The Future of IoT

Joern Ploennigs, John Cohn, and Andy Stanford-Clark, IBM

Abstract

The Internet of Things (IoT) is infiltrating many businesses. It provides simple means to collect and analyze technical system data to identify and optimize the performance of many things in our private and work lives. This technical revolution is also revealing new challenges and issues with our current IoT technologies. New solutions like Artificial Intelligence, Blockchain or 5G promise to overcome these challenges. Within this paper we discuss with leading experts the pros and cons of these technologies and what it means for the future IoT business.

Introduction

IoT is a broad field with many different technologies and applications reflected by the variety of questions and opinions people have about IoT. Within this article we want to discuss some of these questions and review the current state and future of IoT. To echo the variety of opinions, the paper is written as a panel discussion with three experts in IoT. First, we want to introduce our panelists: John Cohn, Andy Stanford-Clark and Joern Ploennigs.

John is an IBM Fellow for IoT and the technical lead at Watson IoT headquarters and now delegate for the IBM AI collaboration with MIT. His background is originally in semiconductors, and he has been building things from small devices to large robots for years. He is one of the first advocates of blockchain for IoT, which he promoted in 2014 when blockchain was largely unknown in this space [2].

Andy is one of the creators of the MQTT protocol, the most common communication protocol in IoT. In addition to his extensive experience in standardization, he is also very hands-on. He has been building IoT solutions for years and IoT-tized his own house in 2000 with MQTT. He is now the CTO for IBM UK and Ireland and rolling out large IoT solutions for clients.

Joern is working at IBM Research on Artificial Intelligence (AI) solutions for IoT and Digital Twin. He combines semantics with machine learning and intuitive user interfaces to automate IoT systems and increase their usability. He is a board member of the IEEE IoT Initiative and active in many conferences in the areas of IoT and AI.

Where is the Value in IOT?

Joern: Let start the discussion with a simple question. Andy, where do you see the value in the Internet of Things?

Andy: IoT allows monitoring and actioning at a distance. It is about knowing about what is happening in a place that one is not. Some ideas for applications go back to Bill Gates' book, *The Road Ahead* [1]. Applications can be a simple thing like getting notifications when the bus is coming. This leads to an improved perceived quality of life for people. IoT makes our lives better in subtle ways.

Joern: This is the idea of ambient intelligence [4]?

Andy: It is similar. The important difference in IoT is that we measure things not only in the environment but also at a distance. We called it remote telemetry in the past.

Joern: I see this value, but don't we already have this?

Andy: It is the amount of data that gets richer and the ability to interpret multidimensional datasets from sensors at different places with machine learning and AI that leads to deeper insights. For businesses this turns data into gold.

John: This will, in particular, have a large impact on industrial production. We started with automation in industry in the 80s. IoT is the next evolution that allows us to automatically configure the production from digital twin models and produce more individualized products. This is the Industry 4.0 value proposition and will lead to increased production efficiency.

Joern: I agree that there will be big societal value in building bigger and more resilient systems with IoT.

John: Also, more customized systems. We see this in the maker space. Here now people can easily build things at home that were reserved to experts in the past. The same happens in industry across domains. IoT makes it easier and cheaper to measure many things and allows us to instrument everything. The value for the customer is that he has more information available. For the business the value is that they do not have to send people with a checklist to collect information across the supply chain.

Joern: Of course, there is value in this. But does just collecting the data create enough business value?

John: There was a recent study [3] that showed that this is currently changing across the IoT industry. In the last few years, most companies only focused on instrumentation. They now have collected the data and look stronger into analytics. The value of IoT is in deriving actionable insights that allow us to optimize business processes. By following some design guidelines as shown in Fig. 1, it is easier to create value. Business value derives from combining and analyzing IoT data from different sources. These data have to be continuously available from a secure, resilient and flexible architecture. Only then can value be holistically delivered.

Andy: Value needs to be well designed. There is a risk that people are too technology centric and do things only because it is technically feasible. They do not think about what the problem is they want to solve. As a result, many developments are just experimental, like smart toothbrushes, and the world will decide what we need.

Joern: There are many more important problems that we need to solve, like climate change and resource limitations. Is IoT not providing us the sensors to measure energy consumption and evaluate and optimize the performance of our systems?

John: To address these problems, we know that collecting the data is necessary and that analytics help derive value. Now is the time when we have to really deliver on the value and roll this out everywhere.

Joern: In summary, IoT solutions can improve the quality of life and productivity, and also help save energy and the planet. There are recipes that we can follow to design good solutions that help us to deploy scalable IoT solutions. We will come back to these aspects later in the discussion.

