a step towards greater consumer autonomy and choice. Equipped with decentralized transaction technologies such as blockchain, they allow consumers to circumvent the hierarchical relationship with intermediaries such as utilities, and create the technological basis for peer-to-peer trading.

The third (and most ambivalent) narrative is the *narrative of control*. Technical devices are able to monitor and record valuable information on individual citizen's interests and habits. Large industrial players and IT service providers ally with local communities to provide resources for data analytics, which may be used to protect residents and increase urban safety and security. However, hackers may exploit access to sensitive information to commit criminal acts, such as demanding ransom or manipulating bills and accounts. Smart meters may become a gateway for illegal intrusion into the privacy of one's home, as it happened in Puerto Rico, where a local electricity utility lost hundreds of millions of dollars.

At "EventHorizon 2017", the first global conference on blockchain in the energy sector, which took place in Vienna in February 2017, a panel of renowned experts and practitioners deliberated on control and security features of smart metering infrastructure. The panel highlighted insufficiently secure protocols regulating communication between utilities, smart meters and home appliances and their high exposure to attacks by hackers, resulting from the current system incentivizing utilities to focus on short-term cost-savings rather than long-term investment in security. Moreover, it deduced that utilities often lack qualified professionals to properly assess all risks and supervise outsourcing of smart meters roll-out.

Given these shortcomings, the responsibilities of the main stakeholders could be stipulated as follows: Governments, including regional authorities, should set up institutional structures that accelerate the process of establishing safety guidelines, considering lessons learned from other industries, such as banking or mobile operators. Device manufacturers and electric utilities as operators of smart meters should pay more attention to security issues. Responsibility for liability issues should be fully clarified.

Could blockchain provide a remedy for smart metering infrastructure vulnerabilities? Panelists deliberations, which largely follow the narrative of innovation, suggest that blockchain has the potential to resolve some

critical issues, albeit with a certain time delay stemming from early technology development. Namely, the currently available public blockchains are still too slow, energy-intensive and inconvenient to be implemented in today's smart metering infrastructure. Yet progress is under way to develop more transaction and energy efficient blockchains, primarily led by the efforts of the Energy Web Foundation, as well as wider industry blockchain alliances such as Ethereum Enterprise Alliance, or HyperLedger.

While technical and digital innovation will be a crucial step towards a more sophisticated and resilient smart meter infrastructure, an institutional and regulatory framework with right incentives and clear liability is required to fully harness the potential for innovation. In this respect, the narrative of control may furnish a valuable context to address critical risks and vulnerabilities for end users, utilities, and the grid infrastructure.

2 Deutsche Zusammenfassung

Kann Blockchain Gefährdungspotenziale im Smart Metering mindern? Erkenntnisse aus einer Podiumsdiskussion der Konferenz „EventHorizon 2017“

Während konventionelle Stromzähler nur die Absolutmengen verbrauchter Energie über einen bestimmten Zeitraum erfassen, können „intelligente“ Zähler („Smart Meters“) Informationen zum aktuellen Verbrauch messen, an Konsumenten, Energieversorger und Verteilnetzbetreiber übermitteln und somit aktiv zur Koordination von Stromerzeugung und -verbrauch eingesetzt werden. Kontinentübergreifend gibt es Bestrebungen, die herkömmlichen Zähler sukzessive mit einer intelligenten Systeminfrastruktur zu ersetzen.

Smart Metering ist ein wichtiger Bestandteil der digitalen Transformation unseres Energiesystems. In der öffentlichen Diskussion lassen sich drei komplementäre Narrative (oder Erzählebenen/Sichtweisen) identifizieren, die eng mit dem allgemeineren Diskurs zu „Smart Cities“ verknüpft sind:

Das *Narrativ der Innovation* rückt den Nutzen technologischer Neuerungen für unseren Lebensalltag in den Vordergrund. Für Endverbraucher bieten intelligente Zähler u.a. die Möglichkeit, Einsparpotenziale zu erkennen. Aus gesamtwirtschaftlicher Sicht wird durch größere Transparenz ermöglicht, Energieflüsse zu optimieren und, wie oben erwähnt, Erzeugung und Verbrauch besser zu koordinieren.

Im *Narrativ der Selbstbestimmung* (auf Englisch „Empowerment“) erfüllen intelligente Zähler eine wichtige Rolle auf dem Weg zu größerer Autonomie der Endverbraucher. Mit Hilfe dezentraler Transaktionstechnologien wie Blockchain können sie für Direkthandel zwischen Produzenten und Konsumenten in sogenannten Peer-to-Peer-Netzwerken genutzt werden, die längerfristig in bestimmten Marktsegmenten sogar die Mittler- und Koordinationsrolle der Energieversorgungsunternehmen infrage stellen könnten.

Die dritte (und ambivalenteste) Sichtweise auf Smart Cities ist das *Narrativ der Kontrolle*. Mit dem Einsatz von technischen Instrumenten wie Sensoren oder Kameras können individuelle Verhaltensmuster aufgezeichnet und dokumentiert werden. Internationale Industrieunternehmen und Kommunikationsdienstleister arbeiten mit lokalen Behörden zusammen und stellen ihnen Ressourcen zur Datenverarbeitung zur Verfügung, die genutzt werden können, um die Sicherheit beispielsweise in Städten zu erhöhen. Sollten Hacker jedoch in den Besitz jener Daten gelangen, wäre es ihnen unter Umständen möglich, Lösegelder von Endverbrauchern zu verlangen oder Rechnungen zu manipulieren. Smart Metering-Geräte könnten als Einfallschneise in die Privatsphäre missbraucht werden, wie es bereits in Puerto Rico geschah: Dort wurde das lokale Energieversorgungsunternehmen mutmaßlich um hunderte Millionen Dollar geschädigt.

Während „EventHorizon 2017“, der ersten weltweiten Konferenz, die sich mit der zukünftigen Rolle von Blockchain im Energiesektor beschäftigte und Anfang 2017 in Wien stattfand, setzten sich namhafte Experten in einer Podiumsdiskussion mit Sicherheitsaspekten des Smart Meterings auseinander. Die dort vorgetragenen Argumente ergänzen den derzeitigen Diskurs insbesondere im Hinblick auf das Narrativ der Kontrolle.

Die Debatte zeigte auf, dass die derzeit gebräuchlichen Protokolle, die für die Kommunikation zwischen Energieversorgern, intelligenten Zählern und Haushaltsgeräten eingesetzt werden, nicht ausreichend geschützt seien, und dass es für Hacker zahlreiche Angriffspunkte im Bereich intelligenter Zähler gebe. Ein Grund hierfür sei den Experten zufolge, dass die Anreizregulierung für Verteilnetzbetreiber Kosteneinsparungen zu Lasten von Sicherheitsaspekten favorisiere. Zudem fehlten in Energieversorgungsunternehmen häufig

Fachkräfte, die die Gefährdungspotenziale hinreichend einschätzen und den von Subunternehmen durchgeführten Ausbau sachgerecht begleiten könnten.

In Anbetracht dieser teils unzureichenden Sicherheitslage stimmten die Experten überein, dass Regierungen ihre Bestrebungen deutlich forcieren und nationale oder regionale Institutionen aufbauen sollten, die die Umsetzung notwendiger Sicherheitsrichtlinien beschleunigen – möglicherweise Vorbildern aus anderen Wirtschaftsbereichen wie dem Bankensektor oder den Mobilfunkbetreibern folgend. Gleichzeitig sollten die Hersteller von intelligenten Zählern und Energieversorger als Betreiber der Geräte mehr Eigeninitiative zeigen und Sicherheitsaspekte stärker berücksichtigen. Zudem müssen Haftungsfragen geklärt werden.

Die Paneldiskussion zur Rolle der Blockchain ließ sich weitgehend dem vorherrschenden Narrativ der Innovation zuordnen: Blockchain habe als dezentrales Transaktionsprotokoll das Potenzial, Lösungen für einige aktuelle Schwachstellen bereitzuhalten – allerdings mit einer gewissen zeitlichen Verzögerung aufgrund des frühen Entwicklungsstadiums dieser Technologie. Es gab Vorbehalte, dass die bislang existierende öffentliche Blockchain zu langsam, zu energieintensiv und generell zu unhandlich sei, um in intelligenten Zählsystemen heute schon eingesetzt zu werden. Allerdings sei es nur eine Frage der Zeit, bis weiterentwickelte Blockchains die notwendigen Voraussetzungen bezüglich Transaktionsgeschwindigkeit und Energie-Effizienz erfüllten. Organisationen wie die Energy Web Foundation im Energiebereich oder Ethereum Enterprise Alliance und HyperLedger im industrieübergreifenden Kontext würden an diesem Unterfangen arbeiten.

Die Analyse der Podiumsdiskussion legt nahe, dass technische und digitale Innovationen ein zentraler Schritt in Richtung einer ausgereiften und weniger anfälligen Infrastruktur intelligente Zähler sind. Das Innovationspotenzial kann jedoch nur dann vollständig genutzt werden, wenn die Weiterentwicklung der Technologie von entsprechenden institutionellen und regulatorischen Rahmenbedingungen mit den richtigen Anreizen und eindeutigen Verantwortungen begleitet wird. Im öffentlichen Diskurs zu intelligenten Zählern muss dem Narrativ der Kontrolle jedoch mehr Aufmerksamkeit gewidmet werden, um Risiken und Gefährdungspotenziale für Endverbraucher, Energieversorger und die Netzinfrastruktur aufzuzeigen.

3 Introduction

In the year 2012, executives and regulators in the energy sector started to become aware of challenges related to the large-scale transition towards renewable, decentralized energy. A revolution started, which transforms the way how demand and supply of electricity are organized. Yet the energy community by and large ignored the disruptions that took place in other industries. In October of the same year, the European Central Bank released a report on "Virtual Currency Schemes", with a focus on blockchain and the so-called "Linden Dollars" used in the online gaming platform "Second Life" (European Central Bank 2012). In March 2014, the financial services industry, led by the Union Bank of Switzerland (UBS), acknowledged the benefits of blockchain technology, and explored the role of cryptocurrencies in the microcosm of monetary transactions (De Vries, Crutchley et al. 2014).

Over the last two years, the myopic concentration on the reorganization of the energy system has fundamentally shifted. Corporate players, startups and regulatory entities are increasingly devoting attention to new peer-to-peer trading mechanisms based on decentralized technologies, of which blockchain is both the best known and most popular (Buntinx 2017). It builds upon the advancements of information and communication technologies:

- Blockchain may serve as an IT infrastructure and platform to connect producers and consumers of energy in a decentralized system, especially the so-called prosumers, who own, for example, rooftop photovoltaic panels and want to sell their self-produced energy to peers and neighbors;
- Blockchain and other decentralized technologies thereby enable consumers to bypass incumbent utilities as the sole suppliers of energy services;
- Blockchain has the potential to enrich the spectrum of opportunities for market entrants from other industries, either incumbent players or startups, to expand their businesses into the energy market;
- Blockchain and other decentralized technologies may allow for efficiency gains in internal processes of cash-constrained utilities, and potentially offers new business opportunities for their strategic reorientation towards integrated service solutions (Burger, Kuhlmann et al. 2016).

Consequently, a spectrum of actors in (and beyond) the energy sector devotes considerable time and financial resources to explore blockchain as a potential game-changer of the energy system.

In February 2017, the first global conference on blockchain in the energy sector took place in Vienna, called EventHorizon 2017 summit. Over two days, representatives of relevant interest groups discussed how blockchain might contribute to the (r)evolution of energy business models. The conference served as a podium for visionaries as well as skeptics to voice their opinions about the future of decentralized ledger systems in the field of energy supply.

During the summit, one of the panel discussions focused on the security of smart metering infrastructure. As opposed to conventional meters called Ferraris meters, which simply track electricity consumption over a certain time span and have to be read manually, smart meters are equipped with a digital data transmission facility, which allows utilities to minutely track electricity consumption and send information to the supplier or grid operator. If a control device is added, utilities may remotely lower or switch off electricity supply to individual customers. Across all continents, smart meters are starting to replace the existing metering devices, with North America leading the rollout (IEA 2015). In the USA, the state of Maine leads in terms of percentage of households with a 97 percent adoption rate (Urjanet 2015). In the European Union, Italy and Sweden

have equipped almost all residential consumers with smart meters. The EU “aims to replace at least 80% of electricity meters with smart meters by 2020 wherever it is cost-effective to do so” (European Union 2017).

As smart meters are a core ingredient of the digitally enhanced electricity grid, smart grid and, more encompassing, the smart city, they belong to infrastructure systems commonly denoted as critical infrastructures, essential for societal well-being but prone to structural vulnerabilities. Numerous assessments and academic papers have analyzed the latent danger of the digitalization of the electricity system in this particular context (Ghansah 2009, ENISA 2012, Foreman and Gurugubelli 2016).

The panel discussion of EventHorizon 2017 focused on the question whether blockchain could provide technology and mechanisms to enhance safety features and prevent hacks of smart meters. In addition, the panel discussed potential use cases, as well as technical and institutional hurdles. It consisted of renowned experts in the field, namely

- Christoph Jentzsch, co-Founder of blockchain technology company Slock.it,
- Jan-Peter Kleinhans, IoT-Security Project Leader at the Stiftung Neue Verantwortung, an independent German think tank,
- Netanel Rubin, CEO of Israeli cyber security company Vaultra,
- Thomas Weisshaupt, Director for Smart Energy and IoT markets in the industrial segment for Gemalto, a leading company in digital security.

The panel’s moderator was Dr. Jens Strüker, Süwag Foundation Professor of Energy Management and director of the Institut für Energiewirtschaft (INEWI) at Fresenius University of Applied Sciences[1].

The full panel discussion has been recorded and is available online[2].

[1] More information on the panelists can be found in section 7 of this report.
[2] See Smart Energy Security Talk (hosted by PwC) - EventHorizon 2017, at https://www.youtube.com/watch?v=fXsCMrLMLz8

4 Smart meters and the three narratives of the smart city

Within the last decade, technology has fundamentally transformed our communication practices and social interactions (Castells 2009). With the rise of smartphone and internet services such as Facebook, Google, iTunes, Amazon or Uber, the distinction between private and public life gets further diluted. As we become more willing to share our location, our purchasing preferences, and formerly unobserved aspects of our lives – the so-called 'privacy paradox' (van Zoonen 2016, p. 474) – many commercial opportunities emerge to respond to individual preferences and obtain customized offers from companies that collect and analyze our personal data.

Our daily routines merge into a virtual, collective web of information. Still fragmented but increasingly multifaceted – mirror image of ourselves evolve in the cloud, our digital clone. Our car, house and fridge communicate with each other, we rely on social media for advice on restaurants, and we can plan our trips more effectively by assessing the trade-offs between different kinds of transport. With CCTV (Closed Circuit Television) and intelligent LED lighting, the city becomes a safer place. Early warning systems alert residents to take precautions before adverse local weather conditions may affect them (Singer 2012).