Where are we on the Hype Cycle?

Joern: People often ask me if IoT is hyped and if they can trust that it will grow further and lead to substantial business. What is your answer to this question?

Andy: A very good model for this is the Gartner hype cycle for IoT [7]. The Gartner hype cycle describes the hype around a technical development. It divides it into an initial phase where

Editor's Note: Text appearing in bold indicates a live link in the online version.

Digital Object Identifier: 10.1109/IOTM.2018.1700021

expectations are overhyped. This is followed by a phase of disillusionment where people realize that not all promises come true and then a slope of enlightenment, where productive technologies are established.

John: This is exactly the right model. In IoT we are now at the top of the hype and people have started realizing that it is not about getting the data and connecting it to the cloud. To derive value, they need to analyze the data. Our goal is to help them shorten the trough of disillusionment and move quickly into the enlightenment zone.

Joern: What are our tips to do this?

John: Always start from the business problem. IoT is not the answer looking for a problem. You should start with the business problem, and when you find the way to IoT then it will have lasting value. Not to say that we do not have miraculous innovations. Digital assistants are a good example of a product group that we did not know that we needed, and now they are indispensable.

Joern: But is it a good idea to always start with a business problem or are we are not just solving incremental problems?

John: There should be a proper balance between both. You should not close out any breakout innovations, but they are harder to plan for. If you want to create value intentionally, then people should start backwards from business problems.

Joern: Is the combination of IoT and AI not one of the future breakout innovations as it is enabling new approaches to learn from data? IoT created new ways to collect data. Similarly, AI is changing how we use machine learning. Both together allow us to automatically derive insights and predictions [5] to further optimize the IoT system. This leads step by step to a self-learning Digital Twin of the IoT system that understands its internal function, as shown in Fig. 2. This will build the foundation of Augmented Intelligence systems that assist us in operating complex systems, if not having them operate autonomously.

John: Yes, AI is one of the upcoming innovations in IoT and will change the maturity of IoT to become one part of many in future solutions.

Andy: As someone who grew up with IoT, this is a major change as there are not many pure IoT things anymore. IoT is still treated as something special, but in the future, it will just embed in all processes and become a part of many business architectures.

Joern: So, IoT isn't just hype. In your experience, it adds value to many business processes. Your advice is to see it not in isolation as a singular solution, but rather to analyze what business value it can add to improve existing processes.

What are the Risks For IoT?

Joern: What are the risks in IoT that could lead to a deeper trough of disillusionment?

Andy: One common thing is that people just consider the capability of collecting data, and they are missing business questions. Second is that people think that IoT is easy. They do not consider technical challenges in connectivity, battery life, and analytics. Finally, there is the cost of implementation that can still be large if one wants to roll out solutions globally. We have already discussed several of these things above.

John: I think that privacy is a huge concern. Besides this, we have complexity and robustness. Finally, pushing for standardization is an issue.

Andy: Privacy and security are big issues as people only hear about the security issues of IoT and forget about the benefits.

John: These are the things that lead us into the trough of disillusionment. The data collected by IoT is where the value of IoT is, and we need to protect it. We worry a lot about security and the danger of people hacking IoT systems like a car. That certainly can happen, like the Mirai bot net attack on web cams [6]. But the real danger is about data privacy and that we are sacrificing too much of our own information for no value. Systems will find out more about us than what we intended to reveal.

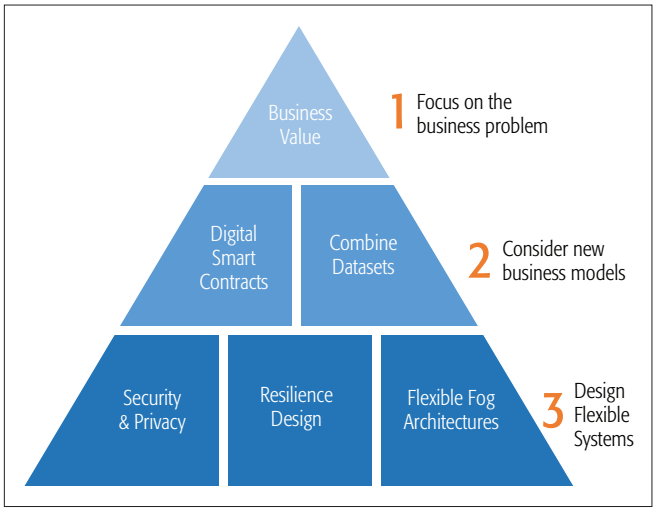


FIGURE 1. Principles to derive business value from IoT.