A smart infrastructure is the key building block for these developments. In particular, urban agglomerations with a high population density emerge as the pioneers in establishing so-called smart cities. They do not encompass only transport, safety, entertainment, and – as connecting element – communication, but also an increased participation and inclusion in local political decision processes (Rodríguez Bolívar 2015), education, and blended learning at the workplace (Huang, Zhuang et al. 2017). One key dimension of the smart city is energy (Maltese, Mariotti et al. 2016, p. 34). Energy provision turns from a unidirectional infrastructure service, typically delivered by a municipal utility, into a complex task of balancing and coordinating a multitude of producers and consumers. The electrification of private transportation and residential heating, which may occur with an increasing amount of electric vehicles and use of stationary storage in private homes, respectively, may contribute to a network of intelligent devices, potentially leading to neighborhoods or industrial areas with a high degree of autonomy. In a smart city, peer-to-peer trading is likely to occur among neighbors. Providers of storage facilities and commercial consumers participate in demand response schemes to shave peak demand, as an alternative to mandating new power plants. Similar dynamics may lead to a more interconnected system that technically depends on multiple access and aggregation networks ranging from private to public as well as wired to wireless. Smart metering is one of the most visible features of this development. One could imagine smart meters without a smart city, but not a smart city without smart meters.

An assessment of smart metering technology is hence embedded into the larger academic discourse on smart cities, which can be categorized into three complementary narratives[3]:

[3] As opposed to scientific theory, a narrative encompasses aspects of story-telling and a contextual construction of meaning, often characterized by an inseparability of facts and values. According to Lyotard, "scientific knowledge does not represent the totality of knowledge; it has always existed in addition to, and in competition and conflict with, another kind of knowledge, which I will call narrative in the interests of simplicity."

- **The narrative of innovation**

  The predominant narrative of smart cities focuses on the benefits that new technologies bring to daily urban life according to the European Commission (2013): "In Smart Cities, digital technologies translate into better public services for citizens, better use of resources and less impact on the environment." The concrete suggestion of this narrative is that smart meters – as part of the smart city – also contribute to improvement of living conditions (see e.g., ESMIG 2017). They enhance an individual's quality of life by providing transparent information about energy consumption, further facilitating fine-tuned tariff structures that correspond to personal preferences and habits. At the same time, they increase overall economic welfare by delivering tacit value derived from better knowledge about patterns of electricity consumption and improved coordination of end users. For instance, they collect and transmit information on the charging behavior of owners of electric vehicles, potentially saving hundreds of millions of dollars in grounding copper wire.

  Typically, the narrative of innovation is based on ordo-liberal ideology. This school of thought suggests that market economies in principle represent a superior form of coordination of economic agents than do planned economies. However, they need a "guiding hand" to steer them, namely to promote certain technologies (and more generally goods and services) that contribute to a higher quality of living and would not have been developed by industry without state aid, to set standards if competing systems delay adoption, and to intervene if dominant players abuse their power.

  Businesses and governments are not considered as adversaries. This is particularly evident in the way that cities, industries, SMEs, investors, researchers and other smart city actors complement each other and work hand in hand, for example in the rollout of the meters, creating a win-win solution for local residents, municipalities, and industry (EIP-SCC 2017).

- **The narrative of empowerment**

  The narrative of empowerment assumes the involvement of the (local) community in public policy and decision-making (Rodríguez Bolívar 2015, p. 5). Digitalization and social media allow citizens to actively participate in public discourse even without leaving their homes. They benefit from enhanced transparency in political decision-making. Accountability of their representatives increases vis-à-vis local, regional, national or even supra-national constituencies. The political system returns to its foundations of fundamental democracy and the ancient Greek notion of "agora" as a virtual public space of assembly, where each member of the community can be heard (Damiris and Wild 1997).

  Smart meters are a step towards consumer empowerment, enabling them to become an integral part of the electricity system. They both increase consumer freedom of choice and turn previously passive recipients of unidirectional energy services into conscientious members of the growing community of prosumers. Consumers are empowered to participate in the quest for a more sustainable energy future, based on the decentralized deployment of renewable energy sources.

  New transaction technologies such as blockchain allow consumers to circumvent the hierarchical, increasingly obsolete pyramid structure of energy distribution that traditional utilities still consider

---

Lyotard, J.-F. (1993). The Postmodern Condition: A Report on Knowledge. Minneapolis, University of Minnesota Press.

to be their main business model. They follow a blockchain-based energy perspective – characterized by peer-to-peer trading that relies on digital transaction platforms and independent, like-minded providers of these services, liberated of the administrative and financial burden of traditional distribution intermediaries (see e.g., Rutkin 2016).

- **The narrative of control**

  Whereas the two discourses centering on innovation and empowerment carry an almost completely positive connotation, the narrative of control introduces both caution and anxiety into the debate. Primarily expressed by sociologists (van Zoonen 2016, Sadowski and Pasquale 2015), it sketches the latent danger of the smart city's quest for total information control over the individual. Technical devices are able to monitor and record valuable data of each citizen's interests and habits, including transportation, health and biometrics, social relations and entertainment, and of course communication. A seamless urban web of constant surveillance, already implemented in some cities such as Dubai (Kumar 2015), protects residents' safety and security but also registers each move. In China, around 176 million surveillance cameras are installed, in the USA around 50 million (Hua 2017). Control centers and super-computers filter and analyze relevant information, and may recognize patterns that potentially intrude into an individual's sphere of privacy and autonomy. Large industrial players and IT service providers enter alliances with local communities and provide tools and capacities for Big Data analytics, for example between US company I.B.M. and the municipal authorities of Rio de Janeiro (Singer 2012), or Cisco and the South Korean city of Songdo (Chan 2016). In a less optimistic (but not entirely unlikely) scenario, individual data may be monetized by commercial entities, even without explicit consent of end users. In the worst case scenario, hackers may exploit the ease of access to one individual consumer's most sensitive information to commit criminal acts, such as demanding ransom or manipulating bills and accounts.

  Smart meters are not exempt from the perils to data security and privacy. They provide an important access gate into the secluded sphere of shelter and comfort of an individual's home. One may assume that tracking patterns of air-conditioning or washing machine use is a relatively trivial type of observation of no value to potential intruders into the privacy of individuals. Researchers at the Universities of Applied Sciences in Münster and Rhein-Waal have demonstrated, though, that even micro-differences in the energy consumption of modern TV sets can potentially be used to deduce information about the TV program watched: "Smart meters are able to become surveillance devices that monitor the behavior of the customers. […] Our test results indicate that a 5 minutes-chunk of consecutive viewing without major interference by other appliances is sufficient to identify the content." (Greveler, Glösekötter et al. 2012)

  The narrative of control builds on the ambiguity of the privacy paradox: On the one hand, services obtained by revealing personal data allow for greater safety, more informed choices, and comfort. On the other hand, information about the individual might be exploited by corporate players or public authorities without explicit consent.

The three narratives allow for different interpretation of smart metering devices: They can serve as an enabler of autonomy (freedom of choice), source of additional income and a means to contribute to sustainable use of resources, but they can also be exploited as a means of control, surveillance and illegal intrusion into the privacy of one's home.

While the narrative of innovation dominates the public debate with an optimistic and somewhat commercially driven belief in technology as a constant enabler of progress, the panel discussion held at EventHorizon 2017 concentrates on the third narrative of control. In particular, deficits in the security and safety of currently available smart metering devices, and the role of setting the right incentives for manufacturers, operators, and consumers are elaborated.

5 What are the vulnerabilities of a smart meter infrastructure?

In a smart city, smart meters are the connecting points between the public and the private sphere. Many residential consumers in rural or suburban areas have transformed themselves into prosumers, generating power via photovoltaic panels on their rooftop, and they may become an even more integrated part of the electricity system once these households are equipped with stationary batteries or electric vehicles whose batteries may be used for ancillary services and secondary balancing markets. In more densely populated agglomerations, real estate developers or housing associations incorporate PV systems into new multi-party dwellings, and residents benefit from a partial reduction of their energy bill. In all topographic conditions, smart meters are the communication devices used as gateway between households and the electricity grid – both in terms of electricity flows as well as information flows. They can even help grid operators to detect bottlenecks in the distribution grid and to prevent thermal stress in cables.

Netanel Rubin, co-founder and CEO of Vaultra, a cyber-security start-up that aims at revolutionizing the Smart Energy industry and critical infrastructure security field, highlights two fundamental differences between the old and the new generation of electricity meters: “Compared to a conventional Ferraris meter, a smart meter has two additional features: It can communicate with the utility remotely, and with the consumer home appliances and devices. The communication with home appliances is just the first step, because in the future smart meters are supposed to communicate with the cities’ smart devices as well.”

The shift from a “basic” to a “smart” meter, from a “basic” electricity grid to a “smart” grid coincides with the rise of the internet as the encompassing domain of our digital economies and lives. Electricity consumers are able to participate in the electricity market, and the “internet 2.0” has become reality. Everyone with internet access can upload photos or movies on social networks. Beyond entertainment and communication with friends and family, the internet increasingly serves as a platform and vehicle for trade and financial transactions.

In addition, it becomes the main communication infrastructure in the “Internet of Things” (IoT), where devices autonomously communicate with other devices to perform programmed actions. For example, a sensor in the fridge recognizes that the last bottle of milk has disappeared and automatically sends a message to the computer in the supermarket to add milk to the list of items for the next delivery. As Rubin explains: “Smart cities are emerging all over the world, in Amsterdam, Singapore, Barcelona. Together with transport, communication and other infrastructure services, smart energy solutions are typically an integral part of the concept of smart cities. Smart energy can be understood as a better understanding of the utility, of its consumer and of its municipal authorities, the cities themselves.”

According to Rubin, utilities can gain from these smart revolutions: “Smart meters are offering great power for energy utilities. They can define different tariffs for different hours, can connect and disconnect power remotely, and receive information about electricity usage instantly. In general, they have better control over their electricity grids. What makes this revolution smart is the smart meter.”

For Rubin, it seems logical that utilities are forcing smart meter installations all over the world. “There is a lot of positive regulation all over the world, in the Middle East, Australia, Japan, even in the USA. Currently there are over 100 million smart meters worldwide that can communicate both with the utility and with consumer home appliances.” The European Union, though, is the key player: “The region with the most progressive regulation in the industry is the European Union, which aims to replace at least 80 percent of its conventional electricity meters with smart meters by 2020. This has created an exponentially growing market. Almost all countries of the European Union are in the process of mass rollout of smart meters.”

While some members of the EU have embarked on a fast deployment of smart meters, like Italy or Sweden, other countries favor a more incremental approach, such as Belgium, the Czech Republic, or Germany, where the rollout may even be stretched until the year 2032. Irrespective of the speed, the progress towards a full rollout of smart meters seems irreversible in most countries.

5.1 Smart meters as risk for a critical infrastructure

Together with transport, water supply and telecommunications, the provision of electric power is considered a critical infrastructure service. Its interruption can cause major economic damage - and even human losses. All critical infrastructures have inherent vulnerabilities. These might be external, such as a storm hitting transmission lines, or internal, for example an accident in a power plant. With the rollout of smart meters across the globe, an additional element of vulnerability of the electricity grid has to be taken into account, when the new devices replace the robust and reliable Ferraris meters. “The problem starts when a product is forced by governments and is basically everywhere, when it gains access to both the consumer and the utility’s internal network”, states Rubin. “The smart meter has critical access points and may be insecure out of several reasons: First of all, there is the privacy breach. If someone gains control over it, one can access the data the consumer has. One could also change the billing amount, a kind of billing fraud. On the utilities’ side, the smart meter may serve as an access point to a utility’s private network, and hackers could potentially communicate with its most critical assets. If they shut down several hundreds of thousands of meters at the same time, the balance of demand and supply in the electricity grid could be severely jeopardized. For example, in Puerto Rico smart meters were hacked. They failed to record the electricity consumption correctly, and the utility lost USD 400m by just getting hacked.”

There are several ways how attackers could gain control over the smart meter. In its most simplistic form, this can be done mechanically, by changing the wiring. Rubin comments: “But this takes a lot of time, there are a lot of hardware safeguards and protections, and hackers are not necessarily favoring that approach. Then there is a wireless way, using protocols such as Zigbee or GSM. For the communication with the utility, the smart meter uses the GSM Protocol, for the home appliances it uses the Zigbee protocol. Attackers can actually use GSM by themselves, unless the code is encrypted. For example, five years ago a group of German hackers gathered sensitive data about consumers. However, most of the time information flows are encrypted.” Rubin points to one fundamental weakness: “When the smart meter is initialized on its first run, it tries to communicate with some hard-coded credentials. Using these credentials, the utility can check whether the meter is viable or not. If it is viable, it sends back the encryption key in order to start communication. If attackers use their own base station and force the meter to connect to them, they will get the credentials and also the network encryption key, which allows them to communicate with the meter themselves. This attack can be extended to all meters by using the same credentials in the same network. In other words, if attackers gain access and are able to extract the network key from one single meter, they can potentially take over the entire network.”

According to Rubin, this could be avoided if there were safe encryption codes, segmentation and monitoring in the network. However, as he warns, “currently the smart meter network is completely exposed, because it lacks any of those features.”

In the home area network, Zigbee is the standard protocol, designed in 2003. Rubin explains why the system was developed without serious means of protection: “More than a decade ago, questions of information security were not as important as today. There are hundreds of different appliances using that protocol, with 15 different flavors, such as Zigbee Home Automation, Zigbee Healthcare, Zigbee Smart Energy.” According to Rubin, there may be weaknesses in the design, the implementation as well as the management of the protocol: “With regards to design, Zigbee is encrypted, as opposed to live screen GSM, but when a device joins the network, the smart meter sends the network keys to whomever wants it. In addition, there is so-

called hub impersonation. If hackers use the keys, they can impersonate themselves as the hub, or the meter, and try to communicate with any type of smart appliances, be it the air-conditioner or the door lock – it does not matter! If the device communicates with ZigBee, hackers can communicate with it. Furthermore, they can also inject themselves as new devices into the network, start communicating with smart meters and hack them. With regard to the implementation of Zigbee, one has to understand that smart meters do not have a lot of CPU power and are very low in memory. Most of the times vendors are skipping all sorts of security checks. That results in memory corruptions inside the meter's software. If hackers successfully exploit one of those memory corruptions, they can take over the meter. If they do not want to hassle with the memory, they can just use one of the hard-coded credentials in the meter, which are exactly the same for all meters of the same model. They can use these credentials on the debug-ports, and on the GSM network. If they get access to one meter, they can take over all of them."

In addition, Rubin identifies possible exposures in the protocol encryption: "In addition, there is also bad implementation of encryption: Even if the encryption is 128 bits of key, it is actually derived out of 48 bits of manufacturer code. So the implementation itself reduces safety." He emphasizes the role of encryption in securing the smart meter: "Encryption is as strong as the device that is using it. Once a device is hacked and the encryption keys are stolen, the encryption is not worth anything. Unless we secure the entirety of the meter, we cannot really expect encryption to do the job for us."