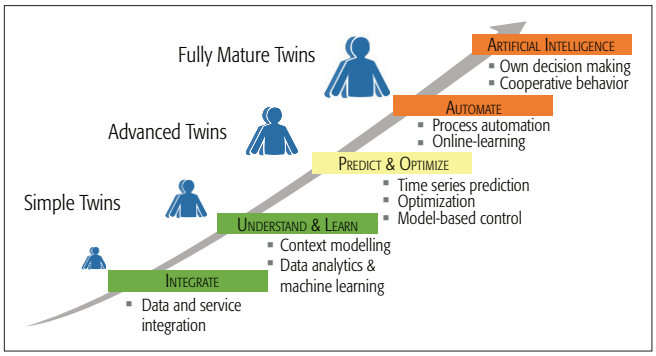


FIGURE 2. Digital Twin as an enabler for AI.

Joern: You can, for example, identify the program people watch on TV by just analyzing the TV's energy consumption [8].

John: Exactly. On the one hand, there are technical things that we can do like ensuring data encryption end to end starting at the edge, that the right data policies are in place and that data is managed according to laws like GDPR [9]. On the other hand, we need to make people aware of what data they share, with whom they share, and how it is used. When we can protect their data and put them in control of it, then it also opens ways for them to use it in a positive way and trade it for services that provide them insights, like how we trade our information in the Internet for search results.

Andy: Data in IoT is a two-sided sword with privacy on one side and business value on the other. I agree that we do not pay enough attention to it and a couple of bad privacy and security examples may slow down the adoption of IoT. Therefore, we all need to get better control of our data and we also need to get value for sharing it. Companies are currently overvaluing the data they have and are only thinking of ways they can sell it. We need to find neutral ways of exchanging the data.

Joern: The question is if the data that we collect in IoT is really that valuable and privacy-invasive. Isn't the data we share with our Google search history or our Facebook social network more dangerous as it is much easier to build personal profiles from it [10] as it contain many kinds of private data?

Andy: The difference there is that it is free, and people forget that the associated cost for the service needs to be earned.

John: I think that most people are aware that they are giving away data, and hopefully, they also understand the potential consequences from cases like Cambridge Analytica. With IoT it is different as it is not that obvious anymore. Take an IoT microwave for example. From the usage of the microwave the manufacturer might learn when you are home, when you eat,

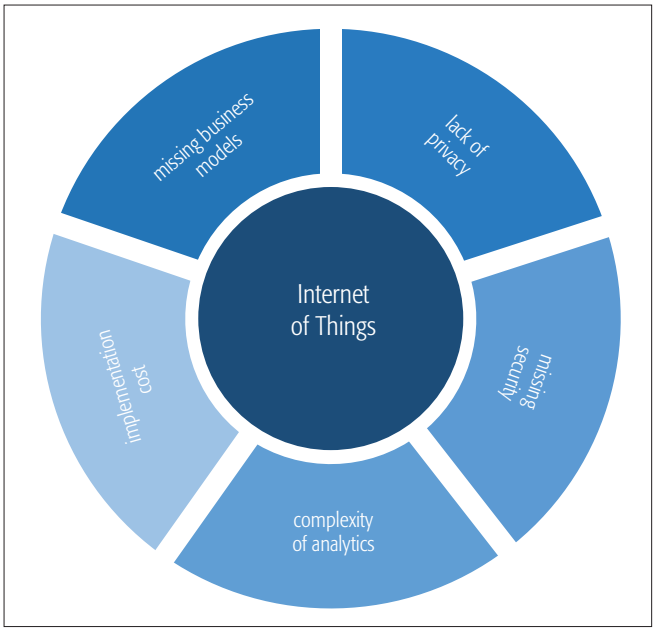


FIGURE 3. Challenges in the Internet of Things.

and what you eat. He might want to sell this data to your health insurance company. The question then is: Who owns this data? Because the manufacturer builds your microwave, does that give him the right to own the data and insights? As another analogy, if someone builds your house, does he keep a key?

Joern: You are right, and the manufacturer should not have the right to the data. The question is generalizable beyond IoT. With the advancements in technology it becomes easier to monitor our lives from many perspectives and we lose control of our data. For example, it is hard to buy a phone that allows you only to make calls. Similarly, it will be hard to buy a microwave that is disconnected.

John: It will be a case of "buyer beware," where people need to make informed choices about the usage agreements they blindly sign. The other side must be legislated, like GDPR, which ensures users' rights like the right to be forgotten, that gives me the right to demand that my data is removed.

Joern: But the issue is that we are not necessarily aware that we provide data.

John: That is the whole problem. With Google you are signing conditions of use, and you are kind of aware of the data you provide. With IoT you are not signing anything and the IoT device is gathering data all the time.

Joern: So we face multiple challenges in IoT, as shown in Fig. 3, to avoid the trough of disillusionment. Most important is that we need to make people more aware of what data they share and we need technical solutions to put them in control of who and for what use they are sharing the data.

How Will Blockchain Change IoT?

Joern: How will technologies like Blockchain change IoT and give us, for example, control over our data?

John: Blockchain is a very flexible technology with many use cases. At its core, it creates a digital ledger in which each transaction that is put into this ledger is encrypted, verified and signed by trusted entities. This creates the first benefit where each transaction is verified and certified with cryptographic keys. The second benefit is that all old transactions are kept in the ledger such that one can always trace back the history of the transaction. This creates a chain of trusted transactions that nobody can modify without breaking the cryptographic code. In the banking industry, it allows banks to trust electronic transactions. In IoT, it allows us to encrypt data at its source and protect it through its life cycle. As the data is encrypted, it can-

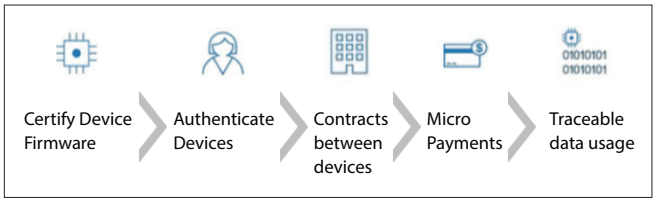


FIGURE 4. Blockchain as universal digital ledger for various IoT transactions.

not be accessed without permission through a smart contract, and every access to the data is logged on the blockchain and is therefore transparent for the user. The blockchain can be further used to implement micro-transactions to pay for data usage such that a full business model can be implemented. This gives individuals more control and gives enterprises ways to monetize the data during the life cycle, as shown in Fig. 4.

Andy: There are already applications of Blockchain for supply chain management. For example, for deep frozen goods you have to ensure that the cold chain is never broken. IoT can monitor this, and every transport company signs the blockchain with IoT data as proof that it handed over the goods in good condition. This creates transparency along the whole supply chain [17].

Joern: I agree that this distributed nature of a Blockchain is very promising and technically feasible nowadays [11]. But IoT is machine-to-machine communication, and we explicitly exclude the human with this definition. Thus, the idea that we have full control of our data is an illusion as we are not part of the process. Will blockchain not enable the IoT device to just sell data to whoever wants to pay for it?

John: This is a matter of contract design and a device should not act autonomously. What I mean is that I as an owner can switch the aftermarket maintenance provider for my system and decide what data I provide. I want to keep contractual flexibility if a service provider goes out of business. Blockchain allows you to define a contract that ensures that the data remains yours and is traded only with your permission.

Joern: I agree that blockchain and smart contracts give us more flexibility than what we have today. Still, how does it work? Is this increased flexibility not overwhelming us? Similarly, the many privacy settings we have now on our phones have become very hard to use. Can we as users really manage this or will we end up blindly signing extensive usage agreements?

Andy: There are two points here. One is about the democratizing of the participants in a multi-way contract, and by that I mean a traditional contract, written in English, and negotiated by humans. The contract and its addendums and modifications and agreements and endorsements and signings are all committed as immutable documents onto a blockchain.

The other point is about smart contracts, which as many people are realizing are very hard to articulate accurately, and once a computer gets involved with executing them and that execution becomes immutable with no "compensating transaction," then you are opening the way to all sorts of problems. Smart contracts are code, and code has bugs that need to be identified and fixed.

John: This means that blockchain in IoT needs to be simple and self-managing. When we build in all these possibilities, it should not translate into complexity. The devices need to address the skill level of the people. What we need are simple protocols for transactions and also for verifying device authenticity and finding them in the Internet, like a search engine for devices and their services.

Joern: You think we need something of a global registration office for devices and services?

John: We need discoverability in a universal registry that lists the functionality, owner, status, and rights. Then devices can

search and negotiate with their own service providers and look them up. This is a core element of the device democracy idea [2]. The negative thing is, this could become big brother.