5.2 Lack of right incentives for utilities

Thomas Weisshaupt, founder and chairperson of the privacy and security working group of the smart metering industry, who serves as Director of Smart Energy Markets and IOT at Gemalto, emphasizes that a smart meter is a device located in a hostile environment: "It is not in a server room, and not in a closed environment. Theoretically, everybody can approach it, retrieve the keys and do whatever they want." According to Weisshaupt, the fundamental problem does not lie with the device manufacturer or vendors: "The key challenges are the tenders of the utilities and the governance that we have in smart metering in Europe."

Weisshaupt recounts a tender for several million devices that contained a single statement about security, which noted: *"You have to use state-of-the-art security."* He criticizes this approach: "That is the mentality and the key problem of utilities: They are using their traditional metering departments to do smart metering, which is an IoT (Internet of Things) implementation. It rather belongs to the innovation department."

Rubin agrees that the utilities' approach to smart meters does not take precautions regarding security: "What are utilities doing wrong? First of all, some of them are still using plain information protocols. If they do not have encryption in your communication, they are simply allowing hackers to take over the entirety of the data and their network. They have to encrypt everything. Also, there is no endpoint security. Currently utilities are not implementing any kind of security solution inside smart meters. They are completely exposed. Worst of all, there is no monitoring over the network, neither Zigbee nor GSM."

Weisshaupt stresses an additional weakness in the utilities' approach: "First thing they do is to decide about the communication network, which is supposed to be low-cost. This decision is cost-driven. They go for Zigbee, 2G, and so on. There is a plethora of communication protocols around. Luckily in Europe, the majority of the implemented and the planned meters do not have this home interface. Only a few rollouts in the UK and two or three others have this home interface, whereby you can conquer the home."

A manager of the smart metering rollout of one of the largest utilities in Europe has told Weisshaupt the following: "We planned this in 2007, now we are rolling out in 2014, but the technology and design are from 2007. A secure element in each meter would cost 43 million Euros. You tell it to our customers!"

According to Weisshaupt, utilities are incentivized in capex (capital expenditures), not in opex (operational expenditures): “They are encouraged not to consider risks, because in a regulated environment their financial liability is limited as long as they are compliant. They still exist as a regulated entity.” After the installation, the question for Weisshaupt also becomes how to manage these protocols and keys over the life cycle of the device: “Because the life cycle of the device is now longer than the life cycle of the network. Zigbee in eight years – I do not know! 2G in eight years – not sure! LTE in fifteen or twenty years? How do we manage that? Motivation and incentives are currently lacking, because we define a set of processes based on today’s requirements that need to be fulfilled by an infrastructure literally unchanged over its lifetime. When we design an infrastructure for these particular processes, we fix these processes for minimum five years via regulation, but innovation is incentivized.”

The role of incentives is also vital for Jan-Peter Kleinhans, IoT-Security Project Leader of the think-tank Stiftung Neue Verantwortung: “If we look at blockchain and IoT, it is often about opportunities, potentials and business models. This is understandable, because we are in the starting phase. But only ten percent are about security, and of these ten percent ninety percent are about technology, and what is left is about incentives.” He sees deficits in incentives as being part of a wider phenomenon across all areas of the Internet of Things: “The market failure regarding IoT security, which is happening right now and is true for the entirety of IoT is because of the lack of incentives. We have very good technology, we have strong encryption for years, even for decades, we know how to handle public key infrastructures, how to implement secure devices and to securely store keys. But it just took 61 standard logins and passwords in September 2016 to create one of the largest IoT botnets[4], consisting of hundreds of thousands of devices, to then bring down big companies or randomly attacking journalists and websites through a denial-of-service attack.” (for more information, please see US-CERT 2016)

Kleinhans also finds the mindset and incentive system to be cost-driven rather than than security-driven: “The reason for the market failure is that companies that focused on a completely different aspect for decades – in smart metering it is physical safety, temper-proof – are suddenly connecting their devices, and they are treating security as a feature that nobody pays for. They are not investing in it. To securely implement a smart meter to the network, I would need to hire many specialists to take care of the security aspect. But nobody pays for that. We need to think about positive and negative incentives for companies to treat security not as a feature but as a requirement.”

These remarks of the panel discussion lead to the hypothesis that the utilities’ lack of investment may rather be a *symptom* than the *cause* of concern – hinting towards a more deeply rooted, underlying question: How much money is contemporary society willing to spend on cybersecurity?

5.3 Accountability for smart metering risks

Jens Strüker, the moderator of the panel and Süwag Foundation Professor of Energy Management at Fresenius University, inquires whether the regulatory model in Germany and the UK might provide the appropriate incentive structures, because these are the only two countries in Europe with a deregulated smart meter operator: “In most cases, the meter operation belongs to the grid operator, but in these two countries this is deregulated. What are the consequences? The electricity supplier could enter the meter operation, for example to retrieve data or to avoid balancing energy, etc. It would make economic sense, but what would happen with security on the smart meter level?” Strüker explains his rationale: “If there is an incentive to make use of the data, they might be careful about the data. In the deregulated setting, there may be an opportunity to obtain data from customers, to work with them and offer new tariffs, etc. The damage that can happen after

[4] Botnets may perform a distributed denial-of-service attack (DDoS attack) or other malicious actions by allowing the hacker to access the device of a user.

a breach may lead to more careful behavior at that level. In other countries, where the meter operation belongs to the grid operators, these operators have no incentive at all to increase the security level."

Kleinhans is skeptical with regards to this solution: "Giving electricity suppliers the opportunity to harvest data and gain more insights via the data, does not mean that they will treat it with the utmost importance. We see that all across the board with hacks from Yahoo, LinkedIn, Adobe, MySpace, etc. It is all about liability: Who is taking the blame when something goes wrong? If there is the connection via blockchain between the electric grid and the information grid, it implies that every electric appliance can be hacked and is exposed to all the attack vectors that we see in the information network."

In that case, according to Kleinhans, "the smart home thinks that there are no longer credits available to pay for the electricity, while the electricity company sees that there is no transaction any longer – so: Lights out!" This creates a completely new dimension of vulnerability: "Suddenly one specific home can be attacked, which was not possible in the old energy grid. This was one of the big advantages of an analogue grid: One cannot target a specific home. It would be hard to take down the energy grid. All the instances that happened so far were state-sponsored. They were intelligence agencies, for example in Ukraine, which targeted the power grid. In fifteen years, ransom-ware may lead to a denial-of-service in one's home. Hackers may not stop, for example, until twenty Bitcoins are paid. One can already order these attacks as a service right now in the internet, but who is taking the blame for that? Is it my personal responsibility as a private person? I would have to have another private insurance against electric grid ransom-ware? Or is it the responsibility of the grid owner, the grid operator, or the smart meter manufacturer?"

Kleinhans sketches out the following scenario: "What happens if someone installs a malware on my smart meter, and for every Bitcoin transaction there would be 0.1 percent of the transaction that is going into a different Bitcoin wallet? Users may not realize that because their pre-paid contracts just finishes a little bit quicker, and after two years they realize that they had a malware installed, and they actually lost three Bitcoins over the course of two years – which is a hefty amount of money! Again, is it your private responsibility to double-check your smart meter software every day and to read your logs? Who would be liable?"

The following section summarizes the vulnerabilities and threats identified by the panelists.