Joern: We can avoid big brother with a distributed blockchain registry, as then nobody would know everything, and it also scales better [12]. To summarize the discussion, we know that blockchain allows us to manage access to private and valuable data and solve several data privacy issues. It further enables smart contracts that can realize completely new and more flexible business models around services for devices.

Will AI Change Everything?

Joern: We already discussed that the true value in IoT lies within the created insights. Will AI create completely new value propositions for IoT?

Andy: AI will allow us to derive insights more easily and automate these processes. Particularly for computer vision, the new AI approaches around Deep Learning (DL) are enabling completely new solutions. These are core technologies for autonomous vehicles and also for improving product quality by detecting anomalies in production [18]. However, AI is also adding layers of complexity. In the past we could go through lines of code to understand how it works. The increasing use of DL networks changes this as they are hard to interpret. The more widely DL is used the more problematic this aspect becomes.

Joern: This is one of the greatest challenges that we face in AI. Many practitioners don't want to trust a system that they cannot interpret and thus not understand. Therefore, AI has to become more transparent and capable of explaining itself to build trust and credibility. This is one of the reasons people have doubts about autonomous vehicles. It is not only technically challenging, people simply do not trust a system that they do not understand. Therefore, we are working on technologies that make DL networks more understandable and also improve their training performance.

John: One of the issues must be that devices sort out their own problems. In the distributed systems, we do not have the unified world of the past. This makes it harder to report issues and to build in resilience, in particular in the application of AI for differentiating normal from not normal operation. AI can be used in security to identify what is normal, such as usage patterns that were seen before, or to detect security issues from abnormal patterns. The other day we were looking into the sensors in our IoT headquarters in Munich to build a predictive maintenance solution for Maximo Asset Health Insights. When we looked into the data there were periods of missing data across all sensors, which turned out to be periodic WiFi outages. AI could identify these patterns.

Joern: AI can certainly correlate the data of the WiFi to diagnose the problem. An important function of AI will be to run such analytic tasks and then assist the user in solving the problem. This ensures that the human remains the decision maker and the AI is the helper.

John: There is a theme here in designing for resilience. AI systems have to be understandable; they have to explain their actions, ask for what they need, and point to problems or fix them. Otherwise, we will never manage the complexity of 50 billion IoT devices in the coming decade. AI is just one of the tools.

Joern: It is curious, that while we are facing this growing volume of data, our mobile user interfaces are actually getting smaller and can display less data, as shown in Fig. 5. Automated machine learning and AI are the only way to summarize this data [5] and point to the relevant insights. Many actions need to be automated by the systems and the systems need to be self-diagnosing, self-healing and self-sustained while just serving me rather than bothering me with all kinds of requests.

Andy: This also needs to extend to the system design. Now we have 3rd generation programming languages and compilers

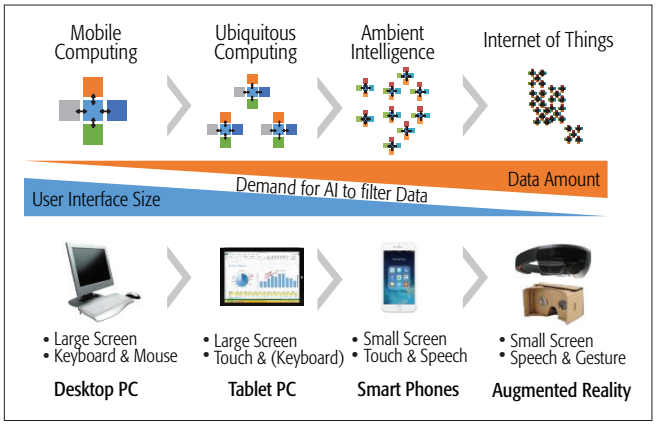


FIGURE 5. Evolution of IoT Devices vs User Interface technologies and the resulting demand for AI to filter the large amount of data onto smaller screens.

that allow us to write programs that we could never have written in machine code. Our tools need to further evolve to help practitioners design autonomous AI solutions that process the data.

Joern: When IoT systems are self-healing and autonomic, don't we end up with Skynet?

John: I am not as worried about Skynet as I am worried about Bedlam. Skynet is less concerning than an unmanageable collection of things that stop working due to lack of robustness.

Joern: So no matter what we do, we end up in both cases with a system that we cannot control for better or worse?

Andy: That is not going to happen. People will turn off the systems when they realize they have gone too far. Like when they switched off the self-learning chatbots that insulted people. We will always be in control of the power switch.

Joern: This is a good conclusion. We should focus on understandable and resilient approaches for AI. Then AI will help us in many ways to deal with the large amount of IoT data and to derive true value from it.

Can we Standardize IOT?

Joern: We have had interoperability problems in communication networks since the beginning. Technological development is usually two steps ahead, and once a standard is defined another new one is already emerging. Within IoT we face the same challenge as we need to connect legacy devices and new device types into one system where we can also run analytics across the created data. What do you think is the role of standardization?

John: There is no single solution to the interoperability problem. It might be good to adapt some paradigms from security: "Any security system that believes that it is invulnerable is already flawed." They have to assume they are already compromised and need to develop robust strategies to deal with this and live with the fact that it is not perfect. The same is true with interoperability. The idea that in the future we have a universal standard that solves these problems will not work. We need to design systems that can deal with interoperability issues and device diversity rather than hoping for uniformity.

Joern: On the protocol level we have some standards like MQTT that Andy worked on. This is one of the most commonly used protocols in IoT.

Andy: MQTT provides a very efficient and lightweight container for device messages. However, it is the content of these messages that is important and their semantics are not very well regulated. We need to resolve this for coexistence of devices. Also, the Internet is designed for diversity of many different protocols from HTTP to email to video. It works because all protocols coexist and

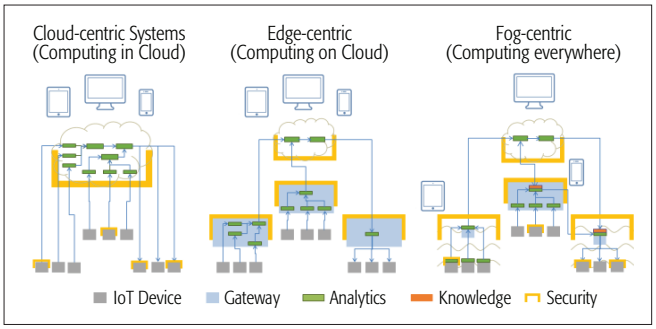


FIGURE 6. Comparison of cloud-, edge- and fog-computing architectures.

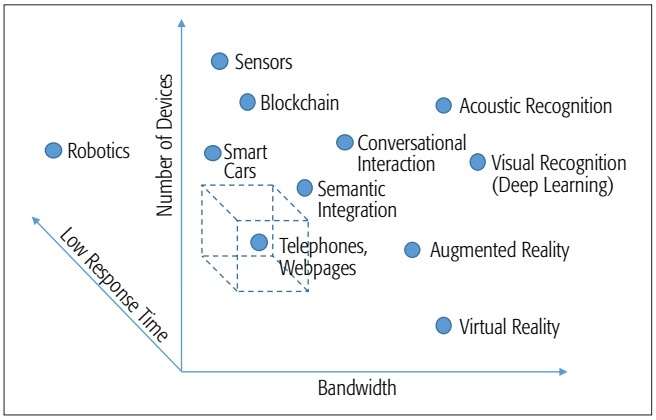


FIGURE 7. Communication requirements of IoT applications.

support the same communication layer TCP/IP. We need something similar for IoT.

John: Semantics will play a central role in this. That is why self-describing systems like Hypercat [14] and semantic domain models like Brick [15] can be helpful. They allow us to create a taxonomy of sensor types that are generalizable across devices and services. AI can be used to map legacy systems to these models and then the whole analytic process can be automated afterwards [5]. On top of this, we need to create standards that control the emergent behavior and robustness of the system and enable systems that can tolerate non-standard inputs.

Andy: We are moving in the right direction. Fully solving this problem is NP-complete. We just don't have the answer to all the questions. We have to start on the problem side and then define what we need. For robustness, we need to have defensive programming that can deal with issues. If a device is missing in the field, then the system should use defaults and keep working. Programmers today don't necessarily consider the robustness, scalability and defensiveness of the solution. If the chaos monkey hits the system, it might lose some nodes, but it is still carrying on and this is intrinsic to the system design.

Joern: Isn't this something that should be covered by the programming language? As a programmer, I want to concentrate on the high-level functionality and these defensive mechanisms are common patterns that can be generated by my compiler.

Andy: Programming tools for IoT need to grow up to handle this. Things like Kubernetes in the cloud already do this and build in redundancy in deploying the system. We need a similar solution for IoT.

Joern: To summarize, standardization may not resolve all interoperability issues in IoT. However, there are many topics that need to be addressed from self-description models to semantic domain models that are essential to automate analytics in IoT. Also, more robust and flexible programming models are needed to create resilience and secure systems.