5.4 Key takeaways: Vulnerabilities

Insights from EventHorizon 2017 panel experts reveal severe vulnerabilities in the implementation of the smart meter rollout. In particular, the following weaknesses pose a threat to grid infrastructure and final consumers:

- → Protocols for communication with the utility and for the communication between smart meters and home appliances are structurally exposed to attacks by hackers;
- → Utilities follow an adverse incentive system that focuses on cost-savings rather than security; they also often lack the personnel to properly assess the risks;
- → Detaching smart meter operations from the accountability of the grid operator, as it happens in Germany and the United Kingdom, is not likely to increase security and improve incentives;
- → If an attack occurs, it is still unclear who is accountable and liable.

6 What is the potential of blockchain for enabling security?

As a transparent and decentralized transaction technology, blockchain may be able to provide the security that is missing in the design of many smart meters today. But is blockchain ready to be used as a communication protocol in the electricity grid? First pilots in peer-to-peer trading are already under way, led by startups Power Ledger from Australia, Grid Singularity from Europe and Lo3 from the USA. However, a large-scale deployment and standardization is still pending. One organization making palpable progress in this direction is the Energy Web Foundation, which has been set up with this mission in early 2017 and launched a test network in October 2017.

Christoph Jentzsch, co-Founder of blockchain startup Slock.it, explains the benefits of blockchain compared to other communication technologies: “Single points of failure can be avoided. When they are distributed, an attacker would have to hack each single device to obtain each single key. In addition, they talk to each other over this decentralized blockchain, which does not have a single point of failure, too, for shutting it down. That is why there is such a good fit between blockchain and smart meters.”

“The real benefit of blockchain is that the protocol and network themselves already have security implemented”, adds Kleinhans.

6.1 Private and public keys in blockchain

One of the main features of blockchain relates to the so-called “keys”. They can be differentiated into private and public keys. While a random private key, for example in a Bitcoin transaction, is a secret number that allows Bitcoins to be spent, a public key can be calculated using the private key to compute the corresponding public key, which can then be given out and used for verification. Applied to the electricity network, “the private keys will be securely stored in devices such as smart meters and cannot be read out”, according to Jentzsch. “Those devices should be able to act autonomously. They should be able to send messages, sign transactions, etc. The public key can be known to everyone; it is the ID of the device. It can have messages, for example about energy consumption, send it out to the utility, and sign it with the private key. Then the utility can be sure that it was signed from this device, because it is impossible that the key has been somewhere else. When we think about the smart meter revolution, it is important that the smart meters have securely stored private keys inside, so that they can interact with the outside world.”

Jentzsch refers to uPort, a self-sovereign identity system built on the Ethereum platform: “A smart proxy contract serves as the ID. Then there is a second smart contract, which is a governance contract and for example states who can back up the keys. If this one gets hacked, there could be a smart contract, which allows a specified number of owners to exchange the keys. In other words, the ID is the proxy contract, and the governance contract determines who can forward messages to it. One key could be stored at the utility, while another key could be in secret with home-owners. We have the promise of being very secure, and we should not be too afraid of building on this at all. When we look now at Smart Contracts, they need to be as simple as possible. We are also making significant progress in the form of proof application, where one can check whether the contracts actually do what they should do. But we need more experience, with such a new technology we do not know the ‘unknown unknowns’.”

Weisshaupt sees the potential of blockchain in its flexibility: “Processes were fixed, and infrastructure was designed to cost. There was no flexibility to do something. Now blockchain has the potential to flexibilize the

processes over the life cycle of the product. Each device needs an identity to publish data in the blockchain, as close to sensor and encryption, because blockchain transactions mean data, which means money."

In this context, Jentzsch indicates a number of questions to which the community does not yet have a concrete response: "Who has the keys? What is the governance model? We should take it step by step and be cautious when we develop those systems."

6.2 Readiness of public and private blockchains

Besides public and private keys, there is a distinction between public and private blockchains. A joint characteristic is that they are both decentralized peer-to-peer networks. "The sole distinction between public and private blockchain is related to who is allowed to participate in the network, execute the consensus protocol and maintain the shared ledger", according to IBM (Jayachandran 2017). "A public blockchain network is completely open and anyone can join and participate in the network, [whereas] a private blockchain network requires an invitation and must be validated by either the network starter or by a set of rules put in place by the network starter." (ibid.)

Jentzsch sketches the reasons why private blockchains are popular among companies: "Currently the main reason for using private blockchains are scalability and privacy. These two issues are not solved in the public blockchain. A private blockchain is a good first step to get to know the technology, but it is not that revolutionary. We will see private blockchains in the beginning, but they also have to be secured with firewalls and tunnels – all the features that big utilities already have installed today to secure their networks. The same features are needed to secure their private chains. A private blockchain is not so different from a SQL database, it is just equipped with a better permission system."

According to Jentzsch, timing is the crucial factor: "When is the time ready to deploy something? For example, Bitcoin is good for payment. One has to pay a high transaction fee, but it is pretty resilient to whatever is happening to it. Ethereum is also getting mature right now." However, if millions of residential consumers are affected by the technology, he expresses reservations: "If one thinks about all households, then one would have to say: 'No, this public chain is not ready to take this amount of risk or assets on it right now!' Private chains can of course be used for this, they can be made secure, but then we have the same problems as of today, one has to secure those networks. They do not give that huge advantage that the public chains provide. The public chain would solve these issues, but it is not yet ready 'for prime time'."

Another reason for Jentzsch' caution is scalability and the switch from the consensus mechanism proof-of-work, which is energy-intensive and lengthy, to the more efficient and lean proof-of-stake: "Proof-of-work is most commonly used in public chains like Ethereum and Bitcoin, but Ethereum is planning to move to proof-of-stake, which allows for gaining scalability and stop wasting energy. Do you know how much energy these proof-of-work chains actually consume? Ethereum is about one nuclear power plant right now! Proof-of-stake is a very important way to reduce the energy consumption of the chains."

As cryptocurrencies such as Bitcoin move from a niche to become mainstream financial instruments, they increasingly shift into the focus of potential attackers. "There is a clear incentive for a hacker to target smart meter protocols. Bitcoins and other blockchain systems are already of interest for hackers, because once they capture the Bitcoins they really own them. Therefore these systems need a lot of protection", comments Jentzsch. "Beforehand, we just had payment providers, banks that took care of this. If there is something wrong in their database, they would fix it, we do not feel it. But with programmable money, there could be something in the Smart Contracts or in the software that does something strange, and it may affect thousands or millions of houses."

There are possibilities to protect the system from ransomware that might affect final users, according to Jentzsch: “The solution could be a monitoring system that checks what is going in and what is going out, because in the blockchain everything can be seen, which can be completely independent of the smart meter. The monitoring system could send me a message if it detects something strange happening.

The following section summarizes the statements by the panelists regarding the application of blockchain protocols in smart meters.

6.3 Key takeaways: Potential of blockchain

Insights from EventHorizon 2017 panel reveal that blockchain technology may not yet be sufficiently advanced to accompany the smart meter rollout. In particular, the following weaknesses pose a hurdle in the implementation:

- → Private blockchains allow for scalability and privacy, they are ready for deployment in smart meters, but they do not provide the benefits of public blockchains regarding safety and transparency;
- → A public blockchain would most likely have sufficient control mechanisms to secure the meters, but it is still not ready for large-scale deployment, most importantly because it is time-consuming and energy-intensive;
- → The next generation of blockchain protocols should resolve these issues, including using proof-of-stake (and proof-of-authority) consensus building mechanisms.

7 How should future regulation be designed?

Having outlined the challenges and vulnerabilities of the current smart meter design it becomes obvious, according to Rubin, that "something has to change." As he elaborates, "we can change the infrastructure, make it more resilient to cyber-attacks, make it more cyber-proof. We can change legislation and force utilities to improve their security using regulation. Alternatively, we can change technology, for example by using a decentralized architecture."

The outlined options are not mutually exclusive but complementary. As Jentzsch states, governance becomes the vital issue: "Who is governing those chains? Who can make protocol changes? If we build a solution for utilities in the energy market, who can make a governance model behind it? Is it completely without any governance structure? It would be created and deployed once, but it would have to be made perfect not to be governed. The alternative is that users, utilities, or maybe government, regulators have a say in governing those Smart Contracts or the protocol we are building. This is the most challenging question, because it is unclear whether all these parties would be able to come to an agreement about how to govern those systems."

When Jens Strüker, host of the panel, asked the audience about the future role of regulators, almost half (48%) of those who participated in the poll (206 persons in total) considered that regulators will certify smart contracts in the future. Only 7% of the audience believed that regulators will disappear, while 16% believed that they would be replaced by robots[5].

7.1 Standard setting by public authorities

In most countries and regions like the European Union, the smart meter revolution is a top-down directive imposed on utilities and consumers. "The regulations are already in place," comments Rubin. "Most of the countries in the European Union have to replace their meters with smart meters, but no one is talking about security, no one is regulating security. Unless there will be some regulation, we cannot really force utilities to implement better security!"

Weisshaupt refers to Germany as an example of this top-down approach: "In Germany, the government was slamming the hammer on it and issued a protection profile, considering privacy, doing a risk analysis, and doing a technology definition. It is of course not clear whether this is the wish of everybody."

Kleinhans points to parallels in internet regulation: "Right now in the internet there is no security on the protocol level and the network level. Security needs to happen at the edges. This is why there are so many screw-ups and problems in the internet. Every single manufacturer and vendor can screw up; they are screwing up, and they will continue to screw up until we shift IT security from a feature to a requirement. Requirement means legislation and mandatory baseline standards. But this is tricky and hard to get it right and get a good balance."

However, defining standards may lead to a lock-in effect with suboptimal solutions, according to Kleinhans: "Different institutions and governments, such as the European Commission and the Department of Commerce in the USA, but also the German government, are talking about these incentives in general for IoT, but of course with a strong focus on cyber-physical systems, for smart meters, automotive, and so on. They are thinking in classical client-server terms, about very specific things such as two-factor authentication, end-to-

[5] See also the presentation on results of the EventHorizon polls and surveys that can be downloaded on the EventHorizon 2018 website https://eventhorizon2018.com/.

end encryption, etc., which are best practices right now. That is good and should indeed be implemented, but I am afraid that they are blocking the way for future technologies, stronger protocols and systems."

Kleinhans is skeptical about government involvement in technical definitions and standards: "Generally, governments are not good with coming up with technical solutions, and they should not! But they are very good in thinking about the right incentive structure and responsibilities. Sadly, they are not doing this right now."

7.2 Incentive design

Governments have the right and the obligation to formulate standards and create incentive systems in case of market failures. Incentives may affect all parts of the value chain, starting from device manufacturers to vendors, and utilities.

Kleinhans sees fundamental differences in smart meter security concerns, compared to, for example, a personal laptop: "If we think about responsibility and liability, it is about how much freedom do we have? The personal responsibility for my laptop is much higher than for a smart meter, because I have full control over the laptop. I can change the software; I can make it more or less secure with software. It is decoupled. The entire software can be changed without having access to the hardware. The smart meter is quite different. If the smart meter manufacturer screws up, I cannot patch it with my own software to make it more secure. It does not work. I literally have to wait until the smart meter manufacturer updates the system. We see that right now especially with routers and in the consumer IoT market. Almost every month there are new Zero-day exploits for home routers. Often the recommendation is: Until there is a new firmware update for your specific router, one should better not use it. If we call ourselves a digital society, that cannot be the right solution! To wait until the manufacturer offers a firmware update, and then blame the customer who is not quick enough and does not understand the right update mechanism, and by updating your software voiding your warranty. The entire system does not make sense in terms of responsibility and liability. As soon as one hands over control of a certain smart device to the manufacturer – and in smart meters this is definitely the case – because one has Zero control of what the device is doing, then I see all the liability with the manufacturer or the grid provider."

One way to overcome the lack of incentives could be to create alliances along the value chain, according to Weisshaupt: "A motivation for the vendors of these devices to implement very strong authentication could be that they could also be application providers with the blockchain, going e.g. with companies like Slock.It."

Weisshaupt further suggests that device makers should be incentivized to insert the appropriate credentials and security mechanisms: "The security implementation is a side effect of a business model. If you have something to lose, you implement it." But the business model is in most cases linked to the utilities that are installing and operating the meters. "Utilities are of course considering the problem. The challenge now is that the cost-benefit analysis changes, and this analysis is the economic basis for the rollout in Europe. Meanwhile, in the USA there are some managers of utilities who cannot sleep at night because of this problem. They do not know what to do."

Rubin criticizes the *laissez-faire* attitude of many utilities: "Utilities really have to step up there. They are the ones that install smart meters everywhere. Sometimes they do not even ask their consumers if they want a smart meter. They have to be the leader in that regard. They need to implement better security in their networks, they are responsible, because they are the ones who are getting hacked while we are paying the price. They should be the first ones to implement security."

7.3 Learning from other industries

Role models of successful implementations of institutional safety frameworks can be found in many industries. Often, these institutions have been established as initiatives of major industrial players sharing a common interest, for example fraud prevention.

Weisshaupt contributes one real-world example from the banking sector: “It is not IoT but payment terminals: If you are around the globe and have your credit card you trust the machine more than the person behind the counter. The bank is reliable if something goes wrong. The banks all over the globe have an interest in defining the security requirements for these payment terminals, including a certification environment. There are institutions in charge of this, and I strongly recommend seeing the patterns of these institutions, of how this evolved, and how the incentive structures are. This is not secure, but the banks have a trade-off: If a hack happens, the damage is like this, and the counter-measure would cost us this. The overall system is still more profitable than cash. One could see it in the USA: Within half a year they gave up the resistance against this chip and pin after two or three supermarkets were hacked. So the reactivity of these private institutions, where liable partners have ‘skin in the game’, the security evolves, because it is an economic factor.” Weisshaupt suggests rapid action: “We have to speed up and not create working groups on the commission level, and have 27 different architectures within Europe, 50 different architectures in the USA. Let us admit, we have a problem, and let us solve it together!”

Weisshaupt also observes tendencies to create global institutions among mobile operators and even utilities. “My main advice would be to have joint initiatives on utility-level, such as the European Network of Cybersecurity, which was founded by large utilities in Europe. It is a somehow independent research institute helping the utilities to define security requirements. Then they can start thinking how the rollout could look like. For the energy space we need that kind of institutions to be involved – and not a technology definition from the government, or ticking the box on security as of today.” This is the approach taken by Energy Web Foundation, which was legally incorporated in early 2017, just weeks before the EventHorizon 2017 conference.

Rubin sends a message to the audience at the summit: “The key to making all of this happen is to inform the public. We as the security community, as security vendors, as blockchain startups and companies and organizations have the power to approach the public and broadcast our message as hard as possible. We can give you the power to retake control. We can allow you to reclaim your home. So reclaim it – or someone else will!”

7.4 Key takeaways: Future regulation

The call for action concerns all parties involved in the rollout of smart meter infrastructure:

- → Governments and regional authorities should set up institutional structures that accelerate the process of establishing safety guidelines; however, they should refrain from defining technical standards;
- → Both device manufacturers and electric utilities as operators of smart meters have to be in charge of appropriately addressing security issues, since final customers cannot exert control over their smart meters;
- → Players in the electricity sector should learn from other industries, such as banking or mobile operators, and implement their best practices in successful institution-building efforts.