From Cloud to Edge and Fog Computing and 5G

Joern: Edge computing is discussed by many people as a core enabler of IoT as it allows processing at the edge where the devices are. Therefore, not all data needs to be sent to the cloud, which reduces communication costs and improves robustness and privacy. What are the challenges for edge computing in IoT?

John: We are going to need something like Kubernetes to deploy our analytics at the edge. Kubernetes allows us to easily deploy and manage containerized applications in the cloud. It allows us to easily scale a solution by starting new containers or to deploy a new version of the code. We need something similar for edge systems.

Andy: Particularly when we think about putting the analytics near the data sources. This would allow us to create more robust solutions. This way each edge system can learn its own customized ML and AI models from all available data and only send out aggregated results. To do this, we need to extend analytic workflow tools that we have in the cloud to include the edge and form a fog of edge and cloud. The question is then, how we can split up our algorithms into components that can be sent and distributed in the fog?

Joern: Aren't the current IoT systems designed oppositely, where the devices are rather simple and send all their data to the cloud? Figure 6 compares the common cloud-centric architecture with an edge-centric one where the processing happens at the edge. The fog-centric architecture merges both approaches and provides flexibility to deploy processing in the cloud or at the edge. However, we are far from this flexible fog design.

Andy: This is just a point in time. The history of communication networks has always iterated between centralized and distributed architectures. We are rapidly moving to a stage where the sensors get more sophisticated and create so much data that we cannot stream it all into the cloud.

John: There are many reasons why one wants to do edge analytics, ranging from latency and bandwidth cost to robustness and resilience, and to privacy and law compliance. There is a great need for standardization in this space too.

Joern: Isn't this demolishing some benefits of IoT? The current beauty of cloud-centric architectures is that they are so easy to deploy. In the past of distributed sensor networks, I had to configure and connect individual devices. Nowadays, I only turn on my device, connect it to the Internet, and I am done.

Andy: With low-power wide range networks [16] it becomes even more simple as we only need to turn it on.

John: The big game changer will be 5G. You do not need to give up bandwidth for low power and universal reach.

Andy: People dangle 5G, like blockchain, as a solution to all problems. The sweet spot for IoT is the ubiquitous connectivity at low bandwidth, and low-power wide range IoT networks are already establishing in the market.

Joern: Both technologies will prevail as we have different communication requirements in IoT, as shown in Fig. 7. 5G will give us a wider range of bandwidth to choose from, and therefore, the ability to create more flexible fog architectures that combine the benefits of edge and cloud architectures and support a wider range of use cases.

Conclusion

Joern: To summarize the discussion: We assessed that the value of IoT is not only in collecting the data, but in building business cases where the insights from analyzing data are creating additional value. We further discussed the hype curve of IoT and identified that we are currently at the top of the hype and that we need ways to quickly pass through the trough of disillusionment. Therefore, it is essential to resolve the data security and privacy issues. Blockchain is one approach to secure

data and regulate data access. It further allows us to build new business models around smart contracts allowing more flexible transactions. Further, we said that standardization might not fully solve the underlying problems in interoperability and that we also need more semantic domain models and better programming tools to really resolve the data security and privacy issues. Within all these points, we discussed pros and cons of the underlying technologies. Extrapolating this to the future: How will IoT look in 20 years? Will IoT then be a bionic implant or a brain interface?

Andy: Maybe we will have those, but this will not be called IoT anymore. IoT will just be part of the enabling infrastructure in the same way a wireless communication or battery is today.

John: The miniaturization in IoT will continue and will lead to a huge explosion of very simple devices. This will allow us to integrate IoT in more systems and processes and lower the cost of their operation. It will also create new problems like the management of so many assets that we will need to address.

Joern: So we will not be out of a job?

John: Definitively not. It is a great time to be a nerd!

References

[1] B. Gates *et al.*, *The Road Ahead*, 1995.

[2] P. Brody, V. Pureswaran, and J., Cohn, "Device Democracy: Saving the Future of the Internet of Things," *IBM*, Sept. 2014.

[3] IDC European Vertical Markets Survey, 2015, 2016, and 2017.

[4] C. Ramos, J. C. Augusto, and D. Shapiro, "Ambient Intelligence — the Next Step for Artificial Intelligence," *IEEE Intelligent Systems*, 23.2, 2008, pp. 15–18.

[5] J. Ploennigs, "Automating Analytics: How to learn Metadata Such That Our Buildings Can Learn from Us," *SECON Wksps. — 2016 IEEE Int'l. Conf. Sensing, Communication and Networking*, 2016.

[6] E. Bertino and N. Islam, "Botnets and Internet of Things Security," *Computer*, 50.2, 2017, pp. 76–79.

[7] A. Velosa, W. R. Schulte, and B. J. Lheureux, *Gartner Hype Cycle for IoT*, 2017.

[8] U. Greveler *et al.*, "Multimedia Content Identification Through Smart Meter Power Usage Profiles.," *Proc. Int'l. Conf. Information and Knowledge Engineering (IKE)*, The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2012.

[9] J. P. Albrecht, "How the GDPR Will Change the World," *Eur. Data Prot. L. Rev.*, 2, 2016, p. 287.

[10] A. Nosko, E. Wood, and S. Molema, "All About Me: Disclosure in Online Social Networking Profiles: The Case of FACEBOOK," *Computers in Human Behavior*, 26.3, 2010, pp. 406–18.

[11] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, 2016, pp. 2292–303.

[12] M. Divya and N. B. Biradar, "IOTA-Next Generation Block Chain," *Int'l. J. Engineering and Computer Science*, 7.04, 2018, pp. 23823–26.

[13] J. Ploennigs, A. Ba, and M. Barry, "Materializing the Promises of Cognitive IoT: How Cognitive Buildings are Shaping the Way," *IEEE Internet of Things J.*, 2017.

[14] M. Blackstock and R. Lea, "IoT Interoperability: A Hub-Based Approach," *IEEE Int'l. Conf. Internet of Things (IOT)*, Oct. 2014, pp. 79–84.

[15] B. Balaji *et al.*, "Brick: Towards A Unified Metadata Schema for Buildings," *3rd ACM Int'l. Conf. Systems for Energy-Efficient Built Environments*, 2016, pp. 41–50.

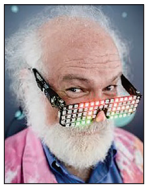
[16] L. Krupka, L. Vojtech, and M. Neruda, "The Issue of LPWAN Technology Coexistence in IoT Environment," *Int'l. Conf. Mechatronics-Mechatronika*, Dec. 2016, pp. 1–8.

[17] H. T. Vo, H. Kundu, and M. Mohania, "Research Directions in Blockchain Data Management and Analytics," *21st Conf. on Extending Database Technology*, 2018.

[18] B. Bhattacharjee *et al.*, "IBM Deep Learning Service," *IBM J. Research and Development*, vol. 61, no. 4, 2017.

Biographies

Joern Ploennigs [M'04, SM'17] (Joern.Ploennigs@ie.ibm.com) leads the team on AI 4 Digital Twins at IBM Research — Ireland. He works on several aspects of enriching IoT by AI including machine learning, semantic reasoning, and natural interfaces to enable autonomous, highly scalable, and accessible IoT solutions for a sustainable future. Prior to joining IBM in 2012, he was leading a junior research group on Energy Design of CPS at Technische Universitaet Dresden, Germany, as well as the data analytics group in the Irish strategic research cluster ITOBO as a Feodor-Lynen fellow of the Humboldt-Foundation. He holds a master in electrical engineering for automation and control and a Ph.D. and a Habilitation in computer science from Technische Universitaet Dresden. He is a program committee member of several renowned international conferences and journals and board member of the IEEE IoT initiative.



John Cohn is an IBM Fellow and is now at the MIT/IBM Watson AI lab. Previously he was technical lead at the Watson IoT headquarters in Munich. There his focus is on physical infrastructure for IoT, open data, Internet of Things communications and real-time data analytics. Before joining the IoT Division, he was an innovator in the area of design automation for both analog and digital custom integrated circuits. He received his undergraduate degree in electrical engineering at MIT and earned a Ph.D. at Carnegie Mellon University. In 2005 he was elected a Fellow of the IEEE in recognition of his contributions to the design automation for high performance custom circuits. He has authored more than 30 technical papers and has contributed to four books on design automation. He has more than 100 patents in the field of design automation, methodology, circuits and smarter systems.

Andy Stanford-Clark is the Chief Technology Officer for IBM in the UK and Ireland. He is an IBM Distinguished Engineer and Master Inventor with more than 80 patents. Andy is based at IBM's Hursley Park laboratories in the UK and has a long background in Internet of Things technologies. He has a BSc in computing and mathematics and a Ph.D. in computer science. He is a visiting professor at the University of Newcastle, an honorary professor at the University of East Anglia, an adjunct professor at the University of Southampton, and a Fellow of the British Computer Society.