8 Conclusions

The narrative of empowerment

Smart meters will become an essential part not only of smart cities, but – sooner or later – of each household with access to a central or local electricity grid. With continuous technical enhancements, they will empower consumers to choose flexible tariff systems, to actively participate in the electricity system, and to save energy. If decentralized ledger technologies are implemented, there may be multiple paths to enable consumers and prosumers of energy to organize financial transactions and physical electricity flows with or without intermediaries such as utilities.

The rollout of smart meters also represents an opportunity of empowerment for utilities or local grid operators. Under favorable legal and regulatory conditions, they would be able to use data on their users' consumption patterns to optimize electricity flows and long-term network investment strategies. It is the task of regulatory bodies to define a transparent legal framework for how critical data can be accessed without jeopardizing privacy issues, and to formulate incentives for all actors to accelerate the technical rollout.

The narrative of control

The panelists issued a warning that the current safety configuration of smart metering devices is not sufficient; in particular communication protocols between smart meters and home appliances and with the utility expose them to the risk of attacks by hackers..

The electricity network as a critical and vulnerable infrastructure has moved from a collective to an individualized asset, exposing private residents to selective attacks and financial harm. These risks stem from a lack of appropriate financial incentives for utilities to increase security of the devices, coupled with human capital constraints in their existing workforce.

Under the current regime and the cost pressure, regional grid operators and utilities organize the mass rollout, in some cases with antiquated standards. Are their experts prepared to cope with vulnerabilities of smart metering infrastructure? Is the current regulatory framework sufficient to ensure an adequate protection against exposure to illegitimate attacks? For the panelists, the most urgent step is to establish an incentive system for both manufacturers of smart meters and utilities, which addresses appropriate safety requirements and liabilities.

Governments should refrain from defining technological standards, though. This task should be accomplished by consortia of private actors with an intrinsic interest to protect the system – analogous to self-regulation of fintech, for example, where private companies congregate and constantly update global standards. They can react more flexibly to technical progress and potential threats than governments.

The narrative of innovation

Can blockchain provide a remedy against these vulnerabilities in smart metering infrastructure? In principle, the experts in the 2017 EventHorizon panel were optimistic, but presented two major caveats:

- The public blockchain is still too slow, energy-intensive and inconvenient to be used in today's smart meters, with progress under way to tackle these issues and develop more efficient decentralized protocols. Advances in transaction technologies will make it very likely that in the near future the public blockchain will have all the capabilities to fulfil requirements in terms of energy efficiency and speed;

- Private blockchains can be successfully deployed already today, but their additional benefits compared to conventional systems are relatively low, in particular with regards to transparency.

In conclusion, technical and digital innovation will take the lead in rendering smart meter infrastructure more sophisticated and resilient, but it has to be accompanied by the right institutional and regulatory framework.

References

Buntinx, J. (2017). Distributed Ledger Technology Vs Blockchain Technology, themerkle.com. 2017.

Burger, C., et al. (2016). Blockchain in the energy transition. A survey among decision-makers in the German energy industry. Berlin.

Castells, M. (2009). The Rise of The Network Society: The Information Age: Economy, Society and Culture. Hoboken, New Jersey, Wiley-Blackwell.

Chan, S. (2016). "Innovation has the smart city of Songdo living in the future." Retrieved 14 Nov, 2017, from https://newsroom.cisco.com/feature-content?articleId=1738492.

Damiris, N. and H. Wild (1997). The Internet: A new agora? An Ethical Global Information Society: Culture and democracy revisited. J. Berleur and D. Whitehouse. Boston, MA, Springer US**:** 307-317.

De Vries, D., et al. (2014). Bitcoins and Banks: Problematic currency, interesting payment system. Global Research, UBS Securities.

EIP-SCC (2017). "The Market Place of the European Innovation Partnership on Smart Cities and Communities." Retrieved 14 Nov, 2017, from http://eu-smartcities.eu/.

ENISA (2012). Smart Grid Security: Recommendations for Europe and Member States.

ESMIG (2017). "Benefits of smart meters." Retrieved 14 Nov, 2017, from http://esmig.eu/page/benefits-smart-meters.

European Central Bank (2012). Virtual Currency Schemes. Frankfurt/Main.

European Commission (2013). "Smart Cities." Digital Single Market. Retrieved 14 Nov, 2017, from https://ec.europa.eu/digital-single-market/en/policies/smart-cities.

European Union (2017). "Smart grids and meters." Retrieved 13 November, 2017, from https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters.

Foreman, J. and D. Gurugubelli (2016). Cyber Attack Surface Analysis of Advanced Metering Infrastructure.

Ghansah, I. (2009). Smart Grid Cyber Security: Potential Threats, Vulnerabilities And Risks. PIER Energy- Related Environmental Research Program.

Greveler, U., et al. (2012). Multimedia Content Identification Through Smart Meter Power Usage Profiles. Computers, Privacy and Data Protection. Brussels, CPDP 2012.

Hua, S. (2017). Wie China die Gesichtserkennung schon nutzt. Handelsblatt. Berlin, Verlagsgruppe Handelsblatt.

Huang, R., et al. (2017). Promoting Citizen's Learning Experience in Smart Cities. Blended Learning. New Challenges and Innovative Practices: 10th International Conference, ICBL 2017. S. K. S. Cheung, L.-f. Kwok, W. W. K. Ma, L.-K. Lee and H. Yang. Hong Kong, China, Springer.

IEA (2015). Energy Technology Perspectives 2015. Paris.

Jayachandran, P. (2017). The difference between public and private blockchain, IBM Blockchain Blog. 2017.

Kumar, A. (2015). "Dubai Now Under Blanket Surveillance by CCTV Cameras." Retrieved 14 Nov, 2017, from https://www.ifsecglobal.com/dubai-now-blanket-surveillance-cctv-cameras/.

Lyotard, J.-F. (1993). The Postmodern Condition: A Report on Knowledge. Minneapolis, University of Minnesota Press.

Maltese, I., et al. (2016). Smart City, Urban Performance and Energy. Smart Energy in the Smart City. R. Papa and R. Fistola. Cham, Springer International Publishing.

Rodríguez Bolívar, M. P. (2015). Smart Cities: Big Cities, Complex Governance? Transforming City Governments for Successful Smart Cities. M. P. Rodríguez Bolívar. Cham, Springer**:** 1-7.

Rutkin, A. (2016). Blockchain-based microgrid gives power to consumers in New York. New Scientist.

Sadowski, J. and F. A. Pasquale (2015). "The spectrum of control: A social theory of the smart city." First Monday **20**(7).

Singer, N. (2012). Mission Control, Built for Cities: I.B.M. Takes 'Smarter Cities' Concept to Rio de Janeiro. The New York Times. New York.

Urjanet (2015). "The Geographic Adoption of Commercial & Industrial Building Smart Meters in the United States." Retrieved 13 November, 2017, from https://urjanet.com/resources/the-geographic-adoption-of-commercial-industrial-building-smart-meters-in-the-united-states/.

US-CERT (2016). "Alert (TA16-288A): Heightened DDoS Threat Posed by Mirai and Other Botnets." Retrieved 14 Nov, 2017, from https://www.us-cert.gov/ncas/alerts/TA16-288A.

van Zoonen, L. (2016). "Privacy concerns in smart cities." Government Information Quarterly **33**(3): 472-480.

9 783981 855838

Art.-No.: 9236

www.dena.de

dena
German Energy Agency